REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN:

MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA DETERMINACIÓN Y VALORACIÓN DE RIESGOS DE LOS ACTIVOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO TULCÁN"

Trabajo de Titulación previo a la obtención del
Título de Magíster en Computación, Mención en Seguridad Informática.

AUTOR: Andrés Javier López Ruano
DIRECTOR: PhD. Jaramillo Alcázar Ángel Gabriel
ASESOR: MSc. Rea Peñafiel Xavier Mauricio

IBARRA - ECUADOR
2025

CERTIFICACIÓN

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 26 de septiembre del 2025.

Ing. Ángel Jaramillo Alcázar, PhD.
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Certifica:

Haber revisado el presente Informe Final del Trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte, en consecuencia, autorizo su presentación para los fines pertinentes.

_____

Ing. Ángel Gabriel Jaramillo Alcázar, PhD.
C.C 1715891964.

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401158985		
APELLIDOS Y NOMBRES:	LÓPEZ RUANO ANDRÉS JAVIER		
DIRECCIÓN:	OLMEDO Y ROCAFUERTE, SAN GABRIEL		
EMAIL:	ajlopezr1@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0980519290

DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA DETERMINACIÓN Y VALORACIÓN DE RIESGOS DE LOS ACTIVOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO “TULCÁN LTDA.”
AUTOR (ES):	LÓPEZ RUANO ANDRÉS JAVIER
FECHA: DD/MM/AAAA	26 – 09 – 2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con Mención en Seguridad Informática
ASESOR /DIRECTOR:	PhD. JARAMILLO ALCÁZAR ÁNGEL GABRIEL

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 26 días del mes de septiembre de 2025

EL AUTOR:

López Ruano Andrés Javier

APROBACIÓN DEL TUTOR

Yo PhD. Jaramillo Alcázar Ángel, en calidad de Tutor del Trabajo de Investigación titulado: “IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA DETERMINACIÓN Y VALORACIÓN DE RIESGOS DE LOS ACTIVOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO TULCÁN”, de autoría del Ing. Andrés Javier López Ruano, para optar por el Grado de Magíster en Computación mención Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del Jurado Examinador que se designe.

En la ciudad de Ibarra, a los 26 días del mes de septiembre del 2025.

PhD. Jaramillo Alcázar Ángel Gabriel.
Tutor.

DEDICATORIA

Con profundo amor dedico este trabajo de investigación a mis adoradas Hijas, Isabelita y Abigail, luz de mi vida e inspiración constante que me motivan a esforzarme cada día más. A mi querida Esposa Alexita, cuyo apoyo incondicional ha sido el pilar fundamental en la consecución del notable objetivo por mi parte trazado; su comprensión, aliento y amor me han dado la fortaleza necesaria para avanzar en cada etapa de este proceso.

A mis Padres; un agradecimiento especial por haberme brindado ejemplo de trabajo, constancia y superación, y, a mis excepcionales Hermanos por sus infinitas y grandiosas muestras de hermandad y apoyo; su presencia en mi vida es un regalo invaluable que me ha acompañado en cada paso del camino de progreso personal que me tracé.

El Autor.

AGRADECIMIENTO

Quiero expresar mi gratitud imperecedera a Dios por permitirme transitar en este hermoso viaje que se llama vida, a mis Padres por ser vivo ejemplo constante de integridad y esfuerzo, a mis Hermanos por su apoyo incondicional en todo momento. Mi Esposa, combustible vital de apoyo y amor incondicional en todo momento, especialmente en los difíciles, en el sendero recorrido, merece mi gratitud singular, perenne e imperecedera; mis dos hermosas Hijas, motor vivificante cotidiano: tiernas, alegres, curiosas y felices, quienes me han tributado, otorgan y contagian a raudales la importancia de vivir plenamente; mis destacados Docentes, columnas primordiales en todo este grandioso proceso académico, y, la vida por darme la oportunidad de existir y concederme estos momentos únicos de logros invaluables e inolvidables, reciban mi franco y sempiterno testimonio sintetizado en dos palabras: ¡INFINITAS GRACIAS!

Andrés Javier López Ruano.

ÍNDICE DE CONTENIDOS

CAPÍTULO I 16
EL PROBLEMA 16
1.1 Problema de Investigación. 16
1.2 Interrogantes de la investigación 18
1.3 Objetivos de la investigación 18
1.3.1 Objetivo General 18
1.3.2 Objetivos Específicos 18
1.4 Hipótesis de Trabajo 19
1.5 Hipótesis Alternativa 19
1.6 Categorización de Variables 19
1.7 Justificación 19
CAPÍTULO II 21
MARCO REFERENCIAL 21
2.1 Antecedentes 21
2.2 Marco Teórico 24
2.2.1 Naturaleza de un Sistema de Gestión de Seguridad de la Información (SGSI) 24
2.2.2 Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) 25
2.2.3 Aplicación de metodologías estandarizadas 26
2.2.4 MAGERIT 26
Ciclo de Mejora Continua 28
2.2.5 Valoración de activos de información. 28
2.3 Clasificación de los activos. 29
2.3.1 Requisitos de seguridad para garantizar la calidad de los activos de información. 29
2.3.2 Amenazas en Seguridad Informática. 30
2.3.3 Estándares de seguridad 33
2.3.4 Riesgos. 35
2.3.5 Marco legal 36
2.3.6 Constitución de la República del Ecuador 36
2.3.7 Ley de Protección de Datos Personales (LOPDP) 37
2.3.8 Código Orgánico Integral Penal (COIP) 37
2.3.9 Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (Ley SNDP) 38

