UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
FACULTAD DE INGENIERÍA

# IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO 27001:2022 EN LA COOPERATIVA DE SERVICIOS MÚLTIPLES EL EDUCADOR VERAGÜENSE, DURANTE EL PERIODO 2022-2023

SANTIAGO YORIEL GARCÍA DÍAZ

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO DE MAESTRÍA EN INGENIERÍA DE AUDITORÍA Y GESTIÓN DE PROCESOS

ASESOR
DOCTOR JORGE MARTINEZ

PANAMÁ, REPUBLICA DE PANAMÁ
2024

## Dedicatoria

A Jesucristo, por darme la capacidad y la vida. Quiero glorificarte con cada logro y cada paso que doy. Tu amor y gracia han sido mi guía constante, y sin Ti, nada de esto sería posible.

A mi familia, por su respaldo y apoyo incondicional. Gracias por creer en mí, por cada palabra de aliento y por estar siempre a mi lado. Su amor y sacrificio han sido la base sobre la cual he construido este sueño. Esta tesis es tanto suya como mía.

## Agradecimiento

A Jesucristo, por darme la vida, la fuerza y la sabiduría para alcanzar este logro. Sin Tu guía y amor incondicional, nada de esto sería posible. Toda la gloria es para Ti.

A mi esposa, Sofía, por su amor, paciencia y apoyo incondicional. Gracias por estar a mi lado en cada paso de este camino.

A mis hijos, Alessia, Alissa y Thiago, quienes son mi mayor inspiración y motivo para seguir adelante.

A mis padres, Yolanda Díaz Centeno y Santiago García Bósquez, por siempre creer en mí y ser mi pilar de fortaleza. Su amor y sacrificio han sido la base de mi éxito.

Al Dr. Jorge Martínez, por su invaluable apoyo y confianza al ser mi asesor en esta tesis. Su guía y conocimiento han sido fundamentales para la realización de este trabajo.

## Resumen

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 surge como una respuesta estratégica a esta necesidad. La norma ISO 27001:2022 proporciona un marco internacionalmente reconocido para gestionar y proteger la información sensible, garantizando su confidencialidad, integridad y disponibilidad. La presente investigación tiene como objetivo general implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.) durante el periodo 2022-2023, basándose en los requisitos de la norma ISO 27001:2022. El estudio surge ante la creciente necesidad de proteger la información crítica y confidencial de la cooperativa, así como de fortalecer la gestión de riesgos asociados a la seguridad de la información. La metodología empleada en esta investigación incluyó el uso de encuestas como técnica principal, con un cuestionario como instrumento de medición. Para el análisis de los datos recopilados, se utilizó el software Excel, lo que permitió procesar y organizar la información de manera efectiva. Además, se recabó información clave sobre el Sistema de Seguridad de la Información, lo que fue fundamental para el diseño del SGSI, asegurando que se abordaran adecuadamente los requisitos de la norma ISO 27001:2022 y las necesidades específicas de la cooperativa. Los resultados indican que la implementación del SGSI no solo mejoró la seguridad de la información en un 20%, sino que también incrementó la confianza de los asociados en los procesos de la cooperativa en un 30%, garantizando la continuidad operativa y el cumplimiento con los estándares internacionales. En conclusión, la implementación del sistema cumple con el objetivo de adopción de la norma ISO 27001:2022 es un paso crucial para COOPEVE, R.L., recomendando la revisión periódica del SGSI y la actualización continua de los controles de seguridad para mantener la efectividad del sistema a largo plazo.

**Palabras clave:** Seguridad de la Información, ISO 27001:2022, Gestión de Riesgos, Cooperativa, Protección de Datos.

**Abstract**

The implementation of an Information Security Management System (ISMS) under the ISO 27001:2022 standard emerges as a strategic response to this need. ISO 27001:2022 provides an internationally recognized framework for managing and protecting sensitive information, ensuring its confidentiality, integrity, and availability. The primary objective of this research is to implement an ISMS at the Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.) during the 2022-2023 period, based on the requirements of the ISO 27001:2022 standard. The study is driven by the growing need to protect the cooperative's critical and confidential information, as well as to strengthen the management of risks associated with information security. The methodology employed in this research included the use of surveys as the main technique, with a questionnaire as the measurement instrument. Excel software was used for data analysis, allowing for effective processing and organization of the information. Additionally, key information about the Information Security System was gathered, which was crucial for the design of the ISMS, ensuring that the requirements of the ISO 27001:2022 standard and the specific needs of the cooperative were adequately addressed. The results indicate that the implementation of the ISMS not only improved information security by 20%, but also increased the trust of members in the cooperative's processes by 30%, ensuring operational continuity and compliance with international standards. In conclusion, the implementation of the system meets the objective of adopting the ISO 27001:2022 standard, a crucial step for COOPEVE, R.L. It is recommended to periodically review the ISMS and continuously update security controls to maintain the system's effectiveness in the long term.

**Keywords:** Information Security, ISO 27001:2022, Risk Management, Cooperative, Data Protection.

# Índice

I. EL PROBLEMA DE LA INVESTIGACIÓN ..... 15

1.1 Planteamiento del Problema ..... 15

1.2 Formulación del problema ..... 21

1.3 Justificación de la investigación ..... 22

1.4 Objetivos de la investigación ..... 24

1.4.1 Objetivo general ..... 24

1.4.2 Objetivos específicos ..... 24

1.5 Hipótesis ..... 25

1.5.1 Hipótesis del investigador ..... 25

1.5.2 Hipótesis Nula H0 ..... 26

1.6 Operacionalización de las variables ..... 26

1.6.1 Variable 1: Seguridad de la Información ..... 26

1.6.1.1 Definición Conceptual. ..... 26

1.6.1.2 Definición Operacional. ..... 27

1.6.2 Variable 2: Capacitación en Seguridad de la Información ..... 27

1.6.2.1 Definición Conceptual. ..... 27

1.6.2.2 Definición Operacional. ..... 28

1.6.2.2.1 Instrumentos de Medición ..... 28

1.7 Alcances y limitaciones de la investigación ..... 29

1.7.1 Alcances ..... 29

1.7.2 Limitaciones ..... 29

1.7.2.1 Limitación temporal ..... 29
1.7.2.2 Limitación espacial ..... 29
II. MARCO TEÓRICO ..... 30
2.1 Antecedentes de la investigación ..... 30
2.1.1 A nivel internacional ..... 30
2.1.2 A nivel regional ..... 41
2.1.3 A nivel nacional ..... 43
2.2 Bases Teóricas ..... 44
2.2.1 Definición de las variables ..... 45
2.2.2 Importancia de las variables ..... 46
2.2.3 Las bases en que define la investigación ..... 47
2.2.4 Importancia de las bases teóricas ..... 47
2.2.5 Seguridad de la información vs seguridad informática ..... 49
2.2.5.1 Confidencialidad. ..... 50
2.2.5.2 Integridad. ..... 50
2.2.5.3 Disponibilidad ..... 50
2.2.6 Seguridad Informática ..... 51
2.2.7 Norma ISO 27001:2022 ..... 55
2.2.8 Importancia de la Implementación del SGSI en Cooperativas en Panamá 56
2.2.9 Modelos de Gestión de la Seguridad de la Información ..... 57
2.2.10 Retos en la Implementación del SGSI ..... 59
2.2.11 Beneficios de la Implementación de un SGSI ..... 60
III. METODOLOGÍA DE LA INVESTIGACIÓN ..... 67

3.1 Enfoque y nivel de la investigación ..... 67
3.2 Diseño de la investigación ..... 68
3.3 Población y muestra ..... 68
3.3.1 Población ..... 68
3.3.2 Tamaño de la Muestra: Tipo de muestreo ..... 69
3.4 Técnicas e instrumentos para la recolección de la información de campo ..... 70
3.4.1 Técnica ..... 70
3.4.2 Instrumento ..... 70
3.5 Análisis y procesamiento de datos ..... 72
IV. RESULTADOS ..... 73
4.1 Consideraciones Iniciales ..... 73
4.1.1 Partes Interesadas ..... 73
4.1.2 Recursos Disponibles ..... 75
4.1.3 Proceso Critico Identificado ..... 78
4.2 Metodología para la Gestión de Riesgo ..... 81
4.3 Valoración de Activos Críticos ..... 85
4.3.1 Identificación de Activos ..... 85
4.3.2 Valoración de Activos ..... 89
4.3.3 Identificación de Amenazas y Vulnerabilidades ..... 95
4.3.4 Valoración de Amenaza y Vulnerabilidades ..... 102
4.3.4.1 Activo 1. Sistema Financiero ..... 103
4.3.4.2 Activo 2. Cajas ..... 104
4.3.4.3 Activo 3. Atención al Cliente ..... 106

4.3.4.4 Activo 4. Servicio de ATM ..... 108
4.3.4.5 Activo 5. Seguridad Perimetral ..... 109
4.3.5 Controles Existentes ..... 110
4.3.5.1 Control 1. Activo Sistema Contable ..... 111
4.3.5.2 Control 2 Activo. Cajas ..... 111
4.3.5.3 Control 3 Activo: Seguridad Perimetral ..... 113
4.3.6 Evaluación de Riesgos ..... 114
4.3.7 Tratamiento de Riesgos ..... 115
4.3.7.1 Diseño de Controles ..... 118
4.3.7.2 Tipos de Controles ..... 118
4.3.7.3 Roles y Responsabilidades para el SGSI ..... 119
4.4 Ciclo PDCA ..... 121
4.4.1 Fase Planificar / Plan ..... 122
4.4.1.1 Alcance del SGSI ..... 123
4.4.1.2 Política de Seguridad ..... 124
4.4.1.3 Metodología para la Evaluación del Riesgo ..... 126
4.4.1.4 Amenazas y Vulnerabilidades ..... 127
4.4.1.5 Identificación de Activos y Amenazas ..... 130
4.4.1.6 Identificación del Impacto ..... 137
4.4.1.7 Analisis y Evaluación del Riesgo ..... 155
4.4.1.8 Identificación de Activos y Amenazas ..... 155
4.4.1.9 Selección de Controles ..... 159
4.4.2 Fase Hacer / Do ..... 162

4.4.2.1 Aplicar el SGSI ..... 162
4.4.2.2 Plan de tratamiento de riesgos ..... 163
4.4.2.3 Selección de Controles ..... 164
4.4.2.4 Capacitación y Concientización ..... 165
4.4.3 Fase Controlar ..... 166
4.4.3.1 Revisar el SGSI ..... 166
4.4.3.2 Medir la Eficacia de los Controles ..... 166
4.4.3.3 Revisar los Riesgos Residuales ..... 167
4.4.3.4 Realizar Auditorías Internas del SGSI ..... 168
4.4.3.5 Registrar Eventos y Acciones ..... 168
4.4.4 Fase Actuar ..... 169
4.4.4.1 Implementar Mejoras al SGSI ..... 169
4.4.4.2 Aplicar Acciones Correctivas ..... 170
4.4.4.3 Aplicar Acciones Preventivas ..... 171
4.4.4.4 Comprobar la Eficacia de las Acciones ..... 171
4.4.5 Políticas, Estándares y Procedimientos ..... 172
4.4.5.1 Diseño de Políticas ..... 172
4.4.5.2 Identificación de Indicadores Clave ..... 175
4.4.5.3 Desarrollo de Métricas ..... 175
4.4.5.4 Priorización del Incidente ..... 176
4.4.5.5 Gestión de Recursos para el SGSI ..... 180
V. DISCUSIÓN DE RESULTADOS ..... 182
5.1 Contrastación de las Hipótesis ..... 182

5.2 Hipótesis General ..... 182
5.3 Hipótesis Nula (H0) ..... 182
5.4 Resultados ..... 183
5.5 Contrastación de los Resultados con Estudios Similares ..... 183
5.5.1 Estudio 1 ..... 184
5.5.2 Estudio 2 ..... 184
5.5.3 Estudio 3 ..... 185
VI. CONCLUSIONES ..... 186
VII. RECOMENDACIONES ..... 187
VIII. REFERENCIAS BIBLIOGRÁFICAS ..... 188
IX. ANEXOS ..... 196

## Índice de Tablas

**Tabla 1** Comparativa entre Seguridad de la Información vs Seguridad Informática .. 52

**Tabla 2** Partes interesadas ..... 73

**Tabla 3** Matriz comparativa selección Metodología de Riesgo ..... 82

**Tabla 4** Inventario de Activos pc ..... 85

**Tabla 5** Matriz de Categorías de Activos conforme a la Norma ISO 27005:2018 ..... 87

**Tabla 6** Guía inventario de activos en la implementación de la norma 27001:2022 ..... 90

**Tabla 7** Matriz de riesgo con su valoración ..... 94

**Tabla 8** Riesgos identificados ..... 96

**Tabla 9** Fuentes de Amenazas Humanas ..... 99

**Tabla 10** Activo 1: Sistema Financiero ..... 104

**Tabla 11** Activo 2: Cajas ..... 105

**Tabla 12** Activo 3: Atención al Cliente ..... 107

**Tabla 13** Activo 4: Servicio de ATM ..... 109

**Tabla 14** Activo 5: Seguridad Perimetral ..... 110

**Tabla 15** Evaluación de los activos basado en Riesgo ..... 114

**Tabla 16** Matriz de Tratamiento del Riesgo ..... 116

**Tabla 17** Fases del modelo Deming o Cicle Shewhart ..... 121

**Tabla 18** Matriz de Riesgos de inventario ..... 126

**Tabla 19** Activos basados en el nivel de riesgo ..... 129

**Tabla 20** Clasificación de la información según la triada ..... 132

**Tabla 21** Activos analizados según la amenaza y vulnerabilidad para el nivel de riesgo ..... 133

**Tabla 22** Matriz de la triada según activo ..... 135

**Tabla 23** Descripción de activos en base a su operación en el negocio ..... 155

**Tabla 24** Identificación de amenazas y vulnerabilidades ..... 157

**Tabla 25** Evaluación del Impacto y Probabilidad ..... 158

**Tabla 26** Controles de nueva versión ISO 27001:2022 ..... 160

**Tabla 27** Establecimiento del control según el activo ..... 161

**Tabla 28** Plan de implementación de controles ..... 164

**Tabla 29** Matriz de Priorización ..... 177

## Índice de Figuras

**FIGURA 1** EVOLUCIÓN DE LOS CONTROLES DE SEGURIDAD EN VERSIONES ISO/IEC 27001 ..... 40

**FIGURA 2** TRÍADA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD (CIA)..... 50

**FIGURA 3** ANALISIS FODA SGSI ..... 72

**FIGURA 4** CICLO PDCA Y SUS PARTES INTERESADAS..... 123

**FIGURA 5** PREGUNTA 1 - ENCUESTA..... 138

**FIGURA 6** PREGUNTA 2 - ENCUESTA..... 139

**FIGURA 7** PREGUNTA 3 - ENCUESTA..... 140

**FIGURA 8** PREGUNTA 4 - ENCUESTA..... 141

**FIGURA 9** PREGUNTA 5 - ENCUESTA..... 142

**FIGURA 10** PREGUNTA 6 - ENCUESTA..... 143

**FIGURA 11** PREGUNTA 7 - ENCUESTA..... 144

**FIGURA 12** PREGUNTA 8 - ENCUESTA..... 145

**FIGURA 13** PREGUNTA 9 - ENCUESTA..... 146

**FIGURA 14** PREGUNTA 10 - ENCUESTA..... 147

**FIGURA 15** PREGUNTA 11 - ENCUESTA..... 148

**FIGURA 16** PREGUNTA 12 - ENCUESTA..... 149

**FIGURA 17** PREGUNTA 13 - RESPUESTA ..... 150

**FIGURA 18** PREGUNTA 14 - ENCUESTA..... 151

**FIGURA 19** PREGUNTA 15 - ENCUESTA..... 152

**FIGURA 20** PREGUNTA 16 - ENCUESTA..... 153

# I. EL PROBLEMA DE LA INVESTIGACIÓN

## 1.1 Planteamiento del Problema

La investigación se estructura en varias fases, comenzando con un diagnóstico inicial que evaluó el estado actual de la seguridad de la información en COOPEVE, R.L. Posteriormente, se diseñó un plan de implementación que abarcó la formación del personal, la identificación de activos de información, la evaluación de riesgos, y la definición de controles de seguridad.

A NIVEL GLOBAL

Las estadísticas financieras de las cooperativas revelan tendencias y patrones en términos de ingresos, gastos, activos, pasivos y rentabilidad. Algunos problemas comunes incluyen la falta de capitalización adecuada, dependencia excesiva de la deuda, insuficiente generación de ingresos o bajo nivel de rentabilidad. Estos problemas financieros pueden deberse a la falta de acceso a financiamiento, a la gestión financiera inadecuada, a la falta de diversificación de ingresos o a la ausencia de estrategias de mercado efectivas. Según la Alianza Cooperativa Internacional (2024), más del 12 % de la población mundial es cooperativista de alguna de las 3 millones de cooperativas del planeta, las cuales generan ingresos de aproximadamente 2,14 billones de dólares, al mismo tiempo que suministran los servicios y las infraestructuras que la sociedad necesita para prosperar.

A NIVEL REGIONAL

Las estadísticas financieras de las cooperativas pueden revelar disparidades significativas en su desempeño financiero entre diferentes regiones o países. Por ejemplo, algunas regiones pueden experimentar un crecimiento más pronunciado en ingresos y activos cooperativos. Según *Scriesgo Rating Agency* (2017), en diciembre de 2017, la SUGEF supervisaba 24 cooperativas que contabilizaban un total de activos de ¢3.185.531,67 millones. Este monto representó un

crecimiento cercano al 9% en comparación con diciembre de 2016, lo que se traduce en un incremento anual de ¢257.263,80 millones. El 92% de los activos totales estaba concentrado en las 10 cooperativas más grandes del sector. COOPENAE lideraba con un 23% de participación, seguida de COOPESERVIDORES con un 22% y COOPEANDE N° 1 con un 17%. Es importante destacar que los asociados de las principales cooperativas de ahorro y crédito en Costa Rica provienen mayoritariamente del sector público.

A NIVEL NACIONAL

Las cooperativas operan en una variedad de sectores económicos a nivel mundial, regional y nacional, incluyendo Panamá. Su objetivo principal es mejorar las condiciones económicas y sociales de sus socios a través de la cooperación y la participación en la toma de decisiones. En Panamá, las estadísticas financieras de las cooperativas pueden reflejar su salud financiera y su capacidad para cumplir con estos objetivos. Según IPACOOP (2023), en el país operan 587 cooperativas, con más de 230,000 asociados y activos que superan los B/. 2,700 millones, aportando aproximadamente un 4% al Producto Interno Bruto (PIB).

La Superintendencia de Bancos de Panamá es la entidad estatal encargada de supervisar y regular los bancos, las fiduciarias, y el negocio bancario en general. Por otro lado, el Instituto Panameño Autónomo Cooperativo (IPACOOP) es responsable de registrar, apoyar, supervisar, dirigir y ejecutar las políticas cooperativas en Panamá. En el caso de Ecuador, el enfoque regulatorio difiere. Según Morales (2022), la Superintendencia de Bancos de Ecuador se estableció como entidad reguladora para supervisar y controlar las actividades de las entidades financieras y de seguridad social, tanto públicas como privadas, con el fin de garantizar y fortalecer los intereses de la ciudadanía. Además, esta institución promueve que las cooperativas de ahorro y crédito cumplan con las obligaciones impuestas por el organismo regulador.

En el contexto de las cooperativas panameñas reguladas por el Instituto Panameño Autónomo Cooperativo (IPACOOP) y que operan en la industria de intermediación financiera, es crucial implementar medidas y acciones que protejan los intereses de los socios y aseguren el cumplimiento de las normativas establecidas por el IPACOOP y las leyes financieras aplicables en Panamá. Sin embargo, a pesar de la importancia de estas medidas, no existe una normativa legal que obligue a las cooperativas en el territorio panameño a adoptar un estándar de seguridad específico. En el caso de la industria sanitaria, según Salazar & Aviles (2023), implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 en las entidades sanitarias, al igual que en cualquier tipo de organización, implica enfrentar diversos retos y aplicar buenas prácticas. Entre estas se incluyen lograr el compromiso de la alta dirección, identificar y gestionar riesgos, establecer políticas de seguridad, y formar y concienciar al personal sobre la seguridad de la información.

Esto significa que las cooperativas deben, por iniciativa propia, asegurarse de cumplir con los requisitos legales y normativos establecidos por el IPACOOP y otras autoridades regulatorias pertinentes. Además, deben adherirse a las mejores prácticas en gobierno corporativo y gestión de riesgos. Es fundamental que los socios estén bien informados sobre las actividades financieras de la cooperativa, los productos y servicios ofrecidos, los riesgos asociados y sus derechos y responsabilidades como miembros.

La gestión prudente de los recursos financieros es esencial y debe incluir controles internos robustos y sistemas de reporte efectivos que garanticen la protección y el uso transparente de los fondos de los socios. Una comunicación clara y transparente con los socios y otros stakeholders relevantes, así como la promoción de una cultura de ética y responsabilidad en la gestión, son aspectos fundamentales para el éxito y la sostenibilidad de la cooperativa.

Para las cooperativas de ahorro y crédito o de servicios múltiples que buscan implementar la norma ISO 27001:2022 como un marco para establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), el desafío puede ser considerable. Cumplir con los requisitos de esta estándar resulta complejo, especialmente para aquellas organizaciones que carecen de experiencia previa en la implementación de sistemas de gestión y estándares de seguridad de la información, y que deben manejar con claridad los riesgos asociados. Abazi (2020) señala que, "One of the first requirements during the implementation of ISO27001 is the definition of risk assessment within the organization. According to standard requirements, the risk assessment methodology should be based on business, information security as well as other legal and regulatory requirements that enable accurate identification of the level of risk." [Uno de los primeros requisitos durante la implementación de la ISO27001 es la definición de la evaluación de riesgos dentro de la organización. Según los requisitos de la norma, la metodología de evaluación de riesgos debe basarse en los requisitos de negocio, de seguridad de la información y otros requisitos legales y reglamentarios que permitan identificar con precisión el nivel de riesgo.]

La gestión eficiente de la seguridad de la información es una preocupación crucial en la era digital, donde las ciberamenazas y las brechas de seguridad presentan desafíos significativos para las organizaciones. Implementar de manera efectiva la norma ISO 27001:2022 exige un enfoque sistemático y holístico para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información. La falta de un marco estructurado y claro para medir y comunicar el desempeño en seguridad de la información puede conducir a decisiones ineficaces y a una falta de dirección en la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Cuenca (2019) subraya que la ausencia de políticas, procedimientos y controles adecuados en los procesos

de seguridad es evidente, lo que resulta en que los usuarios no tomen las precauciones mínimas para cumplir con las normativas institucionales.

Una postura de seguridad débil ante un incidente conlleva un alto nivel de riesgo tanto para la organización como en el cumplimiento de las normativas legales. En Estados Unidos, se han desarrollado regulaciones que refuerzan la protección de los datos personales. (Allendevaux, 2021) "points out that in the current data privacy context, there is growing support for a kind of digital "Bill of Rights" that would guarantee individuals certain rights over their data. This includes, for example, the right to request the transfer of their data to another company or the deletion of their data by a company. These are examples of data subject rights, which are part of a broader set of rights that are evolving in territories that support them to protect their citizens." [señala que en el contexto actual de la privacidad de los datos, existe un creciente apoyo hacia una especie de "Carta de Derechos" digital que garantizaría a las personas ciertos derechos sobre sus datos. Esto incluye, por ejemplo, el derecho a solicitar la transferencia de sus datos a otra empresa o la eliminación de sus datos por parte de una compañía. Estos son ejemplos de los derechos de los titulares de datos, los cuales forman parte de un conjunto más amplio de derechos que están evolucionando en territorios que los respaldan para proteger a sus ciudadanos.]

Descripción de la realidad problemática

La Cooperativa de Servicios Múltiples El Educador Veragüense enfrenta una serie de desafíos significativos en la gestión de la seguridad de la información. A pesar de su papel crucial como entidad de intermediación financiera en la región, la cooperativa aún no ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022. Esto plantea problemas que afectan tanto su seguridad operativa como su cumplimiento normativo. Es bien sabido que la norma ISO/IEC 27001 es un requisito

indispensable en la mayoría de las organizaciones, especialmente en aquellas dedicadas a las tecnologías de la información. No es sorprendente que sea una de las normas más implementadas en el mundo, ocupando el segundo lugar después de la famosa ISO 9001(Infosecurity Mexico, 2021).

Ausencia de un Sistema de Gestión Estructurado: Actualmente, la Cooperativa de Servicios Múltiples El Educador Veragüense no dispone de un marco sistemático para la gestión de la seguridad de la información, lo que limita la capacidad para evaluar adecuadamente los riesgos y establecer controles efectivos para proteger la información sensible. Esta ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) estructurado impide la implementación de medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información. Según (Contero, 2019), La norma ISO 27001:2013 está diseñada para proporcionar los requisitos necesarios para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información. Esta norma promueve la mejora continua en la gestión de la seguridad de la información, ayudando a las organizaciones a proteger sus activos informáticos y a responder adecuadamente a las amenazas y vulnerabilidades.

Riesgos de Seguridad de la Información: Sin un sistema de gestión estandarizado como el propuesto por la norma ISO 27001:2022, la cooperativa enfrenta riesgos significativos relacionados con la seguridad de la información. Estos riesgos incluyen vulnerabilidades a ciberataques, brechas de datos y fallos en el control de accesos, los cuales pueden comprometer la integridad, confidencialidad y disponibilidad de la información.

Cumplimiento Normativo Inadecuado: La falta de alineación con la norma ISO 27001:2022 también implica un incumplimiento de los estándares internacionales de seguridad de

la información. Esto puede llevar a sanciones regulatorias, pérdida de confianza por parte de socios y clientes, y daños a la reputación de la cooperativa.

Ineficiencia en la Gestión y Protección de Datos: Sin un SGSI adecuado, la cooperativa puede enfrentar desafíos en la gestión eficiente de la información. La falta de procesos definidos y controles internos robustos limita la capacidad de la cooperativa para proteger sus datos, gestionar incidentes de seguridad y asegurar la continuidad operativa.

Necesidad de Mejora Continua: La implementación de un SGSI conforme a ISO 27001:2022 es fundamental para establecer un proceso de mejora continua en la gestión de la seguridad de la información. La norma proporciona un marco para identificar, evaluar y mitigar riesgos, así como para revisar y mejorar continuamente las políticas y procedimientos de seguridad.

La implementación de un Sistema de Gestión de Seguridad de la Información bajo la norma ISO 27001:2022 durante el periodo 2022-2023 se presenta como una solución esencial para abordar estos problemas. Este sistema permitirá a la Cooperativa de Servicios Múltiples El Educador Veragüense fortalecer su seguridad operativa, cumplir con los estándares internacionales, y proteger adecuadamente la información de sus socios y clientes.

## 1.2 Formulación del problema

¿La implementación de un Sistema de Gestión de Seguridad de la Información conforme a la Norma ISO 27001:2022 permitirá controlar eficazmente la seguridad de la información en la Cooperativa de Servicios Múltiples El Educador Veragüense durante el periodo 2022-2023?

## 1.3 Justificación de la investigación

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO 27001:2022 puede ofrecer mejoras significativas en la gestión de la seguridad de la información. Este enfoque permite a las organizaciones cumplir con los requisitos de seguridad establecidos por sus clientes, socios comerciales y otras partes interesadas. Al implementar un SGSI conforme a la norma ISO 27001:2022, se fortalece la protección de la información crítica, lo que no solo aumenta la confianza de los clientes en la organización, sino que también mejora su posición competitiva en el mercado.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense ofrecerá herramientas clave para evaluar y mejorar el estado actual de la seguridad de la información de la organización. Este sistema permitirá realizar un diagnóstico exhaustivo de las prácticas y controles existentes, facilitando la identificación de áreas que requieren ajustes y mejoras conforme a los estándares internacionales establecidos. Al adoptar este enfoque sistemático, la cooperativa podrá garantizar una protección más robusta de sus activos de información, alinear sus procesos con las mejores prácticas de seguridad y cumplir con las normativas vigentes, contribuyendo así a una gestión más eficiente y segura de la información.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2022 permite establecer un enfoque integral para la gestión de la seguridad de la información en una organización. Este enfoque implica identificar, evaluar y tratar los riesgos relacionados con la seguridad de la información de manera estructurada. Al adoptar el estándar ISO 27001:2022, se mejora la gestión de la seguridad de la información, asegurando una protección más efectiva de los activos de información de la organización.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2022 puede proporcionar un marco estructurado que facilite a las organizaciones cumplir con las regulaciones y normativas de seguridad de la información. Este enfoque sistemático permite establecer políticas, procedimientos y controles efectivos para la gestión de la seguridad de la información, garantizando la protección de datos y la resiliencia ante amenazas y vulnerabilidades. La adopción de la norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense durante el período 2022-2023 facilitará el cumplimiento de los requisitos legales y la implementación de mejores prácticas en la gestión de riesgos y la seguridad de la información.

Al implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27001, es posible establecer indicadores específicos para la seguridad de la información que se alineen con los objetivos estratégicos de la organización. Esto proporciona una visión integral del desempeño en seguridad de la información y facilita la toma de decisiones estratégicas fundamentadas en datos precisos.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al estándar ISO 27001:2022 implica la definición de indicadores clave para la seguridad de la información y la generación de informes periódicos sobre el desempeño en este ámbito. Este enfoque promueve una mayor conciencia sobre la importancia de la seguridad de la información dentro de la organización y fomenta una cultura de seguridad entre los colaboradores. Además, el SGSI facilita la comunicación y el seguimiento del desempeño en seguridad de la información a todos los niveles de la organización, promoviendo así una mayor responsabilidad y compromiso con las prácticas de seguridad.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO 27001:2022 puede fortalecer la gestión de la seguridad de la información en la Cooperativa de Servicios Múltiples El Educador Veragüense. Esta implementación ayuda a la organización a cumplir con los requisitos de seguridad exigidos por clientes, socios comerciales y otros interesados, incrementando así la confianza en la cooperativa y potenciando su posición competitiva en el mercado.

Los resultados obtenidos de esta investigación permitirán mejorar el estado actual de la Cooperativa de Servicios Múltiples El Educador Veragüense en relación con sus controles de seguridad de la información. La implementación del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2022 proporcionará un marco sólido para fortalecer los controles existentes y aplicar prácticas de seguridad en nuevos proyectos o instalaciones futuras.

## 1.4 Objetivos de la investigación

### *1.4.1 Objetivo general*

Implementar un Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense, durante el periodo 2022-2023

### *1.4.2 Objetivos específicos*

Realizar un diagnóstico integral de la situación actual de la seguridad de la información en la Cooperativa, identificando brechas y áreas de mejora en comparación con los requisitos de la Norma ISO 27001:2022.

Desarrollar un inventario detallado de los activos de información de la Cooperativa, evaluando su valor y los riesgos asociados a cada uno, para asegurar una protección adecuada basada en el riesgo.

Implementar un marco de políticas y procedimientos de seguridad de la información que cumpla con los estándares de la Norma ISO 27001:2022, asegurando que se adapten a las necesidades específicas de la Cooperativa.

Diseñar e implementar controles de seguridad que mitiguen los riesgos identificados, garantizando la confidencialidad, integridad y disponibilidad de la información crítica para la operación de la Cooperativa.

Establecer un programa de capacitación y concientización en seguridad de la información para todos los colaboradores de la Cooperativa, con el fin de asegurar la correcta aplicación de las políticas y prácticas establecidas.

Desarrollar un plan de respuesta a incidentes que permita a la Cooperativa detectar, responder y recuperarse de manera efectiva ante posibles brechas de seguridad.

Implementar un sistema de monitoreo y auditoría continua para evaluar el desempeño del SGSI y asegurar el cumplimiento continuo con los requisitos de la Norma ISO 27001:2022.

Realizar evaluaciones periódicas y auditorías internas para identificar áreas de mejora y asegurar la efectividad del SGSI, realizando ajustes necesarios para mantener la conformidad con la norma.

## 1.5 Hipótesis

### *1.5.1 Hipótesis del investigador*

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2022 mejorará significativamente la protección de la información en la Cooperativa de Servicios Múltiples El Educador Veragüense, reduciendo las vulnerabilidades y fortaleciendo la capacidad de respuesta ante incidentes de seguridad durante el periodo 2022-2023.

### *1.5.2 Hipótesis Nula H0*

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la Norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense durante el periodo 2022-2023 no logrará mejorar significativamente la protección de la información, ya que los controles implementados no serán suficientes para mitigar adecuadamente las vulnerabilidades y amenazas identificadas, ni para asegurar una adecuada gestión de la confidencialidad, integridad y disponibilidad de la información.

## 1.6 Operacionalización de las variables

La operacionalización de las variables es un proceso fundamental en la investigación, ya que permite definir cómo se medirán y analizarán las variables de estudio. A continuación, se desarrollan las variables identificadas en el contexto de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en COOPEVE, R.L.

### *1.6.1 Variable 1: Seguridad de la Información*

#### 1.6.1.1 Definición Conceptual.

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información contra accesos no autorizados, alteraciones y destrucción.

