UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA
CENTRO DE POSTGRADOS

MAESTRÍA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

ELABORACIÓN Y PLAN DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADAS A UNA EMPRESA INDUSTRIAL DE ALIMENTOS

Tesis de titulación previa a la obtención del título de Magister en Gestión Estratégica de Tecnologías de la Información

Autor:
Ing. Franklin Mauricio Arévalo Moscoso
C.I. 0102868080

Directora:
Ing. Irene Priscila Cedillo Orellana Ph.D.
C.I. 0102815842

CUENCA - ECUADOR
2017

Resumen

En las empresas industriales de alimentos, existe información crítica para este tipo de organizaciones, como los datos de sus clientes, proveedores, transacciones diarias y las características principales que definen un producto como son sus recetas, proceso de fabricación, costos, etc. siendo necesario que toda esta información este resguardada confiablemente ante los posibles riesgos que se puedan materializar en cualquier momento.

Para proteger los sistemas de información de los crecientes niveles de amenazas cibernéticas, las organizaciones actualmente tienen la necesidad de establecer programas o proyectos de seguridad informática y, debido a que las políticas de seguridad de la información son una base necesaria de los programas de seguridad organizacional, existe una necesidad de contribuciones académicas en esta área.

Por ello se plantea en el presente trabajo una investigación en temas relativos a la seguridad de la información, gestión de riesgos y políticas de seguridad informática para posteriormente plantear un método adecuado consistente de 3 etapas y un total de 9 pasos para el desarrollo y difusión de políticas de seguridad a partir de la identificación de los posibles riesgos y vulnerabilidades que presenta una organización o un área de la misma, seleccionando los controles más adecuados de la norma ISO/IEC 27002, la cual es una guía aceptada internacionalmente de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información para una organización.

La aplicación de la metodología propuesta se la realiza como un caso de estudio en el departamento de producción de una empresa industrial productora de alimentos en la ciudad de Cuenca - Ecuador. Éste trabajo puede servir como referencia a otras empresas industriales de alimentos que requieran elaborar de manera técnica y apropiada sus políticas de seguridad de la información; sin embargo también podría servir en empresas de diversos tipos, realizando las validaciones correspondientes y su aplicación.

Palabras Clave: seguridad de la información, análisis de riesgos, políticas de seguridad, ISO 27002.

Abstract

In industrial food companies, there is critical information for this type of organizations, such as the data of their customers, suppliers, daily transactions and the main characteristics that define a product such as their recipes, manufacturing process, costs, etc. being necessary that all this information is reliably guarded against the possible risks that may materialize at any time.

To protect information systems from increasing levels of cyber threats, organizations currently have the need to establish computer security programs or projects and, because information security policies are a necessary foundation of organizational security programs, there is a need for academic contributions in this area.

For this reason, a research and review of topics related to information security, risk management and computer security policies is proposed in this work to later propose an adequate method consisting of 3 stages and a total of 9 steps for the development and diffusion of security policies based on the identification of the possible risks and vulnerabilities that an organization or an area of the organization presents, by selecting the most appropriate controls of the ISO / IEC 27002 standard, which is an internationally accepted guide of good practices that describe the control objectives and recommended controls regarding the security of information for an organization.

The application of the proposed methodology is carried out as a case study in the production department of an industrial food production company in the city of Cuenca - Ecuador. This work can serve as a reference to other industrial food companies that need to elaborate in a technical and appropriate way their information security policies; however, it could also be used in companies of different types, making the corresponding validations and their application.

Keywords: information security, risk analysis, security policies, ISO 27002.

Índice

Índice de Figuras

Índice de Tablas

Cláusula de Propiedad Intelectual

Franklin Mauricio Arévalo Moscoso, autor/a del trabajo de titulación "Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 30 de noviembre de 2017

Franklin Mauricio Arévalo Moscoso

C.I: 0102868080

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

Franklin Mauricio Arévalo Moscoso en calidad de autor/a y titular de los derechos morales y patrimoniales del trabajo de titulación "Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 30 de noviembre de 2017

Franklin Mauricio Arévalo Moscoso

C.I: 0102868080

Agradecimientos

A mi directora de tesis, Priscila Cedillo, por su apoyo, paciencia, consejos, enseñanzas y ayuda en la elaboración de este trabajo.

A mi esposa Diana por su apoyo y comprensión incondicional siendo un pilar fundamental para el desarrollo de este trabajo y la culminación de mis estudios.

A mis hijos Victoria y Alejandro, por ser mi inspiración y motivación para llevar adelante mis proyectos.

A mis padres y suegros, por todo su cariño y ayuda incondicional brindados a mi familia.

A mis jefes y compañeros de trabajo, por su ayuda, comprensión y apoyo fundamental con este proyecto y con mis estudios.

En memoria de mi abuelita Victoria por su ejemplo y dedicación como mi inspiración.

Capítulo 1. Introducción

1.1. Motivación

Hoy en día, la información ha llegado a ser uno de los activos más importantes para la operación de una compañía; si esta información es bien usada y explotada se convierte en una ventaja competitiva y en una herramienta de soporte en la toma de decisiones y cumplimiento de los objetivos estratégicos de la organización; se hace por lo tanto necesario proteger adecuadamente dicha información, frente a posibles riesgos y vulnerabilidades de seguridad, identificando potenciales amenazas internas o externas que puedan afectar a los datos, equipos o a la continuidad del negocio. Los problemas de seguridad de la información, acarrean consecuencias muy graves para las empresas, que hoy en día, confían gran parte de sus procesos, operaciones, transacciones y decisiones estratégicas a su información y a los sistemas informáticos que la recopilan, procesan y almacenan. Las consecuencias pueden incluir pérdidas financieras y personales, pérdida de reputación y bases de clientes, problemas operativos, dificultad de expansión y la violación de las leyes y regulaciones del gobierno (Bosworth, Kabay, 2002).

Actualmente, según Eset (2017), debido al desarrollo de nuevas plataformas tecnológicas y la cambiante interacción entre ellas, la superficie de exposición de las empresas ha aumentado de manera significativa y esto implica que existe un mayor número de vectores de ataque que pueden ser utilizados para comprometer la seguridad de los datos; tal como lo demuestra un estudio de seguridad de la información en América Latina realizado por esta empresa de seguridad informática, donde se concluye que de un universo de 4500 empresas de todos los tamaños encuestadas en el 2016, el 49% sufrió ataques por malware, el 16% por ransomware, el 15% por pishing y el 10% por explotación de vulnerabilidades entre las amenazas más importantes. También se indica que el 31% de empresas encuestadas afirmaron no haber sufrido incidentes de seguridad, lo cual quiere decir que el restante 69% si los tuvo. En nuestro país Ecuador el estudio indica que de las empresas encuestadas el 45.6% tuvo ataques por malware y el 20.9% tuvo ataques por pishing. Los datos arrojados de este estudio también demuestran que los controles de seguridad más implementados en Latinoamérica son el antivirus con el 83%, el firewall con el 75% y el respaldo de la información con el 67%. (Eset, 2017). Entonces, a pesar de que en Latinoamérica existen empresas que destinan una parte de su presupuesto a la seguridad de la información y disponen de ciertos controles, todavía se tiene un porcentaje considerable de empresas que tienen problemas de seguridad, por lo que, la seguridad de la información ha sido en realidad un gran desafío para la mayoría de las organizaciones en nuestro medio y debe ser tratada de manera íntegra, con una adecuada identificación, análisis y gestión de riesgos, políticas de seguridad, criptografía, controles, equipos de seguridad perimetral e interna, capacitaciones, concientización al personal, etc.; de hecho, la seguridad de la información es un proceso continuo de gestión de riesgos

que cubre toda la información que necesita ser protegida (Barbosa Martins & Saibel, 2005).

Con la creciente presencia de las tecnologías de la información, hay una necesidad urgente para tomar las medidas de seguridad adecuadas, y la gestión sistemática de la seguridad de la información es una de las principales iniciativas para la gestión de TI; además, cuando se informa acerca de las brechas en la privacidad y la seguridad de la información, las prácticas fraudulentas y los ataques en los sistemas de TI en las empresas, su personal debe reconocer su responsabilidad en el cuidado de los activos de información (Disterer, 2013).

Para proteger los sistemas de información de los crecientes niveles de amenazas cibernéticas, las organizaciones actualmente tienen la necesidad y hasta obligación de establecer programas o proyectos de seguridad informática y, debido a que las políticas de seguridad de la información son una base necesaria de los programas de seguridad organizacional, existe una necesidad de contribuciones académicas en esta importante área (Knapp *et al.*, 2009).

Si bien existen varios estudios y trabajos realizados con respecto a la elaboración de políticas de seguridad para empresas comerciales (Posso, 2009), gubernamentales (Barragán *et al.*, 2011), financieras (Ramos *et al*., 2017), entre otras; sin embargo, considerando que cada una de las organizaciones tiene sus especificidades y problemas propios de su operación, se hace necesaria la investigación de los posibles problemas y soluciones relacionados con la seguridad de la información de una empresa industrial de alimentos en particular; la que por su naturaleza, necesita su propio modelo para la identificación de riesgos, elaboración y plan de implementación de políticas de seguridad de la información. Se destaca además la importancia de tener modelos propios de gestión de seguridad de la información en las industrias: “La automatización de procesos brinda beneficios a la industria a medida que aumenta la cooperación entre las personas, pero también aumenta la vulnerabilidad de seguridad de la información. Como consecuencia, los modelos de gestión de seguridad de la información también tienen que cambiar.” (Dos Santos *et al.*, 2010).

En las empresas industriales de alimentos, la seguridad de la información es un tema crítico, dado que de ella depende la seguridad de los datos de sus clientes, proveedores, transacciones diarias y las características principales que definen un producto (su fórmula o receta, su proceso de fabricación, costos, etc.) siendo necesario que toda esta información esté a buen resguardo. Por otro lado y considerando que la información es uno de los activos más importantes de una empresa, su confidencialidad e integridad son temas cruciales que es necesario asegurar. Por tanto, es necesario que las organizaciones tengan políticas de seguridad de la información claras y bien definidas que representarán un insumo dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

Además es importante mencionar que en la bibliografía consultada en este trabajo de titulación no se establece un método claro y detallado para establecer políticas de seguridad de la información en

base a los riesgos de seguridad identificados y evaluados, y la selección respectiva de controles de la norma ISO/IEC 27002; siendo este el problema y necesidad principal que motivó el desarrollo del presente trabajo de investigación.

Por lo expuesto, en el presente trabajo se plantea una propuesta metodológica para la elaboración de políticas de seguridad de la información y su difusión, donde se ha escogido como base la normativa ISO/IEC 27002, la misma que contribuye con una guía de buenas prácticas que describe los objetivos de control recomendables en cuanto a la seguridad de la información, tomando también como base la metodología planteada por Knapp *et al.* (2009) y ciertas recomendaciones dadas principalmente por Barbosa Martins & Saibel (2005), Bustamante *et al.* (2017) y otros autores creando así una metodología adaptada a la realidad de las empresas industriales de alimentos en nuestro medio. El modelo de Knapp *et al.* (2009) involucra técnicas cualitativas y define un proceso general para la gestión de políticas de seguridad de la información, basado en las respuestas de una muestra de profesionales certificados en seguridad, definiendo así políticas de seguridad para un área o una empresa de una forma integral y distintiva de otros estándares profesionales o publicaciones académicas existentes; sin embargo este modelo no muestra el detalle y resultados de cada una de sus etapas y como lograr conseguir el objetivo de cada una de ellas; por lo que en el presente trabajo se pretende elaborar una metodología integral y completa con los procesos puntuales de desarrollo y difusión de políticas de seguridad de la información basado principalmente en la normativa ISO/IEC 27002, y en un alcance más detallado de 3 de las etapas planteadas en el modelo de gestión de políticas de seguridad que proponen Knapp *et al.* (2009), y en el aporte de otras recomendaciones realizadas por trabajos científicos y expertos en seguridad informática.

Para la identificación, análisis y evaluación de riesgos, etapa que forma parte de la metodología planteada, se toma como base una metodología de gestión de riesgos llamada Ecu@Risk (Crespo,2016), ya que se fundamenta en el análisis de las recomendaciones más importantes e instrumentos de otras metodologías aceptadas internacionalmente como Magerit, Octave-S, CRAMM y Microsoft Risk Management, alineadas con los estándares internacionales ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 y además se sustenta con el análisis de algunas leyes ecuatorianas para empresas de tipo MPYMES (Micro, Pequeñas y Medianas empresas) en nuestro medio, por lo que, con algunas modificaciones esta metodología se puede adaptar a las necesidades de las empresas industriales de alimentos.

En este contexto, se plantea una investigación y revisión de temas relativos a la seguridad de la información y a continuación se propone una metodología para el desarrollo y difusión de políticas de seguridad a partir de la identificación de los posibles riesgos y vulnerabilidades que presenta una organización o un área de la misma, seleccionando los controles más adecuados de la norma ISO/IEC 27002. La aplicación de la metodología propuesta en el presente trabajo de investigación se la realiza en el departamento de producción de una empresa industrial productora de alimentos en la ciudad de

Cuenca - Ecuador. Éste trabajo puede servir como referencia a otras empresas industriales de alimentos, en las que la interacción e involucramiento de los empleados junto con la cooperación y motivación de la alta dirección son factores claves para el éxito en la elaboración e implementación de las políticas de seguridad de la información planteadas.

Finalmente es importante destacar que para el desarrollo de este trabajo, se cuenta con la aprobación y apoyo de los directivos de la empresa, dado que ésta solución forma parte de los proyectos del plan estratégico de la empresa.

1.2. Objetivos e Hipótesis

Este trabajo de investigación tiene como objetivo general identificar y evaluar los riesgos de seguridad de la información existentes en el departamento de producción de una empresa industrial de alimentos mediante el planteamiento de una metodología de manera clara y detallada con el fin de elaborar y difundir las políticas de seguridad de la información más adecuadas.

Como objetivos específicos se han planteado los siguientes:

- Proponer una metodología clara y detallada para establecer políticas de seguridad de la información en base a los riesgos de seguridad identificados y evaluados en una organización o área de la misma, y la selección respectiva de controles de la norma ISO/IEC 27002.
- Identificar y evaluar los riesgos de seguridad de la información existentes en el departamento de producción de una empresa industrial de alimentos, en base a la metodología propuesta.
- Proponer las políticas de seguridad de la información adecuadas para el departamento de producción de una empresa industrial de alimentos, en base a los riesgos identificados y de acuerdo a la normativa ISO/IEC 27002, según la metodología propuesta.
- Realizar un plan de difusión de las políticas planteadas en el departamento de producción una empresa industrial de alimentos, en base a la metodología propuesta.
- Evaluar la solución planteada, aplicado la metodología propuesta al departamento de producción con el personal de TI en una empresa industrial de alimentos para generar las políticas de seguridad de la información más comunes y adecuadas para este tipo de empresas.

Como hipótesis en el presente trabajo se plantea que: “La aplicación de la metodología propuesta permitirá la identificación de riesgos críticos y elaboración de políticas de seguridad informática más adecuadas y comunes en una empresa industrial de alimentos.”

1.3. Alcance y Estructura del Trabajo

El trabajo de investigación propuesto estará estructurado siguiendo una extensión del modelo para la transferencia de tecnología propuesto por Gorschek *et al.* (2006), el mismo que está basado en las necesidades de la industria y es representado en la Figura 1.1. Este modelo incluye actividades de evaluación y observación.

Figura 1.1. *Modelo de Transferencia Tecnológica de Gorschek et al. (2006).*

Este modelo de investigación y transferencia de tecnología, se basa en ocho actividades relacionadas, donde la búsqueda de soluciones adecuadas se realiza en un proceso iterativo por medio de la formulación de soluciones candidatas y la correspondiente validación empírica que permite dirigir los esfuerzos a una solución realista. En el contenido de este trabajo de investigación se cubrirán cada una de las fases del modelo de Gorschek *et al.* (2006), como se muestra en la Figura 1.2. Este trabajo de titulación está conformado por seis capítulos distribuidos de la siguiente manera:

Capítulo 1: Introduce al lector en el contexto y alcance del trabajo de investigación, se indicará la metodología de investigación utilizada y la organización del mismo, así como la problemática, motivación e importancia del tema para las empresas industriales en nuestro medio. Así también se brindará una visión general de la estructura del trabajo de investigación planteado.

Capítulo 2: Presenta el marco teórico del trabajo realizando una revisión de los conceptos necesarios y útiles para el planteamiento de los demás temas a resolver en los posteriores capítulos. Se revisan conceptos como la seguridad de la información, el riesgo informático, los elementos del riesgo, el análisis y gestión de riesgos, el modelo PDCA, así también se revisan brevemente algunas de las metodologías de gestión de riesgos como Magerit, Octave-S, CRAMM, Microsoft Risk Management y, la metodología Ecu@Risk (Crespo, 2016) que se basa en las anteriores; además se realiza una revisión general de la familia de normas o estándares de seguridad de la información dados por la *International Organization for Standardization* (ISO) analizando la familia de estándares ISO 27000 y su principal funcionalidad, enfocándose como base para el desarrollo de las políticas de seguridad de la información en el análisis puntual de los estándares ISO/IEC 27001, que define los requerimientos para un Sistema

de Gestión de Seguridad de la Información (SGSI), e ISO/IEC 27002 que es una guía de buenas prácticas y controles para proporcionar herramientas que contribuyan a mejorar y asegurar la seguridad de la información en una organización; siendo el estándar que dicta las directrices para definir políticas de seguridad, también se analiza su estructura. Se revisa posteriormente el concepto de lo que son e implican las políticas de seguridad y se realiza un análisis de algunas metodologías de gestión de políticas de seguridad informática como son los modelos propuestos por Barbosa Martins & Saibel (2005), Bustamante *et al.* (2017) y Knapp *et al.* (2009), ya que se basan en los estándares de la industria como ISO 27002 o las normas de *National Institute of Standards and Technology* (NIST), y sobre todo el modelo de Knapp *et al.* (2009) aporta con recomendaciones realizadas por expertos en seguridad informática planteando un modelo para la gestión integral de las políticas de seguridad de la información. Finalmente se dan a conocer conceptos sobre las industrias de producción, sus tipos de procesos, su futuro y lo que es el concepto de Industria 4.0, la información que se maneja en este tipo de industrias y el ciberespionaje industrial.

Capítulo 3: Muestra el estado actual de la investigación (estado del arte) en lo referente a los dominios relacionados a este trabajo de investigación como son la seguridad informática en general, en la región y en nuestro país, la identificación y evaluación de riesgos y la elaboración de políticas de seguridad en las organizaciones.

Capítulo 4: Se plantea la metodología para elaborar y difundir las políticas de seguridad de la información más adecuadas en el departamento de producción de una empresa industrial de alimentos, las políticas estarán alineadas con la normativa ISO/IEC 27002 y otras recomendaciones que se consideren pertinentes para la elaboración de políticas de seguridad como el modelo planteado por Knapp *et al.* (2009) y otros estudios como el de Barbosa Martins & Saibel (2005) y el de Bustamante *et al.* (2017). Como parte de esta metodología se deben identificar, clasificar y evaluar los riesgos de seguridad de la información en el departamento de producción de una empresa industrial de alimentos, para ello se utilizará como guía base la metodología Ecu@Risk (Crespo, 2016) con algunas herramientas e instrumentos para ayudar y agilitar la identificación de riesgos en esta etapa.

Capítulo 5: Se evalúa la solución planteada, aplicado la metodología propuesta al departamento de producción con la ayuda del personal de TI en una empresa industrial de alimentos de la ciudad de Cuenca para identificar y evaluar sus riesgos y generar las políticas de seguridad de la información más comunes y adecuadas para el departamento de producción en esta empresa, mostrando los resultados obtenidos; se incluirán además el contexto de la empresa, sus antecedentes, análisis de sus procesos, estructura organizacional, etc. mediante las herramientas propuestas en la metodología. Además se plantea un plan de difusión e implementación de las políticas de seguridad de la información obtenidas y que son aplicables al departamento de producción de una empresa industrial de alimentos.

Capítulo 6: Se presentarán las conclusiones, recomendaciones y posibles trabajos futuros.

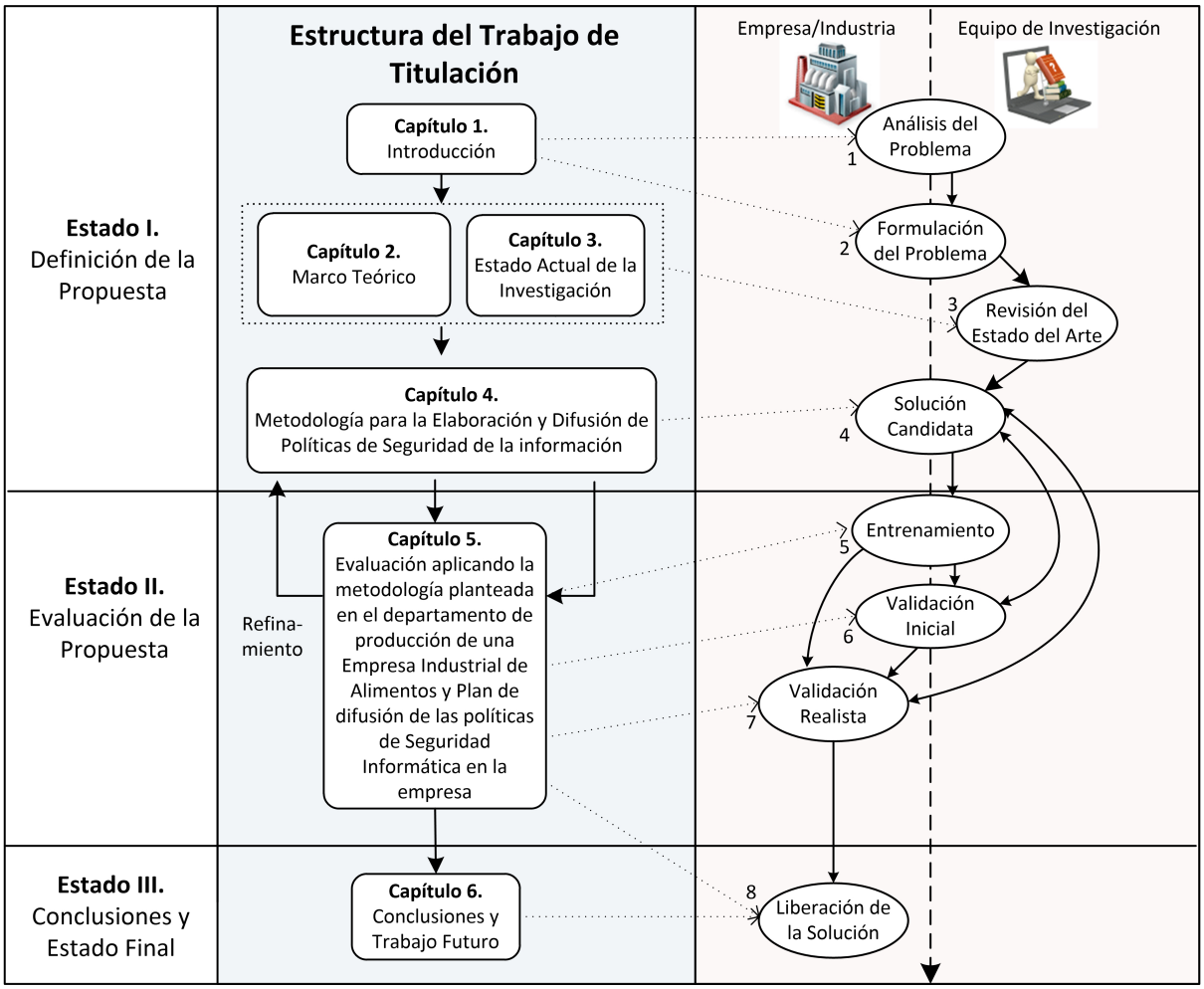

Figura 1.2. *Estructura del trabajo de Investigación alineada al modelo de Gorschek et al. (2006).*

Cabe indicar que el trabajo de investigación no contempla en sí la elaboración de un Sistema de Gestión de Seguridad de la información (SGSI), un Plan de Seguridad Informática; ni un Plan de Continuidad del Negocio (BCP) y tampoco asegura una certificación para la empresa en normas de Seguridad como ISO/IEC 27000, 27001 y 27002. Este trabajo pretende contribuir con el planteamiento de una metodología para la elaboración y difusión de Políticas para la Seguridad de la Información para el departamento de producción de una empresa industrial de alimentos; que podrían servir como insumos para una futura certificación de seguridad con normas ISO 27000, o para la elaboración de un SGSI o un BCP si la empresa decide implementarlos a futuro. Así mismo se podría replicar la metodología en otros departamentos de la empresa, en donde se pueden obtener otros riesgos y políticas de seguridad para mitigarlos aplicando la misma metodología. No se contempla en el trabajo la aprobación e implementación de las políticas de seguridad en la empresa, solamente su planteamiento mediante la metodología propuesta.

Capítulo 2. Marco Teórico

2.1. La Seguridad Informática

Los términos seguridad de la información y seguridad informática son utilizados con bastante frecuencia y según la norma ISO 27000 (ISO, 2016), la finalidad de la seguridad informática es la preservación de la *confidencialidad*, la *integridad* y la *disponibilidad* de la información.

Según esta definición es muy importante el preservar estas tres características, que a su vez son los pilares fundamentales de la seguridad informática, sobre todo en los datos e información crítica para una organización, independientemente del formato que esta tenga, pudiendo ser información electrónica, en papel, en formatos de audio y vídeo, etc. Las organizaciones públicas o privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, proveedores, procesos, etc. por lo que es una necesidad primordial en la actualidad para las organizaciones establecer mecanismos de seguridad informática para proteger su información frente a posibles riesgos y vulnerabilidades de seguridad, identificando potenciales amenazas internas o externas que puedan afectar a los datos, equipos o a la continuidad del negocio.

De la definición anterior también se destaca que la seguridad de la información se fundamenta en tres principios básicos: ***confidencialidad, disponibilidad e integridad*** de la información. Molina (2015) indica lo siguiente refiriéndose a estos tres pilares fundamentales para la seguridad de la información:

Confidencialidad: Asegurar que unicamente los usuarios con acceso autorizado tengan el acceso a la información.

Integridad: Proteger la exactitud y totalidad de los datos y métodos de procesamiento de la información que los usuarios autorizados utilizan.

Disponibilidad: Los recursos deben estar disponibles siempre que sean requeridos en cualquier momento (ISO.es: ISO/IEC 27000, 2012) (Molina, 2015).

Podemos entonces indicar respecto a estos tres principios de la seguridad de la información que la confidencialidad considera los mecanismos que garantizan el acceso a la información solamente a los usuarios y organismos autorizados, la integridad se refiere a la consistencia que la información debe conservar en todo momento y la disponibilidad es la característica de que la información debe estar disponible en el momento que se requiera por un usuario autorizado.

El concepto de seguridad informática o seguridad de la información debe ser concebido como un proceso continuo entre técnicas de hacking ético y de defensa junto con el análisis de riesgos, que

permita a las organizaciones aprender de sus fallas de seguridad y fortalecer así sus esquemas de seguridad que evidencien el nivel de dificultad que deben asumir los intrusos para intentar ingresar a sus sistemas (Cano, 2004). La gestión de la seguridad informática debe enfocarse como un proceso bien definido, con la capacidad de mejorar de manera incremental y continua (Miranda et al, 2013).

Goldes *et al* (2017) sostienen que la seguridad de la información es un tema de creciente importancia para las organizaciones de hoy ya que la profesionalización y la industrialización del delito cibernético, la globalización y la digitalización de los modelos empresariales junto con el creciente enfoque regulatorio en la protección de datos ejerce presión sobre las organizaciones para implementar sofisticados Sistemas de Gestión de Seguridad de la Información o SGSI por sus siglas.

Las investigaciones sobre Seguridad de la Información y Sistemas de Gestión de la Seguridad de la Información (SGSI) han examinado las normas internacionales de seguridad, como ISO/IEC 27001, NITS, ITIL, COBIT, entre otras consideradas guías estandarizadas que sugieren buenas prácticas de seguridad ayudando a las organizaciones a gestionar eficazmente la seguridad de sus datos y de sus activos de información (Gicas, 2010) (Susanto *et al.*, 2011) (Gillies, 2011) (Tsohou *et al.*, 2010) (Benslimane *et al.*, 2016).

Según Benslimane *et al.* (2016), para asegurar la eficacia de la Seguridad de la Información en una organización se requiere que los profesionales que trabajan en esa área de TI posean los conocimientos necesarios en lo que a seguridad de la información se requiere para el éxito del cumplimiento de sus funciones.

Así los profesionales de TI con su conocimiento y experiencia sobre la seguridad de la información, son quienes deben asesorar a los niveles directivos sobre la importancia de este tema y los proyectos que implementen o mejoren deben estar considerados dentro del Plan Estratégico de Tecnologías de Información (PETI) de la empresa.

Para garantizar la seguridad de la información en una organización, sus empleados deben tener una adecuada cultura de la seguridad de la información, que es uno de los temas más importantes en la cultura organizacional. La cultura de la seguridad de la información incluye las tareas diarias, actividades, directrices y prácticas de los empleados de una organización que deberían ayudar a proteger los activos de información y a reducir los riesgos en la organización (Mahfuth *et al.*, 2017). Esta cultura se la puede conseguir en base al entrenamiento y capacitaciones de concientización al personal en temas de seguridad de la información junto con la difusión de las normas o políticas de seguridad informática y el constante monitoreo de su cumplimiento.

2.2. El Riesgo Informático

Para la Real Academia de la Lengua Española (http://www.rae.es/), un riesgo es la contingencia o proximidad de un daño; mientras que la palabra contingencia hace referencia a la posibilidad de que algo suceda o no suceda.

La definición estandarizada de riesgo informático o tecnológico según la Organización Internacional de Normalización (ISO) indica que el riesgo es "la probabilidad de que una amenaza determinada se materialice explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto pueda causar daño o pérdidas a la organización" (ISO/Guide, 2009).

Por lo tanto el riesgo se puede definir como aquella eventualidad o probabilidad de que una amenaza ocurra y que imposibilite el cumplimiento de los objetivos de una organización al afectar a un activo o grupo de activos de información. El riesgo se plantea como la materialización de una amenaza, con la ocurrencia de una posible pérdida (por ejemplo el riesgo de perder información debido al daño de un equipo, virus informáticos, ataques, etc.).

Es importante entonces comprender los riesgos a los que se enfrenta una organización con un Sistema de Gestión de la Seguridad de la Información (SGSI) inadecuado o inexistente de acuerdo a los daños que potencialmente podrían causar dichos riesgos. Según Calder & Watkins (2008), los riesgos se dividen en tres Categorías: daños a las operaciones, daños a la reputación y daños legales de la organización e indican también que los daños ocasionados en cualquiera de estas tres categorías se pueden medir por su impacto en la organización, tanto a corto como a largo plazo.

Según Collard et al. (2017), el concepto de *Clasificación de la Información Digital* es variable y a veces no es muy informativo, pues la mayoría de las definiciones provienen de los estándares y no se han actualizado durante años, aunque el alcance y los desafíos en la seguridad de la información han llegado a ser cada vez más grandes por lo que, en base a una revisión de la literatura, se propone una nueva definición de *Clasificación de Seguridad de la Información*: "La Clasificación de Información Digital es el resultado de asignar una categoría de seguridad a la Información Digital de acuerdo con los aspectos contextuales de esta información. La categorización de seguridad debe ayudar a proteger la información de eventos que podrían afectar involuntariamente al propietario de dicha información, teniendo en cuenta cuatro tipos de riesgos: Riesgo vinculado por la naturaleza intrínseca de la información; Riesgo vinculado a la propiedad de esta información; Riesgo legal; Riesgo de almacenamiento de información" (Collard et al., 2017).

Riesgo vinculado por la naturaleza intrínseca de la Información: Se refiere a todos los riesgos inherentes a la propia información. La organización y el propietario de la información tendrán que evaluar el valor, la sensibilidad, la criticidad, la confidencialidad, la integridad, la disponibilidad, y el

uso de la misma.

Riesgo vinculado a la propiedad de esta Información: Este aspecto recoge el hecho de que cada propietario no tiene la misma madurez en la gestión de datos y por lo tanto en su clasificación. Su comprensión de conceptos como Datos, Información, Clasificación, Seguridad, etc. tiene que ser evaluada y medida para entender el perfil del propietario.

Riesgo legal: En este se muestra la importancia de que la organización y el propietario entiendan todos los riesgos legales que la información puede enfrentar.

Riesgo de almacenamiento de información: Este aspecto debe considerar todos los demás riesgos para evaluar el riesgo de almacenamiento de información, tomando en cuenta los recursos o medios utilizados para ello, y su ubicación.

2.3. Elementos del Riesgo

2.3.1 Activos

Es cualquier elemento que posee valor para la organización, sus operaciones comerciales o su continuidad, incluidos los recursos de información que apoyan la misión de la organización. Se pueden distinguir dos clases de activos: los activos primarios que incluyen a los procesos del negocio, actividades e información; y los activos de apoyo, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software (sistema operativo, servicio, software de aplicación), redes, personal (directores, usuarios, personal de operación y desarrolladores), lugar y estructura de la organización (proveedores y fabricantes) (Molina, 2015).

Los activos de información en una organización, hacen referencia a cualquier elemento que contenga información (Crespo, 2016). Los activos forman uno de los 14 dominios que trata el estándar ISO/IEC 27002, el cual contiene 3 objetivos de control y 10 controles, siendo la finalidad de este dominio que la organización tenga un conocimiento preciso sobre los activos que posee, su responsabilidad y su clasificación como parte importante de la gestión de riesgos.

Según el estándar ISO/IEC 27002, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objetivo de indicar cómo ha de ser tratada y protegida dicha información (ISO/IEC 27002, 2013).

La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y en consecuencia necesita ser protegido adecuadamente. La seguridad informática protege la información de un amplio rango de amenazas con la finalidad de asegurar la continuidad de

los negocios, minimizar el daño comercial y maximizar el reembolso de las inversiones y oportunidades comerciales. La información puede existir en muchas formas; puede ser de forma escrita, impresa, electrónica, transmitida por correo o usando medios electrónicos o hablado en una conversación. (Molina, 2015).

2.3.2 Amenazas

Son vulnerabilidades de un activo que pueden ser explotadas por una o más causas potenciales de un incidente, ocasionando daño a los activos y por consiguiente a la organización (Molina, 2015).

Las amenazas son los elementos que pueden dañar o alterar la información de una u otra forma. Estas generalmente pueden ser encontradas a partir de una vulnerabilidad existente. El riesgo a su vez, es la probabilidad que tiene una amenaza para originarse y que puede generar un cierto impacto en la organización. (Crespo, 2016). Para Molina (2015), las amenazas podrían presentarse de varios tipos:

De origen natural: Incendios, inundaciones, tormentas eléctricas, terremotos, siniestros mayores que afectan la disponibilidad de los activos de información y que son de origen natural.

Del entorno: Incendio, inundación, polvo, sobrecarga eléctrica, corte de suministro eléctrico, condiciones inadecuadas de temperatura o humedad que afectan la disponibilidad de los activos de información; el fallo de los servicios de comunicaciones que afecta la disponibilidad de las redes de comunicaciones; la degradación de los soportes de almacenamiento que afecta la disponibilidad la información; las emanaciones electromagnéticas que afectan a la disponibilidad e integridad de los equipos informáticos y medios de soporte de información; o cualquier otra amenaza que es inherente al entorno o el medio en el cual se desenvuelve la empresa..

Por defecto de aplicaciones: Aquellos problemas que se producen en equipos o sistemas por defectos de fábrica o en su implementación, se denominan también vulnerabilidades técnicas. Por lo general, la recuperación de este tipo de problemas se la obtiene por parte del proveedor o siguiendo una guía de configuración; para ello se debe tener respaldada la información para restaurarla cuando sea necesario.

Causadas por las personas de forma accidental: Los errores accidentales que afectan la disponibilidad, integridad y confidencialidad de la información como errores accidentales de los usuarios que usan el servicio, errores accidentales del administrador responsable de la instalación y operación de sistemas o equipos, errores de monitorización que afectan la trazabilidad de los registros de actividad, los errores accidentales en la configuración o los errores accidentales de enrutamiento que afectan la confidencialidad e integridad de los servicios, aplicaciones y las redes de comunicaciones.

Causadas por las personas de formas deliberada: Como la manipulación de los registros de

aplicaciones y actividades que afectan la información, la suplantación de la identidad del usuario, abuso de privilegios de acceso o acceso no autorizado, la monitorización no autorizada del tráfico y la intercepción de información, el robo y ataque destructivo o inhabilitante de los activos informáticos o la propagación mal intencionada de virus, spyware, gusanos, troyanos, bombas lógicas, malware, ransomware, etc. que afectan la disponibilidad, integridad y confidencialidad de las aplicaciones. (Amutio *et al.*, 2012) (Molina, 2015).

2.3.3 Vulnerabilidades

Los activos se ven influidos por una serie de amenazas; la probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad según la metodología MAGERIT (Ministerio de Hacienda y Administraciones Públicas de España, 2012). Las vulnerabilidades deben ser clasificadas de acuerdo a la clase de activos, es decir: hardware (susceptibilidad a la humedad, polvo, suciedad, almacenamiento sin protección), software (falta de pruebas del software, falta de seguimiento de auditoría), red (líneas inadecuadas, falta de seguridad), sitio (ubicación en un área susceptible a inundaciones, red de energía inestable), y organización (falta de auditorías periódicas, falta de planes de continuidad del negocio) (Molina, 2015).

Las vulnerabilidades hacen referencia a las debilidades que existen en un sistema de información, lo que permite que pueda ser fácilmente atacado, evadiendo el control de acceso y la confidencialidad de los datos y las aplicaciones existentes (Cordero Torres, 2015). Las vulnerabilidades deben ser expresadas en una escala numérica para poder posteriormente cuantificar su impacto, y, citando a Burgos y Campos, se sugiere que éstas sean identificadas y valoradas individualmente (Cordero Torres, 2015) (Burgos Salazar & Campos, 2008) (Crespo, 2016). La vulnerabilidad se puede expresar como indica Castaño, mediante la siguiente fórmula:

Vulnerabilidad*=*Frecuencia estimada / Días al año (Cordero Torres, 2015) (Castaño, 2014) (Crespo, 2016).

Se concluye según esta fórmula que la vulnerabilidad es la relación entre la frecuencia con la que podría ocurrir la amenaza y el número de días al año en la que la misma pudiese ocurrir mientras se encuentra operativo el activo, con la información y/o los servicios que preste el mismo a la organización.

2.3.4 Impacto

Es un indicador de lo que puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando la misma se materializa sobre un activo. El impacto se estima, conociendo el valor de los activos y su degradación causada por las amenazas (Molina, 2015). Para Molina (2015), el impacto sobre los activos se expresa mediante la siguiente formula:

Impacto = *Valor * Degradación del Activo* (Molina, 2015).

Donde notamos que el Impacto es el resultado del producto del valor del Activo multiplicado por la degradación que pudiese llegar a tener el mismo en caso de llegarse a materializar una determinada amenaza.

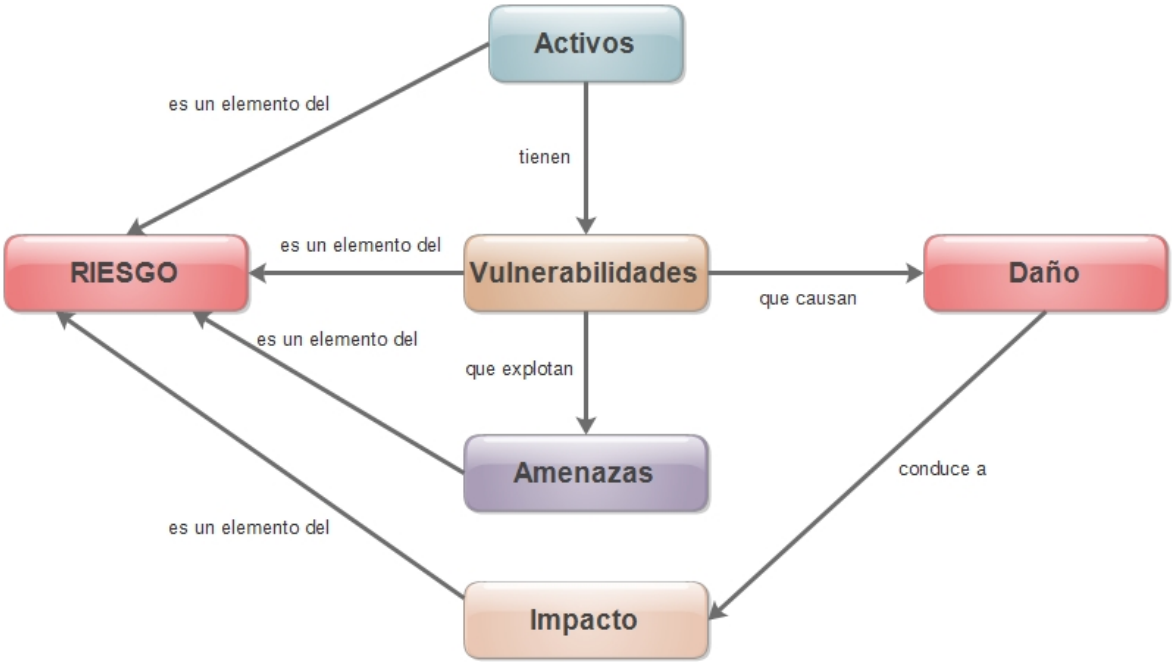

Figura 2.1. *Elementos del Riesgo y sus Relaciones.*

En la Figura 2.1 se resumen gráficamente los elementos del riesgo informático y las relaciones entre los mismos.

2.4. Análisis de Riesgos

Molina (2015) cita a Amutio *et al.* (2012), indicando que el análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización y permite determinar la naturaleza, el costo y la protección que tiene un sistema, siguiendo los objetivos, estrategia y políticas de la organización para elaborar un plan de seguridad integral y, al implantar y operar este plan se deben satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos (Amutio *et al.*, 2012)(Molina, 2015).

El análisis de riesgos, según Molina (2015), se realiza ya sea cuantitativa o cualitativamente. Se recomienda realizar el análisis cualitativo como punto de partida, para lo cual se usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; considerando también la probabilidad de que se produzcan dichas consecuencias. Un análisis

cualitativo permite entre otras cosas:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema actualmente.
- Establecer claramente los activos críticos (sujetos a los riesgos máximos o más peligrosos).

Mientras que el análisis cuantitativo es más detallado, utilizando una escala con valores numéricos para medir las consecuencias y probabilidad, permitiendo lo siguiente:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas o controles de protección.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora continua de la seguridad.

Barbosa Martins & Saibel (2005) indican que se puede estimar el riesgo mediante el producto entre la probabilidad de que ocurra un riesgo y el impacto que causa dicho riesgo:

Riesgo = *Probabilidad* * *Impacto* (Barbosa Martins & Saibel, 2005)

El rol que tiene el análisis de riesgos dentro de la seguridad de la información es resumido en los siguientes puntos (Eloff *et al.*, 1993):

1 - El análisis de riesgos es un prerrequisito no sólo para la compilación de las políticas de seguridad de la información, sino también para el refinamiento paso a paso de una política para definir un plan de protección para su implementación.

2 - La gestión del riesgo empresarial suele considerarse como un factor de éxito por la alta gerencia, por lo que el análisis de riesgos puede utilizarse como un mecanismo para lograr que la alta dirección se involucre en la gestión de riesgos informáticos.

3 - La realización y ejecución de un estudio de análisis de riesgos dentro de una organización sigue siendo una tarea difícil, sin embargo el principal resultado del análisis de riesgos es la identificación de contramedidas para las amenazas identificadas.

4 - El análisis de riesgos puede agregar información profesional significativa necesaria para la realización de un ejercicio de costo vs. beneficio para el plan de seguridad de la información de una organización.

2.5. El Modelo PDCA

Algunos autores como Disterer (2013) y Molina (2015) coinciden en que para ejecutar el análisis y posterior gestión del riesgo, se tiene que seguir un ciclo con cuatro etapas conocido por sus siglas en inglés como **PDCA** (Plan-Do-Check-Act) o Planificar-Ejecutar-Verificar-Actuar, que se ilustra en la Figura 2.2.

"Al igual que con otros estándares de TI, la familia de estándares ISO 27000 se refiere directamente al ciclo "Plan-Do-Check-Act" (ciclo PDCA), conocido por la gestión clásica de calidad de Deming, que enfatiza la necesidad de la orientación al proceso, así como la integración del planeamiento de las operaciones y la verificación constante de la implementación conforme a la planificación." (Disterer, 2013).

"Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos es parte de las actividades de planificación, se toman decisiones de tratamiento y estas decisiones se materializan en la etapa de implantación, en la cual se despliegan elementos que permiten la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo de éstas, dentro de un círculo de excelencia o mejora continua." (Molina, 2015).

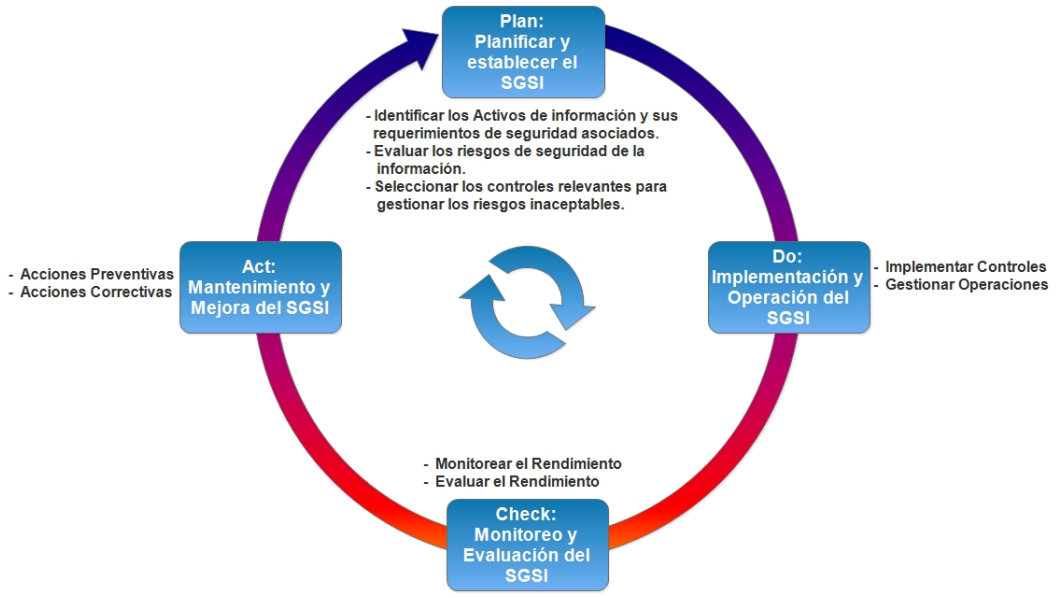

Figura 2.2. *Etapas del ciclo PDCA según ISO 27000. Fuente: (Disterer, 2013)*

Según Disterer (2013), en un Sistema de Gestión de Seguridad de la Información (SGSI), en la etapa de planificación es donde se definirán los requisitos para la protección de la información, se identificarán y evaluarán los riesgos y se desarrollarán los procedimientos y medidas adecuados para reducir los riesgos. Estos procedimientos y medidas se implementan durante la etapa de implementación y operación (o etapa de ejecución). Los informes generados a través del monitoreo continuo de las operaciones (etapa de verificación) se utilizarán en la última etapa (Actuar) para obtener las mejoras y el desarrollo posterior y continuo del SGSI. Estas etapas se resumen en la Figura 2.2.

La mayoría de las metodologías de gestión de riesgos utilizan como base el modelo PDCA (Disterer, 2013), y lo realizan con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua, siguiendo teniendo las siguientes actividades en cada una de sus etapas:

- **Planificar:** Se establecen los objetivos, procesos y procedimientos para la gestión de riesgos tecnológicos. La finalidad de esta etapa es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Además se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.
- **Hacer:** Se realiza la implementación y operación de los controles, procesos y procedimientos e incluye además la operación e implementación de las políticas definidas y la valoración y tratamiento de los riesgos.
- **Verificar:** En esta etapa se evalúa y se mide el desempeño de los procesos contra la política y los objetivos de seguridad. Además se debe informar los resultados obtenidos.
- **Actuar:** En esta etapa se establece la política para la gestión de riesgos tecnológicos y se implementan los cambios requeridos para la mejora de los procesos. En las etapas verificar y actuar, se incluye el monitoreo y la mejora continua, donde se verifican los cambios y el cumplimientos de indicadores establecidos en la etapa de planificación.

2.6. Gestión de Riesgos

La gestión de riesgos consiste en el proceso de analizar, evaluar, tratar, monitorizar y comunicar los riesgos encontrados (Cocho, 2006) (Crespo, 2016). La gestión de los riesgos es un desafío estratégico para las organizaciones, las cuales enfrentan amenazas cada vez más complejas y diversas (Lalonde & Boiral, 2012).

Calder y Watkins indican que todas las organizaciones se enfrentan diariamente a riesgos de un tipo u otro. Estos autores definen a la Gestión de Riesgos como una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida; en cambio, los riesgos especulativos son aquellos a partir de los cuales se puede producir una ganancia o una pérdida, que a menudo son estrategias de negocio de la organización. (Calder &

Watkins, 2008). La gestión de riesgos, según estos autores, suelen tener cuatro objetivos vinculados, los cuales son:

- Eliminar los riesgos,
- Reducir a niveles "aceptables" aquellos riesgos que no pueden eliminarse; y entonces
- Convivir con ellos, ejerciendo cuidadosamente los controles que los mantienen en niveles "aceptables"; o
- Transferirlos, por medio de aseguradoras por ejemplo, a otra instancia u organización.

Según Molina (2015), la gestión del riesgo en general consiste en seis procesos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación de riesgos, comunicación y consulta de riesgos, revisión y seguimiento del riesgo (Molina, 2015). Estos procesos y su interrelación se los puede apreciar en la Figura 2.3:

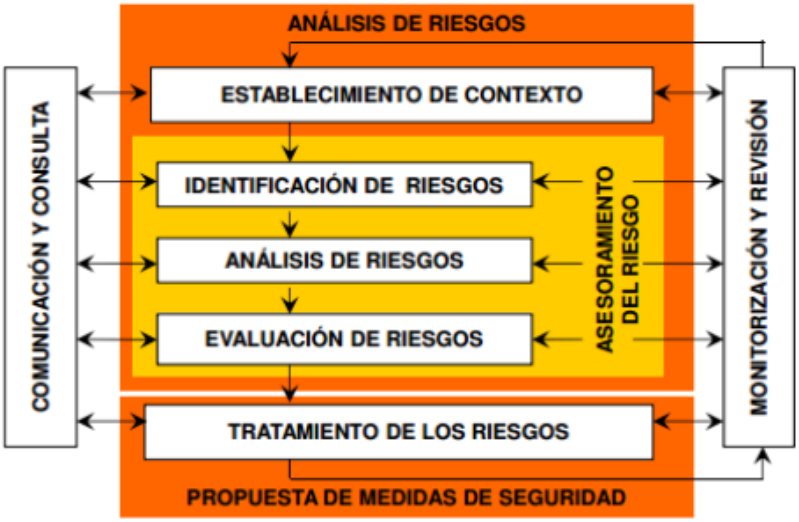

Figura 2.3. *Procesos de la Gestión de Riesgos. Fuente: (Molina, 2015)*

2.7. Metodologías de Gestión de Riesgos

"Un método es un procedimiento o proceso sistemático y ordenado para alcanzar algún objetivo y una metodología se materializa por un conjunto de métodos, técnicas y herramientas." (Molina, 2015).

El significado de la palabra metodología, según el diccionario de la Real Academia Española (http://www.rae.es/), es definido como el "conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal". Se puede determinar entonces basándonos en estos conceptos que una metodología de gestión de riesgos es un conjunto de métodos o procesos sistemáticos y ordenados a seguir para lograr mitigar o anular los riesgos identificados, haciendo uso de herramientas y técnicas necesarias para conseguir este objetivo. Molina (2015) indica que "las metodologías cualitativas son las más adecuadas para el análisis de riesgos y cumplen con los requisitos de la norma

ISO 27001". El nivel de riesgo se basa en niveles de probabilidad e impacto como se muestra en la Tabla 2.1.

La ecuación del riesgo (*Riesgo = Probabilidad * Impacto*) se puede representar mediante una escala de 3 niveles haciendo referencia al impacto de un evento que se da con una probabilidad de ocurrencia, como se muestra en la Tabla 2.2.

Ejemplos de metodologías de gestión de riesgos son: Magerit (Ministerio de Hacienda y Administraciones Públicas de España, 2012), Octave (Alberts *et al.*, 2005), CRAMM (Yazar, 2002), Microsoft Risk Management (Microsoft, 2006), y la metodología Ecu@Risk (Crespo, 2016).

NIVEL DE RIESGO	ACCION REQUERIDA PARA TRATAMIENTO DEL RIESGO
Muy Alto	Inaceptable: las acciones deben tomarse inmediatamente.
Alto	Inaceptable: las acciones deben tomarse en corto plazo.
Medio	Acciones requeridas y que deben tomarse en un plazo razonable.
Bajo	Aceptable: no se requieren acciones como resultado de la evaluación de riesgos.
Muy Bajo	Aceptable: ninguna acción es requerida.

Tabla 2.1. *Niveles de clasificación de Riesgos. Fuente: (Molina, 2015)*

PROBABILIDAD	**ALTA**	***Riesgo Medio***	***Riesgo Alto***	***Riesgo Muy Alto***
	MEDIA	***Riesgo Bajo***	***Riesgo Medio***	***Riesgo Alto***
	BAJA	***Riesgo muy Bajo***	***Riesgo Bajo***	***Riesgo Medio***
		BAJO	**MEDIO**	**ALTO**
		IMPACTO		

Tabla 2.2: *Clasificación de Riesgos según Probabilidad e Impacto. Fuente: (Molina, 2015)*

A continuación se describen brevemente algunas de las metodologías utilizadas para la gestión de riesgos como son: Magerit, Octave-S, CRAMM y Microsoft Risk Management; las mismas que se utilizan como base en la metodología de gestión de riesgos Ecu@Risk y se pueden utilizar en varios tipos de organizaciones, como en las empresas industriales de alimentos.

2.7.1. Magerit

Es una de las metodologías más utilizadas en la gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas de España (Ministerio de Hacienda y Administraciones Públicas de España, 2012) para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000 y, en el año 2012 se actualizó a la versión 3.

La entidad que creo esta metodología, el Ministerio de Hacienda y Administraciones Públicas de España, la define como: "*Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad), depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios*" (Ministerio de Hacienda y Administraciones Públicas de España, 2012) (Crespo & Cordero, 2016) (Crespo, 2016).

Según Molina (2015), los objetivos que busca alcanzar esta metodología son los siguientes:

- Hacer que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarlos a tiempo.
- Ofrecer un método sistemático para el análisis de riesgos.
- Ayudar en la descripción y planificación de las medidas adecuadas para mantener los riesgos bajo control.
- De forma indirecta, preparar la organización de los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. La metodología se resume en el modelo de la figura 2.4.

***Figura 2.4**: Modelo Magerit*

El Ministerio de Hacienda y Administraciones Públicas de España (2012) y Molina (2015) concluyen las siguientes acciones para identificar riesgos en una organización mediante la metodología Magerit:

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.
- Determinar a qué amenazas están expuestos los activos relevantes.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

El ciclo de la metodología Magerit parte de la identificación de los activos de información, para por consiguiente identificar las amenazas lógicas y las del entorno, y posteriormente estimar las frecuencias y el impacto, las mismas que servirán como insumo para la identificación de las salvaguardas, y así gestionar, como aspecto final, el riesgo residual (Crespo & Cordero, 2016) (Cordero, 2015) (Crespo, 2016).

Estos autores indican también que Magerit considera como activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos. Esta metodología además sugiere una escala de valoración de 1 al 10, donde 1

es insignificante y 10 es de muy alta importancia (Cordero, 2015) (Crespo & Cordero, 2016) (Crespo, 2016).

MAGERIT consiste de 3 libros en versiones de inglés, español e italiano, siendo su contenido el siguiente:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas

2.7.2. CRAMM

La metodología CRAMM (CCTA Risk Analysis and Management Method), fue desarrollada en 1985 en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones. Es una metodología cuyo objetivo es proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos, pudiendo ser aplicable a todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad; donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones (Yazar, 2002) (Cordero Torres, 2015) (Crespo & Cordero, 2016) (Crespo, 2016).

CRAMM se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices; las dos primeras se encargan de identificar y analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos deben ser gestionados (Molina, 2015). Según Crespo (2016), estas tres etapas se conocen como *identificación, análisis y evaluación de riesgos*.

La última versión identificada de la metodología, es la versión 5, liberada en el año 2003. Esta metodología recomienda el uso de entrevistas y cuestionarios estructurados para el levantamiento de información (Yazar, 2002).

Según Yazar (2002), CRAMM se puede utilizar en todo tipo de organizaciones para justificar las inversiones relacionadas con la seguridad o la contingencia para los sistemas y redes de información, demostrando la necesidad de actuar a nivel de gestión, sobre la base de resultados cuantificables y contramedidas derivadas del análisis de riesgos específico de una organización o para demostrar el cumplimiento de BS7799 (el estándar británico para la Gestión de la seguridad de la información) durante un proceso de certificación.

CRAMM calcula el riesgo en base a una valoración de las vulnerabilidades, realizada mediante una escala del 1 al 7, utilizando una matriz de riesgos con valores predefinidos, dados por la comparación del valor de los activos frente a los niveles de tretas y vulnerabilidades, donde 1 significa un bajo requerimiento de seguridad y 7 un alto requerimiento. (Yazar, 2002) (Crespo, 2016).

Mollina (2016) cita a Calder y Watkins (2010), quienes indican que CRAMM sigue el siguiente proceso:

- Utiliza reuniones, entrevistas y cuestionarios como herramientas para la recolección de datos.
- Identifica y clasifica los activos de TI en tres categorías; datos, software y activos físicos.
- Requiere que se consideren el impacto de la pérdida de confidencialidad, integridad y disponibilidad del activo.
- Mide la vulnerabilidad por niveles: muy alto, alto, medio, bajo o muy bajo.
- Mide el riesgo por niveles: alta, media o baja.

2.7.3. OCTAVE

OCTAVE es una metodología enfocada en la Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades, según sus siglas en Ingles Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE). Según Alberts *et al.* (2005), esta metodología define una técnica de evaluación y planificación estratégica basada en el riesgo para la seguridad. OCTAVE es un enfoque auto-dirigido, lo que significa que las personas de una organización asumen la responsabilidad para establecer la estrategia de seguridad de la organización. OCTAVE-S es una variación del enfoque adaptado a los medios limitados y restricciones únicas típicamente encontradas en pequeñas organizaciones (menos de 100 personas). OCTAVE-S está dirigido por un pequeño equipo interdisciplinario (tres a cinco personas) de una organización quienes recolectan y analizan información, produciendo una estrategia de protección y planes de mitigación basados en los riesgos de seguridad operacional en la organización. Para llevar a cabo una implementación efectiva de OCTAVE-S, el equipo debe tener un amplio conocimiento de los procesos del negocio y de seguridad de la organización. (Alberts *et al.*, 2005).

A este equipo interdisciplinario, Vásquez & López (2016) lo llaman “equipo de análisis” e indican que debe ser conformado por personas de las áreas de negocio y del área de TI. Además es considerado como fundamental, ya que con un equipo de trabajo adecuado se podrán identificar de una manera ágil, certera y oportuna los activos de información más relevantes, así como las debilidades y vulnerabilidades que pueden presentarse sobre los mismos (Vásquez & López, 2016) (Crespo, 2016).

OCTAVE está enfocada en las actividades diarias de las organizaciones, iniciando desde la identificación y valoración de los activos de información. Esta metodología según Molina (2015), agiliza y optimiza el proceso de evaluación de riesgos de seguridad de la información alineados a los objetivos y metas de la organización. En base a esta, existen tres metodologías publicadas: OCTAVE aplicable en organizaciones con más de 300 empleados, OCTAVE-S aplicable en organizaciones de hasta 100 empleados y OCTAVE Allegro que permite una amplia evaluación del entorno del riesgo operativo sin la necesidad de un amplio conocimiento de evaluación de riesgos y requiere menos tiempo

de implementación.

Los dos objetivos específicos de OCTAVE son: Desmitificar la falsa creencia de que la seguridad informática es solamente un asunto técnico y presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos de la seguridad de la información Molina (2015).

OCTAVE divide los activos en dos tipos: sistemas y personas. En el primer grupo se consideran el hardware el software y los datos. La metodología OCTAVE está compuesta por tres fases:

Visión de la Organización: En esta fase se definen los elementos como los activos, vulnerabilidades, amenazas, exigencias de seguridad y normas existentes de la organización. (Molina, 2015). OCTAVE, tiene cuatro categorías principales de amenazas: problemas debido al acceso a través de la red, errores por acceso físico, problemas del sistema y otros problemas. En esta etapa se construyen los perfiles de amenaza de los activos, describiendo los requerimientos de seguridad para lograr construir un perfil de amenazas para cada uno de los activos identificados como críticos. (Vásquez & López, 2016) (Crespo, 2016).

Visión Tecnológica: En esta fase, se identifican dos componentes, las claves y vulnerabilidades técnicas. El equipo deberá evaluar cada uno de los distintos componentes organizacionales para identificar vulnerabilidades tecnológicas, que habilitarían las acciones sin autorización en contra de los activos críticos. Los resultados de esta etapa se resumen en componentes clave (relacionados con los activos críticos), que serían componentes como firewall, servidores, enrutadores y sistemas de almacenamiento de información; y las vulnerabilidades tecnológicas existentes de la empresa por ejemplo mediante herramientas automáticas de escaneo (Vásquez & López, 2016) (Crespo, 2016).

Planificación de las medidas y reducción de riesgos: Se clasifican los elementos como la evaluación de riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de riesgos. Molina (2015). En esta etapa, luego de haber identificado los riesgos existentes sobre los activos de información críticos, el equipo de trabajo planifica y desarrolla políticas de mitigación de riesgos, basados en la información adquirida en las etapas anteriores. Como resultados de este proceso están los riesgos valorados en una escala de tres niveles: alto, medio y bajo; así como también las estrategias de protección y los planes de mitigación del riesgo.

La metodología OCTAVE Allegro consiste en 8 pasos organizados en 4 etapas, ilustrado en la figura 2.5 donde las salidas de cada paso en el proceso son documentadas en una serie de hojas de trabajo que son usadas como entradas del siguiente paso en el proceso.

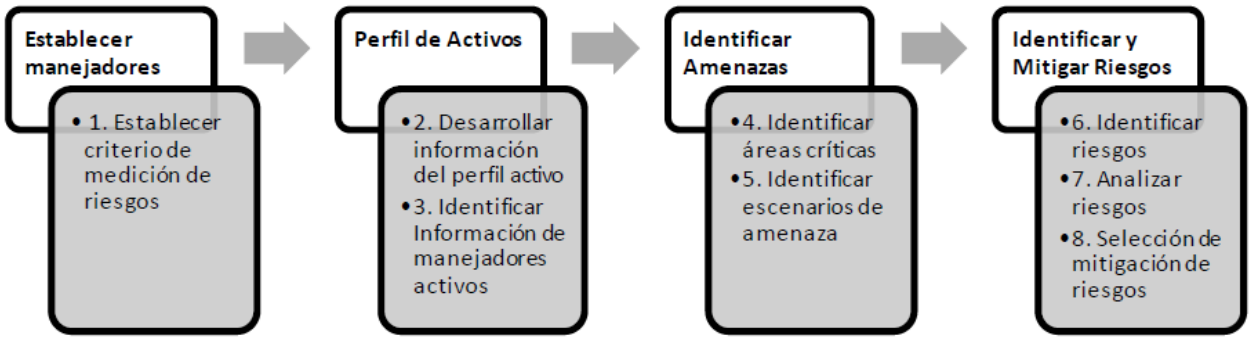

***Figura 2.5**: Procesos de la Metodología OCTAVE Allegro. Fuente: (Molina, 2015)*

2.7.4. Microsoft Risk Management

Security Risk Management es una guía metodológica para la gestión de riesgos desarrollada por la compañía Microsoft en el año 2006. Utiliza los estándares de la industria para entregar un modelo de gestión de riesgos establecido en un proceso iterativo de cuatro fases que busca balancear el costo y la eficacia de la organización. Durante un proceso de evaluación de riesgos, los pasos cualitativos identifican rápidamente los riesgos más importantes y posteriormente se presenta un proceso cuantitativo basado en roles y responsabilidades cuidadosamente definidos. Este enfoque es muy detallado y conduce a una comprensión completa de los riesgos más importantes. Conjuntamente los pasos cualitativos y cuantitativos en el proceso de evaluación de riesgos proporcionan la base sobre la cual se pueden tomar decisiones sólidas sobre los riesgos y su mitigación, siguiendo un proceso de negocio inteligente en la organización. (Microsoft, 2006).

El objetivo principal de esta guía de gestión de riesgos, según Microsoft (2006), es proporcionar una orientación clara y útil sobre la manera de implementar un proceso de gestión de riesgos de seguridad de la información que ofrezca una serie de beneficios, entre ellos:

- Colocar a los usuarios en una posición de seguridad proactiva, liberándolos de un proceso reactivo y frustrante.
- Proveer de una seguridad cuantificable, mostrando el valor de los proyectos de seguridad.
- Dar mayor eficiencia a la mitigación de los riesgos más grandes en sus entornos, en lugar de aplicar recursos escasos a todos los riesgos posibles.

Microsoft (2006), Vásquez & López (2016) y Crespo (2016) citan que esta Guía de Gestión de Riesgos de Seguridad comprende seis capítulos como se indica a continuación, donde cada capítulo se basa en una práctica necesaria para iniciar y operar de manera eficaz un proceso de gestión de riesgos de seguridad continuo en una organización:

Capítulo 1. Introduce a esta guía de gestión de riesgos de seguridad, ofreciendo una breve descripción de cada capítulo.

Capítulo 2. Deja sentadas las bases para el proceso de gestión de riesgos de seguridad de Microsoft revisando las diferentes formas en que las organizaciones han abordado la gestión de riesgos de seguridad. El capítulo comienza con una revisión de las fortalezas y debilidades de los enfoques proactivo y reactivo de la gestión de riesgos, con lo que finalmente se los podrá valorar de forma cualitativa y cuantitativa.