2.3.10 Regulaciones de la Superintendencia de Economía Popular y Solidaria (SEPS) 38
CAPÍTULO III 39
MARCO METODOLÓGICO 39
3.1 Enfoque y Tipo de Investigación 39
3.1.1 Método Cuantitativo: 39
3.1.2 Método Cualitativo: 39
3.2 Procedimiento de investigación 40
3.3 Consideraciones Bioéticas 43
CAPÍTULO IV 45
4 DESARROLLO 45
4.1 Antecedentes de la Cooperativa 45
4.2 Visión 45
4.3 Misión 45
4.4 Estructura organizacional 45
4.4.1 Organigrama del Área de Captaciones. 46
4.4.2 Estado actual de la seguridad 46
4.4.3 Estado actual de los Activos del Área de Captaciones 48
4.5 Nivel de Cumplimiento Detallado – ISO 27002 50
4.6 Diseño del sistema de gestión de seguridad de la información para el Área de Captaciones 52
4.7 Consideraciones Iniciales 52
4.8 Partes interesadas 52
4.9 Partes externas 52
4.9.1 Recursos disponibles 53
4.9.2 Metodología para la gestión de Riesgos 53
4.10 Inventario y Clasificación de Activos de Información 53
4.10.1 Identificación de los Activos de Información 54
4.10.2 Ámbito de los Activos de Información 56
4.10.3 Clasificación de los activos de información 57
4.10.4 Valoración de los Activos de Información 57
4.10.5 Importancia de los Activos de Información. 59
4.11 Identificación de Riesgos 59
4.11.1 Identificación de Amenazas o Fuentes de Riesgos 60

4.11.2 Identificación de Vulnerabilidades. 60
4.11.3 Valoración de las Consecuencias 61
4.12 Evaluación de Riesgos 64
4.12.1 Análisis de los Datos Obtenidos 65
4.12.2 Salvaguardas 66
4.12.3 Análisis de los Datos Obtenidos 66
4.12.4 Objetivos de control y controles 69
4.12.5 Matriz de Declaración de aplicabilidad de los controles 69
4.12.6 Proceso Agregador de Valor 72
4.12.7 Gestión de Captaciones 72
4.13 Resultados para la identificación, valoración y mitigación de riesgos en activos de información utilizando la metodología MAGERIT. 73
CONCLUSIONES Y RECOMENDACIONES 76
Conclusiones 76
Recomendaciones 76
CAPITULO V 93
5.1 Determinación del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) para Cooperativa de Ahorro y Crédito "Tulcán Ltda." 93
5.1.1 Objetivo 93
5.1.2 Justificación 93
5.1.3 Políticas de Seguridad 93
5.1.4 Procedimientos de Auditorías 93
5.1.5 Estructura Organizacional de la Seguridad de la Información 94
5.1.6 Gestión de Indicadores 94
5.1.7 Procedimiento de Revisión por la Alta Dirección 94
5.1.8 Gestión de Roles y Responsabilidades 95
5.1.9 Metodología de Análisis de Riesgos 95
5.1.10 Declaración de Aplicabilidad 95
5.2 Medidas para abordar los riesgos y las oportunidades 95
5.3 Objetivos del Sistema de Seguridad de la Información y los Planes para lograrlo. 96
5.3.1 Objetivos del SGSI 96
5.4 Mejora continua 97
5.4.1 Documentos de referencia 98

Preguntas para los trabajadores (empleados de la cooperativa) sobre la Seguridad de la información. 102

ÍNDICE DE TABLAS

Tabla 1 Requerimientos de los dominios de la norma 47
Tabla 2 Distribución de riesgos en los activos, área de Captaciones 48
Tabla 3 Análisis inicial para identificación de riesgos 48
Tabla 4 Análisis Riesgo de activos 49
Tabla 5 Ámbito de los Activo de Información (Autoría Propia) 56
Tabla 6 Clasificación de los activos de información SGSI (Autoría Propia) 57
Tabla 7 Criterio de Confidencialidad SGSI (Autoría Propia) 57
Tabla 8 Criterio de Disponibilidad SGSI (Autoría Propia) 58
Tabla 9 Criterio de Integridad SGSI (Autoría Propia) 58
Tabla 10 Importancia del Activo de Información SGSI (Autoría Propia) 59
Tabla 11 Resultados del cálculo de valoraciones SGSI (Autoría Propia) 59
Tabla 12 Identificación de amenazas o fuentes de riesgos (Probabilidad) (Autoría Propia) 61
Tabla 13 Análisis Valores e Impacto 62
Tabla 14 Identificación de amenazas o fuentes de riesgos (Impacto o efecto) (Autoría Propia) 62
Tabla 15 Representación del riesgo, matriz de vulnerabilidades 63
Tabla 16 Matriz impacto y probabilidad de ocurrencia 63
Tabla 17 Matriz para determinar la clase de riesgo 64
Tabla 18 Distribución de Activos 65
Tabla 19 Activo por riesgo 65
Tabla 20 Controles para implementar ISO 27002 69
Tabla 21 Matriz de Declaración de Aplicabilidad de Controles 70
Tabla 22 Pregunta 1 78
Tabla 23 Pregunta 2 79
Tabla 24 Pregunta 3 80
Tabla 25 Pregunta 4 81
Tabla 26 Pregunta 5 82
Tabla 27 Pregunta 6 83
Tabla 28 Pregunta 7 84
Tabla 29 Pregunta 8 85
Tabla 30 Pregunta 9 86
Tabla 31 Pregunta 9 87