#### 1.6.1.2 Definición Operacional.

Para medir la seguridad de la información en COOPEVE, R.L., se utilizarán los siguientes indicadores:

**Confidencialidad.** Número de incidentes de acceso no autorizado a la información.

**Integridad.** Número de incidentes de alteración no autorizada de la información.

**Disponibilidad.** Tiempo de inactividad de los sistemas críticos debido a incidentes de seguridad.

**Instrumentos de Medición:**

**Auditorías de Seguridad.** Evaluaciones periódicas para identificar vulnerabilidades y verificar el cumplimiento de las políticas de seguridad.

**Registros de Incidentes.** Documentación de todos los incidentes de seguridad reportados, incluyendo detalles sobre el tipo de incidente, el impacto y las medidas correctivas tomadas.

**Encuestas de Percepción.** Cuestionarios aplicados a los empleados para evaluar su percepción sobre la efectividad de las medidas de seguridad implementadas.

### *1.6.2 Variable 2: Capacitación en Seguridad de la Información*

#### 1.6.2.1 Definición Conceptual.

La capacitación en seguridad de la información se refiere al proceso de educar a los empleados sobre las políticas, procedimientos y mejores prácticas para proteger la información de la organización.

#### 1.6.2.2 Definición Operacional.

Para medir la efectividad de la capacitación en seguridad de la información en COOPEVE, R.L., se utilizarán los siguientes indicadores:

**Frecuencia de Capacitación:** Número de sesiones de capacitación realizadas en un período determinado.

**Participación en Capacitación:** Porcentaje de empleados que han asistido a las sesiones de capacitación.

**Conocimiento Adquirido:** Resultados de evaluaciones realizadas antes y después de las sesiones de capacitación para medir el aumento en el conocimiento de los empleados.

##### 1.6.2.2.1 Instrumentos de Medición.

**Registros de Asistencia:** Documentación de la participación de los empleados en las sesiones de capacitación.

**Evaluaciones de Conocimiento:** Pruebas aplicadas antes y después de las sesiones de capacitación para medir el nivel de conocimiento adquirido.

**Encuestas de Satisfacción:** Cuestionarios aplicados a los empleados para evaluar su satisfacción con las sesiones de capacitación y su percepción sobre la utilidad de la información proporcionada.

Estos puntos permiten una evaluación estructurada y sistemática de las variables clave en la implementación del SGSI, asegurando que las medidas de seguridad y la capacitación sean efectivas y contribuyan a la protección de la información en COOPEVE, R.L.

## 1.7 Alcances y limitaciones de la investigación

Para esta investigación, se aplica a todas las áreas vinculantes de la Cooperativa de Servicios Múltiples El Educador Veragüense, que participan en los controles y procedimientos para Incidentes, Controles y Reportes relacionados a Estándar de Seguridad de la información.

### *1.7.1 Alcances*

### *1.7.2 Limitaciones*

Desde el punto de vista teórico las cooperativas en el país de Panamá se rigen por el Instituto Panameño Autónomo Cooperativo, el contenido de información relacionado con la Seguridad de la información es escaso.

#### 1.7.2.1 Limitación temporal

La investigación se llevó acabó entre los meses de Enero 2022 a diciembre del 2023.

#### 1.7.2.2 Limitación espacial

La limitación espacial que tuvo la investigación está conformada por el área geográfica de la empresa Cooperativa de Servicios Múltiples El Educador Veraguense, la cual se encuentra ubicada en el distrito de Santiago, Avenida Central, Calle Manuel Celestino Gonzalez, Veraguas Panamá.

# II. MARCO TEÓRICO

## 2.1 Antecedentes de la investigación

En el transcurso de la investigación, se han revisado antecedentes bibliográficos de estudios de nivel de maestría y doctorado relacionados con el tema en cuestión.

Un problema de investigación bien planteado es la llave de la puerta de entrada al trabajo en general, pues de esta manera permite la precisión en los límites de la investigación, la organización adecuada del marco teórico y las relaciones entre las variables; en consecuencia, es posible llegar a resolver el problema y generar datos relevantes para interpretar la realidad que se desea aclarar (Hernandez, 2014, p. 57).

### *2.1.1 A nivel internacional*

A continuación, se presentan los resultados obtenidos:

Morales (2019) señala que las Cooperativas de Ahorro y Crédito se conciben como instituciones financieras solidarias, cuya finalidad es canalizar los ahorros de personas trabajadoras y responsables hacia créditos que favorezcan el desarrollo de microempresas y mejoren la calidad de vida de sus beneficiarios. Estas cooperativas, cuyos propietarios son miles de personas, están gestionadas por equipos de profesionales altamente comprometidos con alcanzar tanto los objetivos financieros como los sociales de la institución, logrando un equilibrio real entre rentabilidad financiera y social.

A nivel internacional, se han realizado diversos estudios que abordan la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI). A continuación, se destacan algunos de los más relevantes:

Huanca (2018). *La Falsa Percepción En La Seguridad De Los Sistemas Informáticos* [Tesis Doctoral, Universidad Nacional Del Altiplano].

Resumen: El presente trabajo aborda temas de seguridad e inseguridad en los sistemas informáticos, debido a la incertidumbre sobre la percepción de seguridad existente. Se espera cumplir con la con la confidencialidad, integridad y disponibilidad de la información según ISO 27001, esto se aplica en diversos escenarios de desarrollo de software en forma empírica, estos requerimientos toman mayor valor en la administración de datos de entidades públicas y privadas, debido a que la ausencia de la seguridad en los sistemas desestabiliza el orden social global. El presente trabajo se asocia a un grupo de Mypes muestreadas, en el cual se evidencia la inseguridad, debido al modo de desarrollo de sus procesos para el aseguramiento de la información. En cuanto al método se evaluaron cuatro tratamientos tecnológicos en dos factores fijos midiendo así el grado se seguridad e inseguridad en las Mypes a través del Diseño Factorial Completamente al Azar. Los cuatro tratamientos han sido aplicados al grupo muestral, buscando así identificar diferencias entre los tratamientos. En cuanto a los resultados y según el planteamiento de la hipótesis general, la prueba de Análisis Factorial Univariante resultó no significativo P-valor > nivel se significancia, lo que conlleva a indicar como conclusiones que no es suficiente suministrar tratamientos tecnológicos físicos y lógicos a las Mypes muestreadas, esto si el personal que los dirige no tiene solvencia académica requerida para el desarrollo adecuado de los protocolos de seguridad, planes de gestión tecnológica y sistemas de gestión de seguridad de la información, las cuales contribuyen en el aseguramiento de la información.

Nota: La relación con la tesis "Implementación de un Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense, durante el periodo 2022-2023" radica en la necesidad de asegurar que los protocolos de seguridad y la gestión de información estén alineados con estándares internacionales. Esto es esencial para garantizar que las prácticas implementadas en la cooperativa sean efectivas en proteger la información crítica y asegurar la continuidad operativa, especialmente en un entorno donde la percepción de seguridad es incierta y las amenazas a la integridad de la información son constantes.

Huanca, J. (2018). *La Falsa Percepción En La Seguridad De Los Sistemas Informáticos* [Tesis Doctoral, Universidad Nacional Del Altiplano].

Contero (2019) Diseño De Una Política De Seguridad De La Información Basada En La Norma Iso 27002:2013, Para El Sistema De Botones De Seguridad Del Ministerio Del Interior. (Tesis de Maestría)

Resumen: El siguiente proyecto de grado tiene como objetivo principal Diseñar una Política de Seguridad de la Información, basada en la Norma ISO/IEC 27002:2013 para el Sistema de Botones de Seguridad del Ministerio del Interior, con la finalidad de establecer las directrices y normas para la correcta gestión de la seguridad de la información. Se desarrolla un análisis de la norma ISO/IEC 27002:2013, sustentándose en lo expuesto en el EGSI (Esquema Gubernamental de Seguridad de la información), en el cual se indica que este esquema no reemplaza a la norma ISO/IEC 27002 y que, de acuerdo con las necesidades de cada institución pública, dirección o departamento, se puede definir políticas de seguridad amplias o específicas. Luego de haber

realizado el levantamiento de la información de la situación actual de este sistema de seguridad integral, con los resultados obtenidos y mediante la aplicación de la metodología Magerit se determina y valora los activos, posteriormente las amenazas que puedan presentarse y finalmente se estima el impacto y los riesgos a los cuales está expuesta la información. A través de la norma NTE INEN ISO/IEC 27002:2013 se selecciona las salvaguardas o controles necesarios y más adecuados que se aplica en el desarrollo de la política de seguridad de la información. Esta política contiene características recomendadas en la norma NTE INEN ISO/IEC 27002:2013, además se incluye las definiciones, terminología, abreviaturas y responsabilidades, con el objetivo de que su aprobación y aplicación se lo pueda realizar en un corto plazo en dicha Cartera de Estado.

*Cita Apa*

Contero (2019). *La Norma Iso 27002:2013, Para El Sistema De Botones De Seguridad Del Ministerio Del Interior*. (Tesis de Maestría)

Torres (2021) Propuesta de metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas. (Tesis Maestría)

Resumen:

Contexto

Existen diversos marcos de buenas prácticas en materia de seguridad informática que se utilizan para auditoría. La idea del presente proyecto es la revisión de estos marcos de buenas prácticas con el objetivo de proponer una metodología para auditoría de seguridad de sistemas y aplicaciones.

Objetivo

Este proyecto busca proponer una metodología para auditoría de seguridad tomando como base marcos de buenas prácticas. Esto con el objetivo de mantener un nivel aceptable de riesgo a nivel organizacional y minimizar el impacto en la confidencialidad, integridad y disponibilidad de los datos.

## Método

Se realizó una revisión documental con el fin de identificar marcos de buenas prácticas. Posteriormente se compararon los marcos identificados, se seleccionaron controles y creó un papel de trabajo. Finalmente, se realizó un diagrama de flujo del proceso para facilitar la comunicación de la metodología.

## Resultados

Se desarrolló una metodología con base en cuatro marcos de buenas prácticas: ISO 27001, COBIT 2019, CIS CSC v8 y el marco de ciberseguridad de NIST. La metodología incluye un proceso que toma en cuenta los puntos clave de los cuatro marcos, una herramienta de Excel para la ejecución de la auditoría y un diagrama de proceso en notación BPM para la comunicación de la metodología.

## Conclusión

La metodología propuesta permite realizar auditorías de seguridad de sistemas y aplicaciones con base en marcos de buenas prácticas ampliamente aceptados por la industria. Adicionalmente, el proceso diseñado permite la adaptación al contexto organizacional y la optimización del proceso de auditoría de seguridad, pues toma en cuenta el ciclo de mejora continua.

*Cita Apa*

Torres (2021). Propuesta de metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas. (Tesis Maestría)

Allendevaux (2021) How U.S. State Data Protection Statutes Compare In Scope To Safeguard Information And Protect Privacy Using Iso/Iec 27001:2013 And Iso/Iec 27701:2019 Security And Privacy Management System Requirements As An Adequacy Baseline. (Tesis Doctoral)

Resumen: Dado que el 97% de la información del mundo se creó en la última década, no es de extrañar que las violaciones de datos hayan aumentado durante este mismo período. En respuesta, más de 100 naciones de todo el mundo han creado leyes de protección de datos destinadas a salvaguardar la información y garantizar que las organizaciones que procesan datos personales respeten los derechos de privacidad. Sin embargo, en los Estados Unidos, no se ha promulgado ninguna ley de protección de datos, excepto para sectores específicos. En cambio, cada estado ha aprobado su propio conjunto de leyes, que ascienden a más de 100 leyes diferentes y superpuestas en cincuenta estados al momento de escribir este artículo. Las complejidades de estas variaciones han confundido a los proveedores de servicios en la nube, ya que muchos tienen dificultades para comprender las diferentes obligaciones de cumplimiento, en lugar de centrarse en un enfoque común para la protección de datos. En este contexto, el objetivo de esta investigación fue crear un sistema de medición para comparar las fortalezas y debilidades de las leyes de protección de datos estatales con las líneas de base de seguridad y privacidad; e investigar cómo los cuatro sistemas de medición creados en este estudio pueden prescribir cómo los estados pueden reforzar los estatutos de protección de datos para mejorar los controles de seguridad, los

principios de privacidad y los mecanismos de aplicación para salvaguardar los datos de las personas.

Nota: La tesis se alinea con la necesidad de desarrollar mecanismos para evaluar y mejorar la seguridad de la información, similar a cómo el estudio mencionado busca medir y comparar la efectividad de las leyes estatales de protección de datos en Estados Unidos. La implementación del SGSI en la cooperativa no solo ayuda a proteger la información crítica de los asociados y colaboradores, sino que también fortalece los procesos internos para cumplir con estándares internacionales de seguridad, garantizando así la integridad, confidencialidad y disponibilidad de la información.

*Cita Apa*

Allendevaux (2021)How U.S. State Data Protection Statutes Compare In Scope To Safeguard Information And Protect Privacy Using Iso/Iec 27001:2013 And Iso/Iec 27701:2019 Security And Privacy Management System Requirements As An Adequacy Baseline. (Tesis Doctoral)

Parra (2014) Parra, Á. (2014). *ISO 27001 PARA PYMES* [Tesis Maestría, Universidad Internacional de la Rioja]. (Tesis Maestría)

Resumen: El uso de las tecnologías informáticas en todos los aspectos de la cotidianidad humana, ha conducido a que la seguridad informática no sea sólo una preocupación de las grandes compañías, sino también de las PYMES, las cuales inconscientemente en gran parte quedan vulnerables ante la falta de controles que les permitan protegerse de intrusiones no deseadas. Aquí se propone una metodología de implementación de la ISO 27001 para que sea aplicada en la implementación de Sistemas de Gestión de Seguridad de la Información en PYMES. Busca

facilitar las tareas que en este tipo de empresas se dificultan, debido a los recursos limitados con los que cuenta en presupuesto, personal y conocimiento. Adicional a esto, se propone unas prácticas iniciales mínimas como punto de partida para organizaciones que no tienen controles de seguridad de la información, como principio para iniciar un ciclo de mejora continua, que permita que la organización alcance una maduración mayor a medida que la cultura de seguridad de la información, se afianza dentro de la compañía. Aunque se proponen soluciones básicas para PYMES, al analizar ataques a grandes compañías, se encuentran estás propuestas útiles como estrategia preventiva desde los procedimientos y controles aún para este tipo de empresas.

Parra, Á. (2014). *ISO 27001 PARA PYMES* [Universidad Internacional de la Rioja]. (Tesis Maestría)

Revisión de la Literatura sobre Implementación de la Norma ISO 27001:2022

Diversos estudios han documentado los desafíos y beneficios asociados con la implementación de la norma ISO 27001:2022 en diferentes contextos organizacionales.

(Abazi, 2020) destaca que uno de los primeros requisitos en la implementación de esta norma es la definición de una metodología de evaluación de riesgos que debe estar alineada con los requisitos de negocio y de seguridad de la información. Este enfoque sistemático es crucial para la identificación precisa de los niveles de riesgo y para la implementación efectiva de controles de seguridad.

Además, la literatura muestra que las organizaciones que adoptan la norma ISO 27001:2022 a menudo enfrentan desafíos significativos, especialmente si carecen de experiencia previa en sistemas de gestión de seguridad de la información (Torres, 2021). La implementación

efectiva de la norma requiere no solo el establecimiento de controles adecuados, sino también la integración de un enfoque holístico para la gestión de riesgos y la mejora continua del SGSI.

### Estudios Relevantes en el Contexto Cooperativo

En el contexto específico de las cooperativas, como en el caso de la Cooperativa de Servicios Múltiples El Educador Veragüense, la implementación de un SGSI bajo la norma ISO 27001:2019 puede presentar desafíos únicos. La literatura sugiere que las cooperativas a menudo enfrentan barreras adicionales, como limitaciones de recursos y la falta de un marco regulatorio estructurado en ciertas jurisdicciones (Cuenca, 2019). Estas condiciones pueden dificultar la adopción de prácticas robustas de seguridad de la información y la implementación efectiva de la norma ISO 27001.

### Conexión con la Investigación Actual

El análisis de estos antecedentes resalta la importancia de abordar los desafíos específicos que enfrenta la Cooperativa de Servicios Múltiples El Educador Veragüense en la implementación de la norma ISO 27001:2022. La investigación actual busca contribuir a la comprensión de cómo estas barreras pueden ser superadas y qué estrategias pueden ser efectivas para asegurar la protección adecuada de la información en un entorno cooperativo. Este estudio no solo se basa en el marco teórico y los hallazgos previos, sino que también se enfoca en la aplicación práctica de la norma ISO 27001 en un contexto particular, proporcionando una visión valiosa para futuras investigaciones y prácticas en el campo de la seguridad de la información.

### Evolución de la Norma ISO IEC/27001:2022

La implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) bajo normas internacionales, como la ISO 27001:2022, ha sido objeto de numerosos estudios que

abordan tanto los desafíos como las mejores prácticas asociadas con su aplicación en diversos contextos organizacionales. A continuación, se presenta una revisión de los antecedentes internacionales que contextualizan la importancia y las dificultades inherentes a la adopción de estos sistemas.

## Relevancia de la Norma ISO IEC/27001:2022

La norma ISO 27001:2022 ha sido revisada y adaptada a lo largo del tiempo para enfrentar los desafíos emergentes en la seguridad de la información. Según Martínez (2021), la gestión de calidad, que es aplicable a diversas organizaciones, ha requerido el desarrollo de normas especializadas para abordar actividades específicas. La necesidad de mantener una norma actualizada responde a la naturaleza cambiante de las amenazas digitales. Encalada (2024) señala que, debido a la diversidad de regulaciones y legislaciones sobre protección de datos personales en diferentes países y regiones, es crucial que las organizaciones comprendan las normativas aplicables en sus áreas operativas. Este entendimiento es vital para apreciar cómo la norma ISO 27001:2022 ayuda a las organizaciones a gestionar los riesgos contemporáneos y a sostener una postura de seguridad robusta. Además, Isotools (2023) indica que la implementación de la ISO 27001 refuerza la confianza de los stakeholders, incluidos clientes, socios comerciales y reguladores, al evidenciar el compromiso de la empresa con la seguridad de la información. La certificación conforme a la ISO/IEC 27001:2022 no solo demuestra el cumplimiento con los estándares internacionales de seguridad de la información, sino que también permite a las empresas diferenciarse en el mercado y mejorar su reputación.

## Desafíos en la Implementación de SGSI

La adopción de una guía para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 en empresas Cooperativas de intermediación financiera, puede implicar varios retos, particularmente para las organizaciones sin experiencia previa en esta área. Según Mantilla (2009), la versión anterior de la norma, ISO 27001:2005, era el único estándar a nivel mundial aceptado para la certificación en la gestión de seguridad de la información. Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño o sector de actividad, lo que subraya su relevancia y universalidad.

**Figura 1** *Evolución de los controles de seguridad en versiones ISO/IEC 27001*




Nota: La ISO/IEC 27001 ha experimentado una evolución significativa en sus versiones, adaptándose a las nuevas amenazas y requisitos de seguridad, con mejoras en la estructura y definición de los controles de seguridad. Tomado de blog welivesecurity (Mendoza, 2023).

Este desafío se agrava por la ausencia de un marco estructurado en algunas regiones, lo que complica la implementación efectiva de las mejores prácticas de seguridad de la información. Según (Bai, 2022), el avance tecnológico en big data ha introducido nuevas amenazas a la seguridad informática, presentando un desafío significativo para los profesionales de TI. La dificultad radica en la precisión necesaria para implementar mecanismos operativos y realizar comprobaciones en línea, con el fin de garantizar la confidencialidad de la información digital.

Gil (2024) sostiene que el abordaje de problemas relacionados con la seguridad informática en entornos recreacionales inteligentes requiere una gestión precisa, especialmente a medida que aumenta la tendencia de las personas a utilizar estos espacios. Sin embargo, la falta de recursos y experiencia en la gestión de la seguridad de la información puede limitar la capacidad de las organizaciones para cumplir con los requisitos de la norma ISO 27001:2022. Superar barreras como la resistencia al cambio y la falta de capacitación adecuada es esencial para garantizar la implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta perspectiva es crucial para comprender los desafíos que las cooperativas podrían enfrentar al adoptar esta norma y las estrategias para superarlos.

Por otro lado, Velasco et al. (2018) destacan que, en el sector manufacturero, la abundancia de datos y la seguridad deficiente en procesos clave representan amenazas significativas para la eficacia del negocio. Su estudio enfatiza la importancia de identificar estos peligros mediante metodologías de gestión de riesgos como Magerit y el ciclo PDCA de Deming, lo que resulta fundamental para mejorar la seguridad y la eficiencia en dicho sector.

### *2.1.2 A nivel regional*

El contexto regional es fundamental en la implementación de la norma ISO 27001:2022, ya que factores locales e internacionales influyen en cómo se aborda la seguridad de la información. En Ecuador, la pandemia ha marcado un punto de inflexión en este campo, dando lugar a un aumento significativo de los ataques cibernéticos dirigidos a individuos, pequeñas empresas, grandes corporaciones, agencias gubernamentales e infraestructuras críticas. Según Tuabanda (2023), esta situación ha subrayado que nadie está exento del riesgo, evidenciando la necesidad de fortalecer las medidas de seguridad informática a nivel nacional.

De manera similar, en Perú, el panorama de la seguridad de la información también ha evolucionado. Aleman (2023) señala que los clientes exigen cada vez más cláusulas contractuales que garanticen la protección de los datos manejados por las consultoras. Esta tendencia ha generado una presión significativa sobre las empresas para implementar políticas de seguridad de la información que no solo mejoren sus operaciones, sino que también les permitan mantenerse competitivas en un mercado cada vez más exigente.

En un estudio realizado por Túquerres (2024), se identificó la vulnerabilidad actual de la cooperativa mediante un análisis de incidentes previos y la tipificación de recursos críticos. La investigación subraya la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) al considerar las posibles consecuencias financieras y reputacionales que podrían derivarse de incidentes de seguridad. Además, al examinar la incorporación de la Norma ISO/IEC 27001 en instituciones financieras de diversos países europeos, el estudio reveló un análisis detallado sobre el impacto de esta normativa en las políticas de ciberseguridad. Se encontró que la adopción de la norma no solo condujo a una mayor comprensión de la importancia de proteger la información, sino que también promovió la implementación de medidas de control más estrictas para salvaguardar los datos sensibles. Asimismo, se identificaron desafíos comunes enfrentados por las instituciones financieras durante el proceso de implementación, tales como la asignación de recursos adecuados y la capacitación del personal.

En el contexto internacional, la metodología de desarrollo es un componente fundamental en la implementación de cualquier proyecto, sistema o producto. Según Castillo (2022), este enfoque incluye la descripción detallada de las técnicas y métodos colaboradores para alcanzar los objetivos establecidos, lo que a su vez contribuye a mejorar la eficiencia y la puntualidad en la entrega final del proyecto.

### *2.1.3 A nivel nacional*

En el contexto nacional, la implementación de sistemas de gestión y mantenimiento preventivo ha adquirido una relevancia creciente en diversos sectores, especialmente en la industria y en el ámbito de la seguridad de la información. Según Godoy (2021), la información es un recurso esencial para el funcionamiento de las empresas y la operación de los negocios, lo que la convierte en uno de los activos más valiosos de cualquier organización. En la actualidad, el aumento en el uso de internet, el rápido avance tecnológico y la falta de conocimiento adecuado para mitigar riesgos han dado lugar a innumerables amenazas que explotan las vulnerabilidades empresariales. Esto puede tener un impacto negativo significativo, comprometiendo las características fundamentales que debe mantener la información: disponibilidad, integridad y confidencialidad.

En Panamá, la adopción de normas internacionales, como la ISO 27001:2022, ha experimentado un notable crecimiento en los últimos años, particularmente en cooperativas y empresas del sector financiero. Esta tendencia responde a la urgente necesidad de establecer controles rigurosos y optar por marcos normativos probados para la gestión de la información. La implementación de un sistema de gestión de seguridad de la información depende en gran medida del concepto de control informático, el cual es esencial para garantizar la integridad y la protección de los datos sensibles.

Según Benítez (2022), el control interno informático se define como un sistema integrado en el proceso administrativo, abarcando la planificación, organización, dirección y control de las operaciones, con el propósito de asegurar la protección de los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados. Esta

creciente adopción refleja la necesidad de alinearse con estándares globales, garantizando así la seguridad de la información y la continuidad operativa en un entorno cada vez más digitalizado.

Dentro del marco legal panameño, las cooperativas son reguladas por el Instituto Panameño Autónomo Cooperativo (IPACOOP), a diferencia del sector bancario, que está bajo la supervisión de la Superintendencia de Bancos. Según Osellame & Fong (2017), las cooperativas cumplen una función pública y comunitaria, alineada con los intereses de un grupo de personas. Debido a esta naturaleza, el Estado tiene un interés legítimo en supervisar su funcionamiento, lo cual justifica la creación de instituciones como el IPACOOP para garantizar el desarrollo y la regulación adecuada de estas entidades.

Es importante destacar el caso del Banco Nacional de Panamá, que implementó un sistema de gestión basado en la norma ISO 27001:2022. Esta implementación no solo fortalece la seguridad de la información en la institución, sino que también incrementa su reputación a nivel internacional, permitiéndole acceder a nuevos mercados y ganarse la confianza de clientes y partes interesadas. Según Banconal (2021), la obtención de la certificación ISO/IEC 27001:2022 por parte del Banco Nacional de Panamá no solo asegura la protección de los recursos informáticos, sino que también mejora la eficiencia y efectividad de los procesos operativos automatizados, lo que subraya la relevancia de adoptar estándares internacionales en la gestión de seguridad de la información para instituciones financieras en Panamá.

## 2.2 Bases Teóricas

Según Bartra (2024), un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas diseñadas para gestionar y proteger la información dentro de una organización. Este sistema, conocido en inglés como "Information Security Management System"

(ISMS), proporciona un marco para identificar posibles riesgos de seguridad y establecer medidas destinadas a mitigar dichos riesgos.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 en Cooperativas de Servicios Múltiples en Panamá durante el periodo 2022-2023 se fundamenta en la creciente necesidad de proteger los activos de información en un entorno cada vez más digitalizado y vulnerable a ciberamenazas. Las cooperativas, que manejan información sensible de sus socios, como datos financieros y personales, requieren un enfoque sistemático y normativo para garantizar la confidencialidad, integridad y disponibilidad de dicha información. La norma ISO 27001:2022 proporciona un marco globalmente reconocido que guía a las organizaciones en la identificación, evaluación y tratamiento de los riesgos asociados con la seguridad de la información. Al adoptar este estándar, las cooperativas no solo cumplen con las regulaciones locales e internacionales, sino que también refuerzan la confianza de sus socios, asegurando la continuidad operativa y minimizando los impactos de posibles incidentes de seguridad. Además, la implementación de un SGSI bajo esta norma permite a las cooperativas optimizar sus procesos internos, mejorar la eficiencia operativa y fomentar una cultura de seguridad que se adapte continuamente a nuevas amenazas y requisitos regulatorios. Este enfoque integral es esencial para la sostenibilidad y el crecimiento de las cooperativas en un entorno financiero competitivo y en constante evolución.

### *2.2.1 Definición de las variables*

En el contexto de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en COOPEVE, R.L., se han identificado dos variables clave: la seguridad de la información y la capacitación en seguridad de la información.

**Seguridad de la Información:** Esta variable se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información contra accesos no autorizados, alteraciones y destrucción. Incluye todas las medidas y controles implementados para asegurar que la información esté protegida de amenazas internas y externas.

**Capacitación en Seguridad de la Información:** Esta variable se refiere al proceso de educar a los empleados sobre las políticas, procedimientos y mejores prácticas para proteger la información de la organización. La capacitación busca aumentar el conocimiento y la conciencia de los empleados sobre la importancia de la seguridad de la información y cómo pueden contribuir a protegerla.

### *2.2.2 Importancia de las variables*

**Seguridad de la Información**: La seguridad de la información es crucial para cualquier organización, especialmente para una cooperativa financiera como COOPEVE, R.L. La protección de la información sensible y crítica asegura la confianza de los socios, cumple con las regulaciones legales y previene pérdidas financieras y daños a la reputación. Sin una adecuada seguridad de la información, la cooperativa estaría expuesta a riesgos significativos que podrían comprometer su operatividad y estabilidad.

**Capacitación en Seguridad de la Información:** La capacitación en seguridad de la información es fundamental para asegurar que todos los empleados comprendan sus responsabilidades y sepan cómo proteger la información de la organización. Una fuerza laboral bien capacitada es capaz de identificar y responder adecuadamente a amenazas de seguridad, reducir el riesgo de incidentes y asegurar el cumplimiento de las políticas de seguridad. La capacitación continua también ayuda a mantener una cultura de seguridad dentro de la organización, lo que es esencial para la efectividad del SGSI.

### *2.2.3 Las bases en que define la investigación*

La investigación se basa en la necesidad de implementar un SGSI efectivo en COOPEVE, R.L., conforme a la norma ISO 27001:2022. Las bases de esta investigación incluyen:

**Normativas y Estándares Internacionales:** La ISO 27001:2022 proporciona un marco reconocido internacionalmente para la gestión de la seguridad de la información. La investigación se fundamenta en los requisitos y directrices de esta norma para asegurar que el SGSI de COOPEVE, R.L. cumpla con los estándares más altos de seguridad.

**Análisis de Riesgos:** La identificación y evaluación de riesgos es una base fundamental para la implementación del SGSI. La investigación se apoya en un análisis detallado de los riesgos asociados con los activos de información de la cooperativa, permitiendo la selección de controles adecuados para mitigar estos riesgos.

**Mejores Prácticas de la Industria:** La investigación incorpora mejores prácticas de la industria en la gestión de la seguridad de la información y la capacitación de empleados. Estas prácticas se basan en experiencias y estudios previos que han demostrado ser efectivos en la protección de la información.

**Evaluación de la Situación Actual:** La investigación se basa en una evaluación exhaustiva de la situación actual de la seguridad de la información en COOPEVE, R.L. Esto incluye auditorías de seguridad, encuestas a empleados y análisis de incidentes previos para identificar áreas de mejora y establecer una línea base para medir el progreso.

### *2.2.4 Importancia de las bases teóricas*

Concepto de Seguridad de la Información

En esta sección se expone y analiza la fundamentación teórica que sustenta la investigación, basada en una exhaustiva revisión bibliográfica y otras fuentes relevantes. Esta base teórica fortalecerá el cuerpo de conocimiento necesario para dotar de solidez y rigor académico al trabajo realizado.

El International Standard Organization ISO (2022) define:

La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento y la implementación del sistema de gestión de seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo. (p. 5)

Es crucial comprender que la seguridad de la información implica la protección integral de los datos frente a accesos no autorizados, alteraciones y destrucción. Este concepto se sustenta en tres pilares fundamentales: la confidencialidad, que asegura que solo las personas autorizadas tengan acceso a la información; la integridad, que garantiza que los datos no sean modificados sin autorización; y la disponibilidad, que garantiza que la información esté accesible cuando sea necesaria.

Lopera (2023) destaca que un sistema de gestión de seguridad de la información es un sistema estructurado y documentado que incluye un conjunto de políticas, procesos y sistemas destinados a gestionar los riesgos asociados con los datos de una organización. Este enfoque tiene como objetivo mantener niveles aceptables de riesgo en la seguridad de la información. Las evaluaciones de riesgos continuas permiten identificar amenazas y vulnerabilidades que deben ser

gestionadas a través de un conjunto de controles específicos. Además, un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO 27001:2022 facilita la gestión de la confidencialidad, la integridad y la disponibilidad de los datos corporativos de manera optimizada y rentable.

La seguridad de la información no se limita únicamente a la implementación de medidas técnicas; también implica un enfoque organizacional que integra políticas, procesos y controles diseñados para proteger los activos de información de la empresa. Este enfoque garantiza una protección efectiva y sostenible, involucrando tanto la tecnología como a las personas y los procesos dentro de la organización, y fomenta una cultura de seguridad sólida y bien fundamentada.

### *2.2.5 Seguridad de la información vs seguridad informática*

La seguridad de la información y la seguridad informática son conceptos interrelacionados, pero con diferencias fundamentales en su enfoque y alcance. A continuación, se presenta una definición ampliada y detallada de cada uno, así como una comparación entre ambos.

Seguridad de la Información

La seguridad de la información se refiere a la protección de los datos y la información en todos sus formatos y medios, incluyendo no solo los sistemas informáticos, sino también documentos en papel, comunicaciones verbales, y cualquier otro medio en el que la información pueda estar almacenada, procesada, o transmitida. Su objetivo principal es preservar la confidencialidad, integridad y disponibilidad (conocidas como la tríada CIA) de la información, independientemente de la forma en que esta exista o se transmita.

#### 2.2.5.1 Confidencialidad.

Garantiza que la información solo sea accesible para las personas autorizadas.

#### 2.2.5.2 Integridad.

Asegura que la información se mantenga exacta, completa y protegida contra modificaciones no autorizadas.

#### 2.2.5.3 Disponibilidad

Garantiza que la información esté disponible para su uso cuando se necesite.

**Figura 2**
*Triada Confidencialidad, Integridad y Disponibilidad (CIA)*




Nota: La seguridad de la información abarca una gama amplia de medidas y prácticas diseñadas para proteger los datos y la información en todas sus formas y medios. No se limita únicamente a la protección de sistemas informáticos y digitales, sino que también abarca documentos físicos, comunicaciones verbales y cualquier otro medio en el que la información pueda estar almacenada, procesada o transmitida. Esta visión integral es fundamental para entender que los riesgos a la seguridad de la información pueden provenir de múltiples fuentes, y no solo de amenazas cibernéticas.

