
Maestría Profesional en Ciberseguridad

**Trabajo Final de Graduación**

# “Propuesta de Políticas de Seguridad de la Información para la Empresa Cárnicos La JOYA S.A.”

Elaborado por

Bernal Alberto Murillo Ávila

**Heredia, Costa Rica**

**2024**

## TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Murillo Ávila Bernal Alberto.**

Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2024.03.01 15:12:41 -06'00'

*M.Sc. Miguel Pérez Montero*
Tutor

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA)
Fecha: 2024.03.03 10:35:30 -06'00'

*M.Sc. Dennis Alonso Durán Céspedes*
Lector 1

ARTURO RAMIREZ HEGG (FIRMA)
Firmado digitalmente por ARTURO RAMIREZ HEGG (FIRMA)
Fecha: 2024.03.04 15:54:41 -06'00'

*M.Sc. Arturo Ramírez Hegg*
Lector 2

San José, Costa Rica, 27 de febrero de 2024

*Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-*

## Cláusula de Confidencialidad:

Es responsabilidad de los miembros del Comité Evaluador, el Director de la Escuela, el Director del Departamento de Registro y el Moderador de la Defensa, guardar estricta confidencialidad de la documentación presentada para la defensa del Proyecto de Investigación Aplicada 2 del estudiante: **Bernal Alberto Murillo Ávila**, tanto del documento en borrador para la defensa, observaciones y correcciones realizadas, así como la custodia del documento final que debe ser entregado a la institución.

La vigencia de esta cláusula es por un periodo de: **3 años**. Una vez pasado dicho periodo, el documento final del Proyecto se pondrá a disposición de estudiantes, personal docente y administrativo, en la biblioteca de la Universidad, tanto para estudio, consulta o ejemplificación en clases relacionadas con el tema.

De igual forma, la aceptación del acuerdo de confidencialidad, libera a la Universidad Cenfotec de toda responsabilidad, en caso de que la información brindada se convierta en conocimiento público antes del periodo establecido, donde se compruebe que la institución no tuvo parte de acción u omisión para la revelación de la información por vías ajenas.
Firman en acuerdo:

Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2024.03.01 15:10:01 -06'00'

Miguel Pérez Montero, M.Sc.
**Tutor**

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA)
Fecha: 2024.03.03 10:36:35 -06'00'

Dennis Durán Céspedes, M.Sc.
**Lector 1**

ARTURO RAMIREZ HEGG (FIRMA)
Firmado digitalmente por ARTURO RAMIREZ HEGG (FIRMA)
Fecha: 2024.03.04 15:55:53 -06'00'

Arturo Ramírez Hegg, M.Sc.
**Lector 2**

MARIA ISABEL LOSILLA BARRIENTOS (FIRMA)
Firmado digitalmente por MARIA ISABEL LOSILLA BARRIENTOS (FIRMA)
Fecha: 2024.03.01 15:05:10 -06'00'

María Isabel Losilla Barrientos, M.Sc.
**Moderadora**

San José, Costa Rica, 27 de febrero de 2024

*Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-*

# Declaración de Derechos de Autor

Se declara que el siguiente documento fue realizado por el único autor Bernal Alberto Murillo Ávila, el investigador ha utilizado diversas fuentes bibliográficas, las cuales se utilizaron como referencia y base de datos de conocimiento para apoyar las ideas de esta investigación y la propuesta de solución. Debido a la naturaleza del trabajo, y que la seguridad de la empresa en cuestión se puede ver vulnerada, se solicita que el documento se mantenga confidencial por un periodo de 3 años, con el fin de que, una vez se concluya el trabajo, las sugerencias sean aplicadas en la organización y no exista una brecha de seguridad en este periodo.

# Dedicatoria

“A mi hijo, mi razón de ser y mi mayor inspiración. A mi madre quien siempre me ha inculcado valores y me mostró la importancia del estudio en la vida. A mi compañera de vida por ser mi apoyo incondicional siempre”

# RESUMEN EJECUTIVO DEL PROYECTO

La ciberseguridad ha tomado un papel protagónico en los últimos años, esto debido a que los ciberataques aumentan continuamente y que a su vez afectan a todo tipo de empresas e individuos. De igual manera, en este mundo globalizado y cada vez más competitivo, las empresas son impulsadas a una mayor presencia en el ciberespacio con el fin de mantener vigente el negocio y llegar a más lugares.

En ese contexto, las pequeñas empresas tienen que poner un esfuerzo adicional para mantenerse al día, lo que trae consigo un aumento en la cantidad de riesgos a las que las mismas se pueden enfrentar, ya que los ciberdelincuentes están siempre al acecho de nuevas vulnerabilidades y de esta forma desestabilizar estas empresas en crecimiento.

Bajo esta premisa, la intención es poner a disposición de Cárnicos La JOYA S.A. las herramientas necesarias que les permita estar un paso adelante de todos estos riesgos que hoy hay que enfrentar. Se busca fortalecer, con las mejores prácticas del mercado, mediante políticas de seguridad la información, que serán de gran valor para la empresa y que sirvan de base para que la madurez de la organización se mejore y en un futuro cercano se empiece a crear una cultura de seguridad en la compañía.

**Palabras Clave:** PYMES, ciberseguridad, cultura, seguridad de la información, amenazas, riesgos.

# Índice de Contenidos

# Índice de Tablas

# Índice de Figuras

# CAPÍTULO I: Introducción

## 1.1 Generalidades

En el presente trabajo se lleva a cabo un análisis de la situación actual de Cárnicos La JOYA S.A. en cuanto a la seguridad de la información y se busca, de acuerdo con los resultados, desarrollar políticas de seguridad acordes con las necesidades actuales, basándose en los estándares más reconocidos de la industria.

## 1.2 Antecedentes del problema

En nuestro país las pequeñas y medianas empresas utilizan los medios tecnológicos como el camino para hacer crecer su negocio y a la vez es su respaldo para un manejo más controlado y eficiente de los recursos con los que se cuenta.

El auge que están teniendo los ciberataques a nivel mundial y lo evidenciado en Costa Rica en los últimos años hace de este un problema mayor y que no se debe dejar pasar. Durante el 2020 se detectó solo en Latinoamérica el doble de correos de *phishing* que en 2019; y en 2021 la cantidad de detecciones volvió a duplicarse con respecto a 2020. Además, en 2021 se detectaron más de 2.1 millones de archivos únicos relacionados con campañas de *phishing*, 31% más que en 2020 y 132% más que en 2019. (ESET, 2021)

Durante el proceso evolutivo en esta carrera se ha evidenciado, mediante investigaciones y noticias, que las pequeñas y medianas empresas son muy vulnerables en el área de ciberseguridad. En 2021 los ataques contra compañías crecieron 151% y al menos 55% de las pymes a nivel global han sido víctimas de ciberataques al ser consideradas como las más explotables y con menos recursos para protegerse. (López, 2022)

Gracias a las investigaciones y estudios realizados durante toda la carrera, se puede definir con certeza que las políticas de seguridad de la información pueden ayudar, mediante su implementación, a mejorar de forma sencilla, sin necesidad de mucha inversión, la manera en que la seguridad es gestionada dentro de las organizaciones.

## 1.3 Definición y Descripción del problema

Los ciberataques han ido aumentando globalmente, pequeños países y organizaciones son utilizados como prueba previa a realizar ataques mayores y apuntar a grandes objetivos. En el mundo que vivimos hoy la información es el activo más valorado ya que representa la inteligencia del negocio, clientes, operación y otros factores que pueden brindar una ventaja competitiva en sus áreas.

Basados en el informe de investigaciones de violación de datos de Verizon de 2022, 93% de la data sustraída de pequeñas empresas se relaciona a credenciales de usuarios, lo que permite a los perpetradores acceder a información crítica en los negocios (Verizon, 2022). Un ciberataque, en una pequeña y mediana empresa, puede tener un impacto tan grande como para sacarla de operación y que sea incapaz de recuperarse luego del mismo. Adicionalmente, nueve de cada diez Pymes en Costa Rica empezaron a vender vía internet en los últimos dos años, lo que las hace un blanco más apetecido por los atacantes (Soto, 2022).

Por lo tanto, se busca dotar a la empresa Cárnica, de una guía que les permita comprender de mejor forma el estado actual de la seguridad de la información y a la vez orientarlos en las prácticas básicas para enfrentar estos riesgos que se presentan más a menudo, en el día a día de las organizaciones.

## 1.4 Justificación

Con el desarrollo de las políticas de seguridad de la información para la empresa Cárnica se busca generar un impacto positivo que les permita tener una actitud vigilante y proactiva ante la importancia de la seguridad de la información. Adicionalmente, se busca evitar el impacto negativo que tienen los eventos de ciberseguridad como lo son: pérdidas económicas, pérdidas de derechos intelectuales, daños de imagen, entre otros.

## 1.5 Viabilidad

### 1.5.1 Punto de Vista Técnico

El proyecto propuesto es viable desde el punto de vista técnico, ya que se enfoca en el desarrollo de una serie de políticas, las cuales se encuentran debidamente delimitadas en el alcance. Adicionalmente, se cuenta con las herramientas necesarias para la adecuada constitución de estas. Por otro lado, el investigador ha sido capacitado durante el programa de Maestría y cuenta con las habilidades técnicas necesarias, además del apoyo y la guía de personas con experiencia en esta área.

### 1.5.2 Punto de Vista Operativo

Existe viabilidad desde el punto de vista operativo. El proyecto está orientado a una empresa que ha brindado las condiciones necesarias, desde el punto de vista de tiempo, accesos, espacio físico y demás recursos. Durante el proceso de la investigación no se va a ver alterado el funcionamiento normal de la empresa, ya que el proyecto no abarca

la implementación sino más bien un diagnóstico de la actualidad de la seguridad de la información.

### 1.5.3 Punto de Vista Económico

Desde el punto de vista económico, el proyecto es viable, ya que no fue necesario el asesoramiento de terceros debido a que el desarrollador del proyecto cuenta con la debida experiencia en el área. En caso de que haya surgido algún costo durante la investigación, los mismos fueron asumidos por el investigador.

## 1.6 Objetivos

Se ha usado la taxonomía original de Bloom de 1956 para plantear los objetivos de esta investigación, debido a su robustez y uso como estándar de facto en el sistema educativo costarricense.

### 1.6.1 Objetivo general

Proponer las Políticas de Seguridad de la Información para la empresa Cárnicos La JOYA S.A.

### 1.6.2 Objetivos específicos

1. Analizar los principales modelos de gestión de la Seguridad de la Información.
2. Seleccionar las áreas para evaluar el estado de la Seguridad de la Información.
3. Identificar el estado actual del cumplimiento con respecto a las áreas para evaluar el estado de la Seguridad de la Información.