ÍNDICE DE FIGURAS

Figura 1 ISO 31000 - Marco de trabajo para la gestión de riesgos..... 27
Figura 2 Modelo PHVA Norma ISO 27001:2013 28
Figura 3 Modelo PHVA para ISO 27001 Modelo PHVA Norma ISO 27001. Tomada de clases/1889-iso/28231-terminos-y-definiciones, 2022, https://platzi.com..... 35
Figura 4 Estructura organizacional Cooperativa de Ahorro y Crédito "Tulcán Ltda." 45
Figura 5 Organigrama del área de captaciones...... 46
Figura 7 Brecha entre los requerimientos de los dominios de la norma 47
Figura 8 Distribución de riesgo en los activos, área de Captaciones 48
Figura 9 Evaluación de riesgo versus activo 49
Figura 10 Análisis funciones de control existente para activos..... 50
Figura 11. Nomenclatura necesaria para la evaluación..... 50
Figura 12. Rangos de efectividad en los controles de seguridad implementados 50
Figura 13 Aspectos de cumplimiento de la norma ISO 27002..... 51
Figura 14 Relación entre los aspectos de cumplimiento de la norma ISO 27002 51
Figura 15 Madurez en aspectos de mejora..... 52
Figura 17 Evaluación de riesgo versus activo 65
Figura 18 Actividades para el tratamiento de los riesgos 67
Figura 19 Control continuo de los indicadores de evaluación de impacto 68
Figura 20 Política de seguridad de la Información ISO 27001 73
Figura 21 Niveles de cumplimiento en el control posterior a la implementación..... 74
Figura 22 Diferencias en el control actual y posterior a la implementación..... 75
Figura 23 Resultados Pregunta 1 78
Figura 24 Resultados Pregunta 2 79
Figura 25 Resultados Pregunta 3 80
Figura 26 Resultados Pregunta 4 81
Figura 27 Resultados Pregunta 5 82
Figura 28 (Autoría Propia) Pregunta 6 83
Figura 29 Resultados Pregunta 7 84
Figura 30 Resultados Pregunta 8 85
Figura 31 Resultados Pregunta 9 86
Figura 32 Resultados Pregunta 10 87

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA DETERMINACIÓN Y VALORACIÓN DE RIESGOS DE LOS ACTIVOS DE LA COOPERATIVA DE AHORRO Y CRÉDITO TULCÁN

Autor: Andrés Javier López Ruano
Director: PhD. Jaramillo Alcázar Ángel Gabriel
Año: 2025

RESUMEN

El presente Trabajo de Investigación se centra en la Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", con el objetivo de valorar activos e identificar riesgos.
Este análisis se realiza en el contexto actual, en donde la transformación digital, la gestión de la seguridad de la información y la creciente exposición a riesgos cibernéticos han adquirido una relevancia crítica para las instituciones financieras.
Con la finalidad de proteger el activo más valioso de la Cooperativa; la información, se propone la implementación de un SGSI basado en la norma internacional ISO 27001.
El objetivo principal es fortalecer la protección de los activos críticos del Área de Captaciones, mediante la identificación, clasificación y tratamiento de los riesgos asociados a los tres principios principales de la seguridad de la información: confidencialidad, integridad y disponibilidad.
A través de un diagnóstico preliminar de seguridad y un análisis de brechas, se han identificado vulnerabilidades en el área de Captaciones identificando una oportunidad de mejora en los procesos de gestión de información, a partir de estos hallazgos, se plantea la implementación de un SGSI que se alinee con los requerimientos normativos y procedimentales de la Cooperativa.
Se espera que al implementar este sistema de gestión y los controles establecidos en la norma ISO 27002, se logre conseguir una mejora sustancial en la gestión de riesgos, una optimización de los procesos de Captaciones y un cumplimiento efectivo de las normativas aplicables al sector financiero.
De esta manera, la implementación del SGSI establecerá un marco de mejora continua que facilitará la resiliencia operativa de los procesos del área Captaciones frente a posibles amenazas cibernéticas o eventos adversos.

Palabras clave: Seguridad de la información, activos de la información, riesgos, vulnerabilidades.

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN SEGURIDAD INFORMÁTICA

IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR THE RISK IDENTIFICATION AND EVALUATION OF THE ASSETS OF THE TULCÁN SAVINGS AND CREDIT COOPERATIVE

Autor: Andrés Javier López Ruano
Director: PhD. Jaramillo Alcázar Ángel Gabriel
Año: 2025

ABSTRACT

The present research work is focused on the Implementation of an Information Security Management System (ISMS) in the Tulcan Savings and Credit Cooperative Ltda., aiming to value assets and find risks.

This analysis is conducted in the current context, where digital transformation, information security management, and the growing exposure to cyber risks have acquired a critical relevance for financial institutions.

With the goal of protecting the most valuable asset of the organization, information, implementing an ISMS based on the international standard ISO 27001 is proposed.

The main objective is to strengthen the protection of critical assets through the identification, classification, and treatment of the risks associated with the three main principles of information security: confidentiality, integrity, and availability.

Through a preliminary security assessment and gap analysis, vulnerabilities and improvement areas in the information management processes have been identified. From these findings, implementing an ISMS aligned with the regulatory and procedural requirements of the cooperative is proposed.

With the implementation of this management system and controls established in the international standards ISO 27002, it is expected to achieve a crucial enhancement in risk management, a security processes optimization, and a compliance of the norms applicable to the financial sector.

In this sense, the implementation of the ISMS will establish a framework for continuous improvement that will allow organizational resilience against cyber-threats or adverse events.