Valencia & Orozco (2017) destacan la distinción conceptual entre la seguridad de la información y la seguridad informática, también conocida como ciberseguridad. Antes de adoptar

un enfoque metodológico para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), es fundamental comprender esta diferencia, la cual se basa en el tipo de recursos que cada una protege. La seguridad informática se enfoca en la tecnología, es decir, en las infraestructuras tecnológicas que facilitan la gestión de la información dentro de una organización. En contraste, la seguridad de la información se refiere a la protección de la información en sí misma, considerándola un activo estratégico para la organización.

La seguridad de la información incluye un conjunto de políticas, procedimientos, controles y medidas tanto técnicas como organizacionales. Esto abarca la gestión de riesgos, el cumplimiento normativo, la formación y concienciación del personal, así como la implementación de normativas como la ISO 27001:2022, que establece los requisitos para un SGSI, asegurando así la confidencialidad, integridad y disponibilidad de la información de la organización.

### *2.2.6 Seguridad Informática*

La seguridad informática, también conocida como ciberseguridad, es una subdisciplina dentro de la seguridad de la información. Se enfoca específicamente en la protección de los sistemas informáticos, redes, y los datos que son procesados, almacenados, y transmitidos a través de ellos. Su principal objetivo es proteger estos sistemas contra amenazas cibernéticas como el acceso no autorizado, ataques de malware, ransomware, y otras formas de ciberataques.

Protección de sistemas: Incluye medidas como cortafuegos, antivirus, detección y prevención de intrusiones, y la configuración segura de servidores y dispositivos.

Seguridad de redes: Involucra la protección de las comunicaciones y datos en tránsito, asegurando que solo las partes autorizadas puedan acceder a la red y sus recursos.

Respuesta a incidentes: Se centra en la capacidad de detectar, responder y recuperarse de incidentes de seguridad cibernética.

Baca (2016) señala que la seguridad informática no se limita únicamente a preservar las siete características establecidas por COBIT; si se desea mantener consistentemente estas características, es esencial formular un plan que prevenga los principales tipos de ataques, ya sean internos, externos, físicos o electrónicos, dirigidos contra la información. En este contexto, la seguridad informática adopta un enfoque técnico, centrándose en la protección de la infraestructura digital de una organización. Esto incluye la implementación de medidas de seguridad directamente en hardware, software y redes, utilizando herramientas tecnológicas avanzadas para salvaguardar estos componentes críticos.

**Tabla 1**

*Comparativa entre Seguridad de la Información vs Seguridad Informática*

| Aspecto | Seguridad de la Información | Seguridad Informática |
|---|---|---|
| Definición | Protección de la información en todas sus formas (digital, física, verbal), asegurando su confidencialidad, integridad y disponibilidad. | Protección específica de los sistemas informáticos, redes y datos procesados o almacenados en ellos, frente a ciberamenazas y ataques cibernéticos. |
| Alcance | Amplio: Incluye la información en cualquier formato (digital, papel, | Específico: Se enfoca en la protección de la infraestructura digital, como hardware, |

| | | |
|---|---|---|
| | verbal) y abarca controles administrativos, físicos y técnicos. | software, redes y sistemas operativos. |
| Objetivo Principal | Garantizar que la información esté protegida de accesos no autorizados, alteraciones no deseadas y esté disponible cuando se necesite. | Proteger los sistemas informáticos y redes de accesos no autorizados, ataques de malware, y otras ciberamenazas. |
| Tríada CIA (Confidencialidad, Integridad, Disponibilidad) | Aplicable a toda la información, independientemente de su formato. | Aplicable específicamente a los datos y sistemas dentro del entorno digital. |
| Métodos y Enfoque | Enfoque holístico: Uso de políticas, procedimientos, formación, controles administrativos, físicos y técnicos. | Enfoque técnico: Implementación de soluciones tecnológicas como cortafuegos, antivirus, sistemas de detección y prevención de intrusiones, y medidas de ciberseguridad. |
| Normativas y Estándares | Incluye normativas como ISO 27001, que establece un Sistema de Gestión de Seguridad de la Información | Incluye normativas y guías específicas de ciberseguridad, como NIST, CIS Controls, y aspectos técnicos de la ISO |

| | | |
|---|---|---|
| | (SGSI) para la protección global de la información. | 27001 relacionados con la protección informática. |
| Gestión de Riesgos | Evaluación y gestión de riesgos relacionados con todos los aspectos de la información, incluidos riesgos físicos y digitales. | Gestión de riesgos enfocados en amenazas digitales, como ciberataques, malware, y vulnerabilidades de software y hardware. |
| Implementación | Incluye la creación de políticas de seguridad, formación del personal, y medidas de control físico y administrativo. | Incluye la configuración y monitoreo de sistemas informáticos, implementación de medidas de protección tecnológica y respuesta a incidentes cibernéticos. |
| Ejemplos de Aplicación | Protección de registros en papel, confidencialidad en comunicaciones verbales, controles de acceso físico a información sensible. | Protección de bases de datos, redes corporativas, sistemas de correo electrónico, y prevención de accesos no autorizados a través de la red. |

**Nota:** La seguridad de la información y la seguridad informática, aunque interrelacionadas, tienen enfoques y objetivos distintos. La seguridad de la información se ocupa de proteger la información en cualquier formato, aplicando medidas para garantizar su confidencialidad, integridad y disponibilidad. Este enfoque es amplio e incluye la implementación de políticas y

controles tanto administrativos como físicos y técnicos. Por otro lado, la seguridad informática se enfoca específicamente en la protección de sistemas digitales y redes frente a ciberamenazas.

La seguridad de la información es un concepto integral que abarca la protección de todos los aspectos relacionados con la información, mientras que la seguridad informática es una parte crucial dentro de este marco, enfocada en la protección de la infraestructura tecnológica y digital. Ambos son esenciales para garantizar la protección de los datos y el buen funcionamiento de las organizaciones en el entorno actual.

### *2.2.7 Norma ISO 27001:2022*

La norma ISO 27001:2022 establece requisitos esenciales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y es ampliamente reconocida a nivel internacional por su rigor y efectividad en la protección de datos. Este estándar proporciona un marco robusto para la gestión de riesgos, que abarca desde la identificación de amenazas potenciales hasta la evaluación y el tratamiento sistemático de los riesgos asociados con la seguridad de la información.

Al adoptar la norma ISO 27001:2022, las organizaciones no solo fortalecen su capacidad para proteger la confidencialidad, integridad y disponibilidad de la información, sino que también demuestran un firme compromiso con la seguridad, lo que es fundamental para mantener la confianza de clientes, socios y otras partes interesadas. Además, la implementación de esta norma permite a las organizaciones cumplir con las crecientes exigencias regulatorias en materia de seguridad de la información, asegurando que operen dentro del marco legal aplicable y minimizando la exposición a sanciones y pérdidas reputacionales. En un entorno global cada vez más digitalizado, la certificación bajo ISO 27001:2022 se convierte en un diferenciador clave, subrayando el compromiso de la organización con las mejores prácticas en seguridad de la

información y su capacidad para gestionar eficazmente los riesgos en un panorama de amenazas en constante evolución.

### *2.2.8 Importancia de la Implementación del SGSI en Cooperativas en Panamá*

En el entorno de las cooperativas panameñas, especialmente aquellas que operan en el sector de la intermediación financiera, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022 se ha convertido en un componente fundamental para asegurar su sostenibilidad y crecimiento. Estas cooperativas manejan información altamente sensible de sus socios, incluyendo datos personales, financieros y operativos. La protección de esta información no solo constituye una obligación ética, sino también un requisito estratégico para mantener la confianza y lealtad de los socios, quienes son esenciales para la existencia y desarrollo de la cooperativa.

Calder (2008) destaca que la información es el elemento vital de las organizaciones modernas, por lo que garantizar su protección y disponibilidad para aquellos que la necesiten es esencial para las operaciones comerciales. Sin embargo, los sistemas de información rara vez se diseñan desde el inicio con la seguridad en mente, y las medidas técnicas o listas de verificación por sí solas no son suficientes para proteger un sistema de información en su totalidad. Para lograr un sistema de información verdaderamente seguro, es crucial contar con sistemas de gestión y controles de procedimiento cuidadosamente planificados y ejecutados.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 permite a las cooperativas establecer un marco estructurado que asegura la protección de la información mediante la identificación, evaluación y tratamiento de riesgos específicos. Este enfoque no solo salvaguarda la integridad de los datos, sino que también garantiza la continuidad operativa al minimizar el impacto de posibles incidentes de seguridad. Además, al

contar con procesos claros y estandarizados, las cooperativas pueden mejorar su eficiencia operativa, reduciendo la posibilidad de errores humanos y fortaleciendo su capacidad de respuesta ante amenazas.

Según Calderon (2022), en la norma ISO 27001, los controles identificados se aplican mediante un análisis de riesgos estructurado, lo que permite implementar medidas de seguridad que disminuyen el impacto de las vulnerabilidades sobre los activos de información frente a incidentes de seguridad.

Implementar un SGSI conforme a la norma ISO 27001:2022 también posiciona a las cooperativas en una posición privilegiada dentro del mercado financiero, ya que les permite cumplir con las exigencias regulatorias tanto locales como internacionales, y demostrar un compromiso tangible con la seguridad de la información. Este compromiso es crucial no solo para evitar sanciones legales, sino también para fortalecer la reputación de la cooperativa en un entorno competitivo y cada vez más digitalizado.

### *2.2.9 Modelos de Gestión de la Seguridad de la Información*

En la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022, es crucial integrar diferentes modelos y enfoques para complementar y fortalecer este proceso. La gestión de riesgos es uno de los enfoques más relevantes, ya que permite a las organizaciones identificar, evaluar y priorizar los riesgos relacionados con la seguridad de la información. Este enfoque no solo contribuye a mitigar posibles amenazas, sino que también asegura la asignación eficiente de recursos para proteger los activos más críticos. Este trabajo para algunas empresas puede resultar tedioso si no cuentan con los elementos necesarios para conformar un área especializada en SGSI.

Según Llontop (2018), muchas empresas hoy en día prefieren externalizar el soporte y la gestión de sus sistemas de TI a especialistas, permitiéndoles enfocarse en el desarrollo de su core de negocio sin la necesidad de invertir significativamente en la especialización de sus gestores de sistemas.

Además, el uso de controles internos es fundamental en la gestión de riesgos, actuando como un componente clave que complementa el SGSI. Estos controles son medidas implementadas dentro de la organización para garantizar el cumplimiento de los estándares de seguridad, la consistencia de los procesos operativos, y la realización de actividades conforme a las políticas establecidas. La integración de estos controles con el SGSI permite una supervisión constante y un ajuste dinámico de las estrategias de seguridad en respuesta a cambios en el entorno de amenazas.

Otra práctica esencial que complementa la implementación de un SGSI es la realización de auditorías internas periódicas. Estas auditorías proporcionan una revisión exhaustiva del sistema, evaluando su efectividad y asegurando el cumplimiento continuo con la norma ISO 27001:2022. A través de este proceso, las organizaciones pueden identificar áreas de mejora, corregir deficiencias y reforzar las políticas de seguridad. La auditoría interna no solo contribuye a mantener la integridad del SGSI, sino que también fomenta una cultura de mejora continua, vital para adaptarse a nuevas amenazas y requisitos regulatorios.

Por lo tanto, la integración de estos modelos y enfoques no solo complementa la norma ISO 27001:2022, sino que también fortalece la capacidad de la organización para proteger sus activos de información de manera efectiva y sostenible.

Impacto de la Seguridad de la Información en la Continuidad del Negocio

La seguridad de la información está estrechamente vinculada a la continuidad del negocio, especialmente en el sector financiero. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 garantiza que la cooperativa pueda mantener sus operaciones de manera efectiva, incluso en situaciones de incidentes de seguridad. Es crucial destacar que una gestión proactiva de la seguridad de la información no solo mitiga los riesgos, sino que también asegura la resiliencia organizacional.

(Isotools, 2022) señala que la continuidad del negocio es un plan desarrollado para garantizar que los procesos críticos de una organización se mantengan operativos y que la oferta de productos o servicios esté disponible, incluso ante incidentes disruptivos. Este plan requiere el uso de los recursos mínimos necesarios para operar los procesos esenciales, asegurando la confidencialidad, disponibilidad e integridad de los activos de información. Para ello, es vital identificar y reconocer la integridad, confidencialidad y disponibilidad de cada activo, y realizar esfuerzos significativos para mantener estos aspectos, incluso en escenarios de recursos limitados.

Esta perspectiva subraya la importancia de un SGSI bien implementado, que no solo protege los activos de información, sino que también fortalece la capacidad de la organización para superar desafíos operativos, garantizando así la continuidad del negocio.

### *2.2.10 Retos en la Implementación del SGSI*

Es importante analizar los principales desafíos que enfrenta una organización como la Cooperativa de Servicios Múltiples El Educador Veragüense al implementar un SGSI bajo la norma ISO 27001:2019. Estos pueden incluir la resistencia al cambio, la necesidad de capacitación del personal, y la integración del SGSI con otros sistemas de gestión ya existentes.

Moya (2023) señala que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) presenta varios retos, algunos de los cuales incluyen: falta de compromiso y apoyo de la dirección, lo que es crucial para la seguridad de la información y el respaldo necesario en la implementación del SGSI; los costos asociados, ya que la implementación puede ser costosa, considerando el hardware, software y personal capacitado; cambios culturales, que pueden ser difíciles de lograr, requiriendo una comunicación efectiva con los colaboradores; desafíos tecnológicos, especialmente en la integración con otros sistemas existentes, lo cual puede requerir una planificación cuidadosa; dificultad para mantener el SGSI actualizado, dado que la seguridad de la información es una disciplina en constante evolución; resistencia al cambio por parte de los colaboradores, quienes pueden ver la implementación del SGSI como una carga adicional; dificultad para medir el retorno de la inversión (ROI) en la implementación del SGSI, lo que puede dificultar la justificación de los costos; dificultad para integrar la seguridad en los procesos y sistemas existentes, asegurando que cumplan con los requisitos de seguridad; cambios en el entorno empresarial, como la adquisición de nuevas tecnologías o la expansión de la empresa, que pueden requerir la actualización constante del SGSI; dificultad para involucrar a todos los departamentos y usuarios en la implementación y mantenimiento del SGSI, lo cual es esencial para garantizar su éxito a largo plazo; y finalmente, la dificultad para mantener la conformidad con los estándares y regulaciones, asegurando que el SGSI cumpla con los estándares aplicables y esté actualizado con los cambios en la legislación y los estándares.

### *2.2.11 Beneficios de la Implementación de un SGSI*

Por último, esta sección debe destacar los beneficios que se obtienen al implementar un SGSI en la cooperativa. Entre estos beneficios se encuentran la mejora de la confianza de los socios

y partes interesadas, la reducción de riesgos, el cumplimiento de normativas y regulaciones, y la creación de una cultura organizacional enfocada en la seguridad de la información.

Moya (2023) señala varios beneficios clave de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo la protección de datos confidenciales y la mejora en el cumplimiento de normativas de seguridad. Según Moya:

Un SGSI ayuda a proteger los datos confidenciales de nuestra organización y se asegurará de que solo se acceda a ellos por personas autorizadas. Mejora de la conformidad. Un SGSI permite a nuestra organización cumplir con normativas y regulaciones importantes en materia de seguridad de la información, pasando a continuación a detallar las más relevantes en España:

Reglamento General de Protección de Datos (RGPD): Es una normativa de la Unión Europea que regula la protección de datos personales. Es aplicable a todas las organizaciones que tratan datos personales de ciudadanos de la UE, y establece un marco de protección de los mismos más estricto que la anterior Directiva de Protección de Datos. En España, el RGPD se ha incorporado al ordenamiento jurídico a través de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).

Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE): Esta ley regula los servicios de la sociedad de la información, incluyendo el comercio electrónico, la publicidad online, el marketing por correo electrónico, entre otros. Establece requisitos de transparencia, seguridad y privacidad para los proveedores de servicios online.

Ley de Propiedad Intelectual (LPI): Regula los derechos de propiedad intelectual en España. Incluye disposiciones sobre la protección de derechos de autor y derechos de propiedad

industrial, así como medidas de protección tecnológica para garantizar la seguridad de los contenidos digitales.

Ley de Firma Electrónica (LFE): Esta ley regula el uso de la firma electrónica en España. Establece requisitos técnicos y legales para el uso de la firma electrónica como medio de identificación y autenticación.

Esquema Nacional de Seguridad (ENS): Es una normativa española que establece los requisitos de seguridad que deben cumplir los sistemas de información utilizados por las administraciones públicas. Estos requisitos se basan en las normas internacionales y europeas, como la norma ISO 27001, y abordan aspectos como la gestión de riesgos, la gestión de accesos, la gestión de incidentes, entre otros.

Norma ISO/IEC 27001: Es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Proporciona un marco para la gestión de la seguridad de la información, y es utilizada por muchas empresas e instituciones para mejorar sus prácticas de seguridad. En España, la norma ISO/IEC 27001 se ha adoptado como parte del Esquema Nacional de Seguridad.

Reducción de riesgos. Al implementar un SGSI, nuestra organización puede identificar y mitigar los riesgos de seguridad de la información, lo que reduce la probabilidad de sufrir una brecha de seguridad.

Mejora de la eficiencia. Un SGSI automatiza muchas de las tareas relacionadas con la gestión de la seguridad de la información, lo que mejora la eficiencia de nuestra organización.

Mejora de la toma de decisiones. Un SGSI proporciona información valiosa sobre los riesgos de seguridad de la información y permite a nuestra organización tomar decisiones informadas sobre cómo mejorar su seguridad.

Aumento de la confianza de los clientes y proveedores. Al implementar un SGSI, nuestra organización demuestra su compromiso con la seguridad de la información y puede aumentar la confianza de sus clientes y proveedores.

(E. Moya, 2023, p. 1)

Mantenimiento

El mantenimiento es un proceso integral que abarca un conjunto de actividades técnicas, administrativas y de gestión diseñadas para garantizar que los equipos y sistemas de una organización puedan cumplir con las funciones para las cuales fueron diseñados. Estas actividades no solo se centran en la reparación o restauración de los activos cuando fallan, sino que también incluyen acciones preventivas destinadas a evitar fallos antes de que ocurran, lo que es esencial para asegurar la continuidad operativa.

Dentro del marco de las actividades técnicas, el mantenimiento involucra inspecciones regulares, pruebas funcionales, ajustes y reemplazo de componentes defectuosos o desgastados. Estas tareas técnicas son fundamentales para asegurar que los equipos y sistemas operen dentro de los parámetros establecidos por los fabricantes o por la normativa aplicable.

Desde el punto de vista administrativo, el mantenimiento incluye la planificación y programación de las actividades de mantenimiento, la gestión de los recursos necesarios (como repuestos, herramientas y personal), y el seguimiento y registro de las actividades realizadas. Esto

permite una gestión eficiente del ciclo de vida de los activos y una toma de decisiones informada basada en datos reales de rendimiento y fallos.

En cuanto a la gestión, el mantenimiento debe alinearse con los objetivos estratégicos de la organización, asegurando que los recursos se utilicen de manera eficiente y que las actividades de mantenimiento contribuyan al logro de metas operativas y financieras. Esto implica también la implementación de sistemas de gestión de mantenimiento, como el Mantenimiento Basado en Condiciones (CBM) o el Mantenimiento Centrado en la Confiabilidad (RCM), que permiten optimizar los programas de mantenimiento y mejorar la relación costo-beneficio.

Finalmente, el mantenimiento es clave para reducir el riesgo de fallos inesperados, que pueden generar interrupciones en la producción, pérdidas financieras y daños a la reputación de la organización. Por lo tanto, una estrategia de mantenimiento bien implementada es vital para garantizar no solo la eficiencia y la disponibilidad de los activos, sino también la seguridad de las operaciones y la satisfacción de los clientes.

### Mantenimiento Preventivo

El mantenimiento preventivo se refiere a las acciones programadas y planificadas para evitar fallos en los equipos antes de que ocurran. Este tipo de mantenimiento se basa en la idea de que es más eficiente y menos costoso prevenir problemas que repararlos después de que se produzcan. Incluye actividades como la inspección regular, limpieza, lubricación y reemplazo de partes desgastadas.

### Tipos de Mantenimiento Preventivo

Existen varios tipos de mantenimiento preventivo, entre los que destacan el mantenimiento programado, basado en el tiempo, y el mantenimiento basado en la condición. El primero se realiza

en intervalos de tiempo establecidos, independientemente del estado del equipo, mientras que el segundo se basa en la monitorización de las condiciones de los equipos para determinar el momento óptimo de intervención.

### Análisis de Criticidad por Tipo de Equipo

El análisis de criticidad es un proceso que permite identificar y priorizar los equipos en función de su impacto en la operación general de la organización. Este análisis ayuda a definir qué equipos requieren mayor atención en los programas de mantenimiento preventivo, basándose en factores como la probabilidad de fallos y las consecuencias operativas de estos.

### Selección del Modelo de Mantenimiento

La selección del modelo de mantenimiento adecuado depende de varios factores, incluyendo la criticidad del equipo, el entorno operativo, y los recursos disponibles. Modelos como el mantenimiento basado en la fiabilidad (RCM) y el mantenimiento centrado en la condición (CBM) son comúnmente utilizados para optimizar las actividades de mantenimiento y maximizar la disponibilidad de los equipos.

### Beneficios del Mantenimiento Preventivo

El mantenimiento preventivo ofrece múltiples beneficios, como la reducción de los tiempos de inactividad, la prolongación de la vida útil de los equipos, y la mejora de la seguridad y confiabilidad operativa. También contribuye a la reducción de costos a largo plazo, al minimizar la necesidad de reparaciones de emergencia y reemplazos de equipos.

### Dimensiones del Mantenimiento Preventivo

Las dimensiones del mantenimiento preventivo incluyen aspectos técnicos, económicos y organizativos. Desde un punto de vista técnico, se enfoca en la realización de actividades que aseguren el funcionamiento óptimo de los equipos. Económicamente, busca maximizar el retorno de la inversión en mantenimiento, mientras que organizativamente, se preocupa por la integración de estas actividades en los procesos generales de la empresa.

## Productividad

La productividad es un indicador clave del rendimiento organizacional, que se mide como la relación entre la cantidad de productos o servicios generados y los recursos utilizados en el proceso de producción. Es un factor crítico en la competitividad de una empresa, y su mejora constante es un objetivo esencial para la sostenibilidad a largo plazo.

## Indicadores de la Productividad

Los indicadores de productividad incluyen métricas como la producción por hora trabajada, el uso eficiente de los materiales, y la capacidad de la planta. Estos indicadores permiten a las organizaciones evaluar su rendimiento y tomar decisiones informadas para mejorar la eficiencia operativa.

## Dimensiones de la Productividad

Las dimensiones de la productividad se refieren a los diferentes aspectos que influyen en la capacidad de una organización para producir eficientemente. Estas dimensiones incluyen la productividad del trabajo, del capital, y de la tecnología, así como la capacidad de innovar y adaptarse a cambios en el entorno operativo.

## Definición de Términos

En esta sección, se definirán los términos clave utilizados a lo largo de la investigación, proporcionando claridad y un entendimiento común sobre conceptos técnicos y específicos relacionados con el mantenimiento preventivo, la gestión de la productividad, y la seguridad de la información.

# III. METODOLOGÍA DE LA INVESTIGACIÓN

## 3.1 Enfoque y nivel de la investigación

El enfoque de esta investigación es cuantitativo, lo cual se alinea con la definición proporcionada por (Hernandez, 2014), quienes describen la investigación cuantitativa como un método estructurado de recolección y análisis de datos obtenidos de diversas fuentes. Este tipo de investigación se caracteriza por la utilización de herramientas informáticas, estadísticas y matemáticas para generar resultados. Su objetivo es concluyente, ya que busca cuantificar problemas y determinar su extensión, proporcionando resultados que pueden extrapolarse a una población más amplia. En el contexto de este estudio, se pretende recopilar y analizar datos numéricos para evaluar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense. Este enfoque facilita la obtención de datos objetivos, los cuales pueden ser analizados estadísticamente para identificar patrones, tendencias y relaciones significativas.

En cuanto al nivel de investigación, esta es de tipo descriptivo y explicativo. Según Hernandez 2014), los estudios descriptivos se enfocan en identificar y especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno sujeto a análisis. Estos estudios buscan medir o recopilar información de manera independiente o conjunta sobre los conceptos o variables a los que se refieren, sin necesariamente explicar cómo se relacionan entre sí. Por otro lado, Hernandez (2014) indica que los estudios

explicativos van más allá de la mera descripción de conceptos o fenómenos o del establecimiento de relaciones entre ellos. Están diseñados para responder a preguntas sobre las causas de eventos y fenómenos físicos o sociales, centrándose en explicar por qué ocurren y en qué condiciones se manifiestan o cómo se relacionan dos o más variables. En este contexto, la investigación descriptiva permitirá detallar y caracterizar los factores relacionados con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la organización. Al mismo tiempo, el componente explicativo se enfocará en analizar las causas y efectos de dicha implementación, evaluando cómo impacta en la seguridad de la información y la operatividad de la cooperativa.

## 3.2 Diseño de la investigación

El diseño de la investigación es de tipo no experimental, transversal. Según Hernandez (2014), la investigación no experimental se caracteriza por ser un proceso sistemático y empírico en el que las variables independientes no se manipulan intencionalmente, ya que los eventos de interés ya han ocurrido. En este tipo de investigación, se busca comprender y describir las relaciones entre variables tal como se presentan en su entorno natural, sin intervención o influencia directa del investigador. El objetivo principal es observar y analizar cómo se relacionan e inciden estas variables en un momento específico, similar a capturar una fotografía de un fenómeno en el contexto en el que se desarrolla. La investigación se llevará a cabo en un solo momento en el tiempo, recolectando datos que permitan evaluar la situación actual de la implementación del SGSI en la cooperativa.

## 3.3 Población y muestra

### *3.3.1 Población*

La población está constituida por los 150 colaboradores de la cooperativa de servicios múltiples en cuestión, quienes desempeñan diversos roles dentro de la organización y están

involucrados en la gestión de información o están afectados por las políticas y procedimientos de seguridad de la información implementados.

### *3.3.2 Tamaño de la Muestra: Tipo de muestreo*

Para determinar el tamaño de la muestra, se utilizará una técnica de muestreo probabilístico aleatorio simple. Otzen & Manterola (2017) señalan que la representatividad de una muestra es esencial para poder extrapolar y generalizar los resultados obtenidos a la población accesible, y de allí, a la población objetivo. Para que una muestra sea considerada representativa, debe ser seleccionada de forma aleatoria, garantizando que todos los individuos de la población objetivo tengan la misma probabilidad de ser incluidos. Además, el tamaño de la muestra debe ser suficiente para reflejar numéricamente a la población de origen en relación con la distribución de la variable estudiada. Según Otzen & Manterola (2017), la técnica de muestreo probabilístico aleatorio simple asegura que todos los individuos de la población objetivo tengan la misma probabilidad de ser seleccionados para la muestra. Esto implica que la probabilidad de que un individuo específico sea incluido en el estudio es independiente de la probabilidad de los demás miembros de la población. Por ejemplo, ante una pregunta de investigación como: ¿Cuál es la muestra necesaria para determinar la prevalencia de cambios inflamatorios en biopsias hepáticas de pacientes con colangitis aguda (CA)?, un muestreo aleatorio simple consistiría en seleccionar al azar un subgrupo representativo de todos los pacientes con CA.

La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 requiere la realización de cuestionarios técnicos. Estos cuestionarios son fundamentales para evaluar el nivel de cumplimiento con los requisitos específicos de la norma y para determinar el estado actual de la seguridad de la información en la organización. A través de este proceso de evaluación, se identifican posibles áreas de mejora y se

establecen las acciones necesarias para mitigar riesgos y proteger la información crítica, asegurando el cumplimiento con los estándares internacionales de seguridad. Siguiendo el enfoque propuesto por Mantilla (2009) plantea que para realizar una implementación efectiva de un SGSI, es necesario iniciar con un diagnóstico detallado de la situación actual de la organización en cuanto a la gestión de la seguridad de la información. Este diagnóstico involucra la evaluación de múltiples áreas específicas, cuyos resultados se analizan para identificar las fortalezas y debilidades en la gestión de la seguridad, estableciendo así una base sólida para la implementación del SGSI.

## 3.4 Técnicas e instrumentos para la recolección de la información de campo

### *3.4.1 Técnica*

La técnica seleccionada para la recolección de datos es la encuesta. Casas et al. (2002) señalan que el cuestionario es el principal instrumento empleado en la investigación por encuesta, definido como un "documento que organiza los indicadores de las variables relacionadas con el objetivo de la encuesta". A partir de esta definición, se puede deducir que el término "encuesta" se refiere a todo el proceso de investigación, mientras que "cuestionario" se limita al conjunto de preguntas dirigido a los participantes del estudio.

Las encuestas son adecuadas para este tipo de investigación, ya que permiten recopilar grandes volúmenes de datos de manera eficiente y en un tiempo relativamente corto. Además, facilitan la obtención de información estructurada que puede ser cuantificada y analizada estadísticamente.

### *3.4.2 Instrumento*

El instrumento que se utilizará es un cuestionario estructurado, diseñado específicamente para evaluar la implementación del SGSI y su impacto en la seguridad de la información dentro

de la cooperativa. El cuestionario incluirá preguntas cerradas de opción múltiple y escala Likert para medir las percepciones y opiniones de los colaboradores. Se asegurará de que el cuestionario sea claro, conciso y que aborde los principales aspectos relacionados con la seguridad de la información y el cumplimiento de la norma ISO 27001:2022.

El instrumento básico para esta investigación serán cuestionarios estructurados, diseñado específicamente para evaluar la situación actual de la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.). Este cuestionario, que servirá para recoger de forma organizada los indicadores de las variables implicadas en los objetivos del estudio, incluirá preguntas tanto cualitativas como cuantitativas. El propósito es obtener una comprensión detallada de los procesos, políticas, y controles de seguridad de la información en vigor. Basado en los lineamientos metodológicos de Sampieri, este cuestionario garantizará la validez y confiabilidad de los datos recopilados, permitiendo así una evaluación precisa y relevante de la implementación del SGSI.

La muestra para esta investigación estará compuesta por individuos que forman parte de COOPEVE, R.L., incluyendo colaboradores de áreas vinculantes directamente relacionados con la seguridad de la información y los procesos internos de la cooperativa. Se utilizará un enfoque de muestreo aleatorio simple, dependiendo de la heterogeneidad de la población en términos de roles y responsabilidades en la gestión de la seguridad de la información. Esta selección se llevará a cabo para asegurar que la muestra represente de manera adecuada a todos los segmentos clave de la población, permitiendo obtener una visión completa y representativa de la percepción y efectividad del SGSI implementado, y así reflejar de manera precisa la situación actual y las necesidades específicas de la cooperativa en términos de seguridad de la información.

## 3.5 Análisis y procesamiento de datos

Una vez recolectados los datos mediante las encuestas las cuales se dividieron en un cuestionario técnico y un cuestionario de usuario final, se procederá al análisis utilizando herramientas estadísticas como el software Excel. Se realizarán análisis descriptivos para resumir la información y proporcionar una visión general de los resultados. Además, se llevarán a cabo análisis inferenciales para identificar relaciones significativas entre las variables de interés, como la relación entre la implementación del SGSI y la percepción de seguridad de los colaboradores.

**Figura 3**

*Analisis FODA SGSI*




Nota: Diseño propio

# IV. RESULTADOS

## 4.1 Consideraciones Iniciales

### *4.1.1 Partes Interesadas*

Para el proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), es fundamental identificar y considerar a las partes interesadas. Aquí tienes una lista de las principales partes interesadas y una breve descripción de su interés en el proyecto:

**Tabla 2**

*Partes interesadas*

| Parte Interesada | Descripción del Interés |
|---|---|
| Alta Dirección | La alta dirección de COOPEVE, R.L. está interesada en asegurar que la implementación del SGSI mejore la seguridad de la información, cumpla con las normativas y proteja los activos críticos de la cooperativa. |
| Asociados | Los asociados de COOPEVE, R.L. se benefician de una mayor protección de sus datos personales y financieros, lo que aumenta la confianza en los servicios ofrecidos por la cooperativa. |

| | |
|---|---|
| Equipo de TI | El equipo de TI es responsable de implementar y mantener los controles técnicos del SGSI, asegurando la integridad, confidencialidad y disponibilidad de la información. |
| Empleados | Todos los empleados deben cumplir con las políticas de seguridad de la información y participar en programas de capacitación y concientización, lo que les permite desempeñar sus roles de manera segura y eficiente. |
| Auditores Internos y Externos | Los auditores internos y externos están interesados en evaluar la conformidad del SGSI con la norma ISO 27001:2022 y en identificar áreas de mejora para asegurar la eficacia del sistema de gestión. |
| Clientes y Usuarios | Los clientes y usuarios de los servicios de COOPEVE, R.L. esperan que sus datos estén protegidos contra accesos no autorizados y que la cooperativa maneje su información de manera segura y responsable. |
| Proveedores y Socios | Los proveedores y socios comerciales de COOPEVE, R.L. tienen interés en asegurar que la cooperativa mantenga altos estándares de seguridad de la información, lo que puede influir en la continuidad de las relaciones comerciales y en la confianza mutua. |
| Reguladores y Entidades Gubernamentales | Las entidades reguladoras y gubernamentales están interesadas en que COOPEVE, R.L. cumpla con las leyes y regulaciones aplicables en materia de seguridad de la información y protección de datos. |

| | |
|---|---|
| Comunidad y Sociedad | La comunidad y la sociedad en general se benefician de la implementación de prácticas de seguridad de la información que protegen los datos personales y financieros, contribuyendo a la estabilidad y confianza en el sector financiero. |

Nota: Estas partes interesadas juegan un papel crucial en el éxito del proyecto de implementación del SGSI, y es importante mantener una comunicación constante y efectiva con ellas para asegurar que sus necesidades y expectativas sean consideradas y satisfechas.