4. Determinar un conjunto de políticas y procedimientos para la seguridad de la información aplicada a los procesos de la organización.
5. Definir una propuesta de políticas basada en los resultados de la investigación y en las mejores prácticas de la industria.

## 1.7 Alcances y Limitaciones del Proyecto

### 1.7.1 Alcances

El presente trabajo se basa en un análisis de la situación actual de la empresa cárnica, se analiza y cuantifica el cumplimiento actual de la seguridad de la información con el apoyo de los controles de las normas internacionales más notables, se toma lo más relevante de las normas para identificar los puntos más débiles y seleccionar los controles adecuados.

Con el apoyo de las Mejores Prácticas Internacionales se diseñan las políticas de seguridad de la información y se elabora el documento que se entregará a la empresa Cárnica.

El proyecto va a estar limitado a una propuesta de políticas para la seguridad de la información mas no a la implementación de estas.

## 1.8 Marco de Referencia Organizacional y Socioeconómico

### 1.8.1 Historia

Cárnicos La Joya S.A. es una empresa de capital costarricense creada el 13 de agosto de 2003, especializada en la fabricación de embutidos, productos ahumados y carnes procesadas. Gracias a la experiencia de más de 35 años de sus socios

fundadores en la elaboración de productos cárnicos, la compañía ha logrado consolidarse en el mercado nacional en el segmento de carnicerías, pizzerías, sodas, restaurantes y hoteles, a pesar de competir con grandes transnacionales.

Dicha compañía es parte de un consorcio conformado por tres organizaciones relacionadas: Cárnicos La Joya S.A. (la productora), Devaki S.A. (la distribuidora) e Industrias Sol y Sol S.A. (la inmobiliaria), todas ubicadas en Lotes Murillo de Villa Bonita de Alajuela. Actualmente cuenta con 50 colaboradores, de los cuales 35 son parte de la planilla de Cárnicos La Joya S.A. y 15 de Devaki S.A. Industrias Sol y Sol S.A. no tiene empleados.

### 1.8.2 Tipo de Negocio y Mercado Meta

Cárnicos La Joya cuenta con una gran variedad de productos, alrededor de 150 [1]SKU's de embutidos y carnes procesadas, dentro de los cuales se encuentran jamones, tocinetas, salchichones, chorizos, salchichas, carnes mechadas, chuleta, costilla, mano de piedra, etc. Con estos productos logran satisfacer a sus aproximadamente 356 clientes directos a través de dos canales de distribución: rutas propias (Devaki S.A.) y distribuidores independientes. Las rutas propias atienden clientes en el Gran Área Metropolitana (GAM), Guápiles y Limón; mientras que los distribuidores colocan sus productos en parte del Pacífico Norte, Pacífico Central, Pacífico Sur, Pérez Zeledón, San Carlos, entre otros. Por otro lado, cabe resaltar que Cárnicos La Joya S.A. también ofrece los servicios de maquila y desarrollos a la medida para clientes especiales.

### 1.8.3 Misión, Visión y Valores

[1] SKU significa "código de referencia" (stock keeping unit, por sus siglas en inglés) y, como lo indica su nombre, es un número (usualmente de ocho dígitos alfanuméricos) que se asignan a los productos.

A la fecha, el grupo empresarial cuenta con la siguiente misión, visión y valores (tomados de su página Web):

**Misión:** fabricar y comercializar permanentemente productos cárnicos y afines, cumpliendo con altos estándares de calidad, que garanticen a nuestros clientes la mejor relación costo-beneficio y a nuestros colaboradores un ambiente estable que les asegure un crecimiento personal continuo.

**Visión:** ser la empresa más reconocida en el país, por la producción y distribución de los mejores productos cárnicos, desarrollados con materias primas de alta calidad, procesos y maquinaria de última tecnología, beneficiando así; el gusto y la salud del mercado costarricense, el medio ambiente, la estabilidad, el crecimiento de nuestros colaboradores y la rentabilidad de nuestros accionistas.

**Valores:**

- Humildad: todos somos igualmente valiosos.
- Integridad: honestidad, respeto y responsabilidad.
- Pasión por el servicio: todos servimos a todos y todos servimos al cliente.
- Excelencia: calidad, capacitación y mejora continua.
- Trabajo en equipo: unidad hacia la visión, apoyo y respaldo mutuo.

Si bien la Misión y la Visión detallan cuál es la razón de ser de la compañía y dónde quisiera estar a futuro, respectivamente, el investigador considera que pueden ajustarse para reflejar mejor la realidad actual. Los ajustes sugeridos se detallan al final de este documento, en el apartado de “Recomendaciones”.

Con respecto a los valores, se considera que los mismos reflejan el actuar de la compañía ya que contienen los principios básicos de comportamiento ético, así como sus creencias y convicciones para trabajar día a día de manera exitosa.

## 1.9 Estado de la Cuestión

### 1.9.1 Planificación de la Revisión

El propósito de esta revisión será investigar si existen y cuáles son los últimos desarrollos en temas de políticas de seguridad de la información en pequeñas empresas. Se pretende documentar alternativas, con similar enfoque a la que se propone en la presente investigación. Se realiza una revisión bibliográfica, en diferentes fuentes de confianza que permitan determinar investigaciones teóricas en temas de concientización.

#### 1.9.1.1 Formulación de la Pregunta

##### 1.9.1.1.2 Palabras Clave y Sinónimos

A continuación, se definen un conjunto de palabras clave para localizar los trabajos realizados anteriormente, y que al mismo tiempo permitan realizar consultas a las fuentes más relevantes:

Ciberseguridad: Cybersecurity

Seguridad de la información: Information Security

Pequeña y mediana empresa: Small and Medium Business

Políticas de seguridad de la información: Information Security Policies

#### 1.9.1.2 Selección de Fuentes

##### 1.9.1.2.1 Definición del Criterio de Selección de Fuentes

Las fuentes deben cumplir con los siguientes criterios: motores de búsqueda, bases de datos en línea o librerías digitales que permitan la búsqueda u obtención de artículos de investigación. Además, deben ser fuentes fiables que se mantengan dentro del área de las tecnologías de la información, y de preferencia aquellas que provean resultados en el área de la seguridad de la información.

#### 1.9.1.2.2 Lenguaje de Estudio

El lenguaje primario de los estudios será el inglés y los mismos serán extraídos mediante consultas con palabras claves en inglés; sin embargo, se realiza una búsqueda de estudios cuyo lenguaje primario sea el español y serán extraídos mediante consultas con palabras claves en español.

#### 1.9.1.2.3 Identificación de fuentes

La identificación de fuentes se realiza por medio de la experiencia profesional y educacional del autor del presente trabajo con el fin de descartar aquellas fuentes que no guardan relación con el tema de investigación, dicha exploración se realiza al utilizar motores de búsqueda en línea.

#### 1.9.1.2.4 Lista de Fuentes

La lista de fuentes que se utilizan para realizar la revisión sistemática es la siguiente:

Scholar Google

ACM Digital Library

International Organization for Standardization

NIST

#### 1.9.1.2.5 Selección de Fuentes después de la Evaluación

Una vez realizada la revisión de la lista de fuentes, se seleccionan solamente aquellas en donde se encontraron estudios primarios relevantes según la experiencia profesional y educacional del autor.

#### 1.9.1.2.6 Comprobación de las Fuentes

Las fuentes se revisan en primera instancia a través de Scimago Journal & Country Rank (del sitio web www.scimagojr.com) y el Índice H será usado como referencia de comprobación, así como el SJR y el Factor de Impacto. Posteriormente, aquellas fuentes que tengan un Índice H mayor a 20, SJR mayor a 0.2 y un Factor de Impacto mayor a 2, son revisadas en conjunto con el profesor encargado.

### 1.9.1.3 Selección de los Estudios

Seguidamente se procede a describir el proceso y el criterio que se utiliza en la ejecución de la revisión para seleccionar y evaluar los estudios primarios.

#### 1.9.1.3.1 Procedimiento para la selección de los estudios

Para seleccionar los estudios, se utiliza un procedimiento iterativo para la fuente que se listó anteriormente. El procedimiento consiste en ejecutar la consulta en el motor de búsqueda en la fuente seleccionada. Para seleccionar un conjunto inicial de estudios,

se leen los títulos, el Resumen Ejecutivo de los mismos y se evalúan según el criterio de inclusión y exclusión propuesto por el investigador.

#### 1.9.1.3.1.1 Definición del criterio de inclusión y exclusión de estudios

El criterio de inclusión se aplica a los resultados obtenidos después de ejecutar la consulta en el motor de búsqueda en la fuente seleccionada. Este criterio consiste en analizar el título, concordancia con el fin de la investigación y el Resumen Ejecutivo de cada documento.

El criterio de exclusión se aplica al subconjunto de documentos obtenidos en la fase anterior, este involucra la lectura y el análisis del Resumen Ejecutivo, adicionalmente a una revisión de alto nivel del documento completo.

#### 1.9.1.3.2 Extracción de la Información

Se utiliza el siguiente formulario para documentar la información extraída de cada estudio. El formulario incluye lo siguiente:

Identificador del estudio (título, publicación, autores y referencia).

Descripción (área del estudio y resumen).

Aspectos por destacar.

| **Repositorio:** | |
|---|---|
| **Identificador** | |
| Título | |
| Publicación | |
| Autores | |
| Referencia | |

| Descripción | |
|---|---|
| Área del Estudio | |
| Resumen | |
| **Aspectos Por Destacar** | |
| | |

**Tabla 1. Formulario para extracción de información.**

**Fuente: Confección propia.**

### 1.9.2 Ejecución de la Revisión

En esta sección se ejecuta la revisión en cada una de las fuentes seleccionadas, siguiendo los lineamientos especificados anteriormente.

#### 1.9.2.2 Ejecución de la selección en la fuente Scholar Google

La búsqueda se realizó utilizando los siguientes parámetros:

Frases o palabras claves: **Information Security.**

**Policy.**

**SME's Small and Medium Enterprises.**

La ejecución de la búsqueda en Scholar Google encontró 302 estudios por lo que se decidió revisar los 25 más relevantes. Al realizar el criterio de inclusión sobre los mismos; es decir, la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo y posteriormente al realizar el criterio de exclusión, se decidió considerar los siguientes estudios.

| Identificador | Estudio |
|---|---|
| 1 | Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, 11(8), 3383 (2021). Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. |
| 2 | State of the art in information security policy development. Computers & Security, 88, 101608 (2020). Paananen, H., Lapke, M., & Siponen, M. |
| 3 | The hunt for computerized support in information security policy management: a literature review. Information & Computer Security (2020). Rostami, E., Karlsson, F., & Kolkowska, E. |
| 4 | Writing information security policies. New Riders (2016). Barman, S. |
| 5 | Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press (2016). Peltier, T. R. |

**Tabla 2. Estudios primarios obtenidos de la búsqueda Scholar Google. Fuente: Confección propia.**

#### 1.9.2.2.1 Evaluación de la calidad del estudio

Se evaluó la calidad de 3 Journals utilizando Scimago Journal & Country Ranking y a continuación se desarrollan los resultados.