Keywords: Information security, information assets, risks, vulnerabilities.

CAPÍTULO I
EL PROBLEMA

1.1 Problema de Investigación.

En la actualidad las entidades del sector financiero se encuentran sumergidas en medio del acelerado desarrollo de la era digital y de las tecnologías, evolución que ha transformado la manera en todos los ámbitos de acceder a la información, desarrollar negocios, y el consumo de tecnologías, requiriendo cada vez más presencia de entornos digitales para ser más competitivos (Higuera, Plan Estratégico de Seguridad de la Información, 2025).

Con el crecimiento tecnológico en las organizaciones, el procesamiento de la información y la transaccionalidad a través de las plataformas digitales cada vez se incrementa el uso masivo por parte de las personas quienes actualmente utilizan estos medios como una nueva cultura para gestionar servicios financieros, en la medida en que lo requieren (Jhony, 2024).

Esto ha demandado a las organizaciones a disponer de todas las garantías que permitan procesar las transacciones de manera segura y confiable, apoyados en procesos y normas de seguridad internacionales para garantizar la confidencialidad, disponibilidad e integridad de la misma.

Las entidades y sus activos de información sean digitales o físicos, se enfrentan de forma creciente y permanente a amenazas como: fraude asistido por dispositivos informáticos, espionaje, sabotaje, vandalismo, fenómenos naturales, descuido, desconocimiento o mal uso del tratamiento de la información por parte de las personas. (Higuera, Plan Estratégico de Seguridad de la Información, 2025).

Se ha evidenciado que muchas de las amenazas provienen de: expertos hackers, ingenieros sociales, empleados desvinculados, errores operativos, entre otros; que lo único que buscan es dañar la integridad e imagen de una entidad.

Por ello la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el área de Captaciones para la Cooperativa de Ahorro y Crédito “Tulcán Ltda.” permitirá establecer de forma integrada las medidas de protección asegurando la identificación, valoración y gestión de los activos de información y los riesgos asociados en función del impacto que representen para la entidad en los diferentes entornos operativos ya

sean estos físicos o digitales, a través del uso de los sistemas de información digital, mitigando las posibles vulnerabilidades que pudieren existir dentro de la organización.

Por lo antes mencionado, y considerando el número de personas que diariamente usan los canales digitales, plataformas web y aplicaciones celulares, la seguridad en las entidades financieras, debe ser considerada como un factor predominante, de importancia, y de inversión, todo esto con la finalidad de brindar servicios de calidad y confianza al usuario permanente que es el socio o cliente. La transformación digital, y la diversificación de canales para transaccionar, son algunos de los nuevos paradigmas que el sistema financiero busca impulsar para facilitar el acceso de los usuarios, por esta y muchas razones más, se propone en el área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda." la Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para determinar y valorar los riesgos de los activos (Higuera, SGSI Coop Tulcan, 2024); considerando que la información es el activo más importante que posee una organización, por esta razón, es necesario protegerla con el fin de evitar las amenazas como el: malware, acceso no autorizado, ataques a la cadena de suministro, uso indebido, divulgación, denegación de servicios, destrucción o modificación que afecte a toda información confidencial, impresa o digital, ya sea que se utilice para gestionar procesos internos o brindar servicios.

Entre las ventajas importantes en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), más allá de la protección de datos, es la reducción de gastos operativos, aunque comúnmente se percibe a la seguridad de la información como un costo sin un retorno financiero inmediato, sin embargo hay una ganancia financiera si en lo posterior se logra disminuir los gastos ocasionados por incidentes o interrupciones en las operaciones o en los servicios, filtrados de datos que afecten directamente a la disponibilidad de los procesos operativos de la Cooperativa.

El Sistema Gestor de Seguridad de la Información (SGSI) permite evaluar y demostrar el grado de madurez en las entidades con respecto a sus prácticas de seguridad de la información, lo cual es muy aplicable y necesario en un sector tan crítico como el financiero popular y solidario, concluyendo que la protección de los datos es fundamental para garantizar la confianza y la continuidad del negocio. (Gómez José María, 2023).

1.2 Interrogantes de la investigación

1.2.1.- ¿Qué ventajas obtiene la cooperativa al implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en términos de confianza del cliente?

1.2.2.- ¿Cómo se puede garantizar la protección de la información sensible de sus socios y clientes frente a ciberataques?

1.2.3.- ¿Cómo puede ayudar un Sistema de Gestión de Seguridad de la Información (SGSI) a prevenir pérdidas de dinero de los clientes debido a fraudes electrónicos o vulnerabilidades en los sistemas de la cooperativa?

1.2.4.- ¿Cómo puede un Sistema de Gestión de Seguridad de la Información (SGSI) minimizar el impacto de incidentes de seguridad como fraudes internos, o suplantación de identidad?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Ahorro y Crédito Tulcán, aplicando metodologías estandarizadas y requisitos de seguridad para garantizar la calidad de los activos de información contra amenazas y riesgos.

1.3.2 Objetivos Específicos

1. Realizar un inventario de los principales activos de información de la entidad financiera, identificando y categorizando los sistemas, bases de datos, aplicaciones, documentos y otros recursos críticos que deben ser protegidos con base a la metodología MAGERIT.
2. Clasificar los activos de información en función de su importancia, valor y nivel de sensibilidad, determinando qué activos requieren una protección y controles de seguridad más rigurosos.
3. Valorar los riesgos de los activos de información, considerando la probabilidad de ocurrencia de amenazas, el impacto potencial en la confidencialidad, integridad y disponibilidad de la información.

4. Evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) y la capacidad de la Cooperativa de Ahorro y Crédito Tulcán tomada como caso de estudio para mitigar los riesgos identificados.

1.4 Hipótesis de Trabajo

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en el Área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", aplicando metodologías estandarizadas y requisitos de seguridad que permitirán garantizar la calidad de los activos de información contra amenazas y riesgos.

1.5 Hipótesis Alternativa

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en el Área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", aplicando metodologías estandarizadas y requisitos de seguridad que no permitirá garantizar la calidad de los activos de información contra amenazas y riesgos.

1.6 Categorización de Variables

Variable Independiente: Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en el Área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", aplicando metodologías estandarizadas y requisitos de seguridad

Variable Dependiente: Garantizar la calidad de los activos de información contra amenazas y riesgos.

1.7 Justificación

El proyecto a implementarse fue objeto de un estudio inicial que permitió conocer la situación actual respecto a seguridad de la información en el Área de Captaciones de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", sus procesos internos, documentación, procedimientos y su desempeño con respecto a los objetivos de la Entidad financiera antes referida. El análisis y gestión de riesgos mediante la norma ISO 2700 (2005) que busca generar un esquema global de seguridad a todos los niveles de información, en lo que respecta al análisis de riesgos la metodología a usarse será MAGERIT (2012) que permite levantar el respectivo

tratamiento de riesgos, identificar los activos principales, clasificarlos y valorarlos según su exposición al riesgo.

La metodología a aplicarse es Análisis de Riesgos, proceso que nos conduce a comprender la identificación de activos informáticos, sus vulnerabilidades y amenazas a las que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, con la finalidad de determinar los controles adecuados para mitigar la ocurrencia y exposición al riesgo (Mendoza, 2023).

Las normas de seguridad ayudarán a disponer de un marco de trabajo que permitirá definir de forma muy precisa las responsabilidades, así como las obligaciones de cada actor que interviene en la gestión del Sistema de Gestión de la Seguridad de la Información, de esta forma, se ayudará a reforzar el control interno en el Área de Captaciones en términos de seguridad.

La adopción de estándares internacionales de seguridad por varias instituciones, organizaciones y empresas que hacen gestión a través de sistemas de información y de comunicaciones sobre los activos de información, buscan mantener un rendimiento estable y eficaz, fortaleciendo la confianza de clientes y socios al demostrar un compromiso sólido con la protección de datos, logrando de manera permanente mantener los niveles de seguridad adecuados (Guerrero, 2025).

CAPÍTULO II
MARCO REFERENCIAL

2.1 Antecedentes

En este Capítulo se plantean los antecedentes de la investigación, punto importante que nos permite verificar investigaciones anteriores que abarcan la variable, la misma que forma parte del objeto de estudio del presente proyecto investigativo.

En nuestro país se han encontrado diferentes investigaciones relacionadas a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), de las cuales se hará referencia a las que se considera aportarán al presente trabajo:

Para Pilla (2019), en la investigación realizada "Diseño de una política de seguridad de la información para el área de tecnología de la información de la Cooperativa de Ahorro y Crédito Chibuleo LTDA., metodología basada en la norma ISO/IEC 27002: 2013 (López, 2005)", Proyecto de Investigación que sirvió para la obtención de la maestría en tecnologías de la información de la Universidad Internacional SEK, año 2019, en donde se pudo determinar lo siguiente:

- El investigador realiza el análisis y la revisión a profundidad de la norma internacional para la implementación de controles ISO/IEC 27002:2013, diseñando una política de seguridad de la información para el área de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. En la propuesta; se tomó en cuenta tres aspectos fundamentales: la confidencialidad, integridad y disponibilidad de los datos que posee la Institución. En base a estos elementos se realizó un análisis actual de las medidas de seguridad que el área de tecnología ha implementado, además de plasmar en una matriz los incidentes de seguridad.
- Tomando como referencia a los incidentes de seguridad suscitados, se desarrolló una matriz de riesgos, basada en la metodología Deloitte y la del Banco de España, en la que se identificaron las principales amenazas, eventos de riesgo y vulnerabilidades que afectan los activos de información dentro del área de Tecnología. Con la matriz de riesgo completa, se realizó una valoración de los activos de información, además de una reunión con el jefe de tecnología, el analista de riesgos y el oficial de seguridad de la información, quienes con criterios ponderaron los eventos y calificaron la

vulnerabilidad y ocurrencia, los informantes identificaron los eventos críticos de seguridad de información que tiene el área de Tecnología.

- Para minimizar los incidentes críticos de ciberseguridad de la información, en el departamento de tecnologías es fundamental llevar a cabo una evaluación exhaustiva de la norma ISO/IEC 27002:2013, todo esto con el objetivo de determinar los controles adecuados para reducir dichas incidencias relacionadas a la seguridad de la información. En el desarrollo de esta investigación, el área de Tecnologías de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., estableció una política de seguridad de información basado en los controles de la norma ISO 27002:2013, la cual contiene lineamientos y controles de seguridad de información que deben cumplir todas las áreas de la cooperativa.