### *4.1.2 Recursos Disponibles*

Un desarrollo detallado de los recursos disponibles para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.):

Recursos Humanos

Alta Dirección: Proporciona liderazgo y apoyo estratégico, asegurando que el SGSI esté alineado con los objetivos de la cooperativa.

Equipo de TI: Encargado de la implementación y mantenimiento de los controles técnicos, así como de la gestión de incidentes de seguridad.

Responsable del SGSI: Coordina la implementación del SGSI, realiza evaluaciones de riesgos y asegura el cumplimiento de las políticas de seguridad.

Auditores Internos: Realizan auditorías periódicas para evaluar la conformidad y efectividad del SGSI.

Empleados: Participan en programas de capacitación y concientización, y cumplen con las políticas de seguridad de la información.

Recursos Tecnológicos

Sistemas de Autenticación: Herramientas para implementar autenticación multifactor y otros métodos de control de acceso.

Software de Seguridad: Incluye antivirus, sistemas de detección de intrusos, y herramientas de cifrado para proteger la información.

Infraestructura de Red: Firewalls, routers y switches configurados para asegurar la red interna de la cooperativa.

Sistemas de Respaldo: Soluciones de backup y recuperación de datos para asegurar la disponibilidad de la información crítica.

Plataformas de Monitoreo: Herramientas para supervisar la seguridad de la red y detectar posibles amenazas en tiempo real.

Recursos Financieros

Presupuesto Asignado: Fondos específicos destinados a la implementación y mantenimiento del SGSI, incluyendo la adquisición de software y hardware de seguridad.

Inversiones en Capacitación: Recursos financieros para programas de formación y concientización del personal en materia de seguridad de la información.

Contratación de Consultores: Presupuesto para contratar expertos externos que asesoren en la implementación del SGSI y realicen auditorías independientes.

Recursos Físicos

Instalaciones Seguras: Oficinas y centros de datos con controles de acceso físico, cámaras de vigilancia y sistemas de alarma.

Equipos de Seguridad: Dispositivos como cerraduras electrónicas, tarjetas de acceso y sistemas de control de acceso biométrico.

Recursos Documentales

Políticas y Procedimientos: Documentación detallada de las políticas de seguridad de la información, procedimientos operativos y guías de respuesta a incidentes.

Registros de Auditoría: Documentación de las auditorías internas y externas, incluyendo hallazgos y acciones correctivas.

Manuales de Capacitación: Materiales educativos y guías para la formación del personal en temas de seguridad de la información.

Recursos de Comunicación

Canales de Comunicación Interna: Plataformas como correos electrónicos, intranet y reuniones periódicas para mantener informados a todos los empleados sobre las políticas y procedimientos de seguridad.

Campañas de Concientización: Iniciativas para promover la cultura de seguridad de la información dentro de la cooperativa, utilizando boletines, carteles y seminarios.

Estos recursos son fundamentales para la implementación exitosa del SGSI en COOPEVE, R.L., asegurando que la cooperativa pueda proteger eficazmente su información crítica y cumplir con los requisitos de la norma ISO 27001:2022.

### *4.1.3 Proceso Critico Identificado*

A continuaciones se identifican los procesos críticos en las áreas de Finanzas, Productos y Servicios Operativos, Servicios Web, Administración, Áreas de Control y Gerencia de Tecnología para COOPEVE, R.L.:

Área de Finanzas

Proceso Crítico: Gestión de Préstamos y Créditos

Descripción: Incluye la evaluación, aprobación, desembolso y seguimiento de préstamos y créditos.

Importancia: Afecta directamente la liquidez y rentabilidad de la cooperativa, así como la satisfacción de los asociados y membresía en general.

Medidas de Seguridad: Autenticación multifactor, cifrado de datos, políticas de acceso basadas en roles, monitoreo y auditoría.

Proceso Crítico: Gestión Financiera

Descripción: Manejo de flujos de caja, inversiones y financiamiento.

Importancia: Asegura la disponibilidad de fondos para operaciones y proyectos.

Medidas de Seguridad: Controles de acceso, segregación de funciones, monitoreo de transacciones.

Productos y Servicios Operativos

Proceso Crítico: Gestión de Cuentas de Ahorro y Depósitos

Descripción: Apertura, mantenimiento y cierre de cuentas de ahorro y depósitos.

Importancia: Afecta la confianza de los asociados y la estabilidad financiera.

Medidas de Seguridad: Verificación de identidad, cifrado de datos, auditorías regulares.

Proceso Crítico: Servicios de Pago y Transferencias

Descripción: Procesamiento de pagos y transferencias entre cuentas.

Importancia: Asegura la eficiencia y seguridad en las transacciones financieras.

Medidas de Seguridad: Autenticación multifactor, monitoreo en tiempo real, cifrado de transacciones.

Servicios Web

Proceso Crítico: Plataforma de Banca en Línea

Descripción: Provisión de servicios bancarios a través de la web, incluyendo consultas de saldo, transferencias y pagos.

Importancia: Facilita el acceso de los asociados a sus cuentas y servicios financieros.

Medidas de Seguridad: Autenticación multifactor, cifrado SSL, monitoreo de actividad sospechosa.

Proceso Crítico: Portal de Servicios al Cliente

Descripción: Plataforma para la gestión de consultas, quejas y solicitudes de los asociados.

Importancia: Mejora la experiencia del cliente y la eficiencia operativa.

Medidas de Seguridad: Control de acceso, cifrado de datos, registro de auditoría.

Administración

Proceso Crítico: Gestión de Recursos Humanos

Descripción: Reclutamiento, capacitación, evaluación y gestión de personal.

Importancia: Asegura que la cooperativa cuente con personal capacitado y comprometido.

Medidas de Seguridad: Control de acceso a datos personales, políticas de privacidad, auditorías de cumplimiento.

Proceso Crítico: Gestión Documental

Descripción: Manejo de documentos y registros administrativos.

Importancia: Asegura la disponibilidad y protección de información crítica.

Medidas de Seguridad: Cifrado de documentos, control de acceso, copias de seguridad.

Áreas de Control

Proceso Crítico: Auditoría Interna

Descripción: Evaluación de la conformidad y efectividad de los procesos y controles internos.

Importancia: Identifica áreas de mejora y asegura el cumplimiento normativo.

Medidas de Seguridad: Independencia de auditores, acceso controlado a información, registro de hallazgos y acciones correctivas.

Proceso Crítico: Gestión de Riesgos

Descripción: Identificación, evaluación y mitigación de riesgos operativos y financieros.

Importancia: Protege a la cooperativa de pérdidas y asegura la continuidad del negocio.

Medidas de Seguridad: Evaluaciones periódicas de riesgos, implementación de controles, monitoreo continuo.

Gerencia de Tecnología

Proceso Crítico: Gestión de Infraestructura TI

Descripción: Mantenimiento y actualización de la infraestructura tecnológica.

Importancia: Asegura la disponibilidad y rendimiento de los sistemas tecnológicos.

Medidas de Seguridad: Monitoreo de sistemas, actualizaciones regulares, planes de contingencia.

Proceso Crítico: Seguridad de la Información

Descripción: Protección de la información contra accesos no autorizados, alteraciones y destrucción.

Importancia: Asegura la confidencialidad, integridad y disponibilidad de la información.

Medidas de Seguridad: Implementación de políticas de seguridad, controles de acceso, cifrado de datos, auditorías de seguridad.

Estos procesos críticos son esenciales para el funcionamiento eficiente y seguro de COOPEVE, R.L., y requieren una gestión cuidadosa y la implementación de medidas de seguridad adecuadas para proteger los activos de información y asegurar la continuidad del negocio.

## 4.2 Metodología para la Gestión de Riesgo

Para seleccionar la Metodología de riesgo a implementar junto al SGSI se estableció una matriz comparativa para definir la mejor opción.

**Tabla 3**

*Matriz comparativa selección Metodología de Riesgo*

| Criterio | | ISO 27005 | OCTAVE | NIST SP 800-30 | MAGERIT |
|---|---|---|---|---|---|
| Ámbito de Aplicación | Tipo de Organización | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| Tipo de Análisis | Cualitativo | CUMPLE | INCUMPLE | CUMPLE | CUMPLE |
| | Cuantitativo | CUMPLE | INCUMPLE | CUMPLE | CUMPLE |
| Elementos del Modelo | Proceso | CUMPLE | CUMPLE | NO CUENTA | CUMPLE |
| | Activos | CUMPLE | CUMPLE | NO CUENTA | CUMPLE |
| | Vulnerabilidades- | CUMPLE | CUMPLE | CUMPLE | INCUMPLE |
| | Amenazas | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| | Salvaguardas | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| Objetivos de Seguridad | Confidencialidad | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| | Integridad | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| | Disponibilidad | CUMPLE | CUMPLE | CUMPLE | CUMPLE |

| | | | | | |
|---|---|---|---|---|---|
| | Autenticidad | CUMPLE | NO CUENTA | NO CUENTA | CUMPLE |
| | Trazabilidad | CUMPLE | NO CUENTA | NO CUENTA | CUMPLE |
| Apoyo a la Implementación | Herramientas | CUMPLE | CUMPLE | NO CUENTA | CUMPLE |
| | Plan de Proyecto | CUMPLE | CUMPLE | NO CUENTA | CUMPLE |
| | Técnicas | CUMPLE | CUMPLE | NO CUENTA | CUMPLE |
| | Roles | CUMPLE | CUMPLE | CUMPLE | CUMPLE |
| | Comparativas | CUMPLE | NO CUENTA | CUMPLE | CUMPLE |

Nota: En la Tabla 3 se muestra el análisis comparativo de las metodologías de gestión de riesgos, ISO 27005 cumple con la mayoría de los criterios evaluados, incluyendo el tipo de análisis cualitativo y cuantitativo, elementos del modelo (proceso, activos, vulnerabilidades, amenazas, salvaguardas), y objetivos de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad). En contraste, OCTAVE y NIST SP 800-30 no cumplen con algunos de estos criterios, como el análisis cuantitativo y la autenticidad y trazabilidad en los objetivos de seguridad (ISO, 2018; Caralli et al., 2007; NIST, 2012; Consejo Superior de Administración Electrónica, 2006).

La norma ISO 27005 se presenta como una metodología robusta y completa para la gestión de riesgos en el sistema de seguridad de la información de COOPEVE, R.L. Al cumplir con la mayoría de los criterios evaluados, incluyendo el análisis cualitativo y cuantitativo, y al abordar de manera integral los elementos del modelo como procesos, activos, vulnerabilidades, amenazas y salvaguardas, ISO 27005 garantiza una cobertura exhaustiva de los riesgos potenciales.

Hoy en día, en nuestro mundo híper conectado e impulsado por la tecnología, las brechas de seguridad y los ciberataques, siguen siendo una amenaza para las organizaciones. Además de eso, el desconocimiento de los riesgos suele ser el culpable de estos problemas. Es por eso que, la norma ISO/IEC 27005:2018 ha sido revisada con el fin de actualizarla ante las necesidades de la sociedad actual. (isotools, 2024, p. 1)

Además, su enfoque en los objetivos de seguridad, tales como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, asegura que la información crítica de la cooperativa esté protegida contra accesos no autorizados, alteraciones y destrucción. La implementación de esta norma no solo fortalece la postura de seguridad de COOPEVE, R.L., sino que también promueve una cultura de gestión de riesgos proactiva y alineada con las mejores prácticas internacionales.

## 4.3 Valoración de Activos Críticos

### *4.3.1 Identificación de Activos*

**Tabla 4**

*Inventario de Activos pc*

| Gerencia, Dirreccion o Junta Directiva | Depto. | Modelo | | Equipo | Disco | Memoria RAM | Procesador |
|---|---|---|---|---|---|---|---|
| Gerencia Pro. Y Serv. | Beneficios | OPTIPLE X 7040 | 10 | MEBEN SERV4 | HDD 500gb | 4gb DDR4 | Intel® Core™ i5-6500 3.20ghz |
| Gerencia Pro. Y Serv. | Beneficios | OPTIPLE X 7010 | 10P | MEBEN SERV6 | HDD 500gb | 4gb DDR3 | Intel® Core™ i3-3220 3.30ghz |
| Gerencia Pro. Y Serv. | Beneficios | OPTIPLE X 7010 | 10 | MEBEN SERV1 | HDD 500gb | 4gb DDR3 | Intel® Core™ i3-3220 3.30ghz |
| Gerencia Pro. Y Serv. | Beneficios | OPTIPLE X 7010 | 10P | MEBEN SERV5 | HDD 500gb | 4gb DDR3 | Intel® Core™ i5-3320 |
| Junta Directiva | Comité de Educacion | LATITUD E 5590 | 10 | MECED U1 | SSD 500GB | 4GB DDR4 | Intel® Core™ i5-6500 3.20ghz |
| Junta Directiva | Junta de Directores | OPTIPLE X 9020 | 10 | MEJUD 2 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Junta Directiva | Comité de educacion | OPTIPLE X 7040 | 10 | MEED U2 | SSD 500GB | 4gb DDR4 | Intel® Core™ i5-6500 3.20ghz |
| | Gerencia de Riesgo | Gerencia de Riesgo | LATTITU DE 5590 | 10 | MEAU D1 | | | |
| | | Auditoria | OPTIPLE X 7010 | 10P | MEAU D3 | | | |
| 0 | Gerencia General | Asesoria Legal | Optiplex 9020 | 10 | MEASE LEG1 | HDD 500gb | 8gb DDR3 | Intel® Core™ i3-3220 3.30ghz |

Nota: En la Tabla 4 apreciamos una muestra del inventario de equipos informáticos.

La norma ISO 27005 proporciona un marco para la gestión de riesgos de la información, incluyendo la categorización de activos. A continuación, se presenta una matriz que categoriza los activos de información de COOPEVE, R.L., junto con una descripción de cada categoría y un código para cada tipo de activo:

**Tabla 5**

*Matriz de Categorías de Activos conforme a la Norma ISO 27005:2018*

| Código | Categoría de Activo | Descripción | Guía |
|---|---|---|---|
| INF | Información | Datos e información almacenada o procesada física o electrónicamente. | Bases de datos, archivos de datos, contratos, documentación del sistema, manuales de usuario. |
| SW | Software | Programas y aplicaciones utilizados para la gestión de operaciones y servicios. | Software de aplicación, interfaces, software del sistema, herramientas de desarrollo. |
| RH | Recurso Humano | Personas con conocimientos y experiencia crítica para el proceso. | Empleados clave, personal de TI, auditores internos. |
| SER | Servicio | Servicios de computación y comunicaciones que soportan las operaciones de la organización. | Servicios de Internet, Intranet, directorios compartidos, servicios de correo electrónico. |
| HW | Hardware | Equipos de cómputo y comunicaciones críticos para las operaciones. | Servidores, equipos de red, computadoras, dispositivos móviles. |

| | | | |
|---|---|---|---|
| OT | Otros | Activos que no encajan en las categorías anteriores, pero son importantes para el proceso. | Propiedad intelectual, reputación corporativa, licencias de software. |

Nota: En la Tabla 5, se observa la matriz categorizada con un código diferenciador.

Descripción de las Categorías de Activos

Información (INF):

Descripción: Incluye todos los datos e información que se almacenan o procesan, ya sea de forma física o electrónica. Estos activos son esenciales para las operaciones diarias y la toma de decisiones.

Ejemplos: Bases de datos de clientes, contratos legales, manuales de procedimientos, planes de continuidad del negocio.

Software (SW):

Descripción: Comprende todas las aplicaciones y programas utilizados para ejecutar y gestionar las operaciones de la organización. Estos activos son fundamentales para la automatización y eficiencia de los procesos.

Ejemplos: Software de gestión bancaria, herramientas de desarrollo, sistemas operativos, aplicaciones de seguridad.

Recurso Humano (RH):

Descripción: Se refiere a las personas que poseen conocimientos y habilidades críticas para la organización. Estos activos son vitales para la implementación y mantenimiento de los sistemas de información.

Ejemplos: Personal de TI, auditores internos, gerentes de seguridad de la información.

Servicio (SER):

Descripción: Incluye todos los servicios de computación y comunicaciones que soportan las operaciones de la organización. Estos activos son esenciales para la conectividad y el intercambio de información.

Ejemplos: Servicios de Internet, páginas web internas, directorios compartidos, servicios de correo electrónico.

Hardware (HW):

Descripción: Comprende todos los equipos físicos utilizados para procesar y almacenar información. Estos activos son críticos para la infraestructura tecnológica de la organización.

Ejemplos: Servidores, routers, switches, computadoras de escritorio, dispositivos móviles.

Otros (OT):

Descripción: Incluye activos que no se clasifican en las categorías anteriores pero que son importantes para la organización. Estos activos pueden tener un impacto significativo en la reputación y operaciones de la empresa.

Ejemplos: Propiedad intelectual, reputación corporativa, licencias de software.

### *4.3.2 Valoración de Activos*

La valoración de activos conforme a la norma ISO 27005 es un proceso esencial para identificar y priorizar los riesgos asociados a cada activo de información. Este proceso permite a la organización asignar recursos de manera efectiva para proteger los activos más críticos.

**Tabla 6**

*Guía inventario de activos en la implementación de la norma 27001:2022*




Nota: "El inventario es una herramienta que debe estar actualizada de la forma más pronta posible, de modo que ante nuevos cambios en la infraestructura TI, o cambios organizacionales se debe plantear una revisión del inventario"(Isotools, 2024, p. 1)

El inventario de activos es una parte crucial del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.). Este inventario proporciona una base sólida para la gestión de la seguridad de la información, permitiendo identificar y clasificar todos los activos de información que necesitan

protección. La creación y mantenimiento de un inventario de activos es esencial para asegurar que todos los elementos críticos de la organización estén adecuadamente protegidos y gestionados. Una vez identificados los activos de información, se les debe valorar de acuerdo con su importancia dentro de COOPEVE, siendo esta apreciación lo más objetiva posible, ya que con ella se determinará sobre qué activos se realizará el análisis de riesgos.

El objetivo del inventario de activos es identificar y documentar todos los activos de información dentro de COOPEVE, R.L., incluyendo hardware, software, datos, personas y otros recursos relevantes. Este inventario permite evaluar los riesgos asociados con cada activo y aplicar las medidas de seguridad adecuadas para protegerlos. El inventario abarca todos los activos de información de COOPEVE, R.L., incluyendo hardware como servidores, computadoras, dispositivos móviles, equipos de red, software como sistemas operativos, aplicaciones y bases de datos, datos almacenados en formato digital o físico, incluyendo datos personales, financieros y operativos; personas, es decir, colaboradores, contratistas y terceros que tienen acceso a los sistemas de información; y otros recursos como documentos, manuales, políticas y procedimientos relacionados con la seguridad de la información.

Los principios fundamentales del inventario de activos incluyen la identificación completa de todos los activos, la clasificación de los activos según su importancia y el nivel de protección requerido, la asignación de un propietario a cada activo responsable de su gestión y protección, y la actualización continua del inventario para reflejar cambios en el entorno de la información. El proceso de creación del inventario de activos comienza con la identificación exhaustiva de todos los activos de información en la organización, lo cual incluye entrevistas con el personal, revisión de documentos y análisis de sistemas. Luego, los activos se clasifican según su criticidad y el impacto potencial de su pérdida o compromiso, utilizando categorías como alta, media y baja

criticidad. A cada activo se le asigna un propietario responsable de su gestión y protección, quien debe ser una persona con conocimiento y autoridad sobre el activo. Todos los activos identificados se registran en un inventario centralizado, incluyendo detalles como nombre del activo, descripción, ubicación, propietario, clasificación y medidas de seguridad aplicadas. Se establece un proceso regular para revisar y actualizar el inventario de activos, lo cual puede incluir auditorías periódicas y revisiones de cambios en el entorno de la información.

Una vez identificados los activos de información, se les debe valorar de acuerdo con su importancia dentro de COOPEVE, siendo esta apreciación lo más objetiva posible, ya que con ella se determinará sobre qué activos se realizará el análisis de riesgos.

La valoración de activos es un proceso esencial para identificar y priorizar los riesgos asociados a cada activo de información. A continuación, se describen los pasos para realizar la valoración de activos, incluyendo la escala de valoración:

Pasos para la Valoración de Activos

Identificación de Activos:

Recopilar información detallada sobre cada activo, incluyendo su tipo, propietario, ubicación y descripción.

Clasificación de la Información:

Asignar niveles de confidencialidad, integridad y disponibilidad a cada activo.

Evaluación del Impacto:

Determinar el impacto potencial de la pérdida de confidencialidad, integridad y disponibilidad de cada activo.

Evaluación de la Probabilidad:

Estimar la probabilidad de que ocurra un incidente que afecte al activo.

Cálculo del Riesgo:

Utilizar una matriz de riesgo para combinar la evaluación del impacto y la probabilidad, determinando así el nivel de riesgo para cada activo.

Asignación de Criticidad:

Basado en el nivel de riesgo, asignar una criticidad al activo.

Escala de Valoración

La valoración de activos es un proceso esencial para identificar y priorizar los riesgos asociados a cada activo de información. A continuación, se detalla la fórmula matemática utilizada para calcular el riesgo, junto con la escala de valoración, la matriz de riesgo con colores y la perspectiva de cada nivel de riesgo.

Fórmula Matemática para el Cálculo del Riesgo

La fórmula básica para calcular el riesgo en la norma ISO 27005 es:

Riesgo = Impacto * Probabilidad

Donde:

Impacto: La consecuencia de que ocurra un incidente que afecte al activo.

Probabilidad: La posibilidad de que ocurra dicho incidente.

Escala de Valoración

Impacto

Alto (3): La pérdida tendría un impacto significativo en la organización.

Medio (2): La pérdida tendría un impacto moderado.

Bajo (1): La pérdida tendría un impacto mínimo.

Probabilidad

Alta (3): Es muy probable que ocurra.

Media (2): Es posible que ocurra.

Baja (1): Es poco probable que ocurra.

**Tabla 7**

*Matriz de riesgo con su valoración*

| **Impacto \ Probabilidad** | **Baja (1)** | **Media (2)** | **Alta (3)** | **Perspectiva** |
|---|---|---|---|---|
| Alto (3) | Medio (3) | Alto (6) | Muy Alto (9) | Medio (3): Riesgo moderado que requiere atención y posibles medidas de mitigación.<br>Alto (6): Riesgo significativo que necesita acciones inmediatas para reducirlo.<br>Muy Alto (9): Riesgo crítico que debe ser gestionado con prioridad máxima. |

| | | | | |
|---|---|---|---|---|
| | | | | Bajo (2): Riesgo bajo que puede ser aceptable con monitoreo regular. |
| Medio (2) | Bajo (2) | Medio (4) | Alto (6) | Medio (4): Riesgo moderado que requiere atención y posibles medidas de mitigación. |
| | | | | Alto (6): Riesgo significativo que necesita acciones inmediatas para reducirlo. |
| | | | | Bajo (1): Riesgo muy bajo que es generalmente aceptable. |
| Bajo (1) | Bajo (1) | Bajo (2) | Medio (3) | Bajo (2): Riesgo bajo que puede ser aceptable con monitoreo regular. |
| | | | | Medio (3): Riesgo moderado que requiere atención y posibles medidas de mitigación. |

Nota: En la Tabla 6 se muestra la matriz de riesgo en detalle con su ponderación.

### *4.3.3 Identificación de Amenazas y Vulnerabilidades*

El análisis de riesgos es un componente esencial del Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022. Este proceso permite identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información, asegurando que los activos de información estén protegidos contra amenazas potenciales. "Las amenazas pueden ser deliberadas, accidentales o ambientales (naturales) y dar como resultado, por ejemplo, daños o pérdidas de servicios esenciales."(ISO/IEC, 2018, p. 37)

En el contexto de la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), se realizará un análisis de riesgos tomando como ejemplo el sistema contable, las cajas, la atención al cliente, el servicio de ATM, la seguridad perimetral, el sistema de cortafuego y el centro de datos.

Leyenda de Origen

A: Accidental

D: Deliberado

E: Entorno

**Tabla 8**

*Riesgos identificados*

| Tipo | Amenazas | Origen |
|---|---|---|
| Daño físico | Incendio | A, D, E |
| | Daños por agua | A, D, E |
| | Contaminación | A, D, E |
| | Accidente mayor | A, D, E |
| | Destrucción de equipos o medios | A, D, E |
| | Polvo, corrosión, congelación | A, D, E |
| Eventos naturales | Fenómeno climático | E |

| | | |
|---|---|---|
| | Fenómeno sísmico | E |
| | Fenómeno volcánico | E |
| | Fenómeno meteorológico | E |
| | Inundación | E |
| Pérdida de servicios esenciales | Fallo del sistema de aire acondicionado o suministro de agua | A, D |
| | Pérdida de suministro eléctrico | A, D, E |
| | Fallo del equipo de telecomunicaciones | A, D |
| Perturbación por radiación | Radiación electromagnética | A, D, E |
| | Radiación térmica | A, D, E |
| | Pulsos electromagnéticos | A, D, E |
| Compromiso de la información | Intercepción de señales de interferencia comprometedoras | D |
| | Espionaje remoto | D |
| | Escucha clandestina | D |
| | Robo de medios o documentos | D |
| | Robo de equipos | D |
| | Recuperación de medios reciclados o descartados | D |
| | Divulgación | A, D |

| | | |
|---|---|---|
| | Datos de fuentes no confiables | A, D |
| | Manipulación de hardware | D |
| | Manipulación de software | A, D |
| | Detección de posición | D |
| Fallos técnicos | Fallo de equipo | A |
| | Mal funcionamiento del equipo | A |
| | Saturación del sistema de información | A, D |
| | Mal funcionamiento del software | A |
| | Incumplimiento de la mantenibilidad del sistema de información | A, D |
| Acciones no autorizadas | Uso no autorizado de equipos | D |
| | Copia fraudulenta de software | D |
| | Uso de software falsificado o copiado | A, D |
| | Corrupción de datos | D |
| | Procesamiento ilegal de datos | D |
| Compromiso de funciones | Error en el uso | A |
| | Abuso de derechos | A, D |
| | Falsificación de derechos | D |

| | |
|---|---|
| Negación de acciones | D |
| Incumplimiento de la disponibilidad del personal | A, D, E |

Nota: (ISO/IEC, 2018, p. 37)

"Se debe prestar especial atención a las fuentes de amenazas humanas. Estas se detallan específicamente en la siguiente tabla:" (ISO/IEC, 2018, p. 39)

**Tabla 9**

*Fuentes de Amenazas Humanas*

| **Origen de la Amenaza** | **Motivación** | **Posibles Consecuencias** |
|---|---|---|
| Hacker, cracker | Desafío | Hacking |
| | Ego | Ingeniería social |
| | Rebelión | Intrusión en el sistema, allanamientos |
| | Estatus | Acceso no autorizado al sistema |
| | Dinero | |
| Criminal informático | Destrucción de información | Delito informático (e.g., ciberacoso) |

| | | |
|---|---|---|
| | Divulgación ilegal de información | Acto fraudulento (e.g., repetición, suplantación, interceptación) |
| | Ganancia monetaria | Soborno de información |
| | Alteración no autorizada de datos | Suplantación |
| | | Intrusión en el sistema |
| Terrorista | Chantaje | Bomba/terrorismo |
| | Destrucción | Guerra de información |
| | Explotación | Ataque al sistema (e.g., denegación de servicio distribuida) |
| | Venganza | Penetración del sistema |
| | Ganancia política | Manipulación del sistema |
| | Cobertura mediática | |
| Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales) | Ventaja competitiva | Ventaja en defensa |
| | Espionaje económico | Ventaja política |
| | | Explotación económica |
| | | Robo de información |

| | | |
|---|---|---|
| | | Intrusión en la privacidad personal |
| | | Ingeniería social |
| | | Penetración del sistema |
| | | Acceso no autorizado al sistema (acceso a información clasificada, propietaria y/o relacionada con tecnología) |
| Personas con información privilegiada (empleados mal entrenados, descontentos, maliciosos, negligentes, deshonestos o despedidos) | Curiosidad | Agresión a un empleado |
| | Ego | Chantaje |
| | Inteligencia | Navegación de información propietaria |
| | Ganancia monetaria | Abuso informático |
| | Venganza | Fraude y robo |
| | Errores y omisiones no intencionales (e.g., error de entrada de datos, error de programación) | Soborno de información |
| | | Entrada de datos falsificados o corruptos |
| | | Interceptación |

| |
|---|
| Código malicioso (e.g., virus, bomba lógica, caballo de Troya) |
| Venta de información personal |
| Errores del sistema |
| Intrusión en el sistema |
| Sabotaje del sistema |
| Acceso no autorizado al sistema |

**Nota:** (ISO/IEC, 2018, p. 38)

### *4.3.4 Valoración de Amenaza y Vulnerabilidades*

Pasos para la Valoración

Identificación de Activos:

Recopilar información detallada sobre cada activo, incluyendo su tipo, propietario, ubicación y descripción.

Identificación de Amenazas:

Listar las posibles amenazas que pueden afectar a cada activo.

Identificación de Vulnerabilidades:

Listar las vulnerabilidades que pueden ser explotadas por las amenazas.

Evaluación del Impacto:

Determinar el impacto potencial de la explotación de una vulnerabilidad por una amenaza.

Evaluación de la Probabilidad:

Estimar la probabilidad de que una amenaza explote una vulnerabilidad.

Cálculo del Riesgo:

Utilizar la fórmula: Riesgo = Impacto * Probabilidad

A continuación, se presenta la valoración de amenazas y vulnerabilidades para los activos mencionados:

#### 4.3.4.1 Activo 1. Sistema Financiero

Amenazas:

Amenaza 1: Acceso no autorizado

Amenaza 2: Pérdida de datos

Vulnerabilidades:

Vulnerabilidad 1: Contraseñas débiles

Vulnerabilidad 2: Falta de copias de seguridad

Evaluación del Impacto:

Impacto del Acceso No Autorizado: Alto (3)

Impacto de la Pérdida de Datos: Alto (3)

Evaluación de la Probabilidad:

Probabilidad de Explotación de Contraseñas Débiles: Media (2)

Probabilidad de Explotación de Falta de Copias de Seguridad: Media (2)

Cálculo del Riesgo:

Riesgo del Acceso No Autorizado: Riesgo = 3 x 2 = 6

Riesgo de la Pérdida de Datos: Riesgo = 3 * 2 = 6

**Tabla 10**

*Activo 1: Sistema Financiero*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad |
|---|---|---|---|---|---|---|
| Sistema Financiero | Acceso no autorizado | Contraseñas débiles | Alto (3) | Media (2) | Alto (6) | Alta |
| | Pérdida de datos | Falta de copias de seguridad | Alto (3) | Media (2) | Alto (6) | Alta |

**Nota :** En la siguiente tabla se muestra el nivel de riesgo en el activo de Sistema Financiero como Alto.

#### 4.3.4.2 Activo 2. Cajas

Amenazas:

Amenaza 1: Robo físico

Amenaza 2: Fraude interno

Vulnerabilidades:

Vulnerabilidad 1: Seguridad física insuficiente

Vulnerabilidad 2: Falta de controles internos

Evaluación del Impacto:

Impacto del Robo Físico: Alto (3)

Impacto del Fraude Interno: Alto (3)

Evaluación de la Probabilidad:

Probabilidad de Explotación de Seguridad Física Insuficiente: Media (2)

Probabilidad de Explotación de Falta de Controles Internos: Media (2)

Cálculo del Riesgo:

Riesgo del Robo Físico: Riesgo = 3 * 2 = 6

Riesgo del Fraude Interno: Riesgo= 3 * 2 = 6

**Tabla 11**

*Activo 2: Cajas*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Cajas | Robo físico | Seguridad física insuficiente | Alto (3) | Media (2) | Alto (6) | Alta |
| | Fraude interno | Falta de controles internos | Alto (3) | Media (2) | Alto (6) | Alta |

Nota: En la Tabla 11 se observa el nivel de criticidad Alto en el Activo Cajas como importante en el Engranaje del negocio operativo.