Applied Sciences: la revista tiene un Índice H de 75. Este índice indica que esta fuente tiene estudios de calidad que pasan por una serie de filtros y evaluaciones para ser publicados. Adicionalmente cuenta con SJR promedio de 0.57. SJR es una medida de la influencia científica de las revistas que tiene en cuenta tanto el número de citas recibidas por una revista como la importancia o el prestigio de las revistas de donde provienen tales citas.

Computers & Security: la revista tiene un Índice H de 102. Este índice indica que esta fuente tiene estudios de calidad que pasan por una serie de filtros y evaluaciones para ser publicados. Adicionalmente cuenta con SJR promedio de 1.7.

Information and Computer Security: la revista tiene un Índice H de 51. Este índice indica que esta fuente tiene estudios de calidad que pasan por una serie de filtros y evaluaciones para ser publicados. Adicionalmente cuenta con SJR promedio de 0.43.

#### 1.9.2.2.2 Revisión de la selección

Esta selección fue validada por el autor de este trabajo y el interés en su contenido hizo que se incluya en el mismo.

#### 1.9.2.2.3 Extracción de información

Con el formato ya definido, se extrajo la información de los siguientes estudios.

| **Repositorio: Scholar Google** | |
|---|---|
| **Identificador** | |
| Título | Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. |
| Publicación | Applied Sciences, 11(8), 3383. |
| Autores | Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. |
| Referencia | (Ali, Dominic, Ali, & & Sohail, 2021) |
| **Descripción** | |

| | |
|---|---|
| Área del Estudio | Information Security<br>Policy |
| Resumen | Una preocupación grave para la seguridad de la información de una organización es el comportamiento de los empleados cuando no valoran el cumplimiento de la política de seguridad de la información (ISPC). La mayoría de los estudios ISPC evalúan los comportamientos de cumplimiento e incumplimiento por separado. Sin embargo, la literatura carece de una comprensión integral de los factores que transforman el comportamiento de los empleados de incumplimiento a cumplimiento. Por lo tanto, se realiza una revisión sistemática de la literatura (SLR), destacando los estudios realizados sobre el comportamiento de seguridad de la información (ISB) hacia ISPC en múltiples entornos: marcos de investigación, diseños de investigación y metodologías de investigación durante la última década. Se descubre que la investigación de ISPC se centró más en los comportamientos de cumplimiento que en los comportamientos de incumplimiento. Los conflictos de valores, el estrés relacionado con la seguridad y la neutralización, entre muchos otros factores, proporcionaron evidencia significativa hacia el incumplimiento. Al mismo tiempo, las motivaciones internas/externas y de protección resultaron positivamente significativas hacia las conductas de cumplimiento. Los empleados perciben motivaciones internas y externas de su círculo social, comportamientos de gestión y cultura organizacional para adoptar comportamientos conscientes de la seguridad. Las técnicas de disuasión, los comportamientos de gestión, la cultura y la conciencia de seguridad de la información juegan un papel vital en la transformación del incumplimiento de los empleados en comportamientos de cumplimiento. |
| **Aspectos Por Destacar** | |

**Figura 1.** Este estudio concluye que el incumplimiento de los empleados se debe a conflictos de valores, estrés relacionado con la seguridad y neutralización.

**Figura 2.** Los gerentes deben evaluar los comportamientos de los empleados con regularidad y escalar su nivel de conciencia, brindar capacitación si es necesario hasta que finalmente adopten comportamientos conscientes de la seguridad.

**Figura 3.** Se deben organizar campañas de denuncia de irregularidades para convencer a los empleados de que presenten un informe si ven algo sospechoso.

**Figura 4.** Las organizaciones deben brindar capacitación motivacional y transmitir cómo un empleado es un activo para la organización y no permitir que alguien use este activo en contra de la organización.

**Figura 5.** Se deben incluir los programas de concientización en la rutina diaria de trabajo para que los empleados puedan aprender sobre ISP de forma pasiva.

**Tabla 3. Extracción Fuente #1.**

**Fuente: Confección propia.**

| **Repositorio: Scholar Google** | |
|---|---|
| **Identificador** | |
| Título | State of the art in information security policy development. |
| Publicación | Computers & Security, 88, 101608. |
| Autores | Paananen, H., Lapke, M., & Siponen, M. |
| Referencia | (Paananen, Lapke, & & Siponen, 2020) |
| **Descripción** | |
| Área del Estudio | Information Security<br>Policy |
| Resumen | A pesar de la prevalencia de la investigación que existe bajo la etiqueta de "políticas de seguridad de la información" (ISP), no hay consenso sobre lo que significan las ISP o cómo se deben desarrollar las ISP. Este artículo revisa el desarrollo de ISP de última generación mediante el examen de una muestra diversa |

| | |
|---|---|
| | de literatura sobre el tema. Primero se estudia la definición y la función de las ISP, lo que revela un rico tapiz de diferentes nociones detrás del mismo término. Al observar el panorama general de la investigación sobre los métodos de desarrollo de ISP, se encuentran diferentes fases y niveles de detalle. El análisis de los diferentes puntos de vista sobre el contenido, el contexto y la alineación de la estrategia proporciona una mayor comprensión de la complejidad del asunto.<br>Como resultado, se plantean problemas en las definiciones de ISP y los métodos de desarrollo que deben abordarse en futuras investigaciones y aplicaciones prácticas. Esta revisión concluye que, para el desarrollo de ISP de vanguardia, el enfoque debe cambiar más hacia las necesidades de seguridad de la información específicas de la organización, ya que la dirección de la investigación actual aún carece de contribuciones que mostrarían cómo los factores contextuales podrían integrarse con éxito en desarrollo de ISP. |

**Aspectos Por Destacar**

- Análisis de conocimiento sobre las definiciones y descripciones más utilizadas de las funciones de las ISP
- Tener un terreno común en términos de claridad conceptual puede proporcionar una mejor comprensión, así como una mayor eficacia de las ISP dentro de las organizaciones.
- La confusión y la contradicción en las definiciones pueden generar falta de comunicación y políticas ineficaces.
- Hay poco apoyo disponible para la recopilación de requisitos específicos de la organización y para garantizar que se identifiquen todos los requisitos.
- Si bien los 19 métodos de desarrollo de ISP actuales resaltan los factores contextuales, no brindan métodos que garanticen la seguridad de la información que contrarreste las amenazas específicas de la organización.

**Tabla 4. Extracción Fuente #2.**

**Fuente: Confección propia.**

| **Repositorio: Scholar Google** | |
|---|---|
| **Identificador** | |
| Título | The hunt for computerized support in information security policy management: a literature review. |
| Publicación | Information & Computer Security (2002). |
| Autores | Rostami, E., Karlsson, F., & Kolkowska, E. |
| Referencia | (Rostami, Karlsson, & & Kolkowska, 2020) |
| **Descripción** | |
| Área del Estudio | Information Security<br>Policy |
| Resumen | El propósito de este documento es examinar la investigación de gestión de la política de seguridad de la información (ISP) existente para analizar en qué medida se ha sugerido el soporte manual y computarizado, y la forma en que se ha logrado el soporte sugerido. los resultados se basan en una revisión bibliográfica de la investigación de gestión de ISP publicada entre 1990 y 2017. La investigación existente se ha centrado principalmente en el soporte manual para la gestión de ISP. La investigación futura debería abordar en mayor medida la interacción entre las fases de gestión de ISP, aplicar más investigaciones de intervención para desarrollar soporte informático para la gestión de ISP, investigar en qué medida el soporte informático puede mejorar la integración de las fases de gestión de ISP y reducir la complejidad de dicho proceso de gestión. Enfoque limitado en el soporte computarizado para la gestión de ISP afecta el tipo de asesoramiento y artefactos que la comunidad de investigación puede ofrecer a los profesionales. |

| | |
|---|---|
| | hoy en día, no hay revisiones de la literatura sobre hasta qué punto los sistemas informáticos respaldan el proceso de gestión de ISP. Los hallazgos sobre cómo se ha abordado la complejidad de la gestión de ISP y los métodos de investigación utilizados se extienden más allá de la existente |
| **Aspectos Por Destacar** | |
| ● Toda la complejidad del proceso de gestión de ISP ha recibido poca atención.<br>● La investigación existente no se ha centrado mucho en la interacción entre las diferentes fases de gestión de ISP.<br>● Pocos métodos de investigación se han utilizado ampliamente y la investigación orientada a la intervención es rara. | |

**Tabla 5. Extracción Fuente #3.**

**Fuente: Confección propia.**

| **Repositorio: Scholar Google** | |
|---|---|
| **Identificador** | |
| Título | Writing information security policies. |
| Publicación | New Riders. (2002). |
| Autores | Barman, S. |
| Referencia | (Barman, 2007) |
| **Descripción** | |
| Área del Estudio | Information Security Policies |
| Resumen | Hace un caso comercial convincente para tener políticas de seguridad de TI, luego lo guía a través de la creación de las más comunes. El libro toca temas importantes en los que quizás no piense si está intentando desarrollar políticas por su cuenta. Por ejemplo, derechos de propiedad intelectual, cuestiones de |

| | |
|---|---|
| | aplicación de la ley y análisis forense. Estos se mencionan, pero aumentarán su conciencia de su importancia. |
| **Aspectos Por Destacar** | |
| ● Políticas no tan conocidas o exploradas<br>● Ejemplos de políticas y procedimientos<br>● Aumento conciencia en diversos aspectos de la seguridad | |

**Tabla 6. Extracción Fuente #4.**

**Fuente: Confección propia.**

| **Repositorio: Scholar Google** | |
|---|---|
| **Identificador** | |
| Título | Information Security Policies, Procedures, and Standards: guidelines for effective information security management. |
| Publicación | CRC Press. (2016). |
| Autores | Peltier, T. R. |
| Referencia | (Peltier, 2001) |
| **Descripción** | |
| Área del Estudio | Information Security Policies |
| Resumen | Por definición, la seguridad de la información existe para proteger los valiosos recursos de información de su organización. Pero con demasiada frecuencia, los esfuerzos de seguridad de la información se ven como una frustración de los objetivos comerciales. Un programa eficaz de seguridad de la información preserva sus activos de información y lo ayuda a cumplir los objetivos comerciales. Políticas, procedimientos y estándares de seguridad de la información: Directrices para una gestión eficaz de la seguridad de la información proporciona las herramientas que necesita para seleccionar, desarrollar y aplicar un programa de seguridad que no se verá como una molestia |

| | |
|---|---|
| | sino como un medio para alcanzar los objetivos de su organización. Dividido en El libro cubre tres secciones principales: políticas de escritura, procedimientos de escritura y estándares de escritura. Cada sección comienza con una definición de terminología y conceptos y una presentación de las estructuras del documento. Puede aplicar cada sección por separado según sea necesario, o puede usar el texto completo como un todo para formar un conjunto completo de documentos. El libro contiene listas de verificación, ejemplos de políticas, procedimientos, estándares y pautas. Peltier le brinda las herramientas que necesita para desarrollar políticas, procedimientos y estándares. Demuestra la importancia de un programa de seguridad claro, conciso y bien escrito. Su examen de las mejores prácticas recomendadas de la industria ilustra cómo se pueden personalizar para adaptarse a las necesidades de cualquier organización. Políticas, procedimientos y estándares de seguridad de la información: Directrices para una gestión eficaz de la seguridad de la información lo ayuda a crear e implementar procedimientos de seguridad de la información que mejorarán todos los aspectos de las actividades de su empresa. |
| **Aspectos Por Destacar** | |
| ● Listas de verificación de políticas<br>● Ejemplos de políticas y procedimientos<br>● Ejemplos del estándar británico<br>● Directrices para la creación de políticas | |

**Tabla 7. Extracción Fuente #5.**

**Fuente: Confección propia.**

#### 1.9.2.3 Ejecución de la selección en la fuente ACM Digital Library

La búsqueda se realizó seleccionando las siguientes opciones:

Búsqueda en: todo.