Elizabeth Torres, en su Proyecto de Investigación: "Políticas de Seguridad de la Información basado en la Norma ISO/IEC 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato", trabajo realizado en la Universidad Técnica de Ambato, en el año 2015, pudo determinar lo siguiente:

- Al realizar la presente investigación se pudo determinar que el activo más importante de cada organización es la información, por lo tanto, es importante protegerla para lo cual una adecuada norma de protección es fundamental para evitar modificaciones o accesos no autorizados.
- El personal docente, administrativo, y estudiantes realizan sus funciones acorde a la información que brindan los sistemas de la universidad, por lo tanto, es importante que la información y centros de procesamiento tengan restringido el acceso, especialmente a estudiantes estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002, que ayuda a protegerla, puesto que las políticas de seguridad minimizan el riesgo de pérdida de información garantizando el correcto funcionamiento de los procesos (Ambato, 2015).
- La tecnología evoluciona todos los días, por esta razón la universidad debe estar constantemente actualizada en los ámbitos de tecnología, telecomunicaciones y políticas de seguridad, aplicando procedimientos, documentación y manuales para la estandarización de los procesos. (Torres, 2022).

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un marco compuesto de políticas, procedimientos y directrices junto con los recursos y actividades asociados que son gestionados de manera integral por una entidad u organización, con el objetivo de resguardar sus activos de información críticos. Este enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (Porras Ruiz, 2019).

El uso de sistemas de gestión de seguridad de la información implica seguir una serie de pasos o etapas destinados a mantener o a mejorar el nivel de competitividad, rentabilidad y reputación de una empresa. Es importante tener un SGSI yaque a más de establecer políticas, se valora las diferentes amenazas, se analiza el riesgo obteniendo grandes beneficios; algunos de ellos se señalan a continuación: "Estructura e inversiones adecuadas y costos reducidos, control y calificación de activos, dirección, políticas de seguridad, operaciones y comunicaciones, evaluación de riesgos internos y externos" (Torres, 2022).

Según (Morales Alomoto, 2018) Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito (Tesis de grado de Magister en Gerencia de Sistemas de Información) Universidad Técnica de Ambato – Ecuador, comprende que el análisis de los activos críticos del negocio y su grado de riesgo son cruciales para construir un plan de seguridad que impacte positivamente en las áreas de riesgo y de tecnología. Mediante la medición en el Balanced ScoreCard se asegura el monitoreo y seguimiento de las actividades a desarrollar, permitiendo también llevar un adecuado control de la gestión integral de la seguridad de la información, lo cual es replicable a otra actividad económica o proyecto de la institución.

De acuerdo a la visión de Enrique Antón Peregrina: Realidad o Utopía, se evidencia que en la actualidad la Seguridad de la Información es un tema de mayor preocupación en las organizaciones, tomando en cuenta que la información es uno de los activos más valiosos e importantes, al cual se debe aplicar los controles de seguridad con la finalidad de minimizar los riesgos y evitar así ataques o desastres, pérdida de información crítica hasta la interrupción de las operaciones de la organización. Sin embargo, muchas veces estos esfuerzos no son correctamente encaminados. Bajo este contexto es bueno recordar lo señalado por Jorge Sendra Mas, quien indica lo siguiente: La Seguridad de la Información ha

experimentado una continua evolución durante la última década, desde un enfoque puramente tecnológico, donde las necesidades se cubren mediante la adquisición de herramientas con el fin de mitigar las últimas vulnerabilidades conocidas, hasta un enfoque dominado por la necesidad de justificar las inversiones en seguridad de la información, como un activo esencial. Este enfoque se basa en una gestión continua de los riesgos sustentados en la optimización de ratios empresariales como es el de costo/beneficio. (Anton Peregrina, 2020).

En las empresas la importancia de contar con un sistema de gestión de la seguridad de la información ha llamado la atención en los últimos años, lo expuesto en la Jornada Internacional de Forum Spain; allí Lukas Alarcón, experto en seguridad de la información explicó que a pesar de que muchas personas asocian la idea de protección informática con los hackers, esto se deriva a un error debido a que la seguridad informática tiene muchos frentes. La tecnología representa un componente dentro del ámbito de la seguridad que deben de tenerse en cuenta, el cual indica: "En la actualidad existen diversas estrategias para abordar la protección de la información cuyo contenido y estructura refleje el ámbito cultural de la propia empresa y su dinámica respecto a su quehacer, una arista más es la implementación efectiva de las políticas en las que los elementos técnicos que me ayudan en la implementación estén de acuerdo a los objetivos." (Lukas, 2015).

2.2 Marco Teórico

2.2.1 Naturaleza de un Sistema de Gestión de Seguridad de la Información (SGSI)

En toda organización, es esencial contar con un Sistema de Gestión de Seguridad de la Información (SGSI), muchas organizaciones estiman tener sistemas eficientes y eficaces para protegerse y asegurar su información; diseñan controles, disponen de software para aplicar los controles, pero todo esto es aplicable solo cuando se presentan los incidentes de seguridad, actuando de manera reactiva, sin tener un enfoque bien estructurado y claro de un sistema para gestionar la seguridad de la información (Alvarado, 2025).

La seguridad de la información abarca no solo la tecnología, sino el factor humano, la estructura organizativa, la parte normativa, para lo cual se vuelve necesario disponer de un amplio conocimiento sobre la gestión de todos estos recursos, sin embargo, esta gestión puede resultar parcial, insuficiente o ineficaz si se presentan fallas de hardware, software,

fallas humanas, catástrofes naturales, ataques terroristas, entre otros, que puedan comprometer la seguridad de la información. (Suites, 2024)

Ante la evidente y creciente competencia impulsada por la globalización y las nuevas modalidades del negocio, las empresas, sin importar su tamaño, su actividad o ubicación, deben adoptar un enfoque de manera proactiva para asegurar su información, de manera tal, que su productividad mejore, y alcance sus objetivos institucionales (Mantilla, 2009).