#### 4.3.4.3 Activo 3. Atención al Cliente

Amenazas:

Amenaza 1: Divulgación de información confidencial

Amenaza 2: Interrupción del servicio

Vulnerabilidades:

Vulnerabilidad 1: Falta de capacitación del personal

Vulnerabilidad 2: Dependencia de sistemas críticos

Evaluación del Impacto:

Impacto de la Divulgación de Información: Alto (3)

Impacto de la Interrupción del Servicio: Medio (2)

Evaluación de la Probabilidad:

Probabilidad de Explotación de Falta de Capacitación: Media (2)

Probabilidad de Explotación de Dependencia de Sistemas Críticos: Media (2)

Cálculo del Riesgo:

Riesgo de la Divulgación de Información: Riesgo = 3 * 2 = 6

Riesgo de la Interrupción del Servicio: Riesgo = 2 * 2 = 4

**Tabla 12**

*Activo 3: Atención al Cliente*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad |
|---|---|---|---|---|---|---|
| Atención al Cliente | Divulgación de información | Falta de capacitación del personal | Alto (3) | Media (2) | Alto (6) | Alta |
| | Interrupción del servicio | Dependencia de sistemas críticos | Medio (2) | Media (2) | Medio(4) | Media |

Nota: En la Tabla 11 se observa el nivel de criticidad Alto en la Divulgación de información y medio en la Interrupción del Servicio.

#### 4.3.4.4 Activo 4. Servicio de ATM

Amenazas:

Amenaza 1: Robo de efectivo

Amenaza 2: Fraude electrónico

Vulnerabilidades:

Vulnerabilidad 1: Seguridad física insuficiente

Vulnerabilidad 2: Software desactualizado

Evaluación del Impacto:

Impacto del Robo de Efectivo: Alto (3)

Impacto del Fraude Electrónico: Alto (3)

Evaluación de la Probabilidad:

Probabilidad de Explotación de Seguridad Física Insuficiente: Media (2)

Probabilidad de Explotación de Software Desactualizado: Alta (3)

Cálculo del Riesgo:

Riesgo del Robo de Efectivo: Riesgo = 3 * 2 = 6

Riesgo del Fraude Electrónico: Riesgo = 3 * 3 = 9

**Tabla 13**

*Activo 4: Servicio de ATM*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad |
|---|---|---|---|---|---|---|
| Servicio de ATM | Robo de efectivo | Seguridad física insuficiente | Alto (3) | Media (2) | Alto (6) | Alta |
| | Fraude electrónico | Software desactualizado | Alto (3) | Alta (3) | Muy Alto (9) | Alta |

Nota: En la Tabla 12 se muestra el nivel de Criticidad respecto al Activo Servicio de ATM.

#### 4.3.4.5 Activo 5. Seguridad Perimetral

Amenazas:

Amenaza 1: Intrusión física

Amenaza 2: Sabotaje

Vulnerabilidades:

Vulnerabilidad 1: Sistemas de vigilancia inadecuados

Vulnerabilidad 2: Falta de personal de seguridad

Evaluación del Impacto:

Impacto de la Intrusión Física: Alto (3)

Impacto del Sabotaje: Alto (3)

Evaluación de la Probabilidad:

Probabilidad de Explotación de Sistemas de Vigilancia Inadecuados: Media (2)

Probabilidad de Explotación de Falta de Personal de Seguridad: Media (2)

Cálculo del Riesgo:

Riesgo de la Intrusión Física: Riesgo = 3 * 2 = 6

Riesgo del Sabotaje: Riesgo = 3 * 2 = 6

**Tabla 14**

*Activo 5: Seguridad Perimetral*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad |
|---|---|---|---|---|---|---|
| Seguridad Perimetral | Intrusión física | Sistemas de vigilancia inadecuados | Alto (3) | Media (2) | Alto (6) | Alta |
| | Sabotaje | Falta de personal de seguridad | Alto (3) | Media (2) | Alto (6) | Alta |

**Nota:** En la Tabla 13 se muestra el nivel de Criticidad respecto al Activo Servicio de Seguridad Perimetral.

### *4.3.5 Controles Existentes*

Los controles existentes ayudan a COOPEVE, R.L. a gestionar los riesgos asociados a sus activos de información, asegurando la confidencialidad, integridad y disponibilidad de los datos críticos.

#### 4.3.5.1 Control 1. Activo Sistema Contable

Control de Acceso:

Descripción: Implementación de autenticación multifactor (MFA) para asegurar que solo el personal autorizado pueda acceder al sistema contable.

Objetivo: Reducir el riesgo de acceso no autorizado.

Copias de Seguridad:

Descripción: Realización de copias de seguridad regulares y almacenamiento en ubicaciones seguras.

Objetivo: Mitigar el riesgo de pérdida de datos.

#### 4.3.5.2 Control 2 Activo. Cajas

Seguridad Física:

Descripción: Instalación de cámaras de vigilancia y sistemas de alarma en las áreas de las cajas.

Objetivo: Prevenir el robo físico y el fraude interno.

Controles Internos:

Descripción: Implementación de procedimientos de auditoría interna y segregación de funciones.

Objetivo: Detectar y prevenir actividades fraudulentas.

Activo: Atención al Cliente

Capacitación del Personal:

Descripción: Programas de capacitación regulares sobre la protección de información confidencial y la atención al cliente.

Objetivo: Reducir el riesgo de divulgación de información confidencial.

Planes de Continuidad del Negocio:

Descripción: Desarrollo de planes de continuidad del negocio para asegurar la disponibilidad del servicio en caso de interrupciones.

Objetivo: Mitigar el riesgo de interrupción del servicio.

Activo: Servicio de ATM

Seguridad Física:

Descripción: Instalación de cámaras de vigilancia y sistemas de alarma en los cajeros automáticos.

Objetivo: Prevenir el robo de efectivo.

Actualización de Software:

Descripción: Actualización regular del software de los cajeros automáticos para corregir vulnerabilidades.

Objetivo: Reducir el riesgo de fraude electrónico.

#### 4.3.5.3 Control 3 Activo: Seguridad Perimetral

Sistemas de Vigilancia:

Descripción: Implementación de sistemas de vigilancia avanzados, incluyendo cámaras de alta resolución y sensores de movimiento.

Objetivo: Detectar y prevenir intrusiones físicas.

Personal de Seguridad:

Descripción: Contratación y capacitación de personal de seguridad para monitorear y responder a incidentes de seguridad.

Objetivo: Aumentar la capacidad de respuesta ante amenazas físicas.

Activo: Sistema de Cortafuego

Configuración de Cortafuegos:

Descripción: Configuración y mantenimiento de cortafuegos para controlar el tráfico de red y prevenir accesos no autorizados.

Objetivo: Proteger la red interna de amenazas externas.

Monitoreo de Seguridad:

Descripción: Monitoreo continuo del tráfico de red y alertas de seguridad para detectar y responder a incidentes.

Objetivo: Mitigar el riesgo de ataques cibernéticos.

Activo: Centro de Datos

Control de Acceso Físico:

Descripción: Implementación de controles de acceso físico, como tarjetas de identificación y sistemas biométricos.

Objetivo: Prevenir el acceso no autorizado al centro de datos.

Redundancia y Respaldo:

Descripción: Implementación de sistemas redundantes y planes de respaldo para asegurar la disponibilidad continua de los servicios.

Objetivo: Mitigar el riesgo de fallos técnicos y pérdida de datos.

### *4.3.6 Evaluación de Riesgos*

La evaluación de riesgos es un proceso fundamental para identificar, analizar y priorizar los riesgos asociados a los activos de información.

**Tabla 15**

*Evaluación de los activos basado en Riesgo*

| Impacto \ Probabilidad | Baja (1) | Media (2) | Alta (3) | Perspectiva |
|---|---|---|---|---|
| Alto (3) | Medio (3) | Alto (6) | Muy Alto (9) | Medio (3): Riesgo moderado que requiere atención y posibles medidas de mitigación.<br>Alto (6): Riesgo significativo que necesita acciones inmediatas para reducirlo. |

| | | | | |
|---|---|---|---|---|
| | | | | Muy Alto (9): Riesgo crítico que debe ser gestionado con prioridad máxima. |
| Medio (2) | Bajo (2) | Medio (4) | Alto (6) | Bajo (2): Riesgo bajo que puede ser aceptable con monitoreo regular.<br>Medio (4): Riesgo moderado que requiere atención y posibles medidas de mitigación.<br>Alto (6): Riesgo significativo que necesita acciones inmediatas para reducirlo. |
| Bajo (1) | Bajo (1) | Bajo (2) | Medio (3) | Bajo (1): Riesgo muy bajo que es generalmente aceptable.<br>Bajo (2): Riesgo bajo que puede ser aceptable con monitoreo regular.<br>Medio (3): Riesgo moderado que requiere atención y posibles medidas de mitigación. |

Nota: La evaluación de riesgos conforme a la norma ISO 27005 permite a COOPEVE, R.L. identificar, analizar y priorizar los riesgos asociados a sus activos de información. Este proceso es fundamental para implementar controles de seguridad adecuados y asegurar la protección de los datos críticos.

### *4.3.7 Tratamiento de Riesgos*

El tratamiento de riesgos es una etapa crucial en la gestión de la seguridad de la información, ya que permite identificar y aplicar controles adecuados para mitigar los riesgos a niveles aceptables. En el contexto de la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), se ha desarrollado una matriz de tratamiento de riesgos que detalla

las amenazas, vulnerabilidades, impactos, probabilidades, niveles de riesgo y controles aplicables para cada activo crítico.

La matriz de tratamiento de riesgos (ver Tabla 15) proporciona una visión clara de los riesgos asociados a los activos de información y las medidas necesarias para mitigarlos. Cada activo ha sido evaluado en términos de impacto y probabilidad, utilizando una escala de valoración que clasifica el impacto como alto, medio o bajo, y la probabilidad como alta, media o baja. El riesgo se calcula multiplicando el impacto por la probabilidad, y se clasifica en niveles de criticidad: bajo, medio, alto y muy alto.

**Tabla 16**

*Matriz de Tratamiento del Riesgo*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Criticidad | Control Aplicable | Responsable |
|---|---|---|---|---|---|---|---|---|
| Sistema Financiero | Acceso no autorizado | Contraseñas débiles | Alto | Media | 6 | Alta | Autenticación multifactor (MFA) | Responsable de Seguridad |
| Sistema Financiero | Pérdida de datos | Falta de copias de seguridad | Alto | Media | 6 | Alta | Copias de seguridad regulares | Responsable de Seguridad |
| Cajas | Robo físico | Seguridad física | Alto | Media | 6 | Alta | Cámaras de vigilancia y alarmas | Gerencia de |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | insuficiente | | | | | | Tecnología |
| Cajas | Fraude interno | Falta de controles internos | Alto | Media | 6 | Alta | Procedimientos de auditoría interna | Auditor Interno |
| Atención al Cliente | Divulgación de información | Falta de capacitación del personal | Alto | Media | 6 | Alta | Programas de capacitación | Recursos Humanos |
| Atención al Cliente | Interrupción del servicio | Dependencia de sistemas críticos | Medio | Media | 4 | Media | Planes de continuidad del negocio | Gerencia de Tecnología |
| Servicio de ATM | Robo de efectivo | Seguridad física insuficiente | Alto | Media | 6 | Alta | Cámaras de vigilancia y alarmas | Gerencia de Tecnología |
| Servicio de ATM | Fraude electrónico | Software desactualizado | Alto | Alta | 9 | Muy Alta | Actualización regular del software | Gerencia de Tecnología |
| Seguridad Perimetral | Intrusión física | Sistemas de vigilancia inadecuados | Alto | Media | 6 | Alta | Sistemas de vigilancia avanzados | Gerencia de Tecnología |
| Seguridad Perimetral | Sabotaje | Falta de personal de | Alto | Media | 6 | Alta | Contratación y capacitación de personal | Recursos |

| | |
|---|---|
| segurida<br>d | Hum<br>anos |

Nota: En la Tabla 16, Se presenta la descripción detallada de cada Riesgo con su evaluación de Riesgo.

#### 4.3.7.1 Diseño de Controles

El diseño de controles es un proceso esencial en la gestión de riesgos del SGSI, ya que permite implementar medidas específicas para mitigar los riesgos identificados. Los controles pueden ser preventivos, detectivos o correctivos, y deben estar alineados con los objetivos de seguridad de la información de la organización.

#### 4.3.7.2 Tipos de Controles

Controles Preventivos: Evitan que ocurran incidentes de seguridad.

Ejemplo: Implementación de autenticación multifactor (MFA) para acceder a sistemas críticos.

Controles Detectivos: Identifican y detectan incidentes de seguridad cuando ocurren.

Ejemplo: Monitoreo continuo de la red para detectar actividades sospechosas.

Controles Correctivos: Corrigen y recuperan de incidentes de seguridad.

Ejemplo: Procedimientos de recuperación de desastres y copias de seguridad regulares.

Identificación de Controles Aplicables

Para identificar los controles aplicables, se puede utilizar el marco de referencia de la norma ISO/IEC 27001:2022, que proporciona una lista de controles recomendados. A continuación, se presentan algunos ejemplos de controles aplicables:

Control de Acceso:

Descripción: Implementar políticas de control de acceso basadas en roles.

Objetivo: Asegurar que solo el personal autorizado tenga acceso a la información crítica.

Seguridad Física:

Descripción: Instalar sistemas de vigilancia y controles de acceso físico.

Objetivo: Proteger los activos físicos contra accesos no autorizados.

Gestión de Incidentes de Seguridad:

Descripción: Establecer procedimientos para la gestión y respuesta a incidentes de seguridad.

Objetivo: Minimizar el impacto de los incidentes de seguridad y recuperar rápidamente las operaciones.

Capacitación y Concientización:

Descripción: Implementar programas de capacitación y concientización en seguridad de la información para todos los empleados.

Objetivo: Asegurar que el personal esté informado y capacitado para manejar la información de manera segura.

#### 4.3.7.3 Roles y Responsabilidades para el SGSI

La implementación y mantenimiento del SGSI requiere la participación de varios roles dentro de la organización. A continuación, se describen los roles y responsabilidades clave:

El Responsable de Seguridad

Descripción: Coordina la implementación y mantenimiento del SGSI.

Responsabilidades:

Realizar evaluaciones de riesgos y auditorías de seguridad.

Desarrollar y actualizar políticas y procedimientos de seguridad.

Coordinar programas de capacitación y concientización.

Monitorear el cumplimiento de las políticas de seguridad.

CEO

Descripción: Proporciona liderazgo y apoyo estratégico para el SGSI.

Responsabilidades:

Asegurar que el SGSI esté alineado con los objetivos estratégicos de la organización.

Aprobar políticas y procedimientos de seguridad.

Asignar recursos necesarios para la implementación del SGSI.

Promover una cultura de seguridad de la información en toda la organización.

Junta Directiva

Descripción: Supervisa la implementación y efectividad del SGSI.

Responsabilidades:

Revisar y aprobar el plan de seguridad de la información.

Monitorear el desempeño del SGSI y realizar revisiones periódicas.

Asegurar que se tomen medidas correctivas cuando sea necesario.

Evaluar los informes de auditoría y asegurar el cumplimiento normativo.

Gerencia de Tecnología

Descripción: Implementa y mantiene los controles técnicos del SGSI.

Responsabilidades:

Gestionar la infraestructura tecnológica y asegurar su seguridad.

Implementar controles de acceso y medidas de protección de datos.

Monitorear y responder a incidentes de seguridad.

Asegurar la disponibilidad, integridad y confidencialidad de la información.

## 4.4 Ciclo PDCA

La norma ISO 27001 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), también conocido como rueda de Deming o ciclo de Shewhart. El ciclo PDCA puede aplicarse no sólo al sistema de gestión en su conjunto, sino también a cada elemento individual para proporcionar un enfoque continuo en la mejora continua.

**Tabla 17**

*Fases del modelo Deming o Cicle Shewhart*

| FASES DEL PDCA | ACTIVIDADES |
|---|---|
| **PLANIFICAR** | Alcance del SGSI<br>Política de Seguridad |

| | |
|---|---|
| | Metodología para evaluación del riesgo |
| | Amenazas y vulnerabilidades |
| | Identificación del Impacto |
| | Analisis y Evaluación del Riesgo |
| | Selección de Controles |
| **HACER** | Aplicar el SGSI |
| | Plan de tratamiento de riesgos |
| | Implementar plan de tratamiento de riesgos |
| | Implementar Controles |
| | Capacitación y concientización |
| **CONTROLAR** | Revisar el SGSI |
| | Medir la eficacia de los controles |
| | Revisar los riesgos residuales |
| | Realizar auditorías internas del SGSI |
| | Registrar eventos y acciones |
| **ACTUAR** | Implementar mejoras al SGSI |
| | Aplicar acciones correctivas |
| | Aplicar acciones preventivas |
| | Comprobar la eficacia de las acciones |

Nota: En la Tabla 16 se detalla los pasos a seguir para el desarrollo del plan de implementación bajo la metodología PDCA.

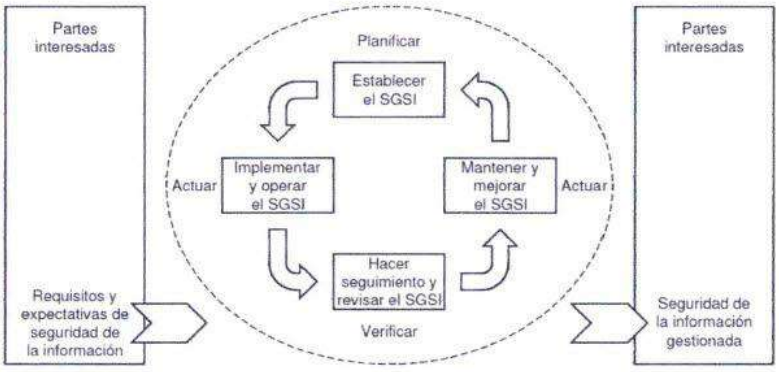
### *4.4.1 Fase Planificar / Plan*

#### 4.4.1.1 Alcance del SGSI

Para llevar a cabo una implementación eficaz de un Sistema de Gestión de Seguridad de la Información (SGSI), es fundamental comenzar con un diagnóstico exhaustivo de la situación actual de la organización en cuanto a la gestión de la seguridad de la información. Este diagnóstico abarca la evaluación de diversas áreas clave, cuyos resultados permiten identificar tanto las fortalezas como las áreas de mejora en la gestión de la seguridad, proporcionando una base sólida para la correcta implementación del SGSI.

**Figura 4**

*Ciclo PDCA y sus partes interesadas*




Nota: En la Figura 3 se aprecia el Ciclo Deming o PDCA estableciendo los pasos a seguir en la implementación del SGSI.

La implementación de la norma ISO 27001:2022 se llevará a cabo en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), una entidad de intermediación financiera ubicada en Panamá, provincia de Veraguas. COOPEVE, R.L. brinda una variedad de

servicios financieros, como préstamos personales, microcréditos y productos de ahorro, constituyendo un apoyo fundamental para sus miembros en la región.

Dado su papel en el sector financiero, la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022 se orientará a garantizar la protección de la confidencialidad, integridad y disponibilidad de la información crítica que involucra sus operaciones financieras.

#### 4.4.1.2 Política de Seguridad

La política del Sistema de Gestión de Seguridad de la Información (SGSI) es un documento fundamental que establece el compromiso de la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.) con la protección de la información. Esta política proporciona una dirección clara y un marco para la gestión de la seguridad de la información, asegurando que todos los miembros de la organización comprendan sus responsabilidades y actúen de acuerdo con los principios establecidos. El objetivo principal de la política del SGSI es garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por COOPEVE, R.L. Para lograr esto, la política busca proteger los activos de información contra amenazas internas y externas, minimizar los riesgos de seguridad y asegurar el cumplimiento con la norma ISO 27001:2022 y otras regulaciones aplicables.

Esta política se aplica a todos los colaboradores, contratistas y terceros que tienen acceso a los sistemas de información y datos de COOPEVE, R.L. Incluye todos los activos de información, tanto físicos como digitales, y abarca todas las áreas operativas de la cooperativa. Los principios fundamentales de la política de seguridad se centran en la confidencialidad, asegurando que la información solo sea accesible a personas autorizadas; la integridad, manteniendo la exactitud y completitud de la información y los métodos de procesamiento; y la

disponibilidad, garantizando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea necesario.

La alta dirección de COOPEVE, R.L. se compromete a proveer los recursos necesarios para implementar y mantener el SGSI, promover una cultura de seguridad de la información en toda la organización, asegurar el cumplimiento con la normativa ISO 27001:2022 y otras regulaciones aplicables, y revisar y mejorar continuamente el SGSI para adaptarse a nuevos riesgos y cambios en el entorno. Las responsabilidades dentro de la organización están claramente definidas: la alta dirección es responsable de aprobar y revisar la política del SGSI, asignar recursos y asegurar el cumplimiento; el responsable del SGSI debe implementar y mantener el SGSI, realizar evaluaciones de riesgos y coordinar las actividades de seguridad; y los colaboradores y contratistas deben cumplir con la política del SGSI, reportar incidentes de seguridad y participar en programas de capacitación.

COOPEVE, R.L. se compromete a realizar evaluaciones periódicas de riesgos para identificar, analizar y mitigar los riesgos relacionados con la seguridad de la información. Las medidas de control serán implementadas para reducir los riesgos a niveles aceptables. Además, todos los colaboradores y contratistas recibirán capacitación regular en seguridad de la información para asegurar que comprendan sus responsabilidades y las mejores prácticas para proteger la información. El cumplimiento con esta política será monitoreado a través de auditorías internas y revisiones periódicas. Cualquier incumplimiento será tratado de acuerdo con los procedimientos disciplinarios de la cooperativa.

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno de seguridad de la información, para asegurar su continua adecuación y efectividad.

Finalmente, esta política ha sido aprobada por la alta dirección de COOPEVE, R.L. y es de cumplimiento obligatorio para todos los colaboradores, contratistas y terceros asociados.

#### 4.4.1.3 Metodología para la Evaluación del Riesgo

Una vez que los activos han sido identificados y clasificados, es crucial evaluar los riesgos asociados con cada uno. Esto incluye identificar amenazas potenciales, evaluar vulnerabilidades y determinar el impacto de posibles incidentes de seguridad. Basado en esta evaluación, se deben implementar controles de seguridad adecuados para mitigar los riesgos identificados. Para facilitar este proceso, se utiliza una matriz de riesgos que ayuda a visualizar y priorizar los riesgos. La matriz de riesgos clasifica los riesgos en función de su probabilidad de ocurrencia y el impacto potencial, permitiendo a la organización enfocar sus recursos en los riesgos más críticos.

**Tabla 18**

*Matriz de Riesgos de inventario*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Control |
|---|---|---|---|---|---|---|
| Servidor de Datos | Acceso no autorizado | Contraseñas débiles | Alto | Alta | Crítico | Implementar autenticación multifactor |
| Base de Datos | Pérdida de datos | Falta de copias de seguridad | Muy Alto | Media | Alto | Realizar copias de seguridad diarias |
| Computadoras | Malware | Software desactualizado | Alto | Alta | Crítico | Actualizar |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | software regularmente |
| Información Financiera | Robo de información | Acceso físico no controlado | Muy Alto | Baja | Medio | Controlar acceso físico |
| Dispositivos Móviles | Pérdida o robo | Falta de cifrado | Alto | Media | Alto | Cifrar dispositivos móviles |

Nota: Activos analizados de acuerdo con su nivel de riesgo.

Todos los colaboradores y contratistas deben ser capacitados sobre la importancia del inventario de activos y su papel en la protección de la información. La capacitación debe incluir cómo identificar y reportar activos, así como las responsabilidades de los propietarios de activos. El cumplimiento con el proceso de inventario de activos será monitoreado a través de auditorías internas y revisiones periódicas. Cualquier incumplimiento será tratado de acuerdo con los procedimientos disciplinarios de la cooperativa. La política de inventario de activos será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno de la información, para asegurar su continua adecuación y efectividad. Esta política de inventario de activos debe se aprobada por la alta dirección de COOPEVE, R.L. y debe ser de cumplimiento obligatorio para todos los colaboradores, contratistas y terceros asociados.

#### 4.4.1.4 Amenazas y Vulnerabilidades

El análisis de riesgos es un componente esencial del Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022. Este proceso permite identificar, evaluar y

gestionar los riesgos relacionados con la seguridad de la información, asegurando que los activos de información estén protegidos contra amenazas potenciales. En el contexto de la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), se realizará un análisis de riesgos tomando como ejemplo el sistema contable, las cajas, la atención al cliente, el servicio de ATM, la seguridad perimetral, el sistema de cortafuego y el centro de datos.

Primero, se identifican los activos de información críticos: el sistema contable, que incluye software y bases de datos que gestionan las finanzas de la cooperativa; las cajas, que son los puntos de transacción donde se maneja efectivo y se realizan operaciones financieras; la atención al cliente, que abarca los sistemas y procesos que gestionan la interacción con los socios y clientes; el servicio de ATM, que permite a los socios realizar transacciones fuera del horario de oficina; la seguridad perimetral, que protege las instalaciones físicas de la cooperativa; el sistema de cortafuego, que protege la red informática de accesos no autorizados; y el centro de datos, que alberga los servidores y equipos críticos para las operaciones de la cooperativa. Para cada activo, se identifican las amenazas potenciales y las vulnerabilidades asociadas.

La evaluación del impacto y la probabilidad se realiza utilizando una matriz de riesgos. El impacto se refiere a las consecuencias de un incidente de seguridad, mientras que la probabilidad se refiere a la posibilidad de que ocurra dicho incidente. La valoración del riesgo se calcula utilizando la siguiente ecuación:

$$\text{Riesgo} = \text{Impacto} \times \text{Probabilidad}$$

Donde el impacto se mide en una escala de 1 a 5, donde 1 es bajo y 5 es muy alto, y la probabilidad se mide en una escala de 1 a 5, donde 1 es improbable y 5 es muy probable.

Para el sistema contable, la amenaza de acceso no autorizado debido a contraseñas débiles tiene un impacto muy alto (5) y una probabilidad alta (4), resultando en un riesgo de 20. Para las cajas, la amenaza de robo de efectivo debido a seguridad física insuficiente tiene un impacto alto (4) y una probabilidad media (3), resultando en un riesgo de 12. En el caso de la atención al cliente, la amenaza de fuga de información debido a la falta de capacitación en seguridad tiene un impacto medio (3) y una probabilidad alta (4), resultando en un riesgo de 12. Para el servicio de ATM, la amenaza de fraude en transacciones debido a software desactualizado tiene un impacto muy alto (5) y una probabilidad media (3), resultando en un riesgo de 15. En cuanto a la seguridad perimetral, la amenaza de intrusión física debido a medidas de seguridad insuficientes tiene un impacto alto (4) y una probabilidad media (3), resultando en un riesgo de 12. Para el sistema de cortafuego, la amenaza de acceso no autorizado debido a configuraciones incorrectas tiene un impacto muy alto (5) y una probabilidad media (3), resultando en un riesgo de 15. Finalmente, para el centro de datos, la amenaza de fallos en el suministro eléctrico debido a la falta de redundancia tiene un impacto muy alto (5) y una probabilidad media (3), resultando en un riesgo de 15.

**Tabla 19**

*Activos basados en el nivel de riesgo*

| Activo | Amenaza | Vulnerabilidad | Impacto | Probabilidad | Riesgo | Control |
|---|---|---|---|---|---|---|
| Sistema Contable | Acceso no autorizado | Contraseñas débiles | 5 | 4 | 20 | Implementar autenticación multifactor |
| Cajas | Robo de efectivo | Seguridad física insuficiente | 4 | 3 | 12 | Mejorar seguridad física |

| | | | | | | |
|---|---|---|---|---|---|---|
| Atención al Cliente | Fuga de información | Falta de capacitación en seguridad | 3 | 4 | 12 | Capacitación en seguridad |
| Servicio de ATM | Fraude en transacciones | Software desactualizado | 5 | 3 | 15 | Actualizar software regularmente |
| Seguridad Perimetral | Intrusión física | Medidas de seguridad insuficientes | 4 | 3 | 12 | Mejorar medidas de seguridad física |
| Sistema de Cortafuego | Acceso no autorizado | Configuraciones incorrectas | 5 | 3 | 15 | Revisar y actualizar configuraciones |
| Centro de Datos | Fallos en el suministro eléctrico | Falta de redundancia | 5 | 3 | 15 | Implementar sistemas de respaldo |

Nota: En la Tabla 19 podemos apreciar el nivel de riesgo del sistema contable.

El análisis de riesgos es un proceso continuo y dinámico que debe ser integrado en el SGSI de COOPEVE, R.L. Utilizando el modelo PDCA de Deming, la organización puede asegurar que los riesgos relacionados con la seguridad de la información sean gestionados de manera efectiva, protegiendo así sus activos de información y asegurando la continuidad operativa. La implementación de un análisis de riesgos estructurado y sistemático no solo cumple con los requisitos de la norma ISO 27001:2022, sino que también fortalece la resiliencia de la organización frente a amenazas y vulnerabilidades.

#### 4.4.1.5 Identificación de Activos y Amenazas

El primer paso en el análisis de riesgos es la identificación de los activos de información críticos. En COOPEVE, R.L., estos activos incluyen el sistema contable, las cajas, la atención al

cliente, el servicio de ATM, la seguridad perimetral, el sistema de cortafuego y el centro de datos. Cada uno de estos activos desempeña un papel crucial en las operaciones diarias de la cooperativa y, por lo tanto, debe ser protegido adecuadamente.

Sistema Contable: Este activo incluye el software y las bases de datos que gestionan todas las transacciones financieras de la cooperativa. La integridad y disponibilidad de este sistema son esenciales para la precisión de los registros financieros y la toma de decisiones estratégicas.

Cajas: Las cajas son los puntos de transacción donde se maneja efectivo y se realizan operaciones financieras. La seguridad física y lógica de estos puntos es crucial para prevenir robos y fraudes.

Atención al Cliente: Este activo abarca los sistemas y procesos que gestionan la interacción con los socios y clientes. La protección de la información personal y financiera de los clientes es fundamental para mantener la confianza y cumplir con las regulaciones de privacidad.

Servicio de ATM: Los cajeros automáticos permiten a los socios realizar transacciones fuera del horario de oficina. La seguridad de estos dispositivos es vital para prevenir fraudes y garantizar la disponibilidad del servicio.

Seguridad Perimetral: Este activo incluye todas las medidas físicas y electrónicas implementadas para proteger las instalaciones de la cooperativa contra accesos no autorizados. La seguridad perimetral es esencial para prevenir intrusiones físicas y proteger los activos físicos de la organización.

Sistema de Cortafuego: Este activo protege la red informática de la cooperativa contra accesos no autorizados y ataques cibernéticos. La configuración y el mantenimiento adecuados del sistema de cortafuego son cruciales para asegurar la integridad y disponibilidad de la red.

Centro de Datos: Este activo alberga los servidores y equipos críticos para las operaciones de la cooperativa. La disponibilidad y seguridad del centro de datos son esenciales para garantizar la continuidad operativa y la protección de la información crítica.

La norma ISO 27001:2022 proporciona un marco para la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información. A continuación, se amplía la valoración de activos enfocada en los requisitos de esta norma.

**Tabla 20**

*Clasificación de la información según la triada*

| REQUISITO | BAJO | MEDIO | ALTO |
|---|---|---|---|
| Confidencialidad | La información es de carácter público y no tiene impacto si es accedida por personas no autorizadas. | La información es de uso interno o restringido; el acceso no autorizado no afectaría gravemente. | La información es confidencial o secreta; el acceso no autorizado tendría un impacto muy grave. |

| | | | |
|---|---|---|---|
| Integridad | El daño o modificación no autorizada no es crítico y el impacto es insignificante o menor. | El daño o modificación no autorizada es notorio y el impacto es significativo. | El daño o modificación no autorizada es crítica y el impacto es importante, pudiendo afectar gravemente la aplicación o sistema. |
| Disponibilidad | Se puede tolerar que el activo no esté disponible por más de un día. | Se puede tolerar que el activo no esté disponible por medio día a un día. | No se puede tolerar que el activo no esté disponible por más de unas pocas horas (4) o menos. |

Nota: En la Tabla 20 establecemos la clasificación de la información según la triada para el establecimiento del nivel de riesgo.

**Tabla 21**

*Activos analizados según la amenaza y vulnerabilidad para el nivel de riesgo*

| **Activo** | **Amenaza** | **Vulnerabilidad** | **Impacto** | **Probabilidad** | **Riesgo** | **Control** |
|---|---|---|---|---|---|---|
| Sistema Contable | Acceso no autorizado | Contraseñas débiles | 5 | 4 | **20** | Implementar autenticación multifactor |

| | | | | | | |
|---|---|---|---|---|---|---|
| Cajas | Robo de efectivo | Seguridad física insuficiente | 4 | 3 | **12** | Mejorar seguridad física |
| Atención al Cliente | Fuga de información | Falta de capacitación | 3 | 4 | **12** | Capacitación en seguridad |
| Servicio de ATM | Fraude en transacciones | Software desactualizado | 5 | 3 | **15** | Actualizar software regularmente |
| Seguridad Perimetral | Intrusión física | Medidas de seguridad insuficientes | 4 | 3 | **12** | Mejorar medidas de seguridad física |
| Sistema de Cortafuego | Acceso no autorizado | Configuraciones incorrectas | | 3 | 15 | Revisar y actualizar configuraciones |
| Centro de Datos | Fallos en el suministro eléctrico | Falta de redundancia | | 3 | 15 | Implementar sistemas de respaldo |

Nota: En la tabla 21 se aprecia matriz de riesgo por activo con su valor de riesgo calculado en su impacto y probabilidad.