Capítulo 3. Ofrece una visión más detallada del proceso de gestión de riesgos de seguridad de Microsoft e introduce algunos de los conceptos y claves importantes para su éxito. También brinda asesoramiento sobre cómo prepararse para el proceso utilizando una planificación eficaz y la creación de un equipo de gestión de riesgos de seguridad con roles y responsabilidades bien definidos

Capítulo 4. Presenta la evaluación del riesgo; los pasos en esta fase incluyen planificación, recolección de datos y priorización de riesgos. El proceso de evaluación de riesgos consiste en múltiples tareas, algunas de las cuales pueden ser muy exigentes para una organización grande.

Capítulo 5. Durante esta fase de Apoyo a la toma de decisiones, el equipo de gestión de riesgos de seguridad determina cómo abordar los riesgos claves de la manera más eficaz y rentable posible. El equipo identifica los posibles controles, determina los costos asociados con la adquisición, implementación y apoyo de cada control, evalúa el grado de reducción del riesgo que cada control logra; Y, finalmente, trabaja con el Comité Directivo de Seguridad para determinar qué controles implementar. El resultado final es un plan claro y manejable para controlar o aceptar cada uno de los principales riesgos identificados en la fase de Evaluación del Riesgo, evaluando de esta manera también los riesgos residuales que pueden presentarse.

Capítulo 6. Este capítulo cubre las dos últimas fases del proceso de administración de riesgos de seguridad de Microsoft: Implementación de los controles y medición de la efectividad del programa. (Microsoft, 2006) (Vásquez & López, 2016) (Crespo, 2016).

Crespo (2016) indica que esta metodología utiliza el modelo de defensa en profundidad, lo que permite al equipo de administración de riesgos de seguridad de la información recopilar datos en el entorno organizacional, además de ofrecer una estructura adecuada.

El proceso de gestión de riesgos de seguridad Microsoft Risk Managment (Microsoft, 2006) define la gestión de riesgos como un proceso continuo con cuatro etapas o fases principales, como se ilustra en la figura 2.6:

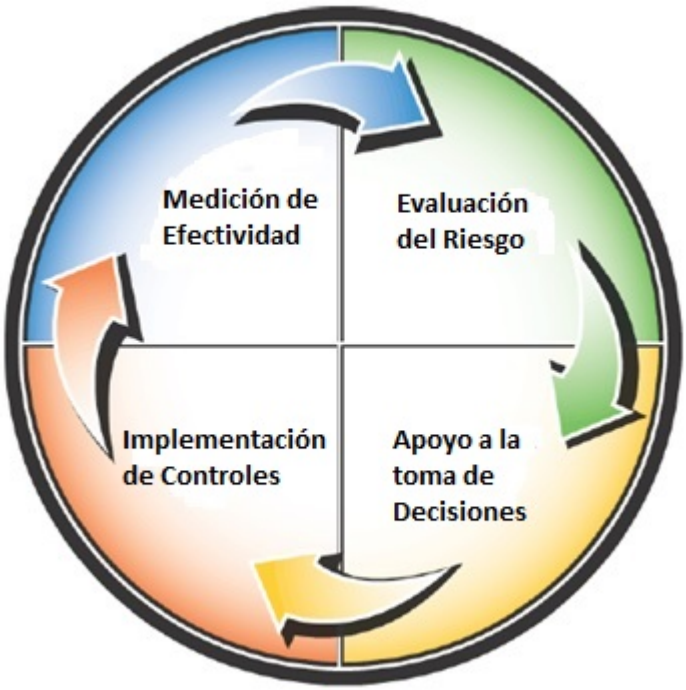

Figura 2.6: *Fases del Proceso de Microsoft Risk Management. Fuente: (Microsoft, 2006)*

A continuación se describen brevemente las 4 etapas de esta metodología:

- **Evaluación del riesgo:** Identificar y priorizar los riesgos para el negocio.
- **Apoyo a la toma de Decisiones:** Identificar y evaluar soluciones de control basadas en un proceso de análisis de costo-beneficio definido.
- **Implementación de controles:** Implementar y operar soluciones de control para reducir el riesgo para el negocio.
- **Medición de la efectividad del programa:** Analizar el proceso de gestión de riesgos para la eficacia y verificar que los controles dados están proporcionando el grado de protección esperado.

2.7.5. Ecu@Risk

La metodología Ecu@Risk propuesta por Crespo (2016), ha sido seleccionada como la metodología base en este trabajo por su análisis de las recomendaciones y herramientas más importantes de otras metodologías aceptadas internacionalmente como Magerit, Octave-S, CRAMM y Microsoft Risk Management, alineadas con los marcos de referencia internacionales como son las normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000; además se sustenta en leyes ecuatorianas que amparan la protección de datos contra divulgación, vigilancia o delito. Esta metodología fue realizada para la gestión del riesgo informático aplicable a las micro, pequeñas y medianas empresas (MPYME) en el Ecuador, por lo que se considera también que puede ser aplicable en las empresas de tipo industrial del país, contribuyendo además en este trabajo con una variación y

mejora de los procesos y materiales para la identificación de riesgos que tiene esta metodología.

La gestión del riesgo debe alinearse a las actividades diarias y a la toma de decisiones con los objetivos y resultados que ayudarán a alcanzar los objetivos estratégicos, o ejecutar con éxito los planes operativos propuestos. (Crespo, 2016). Por lo que, resumiendo, el autor indica que para que la metodología de gestión de riesgos sea exitosa debe ser parte y estar alineada con las actividades y objetivos estratégicos de la organización.

Ecu@Risk se compone de tres secciones principales: a) la introducción al manejo del riesgo, b) el marco de gestión del riesgo, c) el proceso de gestión del riesgo y como una sección adicional presenta los recursos o herramientas que se proponen utilizar en la metodología en cada uno de los procesos de la sección de gestión del riesgo.

En la sección "c" de esta metodología (proceso de gestión del riesgo) se describe el proceso para la aplicación de la gestión del riesgo y es la parte medular de la metodología Ecu@Risk. En esta sección, la metodología Ecu@Risk contiene los siguientes procesos de gestión: determinación del contexto, identificación de los activos de información, identificación de los riesgos, análisis de los riesgos, evaluación de los riesgos, tratamiento de los riesgos e identificación de contramedidas. Se identifican también un proceso de monitoreo y control y un proceso comunicacional: comunicar y consultar como se muestran en la Figura 2.7.

Figura 2.7. *Procesos Generales para la Gestión del Riesgo en la Metodología Ecu@Risk.*

Los procesos de la sección de gestión de riesgos que propone la metodología Ecu@Risk y que interesan para la elaboración de la propuesta metodológica planteada en el presente trabajo para la elaboración de políticas de seguridad de la información, son los primeros cuatro: *la determinación del contexto, la identificación de los activos de información, la identificación de los riesgos y el análisis de los riesgos*; estos procesos se analizan a continuación y se detallan en notación SPEM en la Figura 2.8.

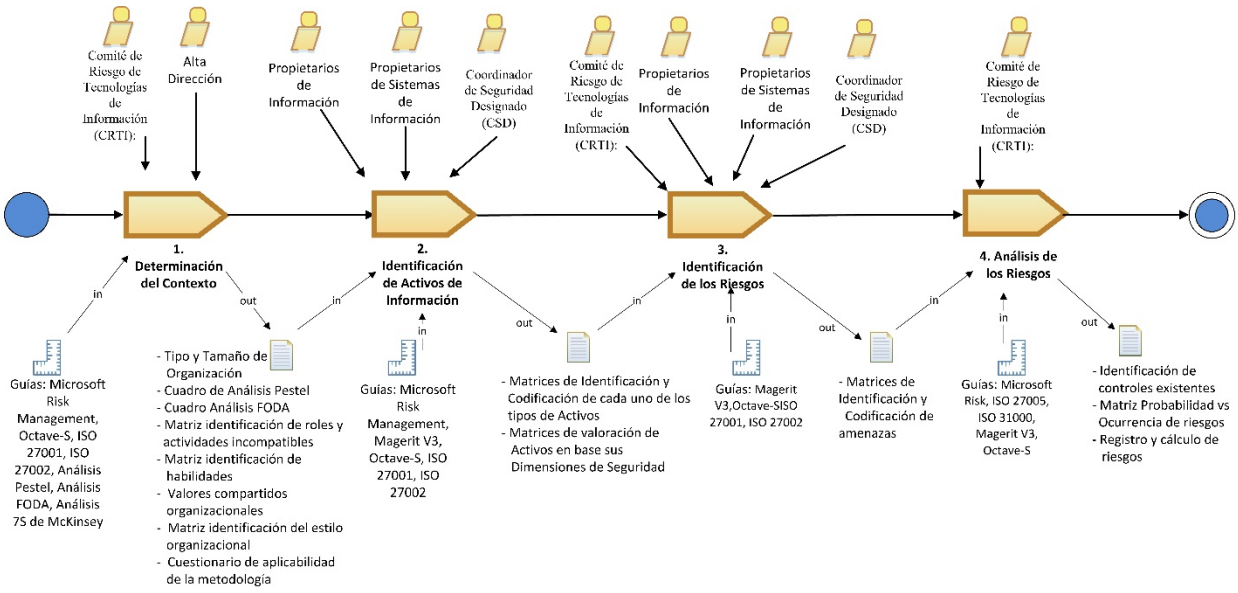

Figura 2.8. *Procesos para la Identificación y Análisis de Riesgos en la Metodología Ecu@Risk.*

Crespo (2016) señala que la gestión del riesgo en la metodología se organiza en base a las 4 etapas del ciclo PDCA (Planificar-Ejecutar-Verificar-Actuar), por lo que existen 5 procesos de gestión, 1 proceso de monitoreo y control y 1 proceso comunicacional. A continuación se presenta brevemente el proceso estándar que deberá seguir una organización, empresa o institución bajo la metodología Ecu@Risk:

- **Paso 1: Determinación del Contexto**: Se verifica el entorno que tiene la empresa con la que se va a trabajar. En este paso se identifica el tipo de organización, y su tamaño. Posteriormente, se tiene que definir el alcance de la investigación y sus objetivos; es decir, qué actividad, decisión, proyecto, programa, o cuestión requiere un análisis. Es importante además identificar a las partes interesadas y/o áreas pertinentes involucradas o afectadas, así como los factores internos y externos que tiene la organización. Se tienen formularios de procesos denominados con las siglas (PEC) que hacen referencia a los procesos para establecer el contexto de la empresa, entre ellos tenemos el procedimiento para la identificación del tipo de organización y del tamaño de la organización, el uso de la herramienta de análisis PESTEL (Análisis de factores Políticos, Económicos, Socio-culturales, Tecnológicos, Ecológicos o ambientales, y Legales) para realizar un Proceso de Análisis Organizacional. Se analizan amenazas y oportunidades de la organización, los cuales se pueden convertir respectivamente en posibles riesgos o contramedidas para mitigarlos. En este paso también se establece el contexto interno de la organización con la finalidad de identificar roles y responsabilidades de los empleados, componentes salariales, compromiso para con la empresa, nivel de madurez profesional, delimitar las áreas de trabajo sensible, mecanismos de comunicación internos, conocimiento sobre el nivel de políticas

institucionales, entre otros factores. Se utilizan herramientas como el análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) como se muestra en la Tabla 2.3 y la herramienta de análisis de las 7S de McKinsey con el objetivo de identificar los perfiles, actividades y roles de los colaboradores de la empresa.

FODA PARA (NOMBRE DE LA ORGANIZACIÓN)		
Fecha:		
Elaborado por:		
Aprobado por:		
Aspectos Positivos (+)	**Aspectos Negativos (-)**	
FORTALEZAS	**DEBILIDADES**	**De origen Interno**
OPORTUNIDADES	**AMENAZAS**	**De origen Externo**

Tabla 2.3. *Matriz para la identificación de FODA institucional. Fuente: (Crespo, 2016)*

- **Paso 2: Identificación de los activos de la Información:** La metodología Ecu@Risk define grupos de activos con su respectiva codificación como se muestran en la Tabla 2.4. En este paso se procede a identificar los activos en cada grupo con su respectiva codificación y subclasificación. Algo importante para tener en cuenta en lo que se refiere a la codificación del activo de información, según Crespo (2016), es que los activos se deben codificar con el formato: *(COD. CLASIFICACIÓN DEL ACTIVO) (SUB CODIGO) (SUB CÓDIGO) (SECUENCIAL)*, siendo este último campo un número incremental para identificar únicamente a un activo. Luego de registrar cada activo que se haya identificado de acuerdo a cada una de sus categorías, se debe valorarlo de acuerdo a las dimensiones de valoración, que son las características o atributos que hacen valioso un activo. Una dimensión, según el Ministerio de Hacienda y Administraciones Públicas de España (2012), es un aspecto de un activo, independiente de otros aspectos, permitiendo realizar el análisis de riesgos centrados en un único aspecto, independientemente de lo que ocurra con otros. Las dimensiones se usan para valorar las consecuencias de la materialización de una amenaza (Ministerio de Hacienda y Administraciones Públicas de España, 2012) (Crespo, 2016). Las dimensiones pueden ser basadas en los tres principios básicos en los

que se fundamenta la seguridad de la información con sus iniciales como códigos: *Confidencialidad (C), Disponibilidad (D) e Integridad (I).* Crespo (2016) cita al Ministerio de Hacienda y Administraciones Públicas de España (2012), quienes indican que para valorar los activos sirve, en teoría, cualquier escala de valores, sin embargo frecuentemente la valoración es cualitativa, quedando a discreción del usuario. En la Tabla 2.5 se presentan los criterios de valoración recomendados en la metodología Ecu@Risk y en la Tabla 2.6 se ilustra un ejemplo del formato de valoración de activos propuesto en la metodología Ecu@Risk.

CODIGO	TIPO DE ACTIVO
ED	Edificaciones
HW	Hardware
SW	Software
IE	Información electrónica
IP	Información en papel
Extraíble	Medios de almacenamiento extraíble
IC	Infraestructura de comunicaciones
RRHH	Recursos Humanos

Tabla 2.4. *Codificación de Activos de la Información*

VALOR	CRITERIO	
10	extremo	Daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante para efectos prácticos

Tabla 2.5: *Criterios de Valoración de Riesgos. Fuente: (Crespo, 2016), (Ministerio de Hacienda y Administraciones Públicas de España, 2012)*

Código del Activo	Descripción	(D)	(I)	(C)	Valoración Total	Valor
(HW)(PC)(01)	Equipo de atención al cliente	5	9	4	9	Muy Alto

Tabla 2.6: *Ejemplo de formato para Identificación y Valoración de Activos. Fuente: (Crespo, 2016)*

- **Paso 3: Identificación de los Riesgos:** La metodología sugiere presentar datos cuantitativos y / o cualitativos para ayudar a describir y calificar posteriormente el riesgo. Las fuentes de información podrían incluir registros de experiencias anteriores, la experiencia del personal, prácticas de la industria, literatura o la opinión de expertos. (Crespo, 2016). Continuamente se deben identificar las amenazas que podrían afectar la continuidad del negocio por lo que la metodología Ecu@Risk propone una guía de posibles amenazas o riesgos (las más frecuentes y conocidas) que pueden afectar a los activos de un sistema de información. Crespo (2016) indica que en Ecuador, las amenazas de las organizaciones se pueden clasificar en 5 grupos: Riesgos de comunicaciones, riesgos informáticos, riesgos provocados (por error), riesgos provocados (deliberados) y riesgos naturales. Para la identificación de las Amenazas, la metodología Ecu@Risk plantea un formato que se muestra en la Tabla 2.7, donde se identifican amenazas dentro de los 5 grupos mencionados.

[Código] Descripción resumida de lo que puede pasar (Amenaza)	
Tipos de Activos/Activos Afectados: Descripción de los Activos que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** Enumerar las dimensiones de seguridad que se pueden ver afectadas por el tipo de amenaza identificado. Se las debe ordenar desde la más relevante hacia la menos relevante
Descripción: Debe ser complementaria o más detallada acerca de la amenaza: lo que le puede ocurrir o como les puede afectar a los activos descritos con las consecuencias indicadas.	

Tabla 2.7: *Formato para la Identificación de Amenazas. Fuente: (Crespo, 2016)*

Crespo (2016), también sugiere plantear algunas consultas iniciales para facilitar la identificación de riesgos en una organización mediante la metodología Ecu@Risk, las cuales se resumen en el capítulo 4 en la Tabla 4.14 y se utilizarán en la metodología propuesta.

- **Paso 4: Análisis de los Riesgos:** Una vez que los riesgos han sido identificados con su contexto, causas y consecuencias, Crespo (2016) plantea que se deben considerar las fortalezas y debilidades de los sistemas y procesos de seguridad designados para ayudar a controlar o mitigar el riesgo. Se debe indicar que controles existen y si dichos controles han sido implementados, si son eficaces para mitigar el riesgo, si es necesario mejorarlos o no colaboran con ninguna acción. Muchas veces estos controles simplemente están presentes como parte natural de la

administración de la organización o de alguna área, pero se deben identificar y analizar su grado de contribución para la mitigación de riesgos. La metodología sugiere un proceso para el análisis de riesgos, que consiste en:

1) **Identificar los controles existentes:** Identificar los controles que ya han sido implementados para mitigar el impacto del riesgo. Los controles pueden ser fuertes o débiles y pueden estar amparados bajo las leyes, políticas o procedimientos, formación del personal, separación de funciones, equipos de protección, barreras físicas y estructurales, etc.; se debe realizar un análisis de la eficacia de los controles existentes.
2) **Evaluar la probabilidad:** La metodología propone que la probabilidad de que ocurra un riesgo se clasifique y evalué en 5 niveles: rara, poco probable, posible, probable o casi seguro que ocurra. (Crespo, 2016).
3) **Evaluar la consecuencia:** Se sugiere también que las consecuencias o impacto de la materialización de un evento o riesgo se clasifiquen o evalúen como insignificante, menor, moderada, grave o extrema.
4) **Valorar el riesgo:** (Crespo, 2016) sugiere la matriz indicada en la tabla 2.8 para valorar los riesgos de acuerdo a su probabilidad de ocurrencia y a sus consecuencias o impacto.

Matriz de Riesgos						
		Consecuencia				
		1. Leve	**2. Menor**	**3. Moderado**	**4. Alto**	**5. Extremo**
Probabilidad	**E- Casi certero (frecuente)**	M	M	A	E	E
	A- Probable	B	M	A	A	E
	M- Posible	B	M	M	A	A
	B- No muy común	B	B	M	M	A
	L- Raro	L	L	B	B	M

Tabla 2.8: *Matriz de Valoración de Riesgos. Fuente: (Crespo, 2016) (University of Adelaide, 2015)*

Con los resultados finales y al igual que otras metodologías, se deben considerar los niveles de riesgo y las acciones requeridas para cada una de ellos para mitigarlos, como se sugieren en la tabla 2.9.

Niveles de Riesgo	Acciones de Gestión Requeridas
Riesgo extremo (E)	Requiere respuesta y atención inmediata
Riesgo alto (A)	Debe otorgársele la atención apropiada
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y efectivos
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios, informar a los gestores locales, supervisar y revisar localmente como sea necesario.
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora

***Tabla 2.9**: Matriz de Niveles de riesgo y acciones de Gestión. Fuente: (Crespo, 2016) (University of Adelaide, 2015)*

2.8. Estándares ISO para la definición de Políticas de Seguridad

El riesgo para las organizaciones cuyos procesos empresariales dependen cada vez más del procesamiento de la información y cuyas infraestructuras de TI complejas e interconectadas son vulnerables a fallas e interrupciones han llevado a dar mucha importancia a la seguridad de la información y el compromiso sistemático con los aspectos de la seguridad que se derivan (Disterer, 2009). Es por ello que para asegurar una adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde la seguridad de la información de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de una organización.

Los estándares de seguridad pueden utilizarse como guía o marco para desarrollar y mantener un adecuado Sistema de Gestión de Seguridad de la Información (SGSI); sobre todo las normativas internacionales ISO/IEC 27000, 27001 y 27002 están recibiendo un creciente reconocimiento y adopción en la industria (Disterer, 2009). A continuación se verán algunos de estos estándares de la familia de la *International Organization for Standardization* (ISO) que servirán en el presente trabajo tanto para la identificación de riesgos como para la elaboración de políticas de seguridad de la información.

2.8.1. ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por los organismos de estandarización ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, o de pequeño o gran tamaño (ISO 27000, 2009).

La norma ISO 27000 se emitió en 2009 para proporcionar una visión general de la familia de normas ISO 27 K y una base conceptual común. Se tienen 46 términos básicos de seguridad de la información que están definidos y diferenciados en la sección "Términos y condiciones" de este estándar.

Disterer (2013) presenta un análisis comparativo de toda la familia de estándares ISO 27000 enfocándose en su desarrollo y clasificación como se resume en la Figura 2.9, e indica que para la protección de la información y de los sistemas de información en una organización, estos estándares son los que proporcionan los objetivos de control, controles específicos, requisitos y directrices necesarias con las que una empresa, sin importar su naturaleza o tamaño, puede asegurar una adecuada seguridad de la información.

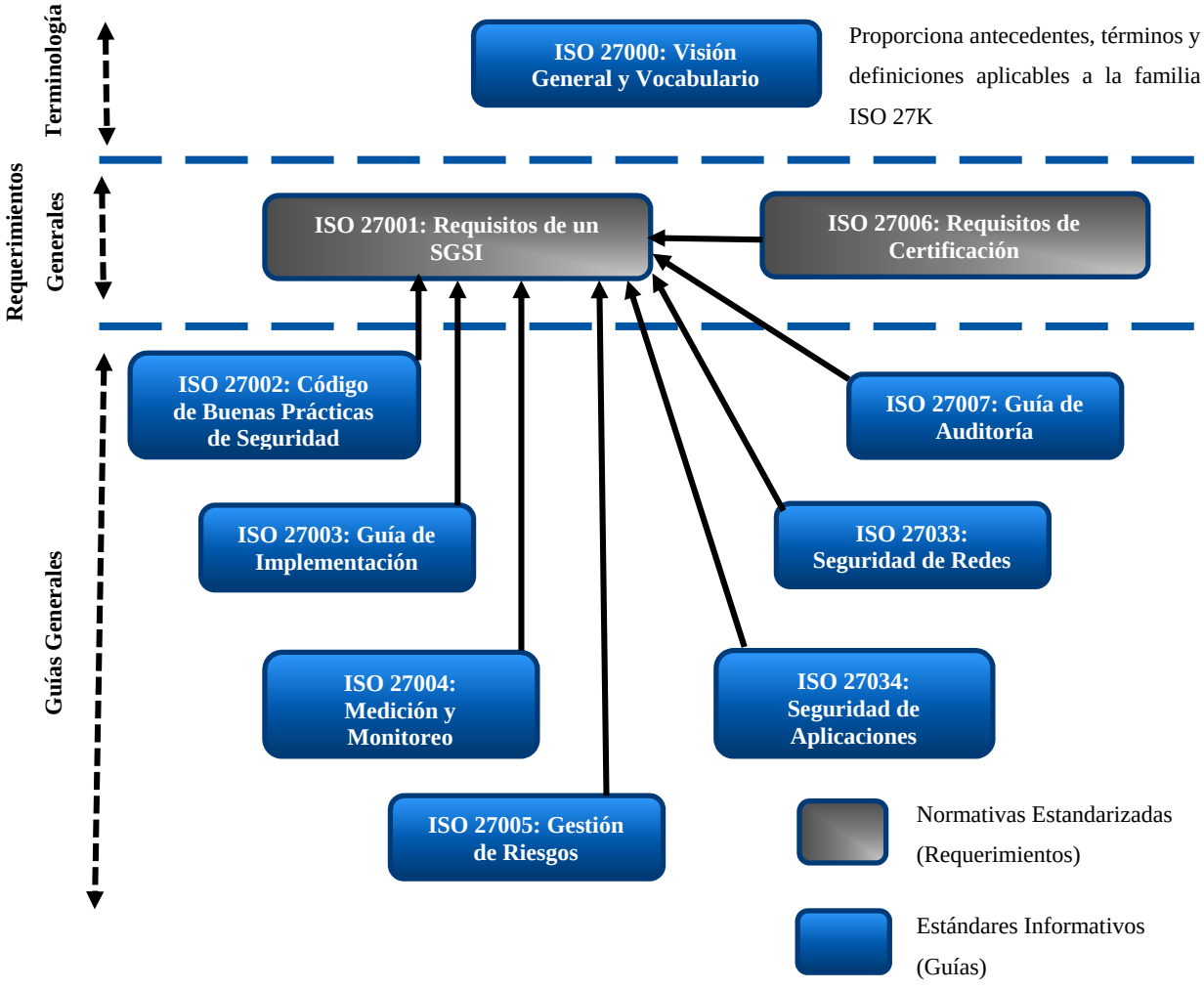

Figura 2.9. *Relaciones entre la familia de Estándares ISO 27 K. Fuente:(Disterer, 2013) (ISO, 2009).*

La versión más actualizada de la norma se publicó en el año 2016, es conocida como ISO/IEC 27000: 2016 y se publicó con el título "*Tecnología de la información - Técnicas de seguridad - Sistemas*

de gestión de la seguridad de la información – Visión general y vocabulario" (ISO 27000, 2016). Esta norma internacional proporciona una visión general de los sistemas de gestión de la seguridad de la información y presenta una definición de sus términos relacionados y necesarios.

Al igual que con otros estándares de Tecnologías de la Información (TI), la mayoría de estándares ISO 27 K se refieren al ciclo "Plan-Do-Check-Act" (ciclo PDCA) ilustrado en la Figura 2.2, que enfatiza la necesidad de la orientación del proceso, así como la integración del planeamiento de las operaciones y el monitoreo o evaluación constante de la implementación conforme a la planificación. En la fase de planificación de un Sistema de Gestión de Seguridad de la Información (SGSI) se definen los requisitos para la protección de la información y los sistemas de información, se identifican y evalúan los riesgos y se desarrollarán los procedimientos y medidas adecuados para reducir dichos riesgos; estos procedimientos y medidas se ponen en marcha durante la etapa de implementación y operación. Además, los informes generados mediante el monitoreo continuo de las operaciones se utilizarán para obtener mejoras y posteriores adecuaciones al SGSI (Disterer 2013).

De manera similar a otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 (ISO, 2009).

2.8.2. ISO 27001

Humphreys (2011) analiza el estándar de seguridad ISO / IEC 27001, como la norma de seguridad de la información más exitosa de ISO, junto con las otras normas de la familia de estándares de seguridad de la información (denominadas ISO / IEC 2700x).

El estándar ISO / IEC 27001: 2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de una organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza (ISO 27001, 2013).

ISO (2013) indica que la norma fue publicada el 15 de Octubre de 2005 y tiene su origen en la norma BS 7799-2:2002 siendo la norma principal de la serie conteniendo los requisitos de un SGSI. En su Anexo “A”, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

En 2005, la norma ISO 27001 se publicó con el título "*Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos*" y se mantiene con esa denominación hasta la versión actual (ISO 27001, 2013). En 42 páginas describe los requisitos que

un SGSI debe cumplir para lograr la certificación. Como marco, la norma está dirigida a empresas de todos los sectores y de todos los tamaños; sin embargo las medidas concretas para el cumplimiento de los requisitos no se estipulan en la norma, sino que deben desarrollarse y aplicarse sobre una base específica de la empresa. Los requisitos de certificación de ISO 27001 se complementan con una guía de implementación dentro de ISO 27002 (Disterer 2013).

Debe existir un entrenamiento o capacitación adecuada al personal de una organización para la implementación del estándar con el fin de impulsar los procedimientos estipulados, establecerlos, y generar conciencia de su necesidad; además las medidas deben ser verificadas y mejoradas continuamente y los riesgos de seguridad deben ser identificados y evaluados con el fin de aumentar constantemente la eficacia y la eficiencia del SGSI (ISO, 2005) (Disterer 2013).

Al establecer un SGSI, una organización debe llevar a cabo una evaluación de riesgos de acuerdo con los requisitos especificados en la norma ISO / IEC 27001 y, según Humphreys (2011), una vez que se ha realizado dicha evaluación, es necesario seleccionar un sistema con los controles más adecuados del Anexo "A" de este estándar que reduzca el conjunto de riesgos identificados. El código de prácticas del estándar ISO/IEC 27002 proporciona asesoramiento y orientación a los usuarios sobre la implementación de estos controles (Humphreys, 2011).

Por lo tanto, luego de definir la cobertura y el alcance de un SGSI, los riesgos deben ser identificados y evaluados, también deben definirse los objetivos de control para los sistemas de información, para tomar las medidas o controles más adecuados para proteger las operaciones de una organización.

En el Anexo "A" de la norma en su versión ISO/IEC 27001:2005 se enumeran un total de 39 objetivos de control y 134 medidas o controles para la gestión de seguridad.

La versión de ISO/IEC 27001 publicada en el año 2013 conocida con la denominación "ISO/IEC 27001:2013" presenta una nueva estructura según el estándar definido por ISO/IEC para todas las normas referentes a sistemas de gestión, facilitando la integración y trabajo conjunto entre los diferentes estándares de gestión publicados por dicha entidad, constando en el Anexo "A" de esta nueva versión del estándar 14 dominios, 35 objetivos de control y 114 controles.

Este estándar es de uso muy común en proyectos de análisis y diseño de un SGSI, dado que establece concretamente los pasos que conlleva este proceso y, a diferencia de su versión anterior (ISO/IEC 27001:2005), la norma actual no menciona el ciclo de Deming (PDCA) como metodología para definir el ciclo de vida y mejora continua del sistema de seguridad a implementar, dejando abierta la posibilidad de la organización a elegir cualquier modelo de mejora continua distinto y que se adapte mejor a sus necesidades. Sin embargo, ya que se deja abierta esa posibilidad, se podrá utilizar el ciclo

Plan-Do-Check-Act (PDCA) para asegurar el cumplimiento de los requerimientos de la Norma Técnica, si la empresa así lo requiere. Esto lo fundamentan Goldes *et al.* (2017) quienes indican que a pesar de que el proceso PDCA fue retirado de la norma en favor de las referencias a procesos de mejora continua, los controles actuales y sus relaciones con determinados contextos empresariales siguen predominando en la norma actual, lo que permite a una organización combinarlos con una estructura de sistema de gestión específica y adecuada para la organización.

Se concluye entonces que el punto clave de la norma ISO/IEC 27001 es presentar los requisitos para la planificación, implementación, operación y monitoreo y mejora continua de un SGSI; además, en la versión ISO/IEC 27001:2005 el enfoque en la versión debe estar alineado con el ciclo PDCA (Figura 2.2), sin embargo en la versión publicada en el año 2013 ya no es necesario este enfoque, dejando a la organización el modelo o ciclo que más se adapte a sus necesidades. El personal debe ser correctamente entrenado para la implementación del estándar para su éxito en la organización; además, la norma su Anexo "A" enumera en forma de resumen los dominios, objetivos de control y controles que se desarrollan a detalle en la norma ISO/IEC 27002.

2.8.3. ISO 27002

Los requisitos codificados en ISO/IEC 27001 se amplían y se explican en ISO/IEC 27002 en forma de una guía. Esta guía se publicó por primera vez en el año 2000, denominándola "ISO 17799" bajo el título de *"Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información"* y en 2007 se revisó el estándar y se alineó con la familia de estándares ISO 27 K y la denominación se cambió a "ISO 27002"; en el desarrollo de esta normativa se ofrecieron prácticas comunes también conocidas como mejores prácticas, como procedimientos y métodos probados que podrían adaptarse a los requisitos específicos de las empresas (Disterer, 2013). La última revisión del estándar se publicó en 2013 (ISO 27002, 2013) con el título de *"Tecnología de la información – Técnicas de Seguridad - Código de Prácticas para los Controles de Seguridad de la Información"*.

Disterer (2013) indica que con la finalidad de explicar la importancia de la seguridad de la información para las empresas, se exponen los riesgos para la seguridad de la información de una empresa y la necesidad de disponer de medidas específicas y acordadas conocidas como "controles" en el marco de un SGSI.

Por estas necesidades surge ISO/IEC 27002, que según Crespo (2016), es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información; es una norma que permite crear principios para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información; posee objetivos de control que se implementan para satisfacer los requisitos analizados por la evaluación de riesgos. (Cordero, 2015) (Vásquez & López,

2016) (Crespo, 2016).

Las directrices fundamentales para garantizar la seguridad de la información deben ser definidas y especificadas en forma de políticas de seguridad por parte de la dirección de la empresa; la difusión y aplicación de estas políticas dentro de la empresa también sirve para enfatizar la importancia de la seguridad de la información y la atención que tiene que brindar la administración a estos temas (Disterer, 2013).

La seguridad de la información debe estar anclada estratégicamente en la empresa para que las medidas de seguridad de la información puedan ser promovidas y establecidas de manera eficiente (Disterer, 2013); este autor también señala que se han de definir las funciones y responsabilidades y, en particular, se deben especificar las obligaciones de mantener la confidencialidad y las normas para las comunicaciones con externos (clientes, proveedores, autoridades, etc.).

El desarrollo continuo de la norma ISO 27002 se basa en la presentación de la norma ISO 27001, en la que se explican con más detalle los 11 dominios y los 39 objetivos de control enumerados en la norma ISO 27001:2005, con un total de 134 controles, justificados y descritos en detalle, asignados a esos objetivos (ISO 27002, 2005). La última edición de este estándar que reemplaza a la ISO/IEC 27002:2005 es la norma ISO/IEC 27002:2013 (ISO 27002, 2013), la misma que contiene 14 dominios, 35 objetivos de control y 114 controles; en correspondencia con el Anexo “A” de la norma ISO 27001:2013 (ISO 27001, 2013).

Para tener éxito en la implementación de los controles para la seguridad de la información, Disterer (2013) indica que se debe tener como un dato referente que más de la mitad de todos los ataques son iniciados por personal interno voluntaria o involuntariamente; sin embargo, una gran proporción también es iniciada por acciones conjuntas de personal interno y externo; además, debido a que el personal interno puede utilizar el conocimiento interno de la organización (como procesos internos, hábitos, puntos débiles, relaciones sociales, etc.) para los ataques, se debe considerar que tienen un potencial más alto para el éxito y el daño que puedan causar. Disterer (2013) señala también que los riesgos correspondientes deben tenerse en cuenta para tomar las medidas de seguridad adecuadas que debe tener el personal, tanto en el reclutamiento, contratación, y en su asignación. Así, por ejemplo, los derechos de acceso de un usuario deben limitarse solamente a la extensión necesaria para llevar a cabo el trabajo al que el usuario está asignado. Con los cambios en las responsabilidades, puestos o tareas del trabajo, los derechos de acceso se deben adaptar a estos cambios y si el personal es retirado de la empresa, entonces los derechos de acceso deben ser revocados oportunamente.

Tanto los estándares ISO / IEC 27001 como ISO / IEC 27002 están sometidos actualmente a una revisión cada 5 años como se aplica a la mayoría de las normas ISO / IEC y el objetivo de esto es para asegurarse de que ambas normas están actualizadas y siguen satisfaciendo las necesidades de las

empresas; por lo que si hubiesen nuevos requerimientos de negocio que deben cumplirse, éstos se incorporarán a las nuevas versiones (Humphreys 2011). Entonces el proceso de revisión considera las contribuciones de muchas fuentes y sectores con el conocimiento de expertos a fin de garantizar que las próximas versiones de estas normas se mantendrán por mínimo 5 años una vez que se han publicado.

2.8.4. Estructura de ISO 27002:2013

El cuerpo del estándar ISO/IEC 27002:2013 se estructura en 18 capítulos o secciones; a continuación se enumeran y describen brevemente estas secciones o capítulos:

0. **Introducción:** Introduce al lector en conceptos como la importancia del estándar, sus objetivos y su relación con la norma ISO/IEC 27001, los requerimientos de la seguridad de la información, la selección de los controles en el estándar, etc.

1. **Alcance:** Este estándar internacional presenta las directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y administración de los controles teniendo en cuenta los entornos de riesgo de seguridad de la información en una organización. Esta norma internacional está diseñada para ser utilizada por organizaciones que tienen la intención de:

a) Seleccionar los controles adecuados dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información basado en ISO / IEC 27001(ISO 27001, 2013).

b) Implementar los controles de seguridad de la información comúnmente aceptados.

c) Elaborar sus propias guías de gestión para la seguridad de la información.

2. **Referencias de la Normativa:** Indica las referencias con otros estándares que son indispensables para su aplicación, en este caso la principal referencia por los conceptos y vocabulario es el estándar ISO / IEC 27000:2016 "*Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Visión general y vocabulario*" (ISO 27000, 2016).

3. **Términos y Definiciones:** Se aplican los mismos términos y definiciones que figuran en la norma ISO / IEC 27000.

4. **Estructura del Estándar:** Presenta la estructura y organización para el desarrollo del estándar, indicando sus cláusulas o dominios y categorías de control. La norma ISO/IEC 27002:2013 contiene 14 cláusulas o dominios de control de seguridad que contienen un total de 35 categorías de controles de seguridad y 114 controles. Cada cláusula que define los controles de seguridad contiene una o más categorías principales de seguridad, además, las cláusulas, categorías y controles de esta norma no están en orden de prioridad o importancia. por lo tanto, cada organización que aplique este estándar debe identificar los controles aplicables, la importancia de éstos y su aplicación a sus procesos empresariales. Cada categoría de controles de seguridad contiene:

a) un objetivo de control que indique lo que se pretende lograr;

b) uno o más controles que se pueden aplicar para lograr cumplir con el objetivo de control.

Las descripciones de los controles se estructuran de la siguiente manera:

Control: Define la instrucción de control específica, para satisfacer el objetivo de control.

Guía de implementación: Proporciona información más detallada para apoyar la implementación del control y cumplir con el objetivo de control. La guía puede que no sea totalmente adecuada o suficiente para algunas situaciones u organizaciones y podría no cumplir con los requisitos específicos de control de la organización, por lo que se debería seleccionar solo los controles más adecuados o establecer su propia metodología o guía de implementación.

Otra información: Proporciona información adicional que puede ser necesaria considerarla, por ejemplo, consideraciones legales y referencias a otros estándares. Si no existe información adicional acerca del control, esta parte no se muestra.

Los capítulos desde el 5 hasta el 18 de este estándar se estructuran cada uno con una cláusula o dominio, siendo en total 14 con sus 35 respectivas categorías, cada una con sus objetivos de control y 114 controles descritos en total, esta estructura se muestra a continuación y se resumen en la Tabla 1.1 del Anexo 1 donde se enumeran los dominios del estándar con sus categorías y sus respectivos objetivos de control, así como en la Tabla 1.2 del Anexo 1, donde se resumen los dominios, categorías y controles del estándar.

5. Políticas de Seguridad de la Información

5.1 Directrices de Gestión para la seguridad de la información

Objetivo: Proporcionar directrices de gestión y soporte para la seguridad de la información de acuerdo a los requerimientos del negocio, leyes y reglamentos relevantes.

Controles:

5.1.1 Conjunto de políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para la seguridad de la información.

6. Organización de la Seguridad de la Información

6.1 Organización interna

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información en la organización.

Controles:

6.1.1 Asignación de responsabilidades para la seguridad de la información.

6.1.2 Segregación de tareas.

6.1.3 Contacto con las autoridades.

6.1.4 Contacto con grupos de interés especial.

6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo

Objetivo: Asegurar la seguridad en el teletrabajo y el uso de dispositivos móviles.

Controles:

6.2.1 Política de uso de dispositivos para movilidad.

6.2.2 Teletrabajo.

7. Seguridad de los Recursos Humanos

7.1 Antes de la contratación

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las cuales son considerados.

Controles:

7.1.1 Investigación de antecedentes.

7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación

Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información.

Controles:

7.2.1 Responsabilidades de gestión.

7.2.2 Concientización, educación y capacitación en seguridad de la información.

7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambo o terminación del empleo, de manera ordenada y segura.

Controles:

7.3.1 Cese o cambio de puesto de trabajo.

8. Gestión de Activos

8.1 Responsabilidad sobre los activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección apropiadas.

Controles:

8.1.1 Inventario de activos.

8.1.2 Propiedad de los activos.

8.1.3 Uso aceptable de los activos.

8.1.4 Devolución de activos.

8.2 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

Controles:

8.2.1 Directrices de clasificación.

8.2.2 Etiquetado y manipulado de la información.

8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de la información guardada en medios de almacenamiento.

Controles:

8.3.1 Gestión de soportes extraíbles.

8.3.2 Eliminación de soportes.

8.3.3 Soportes físicos en tránsito.

9. Control de Accesos

9.1 Requisitos de negocio para el control de accesos

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de información.

Controles:

9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario

Objetivo: Garantizar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

Controles:

9.2.1 Gestión de altas/bajas en el registro de usuarios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario

Objetivo: Responsabilizar a los usuarios por la protección de su información de autenticación.

Controles:

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones

Objetivo: Prevenir el acceso no autorizado a sistemas y aplicaciones.

Controles:

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas.

10. Cifrado

10.1 Controles criptográficos

Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

Controles:

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

11. Seguridad Física y Ambiental

11.1 Áreas seguras

Objetivo: Evitar accesos físicos no autorizados, daños e interferencias a la información de la organización y a las instalaciones de procesamiento de información.

Controles:

11.1.1 Perímetro de seguridad física.

11.1.2 Controles físicos de entrada.

11.1.3 Seguridad de oficinas, despachos y recursos.

11.1.4 Protección contra las amenazas externas y ambientales.

11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos

Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos informáticos e interrupción de las operaciones de la organización.

Controles:

11.2.1 Emplazamiento y protección de equipos.

11.2.2 Instalaciones de suministro.

11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de los equipos.

11.2.5 Salida de activos fuera de las dependencias de la empresa.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

11.2.8 Equipo informático de usuario desatendido.

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. Seguridad de las Operaciones

12.1 Responsabilidades y procedimientos operacionales

Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.

Controles:

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso (malware)

Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información se encuentren protegidas contra el malware.

Controles:

12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad

Objetivo: Brindar protección contra la pérdida de datos.

Controles:

12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y monitoreo

Objetivo: Registrar eventos y generar evidencia.

Controles:

12.4.1 Registro y gestión de eventos de actividad.

12.4.2 Protección de los registros de información.

12.4.3 Registros de actividad del administrador y operador del sistema.

12.4.4 Sincronización de relojes.

12.5 Control del software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales.

Controles:

12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas.

Controles:

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

Controles:

12.7.1 Controles de auditoría de los sistemas de información.

13. Seguridad en las Telecomunicaciones

13.1 Gestión de la seguridad en las redes

Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

Controles:

13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas

***Objetivo*:** Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.

Controles:

13.2.1 Políticas y procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.3 Mensajería electrónica.

13.2.4 Acuerdos de confidencialidad y secreto.

14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información como una parte integral de los sistemas de información a lo largo de todo su ciclo de vida. Esto también incluye los requerimientos para los sistemas de información que proporcionan servicios sobre redes públicas.

Controles:

14.1.1 Análisis y especificación de los requisitos de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información.

Controles:

14.2.1 Política de desarrollo seguro de software.

14.2.2 Procedimientos de control de cambios en los sistemas.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4 Restricciones a los cambios en los paquetes de software.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.

14.2.7 Externalización del desarrollo de software.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9 Pruebas de aceptación.

14.3 Datos de prueba

Objetivo: Asegurar la protección de los datos utilizados para las pruebas.

Controles:

14.3.1 Protección de los datos utilizados en pruebas.

15. Relaciones con Suministradores

15.1. Seguridad de la información en las relaciones con suministradores

Objetivo: Asegurar la protección de los activos de la organización a los que pueden acceder los proveedores.

Controles:

15.1.1 Política de seguridad de la información para suministradores.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores

Objetivo: Mantener un nivel adecuado de seguridad de la información y prestación de servicios alineado con los acuerdos con los proveedores.

Controles:

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. Gestión de Incidentes de Seguridad de la Información

16.1 Gestión de incidentes de seguridad de la información y mejoras

***Objetivo*:** Garantizar un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre los eventos y debilidades de seguridad.

Controles:

16.1.1 Responsabilidades y procedimientos.

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.

17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

17.1 Continuidad de la seguridad de la información

***Objetivo*:** La continuidad de la seguridad de la información debe ser integrada en los sistemas de gestión de la continuidad del negocio de la organización.

Controles:

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias

***Objetivo*:** Asegurar la disponibilidad de las instalaciones de procesamiento de información

Controles:

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información.

Controles:

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información

Objetivo: Asegurar que la seguridad de la información sea implementada y opere de acuerdo con las políticas y procedimientos organizacionales.

Controles:

18.2.1 Revisión independiente de la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

18.2.3 Comprobación del cumplimiento.

Como una sección final en el estándar se indica la bibliografía, que en su mayoría son otros estándares de ISO que apoyan a los controles sugeridos por ISO/IEC 27002:2013.

2.9. Políticas de Seguridad de la Información

Según Barbosa Martins & Saibel (2005), una política de seguridad es un documento que debe describir las recomendaciones, las reglas, las responsabilidades y las prácticas de seguridad; sin embargo, se sabe que no existe una "política de seguridad modelo" que pueda ser implementada en cualquier organización, pues una política deberá ser moldeada según las especificaciones de cada caso; por lo tanto, elaborar una política de seguridad es una tarea compleja que necesita ser constantemente monitoreada, revisada y actualizada; además, sus resultados normalmente sólo se pueden observar a mediano y largo plazo. Es fundamental la existencia de políticas de seguridad que sean realmente una referencia para los colaboradores de una organización, posibilitando así la garantía de los tres principios básicos de la seguridad de la información: integridad, disponibilidad y confiabilidad (Barbosa Martins & Saibel, 2005).

La información en medios informáticos es altamente utilizada en todas las empresas, hogares,

instituciones educativas, etc., y por esta razón es importante determinar qué hacer para protegerla y evitar que caiga en manos de personas no autorizadas; obteniendo esta protección y seguridad mediante la implementación de políticas de seguridad informática (Posso, 2009).

Dussan (2006) indica que podemos definir la política como un instrumento gerencial que indica una dirección predeterminada describiendo la manera de manejar un problema o situación; indica también que las políticas son planteamientos de alto nivel que transmiten a los colaboradores de la empresa la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos formalmente y comunicados a todos los involucrados o partes interesadas dentro y en algunos casos fuera de la organización (Dussan, 2006).

Según ISO/IEC 27002 (2013), un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Las organizaciones perciben cada vez más a sus empleados como un activo importante que necesita ser cuidado; sin embargo, al mismo tiempo, consideran a los empleados como una de las mayores amenazas potenciales para su seguridad informática, pues la responsabilidad de los empleados es reconocida como una de las brechas de seguridad en las organizaciones, y es importante que se les preste la atención necesaria como a los aspectos técnicos de la seguridad de la información (Alotaibi *et al.*, 2016).

Alotaibi *et al.* (2016) indican que se debe continuamente brindar a los usuarios una sensibilización y capacitación en la seguridad informática y en las políticas de seguridad vigentes en una organización, supervisando dinámicamente su adhesión a las políticas de seguridad de la información, lo cual debería aumentar el nivel de su cumplimiento.

Dussan (2006) indica que una política de seguridad se considera como un conjunto de directrices, normas, procedimientos instrucciones que guían las tareas del trabajo y definen los criterios de seguridad para que sean adoptados en toda la organización o una parte de ella, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico.

- El ámbito tecnológico se refiere a los esfuerzos que se deben realizar para el buen funcionamiento de la plataforma de hardware, software y telecomunicaciones; que incluyen por ejemplo servidores, estaciones de trabajo, sistemas operativos, bases de datos, acceso a Internet etc. A veces se relacionan directamente los problemas de seguridad informática con el área tecnológica sin embargo es importante enfatizar que en este tema de seguridad se debe partir de la ética profesional y la buena conducta de los usuarios informáticos.
- El ámbito humano se refiere a todos los individuos involucrados en una organización se vuelven

usuarios informáticos: proveedores, clientes, empleados, instituciones externas etc. y a ellos deben dirigirse los recursos y esfuerzos por mantener la seguridad de la información. Este aspecto va muy ligado a la cultura organizacional y de seguridad y cómo se integran en sus actividades diarias aspectos como la ética, la responsabilidad, capacitación y el mejoramiento continuo.

2.10. Metodologías para la Gestión de Políticas de Seguridad de la Información

Barbosa Martins & Saibel (2005) presentan una propuesta para la elaboración e implementación de un SGSI en una organización, la cual se basa en estándares y normas internacionales (TECSEC, 1985), (ISO 15408:1999), (ISO/IEC TR 13335:1998), (BS7799-2:2001), (ISO/IEC 17799:2001), (IEC 61508:1998) y en la primera etapa de la metodología propuesta, describen el método utilizado para la construcción de políticas de seguridad en una organización basado en el estándar ISO/IEC17799, actualmente conocida como la norma ISO/IEC 27002. Esta metodología, según Barbosa Martins & Saibel (2005), se utiliza para construir políticas de seguridad de la organización, que las consideran como un documento que debe describir las recomendaciones, reglas y responsabilidades y las prácticas de seguridad e indican también que elaborar políticas de seguridad informática es una tarea complicada que implica un constante monitoreo, revisión y actualización, además, sus resultados normalmente podrán ser notados solamente a mediano y largo plazo.

En la Figura 2.10 se resume la metodología de Barbosa Martins & Saibel (2005), donde se puede visualizar el modelo de desarrollo de políticas presentado por estos autores, el cual empieza por un proceso de conformación de un comité de seguridad creado para ser responsable de la gestión de la seguridad de la información, por tanto, este grupo es el encargado de proponer las políticas necesarias para la gestión de la seguridad de la información. Posteriormente este comité interviene en las etapas: la clasificación de la información como la información crítica o relevante que debe ser protegida, la definición de objetivos y alcance de la seguridad de la información que deben ser atendidos en la organización, el análisis de las necesidades de seguridad, la elaboración de las políticas de seguridad de la información propuestas y su discusión con los involucrados en la organización, llegando a consensos y presentando como entregable un documento formal a la dirección de la empresa, la cual lo revisará y aprobará para la posterior implementación y difusión mediante capacitaciones de concientización sobre seguridad informática al personal de la organización.

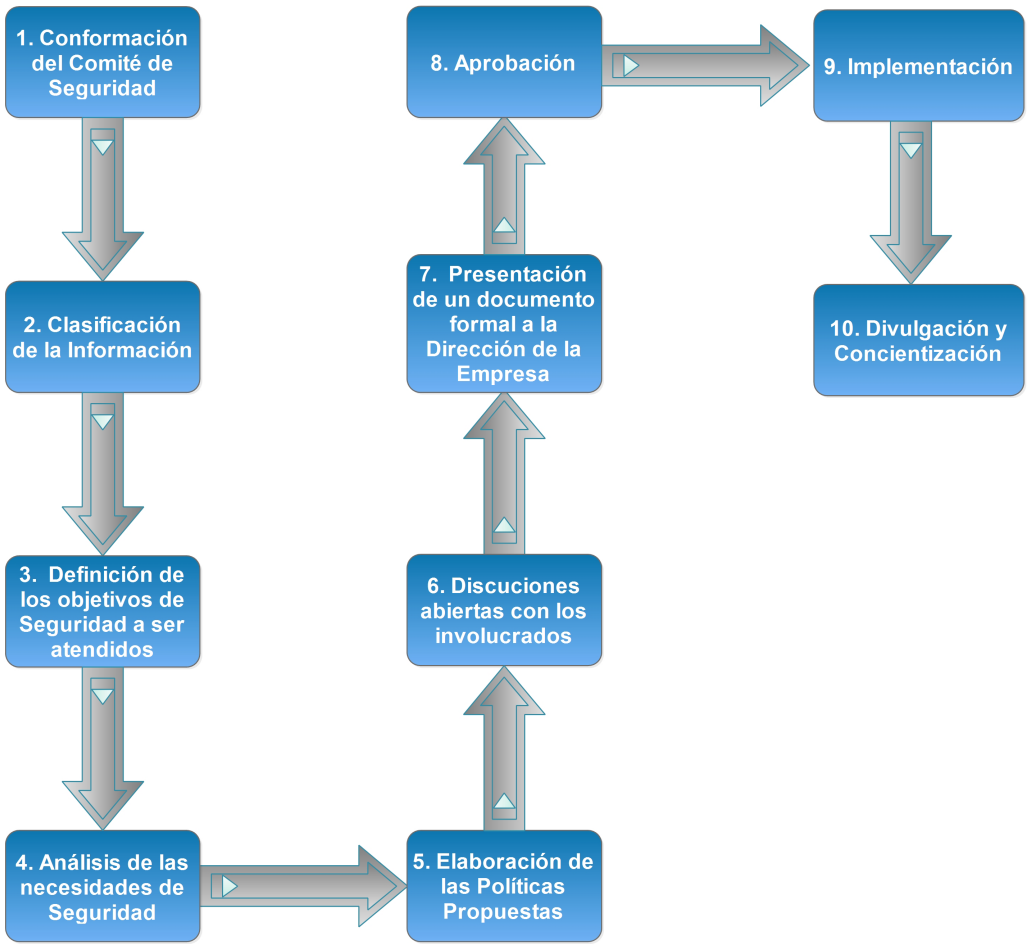

Figura 2.10. *Metodología de Desarrollo de Políticas de Seguridad (Barbosa Martins & Saibel, 2005)*

Las políticas de Seguridad deberán presentar algunas características como ser aprobadas por el directorio, divulgadas y publicadas de forma clara para todos los colaboradores de la organización; así también deben ser revisadas regularmente, y estar en conformidad con la leyes y cláusulas contractuales en la organización. Además se debe definir las responsabilidades generales y específicas del personal en cuanto a la seguridad de la información, así como contener las consecuencias en caso de su incumplimiento (Barbosa Martins & Saibel 2005).

Barbosa Martins & Saibel (2005) señalan que es fundamental la existencia de una política de seguridad que sea realmente una referencia para los colaboradores de una organización, posibilitando una garantía de los tres principios básicos de la seguridad de la información: la integridad, disponibilidad y confiabilidad.

Bustamante *et al.* (2017) proponen una metodología para la gestión de la seguridad de la información de los Sistemas de Control Industrial o *Industrial Control System* (ICS), basándose en las normas emitidas por el NIST (*National Institute of Standards and Technology*), específicamente en la

norma *NIST 800-82* que es una Guía de Seguridad para Sistemas de Control Industrial y la norma *NIST 800-30* que es una Guía para la gestión de riesgos de Sistemas de TI. La metodología presentada por Bustamante *et al.* (2017) consiste en una serie de etapas como aportes, como un grupo de estrategias para reducir los riesgos, una guía de instrucciones y las políticas de seguridad para la gestión eficaz de la seguridad de la información basadas en las normas NIST. La estructura de esta metodología enfocándose sobre todo en la parte del desarrollo de las políticas de seguridad se puede observar en la Figura 2.11.

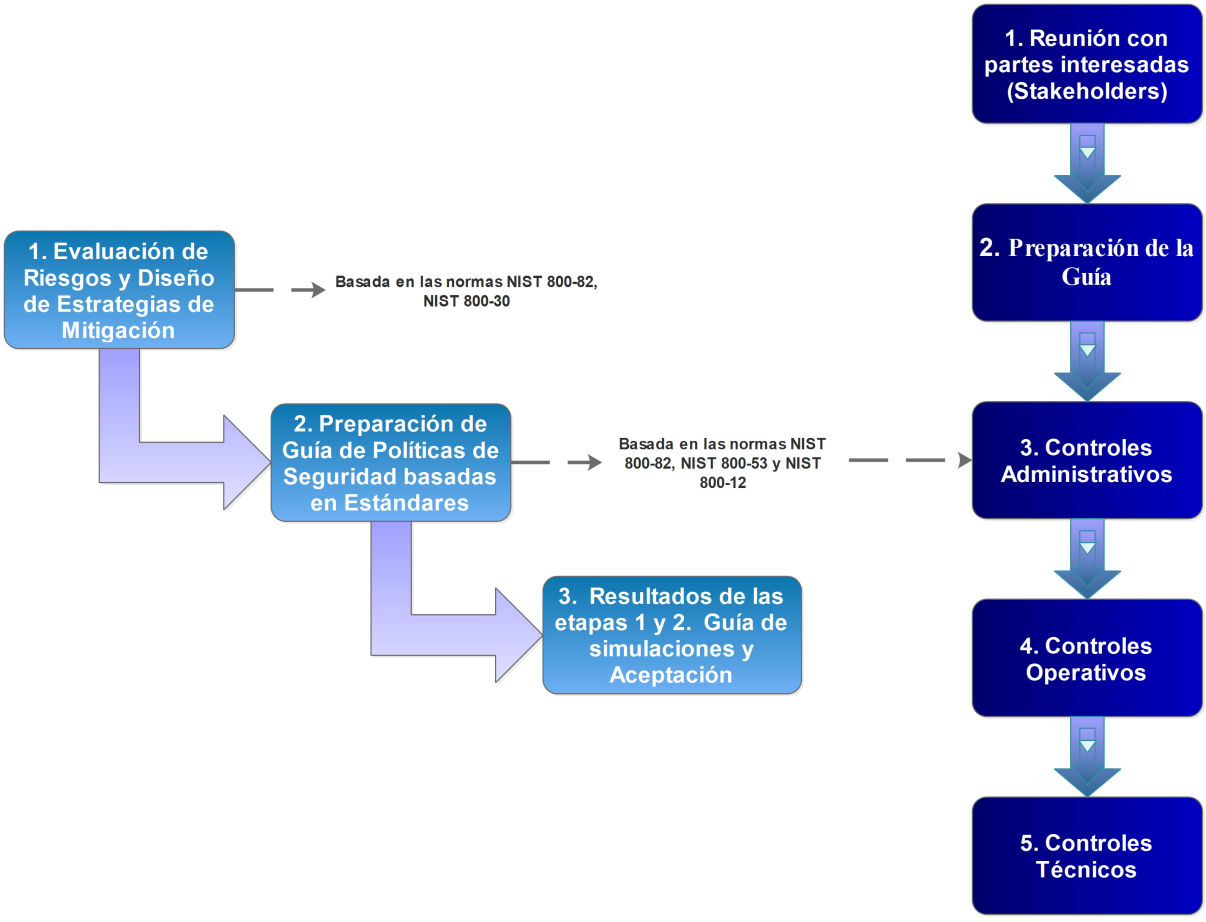

Figura 2.11. *Metodología de Gestión de Seguridad de la Información para sistemas ICS y Desarrollo de Políticas de Seguridad (Bustamante et al., 2017)*

La metodología propuesta por Bustamante *et al.* (2017), que se visualiza en la Figura 2.11, en su parte de desarrollo de políticas de seguridad de la información contiene los siguientes procesos:

1. **Reunión con las partes interesadas (stakeholders):** El propósito de estas reuniones es encontrar los requisitos del proyecto y los controles de seguridad que ya están implementados.
2. **Preparación de la guía:** Los estándares de referencias normativas se toman en consideración en esta etapa, como antecedentes técnicos y guía para desarrollar las políticas de seguridad. El

formato de la Guía se estructura en tres secciones con controles de tipo administrativo, operativo y técnico.

3. **Controles administrativos:** Son medidas o controles de seguridad para un Sistema de Control Industrial (ICS) que se enfocan en la gestión del riesgo y en la gestión de la seguridad de la información como son la evaluación de la seguridad y autorización, planificación, evaluación de riesgos, adquisición de sistemas y servicios y la gestión de programas.
4. **Controles operativos:** Son medidas de seguridad de un ICS, que son implementadas y ejecutadas principalmente por personas: seguridad del personal, protección física y ambiental, plan de contingencia, gestión de la configuración, mantenimiento e integridad del sistema de información, protección de los medios de comunicación, respuesta a incidentes de seguridad y entrenamiento de sensibilización en seguridad informática.
5. **Controles técnicos:** Este tipo de controles de seguridad para un ICS, son implementados y ejecutados principalmente por un sistema a través de mecanismos que contienen hardware, software o firmware; por ejemplo la identificación y autenticación, control de accesos, auditoría y responsabilidad, protección de sistemas y comunicaciones.

Según Knapp *et al.* (2009), se han definido algunos modelos de buenas prácticas de seguridad, sin embargo están más dirigidos hacia la creación de una cultura de seguridad de la información facilitando el pensamiento conceptual y la argumentación del recurso humano en las organizaciones, que a una definición estricta y especifica de políticas centradas en la seguridad de procesos corporativos de los diferentes tipos de organización y su interrelación con el recurso humano; por lo que en su trabajo de investigación, los autores presentan una metodología cíclica para el desarrollo y gestión de políticas de seguridad de la información. En la Figura 2.12 se ilustran los procesos de esta metodología.

Según el método de Knapp *et al.* (2009), el proceso inicia con la identificación y evaluación de riesgos para el desarrollo de las políticas y su posterior aprobación; teniendo luego una tarea cíclica que es la concientización y entrenamiento al personal en las políticas planteadas procediendo después a su implementación y su monitoreo continuo una vez implementadas mediante auditorías o herramientas automatizadas para proceder a una aplicación estricta de estas políticas con recompensas por su correcta aplicación o la respectiva sanción en caso de que no se cumpliesen. Finalmente las políticas pasan por un proceso de revisión y en caso de que necesiten ser modificadas debido a los continuos avances y riesgos de la tecnología, se repite el ciclo desde el proceso de evaluación de riesgos; pero si finalmente la política ya no es necesaria o es sustituida por otras que son más adecuadas, se procede a su retiro (eliminación definitiva).

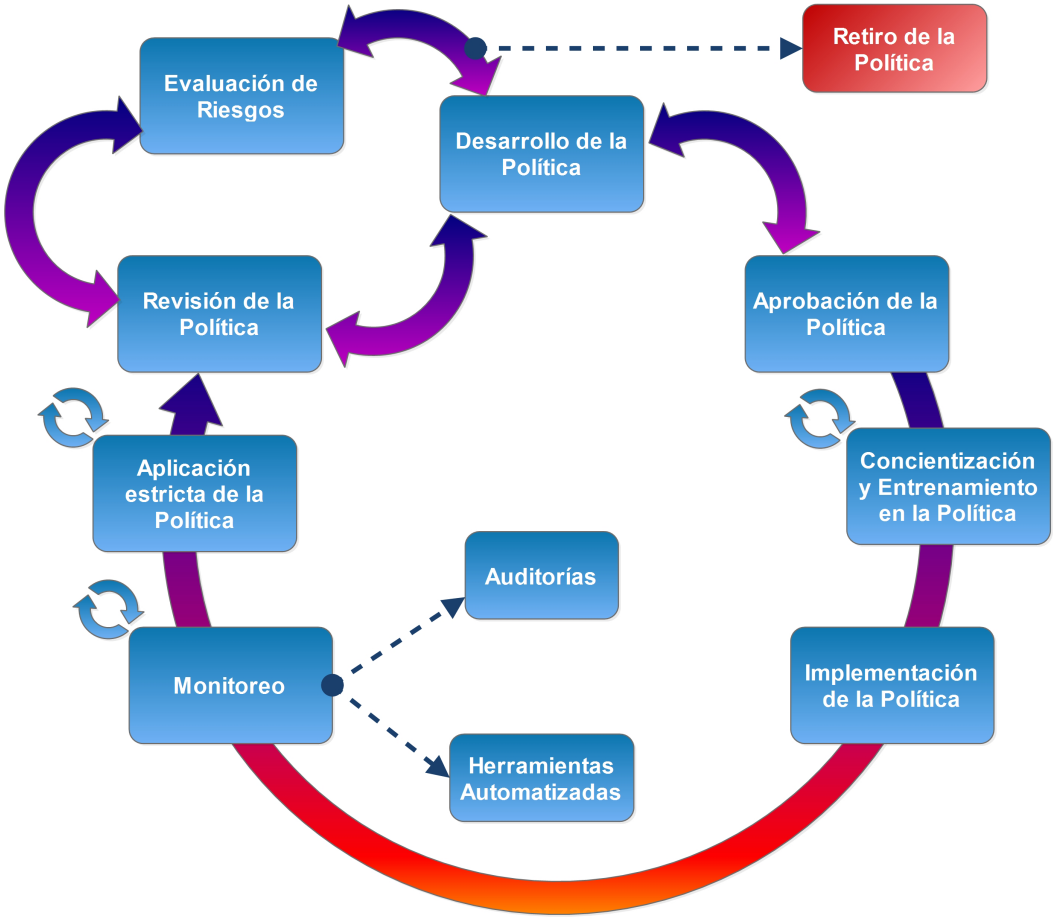

Figura 2.12. *Metodología integral para la Gestión de Políticas de Seguridad (Knapp et al., 2009).*

Las flechas dobles entre cuatro de los procesos de gestión de políticas (revisión de políticas, evaluación de riesgos, desarrollo de políticas y aprobación de políticas) representan la interacción frecuente y la iteración entre estas actividades que ocurren en las organizaciones. Por ejemplo, si una autoridad desaprueba una política propuesta, es posible que los desarrolladores tengan que volver a escribir o revisar una política basada en la retroalimentación de la autoridad de aprobación. Las flechas simples ilustran el flujo secuencial general desde la etapa de aprobación de políticas hasta la fase de revisión de políticas; sin embargo, esta secuencia general no implica una progresión lineal rígida, ya que algunas etapas son concurrentes.

La línea punteada para el retiro de las políticas refleja que a veces, durante la revisión de las políticas, la evaluación de riesgos y el desarrollo de políticas, una organización puede decidir que ciertas políticas ya no son necesarias y por lo tanto deben ser retiradas. En la fase de monitoreo, las líneas punteadas conducen a dos subcategorías claves: auditorías y herramientas automatizadas; por ejemplo el uso de herramientas automatizadas que ayudan en el trabajo tedioso de la supervisión de las operaciones que hacen los empleados. Las flechas de iteración semicirculares representan fases que

tienen una dimensión vital y continua como es el caso de las etapas de capacitación y entrenamiento en las políticas y el monitoreo de las mismas.

Aunque la concientización y la formación son etapas muy importantes deben seguir la etapa de aprobación formal de las políticas, se debe tomar en cuenta en la capacitación algunos eventos para recordar a los empleados la importancia de las políticas de seguridad y la seguridad informática de la organización en general. En conclusión el modelo ilustra la iteración de procesos individuales (por ejemplo, capacitación y entrenamiento sobre políticas), iteración de partes del modelo (entre revisión de políticas, evaluación de riesgos, desarrollo de políticas y aprobación de políticas) e iteración de todos los procesos del modelo cíclico completo.