Frases o palabras claves: **Information Security Policies.**

**SME's Small and Medium Enterprises**

La ejecución de la búsqueda en ACM Digital Library no dio como resultado ningún estudio primario que deba ser evaluado en esta revisión sistemática.

#### 1.9.2.4 Ejecución de la selección en la fuente Journal of Research of NIST

La búsqueda se realizó seleccionando las siguientes opciones:

Frases o palabras claves: **information security policies.**

**Small Business.**

La ejecución de la búsqueda en Journal of Research of NIST encontró 1,151,419 estudios por lo que se decidió revisar los 10 más relevantes. Al realizar el criterio de inclusión sobre los mismos; la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo y posteriormente realizar el criterio de exclusión, se identificó un documento como primario.

| Identificador | Estudio |
|---|---|
| 1 | Small Business Information Security: The Fundamentals<br><br>NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1, Noviembre<br><br>03, 2016 |

**Tabla 8. Estudio primario obtenido de la búsqueda del Journal of Research of NIST.**

**Fuente: Confección propia.**

#### 1.9.2.4.1 Evaluación de la calidad del estudio

Para evaluar la calidad de los documentos ubicados en el Journal of Research of NIST, se realizó la consulta en el sitio web Scimago Journal & City Rank. El resultado de la búsqueda indicó que este Journal tiene un índice H de 49.

#### 1.9.2.4.2 Revisión de la selección

Esta selección fue validada por el autor de este trabajo y la relevancia de su contenido hizo que se incluya en el mismo.

#### 1.9.2.4.3 Extracción de información

Al igual que las fuentes anteriores, se utiliza el formulario para documentar la información extraída de cada estudio primario.

| **Repositorio: Journal of Research of NIST** | |
|---|---|
| **Identificador** | |
| Título | Small Business Information Security: The Fundamentals. |
| Publicación | NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1 |
| Autores | Celia Paulsen, Patricia Toth |
| Referencia | (Paulsen & Toth, 2016) |
| **Descripción** | |
| Área del Estudio | Information Security Policies<br>Small Business |
| Resumen | El documento es un informe que desarrolló NIST como guía de referencia sobre ciberseguridad para pequeñas empresas. Presenta los fundamentos para un programa de seguridad de |

| | |
|---|---|
| | información para pequeña empresa en lenguaje no técnico. |
| **Aspectos Por Destacar** | |
| ● El documento explica su enfoque a pequeña empresa<br>● Administración de riesgos y cómo abordarlo<br>● Describe cómo se debe abordar la seguridad de información según los cinco dominios de NIST | |

**Tabla 9. Información extraída del estudio: Small Business Information Security: The Fundamentals.**

**Fuente: Confección propia.**

### 1.9.3 Análisis de resultados

Ejecutadas las revisiones de las fuentes identificadas y con el conjunto de estudios seleccionados, se presentan las conclusiones del análisis de estos.

#### 1.9.3.1 Estudios Analizados

En el proceso de selección de estudios, como se evidencia en la Tabla 10, se hizo el análisis de 37 documentos y en la misma se muestra un resumen de cuántos fueron considerados relevantes y cuántos fueron seleccionados como primarios, esto basado en su contenido, referencias, año de publicación y calidad.

| Fuente | Estudios | Relevantes | Primarios | Refinados |
|---|---|---|---|---|
| **Scholar Google** | 25 | 25 | 3 | 0 |
| **ACM Digital Library** | 0 | 0 | 0 | 0 |
| **Books** | 2 | 2 | 2 | 0 |
| **NIST** | 10 | 10 | 1 | 0 |
| **Total** | 37 | 37 | 6 | 0 |

**Tabla 10. Estudios Analizados.**

**Fuente: Confección propia.**

### 1.9.3.2 Presentación de Resultados

Los estudios que se analizaron en la investigación muestran la importancia y el peso que tienen las políticas de seguridad dentro de las organizaciones y que existe un interés claro en mejorar la metodología de implementación de estas.

Otro aspecto por considerar es que, a pesar de que existen estudios refiriéndose a la implementación de políticas, no existe una guía clara para el levantamiento de requisitos lo cual presenta un reto para que el resultado de estas sea el óptimo y así garantizar políticas eficaces.

### 1.9.3.3 Conclusiones

Una vez analizados los estudios y luego de hacer la comparación sobre los mismos, se llega a las siguientes concusiones:

Existe material suficiente y estudios que permiten conceptualizar de manera adecuada los aspectos necesarios para desarrollar políticas de seguridad.

El análisis de los conocimientos obtenidos de los estudios permite tener una claridad de conceptos que dan una mejor comprensión sobre los procesos y así proporcionar mayor eficacia en los controles.

Los métodos de desarrollo de Políticas de Seguridad actuales resaltan los factores necesarios para implementarlos, no brindan los métodos que garanticen la seguridad de la información que neutralice las amenazas específicas de la organización.

Hay poca información para la recopilación de requisitos específicos en las organizaciones y se debe hacer un esfuerzo para que se identifiquen todos los requisitos de manera adecuada a la hora de realizar el análisis inicial.

# CAPÍTULO II: Marco Conceptual

Este es un trabajo de investigación en el cual no se expondrán ni contrastarán teorías ni se generará una teoría nueva, sino que se expondrán y utilizarán conceptos existentes e identificados durante la revisión realizada en el Estado de la Cuestión.

Para representar a través de un mapa los conceptos claves de esta investigación, el Estado de la Cuestión se procesó a través de un software que analiza la frecuencia de las palabras en un texto, en este caso se utilizó la herramienta en línea TagCrowd (TagCrowd, s.f.).

A continuación, se puede observar el resultado de los resultados arrojados por la herramienta los cuales se perfeccionaron para obtener las 13 palabras de mayor frecuencia en el Estado de la Cuestión.


**Figura 1.** ***Análisis de Frecuencia de palabras del Estado de la Cuestión.***
**Fuente: Confección propia.**

De acuerdo con el resultado obtenido y la relevancia de la información se desarrolló el Marco Conceptual por medio del cual resulta necesario describir algunos aspectos y características que serán empleados durante la investigación.

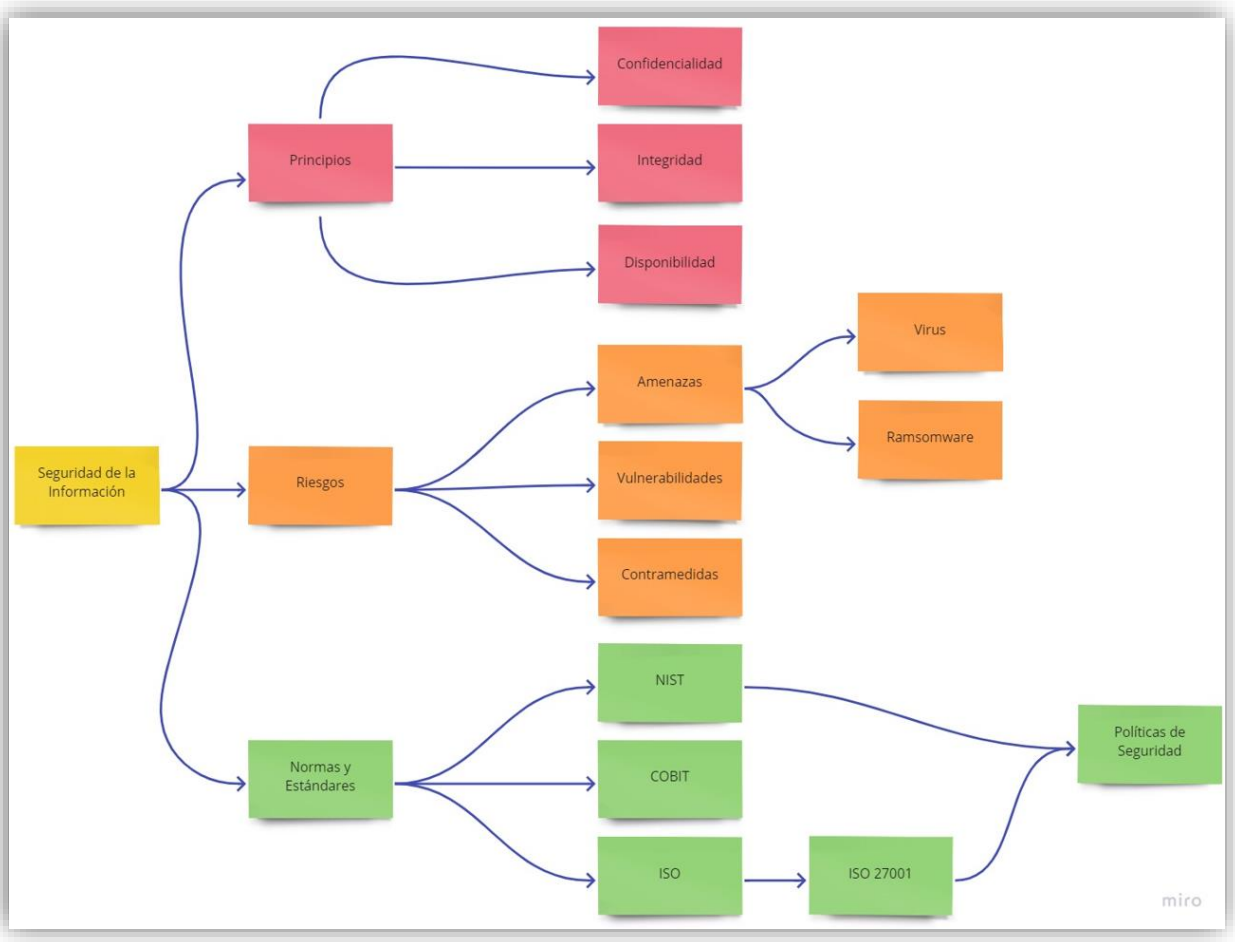


**Figura 2. Mapa del Marco Conceptual.**

**Fuente: Confección propia.**

## 2.1 Seguridad de la Información

La seguridad de la información es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Samaniego Mena & Ponce Ordoñez, 2021)

La Tríada CIA—Confidencialidad, Integridad y Disponibilidad—es un modelo guía en la seguridad de la información. Una estrategia integral de seguridad de la información incluye políticas y controles de seguridad que minimizan las amenazas a estos tres componentes cruciales. La tríada CIA orienta la seguridad de la información en un sentido amplio y también es útil para gestionar los productos y datos de investigación (Washington, 2023).