2.2.2 Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Esta implementación se basa en una serie de pasos y procesos que permiten establecer un enfoque sistemático y eficaz para la gestión de una organización considerándola una estructura integral que ayuda a las organizaciones a proteger su información contra amenazas y riesgos de seguridad.

Para iniciar la implementación de un Sistema de Gestión es necesario llevar a cabo una evaluación exhaustiva de los activos del área de Captaciones, información de la Cooperativa de Ahorro y Crédito Tulcán, esto deriva a identificar y clasificar la información considerada crítica y posterior evaluar los riesgos a los que está expuesta concluyendo que la evaluación servirá como base para determinar objetivos de seguridad y medidas preventivas de seguridad. Realizada la evaluación, se procede a desarrollar una política de seguridad de la información para establecer los principios y las principales directrices para la protección de la información, política aprobada por el Consejo de Administración y Gerencia General según el organigrama de estructura organizacional de la entidad.

Una vez que se establece la política se lleva a cabo la planificación del Sistema del Sistema de Gestión (SGSI), esto implica la identificación de controles y medidas de control necesarias para mitigar los riesgos que se han identificado en la evaluación inicial; estos controles pueden incluir medidas técnicas como: firewalls, sistemas de detección de intrusos y en las mismas condiciones medidas internas de la organización como procedimientos y políticas relacionados a la seguridad, esta planificación abarca la asignación de responsabilidades a los usuarios y la definición de los recursos necesarios para la implementación del Sistema de Gestión.

Completado el proceso de la planificación, se procede a la implementación de los controles y medidas de seguridad definidos, esto incluye la adquisición e instalación de herramientas de seguridad, implementación que debe ser llevada a cabo de manera gradual considerando el impacto en las operaciones de la organización.

Implementados los controles y medidas de seguridad se requiere un monitoreo y revisión permanente para asegurar su efectividad con la finalidad de detectar posibles vulnerabilidades, para esto, se requiere la realización de auditorías internas y externas, la revisión permanente de los controles y la evaluación de incidentes de seguridad, los resultados de estas actividades son utilizados para realizar mejoras continuas en el Sistema de Gestión garantizando mantener actualizado frente a nuevas amenazas y riesgos.

2.2.3 Aplicación de metodologías estandarizadas

La metodología a implementarse en Cooperativa de Ahorro y Crédito "Tulcán. Ltda.", inicia desde la identificación de activos llega hasta concluir con el establecimiento de los controles de riesgo al que están expuestos; para una entidad financiera como una Cooperativa de Ahorro y Crédito, los activos de información entre muchos otros podrían ser: Creación de clientes, Recepción de requisitos, Validación de la información, Comunicación de información y actualizar información del socio o cliente.

Para el inicio de la metodología a implementarse, se identifica a los activos de información ubicándolos y asignando los custodios o responsables, posterior se determina las amenazas y su posibilidad de ocurrencia, acto seguido se identifican las vulnerabilidades y la posibilidad de que estas sean explotadas por cada amenaza. (Cooperativa de Ahorro y Crédito Tulcán, 2024).

2.2.4 MAGERIT

Según el portal de Electrónica, Administración (2024) es identificar, evaluar y gestionar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en una organización o empresa, esta metodología se enfoca en analizar tanto los activos de información como las amenazas y vulnerabilidades existentes en los sistemas de información con el fin de determinar la probabilidad de que ocurran incidentes de seguridad y evaluar el impacto potencial de estos incidentes (MAGERIT, 2012).

El análisis de riesgos permite identificar la naturaleza del riesgo, evaluar su magnitud, e implementar medidas para salvaguardar el sistema, en armonía con los objetivos, tácticas y directrices de la organización, las acciones de gestión de riesgos permiten la creación de un plan de seguridad que una vez que se lo ha establecido y funciona cumple con los objetivos establecidos con el nivel de riesgo aceptable para la cooperativa, a todo este conjunto de actividades se llama el proceso de gestión de riesgos (wordpress.com, 2020)

La implantación de medidas de seguridad requiere una organización gestionada y la participación informada del personal que trabaja en la administración del sistema de seguridad de la información, este personal es el responsable de la operación diaria, y de la rápida reacción ante incidencias, de la monitorización del sistema en general para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo debido a que los sistemas de información rara vez son inmutables, más bien se encuentran sometidos a evolución continua, tanto propia, como de nuevos activos, como del entorno por nuevas amenazas, lo que requiere revisiones periódicas en la que se aprende de la experiencia adaptándose al nuevo contexto.

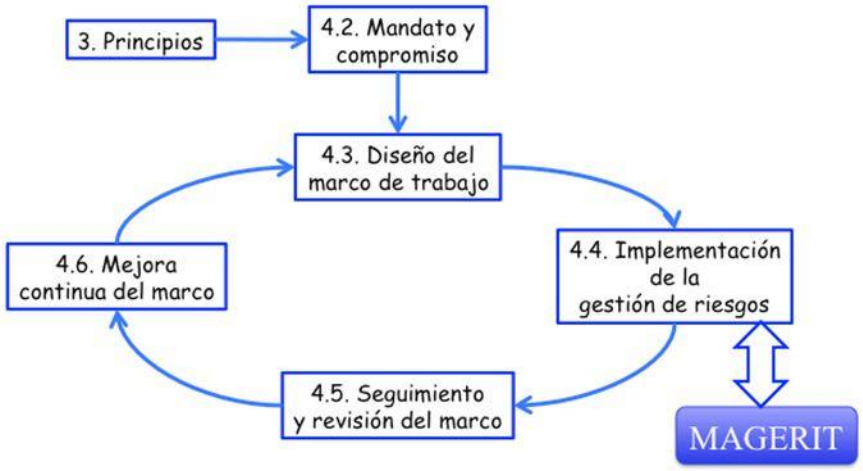

Figura 1 ISO 31000 - Marco de trabajo para la gestión de riesgos

Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información, Tomada de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" 2022, https://administracionelectronica.gob.es/

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, considerada la piedra angular para controlar todas las actividades

relacionadas con la seguridad de la información lo que permite es identificar y evaluar las amenazas y vulnerabilidades que pueden afectar a los activos informáticos.