Esta metodología involucra técnicas cualitativas, desarrollando un modelo de procesos de políticas de seguridad de la información basado en las respuestas de una muestra de profesionales certificados en seguridad de la información y como principal contribución de este estudio de investigación, el modelo propuesto ilustra un proceso de una política general e integral en una forma distintiva de otros estándares profesionales o publicaciones académicas existentes (Knapp *et al.*, 2009); por estas razones, se escogió esta como la metodología base para la elaboración y gestión de políticas de seguridad de la información en el presente trabajo.

2.11. Las Industrias de Producción

Stouffer *et al*. (2015) indican que la manufactura presenta un sector industrial grande y diverso con muchos procesos diferentes, que se pueden categorizar en *fabricación basada en procesos* y *fabricación discreta*. Las industrias manufactureras basadas en *procesos* usan típicamente dos procesos principales:

- **Procesos continuos de fabricación:** Estos procesos se ejecutan continuamente, a menudo con transiciones para hacer diferentes tipos de un producto. Los procesos de fabricación continua típicos incluyen por ejemplo el flujo de combustible o vapor en una planta de energía, el petróleo en una refinería y la destilación en una planta química.
- **Procesos de fabricación por lotes:** Estos procesos tienen etapas de procesamiento distintas, llevadas a cabo sobre una cantidad determinada de material. Hay un inicio y final en cada proceso por lotes con la posibilidad de operaciones breves de estado estable durante las etapas intermedias. Los procesos típicos de fabricación por lotes incluyen las industrias de fabricación de alimentos. Se ilustran con ejemplos estos procesos de producción en la Figura 2.13.

Figura 2.13. *Ejemplos de Procesos de Fabricación por Lotes y Procesos de Fabricación Continuos.*

Las industrias de fabricación basadas en *fabricación discreta* típicamente llevan a cabo una serie de pasos en un único dispositivo para crear el producto final. Ejemplos comunes de este tipo de industrias son las de montaje de piezas electrónicas y mecánicas o ensamblaje de piezas. Tanto las industrias basadas en procesos como las discretas utilizan los mismos tipos de sistemas de control, sensores y redes; teniendo casos donde algunas instalaciones son un híbrido de fabricación discreta y basada en procesos (Stouffer *et al*., 2015).

Tradicionalmente un ambiente industrial presenta particularidades que deben tener en cuenta su protección mediante la seguridad de la información, ya que tienen por ejemplo información sobre nuevos proyectos o productos, transformaciones, creaciones e innovación de productos finales o materia prima que reviste mucha importancia e interés para otras industrias de su sector. Según Dos Santos *et al.* (2010), estos productos son la fuente de vida de muchas organizaciones, que por la importancia de su información que circula dentro de la organización a través de varias funciones y atribuciones de sus empleados, debe ser constantemente protegida, pues toda información referente a un proceso industrial es un activo importante para la industria.

Sauer (2014) sostiene que las tecnologías de la información comunicaciones (TIC) son un factor clave para la fábrica del futuro, actuando como una "tecnología facilitadora". Para la producción, las TIC son una herramienta, no un fin en sí mismo y en el futuro, las plantas de producción estarán cada vez más apoyados por los componentes TIC (Sauer, 2014).

2.11.1. Industria 4.0

Según Rüßmann *et al*. (2015), ahora mismo estamos ya en medio de una cuarta oleada de avance tecnológico en la industria: el surgimiento de la nueva tecnología industrial digital conocida como "*Industria 4.0*", una transformación que está impulsada por avances tecnológicos fundamentales soportados por las TICs. En esta transformación, sensores, máquinas, piezas de trabajo y sistemas de TI estarán conectados a lo largo de la cadena de valor más allá de solamente la empresa, ya que estos sistemas interconectados (también conocidos como sistemas cibernéticos) pueden interactuar entre sí utilizando protocolos estándar basados en Internet y analizar datos para predecir errores, autoconfigurarse y adaptarse a los cambios. *Industria 4.0* permitirá reunir y analizar datos entre máquinas, por ejemplo con el Internet de las cosas (IoT por sus siglas en inglés), permitiendo procesos más rápidos, flexibles y eficientes para producir bienes de mayor calidad a costos reducidos, a su vez que aumentará la productividad de la manufactura, cambiará la economía, fomentará el crecimiento industrial y modificará el perfil de la fuerza de trabajo, cambiando finalmente la competitividad de las empresas (Rüßmann *et al*., 2015).

Citando a Hermann (2016), esta revolución industrial ha sido precedida por otras tres revoluciones industriales en la historia: la primera revolución industrial fue la introducción de instalaciones de producción mecánicas a partir de la segunda mitad del siglo XVIII e intensificación a lo largo de todo el siglo XIX; a partir de la década de 1870, la electrificación y la división del trabajo (introducida por Taylor) condujeron a la segunda revolución industrial; la tercera revolución industrial, también llamada "revolución digital", se inició en los años setenta, cuando la electrónica avanzada y la tecnología de la información (TI) desarrollaron aún más la automatización de los procesos de producción (Drath & Horch, 2014) (Hermann, 2016).

El término "*Industria 4.0*" se hizo público en 2011, cuando esta iniciativa nació de una asociación de representantes de empresas, política, y academia cuando apoyaron la idea de consolidar la competitividad de la industria de fabricación alemana. Los promotores de esta idea esperan que brinde mejoras fundamentales a los procesos industriales involucrados en la fabricación, la ingeniería, el uso de materiales y la cadena de suministro y la gestión del ciclo de vida de los procesos en las industrias. La Industria 4.0 se sustenta principalmente en nueve tecnologías como se ilustra en la Figura 2.14: Big Data y análisis, Robots autónomos, Simulación, Sistemas de Integración Horizontal y Vertical, Internet Industrial de las Cosas (IoT), Ciberseguridad, Computación en la Nube, Fabricación Aditiva y Realidad Aumentada.

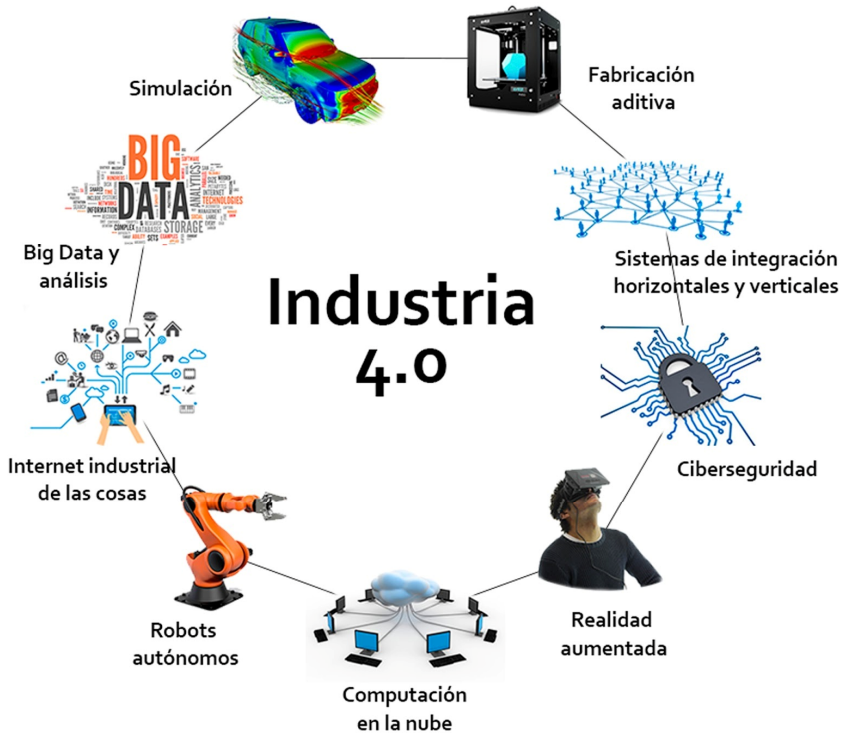

Figura 2.14. *Tecnologías que sustentan la Industria 4.0.*

2.11.2. CiberEspionaje Industrial

El espionaje Industrial es definido por Sinha (2012) como "la adquisición de secretos comerciales de los competidores de negocios", indicando también que el espionaje industrial es una reacción a los esfuerzos de muchas empresas para mantener en secreto sus diseños, fórmulas, procesos de fabricación, investigación y planes futuros para proteger o ampliar sus acciones en el mercado.

Según Raiu (2014), en su informe para Kaspersky Lab, indica que muchos ataques cibernéticos pueden ser mitigados con medidas relativamente simples; sin embargo, algunas empresas y personas no llegan a tomar lo que serían precauciones básicas de seguridad, tales como el uso de contraseñas seguras, aplicar parches al software y ejecutar aplicaciones de seguridad actualizadas, facilitando así en muchos casos irrumpir en la red de una empresa de una manera muy simple.

Raiu (2014) indica también que el espionaje industrial ha sido una característica de la vida de las empresas por un largo tiempo; sin embargo, en los últimos años se ha producido un cambio drástico en el nivel y la naturaleza de las amenazas de espionaje que pueden afectar a empresas de todos los tamaños y naturaleza. El espionaje, de una forma u otra, ha existido desde que varias organizaciones o individuos han considerado que podrían obtener una ventaja obteniendo de manera ilícita la información

confidencial de alguien más, por ejemplo a nivel mundial, se han conocido y descubierto intentos de algunas naciones para robar los secretos de otros países (Raiu, 2014).

Con el esquema actual de "conectividad siempre disponible" en las organizaciones, al tener varios equipos y dispositivos conectados a Internet, se expone la información de la empresa y otros datos delicados, creando más oportunidades atractivas para los ciberdelincuentes.

Debido a que las empresas guardan su propiedad intelectual e información confidencial en sistemas conectados a la red, las operaciones de espionaje son más fáciles de implementar y pueden ser mucho más gratificantes para los perpetradores (Raiu, 2014). En el estudio que realiza Raiu (2014), indica que con las habilidades suficientes de un hacker informático, los individuos y organizaciones pueden espiar a empresas y obtener información valiosa, sin jamás haber salido de la comodidad de su oficina, por ejemplo las empresas pueden ser atacadas por fallas de seguridad en su propio sitio web, a través de puntos vulnerables del software común para negocios que están utilizando o como resultado de que sus empleados descarguen correos electrónicos infectados con malware.

Cuando un ciberdelincuente roba información, el robo puede neutralizar cualquier ventaja de la que disfrutaba el propietario original de dicha información; esto se aplica tanto si el objetivo es un estado o nación que posea secretos militares o una empresa con propiedad intelectual y secretos comerciales o profesionales que les signifique una ventaja competitiva para el ciberdelincuente o para la competencia de la empresa.

Según Sinha (2012), las empresas se dedican a actividades de espionaje principalmente por tres motivos: la primera es ganar un rápido aumento en sus ingresos o beneficios económicos; la segunda es convertirse en un líder del mercado en virtud de productos novedosos e innovadores o de una enorme capitalización de mercado, obtenidos robando la información o ideas novedosas de sus competidores; la tercera es la capacidad de influir en las políticas económicas de los organismos gubernamentales o de control relacionadas con sus industrias.

Según Raiu (2014), el ciberespionaje puede causar pérdidas como la pérdida de la reputación o la pérdida directa de la información crítica para una empresa; cualquiera de las dos implica una pérdida económica, muchas veces incuantificable. En la Figura 2.15, se muestran los resultados de una encuesta sobre riesgos de seguridad global corporativa de TI realizada en el año 2013, por la empresa B2B Internacional (https://www.b2binternational.com/), donde se indican los porcentajes de las empresas encuestadas que han sufrido ciberespionaje por cada tipo de pérdidas que tuvieron.

La infraestructura de espionaje industrial puede variar desde el simple caso de que una empresa espíe a otra a los complejos casos en que los gobiernos también están involucrados indirectamente. (Sinha, 2012). Una organización con fallas o debilidades en su seguridad informática se puede usar

como la primera etapa de un ataque contra otra organización similar o más grande del sector público o privado que si tenga implementada una seguridad más robusta, ya que mediante la primera el atacante puede entrar a los sistemas o servicios prestados y compartidos con la empresa objetivo (Raiu, 2014).

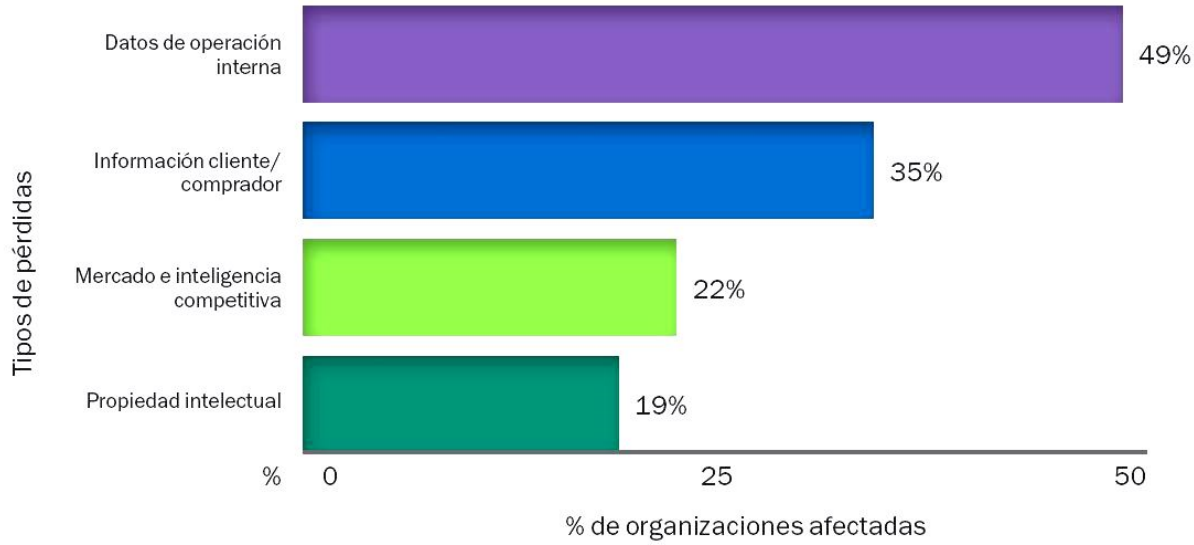

Figura 2.15. *Pérdidas ocasionadas por fuga de datos y ciberespionaje.*
Fuente: (B2B Internacional, 2013) (Raiu, 2014).

Para hacer frente a los peligros de seguridad y el ciberespionaje, Raiu (2014) concluye que uno de los puntos importantes es que todas las empresas evalúen los riesgos actuales que podrían aplicar a su negocio y a continuación, establezcan su propia política de seguridad; por lo cual en el capítulo 4 se realiza una propuesta que contempla una metodología con estas dos actividades esenciales dentro de la seguridad informática.

Capítulo 3. Estado Actual de la Investigación

En este capítulo se analiza el estado del arte sobre la temática tratada en el presente trabajo. Se realiza una revisión de los estudios y trabajos de investigación que se han realizado hasta el momento con el objetivo de que el lector tenga una visión global sobre el estado actual de investigación respecto a temas como la seguridad de la información, las metodologías de identificación y gestión de riesgos tecnológicos y el desarrollo de políticas de seguridad informática.

3.1. Seguridad de la Información

Cano (2004) en su trabajo de investigación desarrolla un análisis y reflexión donde sugiere repensar la seguridad informática como un proceso continuo entre técnicas de hacking ético y análisis de riesgos, que permita a las organizaciones aprender de sus fallas de seguridad y fortalecer así sus esquemas de seguridad, no para contar con mayores niveles de seguridad, sino para evidenciar el nivel de dificultad que deben asumir los intrusos para intentar ingresar a sus sistemas. Con un pensamiento de este nivel, el autor indica que las organizaciones no buscarán solamente incrementar la confianza de sus clientes, sino comprender que la seguridad no es un problema de tecnología y más bien es un problema de riesgos y las diferentes maneras de comprenderlos y gestionarlos o mitigarlos e indica que mientras más se conoce la inseguridad informática de una organización, más se puede comprender las acciones y controles respecto a la seguridad que se deberían aplicar en la misma.

Goldes *et al.*, (2017) indican que la seguridad de la información es un tema de creciente importancia para las organizaciones de hoy ya que la profesionalización y la industrialización del delito cibernético, la globalización y la digitalización de los modelos empresariales junto con el creciente enfoque regulatorio en la protección de datos ejerce presión sobre las organizaciones para implementar sofisticados Sistemas de Gestión de Seguridad de la Información (SGSI). Las mejores prácticas para implementar estos sistemas están dadas por múltiples estándares de la industria, mientras que los planes de diseño para un SGSI son relativamente escasos (Goldes *et al*, 2017). Estos autores discuten sobre los requisitos de diseño para un moderno Sistema de Gestión de Seguridad de la Información, presentando un plan viable para tal sistema, ejemplificando con un caso de estudio en una empresa de seguros.

Con la creciente dependencia que la sociedad de la información tiene de las Tecnologías de la Información y las Comunicaciones (TIC), la necesidad de proteger la información tiene cada vez mayor relevancia para las empresas y en este contexto, surgen los Sistemas de Gestión de la Seguridad de la Información (SGSI), que son una parte importante para la estabilidad de los sistemas de información de las compañías y el hecho de poder disponer de estos sistemas ha llegado a ser cada vez más vital para la evolución de las PYMES (Sánchez *et al.*, 2009); estos autores proponen en su trabajo de investigación

una metodología para el desarrollo, implantación y mantenimiento de un SGSI, adaptada a las necesidades y recursos que disponen las PYMES con un enfoque aplicado a casos reales de este tipo de empresas.

Respecto a la privacidad de la información, que es parte de la seguridad de la misma de acuerdo al principio de confidencialidad, existen estudios de investigación como el de Agustina (2009), en donde se realiza una revisión considerando algunos fundamentos ético-jurídicos de los conflictos entre la privacidad de los trabajadores y las necesidades de prevención del delito en la empresa mediante el uso de TI (Tecnologías de la Información) como son los sistemas de video-vigilancia. El autor indica que en el interior de una empresa, se originan ciertos deberes de vigilancia y control del empresario respecto a los delitos que llegan a cometerse en el entorno de la organización, sin embargo se originan también determinados límites legales que derivan del debido respeto a la privacidad del trabajador y, en base a tales límites, la implementación de estrategias de prevención y controles debe realizarse conforme a ciertos principios logrando un equilibrio entre los intereses contrapuestos de ambas partes (Agustina, 2009).

Se debe tener especial cuidado en verificar la integridad y asegurar que los datos sensibles en una organización estén adecuadamente protegidos y una de las actividades claves para la prevención de la pérdida de datos es la auditoría (Roratto & Dotto, 2014). Estos autores en su trabajo de investigación indican que para poder auditar un sistema informático, es importante contar con registros fiables de sus actividades y por ello los sistemas que almacenan datos críticos, ya sean financieros o productivos, deben tener características tales como el registro de auditoría, también llamado rastro de auditoría, el cual registra todas las actividades sobre los datos críticos, ya que esto permite identificar acciones dañinas que pueden ser internas o externas, provocadas intencionalmente o no. Roratto & Dotto (2014) presentan en su trabajo un análisis y estudio de lo que son los rastros en la auditoría de seguridad informática (registros o logs de auditoría), dando a conocer las herramientas comerciales disponibles en la actualidad y lo que pueden ofrecer respecto a este tema.

El cifrado es la ciencia que escribe o lee mensajes codificados y es considerada una de las técnicas para la protección de la información; siendo también un mecanismo básico para todas las comunicaciones seguras; para ello, es necesario conocer las tres funciones criptográficas básicas: el cifrado simétrico, el cifrado asimétrico y las funciones hash unidireccionales (Kaeo, 2003). La mayor parte de tecnologías vigentes de autenticación, integridad y confidencialidad se derivan de estas tres funciones de cifrado.

Las investigaciones sobre seguridad de la información y Sistemas de Gestión de Seguridad de la Información (SGSI) han examinado las normas internacionales de seguridad, como ISO/IEC 27001 (ISO 27001, 2013), BS 17799 (Barbosa Martins & Saibel, 2005) actualmente ISO 27002 (ISO 27002, 2013), PCIDSS (PCI, 2013), ITIL (Axelos, 2017), COBIT (ISACA, 2012), entre otras consideradas

guías estandarizadas que sugieren buenas prácticas de seguridad ayudando a las organizaciones a gestionar eficazmente la seguridad de sus datos y de sus activos de información (Gicas, 2010) (Susanto *et al.*, 2011) (Gillies, 2011) (Tsohou *et al.*, 2010) (Benslimane *et al.*, 2016).

En cuanto a los estándares que tratan sobre la seguridad de la información, existen trabajos como el de Montaño (2011), en donde se realiza una comparativa de marcos de referencia de seguridad informática como Cobit (ISACA, 2012), ITIL (Axelos, 2017) e ISO 27000 (ISO 27000, 2009) indicando que, la experiencia en varias organizaciones demuestra que resulta muy complicado implementar un Sistema de Gestión de Seguridad de la Información (SGSI) sin basarse en una revisión de este tipo de modelos y estándares, mencionando también que de existir en la organización un SGSI se lo puede mejorar mediante la inclusión de áreas de aplicación ISO 27000 (ISO 27000, 2016), o midiendo el estado de madurez del SGSI a través de Cobit (ISACA, 2012) o ITIL (Axelos, 2017).

El trabajo presentado por Humphreys (2011) analiza el estándar de seguridad ISO / IEC 27001 (ISO 27001, 2013), como la norma de seguridad de la información más exitosa de ISO, junto con las otras normas de la familia de estándares de seguridad de la información (denominadas ISO / IEC 2700x). En este trabajo se examina brevemente la historia y el progreso de estos estándares, de donde se originaron, cómo se relacionan entre ellos y cómo se convirtieron en el lenguaje común de las organizaciones de todo el mundo para mantener la seguridad de su información y operaciones, siendo implementados y aplicados en la práctica en los sectores empresariales, financieros, comerciales y gubernamentales. En sus conclusiones también realiza una breve presentación de lo que conlleva el proceso de certificación para un SGSI con las normas ISO 2700x.

Los estándares de seguridad se pueden utilizar como guías o marcos de trabajo para desarrollar y mantener un adecuado Sistema de Gestión de la Seguridad de la Información (SGSI), siendo los estándares ISO / IEC 27000 (ISO 27000, 2016), 27001 (ISO 27001, 2013) y 27002 (ISO 27002, 2013) internacionalmente reconocidos y adoptados como un "lenguaje común para las organizaciones alrededor del mundo" para la seguridad de la información (Humphreys, 2011)(Disterer, 2013).

El estándar ISO/IEC 27001: 2013 (ISO 27001, 2013) es la norma dada por las organizaciones ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), la misma que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del contexto de una organización e incluye también los requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001 (2013) son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza (ISO 27001, 2013). El contar con estos estándares genéricos, como los mismos señalan para ser aplicables a cualquier tipo de empresa, hace necesaria la investigación de su aplicabilidad en ciertos tipos de empresas específicas como las empresas

industriales de alimentos.

Los trabajos de investigación sobre los SGSI han cubierto la adopción de los estándares de seguridad identificando las razones para ello, incluyendo el tiempo y el coste que conlleva su implementación, su complejidad y además su falta de guías para su implementación (Gillies, 2011) (Benslimane *et al.*, 2016), su carácter excesivamente genérico (Siponen & Wilson, 2009) (Benslimane *et al.*, 2016), sumado al hecho de que el cumplimiento de los estándares de seguridad no garantiza una seguridad efectiva (Duncan & Whittington, 2014) (Wiander, 2008) y el hecho de que las certificaciones en un SGSI no mejoran el valor de las acciones de una organización o su rentabilidad (Wander, 2007) (Fomin *et al*., 2008) (Hsu *et al*., 2016) hacen que sea necesario la adaptación de los estándares de seguridad de la información para ciertos tipos de empresas en particular, según su naturaleza y necesidades. Sin embargo, para las organizaciones que adoptaron una norma o estándar de seguridad, la reducción de los costes de seguridad, la adopción de mejores prácticas, la prevención de incidentes de seguridad y la presión de sus clientes, socios y competidores fueron los principales impulsores para esa adopción (Wander, 2007) (Hone, 2002) (Benslimane *et al.*, 2016).

El trabajo presentado por Benslimane *et al.* (2016), investiga el papel relativo de los estándares de seguridad, las certificaciones profesionales de seguridad informática y las herramientas tecnológicas para la protección de la información en las organizaciones; los autores realizan el análisis del contenido de 100 trabajos publicados por analistas y gerentes de seguridad de la información concluyendo que, en general, las organizaciones dan mayor importancia al conocimiento validado por las certificaciones profesionales relevantes y al conocimiento práctico de los productos y soluciones de TI para la gestión de su seguridad de la información que al conocimiento de un estándar de seguridad en particular. En este estudio se indica también que existen organizaciones que por diversas causas no tienen y no buscan necesariamente una certificación en seguridad de la información, y en futuros trabajos se plantea investigar cómo se podrían usar y aplicar los estándares de seguridad en dichas organizaciones.

En el trabajo de titulación que presentan Pantaleone & Silva (2012), realizan un análisis de las herramientas disponibles que ayudan al cumplimiento de la norma ISO/IEC 27001 (ISO 27001, 2013), observando las características que éstas presentan y unificando criterios en cuanto a los requerimientos que debería tener un sistema ideal de gestión de seguridad de la información; para ello los autores realizan un estudio previo de la norma ISO/IEC 27001 (2013), que es la norma principal que sugiere los requerimientos de un Sistema de Gestión de Seguridad de la Información (SGSI), y de la norma ISO/IEC 27004 (ISO 27004, 2016), la cual sirve de apoyo para implementar el programa de medición del SGSI con el cual se puede medir la eficacia y eficiencia de los controles aplicados y posteriormente se realiza un estudio comparativo de las herramientas de monitoreo y cumplimiento disponibles como OSSIM, OpenNMS, Hyperic HQ, Securia SGSI y Easy2Comply; analizando en cada una de ellas los requerimientos de la norma ISO/IEC 27001 (ISO 27001, 2013) a la que dan soporte para finalmente

obtener en las conclusiones los requerimientos funcionales que una herramienta de gestión de seguridad de la información debería tener y que una organización debería considerar para lograr una certificación en el estándar ISO/IEC 27001 (ISO 27001, 2013).

Existe una diversidad de trabajos de investigación para algunos tipos de empresas en particular sobre la seguridad informática. Geramiparvar & Modiri (2015) realizan un estudio específico en los sistemas de banca electrónica para instituciones financieras e indican que, principalmente debido a la información financiera, crediticia y personal de los clientes, no sólo es esencial e importante la seguridad de la información, sino también forma una parte inseparable de todos los procesos y operaciones bancarias en dichas organizaciones; ya que si la seguridad se pone en riesgo, termina afectando la reputación de una institución financiera como una grave consecuencia. Su trabajo tiene como objetivo analizar los comportamientos de uno de los malware financieros más complicados y dañinos llamado Emmental e identificar y modelar sus patrones de comportamiento y sus amenazas a la seguridad de una institución financiera, utilizando un modelo métrico y proponiendo posibles políticas de seguridad como solución para detener y prevenir tales amenazas y ataques ocasionados por este tipo de malware.

Pinto (2006) analiza que en la actualidad son muchos los riesgos que afectan la seguridad de las empresas en nuestro país y por lo general el capital con el que se cuenta para protegerlas no es el suficiente, por lo que, al menos en base a alguna normativa se deben tener identificadas y controladas las vulnerabilidades de seguridad en una organización y esto se logra con un adecuado plan de seguridad elaborado en base a un análisis de riesgo previo, por ello es que Pinto (2006) presenta en su trabajo un diseño de un plan estratégico de seguridad de información en base a estándares internacionales como COSO (COSO, 2017), COBIT (ISACA, 2012) e ISO 27001 (ISO 27001, 2013) con un caso práctico en una empresa de tipo comercial.

Existen varias medidas se Seguridad de la Información recomendadas por los estándares internacionales y su literatura, sin embargo la adopción de dichas medidas en las organizaciones debería ser designada por las necesidades específicas identificadas de cada organización (De Albuquerque & dos Santos, 2015). El estudio de estos autores tuvo como objetivo investigar si en los institutos públicos de investigación la adopción de medidas de Seguridad de la Información está influenciada por factores organizacionales relacionados con la Gobernanza de la Seguridad de la Información y por factores externos relacionados con su entorno institucional. Los resultados muestran que estas organizaciones están sujetas a influencias institucionales más que a influencias organizacionales.

El comportamiento humano dentro de las organizaciones se considera como la principal amenaza para dichas organizaciones, además, en la seguridad de la información el elemento humano es considerado como el eslabón más débil en general (Mahfuth *et al.*, 2017). Por esta razón, en su trabajo de investigación los autores indican que es crucial crear una *Cultura de Seguridad de la Información*

para proteger los activos de la organización desde dentro y para influir en el comportamiento de seguridad de los empleados; en base a esto, Mahfuth *et al.* (2017) centran su trabajo en la identificación de las definiciones y marcos de trabajo para establecer y mantener una cultura de seguridad de la información dentro de las organizaciones; para ello llevan a cabo una revisión sistemática de la literatura de los documentos científicos publicados sobre la cultura de la seguridad de la información de 2003 a 2016. Su revisión identificó 68 artículos que se centran en esta área, 18 de los cuales proponen una cultura de seguridad de la información y, luego de realizar un análisis de estos documentos, concluye que hay una relación positiva entre los niveles de conocimiento sobre seguridad informática y el comportamiento de los empleados; por lo que el nivel de conocimiento de los empleados afecta significativamente su comportamiento respecto a la seguridad de la información y debe ser considerado como un factor crítico en la eficacia de la cultura de la seguridad de la información y por lo tanto, hay una necesidad de más estudios para identificar el conocimiento de seguridad que necesita ser incorporado en las organizaciones y encontrar las mejores prácticas para construir una cultura de seguridad de la información adecuada dentro de las organizaciones.

La seguridad de la información en el entorno industrial es un factor clave para el éxito de las organizaciones modernas, ya que se refiere a las características del producto y su proceso de fabricación; dicha información es muy sensible y no puede divulgarse a los competidores, bajo pena de incurrir en pérdida de la competitividad (dos Santos Roque *et al.*, 2010). Estos autores indican que la informatización en curso trae beneficios a la industria, ya que aumenta la cooperación entre las personas, pero también aumenta la vulnerabilidad de la seguridad de la información; como consecuencia, los modelos de gestión de la seguridad de la información también deben cambiar (dos Santos Roque *et al.*, 2010). Estos autores en su trabajo de investigación presentan un análisis sobre la temática de la seguridad de la información en entornos industriales y proponen un modelo dinámico de gestión de seguridad de la información en el que se priorizan la interacción, cooperación y motivación de directivos y empleados de una organización cumpliendo con los requisitos que consideran necesarios para lograr una adecuada gestión de seguridad de la información: la responsabilidad, confianza y la ética.

Los informes internacionales más recientes sobre temas de seguridad documentan un creciente número de ataques cibernéticos a los Sistemas de Control Industriales (ICS por sus siglas en inglés), por lo tanto, las implementaciones de Tecnologías de Información (TI) en los procesos de fabricación surgen ofreciendo soluciones en Seguridad de la Información por parte de los fabricantes y profesionales involucrados, ya que es notable también una tendencia en la que la seguridad de la información ha sido especialmente destinada a ser utilizada en las áreas administrativas de las empresas, donde la norma ISO-27000 (ISO 27000, 2016) es el estándar preferido; sin embargo, se ha determinado que no existen estudios de este estándar con un enfoque industrial, debido a que no se ha creado para estos sistemas (Bustamante *et al.*, 2017). En el contexto del trabajo de estos autores, se proponen un diseño e implementación de una metodología para la gestión de la seguridad de la información de los

Sistemas de Control Industrial, basándose en las normas emitidas por el NIST (National Institute of Standards and Technology), específicamente en la norma *NIST 800-82* (NIST, 2015) que es una Guía de Seguridad para Sistemas de Control Industrial y la norma *NIST 800-30* (NIST, 2002) que es una Guía para la gestión de riesgos de Sistemas de TI. La metodología presentada por Bustamante *et al.* (2017) consiste en una serie de etapas, las cuales aportan con dos contribuciones principales: en primer lugar un grupo de estrategias para reducir los riesgos y, en segundo lugar, una Guía de instrucciones basadas en normas, así como políticas de seguridad para la gestión eficaz de la seguridad de la información.

Las empresas que se dedican a actividades de espionaje industrial, lo hacen principalmente por tres razones: (i) La primera es ganar un rápido aumento en sus ingresos o beneficios, (ii) la segunda es convertirse en un líder de mercado en virtud de productos y procesos novedosos e innovadores antes que sus competidores y (iii) la tercera es la capacidad de contribuir con organismos gubernamentales para influir en las políticas económicas relacionadas con sus industrias Sinha (2012). Este autor presenta una visión general del espionaje industrial con una perspectiva de seguridad y privacidad para garantizar una mayor seguridad tecnológica y económica en las industrias, a través de estos conocimientos y práctica por parte sus profesionales, minimizando así el espionaje industrial.

Revisando estos trabajos respecto al tema de "Seguridad de la Información", se concluye que se han realizado varios estudios que indican que es un tema muy importante en la actualidad para las organizaciones de todo tipo ya que los riesgos y amenazas a los que están expuestas son cada vez más avanzados, considerando también la dependencia actual que la sociedad tiene de las TICs. Se tienen además estudios sobre la privacidad en los sistemas de TICs, los registros para auditorias de seguridad, el cifrado de la información y varios estudios sobre los estándares reconocidos internacionalmente como las normas de ISO (ISO 27000, 2016), NIST (NIST, 2015), COBIT (ISACA, 2012), ITIL (Axelos, 2017), COSO (COSO, 2017), donde sobre todo sobresalen las normas de la familia conocida como ISO / IEC 2700x, ya que son los estándares que sugieren las directrices para contar con un adecuado Sistema de Gestión de la Seguridad de la Información (SGSI) y su respectivo seguimiento.

El comportamiento humano dentro de las organizaciones también se considera como la principal amenaza de seguridad, por lo que se debe concientizar al personal sobre la importancia, conceptos y controles de seguridad informática, tanto a los usuarios de sistemas informáticos como a los profesionales de TI, evitando o reduciendo los riesgos informáticos a los que se enfrenta una organización, como por ejemplo el espionaje industrial en el caso de las empresas industriales. Sin embargo, se podría profundizar más en la manera de como las normativas aceptadas internacionalmente como las normas ISO se pueden aplicar para tipos específicos de empresas, como lo son las empresas industriales, considerando que tienen distintos procesos y se desenvuelven en distintos ambientes a los de otros tipos de empresas como comerciales o financieras, tomando en cuenta también la naturaleza

de sus operaciones, servicios o productos que se ofrecen en cada tipo de organización, por lo que las empresas industriales de manufactura, como son las de producción de alimentos, necesitan su propio modelo de gestión de seguridad de la información.

3.2. Metodologías de Gestión de Riesgos

Existen algunos trabajos relacionados con el planteamiento de metodologías de gestión de riesgos de seguridad como el de Bojanc & Blazic (2008), en donde se da a conocer un enfoque que permite el modelado económico de la gestión de riesgos de seguridad de la información para empresas contemporáneas, proponiendo un método para la identificación de los activos, amenazas y vulnerabilidades de los sistemas y un procedimiento que permite seleccionar la inversión óptima en tecnología de seguridad necesaria basada en la cuantificación de los valores de los sistemas que se protegen.

Eloff *et al.* (1993) indican que hace tres décadas atrás ya se viene demostrando la importancia de la seguridad de la información, con un especial énfasis en la seguridad de las redes, la recuperación de desastres y la gestión de riesgos. Una serie de estudios con enfoques automatizados para la facilitación del análisis de riesgos han aparecido en el mercado y las organizaciones no solo deben realizar la difícil tarea de ejecutar el análisis y gestión de riesgos, sino también de seleccionar el método que mejor se adapte a sus necesidades; para ello existen varios métodos disponibles, que utilizan terminología diferente para conceptos similares. El análisis de riesgos se utiliza principalmente para identificar los objetos que necesitan protección y los riesgos a los que están expuestos, mientras que la "gestión de riesgos" también podría incluirse como parte del análisis de riesgos, dependiendo de la funcionalidad del método utilizado. Los métodos automatizados de análisis de riesgos necesitan considerarse no sólo desde el funcionamiento interno del método, sino también desde el punto de vista terminológico (Eloff *et al.*, 1993), por lo que el trabajo que presentan estos autores, sugieren un marco de trabajo (framework) para la terminología utilizada en la gestión de riesgos y, para el desarrollo de este framework, consideran un análisis y discusión sobre los métodos de análisis de riesgos como CRAMM, LAVA y MELISA.

Solarte *et al.* (2015) en su trabajo de investigación exponen como objetivo el desarrollar habilidades para conducir proyectos de diagnóstico e implementación de sistemas de seguridad de la información basándose en el estándar ISO/IEC 27001 (ISO 27001, 2013) y en el sistema de control propuesto en la norma ISO/IEC 27002 (ISO 27002, 2013). En este trabajo, los autores indican los resultados de una experiencia aplicando las fases de la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que permitieron establecer el diagnóstico de seguridad en una organización; aplicando luego una lista de chequeo basada en los estándares, para verificar la existencia de controles de seguridad en los procesos

organizacionales. Finalmente y de acuerdo a los resultados del análisis y evaluación de los riesgos, los autores proponen los controles de seguridad adecuados para que sean integrados posteriormente dentro de un SGSI (Sistema de Gestión de Seguridad de la Información) que responda a las necesidades de seguridad informática de la organización objeto de estudio.

Frente a los desafíos emergentes de la era de Internet, los administradores y los profesionales de la seguridad de la información en las empresas privadas y públicas deben gestionar riesgos específicos para sus organizaciones para asegurar de esta manera operaciones eficientes (Yazar, 2002). El artículo de investigación que presenta este autor explica los componentes básicos de los procesos de análisis y gestión de riesgos y menciona diferentes metodologías y enfoques. Posteriormente, describe y discute la metodología CRAMM (*CCTA Risk Analysis and Management Method*), como una herramienta automatizada basada en una metodología cualitativa de evaluación de riesgos, y se presenta una revisión de las etapas de esta metodología como son: la identificación y valoración de activos, la evaluación de amenazas y vulnerabilidades y las recomendaciones de contramedidas. El autor concluye que junto con una adecuada concientización organizacional, CRAMM es una herramienta integral y flexible especialmente para justificar las contramedidas que se priorizan en la gestión de riesgos, necesitando sin embargo, profesionales calificados, capacitados y experimentados para obtener resultados eficientes con la metodología (Yazar, 2002).

Investigadores de la Universidad de Adelaide (University of Adelaide, 2015) han desarrollado un manual de gestión de riesgos adaptado a las necesidades de la Universidad, denominado "*The Risk Management Handbook*", adoptando los principios de gestión de riesgos establecidos en la norma internacional de gestión de riesgos ISO 31000 (ISO 31000, 2009) para la institución educativa mencionada. La política de riesgos afirma formalmente el compromiso estratégico de la Universidad de construir una cultura de gestión de riesgos en la cual los riesgos y las oportunidades son identificados y manejados efectivamente. Esta guía de Gestión de Riesgos proporciona detalles sobre los principios y procesos identificados e incluye recursos y herramientas que han sido diseñados para ayudar con el proceso de gestión de riesgos y fomentar un lenguaje coherente y comprensivo con un enfoque para la gestión del riesgo en toda la Universidad.

Existen además localmente algunos trabajos de titulación relacionados con las metodologías de identificación y gestión de riesgos como la propuesta de Molina (2015), donde el autor aplica la metodología MAGERIT (Ministerio de Hacienda y Administraciones Públicas de España, 2012) para gestionar los riesgos en una institución de educación superior. En su trabajo, el autor indica la necesidad de desarrollar con esta metodología un análisis de riesgo tecnológico de orden cualitativo aplicado al centro de administración de servicios de red y sistemas de la Escuela Superior Politécnica del Litoral, partiendo de una descripción de la situación actual de la organización, para luego identificar los activos con sus respectivas amenazas, y posteriormente realizar la medición de riesgos existentes y sugerir las

salvaguardas necesarias que forman parte del plan de implementación, utilizando para la evaluación de riesgos la herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos), la cual soporta el análisis y gestión de los riesgos de sistemas informáticos siguiendo la metodología MAGERIT, obteniendo resultados que muestran los niveles de riesgo e impacto potencial en la institución. El aporte del estudio de Molina (2015) es identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad implementada, y sobre todo incentivar al personal de la institución a seguir las respectivas normas y procedimientos referentes a la seguridad de la información. Las etapas o pasos de esta metodología basada en Magerit se las ilustra en la Figura 3.1.

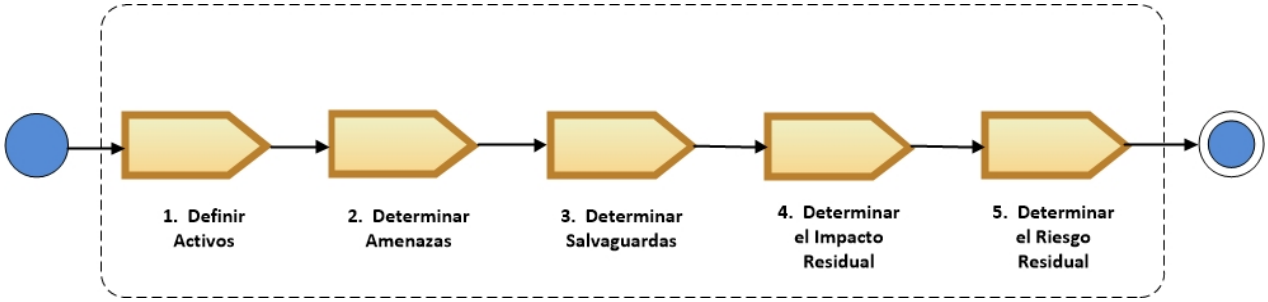

Figura 3.1. *Procesos de la Metodología basada en Magerit (Molina, 2015).*

Crespo (2016), propone por su parte una metodología de gestión de riesgos llamada *Ecu@Risk* en su trabajo de titulación, donde fundamenta su metodología en el análisis y herramientas sugeridas de otras metodologías importantes y aceptadas internacionalmente como Magerit (Ministerio de Hacienda y Administraciones Públicas de España, 2012), OCTAVE-S (Alberts *et al.*, 2005), CRAMM (Yazar, 2002) y Microsoft Risk Management (Microsoft, 2006), las mismas que van alineadas con los marcos de referencia internacionales como las normas ISO/IEC 27001 (ISO 27001, 2013), ISO/IEC 27002 (ISO 27002, 2013), ISO/IEC 27005 (ISO 27005, 2011) e ISO/IEC 31000 (ISO 31000, 2009). Además el autor sustenta su trabajo mediante la revisión de algunas leyes ecuatorianas que amparan la protección de datos contra divulgación, vigilancia o delito.

La metodología Ecu@Risk (Crespo, 2016) fue realizada para la gestión del riesgo informático aplicable a las Micro, Pequeñas y Medianas empresas (MPYME) en el Ecuador, que por diversos motivos no se pueden certificar con alguna otra metodología o estándar internacional para la gestión de riesgos.

Esta metodología se compone de tres secciones principales: *a) la introducción al manejo del riesgo, b) el marco de gestión del riesgo, c) el proceso de gestión del riesgo* indicando además los recursos o herramientas que se proponen utilizar en la metodología en cada uno de los procesos de la sección de gestión del riesgo.

Las secciones mencionadas se resumen en la Figura 3.2 mediante notación SPEM (*Software Process Engineering Metamodel*), la misma que es propuesta y soportada por el Object Managment Group (2008).

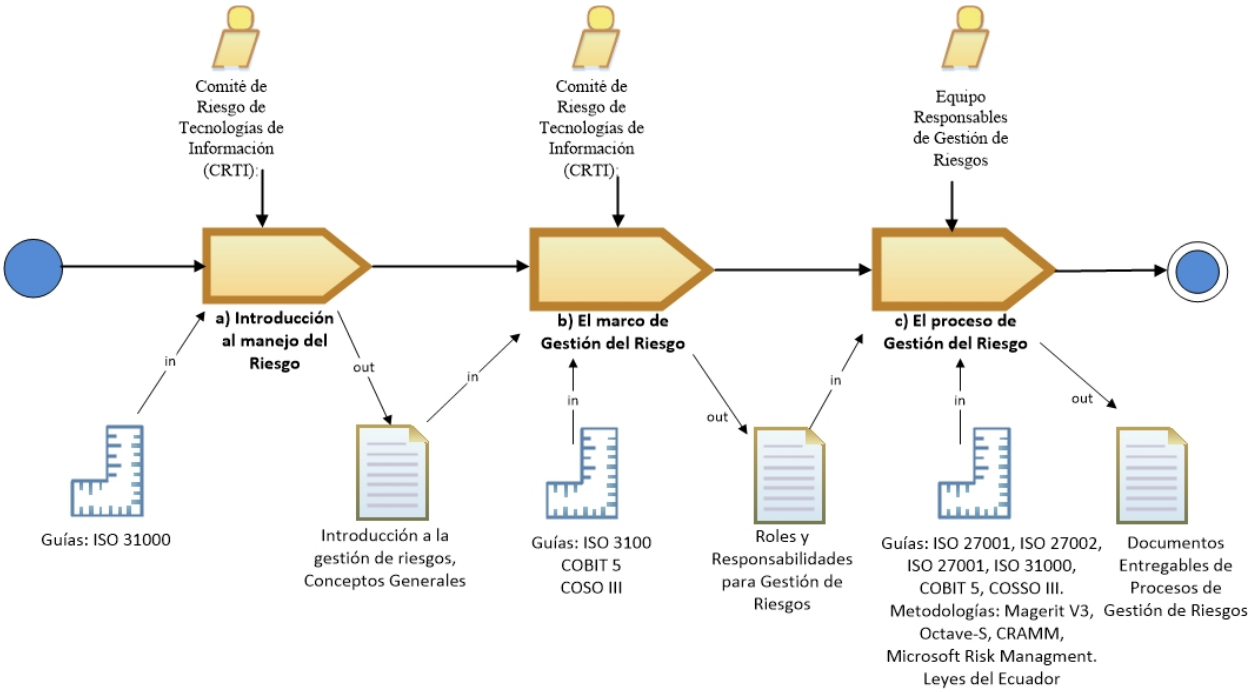

Figura 3.2. *Secciones Generales de la Metodología Ecu@Risk (Crespo, 2016).*

Mejía *et al.* (2016) en su trabajo de investigación proponen identificar las debilidades y fortalezas a las que están sometidos los activos de la dirección de TIC (Tecnologías de la Información y Comunicaciones) de la Universidad Técnica de Babahoyo, ubicada en la Provincia de Los Ríos en el Ecuador, con la finalidad de establecer los objetivos, dominios y controles para minimizar la ocurrencia de las amenazas que puedan explotar vulnerabilidades en la infraestructura tecnológica de esta institución. Este estudio permitió a sus autores recoger información a través de instrumentos de recolección de datos, como entrevistas, reuniones de trabajo y revisión bibliográfica, además de visitas técnicas a las instalaciones de la Universidad, revisando aspectos de seguridad física previstos en las Normas ISO 27001 (ISO 27001, 2013). Los autores proponen en la metodología de su estudio partir de un levantamiento de los activos de información: dispositivos de hardware, software, información electrónica, física y demás activos, para luego realizar una valoración adecuada de los mismos de acuerdo a su incidencia en la integridad, confidencialidad y disponibilidad; realizando también una asignación de las amenazas más significativas que pueden causar daño a los activos identificados y afectar su actividad para finalmente realizar una valoración del riesgo, siendo necesario para todo este proceso la aplicación de controles de las Normas ISO 27002 (ISO 27002, 2013).

En el año 2009, se introduce la norma ISO 31000 (ISO 31000, 2009), la cual pretende ayudar a las organizaciones a gestionar de manera sistemática y comprensiva diversos tipos de riesgo, ofreciendo un marco universal que ayude a la organización a integrar la gestión de riesgos en su sistema de gestión global (ISO, 2009)(Lalonde & Boiral, 2012). El trabajo de investigación de Lalonde & Boiral (2012) da a conocer las contribuciones realizadas para este estándar, enfatizando con crítica las dificultades que pueden surgir de los conceptos erróneos sobre la norma ISO 31000 (ISO 31000, 2009) y su uso como una herramienta para controlar los riesgos. La conclusión sugiere que la gestión del riesgo debe considerarse como un enfoque basado en la práctica, una estrategia que los gerentes o directivos deben ejecutar y no una estrategia que solamente la deben tener; así también, los gerentes deben cuestionar sus propios supuestos en la implementación de tal norma, teniendo en cuenta las especificidades de su entorno organizativo interno y externo permaneciendo constantes en su monitoreo (Lalonde & Boiral, 2012).

Ramírez & Ortiz (2011) presentan una metodología para gestionar riesgos tecnológicos basándose en los estándares ISO (International Organization for Standardization) 31000 (ISO 31000, 2009) e ISO/IEC (International Electrotechnical Commission) 27005 (ISO 27005, 2011), considerando que dichos estándares indican lo que se requiere para la gestión de riesgos más no indican exactamente como se puede realizar esta gestión; además, incluyen en su trabajo recomendaciones y buenas prácticas de otros estándares y guías internacionales para el manejo de riesgos, presentando una forma de aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde una perspectiva tecnológica integrando finalmente la metodología propuesta a la gestión de continuidad de negocios de una organización. El proceso general de la metodología de gestión de riesgos propuesta por Ramírez & Ortiz (2011), se resumen en la Figura 3.3.

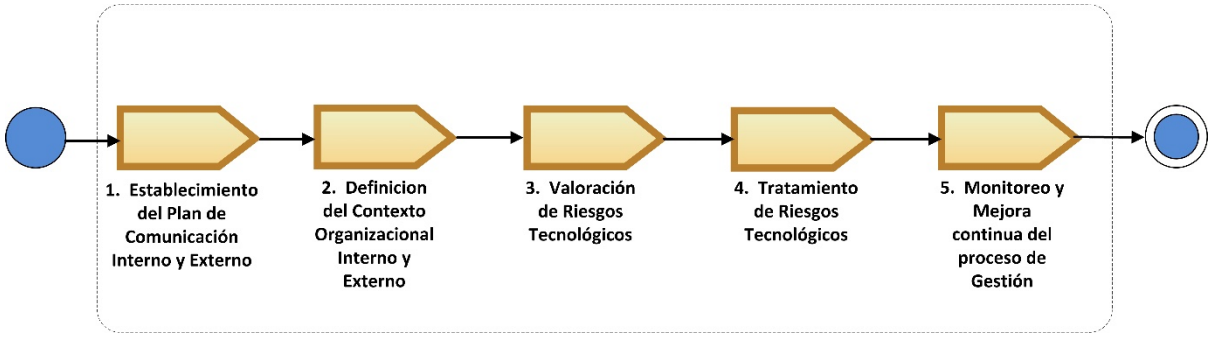

Figura 3.3. *Procesos de la Metodología basada en ISO/IEC 31000 e ISO/IEC 27005 (Ramírez & Ortiz, 2011).*

El estándar IS0 31000 (ISO 31000, 2009) aceptado mundialmente para la gestión de riesgos se desarrolló a través de un proceso basado en consenso con la participación de varios profesionales de la gestión de riesgos en todo el mundo, el mismo surgió con el objetivo de resolver las muchas

inconsistencias y ambigüedades que existen entre algunos enfoques y definiciones diferentes (Purdy, 2010). La norma ISO 31000 (ISO 31000, 2009) pretende ayudar a las organizaciones a gestionar de manera sistemática y completa diversos tipos de riesgo, ofreciendo un marco universal para ayudar a las organizaciones a integrar la gestión del riesgo en su sistema de gestión global (Lalonde & Boiral, 2012).

Por lo expuesto, el desarrollo y uso de metodologías integradas para gestionar riesgos, en especial el tecnológico, es importante con el fin de asegurar en una empresa el cumplimiento de las dimensiones y pilares fundamentales de la seguridad de la información: la confidencialidad, integridad y disponibilidad (ISO 27000, 2016).

Una vez realizando el análisis y revisión de los trabajos mencionados, se concluye que los mismos no mencionan que sus respectivas metodologías o estándares han sido probadas para realizar una identificación y análisis de riesgos específica para empresas industriales de alimentos, que tienen particularidades propias de su operación sobre todo en sus procesos de fabricación, sin embargo se hace necesario en este trabajo la selección de una metodología adecuada para identificación y análisis de riesgos en este tipo de empresas para que, posteriormente con el planteamiento de la elaboración de políticas de seguridad, se puedan mitigar dichos riesgos.

Hasta el momento, según los estudios realizados, el marco existente más común y utilizado para la gestión de riesgos lo conforman los estándares ISO 31000: Gestión de Riesgos (ISO 31000, 2009) e ISO/IEC 27005: Gestión de Riesgos de Seguridad de la Información (ISO 27005, 2011), sin embargo estos estándares proveen lineamientos generales sobre la gestión de riesgos pero hace falta una guía más precisa que ofrezca pautas sobre la forma de lograr los aspectos de seguridad requeridos; adicionalmente este marco hace referencia a la gestión sobre los riesgos como concepto global y deja de lado el análisis de riesgos específicos como el tecnológico, lo más cercano es la administración del riesgo operativo en el que se relaciona de forma tangencial el riesgo tecnológico (Ramírez & Ortiz, 2011). Además no se conocen estudios que han implementado o probado estos estándares aplicándolos en empresas industriales en el contexto de nuestro país considerando las normativas legales y la naturaleza de estas empresas en nuestro medio.

Por ello, la metodología de gestión de riesgos Ecu@Risk, propuesta por Crespo (2016), ha sido seleccionada como la metodología base en este trabajo para la identificación y análisis de riesgos en empresas industriales de alimentos, ya que se fundamenta en el análisis de las partes más importantes e instrumentos de otras metodologías aceptadas internacionalmente como Magerit (Ministerio de Hacienda y Administraciones Públicas de España, 2012), Octave-S (Alberts *et al*., 2005), CRAMM (Yazar, 2002) y Microsoft Risk Management (Microsoft, 2006), estando alineadas con los estándares internacionales ISO/IEC 27001 (ISO 27001, 2013), ISO/IEC 27002 (ISO 27002, 2013), ISO/IEC 27005 (ISO 27005, 2011) e ISO/IEC 31000 (ISO 31000, 2009) y además se sustenta con el análisis de algunas

leyes ecuatorianas que amparan la protección de datos contra divulgación, vigilancia o delito, siendo una metodología propuesta y diseñada para empresas de tipo MPYMES del Ecuador. Por todo esto se considera que la metodología Ecu@Risk (Crespo, 2016) puede ser aplicable en las empresas de tipo industrial del Ecuador, contribuyendo a la investigación realizada en el presente trabajo con una variación y mejora de los procesos y materiales para la identificación de riesgos que tiene esta metodología. La metodología propuesta se valida aplicando la misma como un caso de estudio en una empresa industrial de alimentos de la ciudad de Cuenca - Ecuador y midiendo su efectividad mediante la comparación de los riesgos obtenidos usando la metodología propuesta con los riesgos teóricos más importantes que se sabe que tiene la organización indicados por parte del jefe del área de TI mediante una entrevista guiada.

3.3. Políticas de Seguridad de la Información

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten una nueva forma de hacer negocios, donde el uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y confidencialidad de la información y, como uno de estos proyectos, la creación de políticas de seguridad es una labor fundamental que involucra a las personas, procesos y recursos de una compañía (Dussan, 2006). Este autor presenta en su trabajo de investigación un análisis y revisión de conceptos teóricos y aporta con puntos claves a tener en cuenta para diseñar una política de seguridad de la información basándose en la norma ISO 17799, actualmente ISO/IEC 27002 (ISO 27002, 2013).

Una importante corriente de investigación en el campo de la seguridad de los sistemas de información examina el uso de políticas de seguridad organizacionales que especifican cómo deben comportarse los usuarios de los recursos de información y tecnología para prevenir, detectar y responder a incidentes de seguridad; sin embargo, este creciente (y en ocasiones conflictivo) tema de investigación ha hecho que sea difícil para los investigadores y profesionales comprender el estado actual del conocimiento sobre la formación, implementación y efectividad de las políticas de seguridad de la información en las organizaciones (Cram *et al.*, 2017). Estos autores en su trabajo de investigación realizan una síntesis de la literatura académica que consideran relevante en el tema de las políticas de seguridad de la información, pretendiendo una comprensión holística de las mismas, realizando la revisión de 114 artículos influyentes de revistas relacionadas con políticas de seguridad e identifican las relaciones fundamentales examinadas en la literatura.

Barbosa Martins & Saibel (2005) indican en su trabajo de investigación que a pesar de que existen varios trabajos relacionados al tema de seguridad de la información, poco enfoque se ha dado a la definición de una metodología para asegurar la misma, con un conjunto de directrices consistentes y coherentes que ayuden a la planificación e implementación de un Sistema de Gestión de Seguridad de

la Información (SGSI) en un ambiente de red con sistemas computacionales heterogéneos, por lo que, para suplir esta deficiencia presentan en su trabajo de investigación una metodología teórico-conceptual para ayudar a la elaboración e implementación de un SGSI en una organización, la cual se basa en estándares y normas internacionales (TECSEC, 1985), (ISO 15408, 1999), (ISO/IEC TR 13335, 1998), (BS7799-2, 2001), (ISO/IEC 17799, 2001), (IEC 61508, 1998) y en la primera etapa de la metodología propuesta, describen el método utilizado para la construcción de políticas de seguridad en una organización basado en el estándar ISO/IEC17799, actualmente conocida como la norma ISO/IEC 27002 (ISO 27002, 2013).

La gestión de la seguridad de la información es un factor cada vez más determinante en la competitividad de las organizaciones; además, la gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IEC 27002 (ISO 27002, 2013); sin embargo, el proceso de implementación de esta norma y su gestión constante se facilita a través del uso de software, que en la actualidad es comercial en su gran mayoría, con restricción del idioma, poca documentación y limitada disponibilidad de software libre que se ajuste a requerimientos particulares de organizaciones en el contexto latinoamericano, limitando la aplicación de la norma y la efectividad de su uso (Franco & Guerrero, 2013). Estos autores indican en su trabajo de investigación que la mayoría de las herramientas de software disponibles para seguridad informática están basadas en el estándar ISO 27001 (ISO 27001, 2013) y algunas tienen incorporados otros estándares como COBIT (ISACA, 2012), ITIL (Axelos, 2017), pero son muy pocas las que están directamente relacionadas con ISO 27002 (ISO 27002, 2013) por lo que presentan en su trabajo de investigación una aplicación desarrollada como una plataforma web abierta denominada SGCSI que sirve de ayuda y apoyo para la gestión de controles de seguridad de la información de acuerdo con el estándar ISO 27002 (ISO 27002, 2013), y mediante una evaluación comparativa del uso de la plataforma por parte de expertos en seguridad, lograron evidenciar su efectividad en la auditoria sobre el cumplimiento de los 32 objetivos de control establecidos por esta norma.

Existen otros trabajos relacionados con la norma ISO/IEC 27002 (ISO 27002, 2013); como el de Iqbal *et al.* (2009) en el que se presentan los aspectos a tener en cuenta para el desarrollo de una base de datos que permita el uso eficaz de esta norma. Se analiza el uso de esta norma estándar y también se investiga un método sistemático para la construcción de bases de datos de normas ISO para la seguridad de la información.

Por su parte, Klaic & Hadjina (2011) muestran una visión del estado actual y tendencias en el campo de los métodos y herramientas para el apoyo a los procesos de planificación, implementación, ejecución y cumplimiento de las políticas de seguridad de la información; esto lo consiguen en base a una revisión comparativa de la literatura disponible, planteando algunas hipótesis que se comprueban a través de los análisis más detallados de los trabajos científicos seleccionados.

El trabajo de Horváth & Jakub (2009) está relacionado con la experiencia de un caso de aplicación de controles de seguridad basados en ISO/IEC 27002 (ISO 27002, 2013) para organizaciones pequeñas, en el cual se seleccionan específicamente 88 controles que contiene la norma, ya que se establece que no necesariamente se deben aplicar todos los controles del estándar a una empresa porque ello depende de la naturaleza, tamaño y objetivos de la organización.

El alto número de controles a implementar en un sistema de información dinámico, implica un esfuerzo grande para el personal encargado de la seguridad de la información (Miranda *et al, 2013*); por lo que estos autores presentan en su trabajo una metodología basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, combinando varios métodos orientados a la gestión de riesgos con un enfoque en las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información (SGSI); considerando además que los autores indican que aproximadamente el 30% de los controles contenidos en el estándar internacional ISO/IEC 27002 (ISO 27002, 2013) son automatizables, el objetivo de su investigación es demostrar que la gestión de la seguridad informática puede ser un proceso menos complejo y más efectivo, hipótesis que se valida a través de un análisis estadístico que demuestra la disminución de la complejidad y el aumento de la eficiencia en cuanto al tiempo y el esfuerzo requerido tras la implementación de controles automatizados de seguridad informática.

La creciente importancia que tienen los Sistemas de Información en las organizaciones naturalmente provoca la necesidad de confiar en su uso, para ello Lopes & Oliveira (2016) indican que hay una serie de tecnologías que ayudan a garantizar la seguridad y la confianza en el uso de los Sistemas de Información, sin embargo, la tecnología por sí sola no resuelve todos los problemas, por lo que existe la necesidad de establecer Políticas de Seguridad de la Información bien definidas para garantizar la integridad de los datos, así como su confidencialidad y disponibilidad; sin embargo, al existir poca información sobre los contenidos que dichas políticas deben tener, los autores pretenden contribuir a llenar este vacío presentando en su trabajo de investigación una síntesis de la literatura sobre las políticas de seguridad de la información y un análisis en 15 PYMEs (Pequeñas y Medianas Empresas) de los documentos de políticas de seguridad de la información que disponen en lo que respecta a sus características y componentes para finalmente discutir y proponer como deberían estar estructuradas dichas políticas de seguridad.

Un número significativo de investigadores han argumentado que el incumplimiento de las políticas de seguridad de la información es uno de los principales desafíos que enfrentan las organizaciones y se considera principalmente un problema humano más que un problema técnico; por lo tanto, los empleados son una de las principales causas subyacentes de las violaciones en la seguridad de la información (Alotaibi *et al.*, 2016). Estos autores en su trabajo de investigación revisan la

literatura académica y los informes de los institutos de seguridad de la información relacionados con el cumplimiento de las políticas de seguridad, teniendo por objetivos proporcionar una visión general de los retos claves que rodean la implementación exitosa de las políticas de seguridad de la información e investigar los factores que pueden influir en el comportamiento de los empleados en relación con la implementación y cumplimiento de políticas de seguridad de la información.

En el contexto regional, son escasos los estudios y antecedentes sobre políticas o controles de seguridad informática, sin embargo se encuentran estudios como el que realiza Cano (2009) donde mediante una encuesta a 513 profesionales en TICs que laboran en empresas de distintos tipos en varios países de Latinoamérica y apoyado con otros estudios de empresas como McAfee y otros institutos, concluye que el 66% de las empresas encuestadas en Latinoamérica no cuentan con una política de seguridad definida formalmente o se encuentra en desarrollo, por lo tanto es necesario fortalecer este aspectos junto con regulaciones nacionales e internacionales que lleven a las organizaciones latinoamericanas a fortalecer sus sistemas de gestión de seguridad de la información.

Ramos *et al.* (2017) proponen en su trabajo la adopción e implementación de políticas de seguridad de la información en una institución financiera teniendo en cuenta la norma ISO/IEC 27002 (ISO 27002, 2013), las cuales servirán como guía para proporcionar herramientas que contribuyan a mejorar la gestión de la información obtenida, aplicando dichas políticas en una empresa del sector financiero de Colombia; las políticas de seguridad planteadas facilitan la adopción de lineamientos necesarios para garantizar la seguridad de la información y consideran algunos procesos y procedimientos tales como: registros de incidencias, respaldo de la información, respaldos de la información, mantenimiento de equipos y copias de seguridad.

El estudio de Knapp *et al.* (2009) presenta una metodología para la gestión integral para el desarrollo y gestión de las políticas de seguridad de la información involucrando técnicas cualitativas y definiendo un proceso claro para la gestión de políticas de seguridad de la información basado en las respuestas de una muestra de profesionales certificados en seguridad, siendo la base de la metodología propuesta en el presente trabajo. Esta metodología presenta una definición estricta y especifica de políticas centradas en la seguridad de procesos corporativos para diferentes tipos de organización y su interrelación con el recurso humano.

Existen además localmente trabajos de titulación como el de Posso (2009), que en su proyecto de titulación presenta un análisis de la norma ISO/IEC 27002 (ISO 27002, 2013), y en base a la misma identifica las políticas de seguridad existentes y faltantes en el área de networking de una empresa de venta y asesoramiento de tecnología de la ciudad de Quito - Ecuador; proponiendo así una metodología para obtener políticas de seguridad en empresas de este tipo.

En el trabajo de titulación de Barragán et al. (2011) presentan la implementación de políticas de

seguridad informática en una empresa pública como lo es la Municipalidad de Guayaquil, analizando algunos conceptos de seguridad de la información y de políticas de seguridad informática, proponen además el uso de la metodología MAGERIT (Ministerio de Hacienda y Administraciones Públicas de España, 2012) para el análisis de riesgos y activos que dispone la organización, para finalmente aplicar la implementación de las políticas de seguridad y las estrategias de difusión que pueden utilizarse

Revisando la literatura disponible, se concluye que existen actualmente varios proyectos de seguridad informática para garantizar la integridad, disponibilidad y confidencialidad de la información y, como uno de estos proyectos, están los estudios para la elaboración de políticas de seguridad de la información realizados para empresas comerciales, gubernamentales, financieras, entre otras; sin embargo, considerando que cada una de las organizaciones tienen problemas y procesos propios de su operación, se hace necesaria la investigación del desarrollo de políticas de seguridad de la información para empresas industriales de alimentos en particular, las que, por su naturaleza necesitan su propio modelo para la identificación de riesgos, elaboración y plan de implementación de políticas de seguridad de la información.

Se tienen estudios sobre el comportamiento del recurso humano, que es considerado como una de las principales amenazas de seguridad para las organizaciones, sin embargo se indica que se puede mitigar dicha amenaza mediante instrucción o capacitaciones que hagan tomar consciencia al personal del problema de seguridad de la información al que se enfrentan actualmente las empresas, así como de las políticas y controles que se deben implementar en las empresas para asegurar su información y la continuidad de sus procesos.