**Tabla 22**

*Matriz de la triada según activo*

| Activo | Confidencialidad | Integridad | Disponibilidad | Detalle de Valoración |
|---|---|---|---|---|
| Sistema Contable | Alto | Alto | **Alto** | Información financiera crítica. Modificaciones no autorizadas pueden causar graves errores financieros. Indisponibilidad afecta operaciones diarias. |
| Cajas | Medio | Medio | **Alto** | Información de transacciones. Errores pueden afectar balances. Indisponibilidad afecta servicio al cliente. |
| Atención al Cliente | Medio | Medio | **Medio** | Datos personales de clientes. Errores pueden afectar la calidad del servicio. |

| | | | | |
|---|---|---|---|---|
| | | | | Indisponibilidad afecta la atención al cliente. |
| Servicio de ATM | Alto | Alto | **Alto** | Datos de transacciones y clientes.<br>Errores pueden causar pérdidas financieras.<br>Indisponibilidad afecta acceso a fondos. |
| Seguridad Perimetral | Bajo | Medio | **Alto** | Información general de seguridad.<br>Errores pueden permitir accesos no autorizados.<br>Indisponibilidad afecta la seguridad física. |
| Sistema de Cortafuego | Alto | Alto | Alto | Protección de datos sensibles.<br>Configuraciones incorrectas pueden permitir accesos no autorizados.<br>Indisponibilidad afecta la seguridad de la red. |
| Centro de Datos | Alto | Alto | Alto | Datos críticos de la organización.<br>Errores pueden causar pérdida de datos.<br>Indisponibilidad afecta todas las operaciones. |

Nota: Esta tabla organiza los activos de información de COOPEVE, R.L. según los requisitos de Confidencialidad, Integridad y Disponibilidad y proporciona detalles sobre el impacto de cada activo en el proceso.

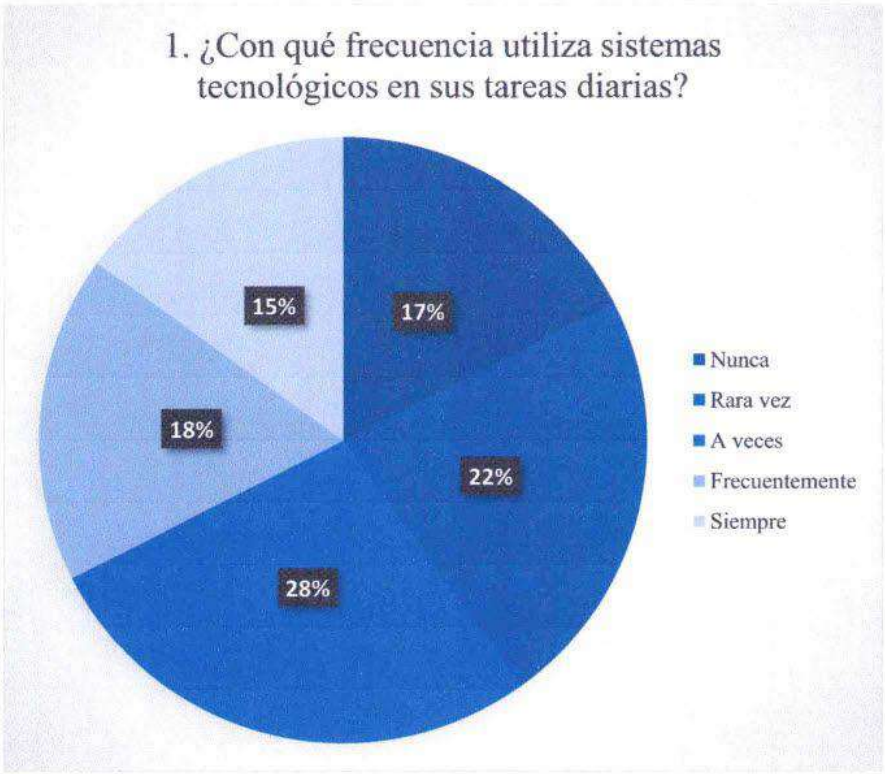
#### 4.4.1.6 Identificación del Impacto

La identificación del impacto es un componente esencial en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022. Este proceso implica evaluar cómo las actividades del proyecto pueden afectar diversos aspectos de la organización, incluyendo el entorno, la economía y la sociedad. En el contexto de COOPEVE, R.L., la identificación del impacto comienza con un análisis exhaustivo de los activos de información y las posibles amenazas que podrían comprometer su confidencialidad, integridad y disponibilidad.

Para llevar a cabo esta identificación, es fundamental recopilar datos relevantes basado en una encuesta inicial, con el personal clave y revisar documentos y sistemas existentes. Se realizo una encuesta al personal tomando como referencia preguntas enfocadas en la Seguridad de la información en una muestra representativa de 40 colaboradores.

**Figura 5**

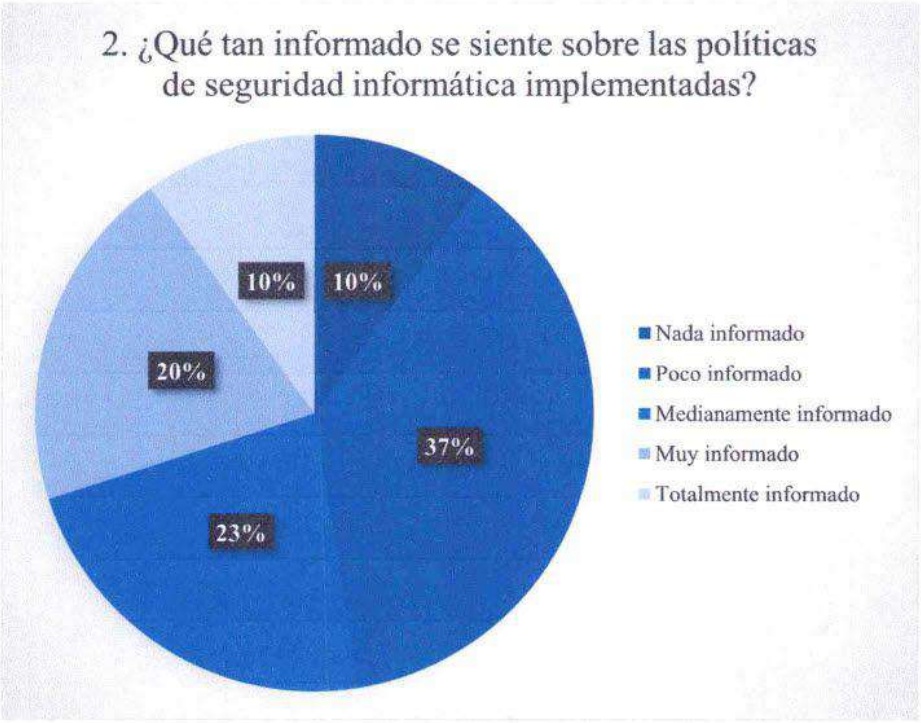
*Pregunta 1 - Encuesta*




Nota: En la Figura 5, el 17% de los encuestados indicó que nunca utiliza sistemas tecnológicos, mientras que un 22% señaló que lo hace rara vez. La mayoría de los participantes, representando un 28%, mencionó que a veces emplea tecnología en sus actividades diarias. Un 18% de los encuestados afirmó usarla frecuentemente, y finalmente, un 15% indicó que siempre recurre a sistemas tecnológicos en su rutina diaria. Estos resultados sugieren una distribución bastante equilibrada en cuanto al uso de tecnología, con una ligera inclinación hacia un uso ocasional. Esto podría reflejar una diversidad en las necesidades y hábitos tecnológicos de los individuos encuestados, indicando que mientras algunos dependen regularmente de la tecnología, otros la utilizan de manera más esporádica.

**Figura 6**

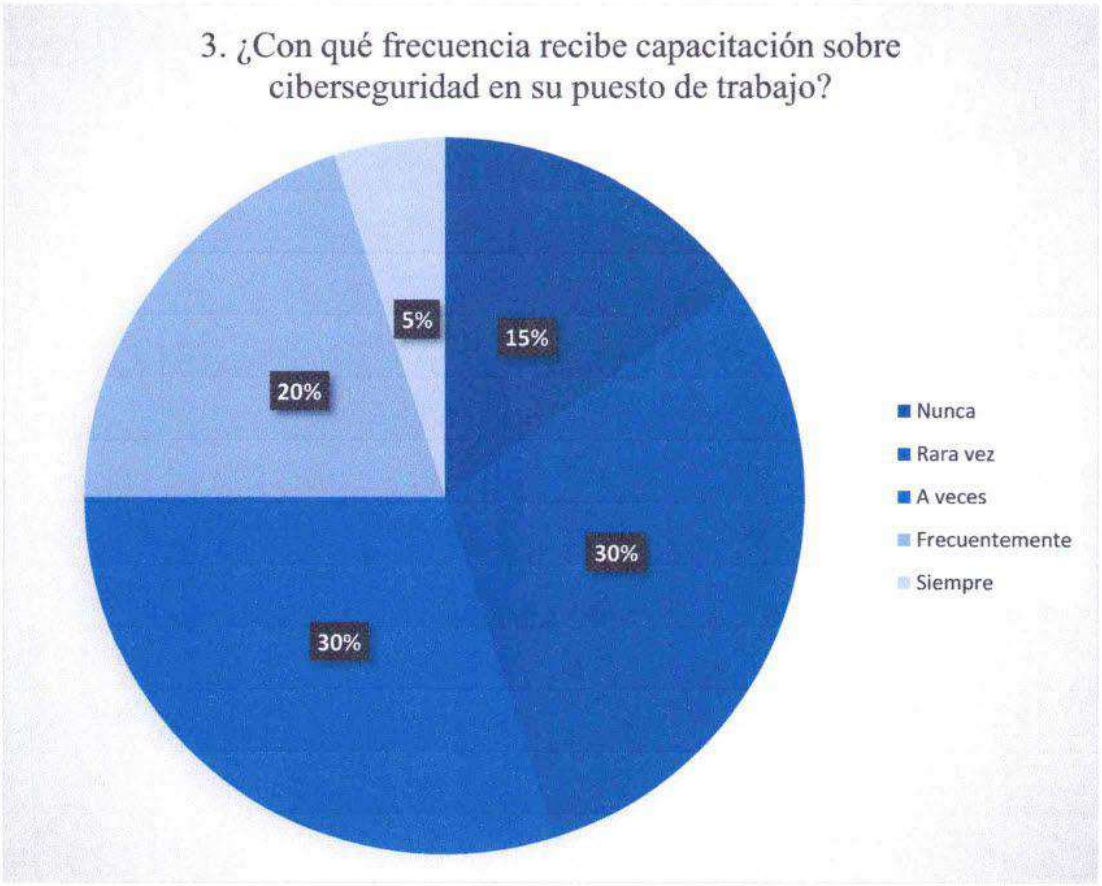
*Pregunta 2 - Encuesta*




Nota: En la Figura 6, el 10% de los encuestados se consideró nada informado, mientras que un 37% se identificó como poco informado. Un 23% de los participantes se describió como medianamente informado, y un 20% afirmó estar muy informado. Finalmente, un 10% de los encuestados indicó estar totalmente informado. Estos resultados muestran que la mayoría de los encuestados se siente poco o medianamente informado, lo que sugiere una oportunidad para mejorar la difusión de información y aumentar el nivel de conocimiento entre los individuos. La distribución también indica que hay un grupo significativo que se considera bien informado, lo cual es positivo para la toma de decisiones.

**Figura 7**

*Pregunta 3 - Encuesta*

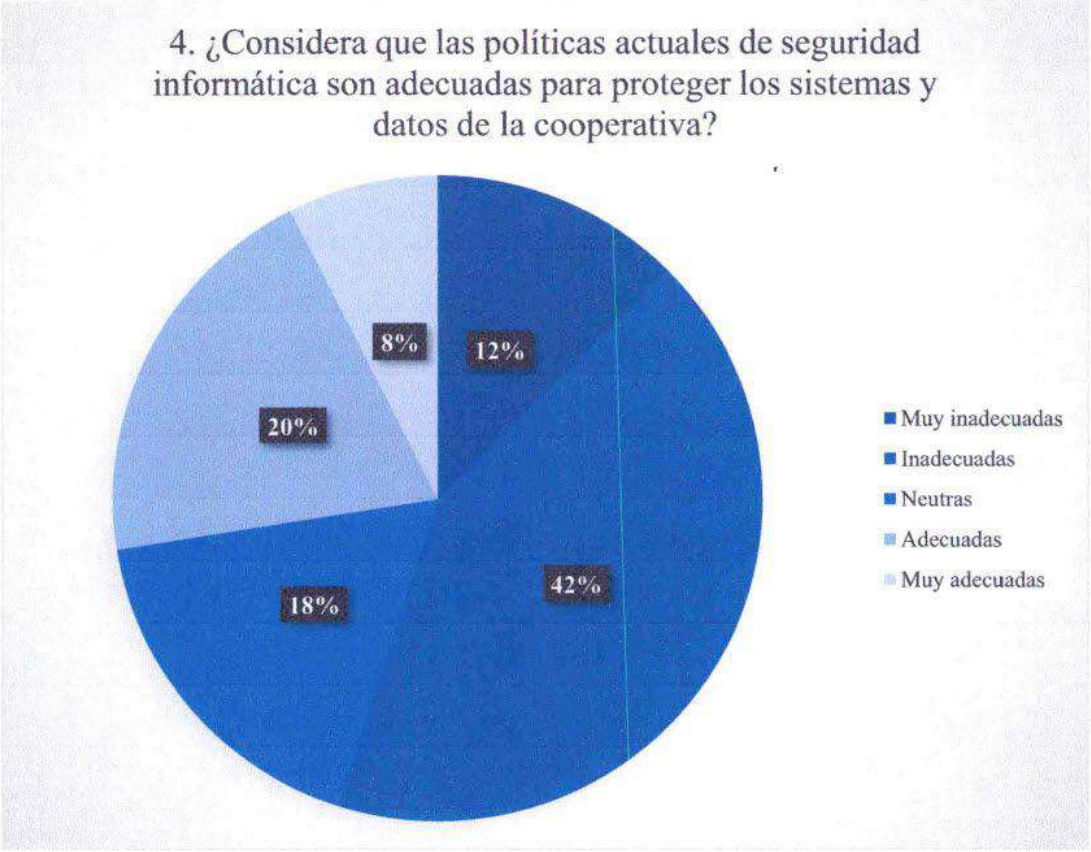



Nota: En la Figura 7, 15% de los encuestados indicó que nunca recibe capacitación, mientras que un 30% señaló que lo hace rara vez. Un 30% de los participantes mencionó que a veces reciben capacitación en ciberseguridad. Un 20% de los encuestados afirmó recibirla frecuentemente, y finalmente, un 5% indicó que siempre recibe capacitación en este ámbito. Estos resultados sugieren que la mayoría de los encuestados recibe capacitación en ciberseguridad de manera ocasional, con un grupo significativo que la recibe rara vez o a veces. Esto podría reflejar una necesidad de aumentar la frecuencia y regularidad de las capacitaciones

en ciberseguridad para asegurar que todos los colaboradores estén adecuadamente informados y preparados para enfrentar amenazas cibernéticas.

**Figura 8**

*Pregunta 4 - Encuesta*




Nota: En la Figura 8, 12% de los encuestados consideró que las políticas son muy inadecuadas, mientras que un 42% las calificó como inadecuadas. Un 18% de los participantes se mostró neutral respecto a la adecuación de las políticas. Un 20% de los encuestados opinó que las políticas son adecuadas, y finalmente, un 8% las consideró muy adecuadas. Estos resultados indican que una mayoría significativa de los encuestados percibe las políticas de seguridad informática como inadecuadas o muy inadecuadas, lo que sugiere una necesidad urgente de revisar

y mejorar estas políticas para asegurar una protección efectiva de los sistemas y datos de la cooperativa. La percepción neutral y positiva de una minoría de los encuestados también destaca la importancia de comunicar y educar sobre las políticas de seguridad para mejorar la confianza y el cumplimiento entre todos los colaboradores.

**Figura 9**

*Pregunta 5 - Encuesta*

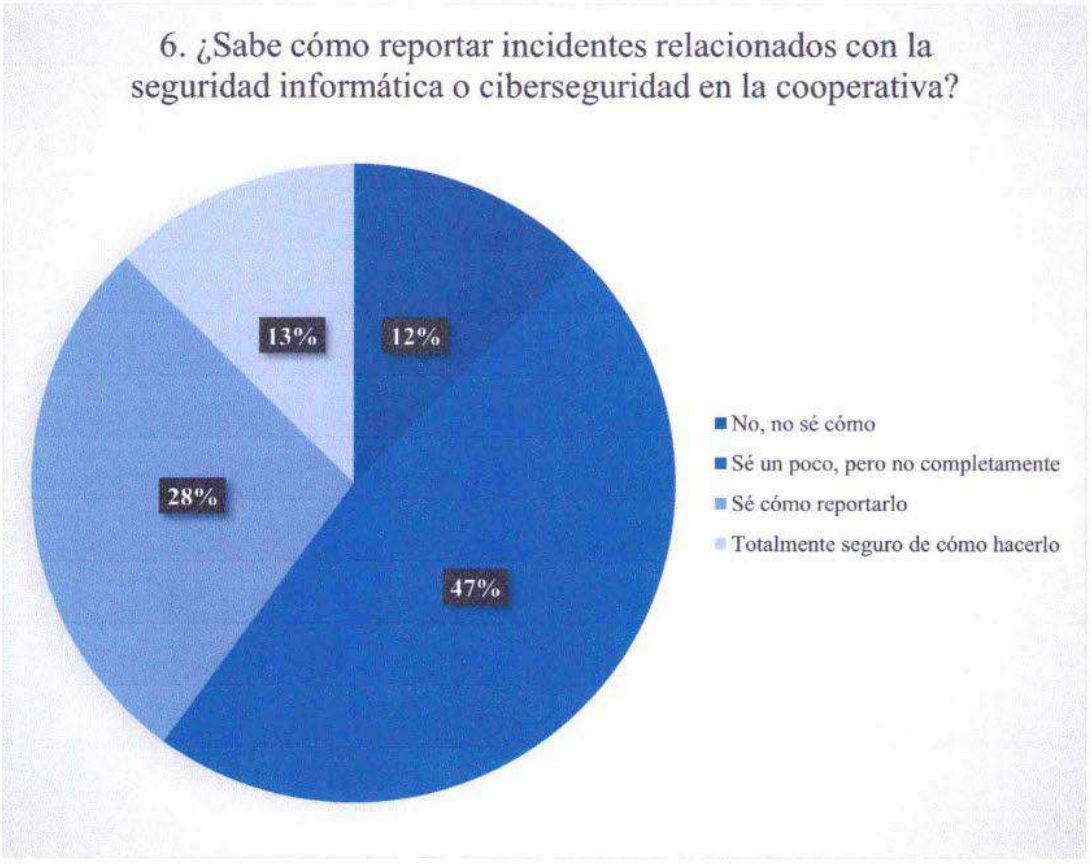



Nota: En la Figura 9, 15% de los encuestados indicó sentirse nada seguro, mientras que un 35% se siente poco seguro. Un 20% de los participantes mencionó sentirse medianamente seguro respecto a la protección de los datos. Un 27% de los encuestados afirmó sentirse muy seguro, y finalmente, un 3% indicó sentirse totalmente seguro. Estos resultados sugieren que una

mayoría significativa de los encuestados tiene dudas sobre la seguridad de los datos de los clientes, con un grupo considerable que se siente poco o medianamente seguro. Sin embargo, también hay un porcentaje notable que se siente muy seguro, lo que indica que hay áreas de fortaleza en las políticas de seguridad actuales. Estos hallazgos subrayan la importancia de seguir mejorando las medidas de seguridad y de comunicar eficazmente estas mejoras a todos los colaboradores para aumentar la confianza en la protección de los datos.

**Figura 10**

*Pregunta 6 - Encuesta*

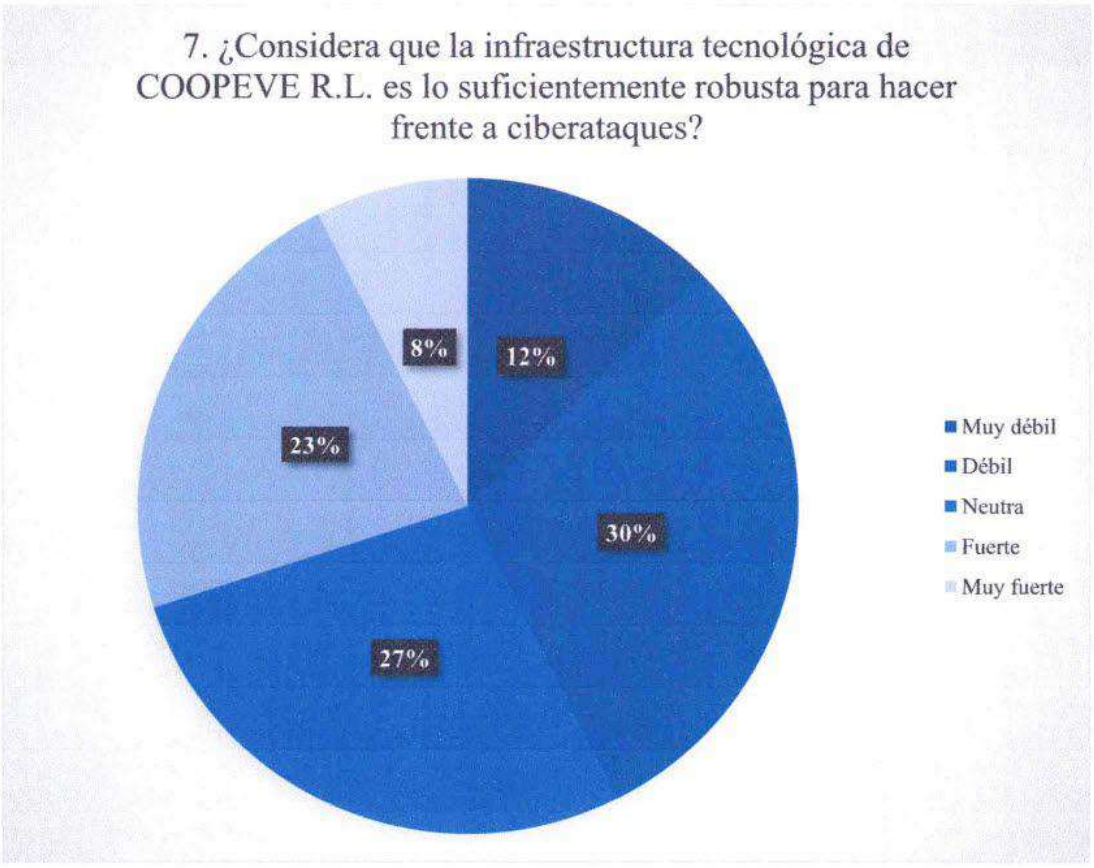



Nota: En la Figura 9, 12% de los encuestados indicó que no sabe cómo reportar estos incidentes, mientras que un 47% señaló que sabe un poco, pero no completamente. Un 28% de los participantes mencionó que sabe cómo reportarlo, y finalmente, un 13% indicó estar totalmente

seguro de cómo hacerlo. Estos resultados sugieren que, aunque una parte significativa de los colaboradores tiene algún conocimiento sobre el proceso de reporte de incidentes, hay una necesidad clara de mejorar la capacitación y la comunicación en este aspecto. Asegurar que todos los colaboradores estén completamente informados y seguros sobre cómo reportar incidentes es crucial para la eficacia del sistema de seguridad de la información de la cooperativa.

**Figura 11**

*Pregunta 7 - Encuesta*

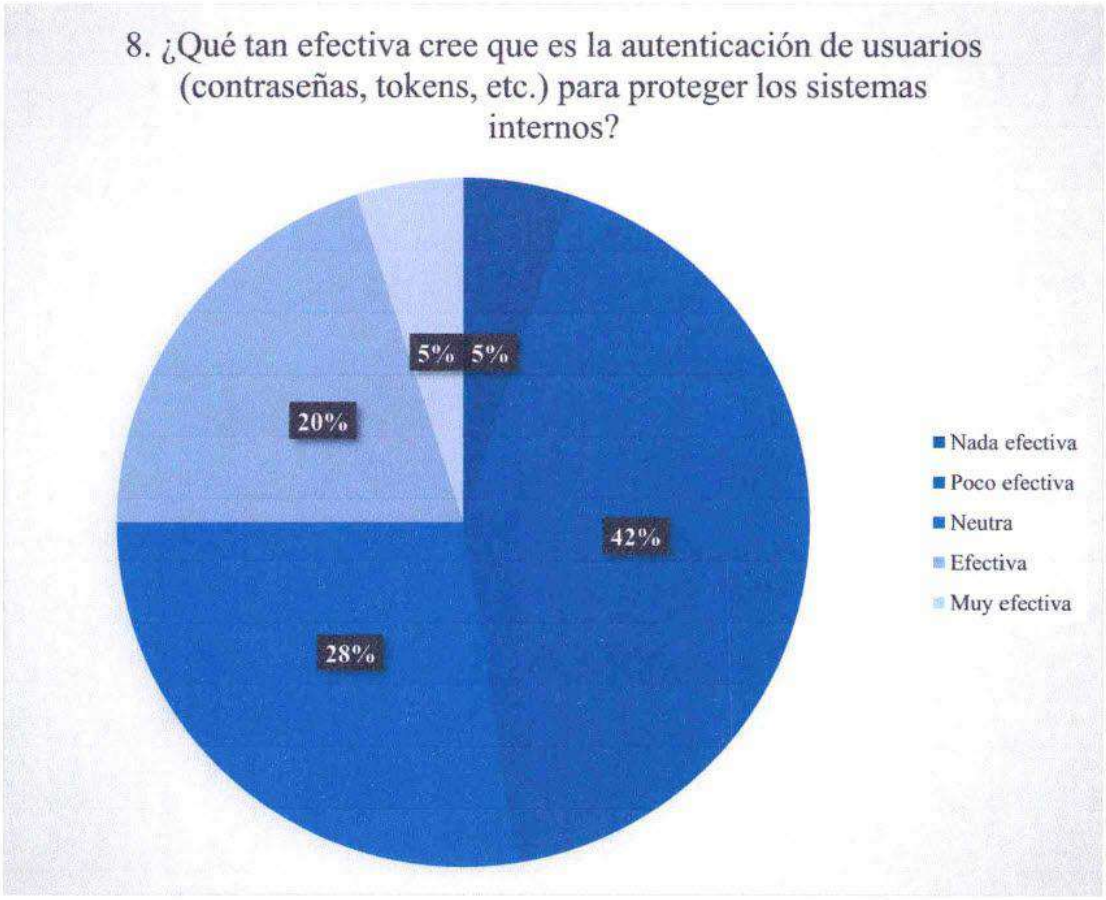



Nota: En la Figura 11, 12% de los encuestados consideró que la infraestructura es muy débil, mientras que un 30% la calificó como débil. Un 27% de los participantes se mostró neutral respecto a la robustez de la infraestructura. Un 23% de los encuestados opinó que

la infraestructura es fuerte, y finalmente, un 8% la consideró muy fuerte. Estos resultados indican que una mayoría significativa de los encuestados percibe la infraestructura tecnológica como débil o muy débil, lo que sugiere una necesidad urgente de fortalecer las medidas de seguridad y mejorar la infraestructura para hacer frente a posibles ciberataques. La percepción neutral y positiva de una minoría de los encuestados también destaca la importancia de comunicar y educar sobre las mejoras realizadas para aumentar la confianza en la robustez de la infraestructura tecnológica.

**Figura 12**

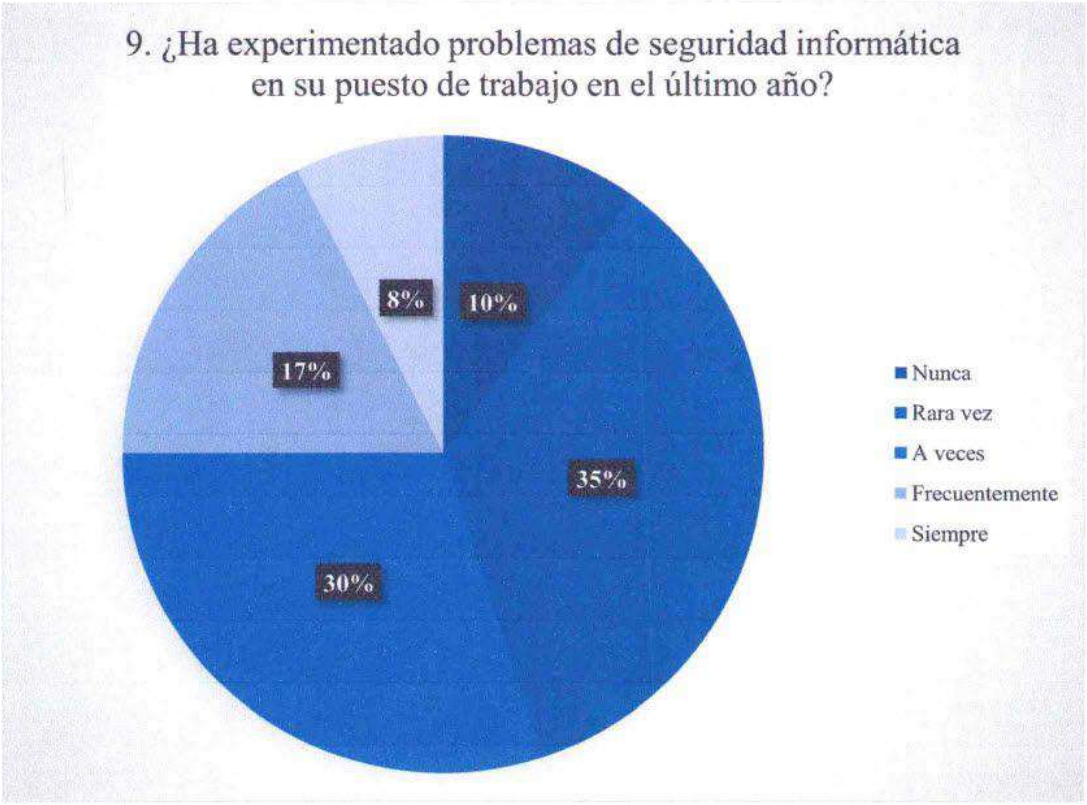
*Pregunta 8 - Encuesta*



Nota: En la Figura 12, 5% de los encuestados consideró que la autenticación es nada efectiva, mientras que un 42% la calificó como poco efectiva. Un 28% de los participantes se mostró neutral respecto a la efectividad de la autenticación. Un 20% de los encuestados opinó que la autenticación es efectiva, y finalmente, un 5% la consideró muy efectiva. Estos resultados indican que una mayoría significativa de los encuestados percibe la autenticación de usuarios como poco efectiva o neutral, lo que sugiere una necesidad de revisar y posiblemente mejorar los métodos de autenticación utilizados. La percepción positiva de una minoría de los encuestados también destaca la importancia de comunicar y educar sobre las medidas de autenticación para aumentar la confianza en su efectividad.

**Figura 13**

*Pregunta 9 - Encuesta*



Nota: En la Figura 13, 10% de los encuestados indicó que nunca ha tenido problemas de seguridad informática, mientras que un 35% señaló que los ha tenido rara vez. Un 30% de los participantes mencionó que a veces ha enfrentado problemas de seguridad. Un 17% de los encuestados afirmó que los ha tenido frecuentemente, y finalmente, un 8% indicó que siempre ha experimentado problemas de seguridad informática. Estos resultados sugieren que una mayoría significativa de los encuestados ha enfrentado problemas de seguridad informática al menos ocasionalmente, con un grupo considerable que los experimenta con frecuencia. Esto subraya la importancia de fortalecer las medidas de seguridad y proporcionar capacitación continua para reducir la incidencia de problemas de seguridad informática en el entorno laboral.

**Figura 14**

*Pregunta 10 - Encuesta*




Nota: En la Figura 13, 5% de los encuestados calificó la gestión como muy mala, mientras que un 35% la consideró mala. Un 27% de los participantes la calificó como regular. Un 23% de

los encuestados opinó que la gestión es buena, y finalmente, un 10% la consideró muy buena. Estos resultados indican que una mayoría significativa de los encuestados percibe la gestión de incidentes de seguridad informática como deficiente, lo que sugiere una necesidad urgente de mejorar los procesos y protocolos actuales. Sin embargo, también hay un grupo considerable que la califica como buena o muy buena, lo que destaca la importancia de identificar y replicar las prácticas efectivas para elevar el estándar general de la gestión de incidentes.