### 2.1.2 Confidencialidad

La confidencialidad se refiere a proteger la información del acceso no autorizado.

### 2.1.3 Integridad

Integridad significa que los datos son confiables, completos y no han sido alterados o modificados accidentalmente por un usuario no autorizado.

### 2.1.4 Disponibilidad

Disponibilidad significa que los datos están accesibles cuando los necesita.

## 2.2 Riesgo

El riesgo es la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños (ISO, 2009).

### 2.2.1 Ciberataque

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o, incluso, utilizada para extorsionar (Iberdrola, 2023).

### 2.2.2 Vulnerabilidad

Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos (Incibe, 2017).

### 2.2.3 Amenaza

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización, pueden ser tanto internas como externas (Incibe, 2017).


**Figura 3. Conceptos Seguridad**

**Fuente: Incibe**

### 2.2.4 Virus Informático

Un virus informático, como un virus de gripe, está diseñado para propagarse de un *host* a otro y tiene la habilidad de replicarse. De forma similar, al igual que los virus, no pueden reproducirse sin una célula que los albergue, los virus informáticos no pueden reproducirse ni propagarse sin utilizar, por ejemplo, un archivo o un documento.

En términos más técnicos, un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos (Norton, 2018).

### 2.2.5 Ramsomware

El *ransomware* es un tipo de *malware*, o software malicioso, que bloquea los datos o el dispositivo informático de una víctima y amenaza con mantenerlo bloqueado, o algo peor, a menos que la víctima pague un rescate al atacante. En 2021, los ataques de *ransomware* representaron el 21 por ciento de todos los ciberataques y costaron a las víctimas un total estimado de 20.000 millones de dólares (IBM, 2023).

## 2.3 Normas

Las normas son reglas o expectativas de conducta que están establecidas por la sociedad para alcanzar una convivencia en armonía y que pueden variar según cada cultura. Son una guía para reconocer el comportamiento aceptable en un ámbito determinado, por lo que varían según el contexto. Por ejemplo, las normas de una organización, de una institución educativa o de una iglesia. El término norma proviene del latín “norma” que significa mandato, prescripción u orden (Equipo editorial, 2023).

### 2.3.1 Estándares

La normalización o estandarización tiene como objeto la elaboración de una serie de especificaciones técnicas – NORMAS – que son utilizadas de modo voluntario. Es la especificación técnica de aplicación, repetitiva o continuada, cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa (BECOLVE, 2021).


**Figura 4. Organismos Normativos**

**Fuente: Becolve Digital**

### 2.3.1 ISO

Organización Internacional de Normalización, es una organización internacional no gubernamental independiente con una membresía de 168 organismos nacionales de normalización. A través de sus miembros, reúne a expertos para compartir conocimientos y desarrollar Normas Internacionales voluntarias, basadas en el consenso y relevantes para el mercado que respaldan la innovación y brindan soluciones a los desafíos globales (ISO, s.f.).

### 2.3.2 NIST

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos (FTC, 2023).

### 2.3.3 COBIT

COBIT nace con la misión de investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información, guías, actualizados, internacionales y aceptados para ser utilizados diariamente por gerentes de negocio y auditores. Su misión es consolidarse como líder mundialmente reconocido en materia de gobierno, control y aseguramiento de la gestión de TI. En 1992 comenzó la actualización de los objetivos de control de ISACA y, en 1996, ISACA proporcionó a los profesionales de TI un marco de prácticas control de la TI generalmente aplicables y aceptadas (Magazine, 2023).

### 2.3.4 ISO-IEC-27001:2022

ISO 27001 es una norma desarrollada por la Organización internacional de Normalización (ISO) con el propósito de ayudar a gestionar la Seguridad de la Información en una empresa (ISO27001, 2023) .

La nomenclatura exacta de la Norma actual es ISO/IEC 27001 que es la revisión de la norma en su primera versión que fue publicada en el año 2005 como una adaptación de ISO de la norma británica BS 7799-2. Actualmente a nivel mundial la norma ISO 27001 es la norma de referencia para certificar la seguridad de la información en las organizaciones.

# CAPÍTULO III: Marco Metodológico

## 3.1 Tipo de Investigación

En este trabajo se realiza una investigación de tipo aplicada ya que se emplean las mejoras prácticas en el ámbito de la ciberseguridad que propone la Organización Internacional de la Normalización (ISO), NIST, COBIT y otras instituciones reconocidas, esto con el objetivo de atender las brechas de seguridad que podría estar enfrentando la empresa en cuestión.

## 3.2 Alcance Investigativo

El alcance investigativo de este trabajo es descriptivo ya que se utiliza el perfil de la empresa en cuestión y sitúa la misma en un contexto de cómo se encuentra en temas de madurez de la seguridad. La intención de este trabajo es que se pueda contrastar el estado actual de la empresa versus las mejores prácticas que proponen las instituciones de mayor reconocimiento a nivel mundial en temas de políticas de seguridad.

## 3.3 Enfoque

En el desarrollo de este trabajo se utiliza un enfoque cualitativo ya que este tipo de enfoque se adapta mejor al contexto de la investigación. Este enfoque no depende de variables para comprobar una teoría como tal, sino que el enfoque es proponer acciones para el cierre de las brechas de seguridad identificadas en la empresa en cuestión. Este enfoque es muy utilizado en la implementación de estándares.

## 3.4 Diseño

En este trabajo se emplea un enfoque cualitativo utilizando una investigación evaluativa. Las características de la investigación evaluativa se adaptan para la implementación de estándares dentro de una organización y, al mismo tiempo, permite evaluar la eficiencia en términos de seguridad informática dentro de una organización.

## 3.5 Población y Muestreo

Para este trabajo se utiliza una técnica de muestreo no probabilístico basado en el método por conveniencia o intencional donde se investigará la empresa Cárnicos La JOYA S.A y el estado actual en materia de Ciberseguridad. La información suministrada por esta muestra de la población es parte de los insumos utilizados para el desarrollo de la propuesta que se detalla y sugiere en la presente investigación.

## 3.6 Instrumentos de Recolección de Datos

El elemento de recolección de datos, al tratarse de un enfoque cualitativo es la entrevista, esto por medio de plantillas predefinidas donde se realizan una serie de preguntas relacionadas con los temas de ciberseguridad de la empresa Cárnicos La JOYA S.A. El resultado obtenido se analiza con el objetivo de identificar brechas de seguridad según las mejores prácticas de ciberseguridad en temas de políticas de las instituciones más reconocidas y de acuerdo con esto proponer soluciones según las brechas identificadas.

## 3.7 Técnicas de Análisis de Información

Para el análisis respectivo de la información, se utiliza el proceso ilustrado en la Figura 3: Diagrama de Flujo de la Técnica de Análisis de la Información:

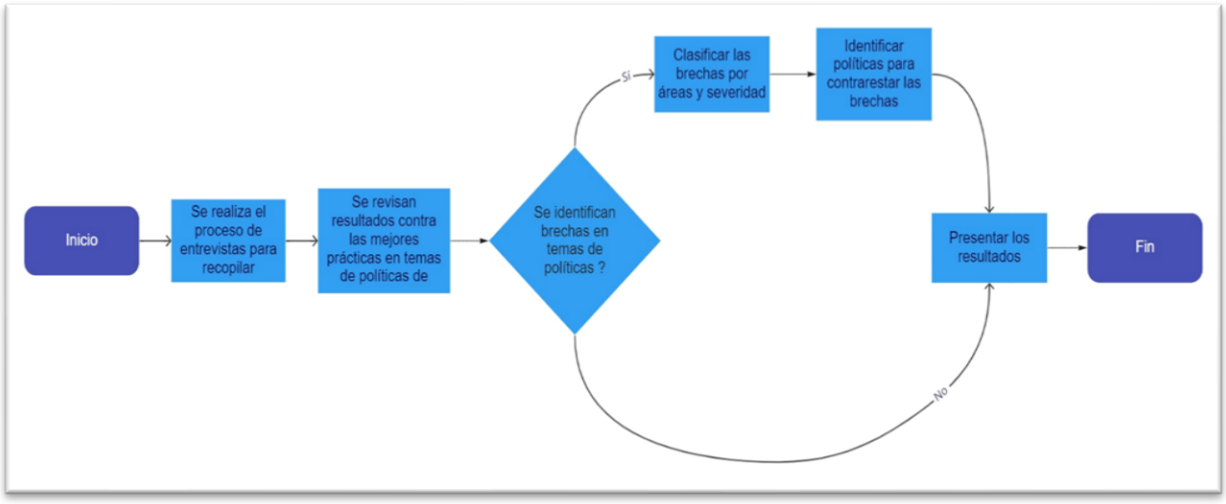


**Figura 5. Diagrama de Flujo de la Técnica de Análisis de la Información. Fuente: Confección propia.**

### 3.8 Estrategia de Desarrollo de la Propuesta

La propuesta es desarrollada mediante dos fases: inicialmente, se identifica la información mediante fuentes primarias y secundarias. De igual manera se hace uso de las encuestas para obtener información específica de las diferentes áreas de interés y las políticas referentes a las mismas, con el fin de determinar la madurez de la organización en Ciberseguridad.

Las encuestas están enfocadas en dos fases: en el estudio de la organización y en el estudio de las políticas existentes. De esta manera los datos recolectados son el indicador para establecer cada una de las variables, factores e indicadores que será necesario tomar en consideración para el desarrollo de la propuesta final.