Existen estándares que tratan sobre las políticas y controles de seguridad como la norma ISO/IEC 27002 (ISO 27002, 2013), que es una guía de buenas prácticas y controles para proporcionar herramientas que contribuyan a mejorar y asegurar la seguridad de la información en una organización, sin embargo se ha dado poco enfoque a la definición de una metodología práctica y sencilla para las organizaciones industriales que les brinde ayuda para la elaboración, implementación y difusión de las políticas de seguridad. Así también se encuentran estudios que tratan sobre software y bases de datos que ayudan en la implementación y gestión de políticas de seguridad, pero no se basan específicamente en el estándar ISO/IEC 27002, (2013). Este estándar se ha seleccionado como la normativa base para la elaboración y difusión de políticas de seguridad en empresas industriales de alimentos, junto con el aporte de otras recomendaciones realizadas por trabajos científicos y expertos en seguridad informática, que consideran técnicas cualitativas para la elaboración de políticas de seguridad de la información basadas en la normativa ISO/IEC 27002 (ISO 27002, 2013), como el modelo planteado por Knapp *et al.* (2009).

Capítulo 4. Metodología Propuesta

La metodología que se plantea en el presente trabajo de titulación y se detalla en este capítulo, presenta de una manera clara y efectiva, cómo se pueden desarrollar y difundir las políticas de seguridad de la información en una empresa industrial de alimentos. Esta metodología se alinea con 3 de las 9 etapas planteadas en el modelo de gestión de políticas de seguridad que propone Knapp *et al.* (2009) detallado en el capítulo 2 (ver Figura 2.12), dado que son las etapas que cubren el desarrollo y difusión de políticas de seguridad, enmarcándose dentro del alcance del presente trabajo. Estas etapas son: la evaluación de riesgos, el desarrollo de la política y la concientización y entrenamiento en la política al personal. En la metodología planteada a estas etapas se las define como:

- Etapa 1: Identificación y análisis de riesgos,
- Etapa 2: Desarrollo de las políticas de seguridad de la información,
- Etapa 3: Difusión de las políticas de seguridad de la información

Ya que en la bibliografía consultada no se detalla la manera en la que se deben desarrollar estas etapas, en este capítulo como aporte a la investigación se propone en cada una de las etapas detallar sus pasos, sirviendo como una guía al equipo de trabajo, conocido como Equipo de Gestión de Seguridad de la Información, para que pueda llevar a cabo el análisis de riesgos, el desarrollo de la política de seguridad de la información y su posterior difusión sin inconvenientes. Se presenta entonces de manera general la metodología planteada gráficamente en la Figura 4.1 mostrando las etapas planteadas y sus respectivos pasos en cada una de ellas.

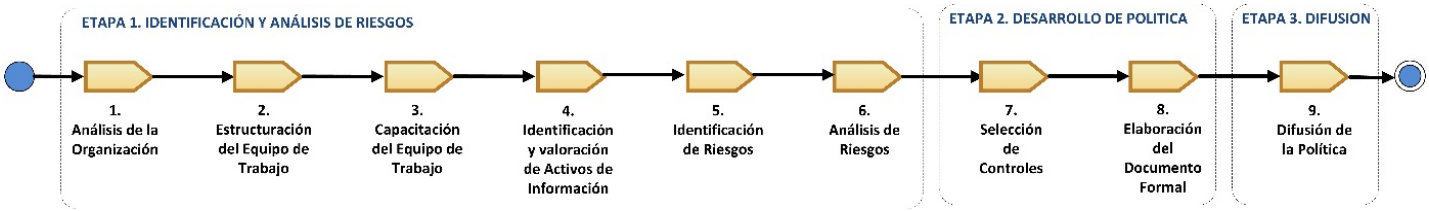

Figura 4.1 *Metodología propuesta para el Desarrollo y Difusión de Políticas de Seguridad de la Información.*

En la Figura 4.1 se pueden observar las 3 etapas con 9 pasos secuenciales que plantea la metodología para el desarrollo de una política de seguridad de la información. La etapa 1 incluye un proceso secuencial que consiste en 6 pasos en la etapa de Identificación y Análisis de Riesgos, 2 pasos en la etapa de Desarrollo de la Política y 1 paso en la etapa de Difusión de la Política; que cubren el alcance de este trabajo. Se parte de una evaluación y análisis de los riesgos informáticos obtenidos en la organización o en un área de la misma y en base a ellos se desarrollará la política de seguridad, seleccionando los controles más adecuados del estándar ISO 27002:2013 para mitigar los riesgos

encontrados y planteándolos como una política de seguridad de la información en un documento formal a la dirección de la empresa para su posterior aprobación; procediendo finalmente a su difusión y concientización a todo el personal de la empresa o área involucrada. Las etapas de la metodología propuesta se detallan a continuación.

4.1. Etapa 1: Identificación y Análisis de Riesgos

La etapa inicial de la metodología propuesta para la elaboración de una política de seguridad en el presente trabajo de titulación es la identificación y análisis de riesgos, por lo cual se presenta a continuación el detalle de esta etapa.

La metodología presentada se basa en la propuesta de Crespo (2016) y se incluyen los procesos, recursos y herramientas adaptados para una empresa industrial de alimentos, con la finalidad de identificar y analizar los riesgos en una determinada área. Esta actividad se compone de 6 tareas consecutivas, sin la necesidad de separarlas en secciones, como se lo plantea en la metodología Ecu@Risk (Crespo, 2016). Estas etapas son: análisis de la organización, estructuración del equipo de trabajo, capacitación del equipo de trabajo, identificación y valoración de activos de información, identificación de riesgos y el análisis de riesgos, tal como se muestran en la Figura 4.2 con notación SPEM identificando los responsables, instrumentos, entradas y salidas que intervienen en cada paso de la etapa.

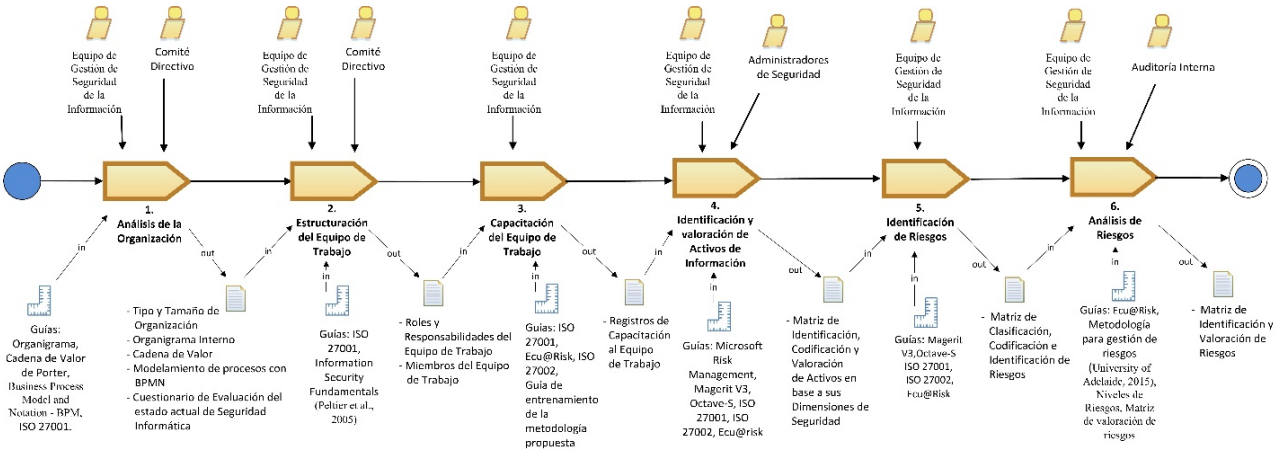

Figura 4.2 *Metodología propuesta para la Identificación y Análisis de Riesgos.*

4.1.1. Paso 1: Análisis de la Organización

Se verifica el entorno que tiene la empresa con la que se va a trabajar. En este paso se debe: (i) identificar el tipo de organización, (ii) su tamaño, (iii) su entorno y procesos; ésto para que el investigador comprenda mejor el contexto de la empresa con la que va a trabajar y por ende los posibles

riesgos o amenazas que pudiese encontrar.

Se utilizan herramientas como el organigrama interno de la empresa (Ferrel *et al.*, 2004) y la cadena de valor de Porter (Olmedo *et al.*, 2016) con el objetivo de identificar la estructura de la empresa y las actividades u operaciones que realiza la misma.

Por otor lado, se considera la importancia de partir con un cronograma de su estructura interna para el conocimiento de la empresa, ya que según Ferrel *et al.* (2004), un organigrama es una "representación visual de la estructura organizacional, líneas de autoridad (cadena de mando), relaciones de personal, comités permanentes y líneas de comunicación"; es decir, el organigrama es una representación gráfica o visual de la estructura orgánica de una institución o de una de sus áreas, en la que se muestran principalmente las relaciones que tienen entre sí los órganos internos que la componen (Franklin, 2004).

Olmedo *et al.* (2016) indican que la herramienta llamada "*Cadena de Valor*" es una forma sistemática de examinar todas las actividades que una empresa desempeña y cómo interactúan entre ellas, además de que, con esta herramienta, se disgrega a la empresa en sus actividades estratégicas relevantes para comprender su comportamiento.

La cadena de valor propuesta por Michael Porter, profesor de la escuela de negocios de Harvard, establece un marco para analizar las empresas en sus sectores industriales, la competencia y la forma de establecer una estrategia que les permita obtener una posición ventajosa respecto de sus competidores (Olmedo et al., 2016).

Además, para tener claros los procesos que se ejecutan en la empresa y su entorno se modelan los procesos de la organización mediante la notación conocida como *Business Process Model and Notation* (BPMN) (http://www.bpmn.org/), ya que la finalidad de dicha notación es comprender los procesos de negocios de una manera legible y entendible para todos los usuarios (Vasquez et al., 2010).

Finalmente, se utiliza una herramienta alineada con la norma ISO 27001 (ISO 27001, 2013), que en la metodología Ecu@Risk se la denomina "cuestionario de aplicabilidad de la metodología" (Crespo, 2016); sin embargo, en la metodología propuesta se lo utiliza como una herramienta de "evaluación del estado actual de la seguridad informática", y sirve para que de manera inicial, el equipo de trabajo tenga una idea en qué estado se encuentra el entorno de seguridad informática de la empresa en la que se va a trabajar.

Este paso es equivalente a la etapa de "determinación del contexto" en la metodología Ecu@Risk, pero con herramientas sencillas de comprender y utilizar por el equipo de trabajo en una empresa industrial de alimentos; que además entregan resultados rápidos a cerca del conocimiento de la organización y las actividades que realiza, siendo el objetivo principal en este paso de la etapa.

4.1.2. Paso 2: Estructuración del Equipo de Trabajo

Este paso es el equivalente a la etapa del marco de gestión del riesgo en la metodología Ecu@Risk, y pretende estructurar el equipo de trabajo para la identificación y análisis del riesgo; sin embargo, Ecu@Risk presenta una estructura de roles compleja para la realidad del tipo de empresas MPYME en nuestro medio, entre ellas las empresas industriales de alimentos, y además no se aclara en el proceso de gestión del riesgo de Ecu@Risk que roles intervienen exactamente en cada una de sus etapas; por lo que se propone en este paso de la metodología establecer los roles que se consideran estrictamente necesarios tanto para las etapas de identificación y análisis de riesgos, como para el posterior desarrollo y difusión de la política de seguridad.

Peltier et al. (2005) sostienen que ningún profesional de la seguridad de la información debe intentar imponer una estructura a una organización donde claramente no encaja, pero las responsabilidades amplias que ellos describen indican que deben ser llevadas a cabo si el programa de seguridad de la información tiene un sólido apoyo desde los directivos en la organización. Estos autores sugieren algunos roles del personal de seguridad de la información con sus responsabilidades, sin embargo esta distribución tiene también roles con responsabilidades parecidas o duplicadas y con el objetivo de simplificar los roles del equipo de trabajo en una empresa industrial de alimentos, se han resumido en los siguientes: Equipo de gestión de seguridad de la información, Auditoría interna, Comité Directivo y Administradores de seguridad, tal como se muestran en la Tabla 4.1 con sus respectivas responsabilidades y equivalencias respecto a los roles en las propuestas que realizan Peltier et al. (2005) y Crespo (2016).

Dentro del *Equipo de Gestión de Seguridad de la Información*, cuando se trabaja con el personal interno de la propia institución, debe considerarse al personal de TI y otras de áreas de la empresa si se desea. En caso de existir un Jefe de la Seguridad de la información o C*hief Information Security Officer* (CISO), es el quien debe liderar este equipo por sus conocimientos y experiencia, sin embargo, este rol respecto al personal de seguridad de la información en las empresas de nuestro medio todavía no se refleja en muchas de ellas, por lo que el jefe del área de TI y quienes él considere idóneos para integrar este equipo serían suficientes, pudiendo pertenecer o no al área de TI, pero deben cumplir con los conocimientos respectivos en el área de seguridad de la información, gestión de riesgos, políticas de seguridad y de ser posible tener certificaciones en algún estándar de seguridad como por ejemplo ISO 27000 o ISO 17001, como aporte y experiencia para el equipo de trabajo.

ROL	RESPONSABILIDADES	COMPARACIÓN (Peltier et al., 2005)	COMPARACIÓN Ecu@Risk(Crespo, 2016)
Equipo de Gestión de Seguridad de la Información	- Proporcionar orientación, capacitación y soluciones a toda la organización sobre el tema de seguridad informática. - Obtener apoyo y comunicación constante con el comité directivo y administradores de seguridad. - Planificar nuevas implementaciones, proyectos y herramientas de seguridad. - Identificar Activos. - Identificar y Analizar los riesgos. - Seleccionar, plantear y difundir las políticas de seguridad adecuadas que ayuden a mitigar los riesgos identificados.	Equipo de gestión de la seguridad de la información, Equipo de trabajo de seguridad	Comité de Riesgo de tecnología de Información (CRTI), Propietarios de Sistemas de información, Comité de Certificación de TI
Auditoría Interna	- Auditar metodología y medidas de seguridad. - Monitorear el cumplimiento de controles de una política de seguridad. - Informar al Comité Directivo sobre la aplicación de las políticas de seguridad.	Auditoría Interna	Auditor de TI
Comité Directivo	- Colaborar con información en la etapa de Análisis de la organización. - Aprobar nuevos proyectos de seguridad. - Aprobar la estructuración del equipo de Trabajo. - Aprobar las políticas de seguridad planteadas.	Comité Directivo	Alta Dirección
Administradores de Seguridad	En cada unidad de negocio: - Vigilar por el cumplimiento de las políticas de seguridad informática recomendadas para proteger la información. - Comunicar instrucciones dadas por el equipo de gestión de seguridad de la información.	Administradores de Seguridad, Coordinadores de Seguridad,	Propietarios de información, Coordinador de Seguridad designado, Profesionales de TI, Proveedores de soluciones tecnológicas

Tabla 4.1. *Roles del equipo de trabajo en la metodología propuesta y equivalencias con otras metodologías.*

El *Equipo de Gestión de Seguridad de la Información* es el que se encargará de aplicar toda la metodología, identificando y valorando los activos de información, también realiza la identificación, análisis y evaluación de los riesgos, para luego seleccionar, plantear y difundir las políticas de seguridad aprobadas por el comité directivo que sean más adecuadas para la empresa, según la norma ISO 27002. Además, los integrantes de este equipo serán los encargados de brindar orientación, capacitación y soluciones a toda la organización sobre el tema de seguridad de la información y también son quienes comunicarán a los otros roles a cerca de nuevos proyectos de seguridad, sobre los riesgos encontrados y controles recomendados, serán quienes deben obtener el apoyo y comunicación constante con el comité directivo y con los administradores de seguridad.

El equipo de *Auditoría Interna* debe ser integrado por personal de la empresa quienes serán los encargados de controlar y auditar que las etapas de la metodología se lleven de manera apropiada y se apliquen todos los controles de la política que el equipo de Gestión de Seguridad de la Información ha determinado en la organización. Además serán los encargados de informar al comité directivo si existiese alguna anomalía o incumplimiento en la aplicación de las políticas de seguridad. Es recomendable que los integrantes de este equipo tengan experiencia en auditoría informática, pero sobre todo tengan conocimientos de seguridad informática, gestión de riesgos y el conocimiento pleno de las políticas de seguridad que se desarrollen para la organización. Es recomendable también que participen junto con el equipo de de Gestión de Seguridad de la Información en las etapas de identificación y análisis de riesgos y en la elaboración de las políticas de seguridad de la información.

El *Comité Directivo* deberá estar integrado por los miembros de la alta dirección de la empresa o sus delegados. Tendrán comunicación directa con el Equipo de Gestión de Seguridad de la Información y serán quienes colaboren con información en la etapa de análisis de la organización, aprueben la estructuración del equipo de trabajo, es decir la conformación de todos y cada uno de los roles, y son quienes deben aprobar las políticas de seguridad planteadas y los nuevos proyectos o inversiones sugeridos por el Equipo de Gestión de Seguridad de la Información.

El grupo de *Administradores de Seguridad* se integra por los jefes, administradores o responsables de cada departamento, área o unidad de negocio de la empresa en donde se aplique la metodología y las políticas de seguridad y son los encargados de mantener y vigilar por el cumplimiento de las políticas de seguridad informática recomendadas en sus respectivas áreas para proteger la información de la empresa. Serán los encargados de comunicar y recordar a su personal las instrucciones, recomendaciones y políticas dadas por el equipo de gestión de seguridad de la información y aprobadas por el comité directivo.

4.1.3. Paso 3: Capacitación del Equipo de Trabajo

Muchas veces se tienen equipos de trabajo multidisciplinarios y heterogéneos donde no siempre están personas del área de TI que entienden perfectamente los conceptos de seguridad informática y el proceso de gestión del riesgo; considerando que esta es una amenaza que puede sesgar los resultados o aplicar equivocadamente la metodología, se debe capacitar al equipo de trabajo que se formó en el paso anterior antes de aplicar la metodología para la identificación y análisis de riesgos, y la posterior selección y propuesta de una política de seguridad informática. Este paso de la etapa se lo podría comparar con la sección de *Introducción al manejo del riesgo* de la metodología Ecu@Risk, sin embargo en dicha metodología, esta sección está separada de las etapas de la gestión de riesgos y es muy teórica para los usuarios que no son técnicos de TI o de seguridad de la información, por lo que en la metodología propuesta la herramienta utilizada en esta etapa es una guía de entrenamiento de la metodología con el objetivo de que todo el equipo de trabajo conozcan los conceptos básicos de seguridad informática y la importancia de la gestión de riesgos, además se pretende con esta guía que estén correctamente capacitados en las etapas que se deben seguir para que la metodología propuesta sea eficiente, y así finalmente obtener y analizar los riesgos a los que está expuesta la empresa o un área determinada de la misma y plantear los controles apropiados que los mitiguen mediante una política de seguridad. Esta guía debe incluir además un entrenamiento en las herramientas que sugiere la metodología como la cadena de valor, modelamiento con BPMN, matrices y tablas utilizadas, etc.

4.1.4. Paso 4: Identificación y Valoración de Activos de Información

Los activos de información en una organización, hacen referencia a cualquier elemento que contenga información (Crespo, 2016). Los activos forman uno de los 14 dominios que trata el estándar ISO/IEC 27002, que contiene 3 categorías con sus objetivos de control y 10 controles, siendo uno de los objetivos de este dominio identificar los activos y que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la gestión de riesgos. Según el estándar, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información (ISO/IEC 27002, 2013).

Este paso de la metodología, al igual que la metodología Ecu@Risk (Crespo, 2016), considera como punto de partida la definición de los grupos de activos de información con su respectiva codificación estandarizada con dos caracteres, como se muestra en la Tabla 4.2.

CODIGO	TIPO DE ACTIVO
ED	Edificaciones
HW	Hardware
SW	Software
IE	Información electrónica
IP	Información en papel
EX	Medios de almacenamiento extraíble
IC	Infraestructura de comunicaciones
RH	Recursos Humanos

Tabla 4.2. *Codificación de Grupos de Activos de Información. Fuente: (Crespo, 2016).*

Algo importante para tener en cuenta en lo que se refiere a la codificación del activo de información, según Crespo (2016), es que los activos se deben codificar con el formato: (COD. GRUPO DEL ACTIVO) (COD. SUBGRUPO1) (COD. SUBGRUPO2) (SECUENCIAL), siendo este último campo un número incremental para identificar únicamente a un activo en la organización.

A continuación y en base a la codificación de activos sugerida por Crespo (2016), se muestra en las Tablas 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9 y 4.10 la clasificación y codificación estandarizada con tres dígitos en los subgrupos de activos para esta metodología por cada grupo de activos, indicando el respectivo subgrupo 1 y subgrupo 2 que se adaptó para su utilización en una empresa industrial de alimentos y sus observaciones; pues en base a esta clasificación se identificarán los activos posteriormente en el siguiente capítulo.

GRUPO PRINCIPAL:	**(ED) Edificaciones**	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(CPD) Centro de Procesamiento de Datos Principal		Lugar principal donde se concentran los equipos servidores y de comunicaciones en la empresa. Debe tener acceso restringido.
(CPS) Centro de Procesamiento de Sucursal		Lugar de una sucursal o unidad de negocios donde se concentran equipos de comunicaciones y servidores, que a su vez se interconectan con el Centro de Procesamiento de Datos Principal. En lo posible debe tener acceso restringido.

(CPA) Centro de Procesamiento Alterno		Centro alterno o de contingencia al Centro de Procesamiento de Datos Principal para mantener la continuidad de los servicios informáticos. Por lo general el centro se encuentra ubicado en un lugar remoto distingo al del Centro de Procesamiento de Datos principal, con acceso restringido.
(ATE) Espacio Público de atención a socios de Negocios: Clientes y Proveedores		Lugar donde se recibe y se atienden a socios de negocios, tanto clientes como proveedores. Estos lugares por lo general tienen equipos de proyección, audio y acceso a internet como zonas WiFi.
(ADM) Área de Administración	(FIN) Área Financiera (CON) Área Contable (CAR) Área Cartera y Cobranza (PAG) Área de Pagos	Áreas de gestión administrativa en la empresa.
(SOP) Área de Soporte	(TIC) Área de Tecnologías de la Información y Comunicaciones (MAN) Área de Mantenimiento (RRH) Área de Recursos Humanos	Áreas de la empresa que prestan sus servicios, apoyo y soporte al resto de áreas.
(VEN) Área de Ventas	(COM) Área Comercialización (MKT) Área Marketing (DIS) Área de Diseño	Áreas que gestionan las ventas y tienen contacto directo con los clientes.
(CMP) Área de Compras y Suministros		Área que gestiona las compras de materia prima, servicios y suministros y tienen contacto directo con los proveedores.
(GER) Área de Gerencia		Áreas de gerencias, presidencias, etc. donde se encuentran los niveles directivos de la empresa y llevan a cabo sus juntas de negocio. Generalmente son de acceso restringido.
(SEN) Área Sensible o Restringida	(OPE) Área Administrativa de Operaciones (BOD) Área de Bodegas, Logística de Recepción de Materia Prima. (CAL) Área de Control de Calidad (INV) Área de Investigación y Desarrollo (PLA) Planta, Sección o Nave de Producción	Áreas críticas en este caso de las empresas industriales de alimentos donde el acceso debe ser estrictamente restringido y controlado.

	(LOG) Área de Logística de Entrega (MAT) Área de Producción, Crianza o Cultivo de Materia Prima	
(SEG) Área de Seguridad Industrial y de Salud	(SAL) – Área Médica o de Salud (IND) – Área de Seguridad Industrial	Área de Seguridad Industrial y Salud (área médica) en la empresa.
(AUD) Área de Auditoría Interna		Área de Auditoría y control interno; con acceso restringido a sus recursos.
(VIG) Área de Vigilancia y Seguridad Física		Área de Vigilancia y Seguridad Física.
(OTR) Otras áreas que no consten en el listado.		Cualquier otra área que no conste en el listado y sea necesario incluirla, puede tener su propia clasificación en el subgrupo2, pero con tres caracteres para mantener la estandarización de la codificación.

Tabla 4.3. *Tabla de Clasificación de Activos: Edificaciones.*

GRUPO PRINCIPAL:	**(HW) Hardware**	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(SRV) Servidores		Se considera cualquier equipo servidor o que preste servicios informáticos al área en la que se está identificando los riesgos y se encuentre dentro de las instalaciones de la empresa.
(PCS) Equipos de Escritorio		Se considera dentro de este grupo a los computadores personales de escritorio que prestan su servicio como clientes o consumidores de servicios informáticos para los usuarios dentro de las instalaciones de la empresa. Su costo es más económico que los servidores y generalmente funcionan con periféricos de entrada/salida.

(LAP) Laptops		Computadores móviles que prestan su servicio como clientes o consumidores de servicios informáticos para los usuarios dentro y fuera de las instalaciones de la empresa.
(CEL) Celulares		Celulares no inteligentes que pertenecen a la empresa y prestan sus servicios a los usuarios que han sido autorizados para su custodia.
(MOV) Equipos Móviles Inteligentes		Celulares, tablets, PDAs, handhelds y toda clase de equipos inteligentes móviles que tienen la capacidad de navegación por internet, gestionar aplicaciones de la empresa, correos, redes sociales o herramientas para gestionar documentos, que pertenecen a la empresa y prestan sus servicios a los usuarios que han sido autorizados para su custodia.
(IMP) Impresoras		Cualquier equipo de impresión que preste solamente este servicio en el área donde se están analizando los riesgos, sea centralizado o conectado directamente a un computador.
(MLT) Impresoras Multifuncionales		Cualquier equipo de impresión multifuncional que preste los servicios de impresión y escaneo en el área donde se están analizando los riesgos, sea centralizado o conectado directamente a un computador.
(SCN) Scanners		Equipos que solamente realizan la función de escaneo.
(BAL) Balanzas		Balanzas industriales con o sin etiquetadoras que están conectadas al sistema informático que se utilizan para capturar los pesos de materia prima, productos en proceso y productos terminados.
(SNR) Sensores	TMP Temperatura PRS Presión PES Peso OTR Otros	Cualquier tipo de Sensor que envíe o reciba señales y datos a un sistema informático capturando información desde los equipos de producción, por ejemplo los PLCs o sensores que envían y reciben datos de sistemas de Supervisión, Control y Adquisición de Datos (SCADA).

Tabla 4.4. *Tabla de Clasificación de Activos: Hardware.*

GRUPO PRINCIPAL:	(SW) Software	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(DES) Software Desarrollado Internamente		Software Desarrollado en la propia empresa o integraciones desarrolladas en la empresa para software de terceros.
(SAT) Software Adquirido a Terceros	(SIO) Sistemas Operativos (OFI) Software de Ofimática (COR) Servidor de Correo Electrónico (SEG) Software de Seguridad Informática (GBD) Gestor de Bases de Datos (ERP) Software de Planificación de Recursos Empresariales. (MRP) Software de Planificación de Requerimientos de Materiales (Producción) (CRM) Software de Gestión de Relaciones con los Clientes (SRM) Software de Gestión de Relaciones con los Proveedores (DIS) Software o paquetes de Diseño Gráfico y CAD (Diseño Asistido por Computador). (VEN) Software para realizar la gestión comercial de Ventas o Publicidad. (PRG) Software para desarrollo (SBI) Software y herramientas de Inteligencia de Negocios (BAK) Software de Respaldos (MON) Software de Monitoreo y control de equipos, sensores, videovigilancia. (AYU) Software de Soporte o Mesa de Ayuda	Software adquirido a terceros, sea comercial o de libre uso y distribución. Debe ser instalado en los servidores o equipos de escritorio de la empresa. Una vez adquirido se concede su uso a la empresa mediante contratos y licencias comerciales o de software libre.
(SAS) Software como Servicio		Software contratado o alquilado como servicio a terceros y cuyos pagos de licencias o servicios son por períodos mensuales, anuales, etc. El software se encuentra instalado en equipos servidores remotos, bajo custodia y responsabilidad del Proveedor del Servicio. El subgrupo2 puede tener la misma clasificación que tiene el grupo de

		Software adquirido a Terceros e instalado en la empresa (grupo SWA).

Tabla 4.5. *Tabla de Clasificación de Activos: Software.*

GRUPO PRINCIPAL:	**(IE) Información Electrónica**	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(ARC) Archivos		Se puede considerar cualquier documento electrónico que no se encuentre clasificado en los otros subgrupos.
(ELE) Documentos Electrónicos Enviados y Recibidos desde entidades de Control		Documentos enviados y recibidos del ente de control, en nuestro medio el SRI, y que son los comprobantes válidos de las transacciones de ventas y compras. Deben ser firmados electrónicamente
(BAK) Copias de Respaldo		Archivos electrónicos de respaldo (copias del original).
(CON) Archivos de Configuración		Archivos de Configuraciones de Equipos o periféricos.
(LOG) Archivos de Registros de Actividades		Archivos de registros de actividades o errores de sistemas.
(CRI) Archivos Críticos o Sensibles	(FOR) Formulas, recetas, rutas o recursos para fabricación de productos (PRC) Procedimientos, Procesos (POL) Políticas (FIN) Información Financiera de la Empresa (PRD) Información sobre productos, precios (CLI) Información crítica sobre Clientes, Ventas de la empresa (PRV) Información crítica sobre Proveedores, Compras de la empresa (CON) Contratos con Terceros (SAN) Información Sanitaria	Archivos muy críticos, puesto que pueden contener información relevante sobre procesos, fórmulas o recetas de los productos que fabrica la empresa, y otros aspectos como información sobre productos, clientes, proveedores, compras, ventas de la empresa y su situación financiera/contable; así como los contratos con terceros que deben ser de acceso restringido.

(BBD) Bases de Datos	Bases de Datos que se manejan en el área o en toda la empresa.
(EXE) Código Ejecutable	El código ejecutable generalmente tiene una extensión EXE, COM o BAT. Es el resultado de la compilación del código fuente.
(FUE) Código Fuente	Archivos que contienen código de desarrollo, módulos o componentes de un Sistema.

Tabla 4.6. *Tabla de Clasificación de Activos: Información Electrónica*

GRUPO PRINCIPAL:	**(IP) Información en Papel**	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(DOC) Documentos en Papel		Se puede considerar cualquier documento escrito o impreso en papel que no se encuentre clasificado en los otros subgrupos, y que tenga alguna importancia para la empresa.
(CRI) Documentos Críticos o Sensibles en Papel	(FOR) Formulas, recetas, rutas o recursos para fabricación de productos (PRC) Procedimientos, Procesos (POL) Políticas (FIN) Información Financiera de la Empresa (PRD) Información sobre productos, precios (CLI) Información crítica sobre Clientes, Ventas de la empresa (PRV) Información crítica sobre Proveedores, Compras de la empresa (CON) Contratos con Terceros (SAN) Información Sanitaria	Archivos impresos o escritos muy críticos, puesto que pueden contener información relevante sobre procesos, fórmulas o recetas de los productos que fabrica la empresa, y otros aspectos como información sobre productos, clientes, proveedores, comprobantes de compras y ventas de la empresa y documentos impresos sobre su situación financiera/contable; así como los contratos con terceros que deben ser de acceso restringido.

Tabla 4.7. *Tabla de Clasificación de Activos: Información en Papel*

GRUPO PRINCIPAL:	(EX) Medios de Almacenamiento Extraíble	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(OPT) Medios Ópticos	(CDS) CDs (DVS) DVDs (BLU) Blue Ray Disc	Medios que requieren cuidado en su almacenamiento y manipulación, con un lector óptico se puede tener acceso a su contenido.
(ELE) Medios Electrónicos	(FLA) Flash Memory	Medios de almacenamiento Electrónicos Extraíbles, tipo Pen Drive, por lo general con interfaz USB.
(MEC) Medios Mecánicos	(DEX) Discos Duros Extraíbles	Medios de almacenamiento Mecánicos Extraíbles, tipo Disco Duro Externo, por lo general con interfaz USB.

Tabla 4.8. *Tabla de Clasificación de Activos: Medios de Almacenamiento Extraíble*

GRUPO PRINCIPAL:	(IC) Infraestructura de Comunicaciones	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(ROU) Router		Equipos de capa 3 para la interconexión y ruteo de paquetes de información entre redes distintas de la empresa.
(SWT) Switch		Switches de capa 2 y 3 para la interconexión de los equipos en la red de área local LAN dentro de las edificaciones de la empresa.
(TEL) Central Telefónica		Centrales telefónicas analógicas, IPs o Híbridas.
(WIF) Red WiFi		Redes inalámbricas de tipo WiFi en la empresa
(LAN) Red LAN		Red de Área Local (LAN) dentro de un mismo edificio en la empresa
(WAN) Red WAN		Red de Área Extensa (LAN) de la empresa para interconexión entre sucursales o locales de la empresa.
(FWR) Firewall		Firewall para controlar paquetes entrantes y salientes en la red, o equipos integrados conocidos como Unified Threat Management (UTM) o Gestión Unificada de Amenazas que integran

		varias funciones para la seguridad perimetral como Firewall, Proxy, Antispam, Sistema de Prevención de Intruciones (IPS), etc.

Tabla 4.9. *Tabla de Clasificación de Activos: Infraestructura de Comunicaciones*

GRUPO PRINCIPAL:	**(RH) Recursos Humanos**	
SUBGRUPO 1	**SUBGRUPO 2**	**OBSERVACIONES**
(UEX) Usuario Externo		Usuarios informáticos Externos, por ejemplo socios de negocios como Proveedores o Clientes.
(UIN) Usuario Interno Normal		Usuarios informáticos que pertenecen a la empresa.
(TIC) Usuario de TI		Personal que pertenece al departamento de Tecnologías de la Información.
(DIR) Directivo		Usuarios del equipo directivo de la empresa como el gerente, presidente o miembros de la junta directiva. Por lo general manejan información con acceso restringido.
(JEF) Jefe o Administrador del área o sucursal		Usuario que maneja información crítica o confidencial y que está a cargo o administra un área, departamento, sucursal o unidad de negocio. Por lo general manejan información con acceso restringido.
(INV) Usuario Crítico de Investigación y Desarrollo		Usuarios críticos con conocimiento y acceso a información de procesos, fórmulas o recetas de los productos que se fabrican en una empresa industrial.

Tabla 4.10. *Tabla de Clasificación de Activos: Recursos Humanos*

En la Figura 4.3 se muestra un ejemplo explicativo para la clasificación y codificación de activos de información para referirse por ejemplo a la planta de producción (01) dentro del grupo de Activos Edificaciones (ED) y como es una planta de producción se considera un área restringida o Sensible (SENS) dentro de una empresa industrial de alimentos.

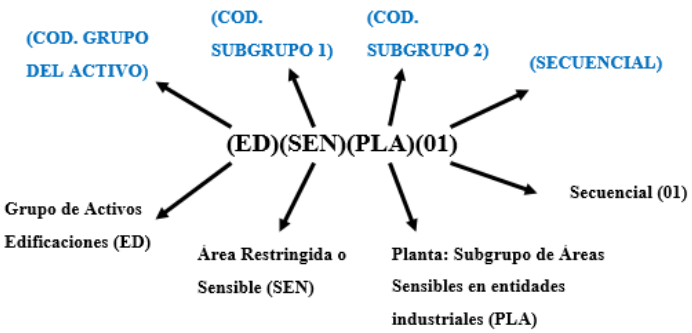

Figura 4.3 *Ejemplo de clasificación y codificación de activos de información (Crespo, 2016).*

A continuación, se deben valorar los activos de acuerdo a las dimensiones de valoración, que son las características o atributos que hacen valioso un activo. Una dimensión, según el Ministerio de Hacienda y Administraciones Públicas de España (2012), es un aspecto de un activo, independiente de otros aspectos, que permite realizar el análisis de riesgos centrados en un único aspecto o característica. Las dimensiones se usan para valorar las consecuencias de la materialización de una amenaza. (Ministerio de Hacienda y Administraciones Públicas de España, 2012) (Crespo, 2016). Las dimensiones se basan en los tres principios básicos en los que se fundamenta la seguridad de la información con sus iniciales como códigos: Confidencialidad (C), Disponibilidad (D) e Integridad (I). Crespo (2016) cita al Ministerio de Hacienda y Administraciones Públicas de España (2012), quienes indican que para valorar los activos sirve, en teoría, cualquier escala de valores, sin embargo frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos. La Tabla 4.11 presenta los criterios de valoración recomendados en esta metodología con escala o rango de 0-10.

VALOR	CRITERIO	IMPACTO SOBRE EL ACTIVO
10	Extremo	Daño extremadamente grave
9	muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	despreciable	irrelevante a efectos prácticos

Tabla 4.11. *Escalas de criterios de valoración de riesgos. Fuente: (Crespo, 2016) (Ministerio de Hacienda y Administraciones Públicas de España, 2012).*

En la Tabla 4.12 se muestra a continuación un ejemplo con el formato completo de identificación y valoración de Activos propuesto en la metodología en base a sus dimensiones de seguridad.

Código del Activo	Descripción	(D)	(I)	(C)	Valoración Total	Valor
(HW)(PCS)(01)	Equipo de Facturación	5	9	8	7.3	Alto

Tabla 4.12. *Formato con ejemplo para la identificación y valoración de activos de información con rango 0-10. Fuente: (Crespo, 2016).*

Como se puede ver en el ejemplo de la Tabla 4.12., para valorar un activo primero se tiene que codificarlo como en este caso, se trata de un activo del grupo Hardware (HW), subgrupo de computadores de escritorio (PCS) y con un secuencial único (01), que es un equipo de facturación y sirve para emitir las facturas electrónicas e impresas para los clientes de la empresa, se lo valoró en cuanto tiene que ver a sus dimensiones de seguridad de la siguiente manera:

- En cuanto a su **Disponibilidad** (D) con un valor de 5 sobre 10 (medio) debido a que si bien es un equipo imprescindible actualmente para cumplir con las operaciones de logística de entrega en cuanto a los procesos internos y el cumplimiento tributario con el organismo de control como lo es el Servicio de Rentas Internas (SRI), puede ser reemplazado en cualquier momento en corto tiempo por otro equipo en caso de algún defecto o problema, ya que el software que realiza la facturación se encuentra centralizado en un Servidor y no depende de este equipo de facturación.
- Respecto a su **Integridad** (I) ha sido calificado con un valor de 9 sobre 10 (muy alto) debido a que el usuario que tiene acceso al equipo y al software instalado en él para realizar la transacción de facturación; podría alterar esta información de ventas ocasionando daños e inexactitud en la misma, posibles pérdidas económicas, pérdidas de reputación y credibilidad para con los clientes y lo que es peor y más grave problemas legales y tributarios para la empresa con el ente de control (SRI).
- Se valoró su **Confidencialidad** (C) con un valor de 8 sobre 10 (alto), ya que el usuario que tiene acceso al equipo y al software de facturación, podría obtener información crítica para la empresa y apetecida por la competencia, como datos de clientes, precios, productos de venta y promociones.

Finalmente en este proceso de valoración de activos se realiza una media aritmética o promedio entre los valores de las 3 dimensiones valoradas (Disponibilidad, Integridad y Confidencialidad) y se obtiene un resultado de esta media, en este caso una valoración total de 7.3, que según la escala de valores de la Tabla 4.11 es calificada con un criterio “Alto” por estar dentro del rango 6-8, que podría ocasionar un impacto catalogado como un “Daño Grave” sobre el activo.

4.1.5. Paso 5: Identificación de Riesgos

Por lo expuesto en capítulos anteriores, se hace necesario identificar los riesgos que podrían afectar la información, activos y en sí a la continuidad del negocio de una empresa; por lo que en la metodología propuesta se sugiere una clasificación de las posibles amenazas o riesgos (las más frecuentes y conocidas) que pueden afectar a los activos de información en una organización. Crespo (2016) indica que en Ecuador, las amenazas de las organizaciones se pueden clasificar en 5 grupos: riesgos naturales, riesgos de comunicaciones, riesgos provocados (Intencionados), riesgos provocados (No intencionados) y riesgos lógicos; por lo que se tomará como base esta clasificación en la presente propuesta metodológica ya que se considera que se adapta también a las empresas industriales de alimentos en nuestro medio. En la Tabla 4.13 se muestra esta clasificación con su respectiva codificación con 2 dígitos y sus conceptos.

TIPO DE RIESGOS	CODIGO	CONCEPTO
Riesgos Naturales	**[RN]**	Incidentes naturales que se producen sin intervención humana afectando a los activos de información: rayos, tormenta eléctrica, terremoto, aludes, ciclones, avalancha, corrimiento de tierras, incendios e inundaciones.
Riesgos de Comunicaciones	**[RC]**	Incidentes en Telecomunicaciones que afectan a este tipo de activos de información: Errores de enrutamiento, alteración o intercepción de tramas de datos en la comunicación, errores en los activos de comunicaciones.
Riesgos Provocados (Intencionados)	**[PR]**	Desastres debidos a la actividad humana causados intencionalmente: explosiones, derrumbes, contaminación, sobrecarga eléctrica, alteración de fórmulas, corte energético, incendio e inundación, alteración o eliminación de Información provocada, etc.
Riesgos Provocados (No Intencionados)	**[NI]**	Son riesgos que por error o descuido del usuario de manera NO intencionada pueden ocasionar desastres como explosiones, accidentes, contaminación, sobrecarga eléctrica, corte energético, incendio e inundación, etc. Además los fallos NO intencionales causados por los usuarios que pueden desencadenar en ataques deliberados provocando la alteración o destrucción de la información, por ejemplo: Error de usuario, Error del administrador, Errores de monitorización (logs), Errores de configuración, Deficiencias en la organización, Alteración o eliminación de Información accidentales.

Riesgos Lógicos	**[RL]**	Amenazas que afectan directamente al software, datos y a la información electrónica en general de la empresa, ocasionando daños en su integridad, confidencialidad o disponibilidad. Estos pueden producirse de manera intencionada o no, por ejemplo por malware como virus, ransomware, troyanos, etc. que pueden ingresar a los equipos de la empresa por copias ilegales, mails, pishing, dispositivos extraíbles o móviles no autorizados, entre otras posibles alternativas. Ejemplos: difusión de software dañino, copia no controlada de información, escapes o fugas de información, infección con malware, ataques o intrusiones no autorizadas del personal.

Tabla 4.13. *Clasificación de riesgos. Fuente: (Crespo, 2016).*

Para la identificación de riesgos dentro de las categorías detalladas en la tabla 4.13., Crespo (2016) propone que el equipo de trabajo utilice como apoyo en este paso el cuestionario resumido en la Tabla 4.14.

Consulta Principal	***Posibles Preguntas***
¿Qué puede suceder?	¿Qué podría ir mal, que podría evitar el logro de los objetivos pertinentes?
	¿Qué acontecimientos o sucesos podría poner en peligro los resultados esperados?
¿Cómo puede suceder?	¿Qué pasó?
	¿Es probable que pueda volver a ocurrir?
	¿Qué factores podrían accionar su reincidencia?
¿Dónde puede suceder?	¿Dónde podría suceder?
	¿Es probable que el riesgo ocurra en cualquier lugar o en cualquier contexto?
	¿Es un riesgo que depende de la ubicación, área física o actividad?
¿Por qué podría suceder?	¿Qué factores deben estar presentes para que exista mayor probabilidad de que el riesgo se materialice o vuelva a ocurrir?
¿Cuál podría ser el impacto?	¿Qué impacto o consecuencias se presentan o podrían presentarse si el riesgo se materializa?
	¿En caso de ocurrir el impacto a qué tipo de activos afectaría?
	¿El impacto causaría consecuencias solo en un departamento, o en toda la organización?
	¿El impacto implica consecuencias de reputación o sólo financieras?

Tabla 4.14: *Consultas Iniciales para Identificación de Riesgos. Fuente: (Crespo, 2016)*

El cuestionario resumido en la Tabla 4.14 es una herramienta que facilitará la identificación de los riesgos en un área de la empresa, por lo que también se considera que en la metodología propuesta puede servir de ayuda al Equipo de Gestión de Seguridad de la Información quien es el encargado de identificar y analizar posteriormente los riesgos.

En la Tabla 4.15 se propone una matriz para la identificación y codificación de riesgos, para ser usada dentro de este paso y posteriormente complementarla en el siguiente (análisis de riesgos) como se ilustra y se explica en la Tabla 4.18.

COD RIESGO	NOMBRE RIESGO	DESCRIPCIÓN	ACTIVOS INVOLUCRADOS	ACTIVOS AFECTADOS	UBICACIONES (DONDE SE PUEDE DAR)
[RL.3]	Escapes o Fugas de Información	La información llega al conocimiento de personas que no deberían tener acceso a la misma, sin que la información en sí misma se vea alterada.	[SW.*] [HW.*] [IC.*] [EX.*] [RH.*]	[IE.*][IP.*]	[ED.*]

Tabla 4.15: *Matriz de identificación de Riesgos.*

En el ejemplo de la Tabla 4.15 se observa en la primera columna (COD RIESGO) que el riesgo es codificado entre corchetes dentro del grupo de Riesgos Lógicos (RL) con una secuencia (3), en la siguiente columna (NOMBRE RIESGO) se coloca una descripción corta pero clara del riesgo para que cualquier lector sepa rápidamente de que se trata, en el ejemplo son “escapes o fugas de información”, en donde la información puede llegar de manera accidental o intencionada a personas que no deberían tener acceso a la misma, sin que la información en sí misma se vea alterada o eliminada; esta información detallada acerca del riesgo se coloca en la tercera columna (DESCRIPCIÓN). Finalmente, este o cualquier otro riesgo involucra o afecta de alguna manera a uno o varios tipos de activos de información, que por espacio y facilidad de manejo de la matriz, se los lista en las columnas de “TIPOS DE ACTIVOS INVOLUCRADOS” Y “TIPOS DE ACTIVOS AFECTADOS” citándolos solamente por su codificación entre corchetes vista en el paso anterior y separando los grupos, subgrupos y secuencial de activos por un punto (.); por ejemplo, en este caso la fuga de información afecta directamente a cualquier información en papel [IP.*] e información Electrónica [IE.*] de la empresa, y este riesgo se puede materializar mediante el mal uso de activos involucrados como cualquier tipo de medio de almacenamiento extraíble [EX.*], Software [SW.*], Hardware [HW.*], Infraestructura de

Comunicaciones[IC.*], y por lo general este riesgo es ocasionado deliberadamente o sin intención por cualquier recurso humano [RH.*] que tenga acceso a los equipos e información. En este ejemplo se considera que el riesgo puede materializarse desde cualquier local, ubicación o Edificación [ED.*] de la empresa, debido a que la fuga de información no necesariamente se puede dar desde una localidad en particular, ya que independiente del lugar simplemente disponiendo de acceso a alguno de los activos involucrados se podría materializar el riesgo.

El símbolo de asterisco (*) en la codificación de activos del ejemplo visto en la Tabla 4.15 hace referencia a que son afectados, involucrados todos los activos que pertenecen a ese grupo o subgrupo de activos; sin embargo, la metodología deja la libertad al equipo de trabajo que los activos afectados, involucrados o los lugares se pueden especificar hasta el nivel de detalle que se considere necesario, siguiendo el formato: *[Grupo.Subgrupo1.Subgrupo2.Secuencial]*.

4.1.6. Paso 6: Análisis de Riesgos

En este paso de la etapa, se busca analizar los riesgos encontrados en el paso anterior mediante la valoración de la probabilidad de que ocurra un riesgo y su consecuencia o impacto. Para ello Crespo (2016) toma esta parte de la metodología de gestión de riesgos propuesta por la Universidad de Adelaide (2015), donde se plantean 5 niveles de probabilidad de ocurrencia de riesgos: *rara, poco probable, posible, probable, casi segura* (Crespo, 2016) (University of Adelaide, 2015). Este proceso clasifica también las consecuencias o impacto de la materialización de un evento o riesgo como *insignificante, menor, moderada, grave o extrema*.

En la metodología propuesta en este paso, se analiza cada riesgo mediante una matriz de valoración de riesgos (University of Adelaide, 2015), como se puede ver en la Tabla 4.16, y se ubica al riesgo de manera cualitativa en dicha matriz según su probabilidad de ocurrencia y sus consecuencias o impacto; ubicando así al riesgo en la celda correspondiente de esta matriz, analizando también las posibles acciones de gestión requeridas y sus prioridades para tratar de mitigar cada riesgo como se ilustran en la Tabla 4.17.

		Consecuencia				
		1. Insignificante	**2. Menor**	**3. Moderada**	**4. Grave**	**5. Extrema**
Probabilidad	**A - Casi Segura**	M	M	A	E	E
	B - Probable	B	M	A	A	E
	C - Posible	B	M	M	A	A
	D - Poco Probable	B	B	M	M	A
	E - Rara	B	B	B	B	M

Tabla 4.16. *Matriz de valoración de riesgos según su probabilidad y consecuencias. Fuente: (Crespo, 2016) (University of Adelaide, 2015).*

Niveles de Riesgo	Prioridades y Acciones de Gestión Requeridas
Riesgo extremo (E)	Requiere respuesta y atención inmediata y gestionarse
Riesgo alto (A)	Debe otorgársele la atención apropiada y gestionarse
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes o si son necesarias tomar acciones. Monitoreo y revisión local.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios, informar a los administradores de seguridad locales. Monitoreo y revisión local de considerarse necesario.

Tabla 4.17. *Niveles de riesgos y acciones de gestión requeridas por su Prioridad. Fuente: (Crespo, 2016) (University of Adelaide, 2015).*

En las matrices visualizadas en las Tablas 4.16 y 4.17 es necesario distinguir con los colores indicados los resultados del análisis de riesgos para que el equipo de trabajo identifique claramente los niveles y prioridades de atención y gestión que requiere cada riesgo analizado, información que servirá en la siguiente etapa para el planteamiento de una política de seguridad de la información.

Finalmente y como aporte a la metodología en este paso se sugiere una matriz para la identificación y valoración de los riesgos encontrados en la organización, indicando en dicha matriz los riesgos identificados con los campos definidos en la identificación de riesgos del paso anterior (Tabla 4.15), junto con otra columna donde se indican entre corchetes las iniciales de las dimensiones de seguridad afectadas ([C]onfidencialidad, [I]ntegridad y [D]isponibilidad) si se llega a materializar el riesgo presentando, además una columna adicional indicando el color y codificación de la valoración del riesgo, resultado del análisis cualitativo mediante la matriz de valoración de riesgos según su probabilidad y consecuencias (Tabla 4.16).

Esta nueva matriz se muestra con 2 ejemplos de riesgos en la Tabla 4.18, planteando así un formato tabular completo y sencillo de desarrollar y comprender para la identificación y valoración de riesgos; siendo dicho formato el artefacto final entregable de esta sección de la metodología.

COD RIESGO	NOMBRE RIESGO	DESCRIPCIÓN	ACTIVOS INVOLU_ CRADOS	ACTIVOS AFEC_ TADOS	UBICACION (DONDE SE PUEDE DAR)	DIMENS. AFECTADAS	VALOR RIESGO
[RL.3]	Escapes o Fugas de Información	La información llega al conocimiento de personas que no deberían tener acceso a la misma, de forma intencional o accidental sin que la información en sí misma se vea alterada.	[SW.*] [HW.*] [IC.*] [EX.*] [RH.*]	[IE.*][IP.*]	[ED.*]	[C]	**A**
[RL.5]	Infecciones de Malware en los equipos	Infecciones intencionadas o no de Malware en los equipos, poniendo en riesgo la seguridad de información, alterando o eliminando la misma.	[HW.*] [IC.*] [EX.*] [RH.*]	[IE.*] [SW.*]	[ED.*]	[C][D][I]	**E**

Tabla 4.18. *Matriz de Identificación y Valoración de Riesgos*

De esta manera se podrá visualizar en una sola matriz claramente los riesgos de la organización o de un área específica de la misma, con su codificación, nombre, descripción detallada, los activos involucrados, los activos afectados, las ubicaciones donde se pueden dar los riesgos, las dimensiones de seguridad afectadas y además la valoración de los riesgos para posteriormente, con toda esta información, tomar acciones para mitigar o eliminar dichos riesgos mediante el planteamiento e implementación de controles adecuados dentro de una política de seguridad de la información para la empresa.

4.2. Etapa 2: Desarrollo de la Política de Seguridad de la Información

Siguiendo con la metodología planteada, una vez identificados los activos y los riesgos de seguridad de la información de la empresa o área donde se aplicará la metodología, lo que posteriormente se propone en este trabajo de titulación es continuar con la etapa del desarrollo de una política de seguridad de la información que mitigue los riesgos detectados en un departamento o en una empresa industrial de alimentos. Esta etapa de la metodología junto con la de Difusión de la Política de Seguridad se las resume en la Figura 4.4 con notación SPEM identificando responsables,

instrumentos, entradas y salidas que intervienen en cada paso de la metodología propuesta.

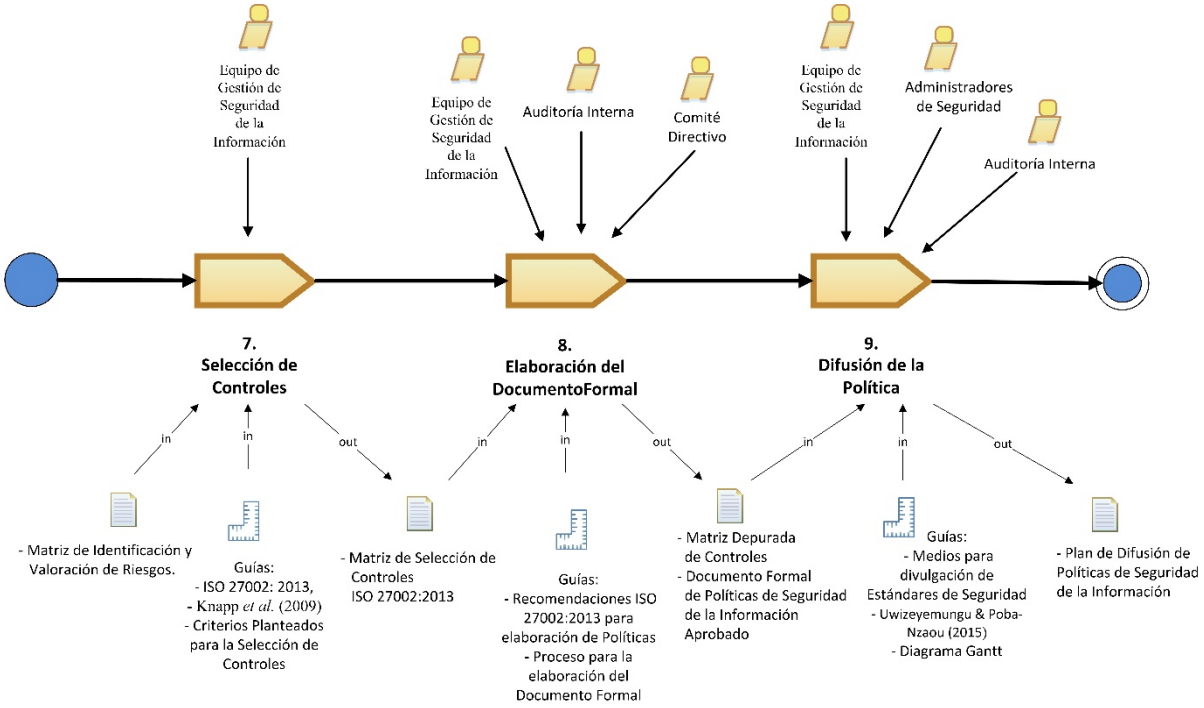

Figura 4.4 *Metodología Detallada de las Etapas de Desarrollo y Difusión de Políticas de Seguridad de la Información.*

4.2.1. Paso 7: Selección de Controles

Cada cláusula o dominio del estándar ISO 27002 (2013) define los controles de seguridad y contiene una o más categorías con objetivos principales de seguridad. El orden de las cláusulas de esta norma no implica su importancia y, dependiendo de las circunstancias, los controles de seguridad de cualquiera o todas las cláusulas de la norma podrían ser importantes, por lo tanto, cada organización que aplique esta norma debe identificar los controles aplicables, la importancia de éstos y su aplicación a los procesos empresariales individuales. Además, el listado de la norma no está en orden de prioridad (ISO 27002, 2013); lo que implica que cada organización puede escoger las cláusulas y controles que más se adapten a sus necesidades.

El estándar ISO 27002 (2013) indica también que la selección de los controles depende de las decisiones organizativas basadas en los criterios de evaluación y aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque general de gestión de riesgos aplicados a la organización, estando alineadas también a la legislación laboral nacional pertinente. La selección de controles también depende de la manera en que los controles interactúan para proporcionar el concepto de defensa en profundidad; además, algunos de los controles de esta norma pueden considerarse como guías

principales para la gestión de la seguridad de la información y son aplicables a la mayoría de las organizaciones (ISO 27002, 2013).

Este paso de la metodología es realizado en su totalidad por el *Equipo de Gestión de Seguridad de la Información*, como se estructuró en el paso 2 (ver Tabla 4.1) para la estructuración del equipo de trabajo, con la revisión del equipo de Auditoría Interna para la constatación de que se están seleccionando los controles adecuados que mitiguen los riesgos identificados.

Conociendo la importancia de seleccionar los controles más apropiados para hacer frente a los riesgos identificados en la organización y posteriormente plantearlos en una política de seguridad de la información, se plantea de una manera sencilla un proceso para la selección de dichos controles, que básicamente se basa en analizar la *Matriz de Identificación y Valoración de Riesgos* (ver Tabla 4.18) y determinar los activos o grupos de activos involucrados en cada riesgo, que son los medios utilizados que ocasionan o pudiesen ocasionar la materialización del riesgo, junto con la ubicación donde el riesgo puede suceder y los activos afectados, que son los que se deben proteger, para con estos criterios más la información y descripción del mismo riesgo escoger el dominio de la norma ISO 27002 (2013), su categoría y los posibles controles siendo importante para ello revisar el objetivo que persigue la categoría de control respectiva y sabiendo que el equipo de trabajo puede seleccionar más de un dominio, categorías de control o controles para un mismo riesgo.

Además se pueden sugerir, de ser necesario, nuevos controles en el caso de que no se los encuentre en el estándar pero se consideren importantes para mitigar o eliminar el riesgo identificado; así lo justifica y sugiere la misma norma ISO 27002 (2013), en su sección de Introducción, en el punto "*0.3 – Selección de Controles*", indica claramente que "los controles se pueden seleccionar a partir de este estándar, sin embargo pueden diseñarse nuevos controles para satisfacer necesidades específicas según sea apropiado"; por lo tanto se pueden seleccionar o agregar controles según sean necesarios y adecuados para una organización. Este proceso y sus criterios de selección de controles se los resume en la Figura 4.5.

Figura 4.5 *Criterios para la Selección de Controles de Seguridad*

Finalmente como entregable en este paso de la metodología, se plantea el formato mostrado en la Tabla 4.19 donde se indica la información sobre cada riesgo indicada en la etapa 6 de la metodología (Tabla 4.18) junto con el Dominio, Categoría y Controles o Políticas aplicables y adecuados seleccionados del estándar ISO 27002 (2013), o agregados como nuevos controles que se consideren necesarios para mitigar los riesgos identificados. Hay que tener presente que sobre todo que los riesgos calificados como extremos y altos son los que necesitan atención prioritaria y serán los que obligatoriamente deban contener los controles necesarios para mitigarlos. Como ayuda y recomendación en este paso para el equipo de trabajo, se puede observar de una manera rápida y resumida los dominios, categorías de control, objetivos de control y los respectivos controles de seguridad que sugiere el estándar ISO 27002 (2013) en las Tablas 1.1 y 1.2 del Anexo 1.

Como se ilustra en el ejemplo de la Tabla 4.19 la matriz propuesta se conforma de la información de cada riesgo identificado en la etapa anterior (paso 6) más los campos de los Dominios, Categorías y Controles o Políticas de seguridad más adecuados y seleccionados del estándar ISO 27002 (2013) para hacer frente al riesgo puntualmente analizado; siguiendo el método explicado y graficado en la Figura 4.5.

En este paso no tiene relevancia si entre dos o más riesgos se vuelven a repetir dominios, categorías o controles de la norma ISO 27002, ya que en el próximo paso de la etapa es donde se los depura y se los plantea formalmente como un documento de Política de Seguridad de la Información.

COD RIESGO	NOMBRE RIESGO	DESCRIPCIÓN	ACTIVOS INVOLU_ CRADOS	ACTIVOS AFEC_ TADOS	UBICACION (DONDE SE PUEDE DAR)	DIMENS. AFECTADAS	VALOR RIESGO
[RL.3]	Escapes o Fugas de Información	La información llega al conocimiento de personas que no deberían tener acceso a la misma, de forma intencional o accidental sin que la información en sí misma se vea alterada.	[SW.*] [HW.*] [IC.*] [EX.*] [RH.*]	[IE.*][IP.*]	[ED.*]	[C]	**A**

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
6. Organización de la Seguridad de la Información	6.2. Dispositivos para movilidad y teletrabajo	6.2.1. Política de uso de dispositivos móviles.
7. Seguridad de los Recursos Humanos	7.1. Antes de la contratación 7.2. Durante la contratación 7.3. Cese o cambio de puesto de trabajo	7.1.2. Términos y condiciones de la contratación 7.2.2. Concientización, educación y capacitación en seguridad de la información 7.3.1. Cese o Cambio de puesto de Trabajo

8. Gestión de Activos	8.3. Manejo de los soportes de Almacenamiento	8.3.1. Gestión de soportes extraíbles 8.3.2. Eliminación de Soportes 8.3.3. Soportes físicos en Tránsito
9. Control de Accesos	9.3. Responsabilidades del Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones	9.3.1. Uso de información confidencial para la autenticación 9.4.1. Restricción del Acceso a la Información 9.4.2. Procedimientos Seguros de inicio de sesión 9.4.3. Gestión de Contraseñas de Usuario
10. Cifrado	10.1. Controles Criptográficos	10.1.1. Política de uso de controles criptográficos
11. Seguridad Física y Ambiental	11.2. Seguridad de los Equipos	11.2.5. Salida de activos fuera de las dependencias de la empresa. 11.2.6. Seguridad de los quipos y activos fuera de las instalaciones 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento 11.2.8. Equipo informático de usuario desatendido 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla
13. Seguridad en las Telecomunicaciones	13.2 Intercambio de información	13.2.1. Políticas y procedimientos de intercambio de información 13.2.2. Acuerdos de intercambio 13.2.3. Mensajería electrónica 13.2.4. Acuerdos de Confidencialidad y Secreto

Tabla 4.19. *Matriz de Selección de Controles ISO 27002 para los Riesgos de Seguridad identificados*

4.2.2. Paso 8: Elaboración del Documento Formal

El objetivo de este paso de la metodología es plantear los controles y políticas específicas obtenidas en el paso anterior como una política de seguridad de la información para la organización en un documento formal dirigido a la dirección de la empresa para su aprobación y posterior difusión a todo el personal que pertenece al área o empresa analizada.

Según Barbosa Martins & Saibel (2005), una política de seguridad es un documento que debe describir las recomendaciones, las reglas, las responsabilidades y prácticas más adecuadas de seguridad para la empresa; sin embargo, se sabe que no existe una "política de seguridad modelo" que pueda ser implementada en cualquier organización, pues una política deberá ser moldeada según las especificaciones de cada caso.

Entonces como una guía en este paso, se utiliza también la norma ISO/IEC 27002 (2013), donde en el alcance del dominio o cláusula número 5 hace referencia a las "*Políticas de seguridad de la información*", que contiene una categoría de control: "*Directrices de Gestión para la seguridad de la información"* y cuyo objetivo es "*Proporcionar directrices de gestión y soporte para la seguridad de la información de acuerdo a los requerimientos del negocio, leyes y reglamentos relevantes*". En el primer control de esta categoría, llamado "*Políticas para la seguridad de la información*" se indica que

se debe definir una política para la seguridad de la información en un documento aprobado por la dirección, publicado y comunicado a los empleados y a las partes externas relevantes.

Para lograr plasmar los controles identificados en el paso 7 (Selección de Controles) en un documento formal como una política de seguridad informática, se sugiere seguir el siguiente proceso: reunir todos los controles y políticas identificados en la *Matriz de Selección de Controles ISO 27002* para los riesgos de seguridad identificados (Tabla 4.19) y ordenarlos por dominios, categorías y controles en el mismo orden y numeración que plantea el estándar, por facilidad de ordenamiento. Se procede luego a descartar los elementos de control duplicados en esta nueva matriz y de esta manera finalmente se arma una sola matriz de Dominios, Categorías y Controles llamada *Matriz Depurada de Controles* (Tabla 4.20) a utilizarse para elaborar con esos controles finalmente en el documento formal de políticas de seguridad de la información, siguiendo las recomendaciones hechas por el estándar ISO 27002. Este proceso se ilustra en la Figura 4.6.