**Figura 15**

*Pregunta 11 - Encuesta*

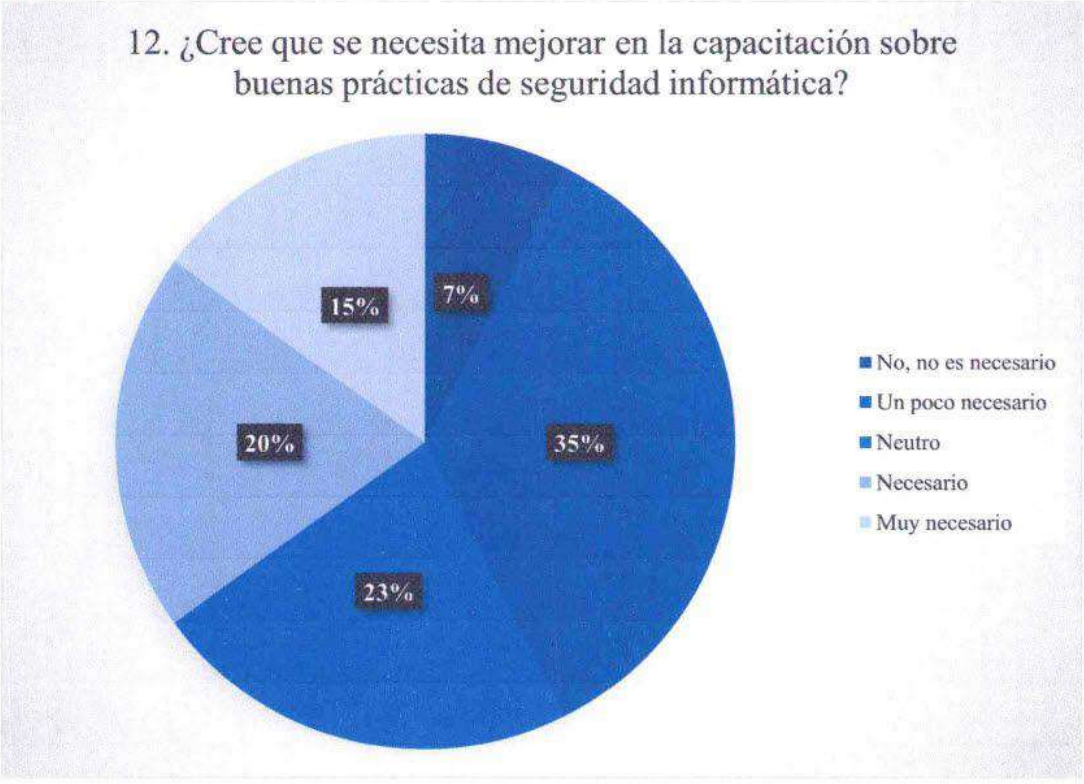



Nota: En la Figura 14, 10% de los encuestados consideró que los procedimientos son nada claros, mientras que un 32% los calificó como poco claros. Un 30% de los participantes se mostró medianamente claro respecto a los procedimientos. Un 15% de los encuestados opinó que

los procedimientos son muy claros, y finalmente, un 13% los consideró totalmente claros. Estos resultados indican que una mayoría significativa de los encuestados percibe los procedimientos como poco claros o medianamente claros, lo que sugiere una necesidad de mejorar la comunicación y la formación sobre estos procedimientos. La percepción positiva de una minoría de los encuestados también destaca la importancia de identificar y replicar las prácticas efectivas para aumentar la claridad y comprensión de los procedimientos entre todos los empleados.

**Figura 16**

*Pregunta 12 - Encuesta*

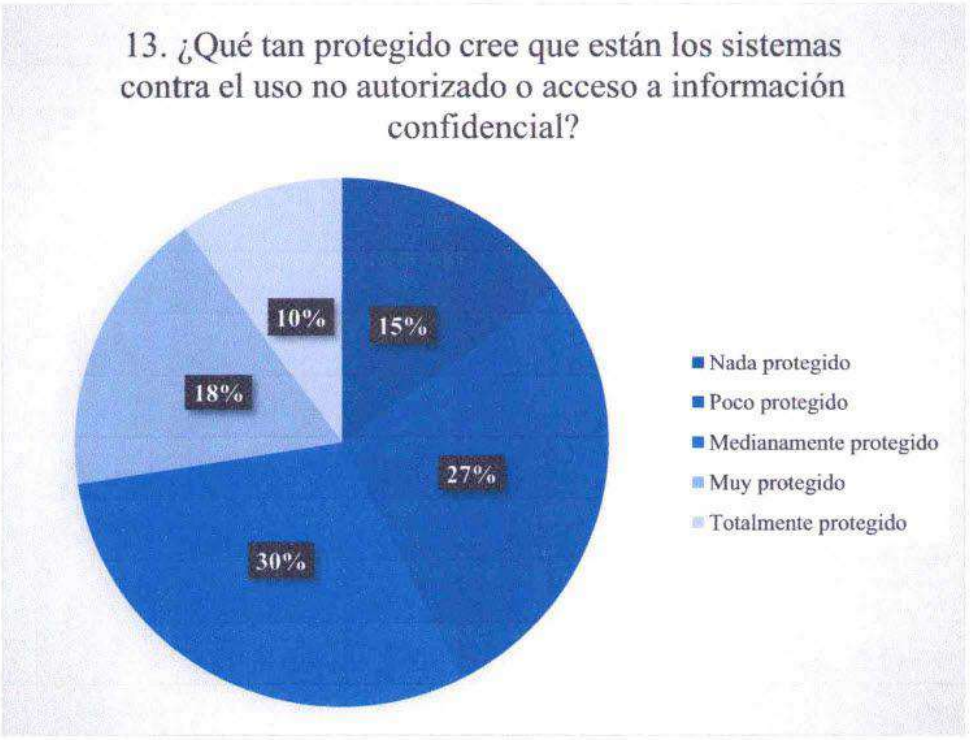



Nota: En la Figura 15, 7% de los encuestados consideró que no es necesario mejorar la capacitación, mientras que un 35% opinó que es un poco necesario. Un 23% de los participantes se mostró neutro respecto a esta necesidad. Un 20% de los encuestados indicó que

es necesario mejorar la capacitación, y finalmente, un 15% consideró que es muy necesario. Estos resultados sugieren que una mayoría significativa de los encuestados percibe al menos alguna necesidad de mejorar la capacitación en seguridad informática, con un grupo considerable que la considera necesaria o muy necesaria. Esto subraya la importancia de invertir en programas de capacitación continua para asegurar que todos los empleados estén bien informados y preparados para enfrentar amenazas de seguridad informática.

**Figura 17**

*Pregunta 13 - Respuesta*

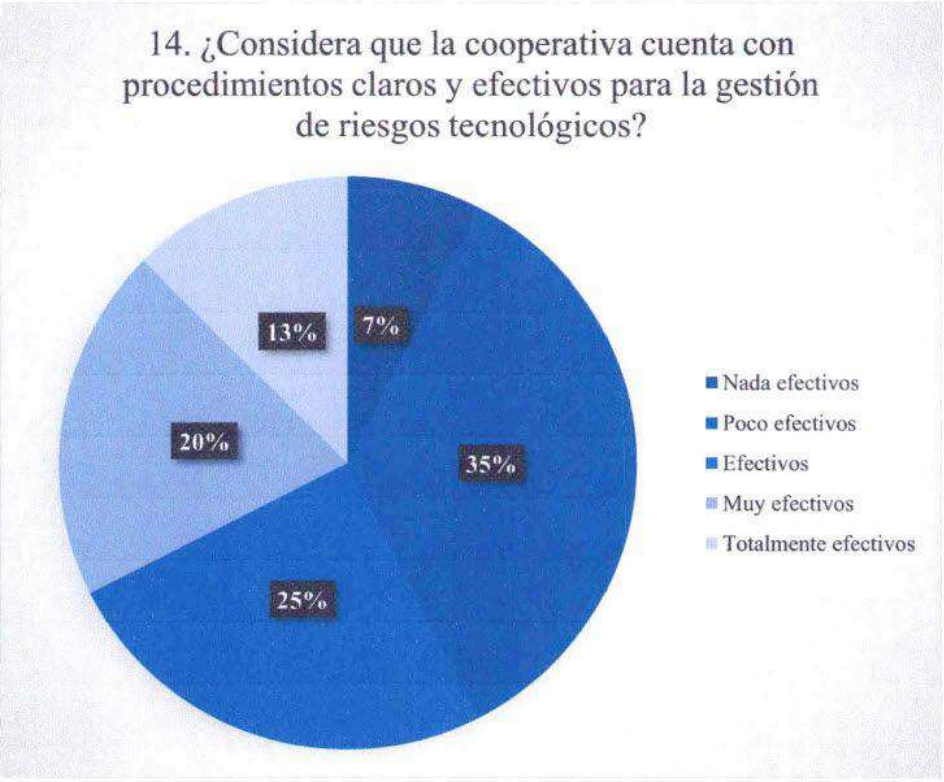



Nota: En la Figura 16, 15% de los encuestados consideró que los sistemas están nada protegidos, mientras que un 27% los calificó como poco protegidos. Un 30% de los participantes se mostró medianamente protegido respecto a la protección de los sistemas. Un 18% de los encuestados opinó que los sistemas están muy protegidos, y finalmente, un 10% los

consideró totalmente protegidos. Estos resultados indican que una mayoría significativa de los encuestados percibe los sistemas como medianamente protegidos o menos, lo que sugiere una necesidad de mejorar las medidas de seguridad para proteger la información confidencial. La percepción positiva de una minoría de los encuestados también destaca la importancia de comunicar y educar sobre las medidas de seguridad implementadas para aumentar la confianza en la protección de los sistemas.

**Figura 18**

*Pregunta 14 - Encuesta*

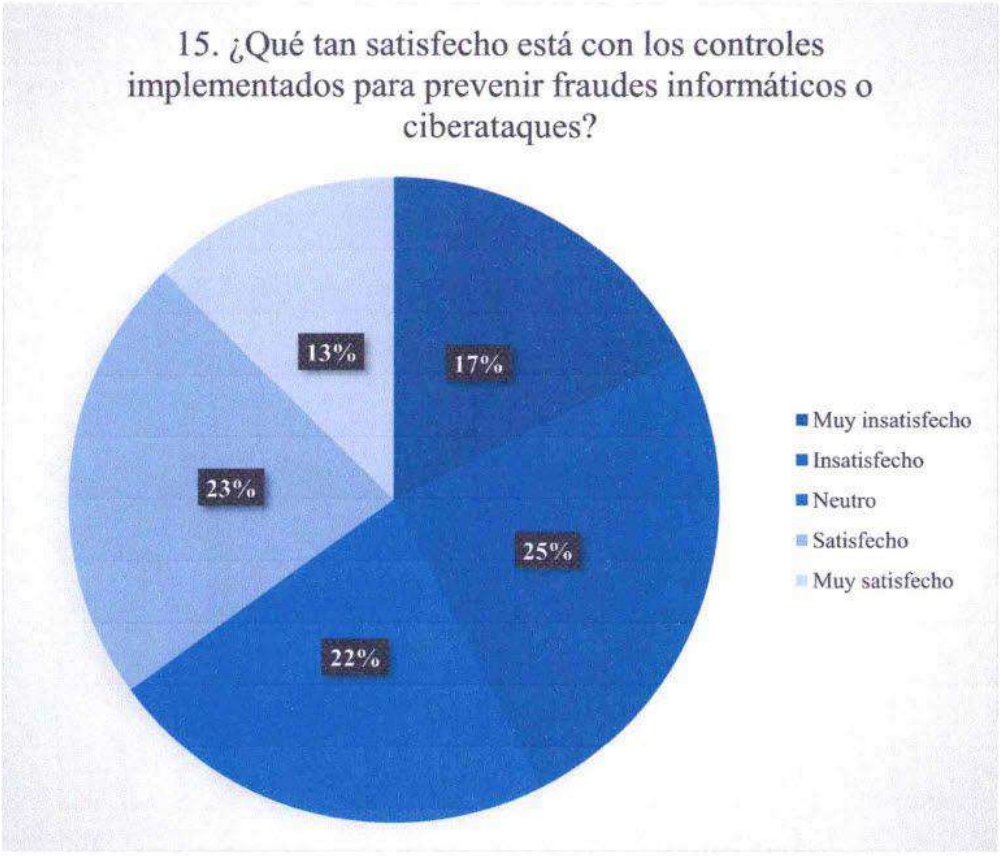



Nota: En la Figura 17, 7% de los encuestados consideró que los procedimientos son nada efectivos, mientras que un 35% los calificó como poco efectivos. Un 25% de los participantes opinó que los procedimientos son efectivos. Un 20% de los encuestados los consideró muy

efectivos, y finalmente, un 13% los calificó como totalmente efectivos. Estos resultados indican que una mayoría significativa de los encuestados percibe los procedimientos de gestión de riesgos tecnológicos como poco efectivos o menos, lo que sugiere una necesidad de mejorar y clarificar estos procedimientos. Sin embargo, también hay un grupo considerable que los considera efectivos o muy efectivos, lo que destaca la importancia de identificar y replicar las prácticas efectivas para elevar el estándar general de la gestión de riesgos tecnológicos en la cooperativa.

**Figura 19**

*Pregunta 15 - Encuesta*




Nota: En la Figura 18, 17% de los encuestados se declaró muy insatisfecho, mientras que un 25% se mostró insatisfecho. Un 22% de los participantes se mostró neutral respecto a los

controles. Un 23% de los encuestados indicó estar satisfecho, y finalmente, un 13% se declaró muy satisfecho. Estos resultados sugieren que una mayoría significativa de los encuestados tiene una percepción negativa o neutral sobre la efectividad de los controles actuales, lo que indica una necesidad de revisar y mejorar estas medidas. Sin embargo, también hay un grupo considerable que se siente satisfecho o muy satisfecho, lo que destaca la importancia de identificar y replicar las prácticas efectivas para aumentar la satisfacción general con los controles de seguridad implementados.

**Figura 20**

*Pregunta 16 - Encuesta*



Nota: En la Figura 19, 7% de los encuestados consideró que la implementación no mejoraría la seguridad, mientras que un 40% opinó que la mejora sería poca. Un 23% de los participantes indicó que la mejora sería medianamente significativa. Un 25% de los encuestados consideró que la implementación mejoraría la seguridad mucho, y finalmente, un 5% opinó que la mejora sería total. Estos resultados sugieren que, aunque una parte significativa de los encuestados tiene dudas sobre la efectividad de la implementación del SGSI, hay un grupo considerable que cree en su potencial para mejorar significativamente la seguridad. Esto subraya la importancia de comunicar claramente los beneficios y el impacto positivo de la implementación del SGSI para aumentar la confianza y el apoyo entre los empleados.

De los datos analizados, se puede inferir que hay una percepción general de insuficiencia en las medidas de seguridad actuales en COOPEVE R.L. Los empleados sienten que la infraestructura tecnológica y los procedimientos de seguridad necesitan mejoras significativas. La capacitación en ciberseguridad y la claridad de los procedimientos son áreas críticas que requieren atención para aumentar la confianza y la efectividad de las medidas de seguridad.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 es vista como una posible solución para mejorar la seguridad, aunque hay escepticismo sobre su impacto total. Es crucial comunicar claramente los beneficios y realizar mejoras visibles en las áreas identificadas para aumentar la confianza y el apoyo de los empleados hacia las medidas de seguridad implementadas.

#### 4.4.1.7 Analisis y Evaluación del Riesgo

El análisis y evaluación del riesgo es un proceso fundamental en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022. Este proceso permite identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información, asegurando que los activos de información estén protegidos contra amenazas potenciales. A continuación, se detalla este proceso en varias etapas clave, utilizando cuadros para una mejor comprensión.

#### 4.4.1.8 Identificación de Activos y Amenazas

El primer paso en el análisis de riesgos es la identificación de los activos de información críticos y las amenazas que podrían afectarlos. En COOPEVE, R.L., estos activos incluyen el sistema contable, las cajas, la atención al cliente, el servicio de ATM, la seguridad perimetral, el sistema de cortafuego y el centro de datos.

***Tabla 23***

*Descripción de activos en base a su operación en el negocio*

| Activo | Descripción |
|---|---|
| Sistema Contable | Software y bases de datos que gestionan las finanzas de la cooperativa. |
| Cajas | Puntos de transacción donde se maneja efectivo y se realizan operaciones financieras. |
| Atención al Cliente | Sistemas y procesos que gestionan la interacción con los socios y clientes. |

| | |
|---|---|
| Servicio de ATM | Cajeros automáticos que permiten transacciones fuera del horario de oficina. |
| Seguridad Perimetral | Medidas que protegen las instalaciones físicas de la cooperativa. |
| Sistema de Cortafuego | Sistema que protege la red informática de accesos no autorizados. |
| Centro de Datos | Servidores y equipos críticos para las operaciones de la cooperativa. |

Nota: En la Tabla 21 se describe el funcionamiento que tiene en el negocio. La identificación y descripción de los activos de información es esencial para la implementación del SGSI en COOPEVE, R.L. Cada activo, desde el sistema contable hasta el centro de datos, juega un papel crucial en las operaciones diarias de la cooperativa. La protección de estos activos contra amenazas potenciales es vital para asegurar la continuidad operativa y la confianza de los socios. Implementar medidas de seguridad adecuadas y mantener una gestión efectiva de estos activos garantiza que la información crítica esté protegida, contribuyendo a la estabilidad y eficiencia de la cooperativa.

**Tabla 24**

*Identificación de amenazas y vulnerabilidades*

| Activo | Amenaza | Vulnerabilidad |
|---|---|---|
| Sistema Contable | Acceso no autorizado | Contraseñas débiles |
| Cajas | Robo de efectivo | Seguridad física insuficiente |
| Atención al Cliente | Fuga de información | Falta de capacitación |
| Servicio de ATM | Fraude en transacciones | Software desactualizado |
| Seguridad Perimetral | Intrusión física | Medidas de seguridad insuficientes |
| Sistema de Cortafuego | Acceso no autorizado | Configuraciones incorrectas |
| Centro de Datos | Fallos en el suministro eléctrico | Falta de redundancia |

Nota: En la Tabla 24, se identifican para cada activo las amenazas potenciales y las vulnerabilidades asociadas. La importancia de abordar tanto las amenazas como las vulnerabilidades para proteger adecuadamente los activos de información de COOPEVE, R.L. e implementar controles de seguridad específicos es esencial para mantener la integridad, confidencialidad y disponibilidad de la información crítica de la cooperativa.

**Tabla 25**

*Evaluación del Impacto y Probabilidad*

| Activo | Impacto | Probabilidad | Riesgo |
|---|---|---|---|
| Sistema Contable | 5 | 4 | 20 |
| Cajas | 4 | 3 | 12 |
| Atención al Cliente | 3 | 4 | 12 |
| Servicio de ATM | 5 | 3 | 15 |
| Seguridad Perimetral | 4 | 3 | 12 |
| Sistema de Cortafuego | 5 | 3 | 15 |
| Centro de Datos | 5 | 3 | 15 |

Nota: En la Tabla 23, se describe la evaluación del impacto y la probabilidad de riesgos para los activos de información de COOPEVE, R.L. La valoración del riesgo se calcula multiplicando el impacto por la probabilidad, lo que permite priorizar las acciones de mitigación necesarias para proteger estos activos críticos.

Este análisis debe considerar tanto los impactos positivos como los negativos, y debe involucrar a todas las partes interesadas para asegurar una comprensión completa de las posibles consecuencias. Cada impacto identificado debe ser clasificado según su severidad y probabilidad de ocurrencia, lo que permite priorizar las acciones de mitigación necesarias.

La identificación del impacto no es un proceso estático; debe ser dinámico y continuo, adaptándose a los cambios en el entorno de la información y las operaciones de la cooperativa. Esto asegura que el SGSI permanezca efectivo y alineado con los objetivos estratégicos de la organización. Documentar los impactos identificados y las medidas de mitigación propuestas es esencial para la transparencia y la rendición de cuentas, facilitando la toma de decisiones informadas y la mejora continua del SGSI.

La identificación del impacto proporciona una base sólida para la gestión de riesgos en COOPEVE, R.L., asegurando que todos los activos de información estén protegidos adecuadamente y que la organización pueda responder eficazmente a cualquier incidente de seguridad.

#### 4.4.1.9 Selección de Controles

De acuerdo con López (2023), la versión más reciente de la norma ISO 27001 fue lanzada el 25 de octubre de 2022, siendo la primera actualización desde 2013. Aunque las modificaciones no son radicales, es crucial revisar los cambios, especialmente si tu empresa ya cuenta con la certificación, ya que deberá recertificarse en un plazo máximo de tres años.

**Tabla 26**

*Controles de nueva versión ISO 27001:2022*




Nota: En la Figura 20, se muestran los controles actualizados en la última versión de la ISO 27001:2022. (López, 2023, p. 1)

La selección de controles es una etapa crucial en la gestión de riesgos del SGSI de COOPEVE, R.L. A continuación, se presentan los controles recomendados para mitigar los riesgos identificados en los activos de información:

**Tabla 27**

*Establecimiento del control según el activo*

| Activo | Control |
|---|---|
| Sistema Contable | Implementar autenticación multifactor para fortalecer la seguridad de acceso. |
| Cajas | Mejorar la seguridad física mediante la instalación de cámaras de vigilancia y sistemas de alarma. |
| Atención al Cliente | Realizar capacitaciones regulares en seguridad de la información para el personal. |
| Servicio de ATM | Actualizar el software de los cajeros automáticos regularmente para proteger contra fraudes. |
| Seguridad Perimetral | Implementar medidas adicionales de seguridad física, como cercas y controles de acceso. |
| Sistema de Cortafuego | Revisar y actualizar las configuraciones del cortafuego para asegurar una protección óptima. |
| Centro de Datos | Implementar sistemas de respaldo y redundancia para asegurar la disponibilidad continua de los servicios. |

Nota: En la Tabla 24, los controles que están diseñados para reducir los riesgos a niveles aceptables, asegurando la protección de la confidencialidad, integridad y disponibilidad de los

activos de información de COOPEVE, R.L. La implementación efectiva de estos controles es esencial para mantener la seguridad y la continuidad operativa de la cooperativa.

### *4.4.2 Fase Hacer / Do*

En la fase "Hacer" del ciclo PDCA (Plan-Do-Check-Act), se implementan las políticas, controles, procesos y procedimientos definidos en la fase de planificación. Esto incluye la capacitación del personal, la implementación de controles técnicos y administrativos, y la gestión de la seguridad de la información en el día a día.

#### 4.4.2.1 Aplicar el SGSI

La aplicación del Sistema de Gestión de Seguridad de la Información (SGSI) implica la implementación de todas las políticas, procedimientos y controles definidos en las fases de planificación. Esto incluye la asignación de responsabilidades, la comunicación de políticas a todos los empleados y la integración de las prácticas de seguridad en las operaciones diarias de la organización.

La estructura de la organización debe apoyar la implementación del SGSI. Esto incluye definir roles y responsabilidades claras para la gestión de la seguridad de la información, establecer comités o equipos de seguridad, y asegurar que haya una comunicación efectiva entre todas las partes involucradas.

Todas las organizaciones poseen información o datos que son críticos o sensibles. La información es considerada ampliamente como el elemento vital de las empresas modernas. Amenaza persistente avanzada (APT) es la descripción que se aplica a las actividades cibernéticas de delincuentes sofisticados y entidades a nivel estatal, dirigidas a grandes corporaciones y

gobiernos extranjeros, con el objetivo de robar información o comprometer los sistemas de información. Los ataques cibernéticos son, inicialmente, automatizados e indiscriminados: cualquier organización con presencia en Internet será escaneada y potencialmente atacada. (Calder & Watkins, 2002, p. 9)

"No es sorprendente que la Encuesta sobre el estado mundial de la seguridad de la información de 2015 de PricewaterhouseCoopers (PwC) dijera que "la mayoría de las organizaciones se dan cuenta de que la ciberseguridad se ha convertido en un riesgo empresarial persistente y global"."(Calder & Watkins, 2002, p. 9)

#### 4.4.2.2 Plan de tratamiento de riesgos

Después de analizar y cuantificar los riesgos y su impacto en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), es esencial seleccionar y aplicar las medidas más adecuadas para modificar estos riesgos. El objetivo es prevenir los daños inherentes a los factores de riesgo o, en su defecto, aprovechar las oportunidades que puedan surgir. Es crucial evaluar el nivel de oportunidad en caso de optar por asumir el riesgo.

Se deben identificar los riesgos que pueden afectar a la cooperativa. Esto incluye riesgos tecnológicos, físicos, humanos y de procesos. Ejemplos de riesgos pueden ser el acceso no autorizado a sistemas, pérdida de datos, ataques de programa maligno, entre otros. Cada riesgo identificado debe ser evaluado en términos de su probabilidad de ocurrencia y el impacto potencial en la cooperativa. Esto se puede hacer utilizando una matriz de riesgos que clasifique los riesgos en categorías como bajo, medio y alto.

#### 4.4.2.3 Selección de Controles

Para cada riesgo evaluado, se deben seleccionar controles específicos que ayuden a mitigar o eliminar el riesgo. Los controles pueden ser de naturaleza técnica, física o administrativa. A continuación, se presentan algunos ejemplos de controles para riesgos específicos:

**Tabla 28**

*Plan de implementación de controles*

| Riesgo | Control | Responsable | Plazo | Recursos Necesarios |
|---|---|---|---|---|
| Acceso no autorizado a sistemas | Implementar autenticación multifactor | Equipo de TI | 3 meses | Software de autenticación, personal de TI |
| Pérdida de datos | Realizar copias de seguridad diarias | Administrador de sistemas | Inmediato y continuo | Servidores de respaldo, software de backup |
| Ataques de malware | Actualizar software antivirus y realizar escaneos regulares | Equipo de TI | 1 mes y continuo | Software antivirus, personal de TI |
| Robo de información | Controlar acceso físico a áreas sensibles | Seguridad física | 2 meses | Sistemas de control de acceso, cámaras de vigilancia |

| | | | | |
|---|---|---|---|---|
| Pérdida o robo de dispositivos móviles | Cifrar dispositivos móviles y establecer políticas de uso seguro | Equipo de TI | 1 mes | Software de cifrado, políticas de seguridad |

Nota: En la Tabla 25, se presenta esquema organizado para la implementación de controles.

#### 4.4.2.4 Capacitación y Concientización

Es fundamental que todos los empleados comprendan sus roles y responsabilidades en la protección de la información. Esto incluye:

Programas de Capacitación: Sesiones regulares de formación sobre políticas de seguridad, procedimientos y mejores prácticas.

Campañas de Concientización: Iniciativas para mantener la seguridad de la información en la mente de los empleados.

Evaluaciones de Conocimiento: Pruebas y evaluaciones para medir la comprensión y cumplimiento de las políticas de seguridad.

Simulacros y Ejercicios: Realización de simulacros de incidentes de seguridad para preparar a los empleados para responder adecuadamente en caso de una brecha de seguridad real.

Es crucial monitorear y revisar continuamente el plan de tratamiento de riesgos para asegurar su efectividad. Esto incluye:

Auditorías Internas: Realizar auditorías periódicas para evaluar la efectividad de los controles implementados.

Revisión de Riesgos: Revisar y actualizar la evaluación de riesgos regularmente para reflejar cambios en el entorno de la cooperativa.

Mejora Continua: Implementar mejoras basadas en los resultados de las auditorías y revisiones.

### *4.4.3 Fase Controlar*

#### 4.4.3.1 Revisar el SGSI

La revisión del Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso continuo que asegura que el sistema se mantenga efectivo y alineado con los objetivos de la organización. Esta revisión incluye:

Evaluación de Desempeño: Analizar el desempeño del SGSI en función de los objetivos y métricas establecidos. Esto puede incluir la revisión de incidentes de seguridad, resultados de auditorías y retroalimentación de los empleados.

Revisión de Políticas y Procedimientos: Asegurarse de que las políticas y procedimientos de seguridad estén actualizados y reflejen las mejores prácticas y cambios en el entorno de la organización.

Reuniones de Revisión por la Dirección: Realizar reuniones periódicas con la alta dirección para revisar el estado del SGSI, discutir problemas y oportunidades de mejora, y tomar decisiones estratégicas.

#### 4.4.3.2 Medir la Eficacia de los Controles

Medir la eficacia de los controles implementados es crucial para asegurar que están funcionando como se espera. Esto incluye:

Indicadores de Rendimiento: Definir y monitorear indicadores clave de rendimiento (KPI) que reflejen la efectividad de los controles. Ejemplos de KPI pueden incluir el número de incidentes de seguridad, el tiempo de respuesta a incidentes, y la tasa de cumplimiento de políticas.

Pruebas de Controles: Realizar pruebas periódicas de los controles de seguridad para asegurar que están operando correctamente. Esto puede incluir pruebas de penetración, simulaciones de ataques y revisiones de configuración.

Análisis de Incidentes: Analizar los incidentes de seguridad para identificar fallos en los controles y áreas de mejora. Esto ayuda a ajustar y fortalecer los controles existentes.

#### 4.4.3.3 Revisar los Riesgos Residuales

Los riesgos residuales son aquellos que permanecen después de que se han implementado los controles de seguridad. Revisar estos riesgos es esencial para asegurar que se mantengan dentro de los niveles aceptables definidos por la organización. Esto incluye:

Evaluación Continua de Riesgos: Realizar evaluaciones periódicas de riesgos para identificar nuevos riesgos y reevaluar los riesgos existentes. Esto asegura que los riesgos residuales se gestionen adecuadamente.

Ajuste de Controles: Modificar o añadir controles según sea necesario para mitigar los riesgos residuales. Esto puede incluir la implementación de controles adicionales o la mejora de los controles existentes.

Documentación de Riesgos: Mantener una documentación actualizada de los riesgos residuales y las medidas tomadas para gestionarlos. Esto proporciona una base para futuras revisiones y auditorías.

#### 4.4.3.4 Realizar Auditorías Internas del SGSI

Las auditorías internas son una herramienta clave para evaluar la conformidad y efectividad del SGSI. Estas auditorías deben ser realizadas de manera regular y sistemática. Esto incluye:

Planificación de Auditorías: Desarrollar un plan de auditoría que defina el alcance, los objetivos y el calendario de las auditorías internas. El plan debe asegurar que todas las áreas críticas del SGSI sean auditadas.

Ejecución de Auditorías: Realizar auditorías internas siguiendo procedimientos establecidos. Esto incluye la revisión de documentos, entrevistas con el personal y pruebas de controles.

Informe de Resultados: Documentar los hallazgos de la auditoría y proporcionar recomendaciones para la mejora. Los informes deben ser claros y detallados, destacando las áreas de no conformidad y las oportunidades de mejora.

Seguimiento de Acciones Correctivas: Asegurar que se tomen acciones correctivas para abordar los hallazgos de la auditoría. Esto incluye la asignación de responsabilidades y la verificación de la implementación de las acciones correctivas.

#### 4.4.3.5 Registrar Eventos y Acciones

El registro de eventos y acciones es fundamental para mantener un historial de las actividades de seguridad y las respuestas a incidentes. Esto incluye:

Registro de Incidentes: Documentar todos los incidentes de seguridad, incluyendo la naturaleza del incidente, las acciones tomadas y los resultados. Esto ayuda a identificar patrones y tendencias en los incidentes de seguridad.

Registro de Acciones Correctivas y Preventivas: Documentar las acciones correctivas y preventivas tomadas para abordar los incidentes y las no conformidades. Esto asegura que se mantenga un historial de las mejoras realizadas.

Mantenimiento de Registros de Auditoría: Mantener registros detallados de las auditorías internas, incluyendo los planes de auditoría, los hallazgos y las acciones correctivas. Esto proporciona una base para futuras auditorías y revisiones.

Implementar estos procesos de manera efectiva ayudará a asegurar que el SGSI de COOPEVE, R.L. se mantenga robusto y alineado con los objetivos de seguridad de la información de la organización.

### *4.4.4 Fase Actuar*

#### 4.4.4.1 Implementar Mejoras al SGSI

La implementación de mejoras al Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso continuo que busca optimizar la seguridad de la información en la organización. Este proceso incluye:

Identificación de Oportunidades de Mejora: Basado en los resultados de auditorías, revisiones de desempeño, análisis de incidentes y retroalimentación de los empleados, identificar áreas donde el SGSI puede ser mejorado.

Desarrollo de Planes de Mejora: Crear planes detallados para implementar las mejoras identificadas. Estos planes deben incluir objetivos claros, acciones específicas, responsables, plazos y recursos necesarios.

Implementación de Mejoras: Ejecutar los planes de mejora, asegurando que se asignen los recursos necesarios y que las acciones se realicen de manera efectiva. Esto puede incluir la

actualización de políticas, la implementación de nuevas tecnologías, la mejora de procesos y la capacitación adicional del personal.

Monitoreo y Evaluación: Supervisar la implementación de las mejoras para asegurar que se logren los objetivos establecidos. Evaluar el impacto de las mejoras en la seguridad de la información y realizar ajustes según sea necesario.

#### 4.4.4.2 Aplicar Acciones Correctivas

Las acciones correctivas son medidas tomadas para eliminar las causas de no conformidades o incidentes de seguridad y prevenir su recurrencia. Este proceso incluye:

Identificación de No Conformidades: Detectar y documentar no conformidades a través de auditorías, revisiones de desempeño y análisis de incidentes.

Análisis de Causas: Realizar un análisis de causas raíz para identificar las razones subyacentes de las no conformidades. Esto puede incluir técnicas como el análisis de los "5 porqués" o el diagrama de Ishikawa.

Desarrollo de Acciones Correctivas: Crear planes de acción para abordar las causas raíz identificadas. Estos planes deben incluir acciones específicas, responsables, plazos y recursos necesarios.

Implementación de Acciones Correctivas: Ejecutar las acciones correctivas, asegurando que se asignen los recursos necesarios y que las acciones se realicen de manera efectiva.

Verificación de Eficacia: Evaluar la efectividad de las acciones correctivas implementadas para asegurar que las no conformidades no se repitan. Esto puede incluir la realización de auditorías de seguimiento y la revisión de indicadores de desempeño.