# CAPÍTULO IV: Análisis de la Situación

## 4.1 Anexo A en ISO-IEC-27001:2022

El Anexo A de la Norma ISO 27001 es un documento normativo que sirve como guía para implementar los controles de seguridad específicos de esta norma. Todos estos controles están dirigidos a mejorar la Seguridad de la Información de una organización. Tras la reciente actualización de la norma ISO 27002, en octubre de 2022 se anunció y publicó la norma ISO 27001:2022 para la gestión de la seguridad de la información. Los conceptos y la práctica de la seguridad de la información han evolucionado masivamente desde que se había publicado la última versión de la norma ISO 27001 en 2013.

Cabe destacar que toda organización que busque el cumplimiento de esta norma debe implementar todos los controles de este Anexo A, si alguno o algunos de estos controles no son implementados por alguna razón especial, la organización debe justificarlo en un documento de descargo que debe documentar las razones para su omisión.

### 4.1.1 Cambios en la Norma ISO 27001

El mayor cambio de la norma actualizada se refiere a los controles del anexo A, que se abordan en su totalidad en la norma ISO 27002.

Los 14 grupos de control y objetivos originales ya no existen y han sido sustituidos por cuatro grupos de control:

- Organización.
- Personas.
- Físicos.
- Tecnológicos.

El número total de controles se ha reducido de 114 a 93.

No se ha suprimido ningún control, pero se han consolidado varios y se han añadido 11 nuevos. Los cuatro grupos de controles se conocen como "temas" y se sugiere el uso de atributos para desarrollarlos, aunque no es obligatorio utilizarlos.

Los nuevos controles añadidos al Anexo A son adiciones muy necesarias y ayudan a poner al día la norma ISO 27001, alineándolos más fácilmente con nuestro clima de seguridad actual (NQA, 2023).

Estos nuevos controles incluyen:

- Seguridad de la información para el uso de servicios en la nube.
- Actividades de seguimiento.
- Inteligencia sobre amenazas.
- Preparación de las TIC para la continuidad de la actividad.
- Vigilancia de la seguridad física.
- Gestión de la configuración.
- Eliminación de información.
- Enmascaramiento de datos.
- Protección contra la fuga de datos.
- Filtrado web.
- Codificación segura.

### 4.1.2 Selección de Controles

Utilizando el criterio experto del autor de este trabajo, se tomó la decisión de utilizar sólo algunas de las secciones de ISO-IEC-27001:2022 que apliquen a la empresa en cuestión; sin embargo, a futuro esta selección puede expandirse dependiendo del mismo crecimiento y necesidades de la empresa y teniendo en cuenta la mejora continua. La Tabla 11 muestra la relación entre la sección del ISO 27001 y la cantidad de preguntas relacionadas a la misma.

| Sección ISO-IEC-27001:2022 | Cantidad de Controles |
|---|---|
| A5.- Controles Organizativos | 7 |
| A6.- Controles de Persona | 4 |
| A7.- Controles Físicos | 4 |
| A8.- Controles Tecnológicos | 5 |

**Tabla 11. Secciones Seleccionadas para la Evaluación.**

**Fuente: Confección propia.**

### 4.2. Recolección de Datos

En este caso se utiliza un análisis de datos cualitativo, ya que buscamos analizar la situación actual de la seguridad de la información que se aplica en la empresa Cárnicos La JOYA S.A. Se procede a obtener datos mediante una encuesta con 32 preguntas relevantes a las áreas seleccionadas con el fin de realizar la confección de políticas basadas en estos resultados.

La entrevista tiene una duración estimada de 20 minutos y se aplica a todos los encargados de la seguridad de la información. A continuación, se detallan las preguntas.

**A5. – Controles Organizativos**

**Controles por cubrir mediante la entrevista**

A 5.9 Inventario de información y otros activos asociados

A 5.10 Uso aceptable de la información y otros activos asociados

A 5.11 Devolución de activos

A 5.12 Clasificación de la información

A 5.13 Etiquetado de la información

A 5.15 Control de acceso

A 5.17 Información de autenticación

1. ¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad específicas?

2. ¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?
3. ¿Existen procedimientos para el manipulado de la información de acuerdo con su clasificación?
4. ¿Se ha realizado un inventario de activos de información que dan soporte al negocio?
5. ¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?
6. ¿Se han establecido normas para el uso de activos en relación con su seguridad?
7. ¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?
8. ¿Existen procedimientos para el traslado de activos de información para proteger su seguridad?
-Control de salidas
-Cifrado etc.
9. ¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?
10. ¿Existen procesos formales de registro de usuarios?
11. ¿Existen procesos formales para asignación de perfiles de acceso?
12. ¿Se ha establecido una política específica para el manejo de información clasificada como confidencial?
13. ¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?
14. ¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?
15. ¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?
16. ¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?
17. ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?

**A6. – Controles de Personas**

**Controles por cubrir mediante la entrevista**

A 6.1 Indagación

A 6.2 Términos y condiciones de empleo

A 6.5 Responsabilidades tras la terminación o el cambio de empleo

A 6.6 Acuerdos de confidencialidad o de no divulgación

1. ¿Se investigan los antecedentes de los candidatos a puestos en la organización?

-Formación

-Experiencia

-Referencias

2 ¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?

3. ¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?

4. ¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?

5. ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?

6. ¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?

**A7. – Controles Físicos**

**Controles por cubrir mediante la entrevista**

A 7.7 Escritorio y pantalla limpia

A 7.8 Ubicación y protección del equipo

A 7.11 Servicios públicos de apoyo

A 7.13 Mantenimiento del equipo

1. ¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?
2. ¿Se protegen los equipos contra fallos de suministro de energía?
3. ¿Se planifican y realizan tareas de mantenimiento sobre los equipos?
4. ¿Se controla y autoriza la salida de equipos, aplicaciones etc.
5. ¿Se establecen protocolos para proteger o eliminar información de equipos que se dan de baja o van a ser reutilizados?
6. ¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?

**A8. – Controles Tecnológicos**

**Controles por cubrir mediante la entrevista**

A 8.2 Derechos de acceso privilegiados
A 8.3 Restricción del acceso a la información
A 8.7 Protección contra el *malware*
A 8.13 Respaldo de información
A 8.32 Gestión de cambios

1. ¿Existen sistemas de detección para Software malicioso o *malware*?
2. ¿Se ha establecido un sistema de copias de seguridad acorde con las necesidades de la información y de los sistemas?
3. ¿Existe un procedimiento establecido para la gestión de cambios en los sistemas?

### 4.3 Evaluación de las preguntas

Para determinar el nivel de madurez de la organización y poder desarrollar las políticas en las áreas que más se requiere, se determinan 3 niveles en una lista con valores que van del 1 al 3. Estos valores determinan el nivel de la seguridad de la información en la empresa y, de acuerdo con estos, la necesidad de implementar políticas en esas áreas. La Tabla 12 muestra la descripción de las tres posibles opciones de respuesta.

| Nivel | Descripción genérica de la opción de respuesta |
|---|---|
| 1 | La empresa no cumple con lo que plantea la pregunta |
| 2 | La empresa cumple parcialmente que plantea la pregunta |
| 3 | La empresa cumple en gran medida lo que plantea la pregunta, pero no de forma estandarizada |

**Tabla 12. Descripción de las opciones de respuesta.**

**Fuente: Confección propia.**

## 4.4 Determinación de Resultados

Para cada 1 de las 4 secciones que se determinaron de relevancia para la investigación, se realiza una recomendación basada en la respuesta obtenida. Por ejemplo, si la respuesta indica que no cumple con lo que plantea la pregunta, se recomienda una política que vaya acorde a esa pregunta. De esta forma, se desarrolla una lista inicial de políticas para su debida revisión y aprobación de la Junta Directiva. En la Tabla 13 se muestra un ejemplo del resultado de una evaluación con sus debidas recomendaciones.

| Pregunta | Nivel de Respuesta | Recomendación |
|---|---|---|
| ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras? | La empresa no cumple con lo que plantea la pregunta | Establecer política de contraseña segura. Incluyendo Longitud, Caracteres especiales. |
| ¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas? | La empresa cumple parcialmente con lo que plantea la pregunta | Robustecer política de respaldos, que incluya cadencia, y se enfoque en los activos críticos. |

| | | |
|---|---|---|
| ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato? | La empresa no cumple con lo que plantea la pregunta | Priorizar política para terminación de contrato y confidencialidad. |

**Tabla 13. Ejemplo de resultado de Evaluación y Recomendaciones.**

**Fuente: Confección propia.**

# CAPÍTULO V: Propuesta de Solución

## 5.1 Contexto de la Compañía

Basado en los resultados de la encuesta, se puede determinar que en la organización existen reglas generales de seguridad informática, las cuales buscan la protección de los equipos de la empresa, sin embargo, no existe una lista de políticas establecidas, las cuales sean requeridas en todas las áreas que abarca la misma.

## 5.2 Determinar las áreas que abarcarán las políticas de seguridad

Con base en el análisis que se llevó a cabo en la empresa y el criterio experto del desarrollador del documento se determinó que se abarcaran las 4 grandes áreas de controles del ISO 27001 pero se delimite a una serie inicial de políticas que puedan tener el mayor impacto en la organización.

Las reglas previas que ya existían se adaptarán a las políticas de seguridad de la información, con base en el estándar ISO 27001, por medio de la unificación en un solo documento. A continuación, se presentan las áreas del documento de políticas de seguridad de la información para Cárnicos La JOYA S.A.

1. Inventario de activos: es importante identificar los activos que se tienen en la empresa y contar con un registro de la(s) persona(s) responsable(s) de cada uno, así se tiene definido el responsable en caso de algún problema. Se puede encontrar en el apartado A.5.9 del documento ISO/IEC 27002:2022.

2. Uso aceptable de los activos: la utilización de un activo se debe llevar a cabo bajo ciertas reglas que velen por el uso responsable de los mismos. Se puede encontrar en el apartado A.5.10 del documento ISO/IEC 27002:2022.

3. Política de clasificación de la información: la información que se maneja en la empresa con diferentes tipos de nivel de importancia, por lo cual debe clasificarse según los

niveles de protección y los tipos de documentos en los cuales se divide. Se puede encontrar en el apartado A.5.12 del documento ISO/IEC 27002:2022.

4. Política de control de acceso: en los sistemas utilizados para manejo interno, se debe tener un control de acceso y deben existir campos de auditoría que lleven un registro de quien llevó a cabo ciertas actividades. Se encuentra en el apartado A.5.15 del documento ISO/IEC 27002:2022.

5. Política de manejo de claves: es determinante que los equipos y usuarios que se utilizan en las labores diarias de la empresa se encuentren resguardados, por esta razón, se procede a definir los controles relacionados a claves. Se encuentra en el apartado A.5.17 del documento ISO/IEC 27002:2022.