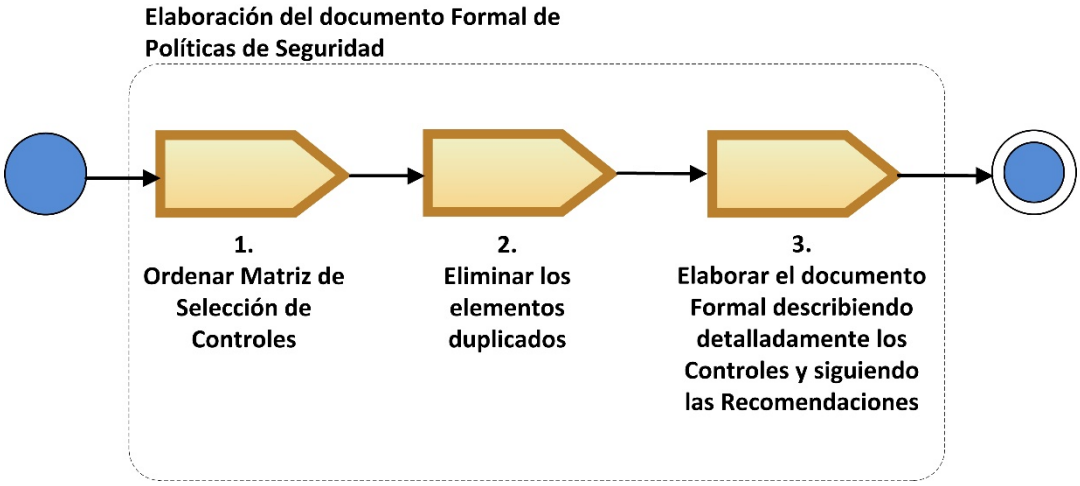

Figura 4.6 *Proceso para la Elaboración del Documento Formal de Políticas de Seguridad*

DIMENSIONES	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
6. Organización de la Seguridad de la Información	6.2. Dispositivos para movilidad y teletrabajo	6.2.1. Política de uso de dispositivos móviles.
7. Seguridad de los Recursos Humanos	7.1. Antes de la contratación 7.2. Durante la contratación 7.3. Cese o cambio de puesto de trabajo	7.1.2. Términos y condiciones de la contratación 7.2.2. Concientización, educación y capacitación en seguridad de la información 7.3.1. Cese o Cambio de puesto de Trabajo
8. Gestión de Activos	8.3. Manejo de los soportes de Almacenamiento	8.3.1. Gestión de soportes extraíbles 8.3.2. Eliminación de Soportes 8.3.3. Soportes físicos en Tránsito
9. Control de Accesos	9.3. Responsabilidades del Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones	9.3.1. Uso de información confidencial para la autenticación 9.4.1. Restricción del Acceso a la Información 9.4.2. Procedimientos Seguros de inicio de sesión 9.4.3. Gestión de Contraseñas de Usuario

10. Cifrado	10.1. Controles Criptográficos	10.1.1. Política de uso de controles criptográficos
11. Seguridad Física y Ambiental	11.2. Seguridad de los Equipos	11.2.5. Salida de activos fuera de las dependencias de la empresa. 11.2.6. Seguridad de los quipos y activos fuera de las instalaciones 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento 11.2.8. Equipo informático de usuario desatendido 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla
13. Seguridad en las Telecomunicaciones	13.2 Intercambio de información	13.2.1. Políticas y procedimientos de intercambio de información 13.2.2. Acuerdos de intercambio 13.2.3. Mensajería electrónica 13.2.4. Acuerdos de Confidencialidad y Secreto

Tabla 4.20. *Matriz Depurada de Controles*

Una vez ordenados y eliminados los elementos duplicados en la *Matriz Depurada de Controles*, como se muestra en la Tabla 4.20, en base a las sugerencias realizadas por la norma ISO 27002 y descritas anteriormente, se plantean estos controles en el Documento Formal de Políticas de Seguridad de la Información, y siguiendo la guía de implementación de este control, ISO/IEC 27002 (2013), recomienda que en el más alto nivel, las organizaciones deben definir una "política de seguridad de la información" que sea aprobada por la administración y que establezca el enfoque de la organización para manejar sus objetivos referentes a la seguridad de la información. Las políticas de seguridad de la información a este nivel deben responder a los requisitos creados por:

a) Una estrategia empresarial.
b) Reglamentos, legislación y contratos.
c) El entorno actual y proyectado de amenazas a la seguridad de la información.

La política de seguridad de la información debe contener declaraciones que hacen referencia a:

a) La definición de la seguridad de la información, objetivos y principios que guíen todas las actividades relacionadas con la seguridad de la información, es decir los objetivos que se persiguen con la política de seguridad y lo que significa la seguridad de la información para la empresa.
b) La asignación de responsabilidades generales y específicas para la gestión de seguridad de la información a funciones definidas, es decir la estructura de responsabilidades vistas en el paso 2 (Estructuración del equipo de Trabajo).
c) Los procesos de manejo de desviaciones y excepciones, es decir salvedades y quien o quienes las debería autorizar en caso de darse las mismas.

En un nivel inferior, la política de seguridad de la información debería estar respaldada por políticas específicas en ciertos temas, que obligan a la implementación de controles de seguridad de la

información y suelen estructurarse para atender las necesidades de ciertos grupos objetivo dentro de una organización o para cubrir determinados temas puntuales (ISO/IEC 27002, 2013). Es en esta sección donde se deben colocar los controles seleccionados y ordenados del estándar en la *Matriz Depurada de Controles* (Tabla 4.20) y detallarlos al nivel que se considere necesario, según las recomendaciones realizadas en cada control por el estándar ISO 27002:2013; agrupándolos por dominios como cláusulas en la política, seguidos por sus categorías o controles en detalle citándolos con letras consecutivas como a) b) c), etc. dentro de cada dominio o cláusula.

La política de seguridad puede incluir cualquiera de los dominios (del 6 al 18 según la estructura que se revisó en el punto 2.8.4 del Capítulo 2 y en las Tablas 1.1 y 1.2 del Anexo 1), con sus categorías de control y controles respectivos que menciona la norma ISO/IEC 27002 (2013); ordenándolos mediante cláusulas enumeradas y consecutivas.

Siguiendo entonces estas recomendaciones de la norma ISO 27002 para la elaboración del Documento Formal de Políticas de Seguridad de la Información, se plantea el siguiente formato:

LOGO Y NOMBRE DE LA EMPRESA	**POLITICA DE SEGURIDAD DE LA INFORMACIÓN**	**Versión:** (*Versión de la Política*) **Fecha de Elaboración:** _____ **Fecha Actualización:** _____
	Departamento o Área Responsable	**Codificación:** (*Codificación Interna del Documento*)

1. FIRMAS DE APROBACIÓN DEL DOCUMENTO

ROL	NOMBRE / CARGO	FIRMA	FECHA
APROBADO POR:			
REVISADO POR:			
ELABORADO POR:			

2. INDICE Y CONTENIDO

Detallar índice y contenido completo del documento.

3. OBJETIVOS

Definir los Objetivos de la política teniendo en cuenta las recomendaciones vistas de ISO 27002,

y lo que la empresa quiere lograr con la implementación de las políticas de seguridad de la información.

4. ALCANCE

Definir el alcance que tendrá la política y a que usuarios o áreas está dirigida.

5. PRINCIPIOS

Indicar los principios de seguridad de la información en los que se fundamenta el documento.

6. BASE LEGAL

Indicar la base legal nacional y laboral sobre la cual las políticas pueden sustentarse sin infringir las leyes; por ejemplo en el caso de las empresas industriales de alimentos en el Ecuador sería el Código de Trabajo, la ley de propiedad intelectual, acuerdos ministeriales del ministerio de trabajo o también el reglamento interno de la empresa, siempre que está aprobado por el ministerio de trabajo.

7. RESPONSABILIDADES

Se deben definir las responsabilidades del equipo de trabajo, como se encuentran en la Tabla 4.1. También se deben definir las responsabilidades de los usuarios de la empresa en cuanto a la política de seguridad de la información se refiere. En este punto también se establecen la responsabilidad de la autorización de salvedades o excepciones para los controles que se enumeran a continuación en la política.

8. DESCRIPCION DE LA POLITICA

En esta sección donde es donde se describen los controles seleccionados y ordenados del estándar en la Matriz Depurada de Controles (Tabla 4.20), detallándolos como se considere necesario, según las recomendaciones realizadas en cada control por el estándar ISO 27002:2013. Además se los debe agrupar por dominios como cláusulas en la política, seguidos por sus categorías o controles en detalle citándolos con letras consecutivas como a) b) c), etc. dentro de cada dominio o cláusula. Por ejemplo:

8.10. SEGURIDAD EN EL DESARROLLO, MANTENIMIENTO Y ADQUISICION DE SISTEMAS (*Este es el Dominio o cláusula principal*)

Aquí va el detalle del Dominio o Categoría Seleccionados. Ejemplo: El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar

los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Para esto, el departamento de Tecnologías de la Información y Comunicaciones (TICs) será responsable de:

Aquí van los controles seleccionados detallándolos siguiendo las recomendaciones que ISO 27002: 2013 hace en su detalle para la aplicación de cada control. Ejemplo:

a) Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información;

b) Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan;

c) Definir los métodos de protección de la información crítica o sensible;

4.3. Etapa 3: Difusión de la Política de Seguridad

El objetivo de esta etapa de la metodología es recomendar los medios o herramientas para dar a conocer en la empresa las políticas de seguridad de la información desde un punto de vista sencillo, práctico y amistoso, tratando de llegar al usuario de una manera amigable para motivarlo a que se capacite, cumpla y promueva el uso de las Políticas de Seguridad de la Información en todo momento tanto dentro como fuera de la organización.

4.3.1. Paso 9: Difusión de la Política

Es fundamental la existencia de políticas de seguridad que sean realmente una referencia para los colaboradores de una organización, posibilitando así la garantía de los tres principios básicos de la seguridad de la información: integridad, disponibilidad y confiabilidad (Barbosa Martins & Saibel, 2005). Así, para lograr la elaboración de una política de seguridad de la información hasta el momento se ha propuesto una metodología que va desde la etapa de identificación y análisis de riesgos hasta la elaboración de un documento formal de políticas de seguridad de la información, pasando por una etapa muy importante que es la selección de los controles del estándar ISO 27002.

Sin embargo no sirve de mucho todo este proceso si no se concientiza y difunde la política al personal de la empresa, de manera que quede registrada su capacitación y comprensión sobre la política de seguridad de la información, para que posteriormente el cumplimiento de la política pueda ser monitoreado y auditado; pudiendo así incentivar al cumplimiento de la política o sancionar por su incumplimiento. Finalmente y debido a los cambios acelerados de las Tecnologías de Información y

Comunicaciones y las amenazas que enfrenta la seguridad de la información, la política puede ser evaluada cada cierto tiempo y actualizada o eliminada de ser el caso. Esto lo corroboran Barbosa Martins & Saibel (2005) quienes indican que elaborar una política de seguridad es una tarea compleja que se debe modelar de acuerdo a las especificaciones y requerimientos de cada organización y necesita ser constantemente monitoreada, revisada y actualizada; además, sus resultados normalmente sólo se pueden observar a mediano y largo plazo.

Es importante para los investigadores, y diseñadores de políticas de seguridad de la información comprender que existen bajos niveles de difusión de los estándares de seguridad de la información en las organizaciones (Uwizeyemungu & Poba-Nzaou, 2015); el estudio de estos autores sobre la base de una perspectiva institucional, muestra que muchos de los estándares de seguridad de la información, como lo son las normas ISO, han llegado a fracasar o a tener un cumplimiento incompleto o inadecuado debido principalmente a una falta de difusión adecuada de los estándares en las organizaciones.

Uwizeyemungu & Poba-Nzaou (2015) indican que una correcta etapa de difusión consiste en propagar, divulgar y difundir la Política de Seguridad de la Información, así como sus objetivos y beneficios para crear conciencia en todo el personal de la organización sobre de la importancia que tiene el cumplimiento de los controles indicados en la política dentro y fuera de la empresa.

Es necesario que se tenga en cuenta que existen usuarios, los cuales no tienen un conocimiento básico o tienen limitaciones con respecto al lenguaje relacionado con los temas de la seguridad informática, por lo que es necesario el uso de un lenguaje y términos adecuados mediante los cuales dichos usuarios puedan comprender correctamente la política de seguridad.

Es necesario también la motivación que se debe dar a los usuarios para querer aprender acerca del tema de seguridad de la información, a que estén interesados en el mismo de manera que puedan ser capacitados de una manera adecuada y eficiente. Con la finalidad de la motivación es necesario mostrar las ventajas o beneficios que se obtienen al cumplir con las políticas de seguridad, es decir, se debe mostrar a los usuarios la parte práctica en la cual se muestre la eficacia de esta estrategia que busca no solamente proteger a la organización, sino que va más allá protegiendo también los activos personales de cada usuario.

Entonces, la difusión es dar a conocer las políticas de seguridad de la información desde un punto de vista sencillo, práctico y amistoso, buscando llegar con estos temas al usuario de una manera amigable con el objetivo de motivar a todo tipo de usuario para que se capacite, cumpla y promueva el uso de las Políticas de Seguridad de la Información en todo momento tanto dentro como fuera de la organización.

Las políticas deben comunicarse a los empleados y a las partes externas pertinentes de una forma

que sea relevante, accesible y comprensible para el lector, por ejemplo mediante un *"programa de sensibilización, educación y formación en materia de seguridad de la información"* como lo indica el control 7.2.2 (Concientización, educación y capacitación en seguridad de la información) en la estructura del estándar ISO/IEC 27002 (2013).

Por ello en esta sección de la metodología se dan algunas recomendaciones para que esta importante etapa de difusión se lleve con éxito una vez que se tenga la política en un documento formal aprobado por el Comité Directivo.

Uso de publicidad: El uso de publicidad que contenga información concreta acerca de las Políticas de Seguridad en la empresa o área, esta información puede ser un anuncio electrónico en la página web o intranet de la empresa, un link en un correo institucional o un anuncio colgado en papel en un sitio de la empresa frecuentado, con el objetivo de que la información que contenga este cartel sólo sea para informar al usuario acerca del lugar donde se puede encontrar dicha información, sin embargo, es necesario que el cartel contenga información acerca del tema de seguridad de la información y de la política de seguridad, que indique lo que encontrará y para qué es, así como alguna ilustración acorde con el tema que pueda dar una idea y atrape la atención del usuario.

Campañas de Capacitaciones y Conferencias de Concientización: Brindar charlas o capacitaciones en temas de seguridad informática para motivar al personal y luego ir concientizando en la importancia del cumplimiento de las políticas de seguridad tanto para la empresa como personalmente, es una de las maneras en las que se puede propagar y capacitar a una buena parte del personal entregando directamente todo el conocimiento necesario a los asistentes. Para locales remotos o nuevos empleados que no pudiesen asistir directamente a la capacitación, existen herramientas de TI que se pueden utilizar, grabando la capacitación y enviándola remotamente o colgándola en la página web empresarial o en la intranet para que la puedan revisar tanto los empleados que no pudieron asistir, como los que si asistieron pero tienen dudas y podrían volverla a ver.

Sitio Web: Un sitio web sea una intranet o la página web empresarial expuesta al público es una gran herramienta para la difusión de las Políticas de Seguridad de la Información; sin embargo su diseño debe ser sencillo, de fácil navegabilidad y usabilidad, buscando sobre todo que auxilie al usuario en la búsqueda, capacitación y enseñanza de la información sobre las políticas de seguridad, de manera que esta información no sea ajena o tediosa para los usuarios sino que sea una herramienta práctica que promueva el uso y consulta de documentos como las políticas de seguridad para conservar la integridad, disponibilidad y confidencialidad

estableciendo un nivel apropiado de seguridad informática.

Otros: Se puede utilizar cualquier otro medio de difusión y conocimiento de las políticas de seguridad de la información que la empresa lo requiera, con tal de que cumplan la finalidad de dar a conocer las políticas de seguridad de la información a todo el personal del área involucrada o empresa de una manera sencilla, práctica y amistosa.

En este paso de la metodología es necesario escoger los tipos de medios por los que se pueden difundir las políticas, y de manera sugerida elaborar un cronograma mediante un diagrama de Gantt que contenga todas las actividades necesarias que se tengan que realizar para difundir las políticas por el medio o medios escogidos; presentando así finalmente un Plan de Difusión de las Políticas de Seguridad de la Información.

4.4. Conclusiones del Planteamiento de la Metodología

En resumen, en este capítulo se realizó el planteamiento de un método técnico y adecuado consistente de 3 etapas y un total de 9 pasos para la identificación, análisis y evaluación de riesgos y la elaboración formal de las políticas de seguridad en base a una selección de controles de la norma ISO/IEC 27002 (2013) que mitiguen los riesgos identificados en una empresa industrial de alimentos.

Las 3 etapas planteadas en la metodología son:

- Etapa 1: Identificación y Análisis de Riesgos
- Etapa 2: Desarrollo de la Política de Seguridad de la Información
- Etapa 3: Difusión de la Política de Seguridad de la Información

La primera etapa de *identificación y análisis de riesgos*, se divide en 6 pasos:

- Análisis de la organización
- Estructuración del equipo de trabajo
- Capacitación del equipo de trabajo
- Identificación y valoración de activos de información
- Identificación de los riesgos
- Análisis de los riesgos.

En cada uno de los procesos indicados se describen las herramientas o instrumentos que ayudan a conseguir los resultados que sirven como insumo o entrada al siguiente paso o proceso.

Entre estas herramientas utilizadas se encuentran el organigrama de la empresa, su cadena de valor y su modelo de procesos con Notación BPMN para tener claro la estructura de la empresa así

como su entorno interno y externo en el paso de *análisis de la organización*. Además, para evaluar de manera preliminar el estado de seguridad informática que tiene una empresa, se utiliza como herramienta un "cuestionario de evaluación del estado actual de seguridad informática".

En el paso de *estructuración del equipo de trabajo* se estructuraron los roles que debe tener la organización para gestionar correctamente los proyectos de seguridad informática como el tratado en este trabajo; donde se sugiere la conformación de 4 equipos de trabajo con sus respectivas responsabilidades o roles respecto a la seguridad de la información con el personal interno que labora en la empresa. Estos roles son los siguientes:

- Equipo de gestión de seguridad de la información
- Auditoría interna
- Comité Directivo
- Administradores de Seguridad

En el paso de *capacitación del equipo de trabajo*, se indica que los miembros del equipo de gestión de seguridad deben ser entrenados y capacitados antes de la aplicación de la metodología con una guía de entrenamiento, evitando de esta manera una amenaza a la validez de la aplicación de la metodología, considerando que el personal del equipo de trabajo muchas veces es heterogéneo y pertenece a distintas áreas de la empresa, se podría aplicar equivocadamente la metodología si no se capacita previamente a los integrantes del equipo.

En el paso de *identificación y valoración de activos de información* se explica la codificación y clasificación de los activos agrupándolos de acuerdo a su tipo y colocándolos en un formato con el debido proceso para identificar y valorar los activos de información, considerando las 3 dimensiones básicas de la seguridad de la información en las que pueden ser afectados: la confidencialidad, disponibilidad e integridad.

En el paso de *identificación de los riesgos* se explica la respectiva clasificación de riesgos y su codificación; además de un cuestionario para identificar los riesgos en una organización mediante unas consultas iniciales para la identificación de riesgos. Se utiliza finalmente una herramienta para documentar los riesgos formalmente: la matriz de identificación de riesgos.

En el paso de *análisis de los riesgos*, se analiza cada riesgo mediante una matriz de valoración de riesgos (University of Adelaide, 2015), y se ubica a cada riesgo de manera cualitativa en dicha matriz según su probabilidad de ocurrencia y sus consecuencias de impacto. Al finalizar este paso se sugiere una matriz para la identificación y valoración de los riesgos encontrados en la organización, indicando en dicha matriz los riesgos identificados con los campos definidos en la identificación de riesgos del paso anterior, junto con otra columna donde se indican las iniciales de las dimensiones de seguridad

afectadas ([C]onfidencialidad, [I]ntegridad y [D]isponibilidad) si se llega a materializar el riesgo, y una columna adicional indicando el color y codificación de la valoración del riesgo, resultado del análisis cualitativo de riesgos descrito según la probabilidad y consecuencias del riesgo.

La segunda etapa de la metodología propuesta, que es *el desarrollo de la política de seguridad de la información*, se compone de 2 pasos:

- Selección de controles
- Elaboración del documento formal

El paso de la *selección de controles* en el procedimiento indicado en la metodología, consiste en seleccionar los controles más adecuados del estándar ISO 27002 (2013) para los riesgos identificados en la etapa anterior según los criterios de la descripción del riesgo, los activos involucrados para que el riesgo se materialice, los activos afectados si el riesgo se llega a dar y la ubicación donde el riesgo pudiese suceder. Los controles seleccionados se ubican en la "Matriz de selección de controles ISO 27002 para los riesgos de seguridad identificados"

En el paso de *elaboración del documento formal* se depuran los controles seleccionados duplicados mediante una "matriz depurada de controles ISO 27002" y se elabora en base a los controles identificados la política de seguridad de la información donde se plasman los controles identificados detallándolos en un documento en forma de políticas de seguridad, con las recomendaciones o directrices dadas por la norma ISO 27002 (2013) para la elaboración de políticas de seguridad de la información, en el formato planteado en este paso, siendo este el entregable final de la metodología.

La última etapa se conoce como la *difusión de la política de seguridad de la información.* La aplicación de esta etapa de la metodología consiste en recomendar los medios para dar a conocer en la empresa las políticas de seguridad de la información desde un punto de vista sencillo, práctico y amistoso, tratando de llegar al usuario de una manera amigable para motivarlo a que se capacite, cumpla y promueva el uso de las Políticas de Seguridad de la Información en todo momento tanto dentro como fuera de la organización.

De esta manera, en este capítulo se ha logrado el planteamiento de un método apropiado, que consiste de 3 etapas y un total de 9 pasos propuestos para la identificación, análisis y evaluación de riesgos y la elaboración formal de las políticas de seguridad de la información que los mitiguen. El método está diseñado para ser aplicado en empresas industriales de alimentos, pero no se descarta que pueda ser aplicado también en otro tipo de empresas, con su respectiva validación.

Capítulo 5. Aplicación de la Metodología

La metodología planteada en el presente trabajo de titulación se evalúa en este capítulo mediante su aplicación en el departamento de producción de una empresa industrial de alimentos de la ciudad de Cuenca - Ecuador con la ayuda de su personal de Tecnologías de la Información (TI) y del departamento de Auditoría Interna de la empresa, conformando así el "*Equipo de Gestión de Seguridad de la Información*" sugerido en la estructuración del equipo de trabajo en la metodología propuesta; los colaboradores de este equipo fueron los encargados de identificar los activos de información e identificar y evaluar los riesgos obtenidos en el departamento de producción y como solución para mitigarlos, desarrollaron una política de seguridad de la información con los controles que consideraron más adecuados del estándar ISO 27002 (ISO 27002, 2013), según lo indicado en la metodología, y los plantearon como políticas de seguridad de la información en un documento formal para el departamento de producción de la empresa, diseñando también un plan para su difusión e implementación. A continuación se detalla la aplicación y resultados de las 3 etapas y los 9 pasos de la metodología propuesta en el capítulo 4.

5.1. Etapa 1: Identificación y Análisis de Riesgos

Como se vio en la descripción de la metodología planteada en el capítulo anterior, es necesario realizar la identificación y el análisis de los riesgos existentes en la empresa, para así poder determinar qué políticas deben ser planteadas para salvaguardar a la compañía de ataques o vulnerabilidades existentes. Esta es la etapa inicial de la metodología propuesta para la elaboración de políticas de seguridad en el presente trabajo, cuya finalidad es identificar y analizar los riesgos en una determinada área de la empresa. Esta actividad se compone de 6 tareas o pasos consecutivos, los cuales son: análisis de la organización, estructuración del equipo de trabajo, capacitación del equipo de trabajo, identificación y valoración de activos de información, identificación de riesgos y el análisis de riesgos. En cada uno de estos pasos se detalla a continuación los detalles y resultados de su implementación.

5.1.1. Paso 1: Análisis de la Organización

La organización en la que se aplicó la metodología se dedica a la producción, comercialización y distribución de cárnicos y embutidos en el Ecuador. Se trata de una empresa industrial privada de tipo PYME (Pequeñas y Medianas Empresas) con un total de 350 empleados distribuidos entre su matriz y planta de producción en la ciudad de Cuenca, una granja de materia prima (cerdos y reses) en las afueras de la ciudad y dos centros de distribución en las ciudades de Quito y Guayaquil.

La empresa tiene como cultura organizacional su misión y visión siempre orientadas hacia el cliente con integridad, responsabilidad, solidaridad e innovación como valores de sus colaboradores.

En su plan estratégico consta dentro de la perspectiva de “Procesos Internos” el objetivo estratégico de “Implementar seguridad en los sistemas informáticos y en la información de la empresa”, por lo que uno de los proyectos estratégicos para la empresa dentro de este objetivo es el desarrollo y planteamiento de políticas de seguridad de la información en sus distintos departamentos, ya que actualmente no tiene una política de seguridad formalizada, razón por la que este trabajo tiene una gran importancia para la empresa, como metodología modelo y aplicación en su departamento de producción.

Una vez conocidos el tipo, tamaño y contexto de la empresa, siguiendo la metodología propuesta, se analiza su organización y los procesos que se manejan internamente, para lo cual se utilizan las siguientes herramientas:

a) Organigrama de la Empresa

Como se puede observar en la Figura 5.1, el organigrama de la empresa tiene una organización vertical, dando una representación gráfica de la estructura general de la empresa, donde se puede indicar que es una estructura típica de una empresa de producción y comercialización de alimentos; con gerencias de producción, investigación y desarrollo, comercial, financiera y de granjas (materia Prima) directamente debajo de la gerencia general. Además se tienen jefaturas y departamentos de apoyo como el de aseguramiento de calidad, compras, logística, gestión humana, mantenimiento y Tecnologías de la Información (TI).

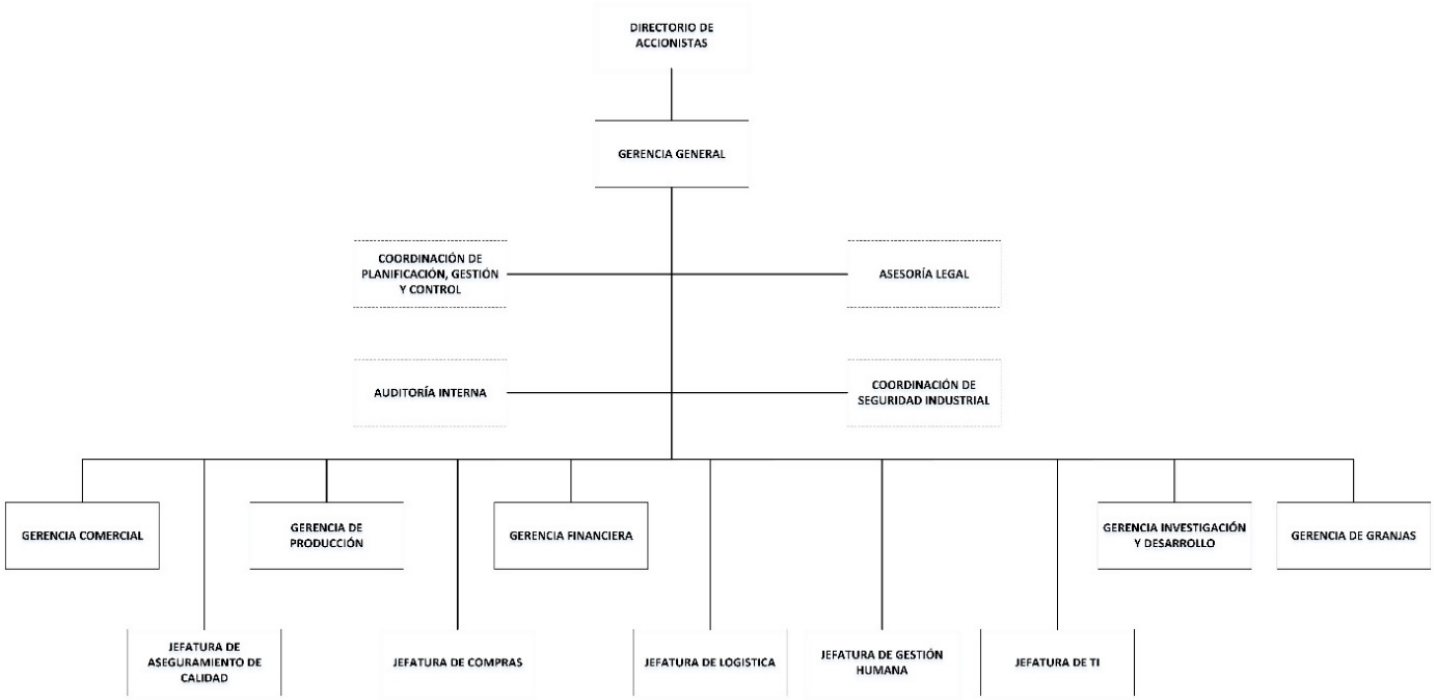

Figura 5.1. *Organigrama de la Empresa.*

b) Cadena de Valor

Con esta herramienta, como se ilustra en la Figura 5.2, se pueden examinar las principales actividades que se ejecutan en la empresa y cómo interactúan entre ellas; además, según Olmedo *et al.* (2016), se analiza a la empresa en sus actividades estratégicas y de apoyo relevantes para comprender mejor su comportamiento.

La cadena de valor de la empresa en la que se aplica la metodología (Figura 5.2), tiene una organización típica de una empresa industrial de manufactura, donde se da mucha importancia a sus áreas estratégicas principales como son: producción (operaciones), comercialización (marketing y ventas) y la logística interna y externa para el aprovisionamiento. Estas áreas se apoyan en otras que son de soporte como la gerencia financiera, contabilidad, auditoría interna, recursos humanos, investigación y desarrollo, tecnologías de la información (TI), compras, seguridad industrial, recursos humanos, aseguramiento de la calidad, entre otras que desempeñan actividades de soporte o apoyo para las áreas estratégicas.

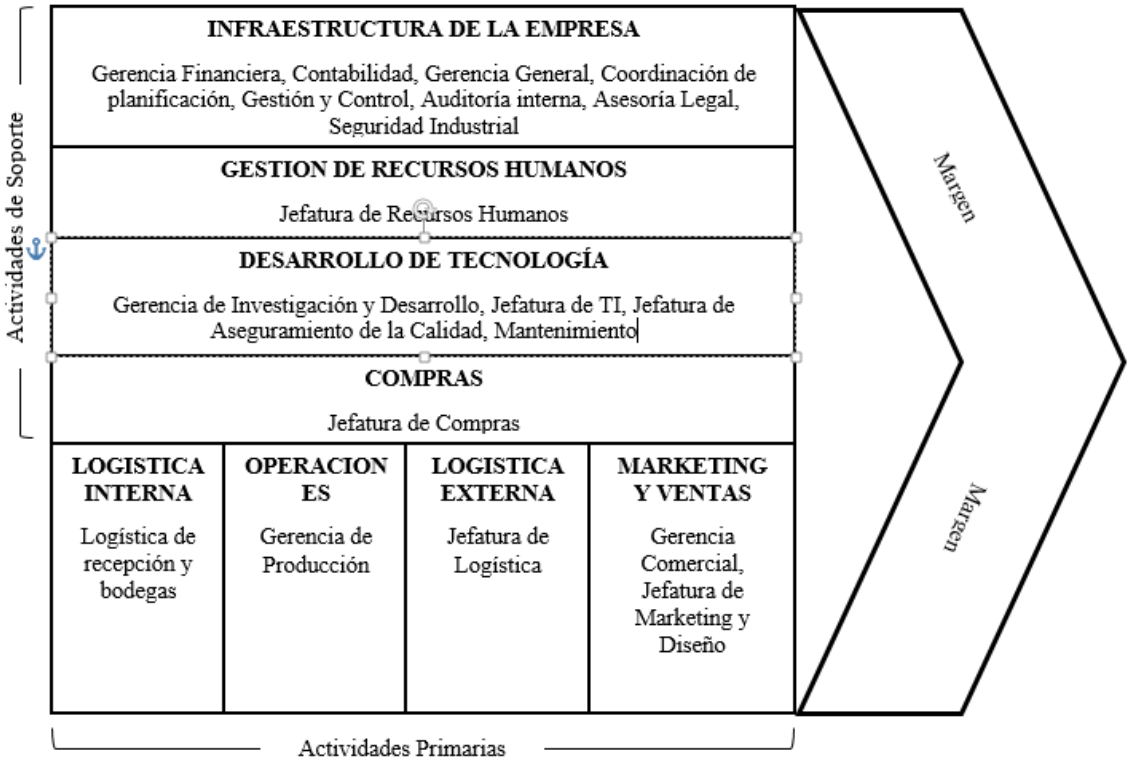

Figura 5.2. *Cadena de Valor de la Empresa.*

c) Modelo de Procesos de la Empresa con Notación BPMN

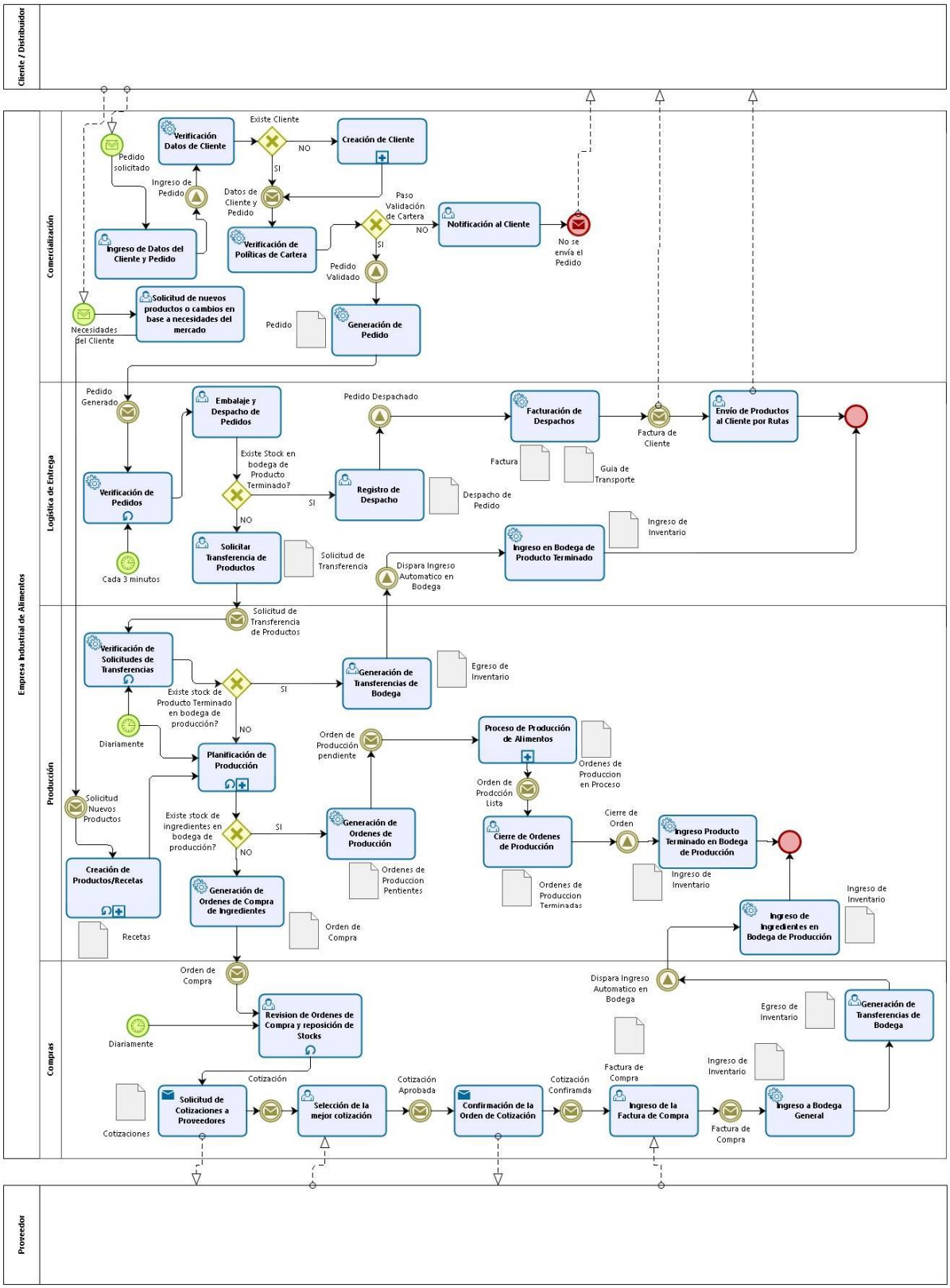

Figura 5.3. *Modelado de Procesos de la Empresa con Notación BPMN.*

Se ha utilizado *Business Process Model and Notation* o BPMN (http://www.bpmn.org/) que constituye un lenguaje de dominio específico (DSL – Domain Specific Language) para la representación de procesos de negocios y se ha aplicado en la Figura 5.3, para determinar los procesos de negocio de la empresa analizada, en donde se determinan los actores externos "Clientes", quienes son los que disparan la necesidad y los procesos comerciales de la empresa para comenzar a trabajar, generando solicitudes de abastecimiento en el área de logística, la misma que a su vez comunica sus necesidades de abastecimiento al área de producción en donde se planifica la fabricación y el aprovisionamiento de los ingredientes o materiales según las fórmulas o recetas preestablecidas para fabricar un producto.

Con el análisis del modelo de procesos de la empresa con notación BMPN (Figura 5.3), se determina también que el área de compras y abastecimiento tiene la función principal de aprovisionar al área de producción de los ingredientes necesarios para la fabricación de productos y para realizar dicha función tiene constante contacto con los otros actores externos que son los "Proveedores"; formándose así una cadena de valor en donde todas las áreas y sus procesos deben estar sincronizados en constante comunicación para no tener retrasos o problemas en la logística de entrega, cumpliendo oportunamente con los pedidos a los clientes entregándoles los productos con el servicio y calidad deseados.

d) Cuestionario de Evaluación del Estado Actual de Seguridad Informática en la Empresa

El cuestionario que se aplicó según la sugerencia de la metodología planteada, se basa en el estándar ISO 27001 (ISO 27001, 2013) y en las recomendaciones de Crespo (2016), siendo su finalidad que el equipo de trabajo tenga una idea clara del estado actual de seguridad informática en el que se encuentra el entorno de la empresa con la que se va a trabajar. El cuestionario fue aplicado al Supervisor de Infraestructura de TI de la empresa, que por su experiencia en la misma y sus conocimientos técnicos fue el más indicado para responder a este cuestionario. El cuestionario se elaboró con 71 preguntas cerradas sobre algunos temas de seguridad de la información; esto para que el encuestado no tenga oportunidad de dar respuestas ambiguas, irrelevantes o extensas, ya que el objetivo principal de esta herramienta es conocer de una manera ágil el estado de seguridad informática en que se encuentra la empresa en la actualidad. Se presenta en la Tabla 5.1 un resumen de las respuestas de este cuestionario resumido por el tema o asunto de las preguntas que se realizaron, el cuestionario completo y sus respuestas se muestra detallado en la Tabla 2.1 del Anexo 2.

Con los resultados de la tabla 5.1, los mismos que se reflejan en la gráfica de la Figura 5.4, se puede concluir que la empresa con la que se trabajó tiene actualmente un nivel medio de seguridad de la información con un 58% de respuestas afirmativas sobre seguridad informática, y que si bien tienen algunos controles y disposiciones en cuanto a los temas encuestados, existen también varias deficiencias en cada asunto consultado; sin embargo el problema más urgente y necesario para la empresa es de que

no poseen ninguna política de seguridad informática documentada formalmente, pues se indicó, según el Supervisor de infraestructura de TI, que se dan charlas de concientización en seguridad informática al personal, que se tienen equipos de protección de la seguridad perimetral y software antivirus en todos los equipos para la seguridad interna, que se tienen controles de acceso a los equipos sensibles como servidores en la empresa, pero no se tienen documentados los controles y políticas de seguridad necesarios para formalizar estos temas a los empleados, sino que muchas veces se indica y se capacita a los usuarios sobre los temas de seguridad informática de manera empírica, sin tener por escrito ningún documento formal que sustente esto.

ASUNTO	RESPUESTAS	
	SI (Nro.)	NO (Nro.)
Políticas de Seguridad de la Información	0	3
Seguridad Organizacional	3	4
Clasificación y control de activos	2	2
Seguridad y personal	3	2
Seguridad física y ambiental	12	2
Gestión de la operación y las comunicaciones	7	6
Control de acceso	9	3
Desarrollo y mantenimiento de sistemas	2	2
Gestión de la continuidad del negocio	0	2
Cumplimiento con el marco jurídico	3	4
TOTAL	**41 (58%)**	**30 (42%)**

Tabla 5.1. *Resultados del Cuestionario de Evaluación del Estado Actual de la Seguridad Informática en la Empresa.*

Otro tema preocupante que se deduce del cuestionario aplicado, es de que no se tiene un plan de contingencia o plan de continuidad de negocio para los equipos más críticos que prestan sus servicios a la organización; situación que es confirmada por el Supervisor de infraestructura de TI, ya que por cuestiones económicas indica que los proyectos de continuidad del negocio y contingencia se no se los ha podido implementar hasta el momento, sin embargo se indica que los tienen como proyectos urgentes dentro del Plan Estratégico de la empresa para implementarlos en los primeros meses del nuevo año.

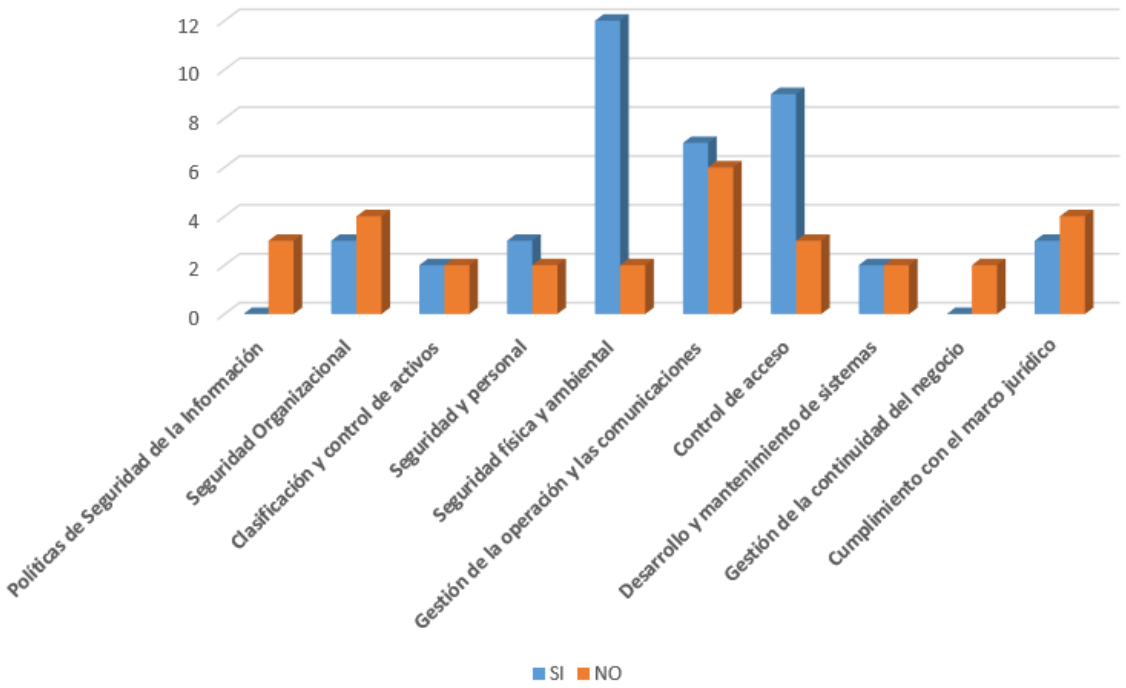

Figura 5.4. *Gráfica Comparativa de Resultados del Cuestionario de Evaluación del Estado Actual de la Seguridad Informática en la Empresa.*

Con los resultados indicados se culmina este punto de la aplicación de la metodología, donde se tuvo una idea clara a cerca del contexto de la empresa, las actividades a las que se dedica y su organización interna con sus áreas estratégicas y de apoyo, conociendo también los procesos más importantes de su operación y además, su estado actual referente a la seguridad de la información; cumpliendo así la finalidad de este paso de la etapa, dando al equipo de trabajo suficiente información acerca de la empresa para seguir desarrollando los siguientes pasos de la metodología planteada.

5.1.2. Paso 2: Estructuración del Equipo de Trabajo

La aplicación de la metodología planteada fue realizada conformando un equipo de trabajo con seis empleados internos de la empresa para identificar y analizar los riesgos para el departamento de producción y realizar en base a ellos el desarrollo y planteamiento de las políticas de seguridad de la información más adecuadas para el departamento de producción de la empresa. Siguiendo las recomendaciones de la metodología con la estructuración y roles del equipo de trabajo indicados en la Tabla 4.1, cinco de los empleados escogidos pertenecen al departamento de TI de la empresa y son dos analistas/desarrolladores, un supervisor de infraestructura, un asistente de soporte y el jefe del departamento de TI quienes son los que más experiencia tienen en el área de TI en la empresa y conocen sus procesos, riesgos y medidas de seguridad existentes. El otro integrante del equipo es el auditor interno de la empresa quien es el encargado de evaluar cada cierto tiempo los procesos y controles de la organización y encontrar deficiencias en sus procesos y políticas; se lo consideró dentro del equipo

de trabajo para que se involucre desde el desarrollo de la política de seguridad de la información y así tenga los conocimientos y argumentos suficientes para posteriormente realizar correctamente la tarea de monitoreo y auditoría de los controles de la política de seguridad.

Todos estos colaboradores son los que conformaron el rol de *"Equipo de Gestión de Seguridad de la Información"*, siendo un equipo de trabajo integrado por profesionales de dos áreas de la empresa sin relación directa con el departamento de producción, que es donde se aplicó la metodología para que exista imparcialidad en los resultados. Este equipo tuvo la responsabilidad del desarrollo y planteamiento de las Políticas de Seguridad de la Información y también la responsabilidad de comunicación directa de los resultados del proyecto para su aprobación con los miembros del "*Comité Directivo"*, que se conforma por los directivos de la empresa o sus delegados y el gerente general. Este grupo directivo tuvo la responsabilidad de colaborar con la información en esta etapa de análisis de la organización, aprobar la conformación del Equipo de Gestión de Seguridad de la Información y de aprobar la política de seguridad planteada en un documento entregable formal.

El auditor interno de la empresa junto con un asistente de su departamento cumplieron con el rol de *"Auditoría Interna"*, que según los roles recomendados en la metodología (Tabla 4.1), su responsabilidad principal es el control de la aplicación de la metodología y su cumplimiento. Una vez implementada la política de seguridad de la información para el departamento de producción de la empresa, también deberán monitorear el cumplimiento de dicha política de seguridad con la aplicación de los controles recomendados e informar al Comité Directivo sobre la correcta aplicación o incumplimiento de la política de seguridad.

Finalmente se tuvo la conformación del grupo que cumple con el rol de "*Administradores de Seguridad*" que se integra por los jefes, administradores o responsables de cada departamento, área o unidad de negocio de la empresa en donde se aplique la metodología y que son los encargados de mantener y vigilar por el cumplimiento de las políticas de seguridad informática recomendadas en sus respectivas áreas para proteger la información de la empresa, teniendo también la responsabilidad de comunicar y recordar a su personal las instrucciones, recomendaciones y políticas dadas por el Equipo de Gestión de Seguridad de la Información y aprobadas por el Comité Directivo. A este grupo de "*Administradores de Seguridad*" se los tendrá que capacitar y dar a conocer la política de seguridad de la información inclusive antes que el personal que está bajo su mando; para que tengan un conocimiento claro de los riesgos y las políticas de seguridad para que sean conscientes de los mismos, de su importancia para la continuidad de las operaciones de la empresa y a su vez lo puedan transmitir a su equipo de trabajo. Este rol en la empresa lo conformaron el Gerente del departamento de producción, sus 3 supervisores principales de planta (planta de carnes, planta de producción, y planta de empacado) y el jefe del área de Investigación y desarrollo; que es un área crítica o sensible del departamento de producción.

Los roles o grupos de trabajo indicados y sus integrantes se resumen en la Tabla 5.2, donde se puede verificar que existen en total 6 integrantes del grupo que cumplen el rol de *Equipo de Gestión de Seguridad de la Información*, 2 integrantes del grupo que tiene el rol de *Auditoría Interna*, 5 miembros del grupo que cumple el rol del *Comité Directivo* y 5 integrantes del grupo con el rol de *Administradores de Seguridad*; dando un total de 18 Integrantes de los Grupos o Roles de Seguridad de la Información y también como un dato importante se indica que existen un total de 105 empleados que trabajan directamente para la empresa en el departamento de Producción y que tienen acceso a una o varias de sus áreas internas.

ROL (GRUPO DE TRABAJO)	**INTEGRANTES**
Equipo de Gestión de Seguridad de la Información	- 5 colaboradores del departamento de TI de la empresa - 1 auditor interno de la empresa
Auditoría Interna	- 1 auditor interno de la empresa - 1 asistente de auditoría
Comité Directivo	- 1 Presidente - 3 Accionistas - 1 Gerente
Administradores de Seguridad	- 1 Gerente de Producción - 3 Supervisores Principales de Planta - 1 Jefe del área de Investigación y Desarrollo
TOTAL	- 18 Integrantes de los Grupos o Roles de Seguridad de la Información - 105 usuarios que trabajan en el departamento de Producción y que tienen acceso a sus áreas.

Tabla 5.2. *Estructuración del Equipo de Trabajo en la empresa analizada.*

5.1.3. Paso 3: Capacitación del Equipo de Trabajo

El equipo de trabajo fue entrenado y capacitado tres días antes de la aplicación de la metodología con una guía de entrenamiento, como se sugiere en este paso; evitando de esta manera una amenaza a la validez de la aplicación de la metodología, considerando que el personal del equipo de trabajo es

heterogéneo y pertenece a distintas áreas de la empresa, esta amenaza pudiese sesgar los resultados o aplicar equivocadamente la metodología si no se capacita previamente al equipo de trabajo, pues así se indica en el punto 4.1.3 del Capítulo 4, que explica en detalle este paso de la metodología donde no siempre los integrantes del equipo de trabajo son expertos del área de TI que entienden claramente los conceptos de seguridad informática, gestión de riesgos y políticas de seguridad; por lo que se debe capacitar al equipo de trabajo que se conformó en el paso anterior antes de seguir con la aplicación de la metodología.

Así se tuvo que realizar la capacitación utilizando una presentación detallada con todos los conceptos y puntos vistos en el Capítulo 3 (Marco Teórico) y Capítulo 4 (Metodología Propuesta) del presente trabajo de titulación, durando la capacitación y socialización de la metodología un tiempo total de 3 horas en un día laborable; dicha presentación se entregó también al Comité Directivo de la empresa y se la archivó en los documentos de capacitación internos del departamento de Recursos Humanos para que pueda ser revisada o consultada en un futuro. En la Figura 2.1 del Anexo 2 se muestra el formato interno que tiene la empresa para el "Registro de Capacitaciones", siendo esta última la herramienta o artefacto final de este punto de la metodología que deja constancia de la capacitación al equipo de trabajo para la comprensión clara de los pasos a desarrollarse a continuación.

5.1.4. Paso 4: Identificación y Valoración de Activos de Información

En este paso de la metodología, se aplicó lo indicado dentro del Capítulo 4 en el punto 4.1.4 para la "*Identificación y valoración de activos de la información*", donde en base a la clasificación indicada en la Tabla 4.2 de *Codificación de Grupos de Activos de Información* y a las Tablas 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9 y 4.10 donde se indica la *Clasificación y Codificación estandarizada para los distintos tipos de activos de la información*; se aplicó, siguiendo el criterio de *Codificación de Activos* mostrado en la Figura 4.3, la codificación de los activos existentes en el departamento de producción de la empresa. Además para la *Valoración de los activos*, el proceso se basó en las dimensiones de seguridad de la información: Confidencialidad (C), Disponibilidad (D) e Integridad (I) y en la Tabla 4.11, donde se muestran las escalas de los criterios de valoración de riesgos a utilizarse.

Se plasmaron los resultados de este paso de la metodología siguiendo el *Formato para la identificación y valoración de activos* (Tabla 4.12) con un rango de valoración de 0-10. Los activos del departamento de producción identificados y detallados con el formato indicado como entregable de este paso, se muestran en la Tabla 2.2 del Anexo 2.

Finalmente, para concluir la aplicación de este paso de la metodología que es la identificación y valoración de activos, se muestran los resultados resumidos por tipo de activos en la tabla 5.3 y a continuación se los analiza.

En los resultados mostrados en la Tabla 5.3, se concluye que de un total de 201 activos identificados, la mayoría, un 59.20%, tienen un valor calificado como *Alto* respecto a las dimensiones de seguridad; un 31.84% tienen un valor *Medio*, un 6.47% tiene un valor *Muy Alto* y un 2.49 tienen un valor *Extremo*; además, ningún activo tuvo una valoración de *Bajo* o *Despreciable*. Esto se debe a que la mayoría de tipos de activos como edificaciones, hardware, software, información electrónica, información en papel, e infraestructura de comunicaciones tienen un nivel crítico respecto a su confidencialidad, integridad y disponibilidad ya que en esta área los activos de información contienen o gestionan información crítica ya sea electrónica o en papel como las órdenes de producción, formulas o recetas de los productos que fabrica la empresa, datos de operación de la maquinaria, procesos y normas de calidad electrónicos o impresos, la documentación de los procesos de elaboración de productos y sus recursos, el software que controla estos procesos y sus respectivas bases de datos, etc.

			NRO. DE ACTIVOS POR NIVEL DE VALORACIÓN					
COD.	TIPO DE ACTIVO	NRO. ACTIVOS IDENTIFICADOS	EXTREMO	MUY ALTO	ALTO	MEDIO	BAJO	DESPRECIABLE
ED	Edificaciones	12	1	1	9	1	0	0
HW	Hardware	73	0	3	24	46	0	0
SW	Software	28	1	4	13	10	0	0
IE	Información electrónica	32	2	2	24	4	0	0
IP	Información en papel	25	0	0	22	3	0	0
EX	Medios de almacenamiento extraible	1	0	0	1	0	0	0
IC	Infraestructura de comunicaciones	9	0	1	8	0	0	0
RH	Recursos Humanos	21	1	2	18	0	0	0
TOTAL DE ACTIVOS		**201**	**5**	**13**	**119**	**64**	**0**	**0**
%		**100**	**2.49**	**6.47**	**59.20**	**31.84**	**0.00**	**0.00**

Tabla 5.3. *Resumen de Valoración de Activos por Niveles.*

También se considera dentro de las tres categorías más críticas (extremos, muy altos y altos) el 100% del total de los activos identificados como recursos humanos; pues dentro de los recursos humanos están el gerente de producción, el personal de investigación y desarrollo que conocen las recetas y procesos, el personal de planificación de producción, asistentes y los supervisores de las áreas de producción que manejan la información de producción y sus rendimientos; además están todo el

personal de planta que si bien no tienen acceso directamente a las recetas o procesos documentados en papel o electrónicamente, pueden llegar a conocer la información de procesos, recursos y recetas debido a la naturaleza de la operación que realizan y pueden ser un foco de fuga de información de la empresa. Ningún activo se considera con una valoración baja o despreciable, pues pertenecen a esta área crítica y clave como lo es el área de producción en una empresa industrial de alimentos.

5.1.5. Paso 5: Identificación de Riesgos

Este paso es necesario para identificar los riesgos que podrían afectar a los activos de información, en cualquiera de sus dimensiones de seguridad: disponibilidad, integridad o confidencialidad según la metodología propuesta, se realizó la codificación y clasificación de las posibles amenazas o riesgos (las más frecuentes y conocidas) que pudiesen, bajo las condiciones actuales, afectar a los activos de información en el departamento de producción de la empresa y se los clasificó en los 5 grupos que sugiere Crespo (2016): riesgos naturales, riesgos de comunicaciones, riesgos provocados (intencionados), riesgos provocados (no intencionados) y riesgos lógicos.

Se identificaron un total de 30 riesgos divididos en 7 riesgos de tipo provocados (no intencionados), 11 riesgos provocados (intencionados), 3 riesgos de comunicaciones, 6 riesgos lógicos y 3 riesgos naturales. Se concluye entonces que la gran mayoría (un 36.67%) son riesgos provocados por descuido o premeditadamente por el personal; un 23.33% son riesgos que pueden ser causados por el personal pero de manera no intencional; un 10% son riesgos de comunicaciones, un 20% son riesgos lógicos por vulnerabilidades en el software o información electrónica del departamento y un 10% son riesgos naturales que han sido encontrados y analizados por el *Equipo de Gestión de Seguridad de la Información*; los cuales se podrían dar en el medio donde se encuentra la planta de producción de la empresa. Todo esto se lo puede revisar y analizar en la Tabla 2.3 del Anexo 2; donde se detalla la *Matriz de Identificación y Valoración de Riesgos* para el área de producción de la empresa, en el formato indicado en el Capítulo 4, en el punto 4.1.5.

Se debe indicar que en la mayoría de riesgos identificados en esta etapa, dentro de los *Activos Involucrados* que son los activos que generan o sirven de medio para que el riesgo se lleve a cabo, está el recurso humano; lo cual nos indica claramente que una de las principales áreas en las que hay que trabajar es en la selección, contratación, capacitación y concientización de los empleados como los principales actores de la seguridad de la información dentro del departamento de producción de la empresa; pues en ellos se originan los riesgos o hacen que los riesgos se materialicen al no tener buenas prácticas de seguridad y controles, además, varios empleados no tienen firmados contratos de confidencialidad sobre la información crítica del departamento, cuando se pudo constatar que sí tienen acceso a parte de ella. Así también entre los riesgos más importantes están los que se originan al no tener controles sobre el acceso a esta área crítica de la empresa, por ejemplo se constató que los

empleados pueden ingresar al área de producción con dispositivos móviles que son de uso personal y no pertenecen a la empresa, ocasionando esto un riesgo potencial de infección con malware en los equipos del departamento o facilitando la fuga de información.

5.1.6. Paso 6: Análisis de Riesgos

En la Tabla 2.3 del Anexo 2 "*Matriz Identificación y Valoración de Riesgos en el área de Producción de la Empresa*", se puede observar el resultado del análisis de riesgos, donde se analizan los riesgos encontrados en el paso anterior mediante la valoración de la probabilidad de que ocurra un riesgo y su consecuencia o impacto, donde se plantean 5 niveles de probabilidad de ocurrencia de riesgos: *rara, poco probable, posible, probable, casi segura*; clasificando también las consecuencias o impacto de la materialización de un evento o riesgo como *insignificante, menor, moderada, grave o extrema*. Siguiendo la metodología propuesta en este paso, cada riesgo se analizó mediante una matriz de valoración de riesgos (ver Tabla 4.16), donde se ubica al riesgo de manera cualitativa en dicha matriz según su probabilidad de ocurrencia y sus consecuencias o impacto y se obtiene así su valoración. En la matriz resultante también se muestra otra columna donde se indican las dimensiones de seguridad afectadas si se materializara el riesgo ([C]onfidencialidad, [I]ntegridad y [D]isponibilidad), y una columna adicional indicando el color y codificación de la valoración del riesgo, resultado de este análisis cualitativo.

De los riesgos identificados que se resumen en la Tabla 5.4, siendo un total de 30 riesgos, se concluye que 18 riesgos que representan un 60% fueron analizados y valorados con un nivel alto teniendo en cuenta su probabilidad de ocurrencia y sus consecuencias; pues la mayoría de riesgos provocados sin intencionalidad o deliberadamente, los riesgos naturales y los riesgos lógicos se definieron con este nivel ya que si bien algunos de ellos afectan sobre todo la disponibilidad e integridad de la información, se tienen algunas medidas de seguridad como respaldos diarios de la información y una cierta contingencia a nivel de equipos de usuario, que hacen que la información no se pierda totalmente, sin embargo afectan críticamente a la continuidad de los procesos y disponibilidad de la información en el área de producción de la empresa; considerando que no existe en la misma un Plan de Continuidad de Negocios (BCP) o Plan de Contingencia definidos para los servicios informáticos.

Además, 7 riesgos (23.33%) fueron calificados como extremos, partiendo de que la mayoría de ellos afectan a las 1 o varias dimensiones de seguridad y además tienen consecuencias "*graves*" o "*extremas*" con una probabilidad "*probable*" o "*casi segura*", por lo que estos riesgos necesitarían medidas y acciones de gestión urgentes si no las hubiera en la empresa. Dentro de estos riesgos se encuentran 1 riesgo de comunicaciones, 4 riesgos provocados intencionados, 1 riesgo provocado No intencionado y 1 riesgo lógico. La mayoría son riesgos provocados intencionados, teniendo en cuenta la importancia de la concientización que se debe trabajar en el tema de seguridad de la información y

socialización de las políticas de seguridad sobre el Recurso Humano de la empresa.

El restante 16.67%, es decir 5 riesgos fueron catalogados de nivel medio y específicamente caen en esta categoría al menos 1 riesgo de todos los tipos, excepto los riesgos lógicos. Son riesgos de nivel medio por su nivel de probabilidad de ocurrencia y sus consecuencias, que afectan algunas de las dimensiones de seguridad de la información, ocasionando que ciertos procesos se detengan por un período de tiempo de algunas horas en la producción de la empresa hasta solucionar el problema; sin embargo se tienen ciertos procesos o equipos de contingencia para solventar estos riesgos.

Ningún riesgo fue valorado como bajo, pues todos tienen una probabilidad de ocurrencia y un nivel de consecuencias que afectan a una o varias de las dimensiones de seguridad (Disponibilidad, Integridad o Confidencialidad) de los activos de información en el departamento de producción que los hacen tener una valoración media, alta o extrema.

CODIGO	TIPO DE RIESGO	NRO. DE RIESGOS IDENTIFICADOS	NRO. DE RIESGOS CON ESCALAS DE VALORACIÓN			
			EXTREMO	ALTO	MEDIO	BAJO
RN	Riesgos Naturales	3		2	1	
RC	Riesgos de Comunicaciones	3	1	1	1	
PR	Riesgos Provocados (Intencionados)	11	4	5	2	
NI	Riesgos Provocados (No Intencionados)	7	1	5	1	
RL	Riesgos Lógicos	6	1	5		
	TOTAL RIESGOS	**30**	**7**	**18**	**5**	**0**
	%	**100**	**23.33**	**60.00**	**16.67**	**0.00**

Tabla 5.4. *Resumen de la Matriz de Identificación y Valoración de Riesgos en el Área de Producción.*

5.2. Etapa 2: Desarrollo de la Política de Seguridad de la Información

La segunda etapa de la metodología propuesta, es *el desarrollo de la política de seguridad de la información*, y se compone de 2 pasos:

- Selección de controles
- Elaboración del documento formal

A continuación se analiza la implementación y resultados de cada uno de estos pasos para obtener el entregable final de la metodología, que es el documento formal de políticas de seguridad de la información, en base a los controles seleccionados del estándar ISO/IEC 27002 de acuerdo a los riesgos identificados y evaluados en la etapa anterior.

5.2.1. Paso 7: Selección de Controles

Siguiendo con la aplicación de la metodología, en este paso se seleccionan los controles más apropiados de la norma ISO 27002 (2013) para mitigar los riesgos encontrados siguiendo el proceso descrito en el Capítulo 4 en el punto 4.2.1. A continuación en las Tablas desde la 5.5 hasta la 5.34 se muestran los controles más adecuados de la norma ISO 27002 (2013) que se plantearon para mitigar cada riesgo identificado. En esta sección se muestran demasiadas tablas, pero no se tiene suficiente información sobre qué hacer con ellas, pondría una de ejemplo y mencionaría que todas forman parte de un anexo. Es muy dificil leer todas las tablas y no tiene mucho sentido en esta sección poner absolutamente todo, creo que es adecuado incluir un apéndice o anexo con todas las tablas desde la 5.6 hasta la 5.34 y poner claramente para qué sirven y cómo usarlas así como también el significado de cada campo.

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RN.1]	Riesgo por Terremoto	Terremoto, que puede afectar la Disponibilidad de todos los activos de Información de Producción en la empresa.		[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*] [RH.*]	[ED.*]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.1. Áreas seguras		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.1.4. Protección contra las amenazas externas y ambientales.			

Tabla 5.5. *Matriz de Selección de controles ISO 27002 para: Terremoto.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RN.2]	Riesgo por Inundación	Inundaciones que pueden tener las edificaciones de Producción y que afecten a sus activos de información en su Disponibilidad.		[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*]	[ED.*]	[D]	**M**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.1. Áreas seguras		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.1.4. Protección contra las amenazas externas y ambientales.			

Tabla 5.6. *Matriz de Selección de controles ISO 27002 para: Inundación.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RN.3]	Riesgo por Tormenta Eléctrica	Riesgo Natural que tienen las edificaciones de Producción ante una tormenta eléctrica que afecte a sus activos de Información en su Disponibilidad.		[ED.*] [HW.*] [SW.*] [IE.*] [IC.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEN.INV.01] [ED.CDP.01]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.2. Seguridad de los equipos		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.3. Seguridad del cableado.			

Tabla 5.7. *Matriz de Selección de controles ISO 27002 para: Tormenta Eléctrica.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.1]	Incendio	Riesgo que tienen las áreas de producción y activos del Datacenter de sufrir un incendio, afectando a sus activos de información.	[HW.*] [RH.*]	[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*] [RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[ED.*]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.1. Áreas seguras 11.2. Seguridad de los equipos		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.4. Protección contra las amenazas externas y ambientales. 11.2.1. Emplazamiento y protección de equipos.			

Tabla 5.8. *Matriz de Selección de controles ISO 27002 para: Incendio.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.2]	Explosión	Riesgo que tienen las áreas de producción de sufrir una explosión por el equipamiento y materiales que utilizan y el combustible, por ejemplo en hornos, cocinas, calderos, etc.	[RH.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.*] [ED.CPS.*] [ED.INV.01] [HW.*] [IE.*] [IP.*] [IC.*] [RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEN.INV.01]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.1. Áreas seguras 11.2. Seguridad de los equipos		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.4. Protección contra las amenazas externas y ambientales. 11.2.1. Emplazamiento y protección de equipos. 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla.			

Tabla 5.9. *Matriz de Selección de controles ISO 27002 para: Explosión.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.3]	Falla del Generador Eléctrico o UPS	Falla del Generador eléctrico o un UPS ante un Corte del suministro eléctrico.	[ED.*]	[HW.*] [IC.*]	[ED.*]	[D]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental		11.2. Seguridad de los equipos		11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.3. Seguridad del cableado.			

Tabla 5.10. *Matriz de Selección de controles ISO 27002 para: Falla de Generador Eléctrico o UPS.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.4]	Cortocircuito o Descarga Eléctrica	Cortocircuitos o descargas eléctricas internas o externas que afecten a los activos de información.	[ED.*]	[HW.*] [IC.*]	[ED.*]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 11. Seguridad Física y Ambiental		17.1. Continuidad de la seguridad de la información 17.2. Redundancias 11.2. Seguridad de los equipos		17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información. 11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.3. Seguridad del cableado. 11.2.4. Mantenimiento de los equipos.			

Tabla 5.11. *Matriz de Selección de controles ISO 27002 para: Cortocircuito o Descarga Eléctrica.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RC.1]	Temperaturas elevadas en Cuartos de Comunicaciones	Temperaturas elevadas e inadecuadas para los equipos que se ubican en los cuartos de comunicaciones.	[ED.CPS.01] [ED.CPS.02]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental		11.1. Áreas seguras 11.2. Seguridad de los equipos		11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.3. Seguridad del cableado. 11.2.4. Mantenimiento de los equipos.			

Tabla 5.12. *Matriz de Selección de controles ISO 27002 para: Temperaturas elevadas en Cuartos de Comunicaciones.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RC.2]	Daños en los equipos de comunicaciones	Daños en cualquiera de los equipos de comunicaciones afectando su disponibilidad para acceder a los recursos y servicios informáticos.	[IC.*]	[IC.*]	[ED.CPS.01] [ED.CPS.02] [ED.CDP.01]	[D] [I]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental 13. Seguridad en las Telecomunicaciones		11.2. Seguridad de los equipos 13.1. Gestión de la seguridad en las redes		11.2.3. Seguridad del cableado. 11.2.4. Mantenimiento de los equipos. 13.1.1. Controles de red.			