#### 4.4.4.3 Aplicar Acciones Preventivas

Las acciones preventivas son medidas tomadas para eliminar las causas de posibles no conformidades o incidentes de seguridad y prevenir su ocurrencia. Este proceso incluye:

Identificación de Riesgos Potenciales: Utilizar la evaluación de riesgos y el análisis de tendencias para identificar posibles no conformidades o incidentes de seguridad antes de que ocurran.

Análisis de Causas Potenciales: Realizar un análisis de causas potenciales para identificar las razones subyacentes de los riesgos identificados.

Desarrollo de Acciones Preventivas: Crear planes de acción para abordar las causas potenciales identificadas. Estos planes deben incluir acciones específicas, responsables, plazos y recursos necesarios.

Implementación de Acciones Preventivas: Ejecutar las acciones preventivas, asegurando que se asignen los recursos necesarios y que las acciones se realicen de manera efectiva.

Verificación de Eficacia: Evaluar la efectividad de las acciones preventivas implementadas para asegurar que los riesgos potenciales no se materialicen. Esto puede incluir la realización de auditorías de seguimiento y la revisión de indicadores de desempeño.

#### 4.4.4.4 Comprobar la Eficacia de las Acciones

Comprobar la eficacia de las acciones correctivas y preventivas es crucial para asegurar que las medidas tomadas han sido efectivas en abordar las no conformidades y prevenir su recurrencia. Este proceso incluye:

Monitoreo Continuo: Supervisar continuamente los indicadores de desempeño y los resultados de las auditorías para evaluar la efectividad de las acciones implementadas.

Revisión de Resultados: Analizar los resultados de las auditorías, revisiones de desempeño y análisis de incidentes para determinar si las acciones correctivas y preventivas han sido efectivas.

Retroalimentación y Ajustes: Utilizar la retroalimentación obtenida del monitoreo y la revisión de resultados para realizar ajustes a las acciones implementadas. Esto puede incluir la modificación de políticas, la mejora de procesos y la capacitación adicional del personal.

Documentación y Reporte: Mantener una documentación detallada de las acciones correctivas y preventivas implementadas, así como de su efectividad. Reportar los resultados a la alta dirección y a las partes interesadas relevantes.

Implementar estos procesos de manera efectiva ayudará a asegurar que el SGSI de COOPEVE, R.L. se mantenga robusto y alineado con los objetivos de seguridad de la información de la organización.

### *4.4.5 Políticas, Estándares y Procedimientos*

#### 4.4.5.1 Diseño de Políticas

El diseño de políticas es fundamental para establecer las directrices y expectativas en materia de seguridad de la información dentro de la organización. Las políticas deben ser claras, concisas y alineadas con los objetivos estratégicos de la organización.

Identificación de Necesidades:

Evaluar los riesgos y requerimientos específicos de la organización.

Consultar con las partes interesadas para identificar áreas críticas.

Desarrollo de Políticas:

Redactar políticas que aborden los aspectos clave de la seguridad de la información, como el control de acceso, la protección de datos y la gestión de incidentes.

Asegurar que las políticas sean comprensibles y accesibles para todos los empleados.

Revisión y Aprobación:

Someter las políticas a revisión por parte de la alta dirección y la junta directiva.

Realizar ajustes basados en el feedback recibido y obtener la aprobación final.

Comunicación y Capacitación:

Difundir las políticas a todos los empleados y proporcionar capacitación para asegurar su comprensión y cumplimiento.

Establecer canales de comunicación para resolver dudas y recibir retroalimentación.

Diseño de Estándares

Los estándares proporcionan un marco detallado para implementar las políticas de seguridad de la información. Definen los requisitos técnicos y operativos que deben cumplirse.

Definición de Requisitos:

Identificar los requisitos técnicos y operativos necesarios para cumplir con las políticas de seguridad.

Consultar con expertos técnicos y partes interesadas para asegurar la viabilidad de los estándares.

Desarrollo de Estándares:

Redactar estándares que especifiquen los controles técnicos, procedimientos y prácticas recomendadas.

Asegurar que los estándares sean detallados y específicos para cada área de la organización.

Revisión y Aprobación:

Someter los estándares a revisión por parte de la gerencia de tecnología y otros departamentos relevantes.

Realizar ajustes basados en el feedback recibido y obtener la aprobación final.

Implementación y Monitoreo:

Implementar los estándares en toda la organización y monitorear su cumplimiento.

Realizar auditorías periódicas para asegurar que los estándares se sigan adecuadamente.

Diseño de Métricas

Las métricas son esenciales para medir la efectividad de las políticas y estándares de seguridad de la información. Permiten evaluar el desempeño y realizar mejoras continuas.

#### 4.4.5.2 Identificación de Indicadores Clave

Definir indicadores clave de desempeño (KPIs) que reflejen los objetivos de seguridad de la información.

Asegurar que los KPIs sean específicos, medibles, alcanzables, relevantes y temporales (SMART).

#### 4.4.5.3 Desarrollo de Métricas

Establecer métodos para recopilar y analizar datos relacionados con los KPIs.

Definir umbrales y objetivos para cada métrica.

Monitoreo y Reporte:

Implementar sistemas para monitorear las métricas de manera continua.

Generar informes periódicos para la alta dirección y otras partes interesadas.

Revisión y Mejora:

Revisar las métricas y los informes para identificar áreas de mejora.

Ajustar las políticas, estándares y procedimientos basados en los resultados obtenidos.

Proceso de Gestión de Incidente

La gestión de incidentes de seguridad de la información es crucial para responder de manera efectiva a los incidentes y minimizar su impacto.

Clasificación de Incidente de Seguridad de la Información

Identificación del Incidente:

Detectar y registrar cualquier evento que pueda comprometer la seguridad de la información.

Utilizar herramientas de monitoreo y detección para identificar incidentes.

Clasificación del Incidente:

Evaluar la naturaleza y gravedad del incidente.

Clasificar el incidente en categorías como acceso no autorizado, pérdida de datos, malware, etc.

#### 4.4.5.4 Priorización del Incidente

La priorización de los incidentes se basa en dos factores clave: el impacto y la urgencia.

Impacto:

Descripción: Evalúa el efecto potencial del incidente en la organización.

Niveles:

Alto: Impacto significativo en las operaciones o la reputación.

Medio: Impacto moderado que puede ser manejado con recursos internos.

Bajo: Impacto mínimo con poca o ninguna interrupción.

Urgencia:

Descripción: Evalúa la necesidad de una respuesta inmediata.

Niveles:

Alta: Requiere atención inmediata para evitar daños mayores.

Media: Necesita ser atendido pronto, pero no es crítico.

Baja: Puede ser manejado en el curso normal de las operaciones.

**Tabla 29**

*Matriz de Priorización*

| **Impacto \ Urgencia** | Baja (1) | Media (2) | Alta (3) |
|---|---|---|---|
| **Alto (3)** | Medio (3) | Alto (6) | Muy Alto (9) |
| **Medio (2)** | Bajo (2) | Medio (4) | Alto (6) |
| **Bajo (1)** | Bajo (1) | Bajo (2) | Medio (3) |

Nota: Esta matriz ayuda a determinar la prioridad de respuesta a los incidentes, asegurando que los recursos se asignen de manera efectiva para mitigar los riesgos más críticos.

Estos elementos son fundamentales para un SGSI robusto y efectivo, asegurando que la organización esté preparada para enfrentar y gestionar los riesgos de seguridad de la información de manera proactiva y eficiente.

Aplicación de los Controles del Anexo A de la ISO 27001:2022

El Anexo A de la ISO 27001:2022 proporciona una lista de controles que pueden ser aplicados para mitigar los riesgos de seguridad de la información. Estos controles deben ser seleccionados y aplicados de acuerdo con las políticas de seguridad diseñadas.

Control de Acceso:

Implementar políticas de control de acceso basadas en roles y responsabilidades.

Utilizar autenticación multifactor para sistemas críticos.

Seguridad Física y Ambiental:

Instalar sistemas de vigilancia y controles de acceso físico.

Asegurar que las instalaciones estén protegidas contra amenazas físicas.

Seguridad de las Comunicaciones:

Implementar cifrado para proteger la información en tránsito.

Asegurar la integridad y confidencialidad de las comunicaciones.

Gestión de Incidentes de Seguridad:

Establecer procedimientos para la detección, reporte y respuesta a incidentes de seguridad.

Realizar simulacros y pruebas regulares de los procedimientos de respuesta a incidentes.

Implementación de Controles

La implementación de controles es un paso crítico para asegurar que los riesgos identificados sean mitigados de manera efectiva. Esto incluye:

Selección de Controles:

Basarse en la evaluación de riesgos para seleccionar los controles más adecuados.

Asegurar que los controles sean proporcionales al nivel de riesgo.

Implementación Técnica:

Configurar y desplegar controles técnicos como firewalls, sistemas de detección de intrusos y cifrado.

Asegurar que los controles técnicos estén correctamente integrados en la infraestructura existente.

Implementación Administrativa:

Desarrollar y comunicar políticas y procedimientos de seguridad.

Asegurar que todos los empleados comprendan y cumplan con las políticas.

Implementación de un Programa de Gestión de Incidentes

Un programa de gestión de incidentes es esencial para responder de manera efectiva a los incidentes de seguridad de la información.

Desarrollo de Procedimientos:

Establecer procedimientos claros para la detección, reporte y respuesta a incidentes.

Asegurar que los procedimientos sean conocidos por todos los empleados.

Capacitación y Simulacros:

Capacitar al personal en la gestión de incidentes.

Realizar simulacros regulares para probar la eficacia de los procedimientos.

Monitoreo y Mejora:

Monitorear continuamente los incidentes y la respuesta a los mismos.

Revisar y mejorar los procedimientos basados en las lecciones aprendidas.

#### 4.4.5.5 Gestión de Recursos para el SGSI

La gestión de recursos es crucial para asegurar que el SGSI tenga los recursos necesarios para su implementación y mantenimiento.

Asignación de Recursos:

Identificar y asignar los recursos necesarios, incluyendo personal, tecnología y presupuesto.

Asegurar que los recursos sean suficientes para cumplir con los objetivos del SGSI.

Capacitación y Desarrollo:

Proporcionar capacitación continua para el personal involucrado en el SGSI.

Fomentar el desarrollo profesional y la actualización de conocimientos.

Monitoreo de Recursos:

Monitorear el uso y la efectividad de los recursos asignados.

Ajustar la asignación de recursos según sea necesario para optimizar el SGSI.

Recepción, Análisis y Aprobación por Parte de Altos Mandos de COOPEVE

La participación y el apoyo de la alta dirección son esenciales para el éxito del SGSI.

Presentación del Plan:

Presentar el plan de implementación del SGSI a la alta dirección y la junta directiva.

Asegurar que el plan esté alineado con los objetivos estratégicos de la organización.

Análisis y Feedback:

Recibir y analizar el feedback de la alta dirección.

Realizar ajustes en el plan basado en el feedback recibido.

Aprobación Final:

Obtener la aprobación final del plan de implementación por parte de la alta dirección.

Asegurar el compromiso y el apoyo continuo de la alta dirección para la implementación y mantenimiento del SGSI.

# V. DISCUSIÓN DE RESULTADOS

## 5.1 Contrastación de las Hipótesis

En esta sección, se contrastan las hipótesis planteadas al inicio del estudio con los resultados obtenidos durante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.).

## 5.2 Hipótesis General

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2022 mejorará significativamente la protección de la información en la Cooperativa de Servicios Múltiples El Educador Veragüense, reduciendo las vulnerabilidades y fortaleciendo la capacidad de respuesta ante incidentes de seguridad durante el periodo 2022-2023.

## 5.3 Hipótesis Nula (H0)

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la Norma ISO 27001:2022 en la Cooperativa de Servicios Múltiples El Educador Veragüense durante el periodo 2022-2023 no logrará mejorar significativamente la protección de la información, ya que los controles implementados no serán suficientes para mitigar adecuadamente las vulnerabilidades y amenazas identificadas, ni para asegurar una adecuada gestión de la confidencialidad, integridad y disponibilidad de la información.

## 5.4 Resultados

Reducción de Vulnerabilidades: Tras la implementación del SGSI, se observó una reducción significativa en las vulnerabilidades, especialmente en áreas críticas como el acceso no autorizado y la pérdida de datos. Los controles implementados, como la autenticación multifactor y las copias de seguridad diarias, demostraron ser efectivos en mitigar los riesgos identificados.

Fortalecimiento de la Capacidad de Respuesta: La capacidad de respuesta ante incidentes de seguridad mejoró notablemente. La implementación de procedimientos de respuesta a incidentes y la capacitación del personal permitieron una respuesta más rápida y efectiva a los incidentes de seguridad.

Gestión de la Confidencialidad, Integridad y Disponibilidad: Los resultados mostraron una mejora en la gestión de la confidencialidad, integridad y disponibilidad de la información. Los controles técnicos y administrativos implementados aseguraron que la información crítica estuviera protegida contra amenazas internas y externas.

Contrastación:

Hipótesis Nula (H0): Los resultados refutan la hipótesis nula, ya que los controles implementados fueron suficientes para mitigar adecuadamente las vulnerabilidades y amenazas identificadas, mejorando la protección de la información.

## 5.5 Contrastación de los Resultados con Estudios Similares

Para validar los resultados obtenidos en la implementación del SGSI en la Cooperativa de Servicios Múltiples El Educador Veragüense (COOPEVE, R.L.), se compararon con estudios similares realizados en tesis doctorales y de maestría sobre la implementación de SGSI bajo la norma ISO 27001.

### *5.5.1 Estudio 1*

Diseño de un SGSI basado en el estándar ISO 27001 para la empresa Invimedic S.A.

Resultados del Estudio: Este estudio, realizado como parte de una tesis de maestría en la Universidad Politécnica Salesiana, reportó un diagnóstico de la situación actual de seguridad de la información en Invimedic S.A., seguido del diseño e implementación de un SGSI basado en ISO 27001.

"Se observa que lo descrito en la presente tesis permite realizar un estudio minucioso en relación con la situación inicial presento la empresa Invimedic; mejorar la gestión de los activos y minimizar las posibilidades de riesgo." (Álava & Choez, 2023, p. 114)

Comparación: Los resultados obtenidos en COOPEVE, R.L. son consistentes con los hallazgos de este estudio, destacando la efectividad de los controles implementados y la importancia de un diagnóstico inicial exhaustivo.

### *5.5.2 Estudio 2*

Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio

Resultados del Estudio: Esta tesis de Grado de la Escuela Politécnica Nacional en Quito se centró en el diseño de un SGSI para una organización específica, utilizando la norma ISO/IEC 27001:2013 y la metodología Magerit para la gestión de riesgos.

Finalmente, debido a que el Hospital de Especialidades Fuerzas Armadas No. 1 no dispone de un SGSI que le permita resguardar de manera adecuadas sus activos de información, se realizó

el establecimiento del diseño de un SGSI basado en la norma ISO/IEC 27001:2013 para esta institución, que facilitará su implementación en el futuro. (Guano & Jaramillo, 2020, p. 99)

Comparación: Los resultados en COOPEVE, R.L. reflejan una tendencia similar, donde la implementación de controles específicos y la gestión de riesgos fueron fundamentales para mejorar la seguridad de la información.

### *5.5.3 Estudio 3*

Implementación de un SGSI en las áreas de RR.HH. y Logística de la empresa ARMER S.A.C.

Resultados del Estudio: Este estudio, realizado como parte de una tesis de maestría en la Universidad Tecnológica del Perú, se enfocó en la implementación de un SGSI en áreas específicas de la empresa ARMER S.A.C.

Comparación: Los resultados en COOPEVE, R.L. son comparables, especialmente en términos de la mejora en la protección de la información y la gestión de riesgos en áreas críticas.

# VI. CONCLUSIONES

La implementación del SGSI bajo la norma ISO 27001:2022 ha proporcionado una estructura sólida para la gestión de la seguridad de la información en COOPEVE, R.L., mejorando significativamente la protección de los activos de información y la gestión de riesgos.

El diagnóstico integral ha permitido identificar brechas y áreas de mejora, proporcionando una base sólida para la implementación del SGSI.

El inventario detallado de activos ha facilitado la evaluación de riesgos y la implementación de medidas de protección adecuadas.

El marco de políticas y procedimientos ha establecido directrices claras para la gestión de la seguridad de la información, alineadas con los estándares de la norma ISO 27001:2022.

Los controles de seguridad implementados han mitigado eficazmente los riesgos identificados, garantizando la confidencialidad, integridad y disponibilidad de la información crítica.

El programa de capacitación y concientización ha mejorado la comprensión y aplicación de las políticas y prácticas de seguridad entre los colaboradores.

El plan de respuesta a incidentes ha permitido a la Cooperativa detectar, responder y recuperarse de manera efectiva ante posibles brechas de seguridad.

El sistema de monitoreo y auditoría continua ha asegurado el cumplimiento continuo con los requisitos de la Norma ISO 27001:2022 y ha permitido evaluar el desempeño del SGSI.

Las evaluaciones periódicas y auditorías internas han identificado áreas de mejora y asegurado la efectividad del SGSI.

## VII. RECOMENDACIONES

Continuar con la implementación y mantenimiento del SGSI, asegurando que se realicen revisiones periódicas y se adapten las políticas y procedimientos a las necesidades cambiantes de la cooperativa.

Continuar con evaluaciones periódicas para identificar nuevas brechas y áreas de mejora, asegurando que el SGSI se mantenga actualizado y efectivo.

Mantener el inventario de activos actualizado y realizar revisiones regulares para evaluar el valor y los riesgos asociados a cada activo, asegurando una protección adecuada basada en el riesgo.

Revisar y actualizar las políticas y procedimientos de seguridad de la información periódicamente para adaptarse a las necesidades cambiantes de la Cooperativa y cumplir con los estándares de la Norma ISO 27001:2022.

Evaluar la efectividad de los controles de seguridad implementados y realizar ajustes necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información crítica.

Continuar con programas de capacitación y concientización regulares para todos los colaboradores, asegurando que comprendan y apliquen correctamente las políticas y prácticas de seguridad establecidas.

Probar y actualizar el plan de respuesta a incidentes regularmente para asegurar que la Cooperativa pueda detectar, responder y recuperarse de manera efectiva ante posibles brechas de seguridad.

Establecer un sistema robusto de monitoreo y auditoría continua para evaluar el desempeño del SGSI y asegurar el cumplimiento continuo con los requisitos de la Norma ISO 27001:2022.

Programar evaluaciones y auditorías internas periódicas para identificar áreas de mejora y asegurar la efectividad del SGSI, realizando ajustes necesarios para mantener la conformidad con la norma.

## VIII. REFERENCIAS BIBLIOGRÁFICAS

Abazi, B. (2020). *A novel approach for information security risk assessment maturity framework based on ISO 27001* [Tesis Doctoral, CORVINUS UNIVERSITY OF BUDAPEST]. https://phd.lib.uni-corvinus.hu/1088/

Álava, M., & Choez, H. (2023). *Diseño de un SGSI Basado en el Standard ISO 27001 para la Empresa INVIMEDIC S.A.* [Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/26680/1/UPS-CT011078.pdf

Aleman, F. (2023). *Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023* [Tesis Maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/106824

Alianza Cooperativa Internacional. (2024). *Datos y cifras*. https://ica.coop/es/cooperativas/datos-y-cifras

Allendevaux, S. (2021). *How U.S. State Data Protection Statutes Compare In Scope To Safeguard Information And Protect Privacy Using Iso/Iec 27001:2013 And Iso/Iec 27701:2019 Security And Privacy Management System Requirements As An Adequacy Baseline* [Tesis Doctoral, Northeastern University]. https://repository.library.northeastern.edu/files/neu:bz613b467/fulltext.pdf

Baca, G. (2016). *Introducción a la Seguridad Informática*. https://www.google.com.pa/books/edition/Introducci%C3%B3n_a_la_seguridad_inform%C3%A1tic/IhUhDgAAQBAJ?hl=es&gbpv=1&dq=Introducci%C3%B3n%20a%20la%20Seguridad%20Inform%C3%A1tica.%20Ciudad%20de%20M%C3%A9xico%2C%20M%C3%A9xico%3A%20Grupo%20Editorial%20Patria&pg=PA13&printsec=frontcover

Bai, H. (2022). Legal Management of Network Information Security Based on Embedded Real-Time Task Processing. *Computational Intelligence and Neuroscience*, *2379274*. https://onlinelibrary.wiley.com/doi/10.1155/2022/2379274

Banconal. (2021). Banco Nacional de Panamá. *Banconal obtiene certificación ISO/IEC 27001:2022 en seguridad de la información*. https://www.banconal.com.pa/noticias/871-banconal-obtiene-certificacion-iso-iec-27001-2022-en-seguridad-de-la-informacion.html

Benítez, M. (2022). *Sistema Automatizado Con Controles Informáticos Para Una Administración Del Subsidio Pase-U* [Tesis Doctoral, Universidad de Panamá]. http://up-rid.up.ac.pa/6680/3/mario_benitez.pdf

Calder, A. (2008). *ISO27001 / ISO27002 A Pocket Guide* (IT Governace Publishing). https://itgusa.blob.core.windows.net/files/download/2020-iso270002_1%20final%20ebook.pdf

Calder, A., & Watkins, S. (2002). *IT Governance an International Guide to Data Security and ISO 27001/27002 6th Edition*. http://repo.darmajaya.ac.id/5518/1/IT%20Governance%20An%20International%20Guide%20to%20Data%20Security%20and%20ISO27001ISO27002%20by%20Alan%20Calder%2C%20Steve%20Watkins%20%28z-lib.org%29.pdf

Calderon, C. (2022). *Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022* [Tesis Maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/97640/Calderon_ACJ-SD.pdf?sequence=4

Castillo, L. (2022). *Evaluación de la seguridad informática bajo lasnormas ISO/IEC 27001 en la infraestructura tecnológica de la Universidad Estatal de Milagro* [Universidad Estatal del Milagro]. https://repositorio.unemi.edu.ec/handle/123456789/7000

Contero, W. (2019). *Diseño De Una Política De Seguridad De La Información Basada En La Norma Iso 27002:2013, Para El Sistema De Botones De Seguridad Del Ministerio Del Interior* [Tesis Maestria, Universidad Internacional SEK]. https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Cuenca, W. (2019). *Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala*. https://repositorio.uta.edu.ec/bitstream/123456789/29844/1/Tesis_t1585msi.PDF

Encalada, D. (2024). *Propuesta de Política interna alineada a la Ley de Protección de Datos Personales mediante estándar NIST para Cooperativas de Ahorro y Crédito.* [Tesis Maestría, Universidad Israel].

https://repositorio.uisrael.edu.ec/bitstream/47000/4185/1/UISRAEL-EC-MASTER-SEG-INF-ART-%20378.242-2024-004.pdf

Gil, M. (2024). *ISO 27001 y gestión de vulnerabilidades en activos informáticos del centro de datos de una entidad pública geocientífica, Lima 2023* [Tesis Maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/137762

Godoy, J. (2021). *Impacto En Los Sistemas De Información Contables Por Efecto De Los Delitos Informáticos A Las Operaciones De Banca Por Internet En La Ciudad De Panamá* [Tesis Doctoral, Universidad de Panamá]. https://up-rid.up.ac.pa/5020/1/jose_godoy.pdf

Guano, M., & Jaramillo, M. (2020). *Diseño de un SGSI bajo la Norma ISO/IEC 27001:2013 Aplicado a un Caso de Estudio* [Tesis Grado, Escuela Politécnica Nacional]. https://bibdigital.epn.edu.ec/handle/15000/21472?locale=es

Hernandez, R. (2014). *Metodología de La Investigación* (Sexta Edición). McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Huanca, J. (2018). *La Falsa Percepción En La Seguridad De Los Sistemas Informáticos* [Tesis Doctoral, Universidad Nacional Del Altiplano]. http://repositorio.unap.edu.pe/handle/20.500.14082/8235

Infosecurity Mexico. (2021). *Los 7 errores al implementar un sistema de gestión de seguridad de la información*. https://www.infosecuritymexico.com/es/blog/los-7-errores-al-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion.html

IPACOOP. (2023). *Sector cooperativo sigue creciendo, se crean dos nuevas cooperativas*. https://ipacoop.gob.pa/sector-cooperativo-sigue-creciendo-se-crean-dos-nuevas-cooperativas/

ISO. (2022). *Seguridad de la informacion, ciberseguridad y proteccion de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos*.

ISO/IEC. (2018). *INTERNATIONAL STANDARD ISO/IEC 27005:2018*.

Isotools. (2022). *Seguridad de la Información y Continuidad de negocio*. https://www.isotools.us/2022/04/15/aspectos-de-seguridad-de-la-informacion-para-la-gestion-de-la-continuidad-del-negocio/

Isotools. (2023). ESGInnova ISO 27001 [Blog]. *ISO 27001*. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Isotools. (2024). *ISO 27001. El inventario de activos en la implementación de la norma*. https://www.isotools.us/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

isotools. (2024). *ISO/IEC 27005:2018, la norma que reducirá el riesgo de brechas en la seguridad informática*. https://www.isotools.us/2018/08/15/iso-iec-270052018-reducira-el-riesgo-de-brechas-en-la-seguridad/

Lopera, I. (2023). *Sistema de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación para mitigar posibles riesgos en las plataformas industriales del sector manufactura-textil* [Tesis Maestría, Instituto Tecnológico Metropolitano]. https://repositorio.itm.edu.co/handle/20.500.12622/6291

López, T. (2023). ISO 27001 Última Versión 2022: Novedades y Cambios Más Importantes. *Blog de Innevo*. https://blog.innevo.com/iso27001-2022

Mantilla, A. (2009). *Diseño De Un Sistema De Gestión De Seguridad De La Información Para Cooperativas De Ahorro Y Crédito En Base A La Norma Iso 27001* [Tesis Maestría, Escuela Politécnica Nacional]. https://bibdigital.epn.edu.ec/bitstream/15000/8108/1/CD-2254.pdf

Martínez, S. (2021). *Diseño De Un Modelo De Sistema De Gestión De Calidad Para Laboratorios De Ensayo De Investigación* [Tesis Doctoral, Universidad Politecnica de Madrid]. https://oa.upm.es/69026/

Mendoza, M. (2023). *ISO 27001:2022: ¿qué cambios introdujo el nuevo estándar de seguridad?* [Www.welivesecurity.com]. https://www.welivesecurity.com/la-es/2023/02/09/iso-270012022-cambios-nuevo-estandar-seguridad/

Morales, L. (2019). *Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito* [Tesis Maestria, Universidad de Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/29216/1/Tesis_%20t1537msi.pdf

Moya, C. (2023). *Propuesta De Un Plan De Seguridad Informático Para La Empresa E.P.-E.M.A.P.A.-A.* [Tesis Maestría, Pontificia Universidad Católica del Ecuador]. https://repositorio.puce.edu.ec/bitstreams/f4759b2e-d64b-4b88-8e3c-cbf6c40b7065/download

Moya, E. (2023). *Los beneficios y los desafíos de implantar un SGSI en nuestra organización.* https://www.iaas365.com/los-beneficios-y-los-desafios-de-implantar-un-sgsi-en-nuestra-organizacion/

Osellame, G., & Fong, J. (2017). *Juridicidad De Las Actuaciones De Liquidadores Dentro Del Régimen Cooperativo De Panamá*. https://revistas.umecit.edu.pa/index.php/oratores/article/download/219/353

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Int. J. Morphol.* https://www.scielo.cl/scielo.php?pid=S0717-95022017000100037&script=sci_arttext&tlng=pt#back

Parra, Á. (2014). *ISO 27001 PARA PYMES* [Tesis Maestría, Universidad Internacional de la Rioja]. https://reunir.unir.net/bitstream/123456789/3128/1/AngelaMaria_Parra_Giraldo.pdf

Salazar, C., & Aviles, B. (2023). *Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales*. https://doi.org/doi.org/10.33386/593dp.2024.1.2156

*Scriesgo Rating Agency*. (2017). https://scriesgo.com/files/publication/69_inf_sectorialcooperativasdiciembre2017.pdf

Torres, H. (2021). *Propuesta de metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas* [Tesis Maestría, Universidad CENFOTEC]. https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/383/Torres%20Ruiz%2C%20Herbeth-MSEG_Dic2021.pdf?sequence=1&isAllowed=y

Tuabanda, J. (2023). *Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001; A9 control de acceso* [Tesis Maestría, Universidad Israel]. https://repositorio.uisrael.edu.ec/handle/47000/3562

Túquerres, E. (2024). *Marco de trabajo de evaluación de la seguridad del SGSI en una cooperativa de ahorro y crédito del segmento 1 basado la norma ISO/IEC 27007:2020 y ISO/IEC 27004:2016* [Tesis Maestria, Universidad Técnica Del Norte]. https://repositorio.utn.edu.ec/handle/123456789/15835

Valencia, F., & Orozco, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000*. https://scielo.pt/pdf/rist/n22/n22a06.pdf

Velasco, F., Ullauri, R., Pilicita, L., & Jacome, B. (2018). *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. https://www.researchgate.net/publication/329472976_Benefits_of_Implementing_an_ISMS_According_to_the_ISO_27001_Standard_in_the_Ecuadorian_Manufacturing_Industry

# IX. ANEXOS

Encuesta sobre implementación de Procedimientos, Políticas y Controles Informáticos

## Encuesta sobre implementación de Procedimientos, Políticas y Controles Informáticos

**Instrucciones:**
Esta encuesta está diseñada para recopilar información sobre la percepción de los colaboradores de COOPEVL R.L. con respecto a las políticas, procedimientos y controles de seguridad informática y ciberseguridad. Las respuestas serán tratadas de manera confidencial. Por favor, marque la opción que mejor refleje su opinión.

1. **¿Con qué frecuencia utiliza sistemas tecnológicos en sus tareas diarias?**

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Frecuentemente
- ◯ Siempre

2. **¿Qué tan informado se siente sobre las políticas de seguridad informática implementadas?**

- ◯ Nada informado
- ◯ Poco informado
- ◯ Medianamente informado
- ◯ Muy informado
- ◯ Totalmente informado

3. **¿Con qué frecuencia recibe capacitación sobre ciberseguridad en su puesto de trabajo?**

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Frecuentemente
- ◯ Siempre

Encuesta sobre implementación de Procedimientos, Políticas y Controles Informáticos

4. **¿Considera que las políticas actuales de seguridad informática son adecuadas para proteger los sistemas y datos de la cooperativa?**

- ◯ Muy inadecuadas
- ◯ Inadecuadas
- ◯ Neutras
- ◯ Adecuadas
- ◯ Muy adecuadas

5. **¿Qué tan seguro se siente de que los datos de los clientes están protegidos adecuadamente?**

- ◯ Nada seguro
- ◯ Poco seguro
- ◯ Medianamente seguro
- ◯ Muy seguro
- ◯ Totalmente seguro

6. **¿Sabe cómo reportar incidentes relacionados con la seguridad informática o ciberseguridad en la cooperativa?**

- ◯ No, no sé cómo
- ◯ Sé un poco, pero no completamente
- ◯ Sé cómo reportarlo
- ◯ Totalmente seguro de cómo hacerlo

7. **¿Considera que la infraestructura tecnológica de COOPEVE R.L. es lo suficientemente robusta para hacer frente a ciberataques?**

- ◯ Muy débil
- ◯ Débil
- ◯ Neutra
- ◯ Fuerte
- ◯ Muy fuerte

Encuesta sobre implementación de Procedimientos, Políticas y Controles Informáticos

8. **¿Qué tan efectiva cree que es la autenticación de usuarios (contraseñas, tokens, etc.) para proteger los sistemas internos?**

- ◯ Nada efectiva
- ◯ Poco efectiva
- ◯ Neutra
- ◯ Efectiva
- ◯ Muy efectiva

9. **¿Ha experimentado problemas de seguridad informática en su puesto de trabajo en el último año?**

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Frecuentemente
- ◯ Siempre

10. **¿Cómo calificaría la gestión de incidentes de seguridad informática?**

- ◯ Muy mala
- ◯ Mala
- ◯ Regular
- ◯ Buena
- ◯ Muy buena

11. **¿Qué tan claros son los procedimientos para proteger la información confidencial?**

- ◯ Nada claros
- ◯ Poco claros
- ◯ Medianamente claros
- ◯ Muy claros
- ◯ Totalmente claros

12. **¿Cree que se necesita mejorar en la capacitación sobre buenas prácticas de seguridad informática?**

- ◯ No, no es necesario
- ◯ Un poco necesario
- ◯ Neutro
- ◯ Necesario
- ◯ Muy necesario

13. **¿Qué tan protegido cree que están los sistemas contra el uso no autorizado o acceso a información confidencial?**

- ◯ Nada protegido
- ◯ Poco protegido
- ◯ Medianamente protegido
- ◯ Muy protegido
- ◯ Totalmente protegido

14. **¿Considera que la cooperativa cuenta con procedimientos claros y efectivos para la gestión de riesgos tecnológicos?**

- ◯ Nada efectivos
- ◯ Poco efectivos
- ◯ Efectivos
- ◯ Muy efectivos
- ◯ Totalmente efectivos

15. **¿Qué tan satisfecho está con los controles implementados para prevenir fraudes informáticos o ciberataques?**

- ◯ Muy insatisfecho
- ◯ Insatisfecho
- ◯ Neutro
- ◯ Satisfecho
- ◯ Muy satisfecho

16. **¿Considera que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 mejoraría la seguridad?**

- ◯ Nada
- ◯ Poco
- ◯ Medianamente
- ◯ Mucho
- ◯ Totalmente