6. Protección de registros: la organización debe tener cobertura sobre los registros y que estos estén protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada. Se encuentra en el apartado A.5.33 del documento ISO/IEC 27002:2022.

7. Revisión de las políticas: De manera anual se debe realizar una revisión de las políticas con el fin de determinar si las mismas cumplen las expectativas, si hay oportunidad de mejora en las actuales, cuáles ya no aplican y la creación de nuevas políticas para robustecer la seguridad de la información. Se encuentra en el apartado A.5.35 del documento ISO/IEC 27002:2022.

8. Política de términos y condiciones del empleo: es importante que existan acuerdos contractuales con los trabajadores donde se especifiquen las responsabilidades y consecuencias relacionadas a la seguridad de la información. Se puede encontrar en el apartado A.6.2 del documento ISO/IEC 27002:2022.

9. Acuerdos de confidencialidad o de no divulgación: Junto a la política de los términos y condiciones del empleo se deben revisar y firmar periódicamente acuerdos de

confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. Se puede encontrar en el apartado A.6.6 del documento ISO/IEC 27002:2022.

10. Política de pantalla y escritorio limpio: es importante que la pantalla de inicio de las computadoras usadas por los empleados se mantenga con orden, y adicionalmente a esto que los dispositivos extraíbles no sean medios que permitan extracción de archivos con información importante de la empresa. Se puede encontrar en el apartado A.7.7 del documento ISO/IEC 27002:2022.

11. Protección contra el *malware*: es importante el uso de herramientas que le permitan a la organización combatir programas malignos de manera sencilla y en toda la empresa. Se puede encontrar en el apartado A.8.7 del documento ISO/IEC 27002:2022.

12. Política de respaldo de la información: los respaldos de la información son importantes porque permiten acceder a la misma en caso de que algún problema surja y se pueda continuar con la operación. Se puede encontrar en el apartado A.8.13 del documento ISO/IEC 27002:2022.

El documento que se desarrolla con las políticas de seguridad de la información está compuesto de las doce áreas mencionadas previamente. Lo anterior se concluye luego del análisis de la situación actual de la empresa, y se determina que, abarcar estas áreas, cumple con la necesidad inicial que presenta Cárnicos la JOYA S.A. y se convierte en el primer paso hacia el fortalecimiento y estandarización de la seguridad de la información.

### 5.3 Generar un documento con las políticas de la seguridad de la información establecidas para la empresa, basado en los requerimientos de seguridad con el estándar ISO 27001.

Las políticas de seguridad de la información deben velar por que se mantengan protegidos los datos de la empresa, de los empleados y de los clientes. Para definirlas se debe analizar la situación actual de la misma en cuanto a la seguridad de la información y las reglas ya establecidas y a partir de esto se determinaron las áreas que se quieren abarcar en la empresa utilizando los apartados de la norma ISO 27001.

Luego de esto se lleva a cabo la confección del documento formal de Políticas de Seguridad de la Información. En el Apéndice 1, se presenta el documento, en el que se desarrollan los argumentos con el fin de cumplir con el objetivo general de este trabajo.

# CAPÍTULO VI: Conclusiones y Recomendaciones

## 6.1 Conclusiones

El autor de este trabajo llega a las siguientes conclusiones:

A pesar de que se cuenta con reglas internas que establecen una línea base a seguir por los colaboradores, las mismas son muy generales, escuetas y no se encuentran transcritas en un documento.

El análisis de la situación actual que se realizó de la empresa reflejó las áreas principales a abarcar por la seguridad de la información, las cuales son principalmente en el área organizacional, ya que, por la naturaleza de estas, muchos controles tecnológicos no aplicaban.

Es esencial contar con un documento escrito con las políticas de seguridad, ya que el entorno tecnológico actual lo demanda. Esto permitirá a su vez una mejora continua en la empresa, no solo de orden sino también de ventaja competitiva frente a otras empresas.

La norma ISO 27001 es muy rica y cuenta con una gran cantidad de apartados para llevar a cabo controles de seguridad más robustos, sin embargo, por limitaciones en el alcance de la investigación se buscó que con las áreas seleccionadas se logre una mejora significativa y se aplique una mejora continua en la empresa.

El documento de políticas de seguridad de la información representa un avance significativo en la empresa Cárnicos la JOYA S.A. y se convierte en un hito que contribuye con el desarrollo de esta, permitiendo que su enfoque siga siendo las ventas, pero con el sustento de una estructura con bases seguras que la convierta en pionera dentro su área de desarrollo.

## 6.2 Recomendaciones

Una vez confeccionado el documento de políticas de seguridad de la información se plantean las siguientes recomendaciones para los beneficiarios.

Realizar la implementación del documento de políticas de la información a la brevedad, con el fin de que se empiece a fortalecer el área de la seguridad que tanto se requiere.

Realizar una campaña de información con el fin de involucrar a los empleados en estos nuevos cambios que traen las políticas. Esto facilitará la adopción de estas y reducirá la resistencia al cambio.

Llevar a cabo reuniones bimestrales para analizar la situación de la empresa con respecto a las políticas y gestionar cambios o adiciones correspondientes de acuerdo con la política establecida de revisión anual.

Estar abiertos a recomendaciones de los colaboradores, como de entes externos, sobre la creación de nuevas políticas que contribuyan al desarrollo de la empresa en materia de seguridad.

Iniciar un proceso de educación a lo interno de concientización en materia de seguridad de la información con el fin de generar una cultura organizacional que permita una adopción más sinérgica a estos nuevos cambios que trae el mundo que nos une el día de hoy.

# APÉNDICE 1

Fecha: Octubre 11, 2023

**Trabajo Final de Graduación**

**"Propuesta de Políticas de Seguridad de la Información para la Empresa Cárnicos La JOYA S.A."**

Elaborado por: Bernal Murillo Avila

| Nivel | Descripción genérica de la opción de respuesta |
|---|---|
| 1 | La empresa no cumple con lo que plantea la pregunta |
| 2 | La empresa cumple parcialmente que plantea la pregunta |
| 3 | La empresa cumple en gran medida lo que plantea la pregunta, pero no de forma estandarizada |

| A5. – Controles Organizativos | Respuestas | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1. ¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad específicas? | x | | |
| 2. ¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación? | x | | |
| 3. ¿Existen procedimientos para el manipulado de la información de acuerdo con su clasificación? | x | | |
| 4. ¿Se ha realizado un inventario de activos de información que dan soporte al negocio? | | x | |
| 5. ¿Se ha identificado al responsable de cada activo en cuanto a su seguridad? | x | | |
| 6. ¿Se han establecido normas para el uso de activos en relación con su seguridad? | x | | |
| 7. ¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato? | x | | |
| 8. ¿Existen procedimientos para el traslado de activos de información para proteger su seguridad? | x | | |
| -Control de salidas<br>-Cifrado etc. | | | |
| 9. ¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo? | x | | |
| 10. ¿Existen procesos formales de registro de usuarios? | x | | |
| 11. ¿Existen procesos formales para asignación de perfiles de acceso? | x | | |
| 12. ¿Se ha establecido una política específica para el manejo de información clasificada como confidencial? | x | | |
| 13. ¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos? | x | | |
| 14. ¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso? | x | | |
| 15. ¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar? | x | | |
| 16. ¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.? | x | | |
| 17. ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras? | x | | |
| **A6. – Controles de Personas** | | | |
| 1. ¿Se investigan los antecedentes de los candidatos a puestos en la organización? | | x | |
| -Formación | | x | |
| -Experiencia | | x | |
| -Referencias | | x | |
| 2 ¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo? | x | | |
| 3. ¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas? | x | | |
| 4. ¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información? | x | | |
| 5. ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato? | x | | |
| 6. ¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información? | x | | |
| **A7. – Controles Físicos** | | | |
| 1. ¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados? | | | x |
| 2. ¿Se protegen los equipos contra fallos de suministro de energía? | | x | |
| 3. ¿Se planifican y realizan tareas de mantenimiento sobre los equipos? | | x | |
| 4. ¿Se controla y autoriza la salida de equipos, aplicaciones etc. | | x | |
| 5. ¿Se establecen protocolos para proteger o eliminar información de equipos que se dan de baja o van a ser reutilizados? | | x | |
| 6. ¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo? | x | | |
| **A8. – Controles Tecnológicos** | | | |
| 1. ¿Existen sistemas de detección para Software malicioso o *malware*? | | x | |
| 2. ¿Se ha establecido un sistema de copias de seguridad acorde con las necesidades de la información y de los sistemas? | | x | |
| 3. ¿Existe un procedimiento establecido para la gestión de cambios en los sistemas? | x | | |
| | | | |

## APÉNDICE 2

| | |
|---|---|
| Documento: | Políticas de seguridad de la información |
| Versión: | 1 |
| Compañía: | Cárnicos La JOYA S. A. |
| Autor: | Bernal Murillo Avila |
| Fecha: | Julio 2023 |
| Referencia: | ISO/IEC 27001:2023 |

**Tabla 14. Información del Documento de Políticas.**

**Fuente: Confección propia.**

# Políticas de Seguridad de la Información


Cárnicos La Joya S.A.

## Cárnicos La JOYA S.A.

**Alajuela, Costa Rica**

**Última revisión diciembre 2023**

## Política General de Seguridad de la Información

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de Cárnicos La JOYA S.A. con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información, incluido el hardware y el software), que soportan los procesos de la Entidad, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Cárnicos la JOYA S.A., para asegurar la dirección estratégica de la Entidad, establece los siguientes objetivos de seguridad de la información:

- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Cárnicos La JOYA S.A.

## Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de Cárnicos La JOYA S.A.

## Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento en un 100% la política.

## Políticas Específicas Recomendadas para la Implementación

En este documento se presentan recomendaciones de políticas de seguridad de la información basadas en una previa investigación del estado actual de la compañía. Se recomienda, de acuerdo con las mismas realizar una revisión anual con el fin de determinar si se requiere hacer cambios en cuanto a nuevas incorporaciones, modificaciones o exclusiones de estas.

### Política de Gestión de Activos

**Inventario de información:** Los activos de la empresa deberán ser registrados en un inventario. En el mismo se debe establecer el código interno o numeración del activo, la descripción, el responsable, la fecha en la cual se llevó a cabo el ingreso. Los activos nuevos de la empresa deben registrarse una vez que se adquieran.

El registro del inventario debe llevarse a cabo por parte del encargado de seguridad. Se registran todos los activos en el sistema, la información en el registro será considerada como restringida, por lo tanto, solo tendrán acceso los directores de las áreas y empleados específicos. El sistema de registro debe poseer campos de auditoría, en esta se guardará el usuario o nombre de la persona que hace el cambio en cualquiera de los campos, con la fecha y hora del momento en que se realizó el mismo.