Tabla 5.13. *Matriz de Selección de controles ISO 27002 para: Daños en los Equipos de Comunicaciones.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RC.3]	Daños en el cableado físico de la red	Daño en el cableado físico de la red de cobre, fibra o inalámbrica.	[ED.*]	[IC.*]	[ED.*]	[D] [I]	**M**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental 13. Seguridad en las Telecomunicaciones		11.2. Seguridad de los equipos 13.1. Gestión de la seguridad en las redes		11.2.3. Seguridad del cableado. 13.1.1. Controles de red.			

Tabla 5.14. *Matriz de Selección de controles ISO 27002 para: Daños en el Cableado físico de la Red.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.1]	Desconexión intencional de los equipos de comunicaciones	Desconexión física intencional de cualquiera de los equipos de comunicaciones de la red.	[RH.*]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D] [I]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos 11. Seguridad Física y Ambiental 13. Seguridad en las Telecomunicaciones		9.1. Requisitos de negocio para el control de accesos 11.1. Áreas seguras 13.1. Gestión de la seguridad en las redes		9.1.1. Política de control de accesos. 9.1.2. Control de acceso a las redes y servicios asociados. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 13.1.1. Controles de red.			

Tabla 5.15. *Matriz de Selección de controles ISO 27002 para: Desconexión intencional de los Equipos de Comunicación.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.5]	Degradación de los activos de información en Papel	Degradación de los activos de información que se encuentran almacenados en papel y que contienen información crítica para la empresa.		[IP.*]	[ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**M**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental 18. Cumplimiento		11.2. Seguridad de los equipos 18.1 Cumplimiento de los requisitos legales y contractuales		11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla. 18.1.3. Protección de los registros de la organización.			

Tabla 5.16. *Matriz de Selección de controles ISO 27002 para: Degradación de los activos de Información en Papel.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.2]	Pérdida o robo de los activos de información en Papel	Pérdida o robo de información importante para la organización en papel.	[RH.*]	[IP.*]	[ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [C]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos 11. Seguridad Física y Ambiental 18. Cumplimiento		9.1. Requisitos de negocio para el control de accesos 11.1. Áreas seguras 11.2. Seguridad de los equipos 18.1 Cumplimiento de los requisitos legales y contractuales		9.1.1. Política de control de accesos. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla. 18.1.3. Protección de los registros de la organización.			

Tabla 5.17. *Matriz de Selección de controles ISO 27002 para: Pérdida o robo de los activos de información en Papel.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.6]	Degradación y daños en los equipos informáticos de los usuarios	Degradación o daños en los equipos de usuarios por falta de mantenimiento o daños en sus componentes internos		[HW.LAP.*] [HW.PCS.*] [HW.PLA.*] [HW.IMP.*] HW.BAL.*] [IC.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental		11.2. Seguridad de los equipos		11.2.4. Mantenimiento de los equipos.			

Tabla 5.18. *Matriz de Selección de controles ISO 27002 para: Degradación y Daño en los Equipos Informáticos de los Usuarios.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[NI.7]	Daños en los equipos informáticos industriales de usuarios por polvo, humedad o limpieza del ambiente industrial	Daños en los equipos informáticos industriales de usuarios por polvo, humedad, riego de agua o limpieza del ambiente industrial	[ED.SEN.PLA.*] [RH.*]	[HW.LAP.PLA.*] [HW.BAL.PLA.*] [HW.SNR.TMP.*]	[ED.SEN.PLA.*]	[D]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
11. Seguridad Física y Ambiental		11.2. Seguridad de los equipos		11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.4. Mantenimiento de los equipos.			

Tabla 5.19. *Matriz de Selección de controles ISO 27002 para: Daños en los Equipos Informáticos Industriales ocasionados por el Ambiente Industrial.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.3]	Acceso no autorizado a las instalaciones de producción para el personal de otras áreas	No existe un control adecuado para el personal de otras áreas en el acceso a esta área crítica para la empresa.	[RH.*]	[HW.LAP.*] [HW.PCS.*] [HW.IMP.*] [HW.BAL.*] [HW.SNR.*] [SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*] [IP.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos 11. Seguridad Física y Ambiental		9.1. Requisitos de negocio para el control de accesos 11.1. Áreas seguras 11.2. Seguridad de los equipos		9.1.1 Política de control de accesos. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 11.1.5. El trabajo en áreas seguras. 11.1.6. Áreas de acceso público, carga y descarga 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla.			

Tabla 5.20. *Matriz de Selección de controles ISO 27002 para: Acceso no Autorizado a Instalaciones de Producción para el Personal de otras Áreas*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.4]	Acceso no autorizado a los cuartos de comunicaciones	Acceso no autorizado a los cuartos de comunicaciones y sus equipos informáticos	[RH.*]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D] [I]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos 11. Seguridad Física y Ambiental 13. Seguridad en las Telecomunicaciones		9.1. Requisitos de negocio para el control de accesos 11.1. Áreas seguras 13.1. Gestión de la seguridad en las redes		9.1.1 Política de control de accesos. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 13.1.1. Controles de red. 13.1.2. Mecanismos de seguridad asociados a servicios en red.			

Tabla 5.21. *Matriz de Selección de controles ISO 27002 para: Acceso no Autorizado a los Cuartos de Comunicaciones.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.5]	Robo de equipos	Mediante el robo de equipos se puede afectar la confidencialidad y disponibilidad de la información	[RH.*]	[HW.*] [IC.*]	[ED.*]	[D] [C]	**M**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
8. Gestión de Activos 9. Control de Accesos 11. Seguridad Física y Ambiental		8.1. Responsabilidad sobre los activos 9.1. Requisitos de negocio para el control de accesos 11.1. Áreas seguras 11.2. Seguridad de los equipos		8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos. 9.1.1 Política de control de accesos. 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 11.1.6. Áreas de acceso público, carga y descarga 11.2.1. Emplazamiento y protección de equipos.			

Tabla 5.22. *Matriz de Selección de controles ISO 27002 para: Robo de Equipos*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.1]	Fuga de Información	La información llega al conocimiento o poder de personas que no deben tener acceso a la misma de manera intencionada o no, sin que la información en sí misma se vea alterada.	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [SW.SAT.COR.01] [SW.SAT.GBD.01] [HW.LAP.*] [HW.PCS.*] [HW.CEL.01] [HW.MOV.01] [EX.01] [RH.*]	[IE.*][IP.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[C]	**A**

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
6. Organización de la Seguridad de la Información 7. Seguridad de los Recursos Humanos 8. Gestión de Activos 9. Control de Accesos 10. Cifrado 11. Seguridad Física y Ambiental 13. Seguridad en las Telecomunicaciones	6.2. Dispositivos para movilidad y teletrabajo 7.1. Antes de la contratación 7.2. Durante la contratación 7.3. Cese o cambio de puesto de trabajo 8.3. Manejo de los soportes de Almacenamiento 9.1. Requisitos de negocio para el control de accesos 9.3. Responsabilidades del Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones 10.1. Controles Criptográficos 11.1. Áreas seguras 11.2. Seguridad de los equipos 13.2 Intercambio de información	6.2.1. Política de uso de dispositivos móviles. 7.1.2. Términos y condiciones de la contratación 7.2.2. Concientización, educación y capacitación en seguridad de la información 7.3.1. Cese o Cambio de puesto de Trabajo 8.3.1. Gestión de soportes extraíbles 8.3.2. Eliminación de Soportes 8.3.3. Soportes físicos en Tránsito 9.1.1 Política de control de accesos. 9.3.1. Uso de información confidencial para la autenticación 9.4.1. Restricción del Acceso a la Información 9.4.2. Procedimientos Seguros de inicio de sesión 9.4.3. Gestión de Contraseñas de Usuario 10.1.1. Política de uso de controles criptográficos 11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 11.1.5. El trabajo en áreas seguras. 11.1.6. Áreas de acceso público, carga y descarga 11.2.5. Salida de activos fuera de las dependencias de la empresa. 11.2.6. Seguridad de los quipos y activos fuera de las instalaciones 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento 11.2.8. Equipo informático de usuario desatendido 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla. 13.2.1. Políticas y procedimientos de intercambio de información 13.2.2. Acuerdos de intercambio 13.2.3. Mensajería electrónica 13.2.4. Acuerdos de Confidencialidad y Secreto

Tabla 5.23. *Matriz de Selección de controles ISO 27002 para: Fuga de Información.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.2]	Infección con Malware en los equipos de la empresa	Propagación de malware como virus, programas espías (spyware), gusanos, troyanos, Ransomware, botnet, etc.	[HW.LAP.*] [HW.PCS.*] [EX.01][SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*] [IC.FWR.01] [IC.WIF.01] [IC.WIF.02] [RH.*]	[SW.*] [IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
6. Organización de la Seguridad de la Información 7. Seguridad de los Recursos Humanos 10. Cifrado 12. Seguridad de las Operaciones		6.2. Dispositivos para movilidad y teletrabajo 7.2. Durante la contratación 10.1. Controles Criptográficos 12.2. Protección contra código malicioso (malware) 12.3. Copias de seguridad		6.2.1. Política de uso de dispositivos móviles. 7.2.2. Concientización, educación y capacitación en seguridad de la información 10.1.1. Política de uso de controles criptográficos 12.2.1. Controles contra el código malicioso (malware). 12.3.1. Copias de seguridad de la información.			

Tabla 5.24. *Matriz de Selección de controles ISO 27002 para: Infección con Malware en los Equipos.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.3]	Ataques externos que afectan a los Activos de información	Ataques externos que afecten la disponibilidad, confidencialidad e integridad de la información de Producción	[IC.FWR.01] [IC.SWT.*] [IC.ROU.*] [IC.WIF.*] [HW.*] [EX.01] [SW.SAT.SIO.*] [IE.*]	[SW.*] [IE.*]	[ED.*]	[D] [I] [C]	**A**

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
7. Seguridad de los Recursos Humanos 9. Control de Accesos 10. Cifrado 12. Seguridad de las Operaciones 13. Seguridad en las Telecomunicaciones 16. Gestión de Incidentes de Seguridad de la Información	7.2. Durante la contratación 9.4. Control de Accesos a Sistemas y Aplicaciones 10.1. Controles Criptográficos 12.2. Protección contra código malicioso (malware) 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo 13.2. Intercambio de información 16.1. Gestión de incidentes de seguridad de la información y mejoras	7.2.2. Concientización, educación y capacitación en seguridad de la información 9.4.1. Restricción del acceso a la información. 9.4.2. Procedimientos seguros de inicio de sesión. 9.4.3. Gestión de contraseñas de usuario. 9.4.4. Uso de herramientas de administración de sistemas. 9.4.5. Control de acceso al código fuente de los programas. 10.1.1. Política de uso de controles criptográficos 12.2.1. Controles contra el código malicioso (malware). 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad. 13.2.1. Políticas y procedimientos de intercambio de información 13.2.4. Acuerdos de Confidencialidad y Secreto 16.1.1. Responsabilidades y procedimientos. 16.1.2. Notificación de los eventos de seguridad de la información. 16.1.3. Notificación de puntos débiles de la seguridad. 16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5. Respuesta a los incidentes de seguridad. 16.1.6. Aprendizaje de los incidentes de seguridad de la información. 16.1.7. Recopilación de evidencias.

Tabla 5.25. *Matriz de Selección de controles ISO 27002 para: Ataques Externos.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.6]	Manipulación de la configuración en los equipos de producción	Manipulación intencionada de la configuración de equipos en producción, afectando directamente a su disponibilidad	[RH.*]	[HW.LAP.*] [HW.PCS.*] [HW.IMP.*] [HW.BAL.*] [HW.SNR.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**M**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
8. Gestión de Activos 9. Control de Accesos 12. Seguridad de las Operaciones		8.1. Responsabilidad sobre los activos 9.4. Control de Accesos a Sistemas y Aplicaciones 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo		8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 9.4.1. Restricción del acceso a la información. 9.4.2. Procedimientos seguros de inicio de sesión. 9.4.3. Gestión de contraseñas de usuario. 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad.			

Tabla 5.26. *Matriz de Selección de controles ISO 27002 para: Manipulación de Configuración en Equipos de Producción.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.7]	Suplantación de credenciales de usuario	Acceso no autorizado al software de producción o a la información electrónica con otras credenciales	[RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[I] [C]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos 12. Seguridad de las Operaciones		9.1. Requisitos de negocio para el control de Accesos 9.2. Gestión de Acceso de Usuario 9.3. Responsabilidades del Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones 12.4. Registro de actividad y monitoreo		9.1.1. Política de control de accesos. 9.1.2. Control de acceso a las redes y servicios asociados. 9.2.1. Gestión de altas/bajas en el registro de usuarios. 9.2.4. Gestión de información confidencial de autenticación de usuarios. 9.3.1. Uso de información confidencial para la autenticación. 9.4.1. Restricción del acceso a la información. 9.4.2. Procedimientos seguros de inicio de sesión. 9.4.3. Gestión de contraseñas de usuario. 12.4.1. Registro y gestión de eventos de actividad.			

Tabla 5.27. *Matriz de Selección de controles ISO 27002 para: Suplantación de Credenciales.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.8]	Instalaciones y configuraciones es de software no autorizadas	Instalaciones y configuraciones No autorizadas de software en los equipos de la empresa.	[RH.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.CON.01] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
6. Organización de la Seguridad de la Información 7. Seguridad de los Recursos Humanos 12. Seguridad de las Operaciones		6.2. Dispositivos para movilidad y teletrabajo 7.2. Durante la Contratación 12.4. Registro de actividad y monitoreo 12.5. Control del software en explotación 12.6. Gestión de la Vulnerabilidad Técnica		6.2.1. Política de uso de dispositivos para movilidad 7.2.2. Concientización, educación y capacitación en seguridad de la información 12.4.1. Registro y gestión de eventos de actividad. 12.5.1. Instalación del software en sistemas en producción. 12.6.2. Restricciones en la instalación de software.			

Tabla 5.28. *Matriz de Selección de controles ISO 27002 para: Instalaciones y Configuraciones de Software no Autorizadas.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.4]	Privilegios de usuario no correspondientes a su función en el Software e Información electrónica	Cuando un usuario tiene un nivel de privilegios inadecuado en el software, y así puede realizar operaciones que no son de su competencia.	[RH.UIN.*] [RH.JEF.*] [RH.INV.*] [HW.LAP.*] [HW.PCS.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.ARC.*] [IE.CON.01] [IE.LOG.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[I] [C]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
9. Control de Accesos		9.2. Gestión de Acceso de Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones		9.2.1. Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4. Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.4.1. Restricción del acceso a la información.			

Tabla 5.29. *Matriz de Selección de controles ISO 27002 para: Privilegios de acceso del Usuario.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.9]	Alteración o Eliminación de Información Crítica	Eliminación o modificación accidental o no de información crítica (fórmulas, rutas o recursos de productos)	[RH.UIN.*] [RH.JEF.*] [RH.INV.*] [HW.LAP.*] [HW.PCS.*] [SW.SAT.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*]	[IE.ARC.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
7. Seguridad de los Recursos Humanos 9. Control de Accesos 12. Seguridad de las Operaciones		7.2. Durante la Contratación 9.2. Gestión de Acceso de Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo		7.2.2. Concientización, educación y capacitación en seguridad de la información 9.2.1. Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.1. Restricción del acceso a la información. 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad.			

Tabla 5.30. *Matriz de Selección de controles ISO 27002 para: Alteración o Eliminación de Información.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.10]	Ingreso de equipos móviles y de almacenamiento extraíbles no autorizados	Ingreso de equipos laptops, móviles y de almacenamiento extraíbles no autorizados a las áreas de producción de la empresa	[RH. *] [HW.LAP.*] [HW.CEL.01] [HW.MOV.01] [EX.01]	[IE.ARC.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[C]	**E**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
6. Organización de la Seguridad de la Información 7. Seguridad de los Recursos Humanos 12. Seguridad de las Operaciones		6.2. Dispositivos para movilidad y teletrabajo 7.2. Durante la Contratación 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo		6.2.1. Política de uso de dispositivos móviles. 7.2.2. Concientización, educación y capacitación en seguridad de la información 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad.			

Tabla 5.31. *Matriz de Selección de controles ISO 27002 para: Ingreso de Equipos Móviles y de Almacenamiento Extraíbles no Autorizados.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[PR.11]	Salida del personal de Inv. y Desarrollo de la empresa con conocimientos hacia empresas de la competencia	Salida del personal de investigación y desarrollo de la empresa con conocimientos de los procesos y fórmulas a empresas de la competencia.	[RH.INV.*]	[IE.ARC.*] [IE.CRI.FOR.*] [IE.CRI.PCR.01] [IE.CRI.PCR.02] [IE.CRI.PCR.03] [IE.CRI.PCR.05] [IE.CRI.PCR.07] [IE.CRI.PCR.08] [IE.CRI.PCR.10] [IE.BBD.03] [IP.CRI.FOR.*] [IP.CRI.PCR.01] [IP.CRI.PCR.02] [IP.CRI.PCR.03] [IP.CRI.PCR.05] [IP.CRI.PCR.07] [IP.CRI.PCR.08] [IP.CRI.PCR.10]	[ED.SEN.INV.01]	[C]	**A**

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
7. Seguridad de los Recursos Humanos 12. Seguridad de las Operaciones 18. Cumplimiento	7.1. Antes de la Contratación 7.2. Durante la Contratación 7.3. Cese o Cambio de Puesto de Trabajo 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo 18.1. Cumplimiento de los Requisitos Legales y Contractuales	7.1.1. Investigación de antecedentes. 7.1.2. Términos y condiciones de contratación. 7.2.2. Concientización, educación y capacitación en seguridad de la información 7.3.1 Cese o cambio de puesto de trabajo. 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad. 18.1.1. Identificación de la legislación aplicable. 18.1.2. Derechos de propiedad intelectual (DPI).

Tabla 5.32. *Matriz de Selección de controles ISO 27002 para: Salida del Personal de la Empresa.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.5]	Fallos de Seguridad en Software Desarrollado	Fallos o vulnerabilidades de Seguridad en software desarrollado para producción.	[SW.DES.*]	[IE.BBD.03] [IE.BBD.04]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**A**

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
12. Seguridad de las Operaciones 14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	12.1. Responsabilidades y procedimientos de Operación 12.3. Copias de Seguridad 12.6. Gestión de la Vulnerabilidad Técnica 14.1. Requisitos de Seguridad de los Sistemas de Información 14.2. Seguridad en los Procesos de Desarrollo y Soporte 14.3. Datos de Prueba	12.1.4. Separación de entornos de desarrollo, prueba y producción. 12.3.1. Copias de seguridad de la información. 12.6.1. Gestión de las vulnerabilidades técnicas. 14.1.1. Análisis y especificación de los requisitos de seguridad. 14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3. Protección de las transacciones por redes telemáticas. 14.2.1. Política de desarrollo seguro de software. 14.2.2. Procedimientos de control de cambios en los sistemas. 14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4. Restricciones a los cambios en los paquetes de software. 14.2.5. Uso de principios de ingeniería en protección de sistemas. 14.2.6. Seguridad en entornos de desarrollo. 14.2.7. Externalización del desarrollo de software. 14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9. Pruebas de aceptación. 14.3.1. Protección de los datos utilizados en pruebas.

Tabla 5.33. *Matriz de Selección de controles ISO 27002 para: Fallos de Seguridad en Software Desarrollado.*

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RL.6]	Fallos de Seguridad en Software Adquirido	Fallos o vulnerabilidades de Seguridad en software Adquirido a terceros para producción.	[SW.SAT.*]	[IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**A**
DOMINIOS		**CATEGORIAS**		**CONTROLES/POLITICAS APLICABLES**			
12. Seguridad de las Operaciones 14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información 15.Relaciones con Suministradores		12.1. Responsabilidades y procedimientos de Operación 12.3. Copias de Seguridad 12.6.1. Gestión de la Vulnerabilidad Técnica 14.1. Requisitos de Seguridad de los Sistemas de Información 14.2. Seguridad en los Procesos de Desarrollo y Soporte 14.3. Datos de Prueba 15.1. Seguridad de la Información en las Relaciones con Suministradores 15.2. Gestión de la Prestación del Servicio por Suministradores.		12.1.4. Separación de entornos de desarrollo, prueba y producción. 12.3.1. Copias de seguridad de la información. 12.6.1. Gestión de las vulnerabilidades técnicas. 14.1.1. Análisis y especificación de los requisitos de seguridad. 14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3. Protección de las transacciones por redes telemáticas. 14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.7. Externalización del desarrollo de software. 14.2.9. Pruebas de aceptación. 14.3.1. Protección de los datos utilizados en pruebas. 15.1.1. Política de seguridad de la información para suministradores. 15.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3. Cadena de suministro en tecnologías de la información y comunicaciones. 15.2.1. Supervisión y revisión de los servicios prestados por terceros. 15.2.2. Gestión de cambios en los servicios prestados por terceros.		

Tabla 5.34. *Matriz de Selección de controles ISO 27002 para: Fallos de Seguridad en Software Adquirido*

.

5.2.2. Paso 8: Elaboración del Documento Formal

Con la aplicación de la metodología, en este paso se ordenó y se retiraron los controles duplicados, depurando así los controles identificados para mitigar los riesgos, se obtuvieron un total de 13 dominios, 30 categorías de control y 88 controles seleccionados de la norma ISO 27002 (2013) para el departamento de producción de la empresa; esto se ilustra en la tabla 2.4 del Anexo 2 que es la "*Matriz Depurada de Controles ISO 27002*" resultante de este paso. Se encuentran en dicha matriz 13 dominios y no 14 como tiene la norma, porque el dominio número 5 (*Políticas de Seguridad*) no se consideró dentro de la selección de controles ya que solamente es una guía que define las pautas o directrices específicas para elaborar el documento formal de política de seguridad; las mismas que fueron consideradas para desarrollar el documento en el siguiente paso. Un interesante hallazgo para el equipo de trabajo fue que al final unificando todos los controles identificados y seleccionados por cada riesgo, se obtuvieron controles en prácticamente todos los dominios de la norma ISO 27002 (2013); concluyendo que el departamento de producción necesita dichos controles para elaborar una política de

seguridad que mitigue los riesgos identificados; dando una seguridad integral y en profundidad a esta área de vital importancia para la empresa.

A continuación se plantea como entregable final de este paso la política de seguridad de la información para el departamento de producción de la empresa en un documento Formal, siguiendo las directrices dadas por la norma ISO 27002 (2013) para la elaboración de políticas de seguridad de la información con el formato planteado en el Capítulo 4 en el punto 4.2.2.

EMPRESA INDUSTRIAL DE CARNICOS Y EMBUTIDOS	**POLITICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE PRODUCCIÓN**	**Versión:** 1.0 **Fecha de Elaboración:** 15/09/2017 **Fecha Actualización:** 15/09/2017
	Departamento de Tecnologías de la Información y Comunicaciones	**Codificación:** PSI-001

9. FIRMAS DE APROBACIÓN DEL DOCUMENTO

ROL	NOMBRE / CARGO	FIRMA	FECHA
APROBADO POR:	Ing. Telmo Durán **Gerente General**		
REVISADO POR:	Ing. Mauricio Borja **Auditor**		
ELABORADO POR:	Ing. Mauricio Arévalo **Jefe de TI** Ing. Cristian Moreno **Desarrollo TI** Ing. Javier Puga **Desarrollo TI** Ing. Carlos Alvarez **Supervisor de Infraestructura TI** Ing. Carlos Domínguez **Soporte TI**		

10. INDICE Y CONTENIDO

Detallar índice y contenido completo del documento.

11. OBJETIVOS

Son objetivos de la Política de Seguridad de la Información:

a) Fijar las pautas para el establecimiento de procedimientos y actividades relativas a la gestión de seguridad de la información y a la minimización de los riesgos tecnológicos y legales bajo la guía de la norma ISO/IEC 27002; así como, el establecimiento de responsabilidades, capacitaciones, y cumplimiento de los principios de seguridad de la información establecidos.

b) Proteger la información y demás activos relacionados con el tratamiento de la misma. La política será la guía principal para asegurar las características básicas de la seguridad de la información como son la Confidencialidad, Integridad, y Disponibilidad de acceso y el uso adecuado de la información, tanto en documentación física como en sistemas de información automatizados, redes, instalaciones, equipos de cómputo y procedimientos de protección.

c) Prevenir, detectar, controlar y reportar actividades o incidentes que afecten la seguridad de la información en la empresa.

d) Preservar la fuga o divulgación de información crítica y confidencial de la empresa como los datos de sus procesos, recetas, productos, etc.

12. ALCANCE

El alcance de la presente política incluye a todos los empleados de la empresa, así como a los contratistas o personal externo que tuviera acceso a las instalaciones de la empresa o a los activos de información y a aquellos responsables del cumplimiento de la seguridad de los mismos.

13. PRINCIPIOS

La presente política de seguridad de la información se fundamenta en los siguientes principios básicos:

a) PRINCIPIO DE PROPIEDAD DE LA INFORMACIÓN

El conjunto de la información organizada y procesada que se genera dentro de la empresa, fruto de sus procesos y operaciones es de propiedad exclusiva de la empresa independientemente de la forma en que se encuentre archivada y distribuida.

b) PRINCIPIO DE PROTECCIÓN DE LA INFORMACIÓN

El nivel de protección de la información deberá estar establecido en función a su valor y efectos causados en caso de pérdida, alteración o difusión no autorizada de la misma. Dicha protección debe asegurar la *confidencialidad, la integridad y disponibilidad* de la información, que son los principios básicos en que se fundamenta la seguridad de la información.

- **Confidencialidad:** Garantizar de que solo los usuarios con acceso autorizado puedan acceder a la información.
- **Integridad:** Proteger la exactitud, totalidad de los datos y métodos de procesamiento de la información que los usuarios autorizados gestionan.
- **Disponibilidad:** Los recursos deben estar disponibles cuando sean requeridos en cualquier instante de tiempo.

c) PRINCIPIO DE USO ADECUADO DE LA INFORMACIÓN

La información, así como los diferentes elementos utilizados para la generación, transmisión y almacenamiento de la misma, deben ser utilizados exclusivamente para las funciones específicas que le competen a cada trabajador de la empresa.

14. BASE LEGAL

- Constitución de la República del Ecuador, publicada en Registro Oficial No 449, del 20 de Octubre del 2008.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedida por el Congreso Nacional el 10 de abril del 2002 y publicado en el Registro Oficial No 735 del 22 de diciembre del 2002.
- Artículos 42 y 45 del Código de Trabajo donde se indica que los trabajadores tendrán la obligación de sujetarse al reglamento interno legalmente aprobado por el Ministerio de Trabajo.
- El Reglamento Interno de Trabajo vigente de la empresa; en el capítulo V, en los Artículos 25 y 26, donde se indican los literales sobre las obligaciones y prohibiciones respectivamente para los trabajadores de la empresa.

15. RESPONSABILIDADDES

Son responsabilidades de todos los trabajadores de la empresa:

a) Cumplir con todas las políticas específicas y procedimientos de seguridad de la información especificadas en este documento para para proteger los activos de información que se pongan a su disposición en la empresa.
b) Asistir a los diferentes eventos de capacitación en materia de seguridad de la información.
c) Informar a sus superiores o supervisores de cualquier incidente de seguridad que afecte a los activos de información de la empresa.

Los integrantes del *"Equipo de Gestión de Seguridad de la Información"*, tienen la responsabilidad del desarrollo y planteamiento de las Políticas de Seguridad de la Información y también la responsabilidad de la comunicación directa sobre su conocimiento, cumplimiento, difusión y revisiones a los miembros del "*Comité Directivo"*, conformado por los directivos y gerente de la empresa, quienes tienen la responsabilidad de aprobar la conformación del Equipo de Gestión de Seguridad de la Información y de aprobar la política de seguridad planteada en este documento, así como cualquier proyecto nuevo relacionado a seguridad de la información.

Los integrantes de "*Auditoría Interna"*, tienen la responsabilidad principal de controlar y evaluar el cumplimiento de la política y controles de seguridad establecidos. Una vez implementada la política, deberán monitorear el cumplimiento de dicha política de seguridad con la aplicación de los controles recomendados e informar al Comité Directivo sobre la correcta aplicación o incumplimiento de la política de seguridad.

Los "*Administradores de Seguridad*" que se integra por los jefes, administradores o responsables de cada departamento, área o unidad de negocio de la empresa son los encargados de mantener y vigilar el cumplimiento de las políticas de seguridad informática recomendadas en sus respectivas áreas para proteger la información de la empresa, teniendo también la responsabilidad de comunicar y recordar a su personal las instrucciones, recomendaciones y políticas de seguridad dadas por el Equipo de Gestión de Seguridad de la Información y aprobadas por el Comité Directivo.

Solamente existirán excepciones a la política y sus controles descritos a continuación, con autorización por escrito del Gerente General o por un acuerdo con el Equipo de Gestión de Seguridad de la Información, representado por el Jefe del departamento de TI.

16. DESCRIPCION DE LA POLITICA

8.1. Organización de la Seguridad de la Información

8.1.1. Dispositivos para movilidad y teletrabajo

8.1.1.1. Política de uso de dispositivos móviles

Todos los empleados y el personal externo deben cumplir con las siguientes medidas de seguridad de apoyo para gestionar los riesgos introducidos al utilizar dispositivos móviles en cualquiera de las instalaciones que corresponden al área de producción:

a) Todos los empleados de las áreas del departamento de producción y el personal externo que acceda a ellas, salvo las excepciones por escrito dadas por la el Gerente de Producción o la Gerencia General, deberán dejar sus equipos móviles inteligentes, dispositivos de almacenamiento extraíble, cámaras de video y fotografía o cualquier otro tipo de dispositivo electrónico de su propiedad en sus respectivos casilleros o lugares asignados antes de ingresar a las instalaciones de planta; se establecerá un control estricto por parte de los supervisores encargados.
b) Al usar dispositivos móviles con autorización en las instalaciones del área de producción, se debe tener especial cuidado para garantizar que la información crítica de producción no se vea comprometida en las tres características principales de la seguridad de la información: integridad, confidencialidad y disponibilidad; por lo tanto los dispositivos autorizados privados y de propiedad de la empresa deben ser registrados por el departamento de TI en su inventario de equipos y obligatoriamente deben tener instalado un software antivirus o antimalware.
c) Solamente el Gerente de Producción o la Gerencia General de la empresa son quienes podrán autorizar por escrito la conexión de dispositivos móviles a dispositivos de la red cableada o inalámbrica en las áreas de producción; con sus respectivos accesos.
d) En caso de conexión de dispositivos móviles por medio de la red inalámbrica al servicio de Internet para usuarios internos o externos en las instalaciones de producción, previa autorización por escrito del Gerente de Producción o la Gerencia General, esta red estará totalmente separada de la red interna de la empresa; por lo tanto no se podrá acceder a ningún recurso de información de la empresa.
e) En ningún caso se puede guardar información de cualquier índole de la empresa, tales como archivos, documentos, fotografías o videos dentro de sus instalaciones en los dispositivos móviles.

8.2. Seguridad de los Recursos Humanos

El personal interno de la Empresa y prestadores de servicios externos, cualquiera sea su posición o nivel de responsabilidad dentro del departamento de producción, deberá considerar lo siguiente:

8.2.1. Antes de la contratación

8.2.1.1. Investigación de antecedentes

Los controles de verificación de antecedentes de todos los candidatos para el empleo deben llevarse a cabo de conformidad con las leyes, reglamentos y ética pertinentes y deben ser acordes a los requisitos de la empresa, la clasificación de la información a acceder y los riesgos percibidos. La verificación de información debe tener en cuenta toda la privacidad relevante, la protección de la información personal y la legislación laboral, y debe incluir, cuando esté permitido, lo siguiente:

a) Disponibilidad de facilidad de referencias personales y laborales.
b) Verificación (completitud y exactitud) de la hoja de vida del solicitante.
c) Confirmación de calificaciones académicas y profesionales.
d) Verificación de documentos de identidad (cédula o pasaporte).
e) Verificación más detallada, como revisión de crédito, antecedentes penales, etc.
f) Cuando un trabajo involucra a una persona que tiene acceso a las instalaciones de procesamiento de información, a las instalaciones de producción o acceso y manipulación de información confidencial, la organización también debe considerar verificaciones adicionales y más detalladas que sean pertinentes.
g) Se debe garantizar un proceso de selección para los contratistas; donde el acuerdo entre la organización y el contratista debe especificar las responsabilidades de seguridad y confidencialidad de la información.

8.2.1.2. Términos y condiciones de la contratación

Los acuerdos contractuales con empleados y contratistas deben indicar sus responsabilidades y las de la organización tomando en la seguridad de la información, teniendo las siguientes consideraciones:

a) Todos los empleados y contratistas que tienen acceso a información confidencial de la empresa deben firmar un acuerdo de confidencialidad o no divulgación antes de acceder a trabajar en las instalaciones y con la información de la empresa.
b) Responsabilidades del empleado o contratista para el manejo de la información recibida de la empresa o partes externas relacionadas con la misma.
c) Acciones a tomar si el empleado o el contratista ignoran los requisitos de seguridad de la empresa.
d) Las funciones y responsabilidades de la seguridad de la información deben comunicarse a los candidatos a puestos de trabajo durante el proceso de contratación.

e) Cuando corresponda, las responsabilidades incluidas en los términos y condiciones del contrato de empleo deben continuar por un período definido incluso después del final de la salida del empleado de la empresa.

8.2.2. Durante la contratación

8.2.2.1. Concientización, educación y capacitación en seguridad de la información

a) Todos los empleados de la empresa y los contratistas cuando corresponda, deberían recibir educación y capacitación adecuadas sobre la concientización y actualizaciones periódicas en las políticas y procedimientos de seguridad de la organización, según corresponda para su función laboral. Esto comprende los temas y requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones y de los recursos de información en general, como por ejemplo su estación de trabajo.

b) El equipo de Gestión de Seguridad de la empresa debe planificar capacitaciones trimestrales en seguridad informática por distintos medios como presentaciones impresas, capacitaciones en el aula, presentaciones compartidas por videoconferencias, en videos, correo electrónico, en el sitio web de la empresa o cualquier otro medio que se determine.

c) El programa de capacitación en seguridad de la información se debe actualizar periódicamente con las políticas y procedimientos de la organización, además con las últimas amenazas, incidentes y controles de la empresa para la seguridad de la información.

8.2.3. Cese o cambio de puesto de trabajo

8.2.2.1. Cese o Cambio de puesto de Trabajo

a) Las responsabilidades sobre la seguridad y confidencialidad de la información de la empresa siguen siendo válidos aún después de la terminación del contrato o servicio prestado por un tiempo definido en los mismos contratos; los cuales que se harán cumplir legalmente al empleado o contratista.

b) En el caso de los empleados, el departamento de recursos humanos es responsable del proceso de finalización del contrato de trabajo o cambio de puesto y trabajará junto con el jefe inmediato de la persona que se retira de su puesto de trabajo y con el departamento de Activos Fijos para la entrega, verificación y registro de todos los activos de información que se entregaron bajo custodia del empleado que se retira de la empresa o de su puesto de trabajo. El departamento de TI será el encargado de revisar física y lógicamente los equipos informáticos entregados; sacar respaldos de la información contenida en los dispositivos y entregar un informe del estado de los mismos a Recursos Humanos y

Activos Fijos para su respectiva gestión con el empleado. Además se dejarán los equipos listos para su reutilización por otro usuario en caso de necesitarse.

c) En el caso del retiro de un contratista que proporcionó bienes o servicios a la empresa, la seguridad y confidencialidad de la información que se pudo haber conocido durante el tiempo en que se prestó el servicio, seguirá llevándose por la parte externa de acuerdo a lo que estipula el contrato existente entre la empresa y el contratista.

d) Se podrá rotar entre puestos de trabajo cada cierto tiempo, sobre todo entre los empleados que laboran en las áreas de producción, empaques, carnes e investigación y desarrollo de la empresa; según el criterio del jefe inmediato, del gerente de recursos humanos y del gerente de producción.

8.3. Gestión de Activos

8.3.1. Responsabilidad sobre los activos

8.3.1.1. Inventario de activos

La empresa debe tener conocimiento completo de los activos que posee, de tal manera que pueda asignar un propietario debidamente identificado, que pueda tener responsabilidad por el bien que se le entregue, refiriéndose tanto a lo material (equipos) como lo no material (información) y al cual se le pueda aplicar los controles adecuados.

Los activos pueden ser entregados por la empresa a un custodio o propietario específico, al mismo tiempo el término propietario identifica a una persona o grupo de personas a las cuales se les ha designado el uso, control, desarrollo, mantenimiento y seguridad de un activo determinado.

Es necesario elaborar un inventario de todos los activos de TI, en los cuales se muestren detalles relevantes tales como los propietarios asignados, cambios en la estructura del bien con el paso del tiempo, ingresos y salidas de la empresa (en manos de los empleados).

8.3.1.2. Propiedad de los activos

Todos los equipos informáticos dentro del inventario, así como la información relacionada al departamento tienen que pertenecer a un área y custodio determinados, en este caso, en el departamento de Producción.

El procedimiento más común para este tipo de casos es un registro para la asignación del activo al propietario, así como también el retorno del activo a la organización. El propietario debe ser responsable de la gestión del activo a lo largo del tiempo. Adicionalmente el propietario debe:

a) Asegurarse que el activo esté debidamente inventariado.
b) Asegurarse que el activo esté clasificado y protegido.
c) Informar y proceder adecuadamente cuando el activo es retirado, eliminado o destruido.

8.3.1.3. Uso aceptable de los activos

Usar adecuadamente todos los servicios, equipos, dispositivos, materiales y demás elementos entregados a los usuarios de la empresa, los mismos que son de uso exclusivo solamente para actividades laborales.

8.3.1.4. Devolución de activos

Todos los usuarios externos y empleados de la organización deben devolver todos los activos de la empresa que hayan tenido en su custodia al finalizar su contrato de relación laboral con la empresa o el contrato de servicios prestado.

a) El proceso de terminación deber ser establecido de manera formal, en la que se incluya toda la documentación necesaria para la devolución del activo a la empresa, formalizada por escrito en el formato establecido, con firmas y entregada al departamento de Activos Fijos.
b) En caso de que un activo sea adquirido o entregado al personal una vez este haya terminado su relación laboral con la empresa, es importante garantizar que la información relacionada o que pertenece a la empresa sea respaldada en los dispositivos de respaldo designados y eliminada por completo del equipo.
c) Toda la información debe estar documentada y respaldada en los dispositivos de almacenamiento de la empresa, esto en caso de que exista manipulación por parte del personal que deja la organización.
d) Una vez notificado el usuario de la terminación de su relación laboral, el personal de TI debe controlar la copia y manipulación no autorizada de la información contenida en el dispositivo, esto con el fin de evitar apropiamiento indebido de información; y el usuario cesante debería dar todas las facilidades necesarias para el cumplimiento de esta actividad.

8.3.2. Manejo de los soportes de almacenamiento

8.3.2.1. Gestión de soportes extraíbles

Se deben considerar los siguientes controles y guías que la empresa implementa para los medios extraíbles y su oportuna gestión:

a) Todos los equipos informáticos de la empresa tendrán bloqueado el acceso a las entradas para dispositivos extraíbles mediante software de seguridad, salvo las excepciones dadas

por escrito por el Gerente General o el Jefe de TI.

b) Cuando sea necesario el uso de medios extraíbles, cualquier transferencia de información a estos dispositivos debe ser monitoreado por el departamento de TI, y solamente bajo autorización del Jefe de TI o del Gerente General.

c) Cuando la información ya no es requerida, cualquier dato incluido en los medios extraíbles debe ser eliminada para evitar la duplicación.

d) Todos los medios extraíbles deben estar almacenados en un lugar seguro y protegido, y de ser necesario mantener un registro de su uso, esto con la finalidad de hacer el seguimiento correspondiente del dispositivo en caso de auditorías.

e) De acuerdo a la importancia de la información, se hace necesaria la implementación de software de encriptado para proteger los dispositivos extraíbles en caso de pérdidas o robos.

f) Se debe realizar copias de respaldo en medios separados de manera simultánea y periódica antes que el dispositivo extraíble se degrade para evitar pérdidas.

8.3.2.2. Eliminación de los soportes

Todos los soportes extraíbles deben ser desechados de manera segura y con un procedimiento formal cuando éstos ya no sean necesarios. Estos procedimientos se realizarán para minimizar el riesgo de fuga de información y activos, por lo que se debe proceder de la siguiente manera:

a) Los medios que contienen información sensible de la empresa, una vez que no sean necesarios deben ser eliminados de diferentes maneras, tales como borrado completo de la información y en algunos casos por trituración o incineración, de tal forma que la información sea siempre inaccesible.

b) Elaborar un listado de los dispositivos que requieran una eliminación segura, procediendo con la destrucción del dispositivo como se indicó en el punto anterior.

c) Los dispositivos dañados o inaccesibles que aun contienen información deben ser registrados y evaluados antes de desecharse, esto se realiza con la finalidad de evitar que otras empresas o personas puedan intentar acceder a ellos con herramientas más sofisticadas y lograr recuperar información sensible de la organización.

8.3.2.3. Soportes físicos en tránsito

Los medios que contienen información de la organización deben estar protegidos contra accesos no autorizados, uso indebido y robos cuando éstos sean transportados. Muchas veces ocurren intrusiones de personas no autorizadas que pueden robar o eliminar información en perjuicio de la organización. Se recomienda seguir los siguientes parámetros para evitar estos problemas:

a) Utilizar empresas especializadas en mensajería de confiabilidad comprobada.
b) Utilizar mecanismos de seguridad como la firma electrónica y la implementación de software de encriptado para proteger los dispositivos extraíbles.
c) El embalaje de los medios es un factor importante a la hora de realizar envíos, se debe realizar un embalaje lo suficientemente fuerte para soportar agentes externos tales como golpes, exposiciones a humedad o magnetismo que hagan que los medios se deterioren.
d) Mantener un registro de los movimientos de los medios en el que se incluyan datos como el contenido del dispositivo, la protección aplicada y los tiempos de transferencias a los custodios de tránsito y destino, incluyendo también los datos de estos custodios.

8.4. Control de Accesos

8.4.1. Requisitos del negocio para el control de accesos

8.4.1.1. Política de control de accesos

Se deben aplicar controles de acceso tanto lógicos como físicos en el área de producción con las reglas de control de accesos, derechos y restricciones para los usuarios, las mismas se explican a continuación:

a) Gestión y documentación legal de acceso, es decir, obligaciones contractuales con los empleados en cuanto al acceso o limitación a los datos, sistemas o servicios, entregados por el área de Recursos Humanos de la empresa.
b) El departamento de TI recibirá solamente bajo los requisitos y por escrito en el formato establecido por la empresa, las respectivas solicitudes de acceso, que deberán ser elaboradas y enviadas por parte del departamento de Recursos Humanos.
c) Eliminación de los derechos de acceso a un usuario cuando el caso lo amerite.
d) Todo acceso a servicios o sistemas desconocidos que tenga en su poder un usuario, deberá ser informado inmediatamente al departamento de TI estando prohibido a menos que sea expresamente permitido por escrito por la Gerencia General o el Jefe de TI de la empresa.
e) Los roles de acceso se deben aplicar de acuerdo al perfil del empleado, los cuales serán indicados en el formato respectivo y enviado al departamento de TI, una vez que se los apruebe por parte del departamento de Recursos Humanos.
f) Los accesos de usuarios en sistemas, bases de datos y cualquier otro archivo crítico de información se realizará por medio de técnicas de autenticación y autorización.

8.4.1.2. Control de acceso a las redes y servicios asociados

Los usuarios sólo tendrán acceso a las redes y servicios a los que han sido especificados utilizar. La política de acceso a las redes y servicios cubre los siguientes aspectos:

a) Las redes y servicios que se permite acceder con los accesos correspondientes son a las redes de Área Local(LAN) y Redes inalámbricas WiFi tanto para acceder a los sistemas y servicios internos como para acceder a Internet, siempre que el usuario se haya autentificado con una contraseña que solamente el departamento de TI le puede otorgar.

b) El departamento de TI será responsable de actualizar la contraseña de redes WiFi de manera mensual.

c) Se debe respetar el procedimiento de autorización del departamento de TI para definir quién y a qué redes y servicios puede acceder.

d) Los medios autorizados para acceder a la red desde sitios y equipos remotos externos a la empresa, tanto para empleados como para contratistas previa autorización del Gerente General o del jefe de TI, serán a través de una VPN segura configurada por el departamento de sistemas.

e) No se permitirán accesos a través de otros programas de conexión remota de terceros, por ejemplo TeamViewver, AnyDesk, Radmin u otros salvo autorización por escrito del jefe de TI.

f) Se establecerá un monitoreo continuo del uso de los recursos de red y servicios como Internet y correo por parte del personal del departamento de TI.

g) Cualquier intento de conexión o petición de servicios no autorizados, será inmediatamente rechazado y reportado al personal de TI por los equipos de seguridad perimetral que la empresa disponga.

8.4.2. Gestión de Accesos de Usuario

8.4.2.1. Gestión de altas/bajas en el registro de usuarios

El principal objetivo de esta política es garantizar el acceso autorizado de los usuarios y evitar las intrusiones o accesos no autorizados a los sistemas y servicios de la organización, por lo que se debe implementar un registro de formal de movimientos de usuarios para permitir la asignación de derechos de acceso. Se deben tener en cuenta los siguientes parámetros:

a) Utilizar un identificativo de usuario (ID) único para vincularlo tanto para los accesos como para las responsabilidades que tendrán los usuarios en los sistemas y servicios informáticos.

b) Eliminar o deshabilitar de forma definitiva los ID de usuarios que hayan abandonado la organización.

c) Depurar periódicamente las ID de usuarios redundantes.

d) Proporcionar o revocar la habilitación de una ID de usuario, de la misma forma proporcionar o revocar derechos de acceso a esa ID de usuario.

8.4.2.2. Gestión de los derechos de acceso asignados a usuarios

Se debe implementar un proceso formal de aprovisionamiento de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuario a los sistemas y servicios informáticos. El proceso de aprovisionamiento de accesos debe considerar:

a) Obtener la autorización del departamento de TI para el uso del sistema o servicio.
b) Verificar si el nivel de acceso es el apropiado para el usuario, tener en cuenta si es coherente con otros tipos de acceso de acuerdo a las funciones o actividades que desempeña.
c) Garantizar que los derechos de acceso no estén activados hasta que se hayan realizado todos los procedimientos de autorización.
d) Mantener un registro de los derechos de acceso otorgados a una ID de usuario para acceder a los sistemas de información y servicios.
e) Actualizar los derechos de acceso de los usuarios que han cambiado de roles o puestos de trabajos y eliminar de inmediato los derechos de acceso de los usuarios que abandonen la empresa.
f) Revisar y depurar periódicamente los derechos de acceso de los propietarios de los servicios o sistemas de información.
g) Incluir cláusulas en los contratos de personal y contratos de servicios para especificar sanciones si el personal o los proveedores intentan acceder de forma no autorizada a los sistemas o servicios informáticos.

8.4.2.3. Gestión de los derechos de acceso con privilegios especiales

La asignación y el uso de los derechos de acceso privilegiado deben ser restringidos y controlados ya que estos derechos permiten al usuario anular o asignar los controles del sistema o de la aplicación y asignar, modificar o eliminar accesos a otros usuarios; para tal efecto se debe tener un proceso de autorización formal, teniendo en cuenta los siguientes aspectos:

a) Se deben identificar los derechos de acceso privilegiado a cada sistema o proceso, como a bases de datos, sistemas de gestión, aplicaciones y a los usuarios que los utilizarán.
b) Los derechos de acceso privilegiados deben asignarse a los usuarios sobre una base de necesidad de uso, es decir, basada en los requisitos mínimos para sus roles funcionales.
c) Solamente el departamento de TI con autorización del jefe de TI o del Gerente General, será quien otorgue los accesos privilegiados a los usuarios que los necesiten.
d) Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados.
e) Se deben retirar adecuadamente los derechos de acceso privilegiado a los usuarios que

cambien de cargo o se retiren de la empresa.

8.4.2.4. Gestión de información confidencial de autenticación de usuarios

La asignación de la información de autenticación secreta a los usuarios debe controlarse bajo los siguientes requisitos:

a) Los usuarios deben firmar una declaración para mantener confidencialidad sobre la información de autenticación secreta personal; esta declaración firmada se incluirá en los términos y condiciones de empleo, donde se indique que el usuario no podrá prestar o indicar sus credenciales de sistemas, servicios o aplicaciones a terceros, de hacerlo, el usuario a quien se le entregó formalmente las credenciales será el único responsable de lo que puedan realizar con sus credenciales, con las respectivas penalizaciones.
b) Se debe verificar la identidad y funciones que desempeña un usuario antes de proporcionar un nuevo reemplazo de sus credenciales o información de autenticación secreta temporal.
c) La información de autenticación secreta temporal debe darse a los usuarios de manera segura mediante el correo empresarial; el uso de partes externas o mensajes por medios no protegidos como redes sociales o en papel estarán prohibidos.
d) La información de autenticación secreta temporal debe ser exclusiva de un usuario y las contraseñas no deben ser predecibles o descifradas fácilmente; para ello se utilizará la política de contraseñas, donde se debe considerar en la contraseña al menos 8 caracteres, una letra mayúscula, un número y un caracter especial.
e) Los usuarios deben acusar recibo de la información de autenticación secreta por escrito o correo electrónico empresarial.

8.4.2.5. Revisión de los derechos de acceso de los usuarios

Los integrantes del departamento de TI serán los encargados de revisar los derechos de acceso de los usuarios a intervalos regulares de tiempo, para ello se debe considerar lo siguiente:

a) Los derechos de acceso de los usuarios deben revisarse cada 60 días y después de cualquier cambio, como la promoción a otro puesto o la terminación del empleo.
b) Los derechos de acceso de los usuarios deben revisarse y reasignarse de ser el caso al pasar de un rol o función a otro dentro de la empresa.
c) Las autorizaciones para los derechos de acceso privilegiado deben revisarse de manera mensual.
d) Los cambios en las cuentas con privilegios deben ser registradas para su revisión periódica.

8.4.2.6. Retirada o actualización de los derechos de acceso

a) Los derechos de acceso a la información de todos los empleados y usuarios externos y el procesamiento de información en las instalaciones deben eliminarse al finalizar su empleo, contrato o acuerdo, o ajustarse a los cambios necesarios. Los cambios de puesto deben reflejarse en la eliminación de todos los derechos de acceso que no fueron aprobados para el nuevo puesto.

b) Los derechos de acceso que deben ser eliminados o ajustados incluyen los de acceso físico y lógico.

c) La eliminación o el ajuste se realizará mediante la eliminación, revocación o reemplazo de llaves, tarjetas de identificación, credenciales de usuario o la eliminación de cualquier otro mecanismo que de acceso al usuario a las instalaciones o activos de información de la empresa.

d) Toda documentación que identifique los derechos de acceso de empleados y contratistas debe reflejar la eliminación o el ajuste de dichos derechos de acceso.

e) Si un empleado o usuario externo que terminan su relación laboral o contrato con la empresa y conocen contraseñas para los ID de usuario que permanecen activos, estas contraseñas deben cambiarse inmediatamente al finalizar o cambiar de empleo, contrato o acuerdo con el empleado o contratista.

f) En casos de terminación laboral iniciada por la administración, inmediatamente se procederá a eliminarse los derechos de acceso del usuario, solo con la indicación del departamento de Recursos Humanos.

8.4.3. Responsabilidades del Usuario

8.4.3.1. Uso de información confidencial para la autenticación

Los usuarios tienen la obligación de guardar con sigilo la información de autenticación secreta que les haya sido entregada, como las contraseñas de autenticación para acceder a sistemas, servicios, bases de datos, etc.; para esto se deberán seguir las siguientes recomendaciones:

a) Mantener la confidencialidad de la información secreta de autenticación, asegurando que no se divulgue a un tercero, incluidas personas de cargos superiores o jefaturas.

b) Evitar mantener un registro electrónico o en papel (por ejemplo, en papel, archivo de software o dispositivo de mano) de autenticación secreta de información, a menos que se pueda almacenar de forma segura.

c) Cuando las contraseñas se usan como información de autenticación secreta, se debe seleccionar contraseñas de calidad con longitud mínima suficiente que sean:

    1. Fáciles de recordar.
    2. No se basen en nada que otra persona pueda adivinar.
    3. No usar fechas de nacimiento, ID de cédula o teléfonos personales.

4. No constar en diccionarios o palabras conocidas.
5. Que esté libre de caracteres consecutivos idénticos, totalmente numéricos o completamente alfabéticos.
6. Se utilizará la política de seguridad de contraseñas dada por el departamento de TI, donde actualmente se debe considerar en la contraseña al menos 8 caracteres, una letra mayúscula, un número y un caracter especial.

d) No compartir la información de autenticación secreta del usuario a terceros.

e) No usar la misma información de autenticación secreta para contraseñas de asuntos personales.

8.4.4. Control de Acceso a Sistemas y Aplicaciones

8.4.4.1. Restricción del Acceso a la Información

El acceso a la información y las funciones de las aplicaciones deben restringirse de acuerdo con la política de control de acceso. Se deben considerar los siguientes aspectos para soportar los requisitos de restricción de acceso en las aplicaciones desarrolladas internamente o de terceros:

a) Proporcionar menús para controlar el acceso a las funciones de la aplicación.

b) Controlar a qué datos puede acceder un usuario en particular.

c) Controlar los derechos de acceso de los usuarios (leer, borrar, escribir, ejecutar).

d) Controlar derechos de acceso a otras aplicaciones relacionadas.

e) Limitar la información contenida en el sistema.

f) Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles; en el caso de Investigación y Desarrollo; la aplicación de formulación estará separada del resto de aplicaciones y bases de datos de la empresa, tanto en el aspecto físico (distintos servidores) y lógico (distintas aplicaciones y bases de datos).

8.4.4.2. Procedimientos seguros de inicio de sesión

El procedimiento para iniciar sesión en un sistema o aplicación debe minimizar la oportunidad de accesos no autorizados. El procedimiento de inicio de sesión debe revelar el mínimo de información sobre el sistema o la aplicación, para evitar proporcionar a un usuario no autorizado cualquier información innecesaria sobre el sistema.

El procedimiento de inicio de sesión debe:

a) Ocultar el sistema o los identificadores de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito.

b) Mostrar un aviso general advirtiendo que solamente los usuarios autorizados podrán acceder a la aplicación o sistema y que dicho sistema o aplicación es de propiedad de la

empresa, tiene derechos de autor y que la violación de estos términos estarán sujetos a consecuencias legales.

c) No proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que podría asistir a un usuario no autorizado.

d) Validar la información de inicio de sesión solamente al completar todos los datos de entrada.

e) Proteger contra los intentos de inicio de sesión de fuerza bruta.

f) Registrar intentos de accesos fallidos y exitosos.

g) No mostrar la contraseña ingresada al usuario.

h) Las contraseñas de los sistemas o aplicaciones se deben almacenar de forma encriptada en las bases de datos, y de esa manera se deben transmitir por la red.

i) Se deben finalizar las sesiones inactivas después de un período de inactividad de 5 minutos en todos los equipos del área de producción

8.4.4.3. Gestión de contraseñas de usuario

El sistema de administración de contraseñas debe tener en cuenta los siguientes puntos:

a) Hacer cumplir el uso de las identificaciones de usuario y contraseñas individuales para mantener la responsabilidad de los usuarios asignados.

b) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas.

c) En las aplicaciones y sistemas operativos de la empresa se utilizarán contraseñas seguras que cumplan con los requisitos mínimos establecidos por esta política, donde actualmente se debe considerar en la contraseña al menos 8 caracteres, una letra mayúscula, un número y un caracter especial.

d) Los usuarios deben obligatoriamente cambiar su contraseña en el primer inicio de sesión, y regularmente cada 3 meses en los aplicativos e inicios de sesión de los sistemas operativos.

e) En las aplicaciones y sistemas se debe mantener un registro de las contraseñas utilizadas anteriormente y evitar la reutilización.

f) No mostrar contraseñas en la pantalla cuando se ingresan.

g) Almacenar y transmitir contraseñas de forma segura mediante técnicas de encriptación.

h) Diseñar y ejecutar capacitaciones cada semestre sobre temas de seguridad de la información donde se incluya y concientice a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas, equipos y demás servicios informáticos que la empresa proporcione a su personal; indicando también el procedimiento para el cambio de contraseñas de forma periódica así como la eliminación y bloqueo inmediato de los accesos de usuarios por motivos de salidas o cambios de funciones.

8.4.4.4. Uso de herramientas de administración de sistemas

a) El uso de programas utilitarios podría anular o inhabilitar los controles de las aplicaciones y dispositivos de seguridad, causando presencia de vulnerabilidades de seguridad por lo que su aplicación debería ser restringida y estrictamente controlada para todo el personal.
b) Los integrantes del departamento de TI son quienes deben identificar, autenticar y autorizar el uso de programas utilitarios.
c) Se deben registrar todos programas utilitarios existentes y sus usos en la empresa por parte del departamento de TI
d) Se deben definir y documentar los niveles de autorización para programas utilitarios
e) Se deben eliminar de los equipos de la empresa todos los programas utilitarios innecesarios

8.4.4.5. Control de acceso al código fuente de los programas

El acceso al código fuente de las aplicaciones desarrolladas debe estar restringido. El acceso al código fuente de los programas y los elementos asociados (como diseños, especificaciones, pruebas y planes de validación) deberían ser estrictamente controlados, a fin de prevenir la introducción de funcionalidades y evitar cambios involuntarios en los mismos, así como para mantener la confidencialidad de los valiosos datos de propiedad intelectual. Las siguientes pautas deben ser consideradas para controlar el acceso a tales archivos o bibliotecas fuentes de aplicaciones desarrolladas internamente en la empresa:

a) La empresa es la propietaria de cualquier desarrollo realizado por su personal contratado de TI que haya sido elaborado con sus recursos, y está protegido por los derechos de propiedad intelectual. Esto se debe incluir en el contrato del personal de TI de la empresa.
b) Solamente el personal de desarrollo del departamento de TI deben tener acceso irrestricto a las bibliotecas y códigos fuentes del programa.
c) El mantenimiento, las versiones y copias de los códigos fuentes de los desarrollos de sistemas deben estar sujetas a un estricto control de cambios y su registro.

8.5. Cifrado

8.5.1. Controles Criptográficos

8.5.1.1. Política de uso de controles criptográficos

Se debe asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información en la empresa. La política criptográfica debe considerar lo siguiente:

a) Cualquier archivo electrónico que contenga información crítica del área de investigación

y desarrollo debe ser encriptado con algoritmos y las herramientas de software que determine e implemente el departamento de TI. Las claves solamente las podrán tener los respectivos propietarios de la información.

b) Los dispositivos de almacenamiento externo sean de propiedad de la empresa o privada, que con previa autorización del jefe de TI o del gerente general, transporten información crítica del área de investigación y desarrollo o producción, deben tener encriptada la información que transportan con algoritmos y las herramientas de software que determine e implemente el departamento de TI.

c) Los equipos laptops y de escritorio del área de Investigación y desarrollo, gerencia y supervisión de producción deberán tener instalado una herramienta de encriptado a nivel de disco duro; cuya clave solo la podrá conocer el custodio del equipo.

d) En caso de pérdida u olvido de las claves de encriptado, solamente el departamento de TI indicará las instrucciones para resetear la clave o proporcionar una clave nueva con las herramientas necesarias.

e) Se debe tener un cifrado obligatorio de la Información para los códigos y nombres de los Ingredientes de Fórmulas Principales, de manera que no sean legibles en Pantalla ni de manera Impresa para los Operarios. Esta información solo la debe conocer y manejar el jefe del departamento de Investigación y Desarrollo.

8.6. Seguridad Física y Ambiental

8.6.1 Áreas seguras

8.6.1.1. Perímetro de seguridad física

Los perímetros de seguridad se usan para proteger las áreas que contienen los equipos de ingreso y consulta de información crítica, en este caso en las áreas de producción, donde se debe dar cumplimiento a los siguientes puntos:

a) Se restringe el acceso físico al personal a todas las áreas de producción, por la información delicada y crítica que se maneja; salvo los trabajadores, supervisores y jefes que trabajan en esta área.

b) El acceso a esta área para las personas que no trabajan en el área de producción, sean empleados o contratistas, será autorizado solamente por el gerente de Producción, el Gerente General o el supervisor delegado en caso de que él no esté presente.

c) Los controles de acceso apropiados se diseñarán con barreras físicas apropiadas que la empresa determine.

d) La empresa utilizará también perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro, de energía eléctrica,

climatización, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas o servicios de información o que contengan documentos o archivos físicos clasificados como confidenciales o de uso restringido o reservado, como el caso del departamento de Investigación y Desarrollo.

8.6.1.2. Controles físicos de entrada

Las áreas seguras de producción deberán estar protegidas por controles apropiados, para garantizar que solo el personal autorizado tenga acceso, y para esto se debe considerar lo siguiente:

a) El acceso a las áreas seguras, deberá restringirse mediante la implementación de controles de acceso adecuados con barreras físicas; implementando un mecanismo de autenticación que podría ser mediante cerraduras mecánicas, tarjetas de acceso, sistemas biométricos o de reconocimiento dactilar o facial, etc.
b) Al personal de servicio externo como interno de soporte se le deberá otorgar acceso restringido a áreas seguras solo cuando sea necesario; este acceso debe ser autorizado y monitoreado por el Gerente de Producción.
c) Tanto los empleados como contratistas y cualquier personal externo que requiera ingresar a las áreas de producción, deberá ser recibido por el personal de seguridad en la guardianía e inmediatamente notificado al gerente de producción, siendo este el que determine su ingreso o no a las instalaciones de producción, caso contrario lo recibirá en la oficina de recepción.
d) Cualquier personal externo que necesite acceder a las instalaciones de la empresa debe tener cita previa con el respectivo jefe o gerente del área respectiva, deberá dejar su documento de identificación con el personal de la guardianía, quienes notificarán inmediatamente al jefe del área involucrada para que lo reciba en la recepción, y de ser necesario su acceso a las instalaciones de la empresa, ingrese a las mismas siempre acompañado del jefe responsable.

8.6.1.3. Seguridad de oficinas, despachos, y recursos

a) Además de tener los respectivos controles físicos de entrada, las instalaciones de oficinas y despachos de las áreas de producción, que son consideradas como críticas, deberán equiparse y configurarse de manera que se evite que la información o actividades confidenciales sean vistas o escuchadas desde el exterior. Se pueden implementar vidrios con recubrimiento oscuro, insonorizar los ambientes.
b) Solamente las oficinas de producción deberían tener acceso a las redes inalámbricas como WiFi; con las seguridades y autenticación requeridas, autorizadas solamente por el Gerente

General o el Gerente de Producción.

c) En las instalaciones de Planta y despachos de producción no se tendrá acceso a redes inalámbricas WiFi, sin ninguna excepción.

8.6.1.4. Protección contra las amenazas externas y ambientales

a) Se deberá diseñar y aplicar protección contra desastres naturales, ataques maliciosos o accidentes. Para ello se deberá contar con un plan de contingencias actualizado y un Plan de Continuidad de Negocio (BCP o Business Continuity Plan por sus siglas en inglés) donde se detalle el procedimiento a seguir ante desastres como por ejemplo incendios, inundaciones, terremotos, explosiones y otras formas de desastres naturales o provocados por el hombre, tanto en las instalaciones de procesamiento de datos como en las oficinas del departamento de producción.

b) Los centros de procesamiento de datos de la empresa como su Datacenter principal y los cuartos de comunicaciones deben tener todos los requerimientos de seguridad para la correcta operación de los equipos que brindan los servicios y sistemas de información, como su correcta climatización, alimentación y redundancia eléctrica, sensores y equipo automático para el control de incendios; además su emplazamiento debe estar en un lugar adecuado, alejado de maquinaria industrial o combustibles, tuberías, con todas las protecciones eléctricas adecuadas como UPS y reguladores de corriente, así como su desconexión automática e inmediata ante cualquier cortocircuito o desastre.

8.6.1.5. El trabajo en áreas seguras

Se deberán aplicar procedimientos para trabajar en las áreas seguras de producción; considerando algunas pautas como:

a) Las áreas seguras que no se estén usando deberían estar cerradas físicamente y ser revisadas periódicamente.

b) No se deberá permitir ningún dispositivo electrónico como: equipo fotográfico, de video, de audio u otro equipo de grabación, dispositivos móviles inteligentes, dispositivos de almacenamiento extraíble a menos que esté autorizado por la gerencia general o el gerente de producción y dichas autorizaciones deberán ser registradas junto con la información de la persona que ingrese con estos dispositivos.

8.6.1.6. Áreas de acceso público, carga y descarga

Los puntos de acceso tales como las áreas de entrega y recepción de materia prima, productos semiterminados y productos terminados donde personas no autorizadas podrían ingresar a las instalaciones de producción de la empresa deben ser controlados y, de ser posible, aislados de las

instalaciones de procesamiento de información y oficinas críticas como investigación y desarrollo para evitar el acceso de personal no autorizado. Se deben considerar las siguientes pautas:

a) El acceso a un área de entrega y recepción desde el exterior de las edificaciones de producción debe restringirse solamente al personal identificado y autorizado;
b) El área personal que recibe los productos fuera del área de producción no puede ingresar a la misma, tanto por la seguridad de la información como por la seguridad alimentaria y contaminación que puede causar. De la misma manera el personal de producción no puede salir por estas puertas y volver a ingresar con la misma vestimenta; tiene que hacerlo por los filtros sanitarios adecuados indicados por la empresa en su inducción.
c) El material entrante debe ser inspeccionado y examinado en busca de dispositivos electrónicos, información en papel que no pertenece al área, u otros elementos peligros que atenten intencionalmente contra el área de producción como explosivos, productos químicos no autorizados u otros materiales peligrosos; en estos casos es necesario reportar inmediatamente al supervisor encargado antes de que este material ingrese al área de producción.
d) El material saliente debe registrarse en los sistemas informáticos según se establezca en su procedimiento y se revisará minuciosamente que no salga igual con dicho material ningún dispositivo o equipo de información o información en papel que no tuviera relación con la transacción de salida que se efectúa.
e) Tanto en las transacciones salientes como entrantes en las áreas de entrega y recepción de material, se seguirá el proceso establecido de las transacciones entre bodegas, registrando la transacción en el sistema informático de producción de la empresa, con respaldo de un comprobante electrónico y en papel con firmas de entrega/recepción; aceptando de ambas partes los productos recibidos y entregados; junto con la información que respalda la transacción.

8.6.2. Seguridad de los equipos

8.6.2.1. Emplazamiento y protección de equipos

El equipo informático debe ser instalado y tener las protecciones adecuadas para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades que se pueden dar para el acceso no autorizado. Se deben considerar protecciones para posibles amenazas físicas y ambientales como robo, incendio, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia del suministro eléctrico, interferencia de comunicaciones, radiación electromagnética y vandalismo. Se deben considerar los siguientes puntos:

a) Las condiciones ambientales, tales como la temperatura y la humedad de las áreas de producción y los centros de procesamiento de datos deberán ser monitoreados constantemente para detectar condiciones que pudieran afectar a los equipos.

b) En la planta de producción de la empresa, por lo general se tiene un ambiente con polvo, humedad y temperaturas inadecuadas, por lo que la empresa actualmente dispone en estas áreas solamente de equipos portátiles, de los cuales es responsable un supervisor asignado y al terminar la jornada laboral debe dejarlos apagando correctamente y ubicarlos en la oficina de producción, la cual al finalizar la jornada laboral debe quedar correctamente asegurada. Además el departamento de TI debe manejar un plan de mantenimiento trimestral para estos equipos por el ambiente en el que operan.

c) Debido al ambiente al que están expuestos los equipos en la planta industrial, el uso de métodos especiales de protección como teclados de membrana, cajas de protección contra polvo y agua o la adquisición e instalación de computadores industriales con pantallas táctiles para ambientes industriales con un "*Grado de Protección*" mínimo de *IP67* debe considerarse para los equipos que se instalan en la planta industrial de la empresa.

d) Los centros de procesamiento de datos de la empresa como su Datacenter principal y los cuartos de comunicaciones del área de producción, así como las áreas críticas de producción como Investigación y Desarrollo deben tener los controles de acceso físico apropiados para prevenir el acceso de personal no autorizado.

e) Los centros de procesamiento de datos en la empresa deben reunir las condiciones para la correcta operación de los equipos que brindan los servicios y sistemas de información, como su correcta climatización, alimentación y redundancia eléctrica, sensores y equipo automático para el control de incendios; además su emplazamiento debe estar en un lugar adecuado, alejado de maquinaria industrial o combustibles, tuberías, con todas las protecciones eléctricas adecuadas como UPS y reguladores de corriente, así como su desconexión automática e inmediata ante cualquier cortocircuito o desastre.

f) Está terminantemente prohibido, sin excepción alguna comer, beber o fumar cerca o dentro de las instalaciones de procesamiento de información de la empresa o en las áreas de producción, investigación y desarrollo o sus oficinas.

g) La protección contra rayos o descargas eléctricas debe aplicarse a todas las instalaciones de la empresa, y los filtros de protección contra descargas o variaciones eléctricas deben ajustarse a todas las líneas de potencia y comunicaciones entrantes.

8.6.2.2. Instalaciones de suministro

El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas o cortes en los servicios de apoyo o suministro. Los suministros como por ejemplo: electricidad, telecomunicaciones, agua, gas, alcantarillado, climatización, entre otros deberían:

a) Cumplir con las especificaciones del fabricante y los registros legales.
b) Ser evaluados regularmente por su capacidad para satisfacer con el crecimiento del negocio.
c) Ser inspeccionados y probados regularmente para su correcto funcionamiento; registrando estas pruebas y sus resultados. Se debe cumplir con pruebas trimestrales con carga del equipo eléctrico de respaldo del Datacenter de la empresa: UPS y Generador eléctrico, así como del equipo de climatización.
d) De existir la factibilidad, los equipos deben ser monitoreados de manera automática mediante el sistema de monitoreo o alarmas que dispongan para detectar malfuncionamientos de manera oportuna.
e) Tener equipos y repuestos de respaldo en bodega, tanto de climatización como de respaldo de energía y ciertos componentes de equipos servidores que más frecuentemente tienen fallas como son memorias o discos duros por ejemplo.

8.6.2.3. Seguridad del cableado

El cableado de energía y telecomunicaciones de toda la empresa que transporta datos o servicios de información debe estar protegidos contra interferencias o daños. Para esto se debe seguir las siguientes pautas:

a) Las líneas de energía y telecomunicaciones en las instalaciones de procesamiento de información deberán ser subterráneas, cuando sea posible, o estar sujetas a una protección alternativa adecuada.
b) Los cables de alimentación deberán estar separados de los cables de comunicaciones para evitar interferencias.
c) En lo posible, realizar las instalaciones de conductos blindados y cajas cerradas en los puntos de inspección y terminación así como utilizar cable con blindaje electromagnético o malla para proteger los cables de interferencia.
d) Revisar y cumplir con la normativa vigente de cableado estructurado; actualmente la empresa dispone en sus instalaciones de cableado estructurado categoría 6A y las nuevas instalaciones se deben realizar con cableado y materiales de esta misma categoría.
e) Debe existir un acceso controlado y monitoreado a paneles de conexiones y cuartos de comunicaciones.

8.6.2.4. Mantenimiento de los equipos

El equipo deberá mantenerse en correcto estado para garantizar su operatividad; para ello se deben seguir las siguientes cláusulas:

a) Solo el personal de mantenimiento y soporte de TI, debe llevar a cabo las reparaciones; se enviarán equipos para revisión o reparación a proveedores externos solo con la autorización por escrito del jefe de TI. Para ello se deberá cumplir con el respectivo proceso y política del departamento de Activos Fijos para la salida de equipos de la empresa por reparaciones.

b) Se deben mantener registros de todas las fallas de los equipos, y de todo el mantenimiento preventivo y correctivo que se les realice, sea este realizado por personal interno de la empresa o por proveedores externos.

c) Se deben firmar acuerdos de confidencialidad en los contratos con proveedores externos, ya que pueden llegar a conocer información crítica o confidencial en los equipos de la empresa que reparan.

d) Se deben implementar controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; cuando sea necesario, la información crítica o confidencial debe respaldarse y eliminarse del equipo antes de que el mismo salga de la empresa. Esto lo debe revisar el departamento de TI interno.

e) Se deben cumplir todos los requisitos de mantenimiento impuestos por las pólizas de seguros.

f) Antes de volver a poner el equipo en funcionamiento después de su mantenimiento, debe inspeccionarse para asegurarse de que el equipo no haya sido manipulado o presente mal funcionamiento; además se verificará que tenga activadas las herramientas y controles de seguridad que provee la empresa y se realizará una verificación de que el equipo no esté infectado con malware u otro tipo de amenaza.

g) Se debe cumplir con un mantenimiento trimestral y pruebas con carga del equipo eléctrico de respaldo del Datacenter de la empresa: UPS y Generador eléctrico, así como del equipo de climatización.

h) Los mantenimientos preventivos de equipos servidores, de comunicaciones y de respaldo de energía en la empresa deben ser realizados en horarios no laborables, por lo que el jefe de TI informará fechas, horarios y tiempos de duración de estos mantenimientos autorizados previamente por la gerencia general de la empresa; teniendo en cuenta que durante estos horarios los servicios y sistemas de la empresa no se podrán utilizar.

8.6.2.5. Salida de activos fuera de las dependencias de la empresa

a) Los equipos, la información o el software no deben sacarse de la empresa sin autorización previa, dada solamente por el jefe de TI o el gerente general y controlada por el departamento de Activos Fijos de la empresa en los formatos establecidos para ello.

b) Los equipos de la empresa saldrán de la misma para revisión o reparación a proveedores

externos solo con la autorización por escrito del jefe de TI o el gerente general. Para ello se debe cumplir con la política establecida por el departamento de Activos Fijos para el control de la salida de equipos de la empresa hacia proveedores externos por reparaciones o configuraciones.

c) En el formato de salida se debe se deberá establecer límites de tiempo para la reparación y devolución del activo y se deberá verificar el cumplimiento de estas devoluciones.

d) Al recibir el activo se deberá revisar su estado, y si hubiese alguna novedad se reportará inmediatamente al departamento de activos fijos y al proveedor externo para que lo reponga o solucione. Se debe asegurar también de que el equipo no haya sido manipulado o presente mal funcionamiento; además se verificará que tenga activadas las herramientas y controles de seguridad que provee la empresa y se realizará una verificación de que el equipo no esté infectado con malware u otro tipo de amenaza.

8.6.2.6. Reutilización o retirada segura de dispositivos de almacenamiento.

Los medios de almacenamiento que contienen información confidencial o con derechos de autor deben destruirse físicamente o la información debe destruirse, eliminarse o sobrescribirse utilizando técnicas para que la información original no sea recuperable.

Los equipos con medios de almacenamiento que se van a retirar o reutilizar pueden requerir una evaluación de riesgos para determinar si los artículos deberán destruirse físicamente en lugar de enviarse a reparar o desecharse. La información puede verse comprometida por la eliminación descuidada o la reutilización del dispositivo; además del borrado seguro del disco, el cifrado de todo el disco reduce el riesgo de divulgación de información confidencial cuando el equipo se desecha o se redistribuye, siempre que:

- El proceso de encriptación sea lo suficientemente fuerte y cubra todo el disco.
- Las claves de cifrado sean lo suficientemente largas como para resistir intentos de descifrado.
- Las claves de cifrado se mantengan confidenciales; nunca se deben almacenar en el mismo disco.

8.6.2.7. Equipo informático de usuario desatendido

Los usuarios deberán asegurase que los equipos desatendidos (cuando el usuario ya no está utilizando el equipo) tengan la protección adecuada. Todos los usuarios deben conocer los requisitos y procedimientos de seguridad para proteger el equipo desatendido, así como sus responsabilidades para implementar dicha protección. Los usuarios deberán:

a) Finalizar las sesiones activas cuando hayan terminado, bloquear las sesiones o dejar el

equipo con un protector de pantalla protegido con contraseña.

b) Desconectarse de las aplicaciones o servicios de red cuando ya no sean necesarios.

c) proteger los dispositivos móviles inteligentes del uso no autorizado mediante un bloqueo o un control equivalente, como el acceso con contraseña, reconocimiento dactilar o patrón secreto, cuando no estén en uso.

8.6.2.8. Política de puesto de trabajo despejado y bloqueo de pantalla

a) La información sensible o critica, ya sea en papel o en medios de almacenamientos extraíbles del área de producción e investigación y desarrollo, deberán ser guardados, en caja fuerte o en un inmobiliario que tenga la seguridad respectiva; para cuando esta información no se requiera o el área de trabajo este desocupada.

b) Las computadoras y terminales deben dejarse apagadas cuando el usuario se retira de su puesto de trabajo y, de ser el caso cuando el usuario se ausenta de su puesto por períodos cortos de tiempo, protegidas con un mecanismo de autenticación de usuario similar cuando están desatendidas: bloqueo de pantalla y teclado controlado por contraseña, bloquear las sesiones o dejar el equipo con un protector de pantalla protegido con contraseña.

c) se debe evitar el uso no autorizado de fotocopiadoras y otras tecnologías de reproducción (por ejemplo, escáneres, cámaras digitales);

d) los medios en papel que fuesen impresos y que contienen información confidencial o clasificada como formulaciones, datos sobre productos, órdenes de producción deben retirarse de las impresoras de inmediato y almacenarse en los lugares seguros para los documentos confidenciales.

e) Mantener limpios los escritorios, está prohibido dejar en ellos documentos de cualquier tipo que pudieren caer en manos de terceros, los que pudiesen hacer uso incorrecto de esta información.

8.7. Seguridad de las Operaciones

8.7.1. Responsabilidades y procedimientos de Operación

8.7.1.1. Separación de entornos de desarrollo, pruebas y producción

a) Las reglas para la transferencia de software desde el ambiente de desarrollo al ambiente productivo deben definirse y documentarse por parte del departamento de TI.

b) El software de desarrollo y productivo deben ejecutarse en diferentes servidores físicos o virtualizados y en diferentes dominios o directorios.

c) Los cambios en los sistemas y aplicaciones productivas se deben probar previamente en un entorno de desarrollo antes de ser aplicados a los sistemas de producción.

d) Salvo en circunstancias excepcionales, las pruebas no deben realizarse en sistemas productivos.

e) Compiladores, editores y otras herramientas de desarrollo no deberían ser accesibles desde sistemas productivos.

f) Los usuarios deben usar diferentes perfiles de usuario para los sistemas productivos y los de desarrollo, y los menús deben mostrar mensajes de identificación apropiados para reducir el riesgo de error o equivocación por parte del usuario.

g) Los datos confidenciales no deben copiarse en el entorno de desarrollo, a menos que existan controles necesarios para esta información el entorno de desarrollo.

8.7.2. Protección contra código malicioso (malware)

8.7.2.1. Controles contra el código malicioso (malware)

La empresa deberá implementar controles y herramientas necesarios para la detección, prevención y recuperación contra malware, además de concientizar a los usuarios. Se deberá tener en cuenta:

a) En los equipos de la empresa estará prohibido el uso de software no autorizado por parte del departamento de TI, sin excepción alguna.

b) Implementar controles que eviten o detecten el uso de software no autorizado.

c) Implementar controles que eviten o detecten el uso de sitios web maliciosos, y reportar estos accesos al personal del departamento de TI.

d) Queda prohibido el uso de dispositivos externos personales como memorias USB, discos extraíbles etc.; salvo los autorizados por la gerencia general o el jefe de TI.

e) Realizar revisiones periódicas del software de la empresa, así como también del contenido de los datos de los sistemas que respaldan las actividades críticas, en caso de encontrar software no aprobado o modificaciones no autorizadas en los sistemas, deben ser reportadas e investigadas.

f) Deben realizarse actualizaciones periódicas y monitoreadas del software de detección y reparación de malware. Para el escaneo de computadoras de manera rutinaria con este software el escaneo debe incluir:

   - Escanear cualquier archivo recibido a través de redes o cualquier medio de almacenamiento, para detectar malware antes de su uso.
   - Escanear archivos adjuntos y descargas de correo electrónico en busca de malware.
   - Escanear páginas o sitios web en busca de malware.

g) Establecer procedimientos y responsabilidades de la protección contra el malware en los sistemas, capacitaciones de uso, informes y recuperación de ataques de malware.

h) Preparar un plan para la continuidad del negocio en caso de ataques de malware, como

recuperación de copias de seguridad y la recuperación inmediata del software de la empresa; o en casos más graves, la activación en tiempo corto de un centro de procesamiento de datos alterno con la última información extraída de las copias de seguridad que no fueron infectadas por el malware.

i) Aislar entornos donde la información es muy relevante para la empresa y que puede ser catastrófica en caso de infección, como en este caso lo es el Datacenter principal de la empresa.

8.7.3. Copias de seguridad

8.7.3.1. Copias de seguridad de la información

La información constituye el bien más importante de la empresa por lo que las copias de seguridad de la información como archivos electrónicos críticos, bases de datos de los sistemas, respaldos completos de las imágenes de los sistemas operativos de los servidores o información sensible de los equipos de los usuarios se deben realizar con la frecuencia determinada por la empresa, teniendo en cuenta los siguientes aspectos:

a) Se debe tener un registro completo de los eventos que suceden en el proceso de copia de seguridad para tener la fiabilidad de que el proceso se completó correctamente.

b) La frecuencia con la que se debe hacer el proceso de copia de seguridad dependerá de la empresa teniendo en cuenta de que en caso de un catastro la subida del respaldo deberá producir el menor impacto posible en la operación de la organización. Para los archivos electrónicos críticos, bases de datos de los sistemas o respaldos completos de las imágenes de los sistemas operativos de los servidores, la frecuencia será diaria mientras que para la información sensible de los equipos de los usuarios la frecuencia será semanal. Se respaldará la información y datos almacenados en computadores portátiles de propiedad de la empresa que se encuentran en las oficinas de producción e investigación y desarrollo con una frecuencia diaria debido a la información crítica que almacenan.

c) Los respaldos deben ser ubicados fuera de la organización en un lugar en donde en caso de algún desastre no pudieran ser afectados por este. Para tal efecto se almacena la información de respaldos tanto en un medio de almacenamiento en la red de la empresa (servidor NAS) y en un medio óptico (Discos de tipo Blu-Ray) y se los enviará semanalmente a una bodega de un edificio externo a la organización; con las respectivas seguridades y registro de esta información.

d) Los respaldos deben ser probados regularmente en un ambiente de pruebas para verificar los tiempos de restauración e integridad de los datos respaldados.

e) En caso de que la información sea confidencial se requiere de mecanismos de cifrado.

8.7.4. Registro de actividad y monitoreo

8.7.4.1. Registro y gestión de eventos de actividad

La empresa deberá tener documentado los eventos que registran errores o excepciones, fallas y eventos de seguridad de la información; estos eventos deben ser revisados regularmente y sus registros deberán contener la siguiente información

a) Identificación del usuario.
b) Actividad que se realizó.
c) Fecha, hora y detalle de la actividad.
d) Identificación del dispositivo o equipo que registró la actividad.
e) Registro de intento de acceso exitoso y fallidos.
f) Cambios en la configuración del sistema.
g) Uso de privilegios.
h) Archivos accedidos y el tipo de acceso.
i) Dirección de red y protocolos.
j) Alarmas emitidas por el sistema de control de acceso.
k) Activación y desactivación de sistema de protección, como sistemas antivirus.
l) Registro de transacciones ejecutadas por los usuarios en las aplicaciones.
m) Acción tomada para solventar el problema encontrado.

8.7.5. Control del software en explotación

8.7.5.1. Instalación del software en sistemas de producción

La empresa debe implementar procedimientos para una correcta instalación o actualización del software en los sistemas operativos de la organización para lo cual debe tener en cuentas las siguientes pautas:

a) Las actualizaciones de los sistemas operativos solo la debe realizar los administradores del sistema para evitar posibles inconvenientes al momento de realizar esta operación.
b) Los computadores con sus respectivos sistemas operativos solo deben tener el ejecutable de la aplicación y no los códigos fuentes de la misma.
c) Para poder implementar una actualización o instalación de un sistema se deben realizar pruebas rigurosas las cuales deben evaluar la calidad del mismo, con parámetros que midan su usabilidad, la seguridad y el impacto que tendrá en otras aplicaciones además de su facilidad de uso.
d) Se debe tener una documentación de control de actualización del sistema en donde se detallan las nuevas funcionalidades, arreglos en la codificación actual y el desarrollador o

analista que realizo el respectivo análisis para el cambio en las nuevas funciones del sistema, además al realizar un cambio tenemos que tener un procedimiento para respaldar la versión anterior a la actualización para que en caso de que se requiera se pueda regresar al momento previo a la actualización.

e) Toda actualización del software deberá ser archivada junto con toda la información sobre dicha versión como procedimientos, detalles de configuración, recopilación de requerimientos, diagramas, cambios de funcionalidad, etc.

8.7.6. Gestión de la vulnerabilidad técnica

8.7.6.1. Gestión de vulnerabilidades técnicas

Las vulnerabilidades técnicas de los sistemas de la empresa deberán ser identificadas de manera oportuna, la inherencia que tienen estas en la organización y las medidas que deben tomarse en caso de que ocurran estas vulnerabilidades, se deberá detallar en un documento con un listado de sistemas que posee la empresa además del proveedor del software, los números de versión, el estado actual de la implementación del sistema y el responsable del sistema dentro de la empresa que deberá seguir las siguientes recomendaciones en caso de que se encuentren vulnerabilidades:

a) Se deberá definir el o los responsables de la vigilancia de las vulnerabilidades así como el riesgo, parches aplicados, el responsable deberá tener un conocimiento apropiado sobre el sistema que este hecho cargo para poder actuar de manera oportuna en caso de que ocurra tal vulnerabilidad.

b) En caso de que ocurra la vulnerabilidad técnica se deberá identificar los riesgos asociados a esta y las acciones a tomar; dichas acciones podrían implicar un parcheo o aplicar otros controles, en caso de que se aplique un parche se verificara que este venga de una fuente legitima y se evaluara los riesgos asociados con la instalación para demostrar que sean efectivos y con esto no dar lugar a efectos secundarios de los cuales no se puedan controlar luego. En caso de que no exista un parche se deberá aplicar controles como por ejemplo:

- Desactivar servicios
- Adaptar o agregar controles de acceso
- Mayor monitoreo para detectar ataques reales
- Crear conciencia a las personas sobre las vulnerabilidades
- Registro sobre los procesos emprendidos en dicha vulnerabilidad
- El proceso de gestión de la vulnerabilidad técnica deberá ser monitoreado y evaluado regularmente en orden para asegurar su eficiencia
- Los sistemas de alto riesgo deberán ser evaluados prioritariamente
- Se debe definir un procedimiento para abordar la situación en la que se ha identificado una vulnerabilidad, en caso de que sea una vulnerabilidad nueva la

organización deberá identificar los riesgos relacionados con esta y definir las acciones correctivas apropiadas.

8.7.6.2. Restricciones en la instalación de software

Uno de los puntos a tomarse como críticos es la instalación indebida de sistemas en la organización por lo cual la empresa debe aplicar una política estricta sobre qué tipo de software puede ser instalado por el usuario; este listado y autorización la dará el departamento de TI de la empresa. Se debe considerar siempre el principio de mínimo privilegio el que deberá ser aplicado en los sistemas operativos de los usuarios y con esto se podrá restringir la instalación inadecuada de sistemas y se les permitirá realizar ciertas instalaciones que no conlleven a poner en riesgo el funcionamiento normal de la empresa como por ejemplo actualizaciones, parches de seguridad para el software ya instalado, además se prohibirá la instalación de software de uso personal, juegos y software que puede ser considerado potencialmente malicioso. Estos privilegios deben otorgarse siempre teniendo en cuenta los roles o funciones de los usuarios.

8.8. Seguridad en las Telecomunicaciones

8.8.1. Gestión de la seguridad en al redes

8.8.1.1. Controles de red

Las redes deberán ser administradas y controladas para así proteger la información de las aplicaciones correspondientes. Deberán implementarse controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado; para ello se considera lo siguiente:

a) El personal de TI es el único autorizado para gestionar y configurar los dispositivos de seguridad perimetral de la red.
b) Los sistemas o servicios en la red deben ser autenticados.
c) La conexión de los sistemas a la red debe estar restringida solamente con los puertos y servicios necesarios.
d) Se deberán establecer los controles necesarios para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o por redes inalámbricas para proteger los sistemas y aplicaciones conectados.
e) Ningún usuario externo se podrá conectar a la red interna de la empresa, salvo las excepciones autorizadas por la gerencia general o el jefe de TI.

8.8.1.2. Mecanismos de seguridad asociados a servicios en red

Deberán identificarse las disposiciones de seguridad necesarias para servicios particulares, como

características de seguridad, niveles de servicio y requisitos de gestión; la empresa debe asegurarse de que los proveedores de servicios de red implementen estas medidas en sus contratos. Los servicios de red podrían incluir la provisión de conexiones, servicios de red privada y servicios de valor agregado como soluciones de seguridad de red gestionada, por ejemplo firewalls y sistemas de detección o prevención de intrusiones (IDS, IPS).

8.8.2. Intercambio de información

8.8.2.1. Políticas y procedimientos de intercambio de información

Deberán existir políticas, procedimientos y controles formales de transferencia de información para proteger la información mediante el uso de medios de comunicación; para ello se deberá considerar los siguientes elementos:

a) Protección de la información transferida de la interceptación, copia, modificación, desvío y destrucción. Esta protección se la realizará con certificados de seguridad en las aplicaciones web por ejemplo y encriptado las comunicaciones de datos con mecanismos de encriptación como algoritmos tipo 3DES, AES, etc.
b) Software antivirus para la detección y protección contra malware que pueden transmitirse a través del uso de dispositivos extraíbles.
c) Software antispam y de prevención de pérdida de datos o Data Loss Prevention (DLP) para proteger la información sensible por medio de archivos adjuntos.
d) Dentro de la red corporativa en las áreas de producción queda prohibido para los empleados y externos, salvo autorización por escrito de la gerencia general, el uso de la red pública (Internet) para la utilización de redes sociales como Facebook, twitter, instagram, etc.
e) Concientizar y capacitar al personal para que tome las precauciones apropiadas para no revelar información confidencial a través de las aplicaciones de red.

8.8.2.2. Acuerdos de intercambio

Los acuerdos o contratos con externos deberán abordar la transferencia segura de información entre la organización y las partes externas; para ello se deberá considerar lo siguiente:

a) Procedimientos para garantizar la trazabilidad y el no repudio de la información, como por ejemplo una firma electrónica.
b) Responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de datos.
c) Niveles aceptables de control de acceso.
d) Acuerdos de confidencialidad;

e) Estándares de identificación de mensajería;
f) Conexiones a la red corporativa solo podrán realizarse a través de VPNs seguras proveídas por el departamento de TI de la empresa. Estarán prohibidos el uso de otros programas de conexión y escritorio remoto.

8.8.2.3. Mensajería electrónica

La información involucrada en mensajes electrónicos debe estar protegida adecuadamente. Por ende las consideraciones de seguridad de la información para la mensajería electrónica deben incluir lo siguiente:

a) Proteger los mensajes del acceso no autorizado, la modificación o la denegación del servicio con los medios disponibles que dispone la empresa.
b) Asegurar el direccionamiento correcto y el transporte del mensaje.
c) Fiabilidad y disponibilidad del servicio.
d) Consideraciones legales, como por ejemplo, requisitos para firmas electrónicas.
e) Se prohíbe para los empleados y contratistas externos, salvo autorización por escrito de la gerencia general, el uso de la red pública (Internet) para la utilización de redes sociales públicas como Facebook, twitter, instagram, etc.
f) Solamente se autoriza el uso de redes sociales internas de la empresa, como la del sistema de Recursos Humanos, que se dará a conocer en las inducciones al personal con su respectiva autenticación, respetando los controles de contraseñas establecidos en esta política de seguridad.

8.8.2.4. Acuerdos de confidencialidad y secreto

Los acuerdos de confidencialidad o no divulgación deberán abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables tanto a partes externas como a los trabajadores de la empresa; sobre todo a los que trabajen en áreas críticas como producción o investigación y desarrollo. Los elementos del acuerdo de confidencialidad deben seleccionarse o agregarse teniendo en cuenta el acceso o manejo permitido de la información confidencial. Para identificar los requisitos de confidencialidad, se deben considerar los siguientes elementos:

a) Los requisitos para la confidencialidad o los acuerdos de confidencialidad que reflejen las necesidades de la organización para la protección de la información deben identificarse, revisarse periódicamente y documentarse.
b) Responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada.

c) Propiedad de la información, secretos empresariales y propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial; aquí se debe considerar la mayoría de la información que maneja el área de investigación y desarrollo dentro de producción.
d) El uso permitido de la información confidencial y los derechos del signatario para usar información.
e) El derecho de auditar y monitorear actividades que involucran información confidencial;
f) El proceso de notificación e informe de divulgación no autorizada o fuga de información confidencial.
g) Los términos para que la información sea devuelta o destruida al momento del cese del contrato.
h) El tiempo por el cual, luego de la finalización del contrato de trabajo, el trabajador o proveedor externo se obliga a respetar el acuerdo de confidencialidad.
i) Las acciones y sanciones económicas esperadas a tomar en caso de incumplimiento del acuerdo.

8.9. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

8.9.1. Requisitos de Seguridad de los Sistemas de Información

8.9.1.1. Análisis y especificación de los requisitos de seguridad

Los requisitos de seguridad deberán ser estrictos para nuevos sistemas de información o mejoras de los sistemas ya existentes utilizando diversos métodos como, descripción de cumplimiento de requisitos, modelos de amenazas, revisiones de incidentes o uso de umbrales de vulnerabilidad. Los resultados deberán ser documentos y revisados por todas las partes interesadas además de cuantificar un valor comercial por toda la información involucrada y el posible impacto comercial negativo por falta de seguridad adecuada.

La identificación y gestión de requisitos de seguridad deberían integrarse en las primeras etapas del desarrollo de los sistemas de información, en la etapa de diseño se puede realizar los cambios necesarios que pueden conducir a soluciones más efectivas y rentables; además debemos considerar lo siguiente:

a) Autentificación de los usuarios al ingresar al sistema por medio de un usuario y contraseña.
b) Informar a los usuarios sobre sus deberes y responsabilidades dentro del sistema.
c) Manejo de privilegios para determinar los accesos de los usuarios.
d) Protección de los activos involucrados de la empresa con respecto a la disponibilidad, confidencialidad e integridad de la información.

e) Monitoreo de las transacciones realizadas en el sistema para evitar fugas de información.

8.9.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas

La información que utilizan aplicaciones que pasan a través de redes públicas debe estar protegida contra actividad fraudulenta, divulgación y modificación no autorizada de la información.

a) Se requiere que existe autentificación de cada usuario involucrado en el intercambio de información por medio de aplicaciones que utilizan redes públicas.
b) Cumplir los requisitos de confidencialidad, integridad, pruebas de envió de la información.
c) Cifrar la información enviada para evitar capturas no autorizadas de la información.
d) Evitar la pérdida o duplicidad de la información enviada
e) Responsabilidad compartida con cualquier tipo de información fraudulenta

8.9.1.3. Protección de las transacciones por redes telemáticas.

La información que utiliza servicios de aplicaciones debe estar protegida para evitar una transmisión incompleta, enrutamiento incorrecto o divulgación no autorizada. Además se debe tomar en cuenta las siguientes consideraciones.

a) El uso de firmas electrónicas entre las partes involucradas para verificar la veracidad de la información.
b) Proteger los protocolos utilizados en la comunicación entre las partes involucradas.
c) Garantizar que el almacenamiento de la información en la intranet de la organización se encuentre fuera de cualquier acceso publico

8.9.2. Seguridad en los Procesos de Desarrollo y Soporte

8.9.2.1. Política de desarrollo seguro de software

La política para el desarrollo de software debe aplicar a todos los sistemas creados dentro de la organización. Un desarrollo seguro debe considerar los siguientes aspectos.

a) Seguridad en el entorno de desarrollo.
b) Seguridad en la metodología de desarrollo de software.
c) Codificación segura para cada lenguaje de programación utilizado.
d) Seguridad en la fase de diseño.
e) Puntos de control de seguridad dentro de los hitos del proyecto.
f) Seguridad en el control de versiones.
g) Conocimiento requerido sobre la seguridad de la aplicación.
h) Capacidad de los programadores para encontrar y corregir vulnerabilidades.

i) Seguridad en las pruebas del sistema en desarrollo.
j) Estándares de codificación segura.

Estas políticas deberán ser utilizadas tanto para nuevos desarrollos así como también para reingenierías o adaptaciones de software desarrollados en la empresa.

8.9.2.2. Procedimientos de control de cambios en los sistemas

Los cambios dentro del desarrollo del software deberán estar correctamente documentados y aplicados para garantizar la integridad del sistema y posibles mantenimientos posteriores.

La implementación de nuevos sistemas o cambios significativos en sistemas ya existentes deben seguir un proceso formal con una documentación detallada, pruebas, control de calidad e implementación; también se deberá incluir una evaluación de riesgos, un análisis sobre el impacto de los cambios y controles de seguridad para un correcto funcionamiento del sistema.

Los procedimientos de control de cambios de software deberán incluir lo siguiente:

a) Registro de los usuarios que solicitan los cambios en el sistema.
b) Revisar los controles y procedimientos de integridad para verificar que no se vean afectados por los cambios.
c) Verificar el sistema para determinar los recursos que son afectados por el cambio como bases de datos, procedimientos almacenados, servicios, información y hardware.
d) Verificar la seguridad después de los cambios para determinar posibles debilidades del sistema.
e) Pedir la revisión y autorización en un ambiente de prueba a los usuarios que solicitaron los cambios antes de ponerlos en productivo.
f) Garantizar que la documentación se actualice y almacene correctamente después de los cambios que se realizaron en el sistema.
g) Mantener un registro de las versiones para todas las actualizaciones del software.
h) Registro de auditoria en el sistema de todos los cambios realizados en el código fuente.
i) Realizar las pruebas pertinentes y necesarias después de los cambios para determinar que no se vean afectados ningún otro proceso o funcionalidad del sistema.
j) Garantizar que la implementación de los cambios se realicen en un horario que no comprometa el correcto funcionamiento de las operaciones de la empresa.

8.9.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

En caso de cambio o actualización del sistema operativo en servidores o equipos de usuarios, se deberá verificar y probar que las aplicaciones críticas de la organización adquiridas o

desarrolladas internamente no sufran un impacto significativo en la seguridad. Este proceso debe incluir:

a) Una revisión de los procedimientos de control e integridad de la aplicación para garantizar que no hayan sido perjudicados por el cambio del sistema operativo.
b) Asegurar el tiempo necesario para realizar las pruebas y revisiones antes de la implementación de la actualización o cambio del sistema operativo.
c) Garantizar que si se realizan cambios en los sistemas operativos, estos funcionen correctamente en el nuevo sistema operativo y no perjudique o afecte el funcionamiento del negocio.

8.9.2.4. Restricciones a los cambios en los paquetes de software

Es recomendable no realizar cambios en los paquetes de software suministrados por proveedores externos; sin embargo en caso de ser necesarios deberá ser estrictamente controlado y se considerará los siguientes lineamientos:

a) Riesgo de que los controles y procesos integrados se vean comprometidos.
b) Se debe obtener el consentimiento del proveedor.
c) La posibilidad de que los cambios en los paquetes los realice el mismo proveedor como una actualización del paquete.
d) Responsabilidad de la empresa en los mantenimientos del paquete; se debe cumplir con las cláusulas estipuladas en los contratos de software, si se indica que la empresa no puede realizar ningún cambio en el software del proveedor, es el proveedor quien obligatoriamente deberá realizar actualizaciones o cambios en los paquetes de software.
e) Revisar la compatibilidad con otro software que utilice el paquete.
f) Realizar una copia de seguridad antes de realizar los cambios en el paquete.
g) En caso de existir parches o actualizaciones del paquete se deberá realizar pruebas en un ambiente de pruebas separado del productivo.

8.9.2.5. Uso de principios de ingeniería en protección de sistemas

Se debe establecer, documentar y aplicarse la ingeniería de software y sistemas seguros a cualquier implementación de sistema de información mediante el diseño de todas las capas de arquitectura como datos, negocios, aplicaciones y la tecnología utilizada, equilibrando la necesidad de seguridad de la información con la de necesidad de accesibilidad. Para los nuevos desarrollos se analizara los riesgos de seguridad así como también el diseño contra patrones de ataque; conocidos estos procedimientos se deberán revisar y auditar regularmente durante y después del desarrollo para garantizar los mejores estándares de seguridad en los procesos de

ingeniería.

8.9.2.6. Seguridad en entornos de desarrollo

Las organizaciones deben garantizar la seguridad en los entornos de desarrollo teniendo en cuenta que un entorno de desarrollo incluye personas, procesos, tecnologías asociados al sistema en desarrollo e integración. Los entornos de desarrollo deben considerar lo siguiente:

a) Controles de seguridad implementados por la empresa que respalda el desarrollo del sistema.
b) Confiabilidad del personal que trabaja en el ambiente de desarrollo; para ello todo el personal de TI debe tener firmados sus respectivos acuerdos de confidencialidad en sus contratos de trabajo.
c) Aislar el entorno de desarrollo con respecto al productivo.
d) Control de acceso al entorno de desarrollo.
e) Sensibilidad de los datos que se utilizaran en el ambiente de desarrollo; en lo posible no utilizar la información sensible o crítica de la empresa.
f) Tener en cuenta todos los requerimientos internos o externos para los sistemas a desarrollarse.
g) Copias de seguridad de los avances y código fuente de proyectos de desarrollo en ubicaciones fuera del ambiente de desarrollo.
h) Proporcionar por parte de la empresa los procesos claramente documentados sobre los entornos de desarrollo al personal de TI involucrado.

8.9.2.7. Externalización del desarrollo de software

En caso de contratar a personal externo para el desarrollo de software la organización deberá considerar los siguientes puntos:

a) Los acuerdos de licencia, la propiedad del código fuente, los derechos de actualizaciones de software y el mantenimiento del mismo; en lo posible deben quedar en poder y custodia de la empresa.
b) Acuerdos contractuales para prácticas de diseño, codificación y pruebas.
c) Pruebas de seguridad contra amenazas y vulnerabilidades.
d) Pruebas de calidad, funcionalidad y precisión de los entregables.
e) Derecho contractual de auditar procesos y controles de desarrollo.
f) Documentación de los procesos implementados en el sistema.

8.9.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas

Las pruebas de funcionalidad de seguridad durante el desarrollo de software se deben dar tanto para nuevos sistemas como para actualizaciones de sistemas ya existentes en su etapa de desarrollo, detallando un calendario de actividades de pruebas y resultados esperados bajo un rango de condiciones; si el desarrollo es interno las primeras pruebas lo puede hacer el equipo de desarrollo para luego realizar pruebas independientes con los usuarios indicados en un ambiente de pruebas separado para asegurar que el sistema funcione como se espera. La cantidad de pruebas necesarias deben ser proporcionales de acuerdo a la importancia del software desarrollado es decir si el sistema va a tener un grado alto de confidencialidad deberá tener un mayor número de pruebas y verificación de los datos.

8.9.2.9. Pruebas de aceptación

Las pruebas de aceptación se deben dar tanto para nuevos sistemas como para actualizaciones de sistemas ya existentes en donde se debe considerar la seguridad de la información, el cumplimiento de las políticas de desarrollo de software, pruebas con los sistemas que se involucran con el desarrollo. La organización puede aprovechar herramientas automatizadas como herramientas de análisis de código o escáneres de vulnerabilidades.

Las pruebas deben realizarse en un ambiente de pruebas realista con una copia de los datos que se utilizan en el ambiente productivo mientras no sean confidenciales de ser factible, para verificar que el sistema no tenga vulnerabilidades y que las pruebas sean confiables con datos reales.

8.9.3. Datos de Prueba

8.9.3.1. Protección de los datos utilizados en pruebas

La empresa deberá seleccionar cuidadosamente los datos de prueba tratando de evitar entregar datos que contengan información personal o cualquier otra información confidencial como la información de productos, clientes, fórmulas o recetas, etc. Se debe tomar en cuenta las siguientes pautas cuando utilizamos datos operativos para fines de prueba:

a) En caso de hacer uso de información protegida o confidencial al terminar las pruebas se deberá eliminar completamente los datos entregados.
b) Los procedimientos de control de acceso que se aplican a ambientes productivos también se deberá aplicar ambientes de pruebas.
c) Autorización del jefe de TI cada vez que se copie información operacional al ambiente de pruebas.
d) La copia y el uso de la información operativa en pruebas se debe registrar para una futura auditoria.

e) En caso de trabajar con datos confidenciales como formulaciones o recetas de la empresa por ejemplo, se deberá tener mucho cuidado con el personal que realice pruebas; solo el personal de TI o los usuarios propietarios de esa información que tengan acuerdos de confidencialidad serán los encargados de realizar dichas pruebas con datos críticos o confidenciales.

8.10. Relaciones con Proveedores

8.10.1. Seguridad de la Información en las Relaciones con proveedores

8.10.1.1. Política de seguridad de la información para proveedores

La presente política para mitigación de riesgos de seguridad debe ser conocida por los proveedores. La compañía debe mantener un registro con la siguiente información:

- Identificación y registro de los proveedores y el tipo de servicio de TI que prestan.
- Definir el tipo de información a la que el proveedor tendrá acceso y que deberá constar en el respectivo contrato, además de monitorear y controlar el acceso a dicha información y acordar los requerimientos mínimos de seguridad de acceso a las instalaciones, equipos e información de la empresa con dichos proveedores.

Una vez establecidas las relaciones con el proveedor, el personal de seguridad de TI deberá capacitar y concientizar al personal involucrado en la interacción con el proveedor respecto a los controles que se deben tener basados en el tipo y nivel de acceso del proveedor a la información.

8.10.1.2. Tratamiento del riesgo dentro de los acuerdos con el proveedor

Los acuerdos con los proveedores deben ser documentados para asegurarse que no existan malentendidos entre la compañía y sus proveedores de productos o servicios.

Al momento de contratar productos o servicios que puedan manejar información sensible o pongan en riesgo la seguridad de la misma, incluir un acuerdo de confidencialidad con una o varias cláusulas con las siguientes consideraciones:

a) Descripción clara de la información a ser suministrada o accedida por parte del proveedor y los métodos para suministrar o acceder a dicha información.
b) Autorización por escrito por parte de la Gerencia General, del Gerente de producción y del Jefe de TI de la información a ser suministrada o accedida por parte del proveedor.
c) Requerimientos legales y regulatorios, incluyendo protección de datos, derecho de propiedad intelectual y la descripción de cómo van a ser asegurados los datos.
d) Obligatoriedad de cada parte de implementar y acordar el conjunto de controles para el

control de acceso, revisión, monitoreo, reportes y auditoría.

e) Reglas de uso aceptable e inaceptable de información entregada a proveedores.

f) Procesos legales de resolución de conflictos en caso de tenerlos.

8.10.1.3. Cadena de suministro de tecnología de información y comunicaciones

a) Los acuerdos con los proveedores asociados con la cadena de suministro de TI y la seguridad adyacente deben ser propagados por parte de los proveedores en caso que ellos subcontraten partes de sus servicios de tecnología o comunicaciones a terceros.

b) Llevar seguimiento diario de los componentes de funcionalidad crítica que son desarrollados o compilados fuera de la organización por parte de los proveedores.

c) En caso que se necesite compartir información a la cadena de suministro, esta debe ser asignada a un responsable con firma respectiva y un acuerdo de confidencialidad.

d) Determinar los posibles riesgos para componentes que ya no estarán disponibles el momento que el proveedor ya no tiene una relación con la empresa o su tecnología sea obsoleta. En este caso se establece que los acuerdos de confidencialidad se extiendan por un tiempo determinado luego de finalizadas las relaciones contractuales con los proveedores.

8.10.2. Gestión de la prestación del servicio por suministradores

8.10.2.1. Supervisión y revisión de los servicios prestados por terceros

El monitoreo y la revisión de servicios debe asegurar que los términos y condiciones de los requerimientos de seguridad estipulados en los contratos y acuerdos de confidencialidad; así como los *Acuerdos de Nivel de Servicio* (SLA) sean aceptados por los proveedores y que las incidencias de seguridad sean manejadas adecuadamente. Para ello se debe:

a) Monitorear y registrar los niveles de rendimiento de los servicios para verificar el cumplimiento de los acuerdos.

b) Revisar la información acerca de los incidentes de seguridad, problemas operacionales, auditorías del proveedor y fallas o interrupciones del servicio prestado.

c) Respetar los canales de comunicación previstos y los tiempos establecidos para la solución de problemas mediante un Acuerdo de Nivel de Servicio (SLA) firmado con el proveedor.

d) Resolver y administrar los problemas identificados y notificados al proveedor.

8.10.2.2. Gestión de cambios en los servicios prestados por terceros

Los cambios en el suministro de servicios por parte de los proveedores deben ser controlados y registrados, con conocimiento por escrito tanto del proveedor como de la empresa, teniendo en

cuenta la criticidad de la información de la empresa, sistemas y procesos. Se deben considerar los siguientes aspectos:

a) Cambios en los acuerdos con el proveedor.
b) Cambios realizados por la empresa para implementar mejoras en los servicios actualmente prestados, instalación y configuración de nuevos servicios, modificaciones en las políticas o procesos de la empresa, modificación de controles para resolver incidentes de seguridad de la información y mejorar la seguridad.
c) Los cambios de servicios para implementar funcionalidades o mejoras en las redes, uso de nuevas tecnologías, adopción de nuevos productos o versiones, cambios en la ubicación física de los proveedores deben ser notificadas por escrito a la empresa, y de ser necesario presentados como anexos en los respectivos contratos con los proveedores.

8.11. Gestión de incidentes de Seguridad de la Información

8.11.1. Gestión de incidentes y mejoras a la seguridad de la información

8.11.1.1. Responsabilidades y procedimientos

La administración de responsabilidades y procedimientos para la seguridad de la información debe ser establecida para asegurar una efectiva respuesta a los incidentes de seguridad de información. Considerar:

a) Los procedimientos tales como plan de respuesta ante incidentes, monitoreo, detección y reporte de incidencias, manejo de evidencia forense y recuperación de incidentes deben ser comunicados dentro de la organización.
b) Los procedimientos establecidos deben asegurar que el personal competente y asignado maneje los temas de seguridad de información dentro de la compañía y que haya un contacto apropiado con autoridades y grupos externos de interés relacionado a los incidentes de seguridad.
c) En la empresa, el *Equipo de Gestión de Seguridad de la Información*, siendo un equipo de trabajo integrado por profesionales internos de la empresa de las áreas de TI y auditoría, son quienes llevarán la responsabilidad de elaborar los procedimientos para la seguridad de la información y velar por su cumplimiento, teniendo reuniones mensuales para tratar los incidentes de seguridad o incumplimientos de la política de seguridad y sus controles; así como diseñar, implementar y socializar nuevos proyectos de seguridad en beneficio de la empresa.

8.11.1.2. Notificación de eventos de seguridad de información

Todos los empleados y contratistas externos deben tener en cuenta su responsabilidad de reportar problemas de seguridad de la información lo antes posible al departamento de TI de la empresa. Estas situaciones por ejemplo deben ser consideradas como problemas de seguridad: control inefectivo de seguridad, brechas en la integridad y confidencialidad de la información, errores humanos, incumplimientos de las políticas, cambios no controlados en sistemas, fallos en hardware o software, violaciones de accesos o de los derechos de usuarios o cualquier fallo o anomalía inesperada en la información, en las aplicaciones o en el hardware de la empresa.

8.11.1.3. Notificación de puntos débiles de seguridad

a) Todos los empleados y contratistas deben reportar los problemas a los integrantes del departamento de TI, quienes son los encargados de la seguridad de información, lo más pronto posible.
b) Los integrantes del departamento de TI deben identificar y registrar los incidentes de seguridad con la fecha, el usuario que los reporta, el detalle del incidente y las posibles causas y acciones a tomar para solucionar el problema; todos estos incidentes se los notificará formalmente en las respectivas reuniones mensuales al *Equipo de Gestión de Seguridad de la Información* para que se tomen acciones preventivas y correctivas, con inversiones autorizadas de ser el caso por la gerencia general o el comité directivo.
c) No intentar probar debilidades de seguridad sospechosas en el ambiente productivo de la red. Se considera como un uso inadecuado de los sistemas y podría causar daños graves a los sistemas de información. Toda prueba de seguridad debe ser previamente puesta en conocimiento y autorizada por el equipo de gestión de seguridad de la información.

8.11.1.4. Valoración de eventos de seguridad de la información y toma de decisiones

El personal del departamento de TI será el primer punto de contacto y valorará cada evento de seguridad de la información y determinará si se trata de un incidente de seguridad; esta clasificación ayudará a identificar el impacto del incidente y registrar estos detalles para referencias futuras. Se podrán tomar acciones inmediatas de ser necesario, solamente con el conocimiento y autorización del Jefe de TI o el Gerente General de la empresa. Los incidentes y acciones inmediatas tomadas se las notificará formalmente en las respectivas reuniones mensuales al *Equipo de Gestión de Seguridad de la Información* quienes evaluarán y dictarán acciones preventivas y correctivas definitivas, o avalarán y apoyarán la solución tomada por el personal del departamento de TI.

8.11.1.5. Respuesta a los incidentes de seguridad

Como respuesta ante los incidentes y eventos de seguridad, los usuarios y el departamento de TI

deben considerar los siguientes aspectos:

a) Recopilar evidencias tan pronto como ocurra el incidente.
b) Dirigir la información para un análisis forense en caso de ser necesario.
c) Asegurarse que todas las actividades de respuesta queden registradas.
d) Dar a conocer el incidente de seguridad de la información al *Equipo de Gestión de Seguridad de la Información*, quienes deben tener conocimiento dentro de la compañía. A su vez este equipo será el encargado de informar sobre los incidentes y soluciones tomadas al *Comité Directivo* de la empresa.
e) Una vez superado el incidente, se debe realizar un cierre formal documentado.

8.11.1.6. Aprendizaje de los incidentes de seguridad de la información

Se deben establecer mecanismos para obtener los tipos y costos de los incidentes de seguridad de información reportados, los mismos que deberán ser monitoreados. Esto ayudará a determinar si es necesario agregar o mejorar los controles para reducir la frecuencia y costo de los incidentes.

8.11.1.7. Recopilación de evidencias

La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información, lo que puede servir como evidencia. Los procedimientos para tratar evidencias deben proveer su identificación, recopilación y preservación de acuerdo a su tipo y estado. Debe considerarse una cadena de custodia, la seguridad de las evidencias, la seguridad y responsabilidades del personal y los requerimientos legales de la recopilación de evidencias; además se deben desarrollar y seguir los procedimientos internos cuando se trata de evidencia para efectos de acciones disciplinarias y legales.

De ser posible, se deberán buscar certificaciones u otros medios relevantes de calificación de personal y de herramientas de informática forense, a fin de fortalecer el valor de la evidencia preservada. La evidencia forense puede trascender las fronteras organizacionales o jurisdiccionales. En tales casos, se debe garantizar que la empresa tenga derecho a recopilar la información requerida como evidencia forense.

8.12. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

8.12.1. Continuidad de la seguridad de la información

8.12.1.1. Planificación de la continuidad de la seguridad de la información.

La empresa debe determinar sus requisitos de seguridad de la información y la continuidad de las

operaciones de Tecnologías de Información de la empresa ante situaciones adversas, como un desastre natural o provocado por el hombre con o sin intencionalidad. Esto se debe determinar en un Plan de Continuidad de Negocio (BCP o Business Continuity Plan por sus siglas en inglés) que la empresa deberá implementar y elaborar, considerando:

En ausencia de la operación normal del negocio y ante una situación de contingencia para desastres, los requisitos y políticas de seguridad de la información siguen siendo los mismos en estas situaciones adversas, en comparación con las condiciones de operación normales.

8.12.1.2. Implantación de la continuidad de la seguridad de la información.

La empresa debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa dentro del Plan de Continuidad de Negocio (BCP). Este documento debe considerar la continuidad de los servicios y sistemas informáticos para el departamento de producción e investigación y desarrollo, considerando los requerimientos de seguridad en equipos de respaldo y energía instalados en un sitio alterno de procesamiento de información.

8.12.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

El equipo de gestión de seguridad de la información de la empresa debe verificar los controles de continuidad de la seguridad de la información establecidos cada cierto intervalo de tiempo a fin de garantizar que sean válidos y efectivos en situaciones de contingencia.

Se deben integrar la verificación de los controles de continuidad de seguridad de la información con las pruebas de continuidad de negocio o de recuperación ante desastres de la organización.

8.12.2. Redundancias

8.12.2.1 Disponibilidad de instalaciones para el procesamiento de la información

a) Las instalaciones de procesamiento de información en la empresa deben implementarse con redundancia suficiente para cumplir con el requisito de disponibilidad de la información.
b) La empresa debe identificar los requisitos indispensables para la disponibilidad de los sistemas de información. Cuando no se pueda garantizar la disponibilidad utilizando la infraestructura existente, se deben considerar redundancia en los componentes o en la infraestructura completa.
c) Los sistemas de información redundantes deben ser probados de manera semestral para

asegurar que la falla de un componente o equipo funcione con la redundancia necesaria según lo previsto.

d) Se debe considerar la redundancia de equipos informáticos y equipos de alimentación eléctrica ininterrumpida (UPS).

e) Se deben tener en bodega los repuestos más críticos y susceptibles para los equipos en caso de daños o contingencias.

8.13. Cumplimiento

8.13.1. Cumplimiento de los requisitos legales y contractuales

Se debe dar estricto cumplimiento a las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.

8.13.1.1. Identificación de la legislación aplicable

Todos los requisitos legales, reglamentarios y contractuales relevantes deben identificarse explícitamente, documentarse y mantenerse actualizados para cada sistema de información o servicio contratado para la empresa. Los controles específicos y las responsabilidades individuales para cumplir estos requisitos también deben definirse y documentarse en los contratos.

Al momento, esta política se sustenta en los siguientes instrumentos legales:

El Reglamento Interno de Trabajo vigente de la empresa; en el capítulo V: “De las Obligaciones y Prohibiciones de los Trabajadores”, en el Artículo 25, indica los siguientes literales sobre las obligaciones para los trabajadores de la empresa:

El Literal *“a”* indica explícitamente: “Cumplir y acatar el presente Reglamento, y todas las normas e instrucciones que para el desarrollo de sus labores y/o protección le haya sido instruido en la empresa.”

El literal *“c”* del mismo Artículo 25 del Reglamento Interno de Trabajo de la empresa expresa sobre la confidencialidad de la información: “No comunicar ni hacer conocer a terceros, salvo autorización expresa o escrita, la información que tengan sobre su trabajo, en especial, las instrucciones de carácter privado o reservado cuya divulgación puede ocasionar perjuicios a la Empresa”.

Así mismo el literal *“ll”* hace referencia al cuidado de la información confidencial de la empresa, indicando que se debe “Guardar escrupulosamente la información confidencial: técnicas comerciales y administrativas; procesos y recetas que son propiedad de la empresa, quedando

denominado como “Documento Controlado” la información confidencial, sin que se pueda duplicar o sacar fuera de la Empresa, ni siquiera copia simple del mismo documento controlado, sin el debido permiso o autorización del superior, caso contrario se considerará este acto como una falta grave al presente reglamento interno.”

El literal *“d”* del Artículo 25 del Reglamento Interno de Trabajo de la empresa hace referencia al cuidado y uso de los equipos de trabajo, entre ellos los equipos informáticos asignados a los empleados: “Cuidar de los equipos, herramientas, materias primas, productos elaborados, etc. de la empresa, que han sido puestos a su disposición y utilizarlos exclusivamente para su trabajo y mantenerlos en buen estado, excepto por su desgaste normal. El trabajador responderá personal y pecuniariamente por la pérdida, daño o destrucción de los implementos de trabajo, materiales, maquinaria o equipos informáticos como computadores, impresoras, dispositivos móviles o cualquier otro equipo de propiedad de la empresa confiados bajo su responsabilidad y cuidado.”

El literal *“r”* del Artículo 25 del Reglamento Interno de Trabajo de la empresa se refiere a los controles dispuestos por la empresa para las copias no autorizadas del software, donde se indica: “Acatar y cumplir con los sistemas de control establecidos por la empresa para prevenir la realización o uso de copias no autorizadas de software, así como permitir la verificación de estos estándares a través de las medidas pertinentes dictadas para el efecto.”

En el literal *“s”* del mismo Artículo 25 se complementa con el uso e instalación del software en la empresa: “Los empleados deberán usar el software solamente de la empresa establecido con un contrato de licencia tanto en las redes de área local como por Internet, y en caso de duda sobre si un empleado puede copiar o usar un programa de computadora, deberá elevarse la consulta respectiva al departamento de TI de la empresa o a la Gerencia General.”

En el Artículo 26 del Reglamento Interno de Trabajo de la empresa donde se establecen las Prohibiciones para los trabajadores, se especifican los siguientes literales para proteger los activos de información de la empresa:

Literal *“a”*: “Retirar o tratar de retirar del establecimiento cualquier pertenencia de las instalaciones de la empresa sin la debida autorización escrita, o conservar sin autorización artículos, productos, computadores, herramientas, etc. que no han sido asignados a su cargo. La empresa podrá establecer los sistemas de revisión y control que estime conveniente.”

Literal *“e”*: “Utilizar sin la autorización correspondiente, máquinas, herramientas, materiales, computadores o equipos informáticos en general u otros enseres o equipos de la empresa, para fines de carácter particular que no sean para el desarrollo de sus tareas en la empresa.”

Literal *“f”*: “Siendo instrumentos de trabajo los teléfonos, computadores, copiadoras y

dispositivos móviles inteligentes que son de propiedad de la empresa, su utilización para fines particulares y que no revistan caracteres de urgencia, está prohibido sin la debida autorización previa por escrito."

Literal *"i"*: "Copiar o usar copias de software no autorizado."

Literal *"l":* "Suministrar a terceras personas ajenas a la Empresa, informes de carácter técnico, de producción, investigación y desarrollo, producción, negociación, comercialización o de cualquier otra naturaleza, que deban mantenerse como reservados o como secretos."

El Reglamento interno de Trabajo es aprobado por el Ministerio de Trabajo y se sustenta a su vez en el punto 12 del Artículo 42 del Código de Trabajo, que indica que es obligación del empleador y trabajador "Sujetarse al reglamento interno legalmente aprobado". De la misma manera en el Artículo 45 del Código de Trabajo, literal *"e"* se indica que es una obligación del trabajador: "Cumplir las disposiciones del reglamento interno expedido en forma legal".

8.13.1.2. Derechos de propiedad intelectual (DPI)

Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. En este contexto, la empresa y su personal se ven en la obligación de:

a) Dar cumplimiento de los derechos de propiedad intelectual que define el uso legal del software y los productos de información.
b) Adquirir software solo a través de fuentes conocidas y de buena reputación, para garantizar que no se viole los derechos de autor.
c) Mantener en su personal el conocimiento de las políticas para proteger los derechos de propiedad intelectual y dar aviso de la intención de tomar medidas disciplinarias contra el personal que las viola. Los controles de uso de copias autorizadas de software y cumplimiento de la propiedad intelectual están en los literales "r" y "s" del Artículo 25 del Reglamento Interno de Trabajo de la empresa y en el literal "i" del Artículo 26 del mismo Reglamento.
d) Mantener los registros de activos apropiados e identificar todos los activos de software para proteger los derechos de propiedad intelectual.
e) Implementar revisiones para asegurar que no se exceda el número máximo de usuarios permitidos dentro de los contratos de licencias de software.
f) Implementar revisiones para que solo se instale software autorizado y productos con licencia.

g) Respetar y cumplir con los términos y condiciones de los contratos de software respecto a la propiedad intelectual.

h) No copiar, duplicar, convertir a otro formato el software o documentos electrónicos que tienen derechos de autor, sin la debida autorización de sus propietarios.

8.13.1.3. Protección de los registros de la organización

a) Los registros de información de la empresa deben estar protegidos contra la pérdida, destrucción, falsificación o acceso no autorizado, de conformidad con los requisitos legislativos, normativos, contractuales y comerciales.

b) Los registros de información de la empresa deben ser clasificados adecuadamente bajo el esquema de clasificación y los medios de almacenamiento que determine la organización; y durante el período de almacenamiento y formato que determine la empresa o los entes de control externos como el Servicio de Rentas Internas (SRI), la Superintendencia de compañías, etc.

c) Los sistemas de almacenamiento de datos y su formato deben elegirse de forma tal que los datos requeridos puedan recuperarse de una manera aceptable.

d) Se debe realizar la destrucción apropiada de los registros después de ese período si la empresa ya no los necesita, y bajo la autorización por escrito de Auditoría interna y de la Gerencia General.

5.3. Etapa 3: Difusión de la Política de Seguridad

En esta última etapa de la metodología, la difusión consiste en dar a conocer las políticas de seguridad de la información a toda la organización desde un punto de vista sencillo, práctico y amistoso, buscando llegar con estos temas al usuario de una manera amigable con el objetivo de motivar a todo tipo de usuario para que se capacite, cumpla y promueva el uso de las Políticas de Seguridad de la Información en todo momento tanto dentro como fuera de la organización.

5.3.1. Paso 9: Difusión de la Política

En este paso de la aplicación de la metodología se propuso las siguientes recomendaciones para que esta importante etapa de difusión se aplique con éxito al personal de la empresa, una vez que se tenga la política formal aprobada por el Comité Directivo:

- **Uso de publicidad:** Anuncios en papel en la cartelera principal de la empresa y al ingreso del área de producción; anuncio electrónico en la página web institucional de la empresa, y en la página intranet con un enlace para la descarga del documento de políticas y enviando el enlace de descarga a los correos institucionales y personales de los empleados; todos estos medios deben

contener información muy resumida, clara y concreta acerca del tema de seguridad de la información y de la política de seguridad a difundir, indicando lo que el usuario encontrará y para qué es, así como alguna ilustración acorde con el tema que pueda dar una idea y atrape la atención del usuario. En un proyector o televisor que se puede ubicar en el comedor de la empresa donde los empleados se alimentan o descansan unos momentos, también se pueden proyectar presentaciones o videos que lo motiven a interesarse en el tema de seguridad de la información y recordatorio de las políticas de seguridad que debe cumplir en la empresa y personalmente.

- **Campañas de Capacitaciones y Conferencias de Concientización:** Se debe dar charlas o capacitaciones en temas de seguridad informática para motivar al personal y luego ir concientizando en la importancia del cumplimiento de las políticas de seguridad tanto para la empresa como personalmente. Para los locales remotos o nuevos empleados que no pudiesen asistir directamente a la capacitación, existen herramientas de TI que se pueden utilizar, grabando la capacitación y enviándola remotamente o colgándola en la página web empresarial o en la intranet para que la puedan revisar tanto los empleados que no pudieron asistir, como los que si asistieron pero tienen dudas y podrían volverla a ver.

Finalmente cabe indicar que la metodología propuesta se aplicó específicamente en el departamento de producción para identificar y analizar los riesgos, seleccionar los controles de la norma ISO 27002 y elaborar la política de seguridad de la información en un documento formal para esta área, durando un total de 35 horas divididas en 5 días laborables.

Capítulo 6. Conclusiones y Trabajos Futuros

En este capítulo se exponen las conclusiones generales más relevantes de este trabajo, así como los trabajos futuros propuestos enfocados a la continuación de esta investigación en un área que cobra cada vez más importancia a nivel mundial y en nuestro medio como es la seguridad de la información, donde se ha analizado un tema muy interesante en este trabajo como son las políticas de seguridad informática.

6.1. Conclusiones

La información ha llegado a ser uno de los activos más importantes para las operaciones y la toma de decisiones de las organizaciones; por lo tanto surge la necesidad que tienen las empresas de protegerla ante amenazas que cada día son más complejas y sofisticadas.

En las empresas industriales de alimentos, se maneja información crítica para este tipo de organizaciones, como los datos de sus clientes, proveedores, transacciones diarias y las características principales que definen un producto como son sus recetas, proceso de fabricación, costos, etc. siendo necesario que toda esta información tenga la seguridad adecuada. Por lo tanto, las organizaciones de este tipo deben considerar en sus planes estratégicos la elaboración, difusión e implementación de políticas de seguridad de la información apropiadas, siendo un requisito para mejorar su seguridad, ya que representan o sirven como un insumo dentro de un Sistema de Gestión de Seguridad de la Información (SGSI), y se consideran como una base necesaria para desarrollar los programas de seguridad informática organizacional.

La motivación principal para elaborar el presente trabajo es contar con un método adecuado para la elaboración y difusión de políticas de seguridad de la información en empresas industriales de alimentos en base la normativa ISO/IEC 27002; ya que si bien en la bibliografía consultada se indican estudios que proponen metodologías para elaborar políticas y controles de seguridad para establecer una cultura de seguridad de la información en las organizaciones, no establecen un método apropiado, con procesos claros y detallados para elaborar técnicamente políticas de seguridad de la información en base a los riesgos de seguridad identificados y evaluados para empresas industriales de alimentos, mediante la selección respectiva de controles de una norma reconocida internacionalmente como ISO/IEC 27002 que mitigue los riesgos encontrados. Por lo expuesto, la metodología propuesta tiene como aporte el proceso detallado en cada una de sus etapas, tanto para la identificación, análisis y evaluación de riesgos como para la elaboración formal de las políticas de seguridad de la información que los mitiguen. Se proponen herramientas e instrumentos para que la metodología sea ágil, eficiente y aplicable a las empresas industriales de alimentos.

El modelo propuesto en este trabajo va más allá de las metodologías analizadas en la literatura, ya que describe un contexto organizacional más amplio que incluye una visión global de la organización y de sus influencias externas e internas claves que pueden materializar el impacto de riesgos en los procesos organizacionales, mediante el análisis de procesos mediante notación BPMN, el organigrama funcional y la cadena de valor, entre otras herramientas o instrumentos que mejor se adaptan y describen las operaciones y estructura de las empresas industriales en general en nuestro medio.

El modelo se desarrolló a partir del estándar internacionalmente aceptado como lo es ISO/IEC 27002, el mismo que refleja las mejores prácticas recomendadas gracias a la contribución de profesionales certificados en el área de seguridad de la información que aportaron en el desarrollo de dicho estándar. Como los requisitos codificados en ISO/IEC 27001 se amplían y se explican en ISO/IEC 27002 en forma de guía, la empresa mediante este trabajo da un paso muy importante en el tema de seguridad de la información; ya que la política de seguridad de la información obtenida y basada en los controles de la norma ISO/IEC 27002 puede servir de insumo para una futura implementación de un *Sistema de Gestión de Seguridad de la Información* (SGSI) y una posible certificación en ISO/IEC 27001 o para futuras auditorías de seguridad informática.

Se proporcionó además una representación y aplicación práctica que pone a prueba la metodología planteada para el desarrollo de las políticas de seguridad de la información, mediante un caso de estudio cumpliendo de manera integral los pasos y etapas de la metodología propuesta en el departamento de producción de una empresa industrial de alimentos en nuestro medio, cumpliendo satisfactoriamente los objetivos específicos propuestos en este trabajo de titulación.

La implementación práctica de la metodología para la elaboración de políticas de seguridad, consistió de 3 etapas:

- Etapa 1: Identificación y Análisis de Riesgos,
- Etapa 2: Desarrollo de la Política de Seguridad de la Información,
- Etapa 3: Difusión de la Política de Seguridad de la Información

La primera etapa de *identificación y análisis de riesgos*, tiene 6 pasos consecutivos que son:

- Análisis de la organización
- Estructuración del equipo de trabajo
- Capacitación del equipo de trabajo
- Identificación y valoración de activos de información
- Identificación de los riesgos
- Análisis de los riesgos.

La segunda etapa de la metodología propuesta, que es *el desarrollo de la política de seguridad*

de la información, se compone de 2 pasos:

- Selección de controles
- Elaboración del documento formal

La última etapa se conoce como la difusión de la política de seguridad de la información. La aplicación de esta etapa de la metodología consiste en recomendar los medios para dar a conocer en la empresa las políticas de seguridad de la información desde un punto de vista sencillo, práctico y amistoso, tratando de llegar al usuario de una manera amigable para motivarlo a que se capacite, cumpla y promueva el uso de las Políticas de Seguridad de la Información en todo momento tanto dentro como fuera de la organización.