**Política de Uso aceptable de la información y otros activos:** Los equipos deben mantenerse libres de programas maliciosos, por lo tanto, se prohíbe el uso de programas que no sean avalados por la Gerencia ya que estos pueden afectar el funcionamiento y desempeño de la computadora.

La información de la empresa, como documentos, respaldos de bases de datos y licencias no pueden utilizarse en dispositivos que no sean de Cárnicos La JOYA S.A. Además, se debe solicitar la aprobación por parte de la Gerencia para compartir la

información, se excluye la que es confidencial y que solo podrá ser compartida por la Gerencia.

La computadora debe contar con una contraseña con el fin de bloquear la pantalla para evitar que terceros accedan a la información en el equipo, este bloqueo debe hacerse de forma inmediata cuando el empleado se ausente de la computadora.

**Política de Clasificación de la información:** la información que se maneja en la empresa cuenta con diferentes tipos de nivel de importancia, por lo cual debe clasificarse según los niveles de protección y los tipos de documentos en los cuales se divide.

La información se clasificará en tres tipos, las cuales son:

- Información interna: tienen acceso todos los empleados de la empresa.
- Información restringida: tienen acceso los directores de las áreas y empleados específicos.
- Información confidencial: tiene acceso únicamente la Gerencia.

La información que se genere dentro de la organización debe identificarse con una etiqueta, las cuales serán:

**Documentos físicos:** todos aquellos documentos que se encuentran de forma física serán guardados en una carpeta con respecto a su área, el mes y el año en el cual fue generado el documento. Por ejemplo, si una Proforma de Ventas es de junio de 2023, se colocará en una carpeta con el nombre Proformas/Ventas-Junio 2023.

**Documentos digitales:** todos aquellos documentos que se generen de forma digital y que sean de la empresa se almacenarán en una carpeta llamada Documentos LA JOYA, dentro de la cual se encontrarán otras carpetas con el año en el que se generaron los documentos y dentro de esta estarán otras carpetas correspondientes al área del que forman parte. Por ejemplo, si es un documento del área de Compras, un orden de compra de 2023 se encontrará dentro de la carpeta Órdenes de compra que se

encontrará dentro de otra carpeta llamada 2020 que se colocará en una carpeta con nombre Compras.

**Política de Control de Acceso**

**Accesos:** La información referente al uso de los sistemas internos, como las cuentas y las contraseñas de cada empleado será gestionada por el Gerente Operativo. Este último se hará cargo de hacerle llegar la información al empleado, ya sea por un nuevo ingreso o porque se tuvo que llevar a cabo un cambio.

En ninguna circunstancia se puede solicitar información de acceso que no sea del empleado que realiza la solicitud. Las solicitudes deben hacerse de manera formal y por escrito. Los empleados serán los responsables de toda la actividad y el uso que tenga la cuenta, por esto, no se deben compartir las contraseñas.

**Política de Contraseñas:** Las contraseñas deben ser seguras, deben contar con una longitud mínima de diez caracteres y con al menos una letra mayúscula, una letra minúscula, un número y un carácter especial. Las contraseñas no pueden ser iguales a las tres anteriores y deben cambiarse cada tres meses.

Cárnicos LA JOYA S.A. se encargará de proveer las contraseñas cuando ingresa un nuevo empleado, las mismas deben cambiarse el mismo día por el empleado y debe cumplir con todas las especificaciones listadas anteriormente.

Las contraseñas de cada usuario no pueden ser compartidas en ninguna circunstancia con otros empleados, este será responsable de la confidencialidad de sus contraseñas.

Las contraseñas no se deben transcribir de ninguna forma en el área de trabajo. Las contraseñas no pueden guardarse en las preferencias del navegador o ningún tipo de almacenamiento local.

**Política de Pantalla y escritorio limpio:** Las pantallas de las computadoras, las laptops que son de propiedad de Cárnicos LA JOYA S.A., deben contar con los fondos de pantalla de la empresa, estos son proporcionados por la Gerencia. Al entregar los equipos de trabajo se deben incluir las imágenes de fondo de pantalla.

El escritorio debe mantenerse con un máximo de ocho aplicaciones, no se puede guardar en este ningún tipo de archivo como Microsoft Word, Excel, PowerPoint. En el escritorio puede haber un máximo de 10 aplicaciones, entre las que se deben encontrar:

- Dropbox.
- Firefox.
- Google Chrome.
- Microsoft Teams.
- OneNote.
- Outlook.
- Papelera de reciclaje.
- Skype.

**Política de Gestión de las Condiciones del Empleo**

La contratación de un nuevo empleado se debe llevar a cabo con la firma de un contrato entre el empleador y el trabajador, en este se establecen las actividades del trabajador y el compromiso del empleador por su cumplimiento. El contrato debe establecer, además de la información legal y personal inherente a la contratación, claros compromisos con la seguridad de la información, como las siguientes:

- La información que se debe incluir es el nombre completo, edad, estado civil, profesión, identificación y dirección, en conjunto con el nombre y la cédula jurídica de la empresa.
- Los servicios que prestará el empleado dentro de la compañía.
- El salario que se le pagará al empleado, las fechas y la forma en la que se harán los pagos.

- Se debe velar por la protección del material confidencial. La información categorizada como interna, restringida o confidencial no puede publicarse, compartirse o revelarse.
- Se debe proteger la información de los clientes, por lo que no se puede publicar, compartir o revelar ningún tipo de información con la que cuente Cárnicos La JOYA S.A.
- Firmas de empleado y empleador con la fecha, esto define que se reconoce y se entiende lo establecido en el contrato.

**Acuerdos de Confidencialidad:** Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Basados en los requisitos de seguridad de la información de Cárnicos la JOYA S.A. aplica para toda la documentación desarrollada o que forma parte de la empresa en especial la información Confidencial. Durante la firma del contrato se debe firmar un acuerdo de Confidencialidad en el que se incluya la siguiente información.

a) Información a proteger (por ejemplo, información confidencial).
b) Duración esperada de un acuerdo, incluidos los casos en que puede ser necesario mantener la confidencialidad indefinidamente.
c) Las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada.
d) La propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial.
e) El derecho a auditar y monitorear actividades que involucren información confidencial para circunstancias altamente sensibles.
f) Las acciones previstas a tomar en caso de incumplimiento del acuerdo.

**Política para la Gestión de las Políticas de Seguridad**

De manera anual se debe realizar una revisión de las políticas con el fin de determinar si las mismas cumplen las expectativas, si hay oportunidad de mejora en las

actuales, cuáles ya no aplican y la creación de nuevas políticas para robustecer la seguridad de la información.

**Política para la Gestión de las Vulnerabilidades**

Las computadoras o laptops que utilicen los empleados deben tener instalada y sincronizada la aplicación de Kaspersky. La misma debe estar programada para realizar escaneos semanales completos de la computadora. Se debe mantener activo el Anti-Virus y en ninguna circunstancia deberá ser removido o deshabilitado. Como parte del mantenimiento preventivo, el equipo técnico deberá documentar la información relacionada a archivos en cuarentena, amenazas recibidas y correo spam. De igual manera el equipo técnico será el que vele por la actualización del antivirus.

**Política para la Gestión de Respaldos**

Las computadoras o laptops que utilicen los empleados deben tener instalada y sincronizada la aplicación de Dropbox. En la misma se deberá copiar la información que se maneje de la empresa y estas deben encontrarse siempre en sincronización.

Las bases de datos que se crean o son manejadas dentro de la empresa deben mantener un respaldo de seguridad completo diario. En caso de bases de datos de mayor importancia deben mantenerse en conjunto con siete respaldos que corresponden a cada día de la semana.

# Bibliografía


Ali, R. F., Dominic, P. D., Ali, S. E., & & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383.

Barman, S. (2007). *Writing Information Security Policies.* New Riders Publishing.

BECOLVE. (2021). *Becolve Digital.* Obtenido de https://becolve.com/blog/estandares-de-ciberseguridad-que-son-y-para-que-sirven/

Cram, W. A. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems volume*, 605–641 .

Equipo editorial, E. D. (2023). *Enciclopedia Humanidades.* Obtenido de Normas en General: https://humanidades.com/normas-en-general/

ESET. (18 de 11 de 2021). Obtenido de https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-adelanta-hacia-donde-evolucionan-las-amenazas-y-los-desafios-de-la-ciberseguridad/

FTC. (2023). *Federal Trade Comission*. Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Iberdrola, S. (2023). *Iberdrola, S.A.* Obtenido de https://www.iberdrola.com/innovacion/ciberataques

IBM. (2023). *IBM Security.* Obtenido de https://www.ibm.com/es-es/topics/ransomware

Incibe. (2017). *Instituto Nacional de Seguridad.* Obtenido de https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO. (2009). *Guía ISO 73: 2009.* Obtenido de https://www.pmg-ssi.com/2014/08/iso-27001-gestion-riesgos-seguridad-informacion-pymes/

ISO. (s.f.). *ISO*. Obtenido de https://www.iso.org/about-us.html

ISO27001, E. (2023). *Norma ISO27001*. Obtenido de https://normaiso27001.es/

López, I. (24 de 05 de 2022). Obtenido de https://elceo.com/negocios/hot-sale-ciberataques-a-la-orden-del-dia-y-las-pymes-son-las-mas-vulnerables/

Magazine, C. (2023). Obtenido de https://www.ceupe.com/blog/que-es-cobit.html

Norton. (08 de 08 de 2018). Obtenido de https://lam.norton.com/blog/malware/what-is-a-computer-virus#:~:text=En%20t%C3%A9rminos%20m%C3%A1s%20t%C3%A9cnicos%2C%20un,fin%20de%20ejecutar%20su%20c%C3%B3digo.

NQA. (2023). Obtenido de https://www.nqa.com/es-mx/resources/blog/february-2023/iso-27001-transition

Paananen, H., Lapke, M., & & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, 101608.

Paulsen, C., & Toth, P. (2016). Small Business Information Security: The Fundamentals. *NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1*.

Peltier, T. R. (2001). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.* CRC Press, Inc., USA.

Rostami, E., Karlsson, F., & & Kolkowska, E. (2020). The hunt for computerized support in information security policy management: a literature review. *Information & Computer Security.*

Samaniego Mena, E., & Ponce Ordoñez, J. (2021). *Fundamentos de seguridad informática.*

Soto, E. (19 de 05 de 2022). Obtenido de https://www.monumental.co.cr/2022/05/19/nueve-de-cada-diez-pymes-en-costa-rica-empezaron-a-vender-via-internet-en-los-ultimos-dos-anoss/

*TagCrowd*. (s.f.). Obtenido de https://tagcrowd.com/

Verizon. (2022). *2022 DBIR*. Obtenido de https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir-industries.pdf

Washington, U. d. (2023). *Office of Information Security*. Obtenido de https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/