De esta manera, en este capítulo se ha logrado el planteamiento de un método apropiado, que consiste de 3 etapas y un total de 9 pasos propuestos para la identificación, análisis y evaluación de riesgos y la elaboración formal de las políticas de seguridad de la información que los mitiguen. El método está diseñado para ser aplicado en empresas industriales de alimentos, pero no se descarta que pueda ser aplicado también en otro tipo de empresas, con su respectiva validación.

La aplicación práctica de cada una de estas etapas, y su evaluación mediante el análisis de los resultados obtenidos en ellas, se realizó en una empresa industrial de alimentos aplicando la metodología planteada, donde se encontraron un total de 30 riesgos que fueron valorados en base a su probabilidad de ocurrencia y sus consecuencias que afectan a la disponibilidad, integridad o confidencialidad de la información. Además aplicando la metodología planteada se obtuvieron 13 dominios, 30 categorías de control y 88 controles seleccionados de la norma ISO/IEC 27002 en su versión 2013, para mitigar los riesgos identificados y se plasmaron estos controles formalmente en un documento en forma de políticas de seguridad de la información, siendo este el entregable final del presente trabajo de investigación para la empresa en la que se realizó el caso de estudio.

Como se puede observar con lo expuesto, se cumplió con todos los objetivos específicos planteados así como con el objetivo general, mediante el planteamiento de un método adecuado para la identificación, análisis y evaluación de riesgos y la elaboración formal de las políticas de seguridad de la información que los mitiguen con la respectiva aplicación de la metodología propuesta en una empresa industrial de alimentos, dedicada a la producción y distribución de embutidos y cárnicos en la ciudad de Cuenca - Ecuador.

Así también, con todo lo descrito, la hipótesis del presente trabajo que se planteó como: "*la aplicación de la metodología propuesta permitirá la identificación de riesgos críticos y elaboración de políticas de seguridad informática más adecuadas y comunes en una empresa industrial de alimentos*" queda demostrada favorablemente.

6.2. Trabajos Futuros

En beneficio de la comunidad científica, se indica que la metodología propuesta en este estudio ofrece una oportunidad para hacer más avances en una importante y creciente temática como lo es la seguridad informática para determinados dominios, teniendo en consideración la identificación, evaluación y gestión de riesgos y la elaboración, difusión e implementación de políticas de seguridad para una determinado tipo de organización, ya que se debe considerar que no todas las empresas u organizaciones tienen las mismas necesidades de seguridad, pues sus riesgos varían de acuerdo a su localización, su naturaleza y los procesos que se manejan así como los activos de información y controles que disponen; considerando además el enfoque e importancia que los directivos de una organización tienen respecto a la seguridad de su información y la situación o estado actual de una empresa en cuanto a seguridad informática se refiere.

Por lo tanto se podrían proponer otras metodologías y su aplicación basadas en esta propuesta, que sirvan para otro tipo de empresas, como financieras, comerciales, de servicios, etc. pues si bien la metodología de este trabajo se la realizó y probó en una empresa industrial de alimentos, también podría servir en empresas de diversos tipos, realizando las validaciones correspondientes.

Además de las etapas detalladas en este trabajo para la elaboración y difusión de políticas de seguridad informática partiendo de una identificación y evaluación de riesgos, existen otras etapas importantes para una gestión integral y completa de las políticas de seguridad en las que se podrían realizar futuros trabajos de investigación como son la etapa de implementación de las políticas en la empresa, el monitoreo recurrente del cumplimiento de las políticas mediante auditorías o herramientas automatizadas de software que ayuden a realizar esta tarea, la revisión y evaluación de la política para conocer cuando hay que actualizarla o desecharla y como se debe proceder con el retiro de la política de seguridad mediante un proceso adecuado.

Referencias

[1] Agustina Sanllehí, J. R. (2009). Prevención del delito en la empresa: Límites ético–jurídicos en la implementación de sistemas de videovigilancia. Revista Electrónica de Ciencia Penal Y Criminología, 10, 1–48.

[2] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). OCTAVE®-S Implementation Guide. Software Engineering Institute, 1(V 1.0), 1–63.

[3] Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: A review of Challenges and Influencing Factors. The 11th International Conference for Internet Technology and Secured Transactions, 352–358. https://doi.org/10.1109/ICITST.2016.7856729

[4] Barbosa Martins, A., & Saibel, C. (2005). A methodology to implement an information security management system. Journal of Information Systems and Technology Management, 2(2), 121–136. https://doi.org/1807-1775

[5] Barragán, I., Góngora, I., & Martínez, E. (2011). Implementacion de politicas de seguridad informatica para la m.i. municipalidad de guayaquil aplicando la norma iso/iec 27002. Escuela Superior Politécnica del Litoral.

[6] Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

[7] Bosworth, S., & Kabay, M. (2002). Computer Security Handbook (4th ed.). Canada: John Wiley & Sons Inc.

[8] Bustamante, F., Fuertes, W., Díaz, P., & Toulkeridis, T. (2016). A Methodological Proposal Concerning to the Management of Information Security in Industrial Control Systems, 0–5.

[9] Cano, J. J. (2004). INSEGURIDAD INFORMÁTICA: UN CONCEPTO DUAL EN SEGURIDAD INFORMÁTICA. (Spanish). Revista de Ingeniería, (19), 40–44. https://doi.org/10.16924/riua.v0i19.437

[10] Clavijo, D., Antonio, C., Antonio, C., & Clavijo, D. (2006). Políticas de seguridad informática.

[11] Computer Security Division, N., Intelligent Systems Division, N., & Laboratory, E. (2015). DRAFT Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security, 2(May). https://doi.org/10.6028/NIST.SP.800-82r2

[12] COSO. (2017). Enterprise Risk Management Aligning Risk with Strategy and Performance, (June), 0–3.

[13] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. European Journal of Information Systems, (June), 1–37. https://doi.org/10.1057/s41303-017-0059-9

[14] Crespo, P. E. (2016). Metodología de seguridad de la información para la gestión del riesgo

aplicable a MPYMES. Universidad de Cuenca.

[15] De Albuquerque Junior, A. E., De, A. E., Junior, A., Marques, E., & Santos, D. (2015). ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES. JISTEM -Journal of Information Systems and Technology Management, 12(2), 289–316. https://doi.org/10.4301/S1807-17752015000200006.

[16] Del, C. F., Cucúrbita, Z., Elaboración, B. Y., & Productos, D. E. D. O. S. (2008). Escuela politécnica nacional.

[17] Diéguez, M., Cares, C., & Cachero, C. (2017). Information Methodology for the Information Security Controls Selection. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), 1–6. https://doi.org/10.23919/CISTI.2017.7975811

[18] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4(April), 92–100. https://doi.org/10.4236/jis.2013.42011

[19] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4(April), 92–100. https://doi.org/10.4236/jis.2013.42011

[20] Dos Santos Roque, A., Ceretta Nunes, R., & Dias da Silva, A. (2010). Proposition of a dynamic model for managing security information on industrial environments. Revista Eletrónica de Sistemas de Información, 9(2). https://doi.org/10.5329/RESI.2010.0902007

[21] Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. Computers {&} Security, 12(6), 597–603. https://doi.org/10.1016/0167-4048(93)90056-B

[22] ESET. (2017). Eset Security Report Latinoamérica 2017. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

[23] Falco, J., Stouffer, K., Wavering, A., & Proctor, F. (2002). IT Security for Industrial Control Systems. National Institute of Standards and Technology, 3, 1–16. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.9422%7B&%7Drep=rep1%7B&%7Dtype=pdf

[24] Federico, A., Pantaleone, M., Nicolás, M., Díaz, L. F. J., Lic, C., Venosa, P., & Mart, F. (2012). IMPACTO DE LA ISO 27000 EN ORGANIZACIONES: Estudio comparativo de herramientas para la implementación de un SGSI.

[25] Ferrel O.C., Hirt Geofrey, Ramos Leticia, A. M. y F. M. A. (2004). Introducción a los Negocios en un Mundo Cambiante. Mc Graw Hill. Retrieved from https://www.gestion.org/recursos-humanos/5936/organigrama-de-una-empresa/

[26] Franco, D. C., & Guerrero, C. D. (2013). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. 11th Latin American and Caribbean Conference for Engineering and Technology, 1–10. Retrieved from http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

[27] Geramiparvar, S., & Modiri, N. (2015). Security as a Serious Challenge for E-Banking : a Review

of Emmental Malware. International Journal of Advanced Computer Research, 5(18).

[28] Goldes, S., Schneider, R., Schweda, C. M., & Zamani, J. (2017). Building a viable information security management system. In 2017 3rd IEEE International Conference on Cybernetics, CYBCONF 2017 - Proceedings. https://doi.org/10.1109/CYBConf.2017.7985763

[29] Gorschek, T., Garre, P., Larsson, S., & Wohlin, C. (2006). A model for technology transfer in practice. IEEE Software. https://doi.org/10.1109/MS.2006.147

[30] Horváth, M., & Jakub, M. (2009). Implementation of security controls according to ISO / IEC 27002 in a small organisation. Security, 48–54.

[31] Iqbal, A., Horie, D., Goto, Y., & Cheng, J. (2009). A database system for effective utilization of ISO/IEC 27002. 4th International Conference on Frontier of Computer Science and Technology, FCST 2009, 607–612. https://doi.org/10.1109/FCST.2009.88

[32] ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

[33] ISO. (2011). ISO/IEC 27005:2011. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

[34] ISO. (2013). ISO/IEC 27002:2013 Preview Information technology -- Security techniques -- Code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html

[35] Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493–508. https://doi.org/10.1016/j.cose.2009.07.001

[36] Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. Risk Management, 14(4), 272–300. https://doi.org/10.1057/rm.2012.9

[37] Lopes, I. M., & Oliveira, P. (2016). Adoption of an information systems security policy in small and medium sized enterprises. Journal of Information Systems Engineering & Management, 1(1), 3–13. https://doi.org/10.20897/lectito.201605

[38] Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 1–6. https://doi.org/10.1109/ICRIIS.2017.8002442

[39] Microsoft. (2006). The Security Risk Management Guide. Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence.

[40] Ministerio de Hacienda y Administraciones Públicas. (2012). Magerit 3. Madrid, España. Retrieved from https://administracionelectronica.gob.es/pae%7B_%7DHome/pae%7B_%7DDocumentacion/pae%7B_%7DMetodolog/pae%7B_%7DMagerit.html%7B#%7D.WaeCb7LyjIU

[41] Miranda, C., Puga, O. V., Mallea, I. P., Cobas, R. P., & Sánchez, R. (2013). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana De Ciencias Informáticas, 10(2), 14–27.

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

[43] Montaño Orrego, V. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. Revista Pensamiento Americano, 4(6), 21–23. Retrieved from http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/57

[44] Object Management Group (OMG), O. (2008). Software Process Engineering Metamodel (SPEM), 3(2), 92–100.

[45] Olmedo, A. F., Olmedo, O. F., & Plazaola, N. (2016). Cadena de Valor. 19. Retrieved from http://www.estrategiamagazine.com/descargas/Cadena de Valor.pdf

[46] PCI Security Standards Council, L. L. C. (2013). PCI (Industrias de Tarjetas de Pago) Norma de seguridad de datos, 136. Retrieved from https://es.pcisecuritystandards.org/%7B_%7Donelink%7B_%7D/pcisecurity/en2es/minisite/en/docs/PCI%7B_%7DDSS%7B_%7Dv3.pdf

[47] Pinto Hernandez, M. G. (2006). Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial. Revista Pensamiento Americano.

[48] Purdy, G. (2010). ISO 31000:2009 - Setting a new standard for risk management: Perspective. Risk Analysis, 30(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

[49] Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56–66. Retrieved from http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/3833

[50] Ramos, Y., Urrutia, O., & Bravo, A. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO / IEC 27002:2013 para la Cooperativa Codelcauca, 88–95.

[51] Roratto, R., & Dias, E. D. (2014). Security information in production and operations: a study on audit trails in database systems. Journal of Information Systems and Technology Management, 11(3), 717–734. https://doi.org/10.4301/S1807-17752014000300010

[52] Sánchez, L. E., Villafranca, D., & Mario, E. F. (2009). MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. Proceedings V Congreso Iberoamericano de Seguridad Informática, (NOVEMBER).

[53] Sinha, S. (2012). Understanding industrial espionage for greater technological and economic security. IEEE Potentials, 31(3), 37–41. https://doi.org/10.1109/MPOT.2012.2187118

[54] Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. Computer, 43(2), 64–71. https://doi.org/10.1109/MC.2010.35

[55] Solarte, F. N. S., Rosero, E. R. E., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma

ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5), 492–507. Retrieved from http://learningobjects2006.espol.edu.ec/index.php/tecnologica/article/view/456

[56] Teodoro, J., & Viteri, M. (2016). Análisis y Evaluación del Riesgo de la Información: Caso de Estudio Universidad Técnica de Babahoyo. A.R. Núm, (32), 1–19.

[57] The University of Adelaide. (2015). Risk Management Handbook. Annals of Physics, 54, 258. Retrieved from http://scholar.google.com/scholar?hl=en%7B&%7DbtnG=Search%7B&%7Dq=intitle:No+Title+Avail%7B#%7D0

[58] Unlp, F. D. I., Facultad, L., Unlp, D. I., & De, L. F. (2010). Lenguajes Notacionales para Modelado de Procesos: un análisis comparativo, 375–379.

[59] Uwizeyemungu, S., & Poba-Nzaou, P. (2015). Understanding Information Technology Security Standards Diffusion.

[60] Yazar, Z. (2002). A qualitative risk analysis and management tool--CRAMM. SANS InfoSec Reading Room White Paper, 1–13. Retrieved from http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Yazar2002_SANS_QualitativeRiskTool.pdf

ANEXO 1 - Elementos de Control del Estándar ISO 27002:2013

DOMINIO / CATEGORIA DE CONTROL	CONTROLES DE SEGURIDAD
5. POLÍTICAS DE SEGURIDAD.	
5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información.
	5.1.2 Revisión de las políticas para la seguridad de la información.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
	6.1.2 Segregación de tareas.
	6.1.3 Contacto con las autoridades.
	6.1.4 Contacto con grupos de interés especial.
	6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.	6.2.1 Política de uso de dispositivos para movilidad.
	6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes.
	7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.	7.2.1 Responsabilidades de gestión.
	7.2.2 Concienciación, educación y capacitación en segur. de la informac.
	7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.	
8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos.
	8.1.2 Propiedad de los activos.

	8.1.3 Uso aceptable de los activos.
	8.1.4 Devolución de activos.
8.2 Clasificación de la información.	8.2.1 Directrices de clasificación.
	8.2.2 Etiquetado y manipulado de la información.
	8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.
	8.3.2 Eliminación de soportes.
	8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.	
9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.
	9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.	9.2.1 Gestión de altas/bajas en el registro de usuarios.
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	9.2.5 Revisión de los derechos de acceso de los usuarios.
	9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información.
	9.4.2 Procedimientos seguros de inicio de sesión.
	9.4.3 Gestión de contraseñas de usuario.
	9.4.4 Uso de herramientas de administración de sistemas.
	9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.	
10.1 Controles criptográficos.	10.1.1 Política de uso de los controles criptográficos.

	10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.	
11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.
	11.1.2 Controles físicos de entrada.
	11.1.3 Seguridad de oficinas, despachos y recursos.
	11.1.4 Protección contra las amenazas externas y ambientales.
	11.1.5 El trabajo en áreas seguras.
	11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.
	11.2.2 Instalaciones de suministro.
	11.2.3 Seguridad del cableado.
	11.2.4 Mantenimiento de los equipos.
	11.2.5 Salida de activos fuera de las dependencias de la empresa.
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
	11.2.8 Equipo informático de usuario desatendido.
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.	
12.1 Responsabilidades y procedimientos de operación.	12.1.1 Documentación de procedimientos de operación.
	12.1.2 Gestión de cambios.
	12.1.3 Gestión de capacidades.
	12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad.

	12.4.2 Protección de los registros de información.
	12.4.3 Registros de actividad del administrador y operador del sistema.
	12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.	12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
	12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.	12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información.
	13.2.2 Acuerdos de intercambio.
	13.2.3 Mensajería electrónica.
	13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	
14.1 Requisitos de seguridad de los sistemas de información.	14.1.1 Análisis y especificación de los requisitos de seguridad.
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
	14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.1 Política de desarrollo seguro de software.
	14.2.2 Procedimientos de control de cambios en los sistemas.
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

	14.2.4 Restricciones a los cambios en los paquetes de software.
	14.2.5 Uso de principios de ingeniería en protección de sistemas.
	14.2.6 Seguridad en entornos de desarrollo.
	14.2.7 Externalización del desarrollo de software.
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
	14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.	14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.	
15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores.
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
	15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos.
	16.1.2 Notificación de los eventos de seguridad de la información.
	16.1.3 Notificación de puntos débiles de la seguridad.
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
	16.1.5 Respuesta a los incidentes de seguridad.
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.
	16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	
17.1 Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información.
	17.1.2 Implantación de la continuidad de la seguridad de la información.

	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.
	18.1.2 Derechos de propiedad intelectual (DPI).
	18.1.3 Protección de los registros de la organización.
	18.1.4 Protección de datos y privacidad de la información personal.
	18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.	18.2.1 Revisión independiente de la seguridad de la información.
	18.2.2 Cumplimiento de las políticas y normas de seguridad.
	18.2.3 Comprobación del cumplimiento.

Tabla 1.1. *Dominios, Categorías de Control y Controles de Seguridad de la norma IEC/ISO 27002:2013.*

ANEXO 2 - Herramientas Usadas en la Aplicación de la Metodología Planteada

2.1. Cuestionario de Evaluación del Estado Actual de Seguridad Informática en la Empresa

Nro.	ASUNTO	RESPUESTAS	
		SI	NO
	Políticas de Seguridad de la Información		
1	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?		X
2	¿Considera Usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		X
3	¿El documento de seguridad es revisado periódicamente y en caso de ocurrencia de eventos significativos?		X
	Seguridad Organizacional		
4	¿Existe un comité de gestión de seguridad que proponga o de soporte a las iniciativas de seguridad?		X
5	¿Existe algún tipo de coordinación de seguridad de la información desde donde se coordine la implementación de controles a lo largo de todos los componentes de la organización?	X	
6	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?		X
7	¿Existe el soporte y la asistencia de un servicio de consultoría especializado en seguridad de la información?		X
8	¿Están establecidos contactos y acuerdos de cooperación con organizaciones para el manejo de asuntos de seguridad?	X	
9	¿Se realizan auditorias de seguridad independientes a la implantación de las políticas de seguridad de la información de la organización?		X
10	¿Se establecen contratos formales de seguridad cuando recursos de tecnologías de información de su organización serán accedidos y/o manejados por terceros?	X	
	Clasificación y control de activos		
11	¿Se mantiene un inventario de todos los activos sensibles de cada sistema de información de la organización?	X	
12	¿Existen esquemas o directrices para la clasificación de la información de la organización de acuerdo al grado de protección que deban recibir?		X
13	¿Están definidos los controles de protección asociados al grado de protección que deba recibir cada activo de información?		X

14	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?	X	
	Seguridad y personal		
15	¿Incluyen los perfiles de trabajo o cargo responsabilidades en el área de seguridad?		X
16	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?	X	
17	¿Se educa y entrena a los empleados adecuadamente en las políticas y procedimientos de seguridad de la organización?	X	
18	¿Conocen los empleados los procedimientos para reportar amenazas, riesgos, sospechas u ocurrencias de: incidentes de seguridad, debilidades en sistemas o servicios e incorrecto funcionamiento de aplicaciones/software?	X	
19	¿Están definidos los procesos disciplinarios para sancionar a aquellos empleados que incurran en violaciones a las políticas y procedimientos de seguridad de la información de la organización?		X
	Seguridad física y ambiental		
20	¿Las áreas con sistemas basados en tecnologías de la información están protegidas físicamente a través de un perímetro de seguridad?	X	
21	¿Existen controles de entrada a las áreas con activos de información sensibles?	X	
22	¿Son esos controles de entrada efectivos, es decir, sólo permiten el acceso a personal autorizado?	X	
23	¿Las oficinas, cuartos y salas que contienen activos de información con requerimientos de seguridad especiales se encuentran en áreas creadas para ese fin?	X	
24	¿Existen normas, procedimientos y mecanismos de control adicionales para trabajar en las áreas seguras?	X	
25	¿Están las áreas de carga y despacho de la organización aisladas de las zonas donde se localizan los activos y sistemas basados en tecnologías de la información?	X	
26	¿Está el equipamiento en tecnologías de la información adecuadamente protegido para reducir riesgos o la exposición a amenazas ambientales o de acceso no autorizado?	X	
27	¿Está el equipamiento protegido contra fallas o anomalías eléctricas?	X	
28	¿Está el cableado eléctrico y de telecomunicaciones asociado al transporte de datos o al soporte de los sistemas basados en tecnologías de información protegido contra intercepciones o daño físico?	X	
29	¿Los equipos que conforman los servicios basados en tecnologías de la información son sometidos a las labores de mantenimiento indicadas por los fabricantes, así como en el período de tiempo especificado?	X	
30	¿Se autoriza y controla el uso de equipos para procesar información que no cumplan con las directrices de seguridad de la organización?	X	
31	¿Se realiza algún tratamiento a la información almacenada en un equipo previo a su desincorporación o reúso?	X	
32	¿Implementa su organización una política de escritorios y pantallas limpias?		X
33	¿Existen controles que sólo permitan el retiro de: equipamiento, software e información perteneciente o en custodia por la organización con la autorización de la gerencia?		X
	Gestión de la operación y las comunicaciones		

34	¿Están documentados los procedimientos de seguridad contemplados en la política de seguridad de la organización?		X
35	¿Están establecidos los procedimientos y roles para el manejo de incidentes de seguridad?		X
36	¿Los ambientes de prueba y desarrollo de sistemas basados en tecnologías de la información están separados del ambiente operativo?		X
37	¿Existen mecanismos para monitorear el uso de los sistemas de la organización? (Como soporte para planificar crecimiento y evitar el colapso de la capacidad de procesamiento de información de la organización)	X	
38	¿Se definen criterios y planes de prueba para aceptar el uso de nuevos sistemas de información (o nuevas versiones/actualizaciones)?	X	
39	¿Se educa y concientiza a los usuarios en las medidas que deben tomar para evitar ser víctimas de software malicioso?	X	
40	¿Están implantadas medidas efectivas para detectar y prevenir contra la presencia de software malicioso?	X	
41	¿Existen políticas y procedimientos para la ejecución de respaldos y su verificación?		X
42	¿Existen registros de las actividades o trabajos que se realizan o intentan realizarse sobre los sistemas basados en TI de la organización?	X	
43	¿Están implantados mecanismos para proteger la plataforma de red de la organización y la información que pasa a través de ella?	X	
44	¿Los dispositivos o medios de almacenamiento de información removibles como cintas, discos, dispositivos extraíbles, información impresa, etc., tienen definido normas o controles que regulen su manejo (protección) y desecho?		X
45	¿Se protege la documentación de los sistemas de información de la organización?	X	
46	¿Existen reglas y procedimientos que gobiernen y controlen el intercambio de información y programas entre organizaciones?		X
	Control de acceso		
47	¿Posee la organización una política de control de acceso?		X
48	¿Existen diferentes niveles de acceso o privilegios para acceder a la información?	X	
49	¿Existen procedimientos de auditoria para revisar y corregir los derechos de acceso de los usuarios de los sistemas de la organización?		X
50	¿Los usuarios son educados sobre sus responsabilidades o rutinas en el manejo de sus mecanismos de acceso a los sistemas?	X	
51	¿Existe una política de uso de los servicios de la red?		X
52	¿Se restringe o controla el acceso a los servidores de la red?	X	
53	¿La red está segregada siguiendo algún criterio?	X	
54	¿Existen mecanismos de control de tráfico para evitar que flujos de datos y conexiones de otros nodos violenten la política de control de acceso?	X	
55	¿Los atributos de seguridad que poseen los servicios de red que utiliza la organización son adecuados?	X	
56	¿Se utilizan mecanismos y herramientas de monitoreo para detectar usos irregulares de la red?	X	
57	¿Todos los relojes de los sistemas en la red están sincronizados?	X	
58	¿Se controla el acceso a la red y sistemas de la organización desde facilidades de computación móvil y tele-trabajo?	X	

	Desarrollo y mantenimiento de sistemas		
59	¿Son los requerimientos de seguridad incluidos en el desarrollo de nuevos sistemas o en las mejoras a los ya existentes?	X	
60	¿Poseen los sistemas mecanismos de seguridad para prevenir su mal uso?	X	
61	¿Es el proceso de desarrollo de software conducido de una manera segura y metodológica?		X
62	¿La implementación de cambios es realizada utilizando procedimientos formales de control de cambio?		X
	Gestión de la continuidad del negocio		
63	¿Posee la organización un proceso de gestión para desarrollar y mantener planes para la continuidad del negocio ante los efectos de fallas mayores o desastres?		X
64	¿Son los planes de continuidad del negocio constantemente revisados y corregidos para asegurar su efectividad?		X
	Cumplimiento con el marco jurídico		
65	¿Tienen los sistemas de información definidos y documentados todos los requerimientos legales relevantes y las normas para asegurar su cumplimiento?	X	
66	¿Están establecidas directrices para la retención, almacenamiento, manejo y desecho de registros e información de la organización?		X
67	¿Existen directrices a todo nivel (gerencia, usuarios y proveedores de servicio) sobre las responsabilidades y procedimientos a seguir para garantizar la protección e intimidad de la información de los clientes?	X	
68	¿Existen medidas para prevenir del uso de las facilidades de procesamiento de información en propósitos diferentes a los del negocio?	X	
69	¿Están los controles criptográficos adaptados al funcionamiento dentro de la empresa?		X
70	¿Las normas y controles adoptados para recolectar evidencia para soportar una acción legal están acordes con las leyes pertinentes?		X
71	¿Se realizan revisiones programadas a todos los entes involucrados con el negocio para asegurar que cumplen con las políticas y estándares de seguridad de la organización?		X

Tabla 2.1. *Cuestionario de Evaluación del Estado Actual de la Seguridad Informática en la Empresa. Fuente: (ISO 27001, 2013)(Crespo, 2016).*

2.2. Formato Interno de la Empresa para el Registro de Capacitaciones

NOMBRE DE LA EMPRESA *REGISTRO DE CAPACITACIONES INTERNAS*	**LOGO DE LA EMPRESA**

Capacitador: _____

Nombre del Curso/Capacitación: _____

_____

Fecha de Capacitación: _____ **Se realizó Evaluación:** **SI** ☐ **NO** ☐

Tipo de Evaluación: **Oral** ☐ **Escrita** ☐

Digital ☐

Breve Resumen de los puntos importantes de la Capacitación:

_____

_____

ASISTENTES:

NOMBRE	FIRMA	OBSERVACION

_____ **Firma del Capacitador**

_____ **Firma del Jefe de Recursos Humanos**

2.3. Matriz de Identificación y Valoración de Activos

Código del Activo	Descripción	(D)	(I)	(C)	Valoración Total	Valor
ED	**Edificaciones**					
(ED)(SEN)(PLA)(01)	Planta de Producción	7	8	9	8	*ALTO*
(ED)(SEN)(PLA)(02)	Planta de Carnes	4	8	7	6.3	*ALTO*
(ED)(SEN)(PLA)(03)	Planta de Empacado	7	8	6	7	*ALTO*
(ED)(SEN)(SUP)(01)	Supervisión de Carnes	4	9	7	6.6	*ALTO*
(ED)(SEN)(SUP)(02)	Supervisión de Empaques	7	8	7	7.3	*ALTO*
(ED)(GER)(01)	Gerencia de Producción	7	9	9	8.3	*ALTO*
(ED)(SEG)(IND)(01)	Área de Seguridad Industrial	4	5	4	4.3	*MEDIO*
(ED)(CPS)(01)	Cuarto de Comunicaciones Producción y Empaques	9	6	7	7.3	*ALTO*
(ED)(CPS)(02)	Cuarto de Comunicaciones Carnes	9	6	6	7	*ALTO*
(ED)(SEN)(CAL)(01)	Área de Aseguramiento de Calidad	4	8	8	6.6	*ALTO*
(ED)(SEN)(INV)(01)	Área de Investigación y Desarrollo	8	10	10	9.3	*MUY ALTO*
(ED)(CDP)(01)	Centro de Procesamiento de Datos principal	10	10	10	10	*EXTREMO*
HW	**Hardware**					
(HW)(SRV)(BBD)(01)	Servidor de Base de Datos	8	10	10	9.3	*MUY ALTO*
(HW)(SRV)(APL)(01)	Servidor Aplicativo ERP, MRP y Producción	8	7	9	8	*ALTO*
(HW)(SRV)(APL)(02)	Servidor de Aplicaciones	8	8	7	7.6	*ALTO*
(HW)(SRV)(APL)(03)	Servidor de Aplicaciones y Servicios WEB	6	8	6	6.6	*ALTO*
(HW)(SRV)(DNS)(01)	Servidor de Dominio	9	4	3	5.3	*MEDIO*
(HW)(SRV)(COR)(01)	Servidor de Correo	4	4	8	5.3	*MEDIO*
(HW)(SRV)(DVR)(01)	Servidor de Cámaras de Seguridad	3	2	6	3.6	*MEDIO*
(HW)(SRV)(SEG)(01)	Servidor Antivirus	7	8	3	6	*ALTO*
(HW)(SRV)(NAS)(01)	Arreglo NAS Principal IBM	7	10	10	9	*MUY ALTO*
(HW)(SRV)(NAS)(02)	Arreglo NAS Secundario IBM	7	6	9	7.3	*ALTO*
(HW)(SRV)(NAS)(03)	Arreglo NAS para Backups Synology	8	8	9	8.3	*ALTO*
(HW)(LAP)(OFI)(01)	Laptop Gerente Producción	6	9	9	8	*ALTO*
(HW)(LAP)(OFI)(02)	Laptop Supervisor Empaques	3	7	7	5.6	*MEDIO*

(HW)(LAP)(OFI)(03)	Laptop Supervisor Carnes	3	7	7	5.6	*MEDIO*
(HW)(LAP)(OFI)(04)	Laptop Supervisor Producción	3	7	7	5.6	*MEDIO*
(HW)(LAP)(OFI)(05)	Laptop Jefe de Investigación y Desarrollo	8	10	10	9.3	*MUY ALTO*
(HW)(PCS)(OFI)(01)	PC Asistente Carnes	3	6	6	5	*MEDIO*
(HW)(PCS)(OFI)(02)	PC Asistente Empaques	3	6	6	5	*MEDIO*
(HW)(PCS)(OFI)(03)	PC Asistente Producción	3	6	6	5	*MEDIO*
(HW)(PCS)(OFI)(04)	PC Planificador de Producción	5	9	8	7.3	*ALTO*
(HW)(PCS)(OFI)(05)	PC Asistente 1 Investigación y Desarrollo	5	8	9	7.3	*ALTO*
(HW)(PCS)(OFI)(06)	PC Asistente 2 Investigación y Desarrollo	5	8	9	7.3	*ALTO*
(HW)(PCS)(OFI)(07)	PC Jefe de Aseguramiento de Calidad	4	8	8	6.6	*ALTO*
(HW)(PCS)(OFI)(08)	PC Asistente 1 Aseguramiento de Calidad	3	7	8	6	*ALTO*
(HW)(PCS)(OFI)(09)	PC Asistente 2 Aseguramiento de Calidad	3	7	8	6	*ALTO*
(HW)(PCS)(OFI)(10)	PC Pesaje de Carnes 1	3	8	6	5.6	*MEDIO*
(HW)(PCS)(OFI)(11)	PC Pesaje de Carnes 2	3	8	6	5.6	*MEDIO*
(HW)(LAP)(PLA)(01)	Laptop Planta Producción Pesaje Materia Prima	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(02)	Laptop Planta Producción Molido y Mezclado	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(03)	Laptop Planta Producción Pesaje Condimentos	5	8	8	7	*ALTO*
(HW)(LAP)(PLA)(04)	Laptop Planta Producción Semiterminados	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(05)	Laptop Planta Empacados 1	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(06)	Laptop Planta Empacados 2	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(07)	Laptop Planta Carnes Pesaje Cámara	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(08)	Laptop Planta Carnes Pesaje Subproductos	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(09)	Laptop Planta Carnes Pesaje Empaques	5	8	5	6	*ALTO*
(HW)(LAP)(PLA)(10)	Laptop Planta Investigación y Desarrollo	5	9	9	7.6	*ALTO*
(HW)(IMP)(OFI)(01)	Impresora Oficina Producción Láser	8	0	9	5.6	*MEDIO*
(HW)(IMP)(OFI)(02)	Impresora Supervisor Producción Matricial	4	0	7	3.6	*MEDIO*
(HW)(IMP)(OFI)(03)	Impresora Supervisor Carnes Matricial	4	0	7	3.6	*MEDIO*

(HW)(IMP)(OFI)(04)	Impresora Supervisor Empaques Matricial	4	0	7	3.6	*MEDIO*
(HW)(IMP)(OFI)(05)	Impresora Oficina Carnes Láser	8	0	6	4.6	*MEDIO*
(HW)(IMP)(OFI)(06)	Impresora Oficina Investigación y Desarrollo Láser	8	0	9	5.6	*MEDIO*
(HW)(IMP)(OFI)(07)	Etiquetadora Oficina de Investigación y Desarrollo Térmica	8	0	9	5.6	*MEDIO*
(HW)(IMP)(OFI)(08)	Etiquetadora Oficina Carnes Térmica	8	0	6	4.6	*MEDIO*
(HW)(IMP)(OFI)(09)	Etiquetadora Oficina Producción Térmica	8	0	7	5	*MEDIO*
(HW)(BAL)(PLA)(01)	Balanza Sencilla Planta Producción Molido y Mezclado	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(02)	Balanza Sencilla Planta Producción Pesaje	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(03)	Balanza Sencilla Planta Producción Semiterminados	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(04)	Balanza de piso Planta Producción Materia Prima	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(05)	Balanza con banda Etiquetadora Empaques 1	8	5	0	4.3	*MEDIO*
(HW)(BAL)(PLA)(06)	Balanza con banda Etiquetadora Empaques 2	8	5	0	4.3	*MEDIO*
(HW)(BAL)(PLA)(07)	Balanza Sencilla Planta Empaques	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(08)	Balanza Sencilla Planta Carnes	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(09)	Balanza de piso Planta de Carnes 1	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(10)	Balanza de piso Planta de Carnes 2	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(11)	Balanza de Gancho Planta de Carnes	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(12)	Balanza con banda Etiquetadora Carnes 1	8	6	0	4.6	*MEDIO*
(HW)(BAL)(PLA)(13)	Balanza con banda Etiquetadora Carnes 2	8	6	0	4.6	*MEDIO*
(HW)(BAL)(PLA)(14)	Balanza de Precisión Investigación y Desarrollo 1	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(15)	Balanza de Precisión Investigación y Desarrollo 2	8	8	0	5.3	*MEDIO*
(HW)(BAL)(PLA)(16)	Balanza Sencilla de Investigación y Desarrollo	8	8	0	5.3	*MEDIO*

(HW)(SNR)(TMP)(01)	Sensor Planta Producción Temperatura Hornos	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(02)	Sensor Planta Producción Temperatura Cámara 1	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(03)	Sensor Planta Producción Temperatura Cámara 2	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(04)	Sensor Planta Producción Temperatura Cámara 3	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(05)	Sensor Planta Producción Temperatura Enfriamiento	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(06)	Sensor Planta Producción Temperatura Caldero	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(07)	Sensor Planta Carnes Temperatura Cámara 1	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(08)	Sensor Planta Carnes Temperatura Cámara 2	5	8	0	4.3	*MEDIO*
(HW)(SNR)(TMP)(09)	Sensor Planta Carnes Temperatura Cámara 3	5	8	0	4.3	*MEDIO*
(HW)(CEL)(01)	Celulares que no son inteligentes y no son de propiedad de la empresa	2	2	9	4.3	*MEDIO*
(HW)(MOV)(01)	Dispositivos inteligentes (Celulares, tablets, PDAs, HandHelds, etc.) que no son de propiedad de la empresa.	4	6	9	6.3	*ALTO*
SW	**Software**					
(SW)(DES)(01)	Sistema de Captura de Pesos	8	9	9	8.6	*ALTO*
(SW)(DES)(02)	Integración de Sistemas Desarrollados ERP	7	9	5	7	*ALTO*
(SW)(DES)(03)	Reportes Desarrollados del Sistema de Producción	7	2	10	6.3	*ALTO*
(SW)(DES)(04)	Sistemas de Reportes BI	7	2	10	6.3	*ALTO*
(SW)(DES)(05)	Sistema de Formulación de Ingredientes Principales	8	10	10	9.3	*MUY ALTO*
(SW)(SAT)(SIO)(01)	Microsoft Windows 2012 Enterprise	8	2	8	6	*ALTO*
(SW)(SAT)(SIO)(02)	Microsoft Windows 2012 Standar	5	2	4	3.6	*MEDIO*
(SW)(SAT)(SIO)(03)	Microsoft Windows 2008 Server Standar	5	9	6	6.6	*ALTO*
(SW)(SAT)(SIO)(04)	Microsoft Windows 8.1 Pro	3	2	8	4.3	*MEDIO*
(SW)(SAT)(SIO)(05)	Microsoft Windows 10 Pro	3	2	8	4.3	*MEDIO*
(SW)(SAT)(SIO)(06)	Microsoft Windows 7 Pro	3	2	8	4.3	*MEDIO*
(SW)(SAT)(SIO)(07)	Linux Ubuntu Server 14.0	8	7	9	8	*ALTO*
(SW)(SAT)(OFI)(01)	Microsoft Office 2013 Small Bussines	5	8	8	7	*ALTO*

(SW)(SAT)(OFI)(02)	Microsoft Office 2016 Versión Hogar y Empresas	5	8	8	7	*ALTO*
(SW)(SAT)(OFI)(03)	Microsoft Visio 2013	6	6	9	7	*ALTO*
(SW)(SAT)(OFI)(04)	Microsoft Project 2013	6	6	9	7	*ALTO*
(SW)(SAT)(COR)(01)	Servidor de Correo Zimbra 8.6	8	5	9	7.3	*ALTO*
(SW)(SAT)(SEG)(01)	Kaspersky EndPoint Security for Business Version Select	5	5	5	5	*MEDIO*
(SW)(SAT)(SEG)(02)	Kaspersky EndPoint Security for Business Version Advanced	5	5	5	5	*MEDIO*
(SW)(SAT)(GBD)(01)	Microsoft SQL Server 2012	10	10	10	10	*EXTREMO*
(SW)(SAT)(ERP)(01)	SAP Business One Versión 9.2	9	10	10	9.6	*MUY ALTO*
(SW)(SAT)(MRP)(01)	Be.As MRP Manufacturing Version 9.0	9	10	9	9.3	*MUY ALTO*
(SW)(SAT)(PRO)(01)	Sistema de Producción Be.As Manufacturing Versión 9.0	9	10	9	9.3	*MUY ALTO*
(SW)(SAT)(SBI)(01)	Quick Sense Versión 3.1	5	2	9	5.3	*MEDIO*
(SW)(SAT)(BAK)(01)	Cobian Backup and Recovery Version 1.1	8	2	3	4.3	*MEDIO*
(SW)(SAT)(DIS)(01)	Label Pro V 6.0	5	2	8	5	*MEDIO*
(SW)(SAT)(MON)(01)	Software de Monitoreo y Control de Temperaturas de Sensores de Hornos y Cámaras de Frío	6	9	3	6	*ALTO*
(SW)(SAT)(MON)(02)	Software de Video Vigilancia del Área de Producción	5	3	9	5.6	*MEDIO*
IE	**Información Electrónica**					
(IE)(ARC)(PLN)(01)	Archivos de Planificación de Producción	9	9	7	8.3	*ALTO*
(IE)(ARC)(COR)(01)	Archivos de e-mails	4	5	9	6	*ALTO*
(IE)(BAK)(01)	Archivos de Respaldo de Archivos del Usuario	5	8	9	7.3	*ALTO*
(IE)(BAK)(02)	Copias de Respaldo de Bases de Datos	7	9	9	8.3	*ALTO*
(IE)(CON)(01)	Archivo de Configuración Locales del Sistema de Producción	8	9	5	7.3	*ALTO*
(IE)(LOG)(01)	Archivo de Registro de Actividades y Errores del Sistema Operativo	4	6	5	5	*MEDIO*
(IE)(LOG)(02)	Archivo de Registro de Actividades y Errores del Sistema de Producción	4	6	5	5	*MEDIO*

(IE)(LOG)(03)	Archivo de Registro de Actividades y Errores del Sistema ERP	4	6	5	5	*MEDIO*
(IE)(LOG)(04)	Archivo de Registro de Actividades y Errores del Software de Seguridad	4	4	5	4.3	*MEDIO*
(IE)(CRI)(FOR)(01)	Archivo Fórmulas Principales	10	10	10	10	*EXTREMO*
(IE)(CRI)(FOR)(02)	Archivo Fórmulas de Producción	8	10	8	8.6	*ALTO*
(IE)(CRI)(FOR)(03)	Archivo Fórmulas de Carnes	8	10	8	8.6	*ALTO*
(IE)(CRI)(FOR)(04)	Archivo Fórmulas de Empaques	8	10	8	8.6	*ALTO*
(IE)(CRI)(FOR)(05)	Otra Información de Investigación y Desarrollo	9	9	10	9.3	*MUY ALTO*
(IE)(CRI)(PCR)(01)	Archivos Digitales de Procedimientos de Producción	7	8	9	8	*ALTO*
(IE)(CRI)(PCR)(02)	Archivos Digitales de Procedimientos de Carnes	7	8	9	8	*ALTO*
(IE)(CRI)(PCR)(03)	Archivos Digitales de Procedimientos de Empaques	7	8	9	8	*ALTO*
(IE)(CRI)(PCR)(04)	Archivos Digitales de Procedimientos de Normas y Estándares de Calidad (ISO, BPM, etc.)	7	5	9	7	*ALTO*
(IE)(CRI)(PCR)(05)	Archivos Digitales de Inducción al Personal de Planta	8	5	5	6	*ALTO*
(IE)(CRI)(PCR)(06)	Archivos Digitales de Manejo e Inducción en Equipos, Maquinaria y Procesos de Planta	8	5	5	6	*ALTO*
(IE)(CRI)(PCR)(07)	Ficha Técnica de Materias Primas	7	8	8	7.6	*ALTO*
(IE)(CRI)(PCR)(08)	Ficha Técnica de Productos Terminados	7	8	8	7.6	*ALTO*
(IE)(CRI)(PCR)(09)	Archivos de Toma de Inventarios de Productos	7	8	8	7.6	*ALTO*
(IE)(CRI)(PCR)(10)	Archivos de Rutas Definidas para Productos	8	10	8	8.6	*ALTO*
(IE)(CRI)(PCR)(11)	Ordenes de Producción	10	6	5	7	*ALTO*
(IE)(CRI)(SAN)(01)	Documentos Electrónicos de Registros Sanitarios	10	5	7	7.3	*ALTO*
(IE)(CRI)(CAL)(01)	Documentación Electrónica de Problemas de Calidad Internos	8	9	9	8.6	*ALTO*

(IE)(CRI)(CAL)(02)	Documentación Electrónica de Problemas de Calidad Externos	8	9	9	8.6	*ALTO*
(IE)(BBD)(01)	Base de Datos del Sistema de BI	7	5	9	7	*ALTO*
(IE)(BBD)(02)	Base de Datos del Sistema de Monitoreo de Temperatura	7	8	5	6.6	*ALTO*
(IE)(BBD)(03)	Base de Datos del Sistema de Formulación de Ingredientes Principales	8	10	10	9.3	*MUY ALTO*
(IE)(BBD)(04)	Base de Datos Principal del Sistema ERP, MRP y Producción	10	10	10	10	*EXTREMO*
IP	**Información en papel**					
(IP)(CRI)(FOR)(01)	Archivo Impreso Fórmulas Principales	4	9	10	7.6	*ALTO*
(IP)(CRI)(FOR)(02)	Archivo Impreso Fórmulas de Producción	4	8	10	7.3	*ALTO*
(IP)(CRI)(FOR)(03)	Archivo Impreso Fórmulas de Carnes	4	8	10	7.3	*ALTO*
(IP)(CRI)(FOR)(04)	Archivo Impreso Fórmulas de Empaques	4	8	10	7.3	*ALTO*
(IP)(CRI)(FOR)(05)	Otra Información Impresa de Investigación y Desarrollo	4	8	10	7.3	*ALTO*
(IP)(CRI)(PCR)(01)	Archivos Impresos de Procedimientos de Producción	4	8	9	7	*ALTO*
(IP)(CRI)(PCR)(02)	Archivos Impresos de Procedimientos de Carnes	4	8	9	7	*ALTO*
(IP)(CRI)(PCR)(03)	Archivos Impresos de Procedimientos de Empaques	4	8	9	7	*ALTO*
(IP)(CRI)(PCR)(04)	Archivos Impresos de Procedimientos de Normas y Estándares de Calidad (ISO, BPM, etc.)	9	8	8	8.3	*ALTO*
(IP)(CRI)(PCR)(05)	Archivos Impresos de Inducción al Personal de Planta	4	6	6	5.3	*MEDIO*
(IP)(CRI)(PCR)(06)	Archivos Impresos de Manejo e Inducción en Equipos, Maquinaria y Procesos de Planta	8	5	4	5.6	*MEDIO*
(IP)(CRI)(PCR)(07)	Ficha Técnica de Materias Primas Impresa	6	7	8	7	*ALTO*
(IP)(CRI)(PCR)(08)	Ficha Técnica de Productos Terminados Impresa	6	7	8	7	*ALTO*

(IP)(CRI)(PCR)(09)	Archivos Impresos de Toma de Inventarios de Productos	8	9	5	7.3	*ALTO*
(IP)(CRI)(PCR)(10)	Archivos Impresos de Rutas Definidas para Productos	7	9	9	8.3	*ALTO*
(IP)(CRI)(PCR)(11)	Ordenes de Producción Impresas	10	6	5	7	*ALTO*
(IP)(CRI)(SAN)(01)	Documentos Físicos de Registros Sanitarios	9	8	5	7.3	*ALTO*
(IP)(CRI)(CAL)(01)	Documentación Física de Problemas de Calidad Internos	5	8	9	7.3	*ALTO*
(IP)(CRI)(CAL)(02)	Documentación Física de Problemas de Calidad Externos	5	8	9	7.3	*ALTO*
(IP)(CRI)(CAL)(03)	Archivos Impresos de Devoluciones Internas	5	8	9	7.3	*ALTO*
(IP)(CRI)(CAL)(04)	Archivos Impresos de Devoluciones de Clientes	9	8	5	7.3	*ALTO*
(IP)(DOC)(01)	Archivos Impresos de Planificación de Producción	7	9	6	7.3	*ALTO*
(IP)(DOC)(02)	Archivos Impresos de e-mails	3	7	9	6.3	*ALTO*
(IP)(DOC)(03)	Informes Impresos de Rendimientos Diarios de Producción	4	9	7	6.6	*ALTO*
(IP)(DOC)(04)	Informes Impresos del Registro del Sistema de Monitoreo de Temperatura	4	8	5	5.6	*MEDIO*
EX	**Medios de Almacenamiento Extraíble**					
(EX) (01)	Medios de Almacenamiento Extraíble que no son propiedad de la empresa	4	7	9	*6.6*	*ALTO*
IC	**Infraestructura de Comunicaciones**					
(IC)(SWT)(01)	Switch de Core Principal de Data Center	10	8	6	8	*ALTO*
(IC)(SWT)(02)	Switch de Comunicaciones Producción 48 puertos	8	7	6	7	*ALTO*
(IC)(SWT)(03)	Switch de Comunicaciones Carnes 24 puertos	8	7	6	7	*ALTO*
(IC)(ROU)(01)	Router de Comunicaciones Principal	7	6	6	6.3	*ALTO*
(IC)(FWR)(01)	Firewall/ Proxy Principal de Seguridad Perimetral Sonicwall	9	9	9	9	*MUY ALTO*

(IC)(TEL)(01)	Central Telefónica Principal Alcatel Lucent	8	4	8	6.6	*ALTO*
(IC)(WIF)(01)	Red WiFi Planta de Producción y Empaques	5	8	9	7.3	*ALTO*
(IC)(WIF)(02)	Red WiFi Planta de Carnes	5	9	8	7.3	*ALTO*
(IC)(WIF)(03)	Red WiFi Oficinas Producción, Investigación y Desarrollo	5	8	8	7	*ALTO*
RH	**Recursos Humanos**					
(RH)(UEX)(01)	Proveedor de Maquinaria	8	6	8	7.3	*ALTO*
(RH)(UEX)(02)	Proveedor de Equipos de Medición	8	6	8	7.3	*ALTO*
(RH)(UEX)(03)	Proveedor de Software ERP y de Producción	7	8	9	8	*ALTO*
(RH)(UIN)(01)	Asistente de Carnes	8	9	4	7	*ALTO*
(RH)(UIN)(02)	Asistente de Empaques	6	9	6	7	*ALTO*
(RH)(UIN)(03)	Asistente de Producción	6	9	8	7.6	*ALTO*
(RH)(UIN)(04)	Asistente 1 de Aseguramiento de Calidad	5	6	7	6	*ALTO*
(RH)(UIN)(05)	Asistente 2 de Aseguramiento de Calidad	5	6	7	6	*ALTO*
(RH)(UIN)(06)	Operarios de Planta de Producción	5	8	9	7.3	*ALTO*
(RH)(UIN)(07)	Operarios de Planta de Carnes	5	8	7	6.6	*ALTO*
(RH)(UIN)(08)	Operarios de Planta de Empaques	5	8	7	6.6	*ALTO*
(RH)(JEF)(01)	Supervisor de Empaques	7	8	7	7.3	*ALTO*
(RH)(JEF)(02)	Supervisor de Carnes	7	8	7	7.3	*ALTO*
(RH)(JEF)(03)	Supervisor de Producción	7	8	8	7.6	*ALTO*
(RH)(JEF)(04)	Planificador de Producción	9	10	8	9	*MUY ALTO*
(RH)(JEF)(05)	Gerente de Producción	9	10	9	9.3	*MUY ALTO*
(RH)(JEF)(06)	Jefe de Aseguramiento de Calidad	6	7	8	7	*ALTO*
(RH)(JEF)(07)	Jefe de Investigación y Desarrollo	10	10	10	10	*EXTREMO*
(RH)(INV)(01)	Asistente 1 de Investigación y Desarrollo	7	9	10	8.6	*ALTO*
(RH)(INV)(02)	Asistente 2 de Investigación y Desarrollo	7	8	10	8.3	*ALTO*
(RH)(INV)(03)	Operarios de Investigación y Desarrollo	7	8	10	8.3	*ALTO*

Tabla 2.2. *Matriz de Identificación y Valoración de Activos en el área de Producción de la Empresa*

2.4. Matriz de Identificación y Valoración Riesgos

COD	NOMBRE RIESGO	DESCRIPCIÓN	ACT. INVOLUCRADOS	ACT. AFECTADOS	UBICACION	DIM	VALOR
[RN.1]	Riesgo por Terremoto	Terremoto, que puede afectar la Disponibilidad de todos los activos de Información de Producción en la empresa.		[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*] [RH.*]	[ED.*]	[D]	**A**
[RN.2]	Riesgo por Inundación	Inundaciones que pueden tener las edificaciones de Producción y que afecten a sus activos de información en su Disponibilidad.		[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*]	[ED.*]	[D]	**M**
[RN.3]	Riesgo por Tormenta Eléctrica	Riesgo Natural que tienen las edificaciones de Producción ante una tormenta eléctrica que afecte a sus activos de Información en su Disponibilidad.		[ED.*] [HW.*] [SW.*] [IE.*] [IC.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEN.INV.01] [ED.CDP.01]	[D]	**A**
[NI.1]	Incendio	Riesgo que tienen las áreas de producción y activos del Datacenter de sufrir un incendio, afectando a sus activos de información.	[HW.*] [RH.*]	[ED.*] [HW.*] [SW.*] [IE.*] [IP.*] [IC.*] [RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[ED.*]	[D]	**A**
[NI.2]	Explosión	Riesgo que tienen las áreas de producción de sufrir una explosión por el equipamiento y materiales que utilizan y el combustible, por ejemplo en hornos, cocinas, calderos, etc.	[RH.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.*] [ED.CPS.*] [ED.INV.01] [HW.*] [IE.*] [IP.*] [IC.*] [RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEN.INV.01]	[D]	**A**

[NI.3]	Falla del Generador Eléctrico o UPS	Falla del Generador eléctrico o un UPS ante un Corte del suministro eléctrico.	[ED.*]	[HW.*] [IC.*]	[ED.*]	[D]	**E**
[NI.4]	Cortocircuito o Descarga Eléctrica	Cortocircuitos o descargas eléctricas internas o externas que afecten a los activos de información.	[ED.*]	[HW.*] [IC.*]	[ED.*]	[D]	**A**
[RC.1]	Temperaturas elevadas en Cuartos de Comunicaciones	Temperaturas elevadas e inadecuadas para los equipos que se ubican en los cuartos de comunicaciones.	[ED.CPS.01] [ED.CPS.02]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D]	**E**
[RC.2]	Daños en los equipos de comunicaciones	Daños en cualquiera de los equipos de comunicaciones afectando su disponibilidad para acceder a los recursos y servicios informáticos.	[IC.*]	[IC.*]	[ED.CPS.01] [ED.CPS.02] [ED.CDP.01]	[D] [I]	**A**
[RC.3]	Daños en el cableado físico de la red	Daño en el cableado físico de la red de cobre, fibra o inalámbrica.	[ED.*]	[IC.*]	[ED.*]	[D] [I]	**M**
[PR.1]	Desconexión intencional de los equipos de comunicaciones	Desconexión física intencional de cualquiera de los equipos de comunicaciones de la red.	[RH.*]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D] [I]	**A**
[NI.5]	Degradación de los activos de información en Papel	Degradación de los activos de información que se encuentran almacenados en papel y que contienen información crítica para la empresa.		[IP.*]	[ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**M**

[PR.2]	Pérdida o robo de los activos de información en Papel	Pérdida o robo de información importante para la organización en papel.	[RH.*]	[IP.*]	[ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [C]	**A**
[NI.6]	Degradación y daños en los equipos informáticos de los usuarios	Degradación o daños en los equipos de usuarios por falta de mantenimiento o daños en sus componentes internos		[HW.LAP.*] [HW.PCS.*] [HW.PLA.*] [HW.IMP.*] HW.BAL.*] [IC.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.CPS.*] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D]	**A**
[NI.7]	Daños en los equipos informáticos industriales de usuarios por polvo, humedad o limpieza del ambiente industrial	Daños en los equipos informáticos industriales de usuarios por polvo, humedad, riego de agua o limpieza del ambiente industrial	[ED.SEN.PLA.*] [RH.*]	[HW.LAP.PLA.*] [HW.BAL.PLA.*] [HW.SNR.TMP.*]	[ED.SEN.PLA.*]	[D]	**A**
[PR.3]	Acceso no autorizado a las instalaciones de producción para el personal de otras áreas	No existe un control adecuado para el personal de otras áreas en el acceso a esta área crítica para la empresa.	[RH.*]	[HW.LAP.*] [HW.PCS.*] [HW.IMP.*] [HW.BAL.*] [HW.SNR.*] [SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*] [IP.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**E**
[PR.4]	Acceso no autorizado a los cuartos de comunicaciones	Acceso no autorizado a los cuartos de comunicaciones y sus equipos informáticos	[RH.*]	[IC.SWT.02] [IC.SWT.03] [IC.WIF.01] [IC.WIF.02] [IC.WIF.03]	[ED.CPS.01] [ED.CPS.02]	[D] [I]	**A**
[PR.5]	Robo de equipos	Mediante el robo de equipos se puede afectar la confidencialidad y disponibilidad de la información	[RH.*]	[HW.*] [IC.*]	[ED.*]	[D] [C]	**M**

[RL.1]	Fuga de Información	La información llega al conocimiento o poder de personas que no deben tener acceso a la misma de manera intencionada o no, sin que la información en sí misma se vea alterada.	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [SW.SAT.COR.01] [SW.SAT.GBD.01] [HW.LAP.*] [HW.PCS.*] [HW.CEL.01] [HW.MOV.01] [EX.01] [RH.*]	[IE.*][IP.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[C]	**A**
[RL.2]	Infección con Malware en los equipos de la empresa	Propagación de malware como virus, programas espías (spyware), gusanos, troyanos, Ransomware, botnet, etc.	[HW.LAP.*] [HW.PCS.*] [EX.01][SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*] [IC.FWR.01] [IC.WIF.01] [IC.WIF.02] [RH.*]	[SW.*] [IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**E**
[RL.3]	Ataques externos que afectan a los Activos de información	Ataques externos que afecten la disponibilidad, confidencialidad e integridad de la información de Producción	[IC.FWR.01] [IC.SWT.*] [IC.ROU.*] [IC.WIF.*] [HW.*] [EX.01] [SW.SAT.SIO.*] [IE.*]	[SW.*] [IE.*]	[ED.*]	[D] [I] [C]	**A**
[PR.6]	Manipulación de la configuración en los equipos de producción	Manipulación intencionada de la configuración de equipos en producción, afectando directamente a su disponibilidad	[RH.*]	[HW.LAP.*] [HW.PCS.*] [HW.IMP.*] [HW.BAL.*] [HW.SNR.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**M**
[PR.7]	Suplantación de credenciales de usuario	Acceso no autorizado al software de producción o a la información electrónica con otras credenciales	[RH.UIN.*] [RH.JEF.*] [RH.INV.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[I] [C]	**E**

[PR.8]	Instalaciones y configuraciones de software no autorizadas	Instalaciones y configuraciones No autorizadas de software en los equipos de la empresa.	[RH.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.CON.01] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**A**
[RL.4]	Privilegios de usuario no correspondientes a su función en el Software e Información electrónica	Cuando un usuario tiene un nivel de privilegios inadecuado en el software, y así puede realizar operaciones que no son de su competencia.	[RH.UIN.*] [RH.JEF.*] [RH.INV.*] [HW.LAP.*] [HW.PCS.*]	[SW.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*] [SW.SAT.ERP.01] [SW.SAT.MRP.01] [SW.SAT.PRO.01] [SW.SAT.SBI.01] [SW.SAT.MON.*] [IE.ARC.*] [IE.CON.01] [IE.LOG.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[I] [C]	**A**
[PR.9]	Alteración o Eliminación de Información Crítica	Eliminación o modificación accidental o no de información crítica (fórmulas, rutas o recursos de productos)	[RH.UIN.*] [RH.JEF.*] [RH.INV.*] [HW.LAP.*] [HW.PCS.*] [SW.SAT.DES.*] [SW.SAT.SIO.04] [SW.SAT.SIO.05] [SW.SAT.SIO.06] [SW.SAT.OFI.*]	[IE.ARC.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I]	**E**
[PR.10]	Ingreso de equipos móviles y de almacenamiento extraíbles no autorizados	Ingreso de equipos laptops, móviles y de almacenamiento extraíbles no autorizados a las áreas de producción de la empresa	[RH. *] [HW.LAP.*] [HW.CEL.01] [HW.MOV.01] [EX.01]	[IE.ARC.*] [IE.CRI.*] [IE.BBD.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[C]	**E**

[PR.11]	Salida del personal de Inv. y Desarrollo de la empresa con conocimientos hacia empresas de la competencia	Salida del personal de investigación y desarrollo de la empresa con conocimientos de los procesos y fórmulas a empresas de la competencia.	[RH.INV.*]	[IE.ARC.*] [IE.CRI.FOR.*] [IE.CRI.PCR.01] [IE.CRI.PCR.02] [IE.CRI.PCR.03] [IE.CRI.PCR.05] [IE.CRI.PCR.07] [IE.CRI.PCR.08] [IE.CRI.PCR.10] [IE.BBD.03] [IP.CRI.FOR.*] [IP.CRI.PCR.01] [IP.CRI.PCR.02] [IP.CRI.PCR.03] [IP.CRI.PCR.05] [IP.CRI.PCR.07] [IP.CRI.PCR.08] [IP.CRI.PCR.10]	[ED.SEN.INV.01]	[C]	**A**
[RL.5]	Fallos de Seguridad en Software Desarrollado	Fallos o vulnerabilidades de Seguridad en software desarrollado para producción.	[SW.DES.*]	[IE.BBD.03] [IE.BBD.04]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**A**
[RL.6]	Fallos de Seguridad en Software Adquirido	Fallos o vulnerabilidades de Seguridad en software Adquirido a terceros para producción.	[SW.SAT.*]	[IE.*]	[ED.SEN.PLA.*] [ED.SEN.SUP.*] [ED.GER.01] [ED.SEG.IND.01] [ED.SEN.CAL.01] [ED.SEN.INV.01]	[D] [I] [C]	**A**

Tabla 2.3. *Matriz Identificación y Valoración de Riesgos en el área de Producción de la Empresa.*

2.5. Matriz Depurada de Controles ISO 27002

DOMINIOS	CATEGORIAS	CONTROLES/POLITICAS APLICABLES
6. Organización de la Seguridad de la Información	6.2. Dispositivos para movilidad y teletrabajo	6.2.1. Política de uso de dispositivos móviles.
7. Seguridad de los Recursos Humanos	7.1. Antes de la contratación 7.2. Durante la contratación 7.3. Cese o cambio de puesto de trabajo	7.1.1. Investigación de antecedentes. 7.1.2. Términos y condiciones de la contratación 7.2.2. Concientización, educación y capacitación en seguridad de la información 7.3.1. Cese o Cambio de puesto de Trabajo
8. Gestión de Activos	8.1. Responsabilidad sobre los activos 8.3. Manejo de los soportes de Almacenamiento	8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos. 8.3.1. Gestión de soportes extraíbles 8.3.2. Eliminación de Soportes 8.3.3. Soportes físicos en Tránsito
9. Control de Accesos	9.1. Requisitos de negocio para el control de accesos 9.2. Gestión de Acceso de Usuario 9.3. Responsabilidades del Usuario 9.4. Control de Acceso a Sistemas y Aplicaciones	9.1.1. Política de control de accesos. 9.1.2. Control de acceso a las redes y servicios asociados. 9.2.1. Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4. Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3.1. Uso de información confidencial para la autenticación 9.4.1. Restricción del Acceso a la Información 9.4.2. Procedimientos Seguros de inicio de sesión 9.4.3. Gestión de Contraseñas de Usuario 9.4.4. Uso de herramientas de administración de sistemas. 9.4.5. Control de acceso al código fuente de los programas.
10. Cifrado	10.1. Controles Criptográficos	10.1.1. Política de uso de controles criptográficos
11. Seguridad Física y Ambiental	11.1. Áreas seguras 11.2. Seguridad de los equipos	11.1.1. Perímetro de seguridad física. 11.1.2. Controles físicos de entrada. 11.1.3. Seguridad de oficinas, despachos y recursos. 11.1.4. Protección contra las amenazas externas y ambientales. 11.1.5. El trabajo en áreas seguras. 11.1.6. Áreas de acceso público, carga y descarga 11.2.1. Emplazamiento y protección de equipos. 11.2.2. Instalaciones de suministro. 11.2.3. Seguridad del cableado. 11.2.4. Mantenimiento de los equipos. 11.2.5. Salida de activos fuera de las dependencias de la empresa.

		11.2.6. Seguridad de los quipos y activos fuera de las instalaciones 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento 11.2.8. Equipo informático de usuario desatendido 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla.
12. Seguridad de las Operaciones	12.1. Responsabilidades y procedimientos de Operación 12.2. Protección contra código malicioso (malware) 12.3. Copias de seguridad 12.4. Registro de actividad y monitoreo 12.5. Control del software en explotación 12.6. Gestión de la Vulnerabilidad Técnica	12.1.4. Separación de entornos de desarrollo, prueba y producción. 12.2.1. Controles contra el código malicioso (malware). 12.3.1. Copias de seguridad de la información. 12.4.1. Registro y gestión de eventos de actividad 12.5.1. Instalación del software en sistemas en producción. 12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones en la instalación de software.
13. Seguridad en las Telecomunicaciones	13.1. Gestión de la seguridad en las redes 13.2 Intercambio de información	13.1.1. Controles de red. 13.1.2. Mecanismos de seguridad asociados a servicios en red. 13.2.1. Políticas y procedimientos de intercambio de información 13.2.2. Acuerdos de intercambio 13.2.3. Mensajería electrónica 13.2.4. Acuerdos de Confidencialidad y Secreto
14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	14.1. Requisitos de Seguridad de los Sistemas de Información 14.2. Seguridad en los Procesos de Desarrollo y Soporte 14.3. Datos de Prueba	14.1.1. Análisis y especificación de los requisitos de seguridad. 14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3. Protección de las transacciones por redes telemáticas. 14.2.1. Política de desarrollo seguro de software. 14.2.2. Procedimientos de control de cambios en los sistemas. 14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4. Restricciones a los cambios en los paquetes de software. 14.2.5. Uso de principios de ingeniería en protección de sistemas. 14.2.6. Seguridad en entornos de desarrollo. 14.2.7. Externalización del desarrollo de software. 14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9. Pruebas de aceptación. 14.3.1. Protección de los datos utilizados en pruebas.
15.Relaciones con Suministradores	15.1. Seguridad de la Información en las Relaciones con Suministradores 15.2. Gestión de la Prestación del Servicio por Suministradores.	15.1.1. Política de seguridad de la información para suministradores. 15.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3. Cadena de suministro en tecnologías de la información y comunicaciones. 15.2.1. Supervisión y revisión de los servicios prestados por terceros. 15.2.2. Gestión de cambios en los servicios prestados por terceros.

16. Gestión de Incidentes de Seguridad de la Información	16.1. Gestión de incidentes de seguridad de la información y mejoras	16.1.1. Responsabilidades y procedimientos. 16.1.2. Notificación de los eventos de seguridad de la información. 16.1.3. Notificación de puntos débiles de la seguridad. 16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5. Respuesta a los incidentes de seguridad. 16.1.6. Aprendizaje de los incidentes de seguridad de la información. 16.1.7. Recopilación de evidencias.
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	17.1. Continuidad de la seguridad de la información 17.2. Redundancias	17.1.1. Planificación de la continuidad de la seguridad de la información. 17.1.2. Implantación de la continuidad de la seguridad de la información. 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información.
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1. Identificación de la legislación aplicable. 18.1.2. Derechos de propiedad intelectual (DPI). 18.1.3. Protección de los registros de la organización

Tabla 2.4. *Matriz Depurada de Controles ISO 27002 para el Departamento de Producción.*