Los sistemas de gestión de la seguridad de la información (ISO 27001) determinan cuatro etapas cíclicas que se conocen como el Proceso de Ciclo de Mejora Continua.

Ciclo de Mejora Continua: El ciclo de Deming es un proceso repetitivo en el cual se promueve la mejora continua, medición y revisión para lograr su optimización y mejora. Comprende cuatro etapas: Planear (Plan), Hacer, (Do), Verificar (Check) y Actuar (Act), de ahí que se conoce como PDCA (por sus siglas en inglés) o como el Ciclo Deming.

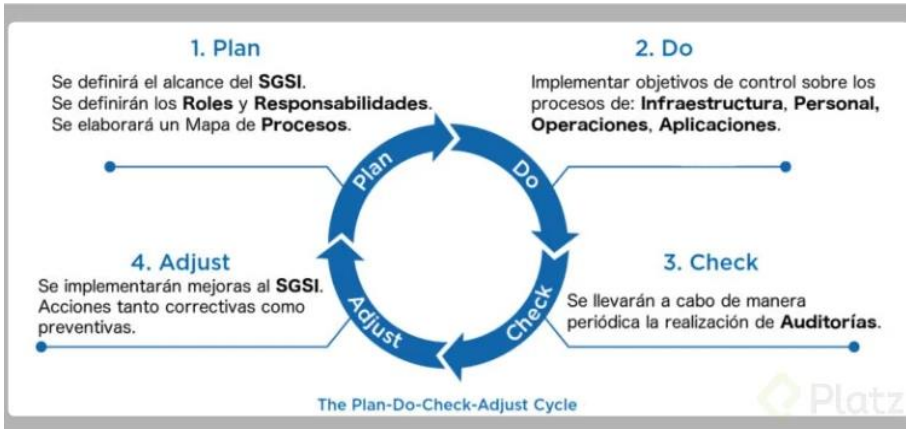

Figura 2 Modelo PHVA Norma ISO 27001:2013 Tomada de clases/1889-iso/28231-terminos-y-definiciones, 2022, https://platzi.com

2.2.5 Valoración de activos de información.

La valoración de los activos es una actividad estratégica para la Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el área de Captaciones de la Cooperativa de Ahorro y Crédito “Tulcán Ltda.”, puesto que determina la criticidad de los activos y finalmente cómo estos deben ser utilizados en los procesos de esta institución financiera, la misma que define los roles y las responsabilidades que tiene el personal sobre los mismos reconociendo sus niveles de Confidencialidad, Integridad y Disponibilidad. Para esta valoración resulta relevante mencionar que el primer paso en la evaluación de riesgos es la: identificación, clasificación y valoración de los activos de información.

2.3 Clasificación de los activos.

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, entre otros.

Los activos de información serán clasificados según la siguiente tabla de datos:

a) **Confidencialidad:** En base a un marco legal que regule y aplique para los procesos donde se encuentren involucrados los activos de información, se establece para que roles, funcionarios o grupos tengan autorizado o no su acceso, y que impacto tendría el incumplimiento de esta condición. Es decir que es una condición que indica que el activo sólo sea accedido por las personas, los procesos o entidades que se encuentran autorizadas y con las apropiadas autorizaciones.

b) **Integridad:** Se establece el efecto de la alteración no autorizada para los datos del activo de información, el impacto que tendría en el proceso en el que se encuentra involucrado; y a la vez las consecuencias que tendría para la organización. Se convierte en una condición de seguridad que garantiza que la información puede ser alterada, incluyendo su creación y borrado, solo por las personas autorizadas.

c) **Disponibilidad:** Significa, garantizar que la información solo sea accesible para las personas autorizadas, se mantenga protegida contra accesos no permitidos en donde los datos sensibles de la cooperativa como los de los socios y sus transacciones, están resguardados para evitar filtraciones, fuga de información, o mal uso.

2.3.1 Requisitos de seguridad para garantizar la calidad de los activos de información.

Una adecuada gestión de los activos de información comienza con el inventario de los activos, esto es identificarlos correctamente para saber con qué activos cuenta la organización; además tomando en cuenta lo que dice la norma ISO 27001:2013, es importante clasificarlos y valorarlos según su criticidad.

Para realizar el inventario de activos es recomendable definir unos elementos claves que ayudarán a su gestión, por ejemplo:

- Proceso
- Subproceso

- Actividad
- Activo
- Descripción del activo
- Categoría del activo
- Custodio del activo
- Criticidad: Disponibilidad, Integridad, Confidencialidad.

Contar con este inventario de activos: claro, detallado, organizado y actualizado permite realizar una mejor gestión de los riesgos y amenazas a los que están expuestos, como pueden ser: daños o alteraciones, pérdidas, destrucción lógica, destrucción física, hackeo, secuestro de datos o eliminación (Escuela Europa Excelencia, 2025).

Para la gestión de estos riesgos hay que tener en cuenta datos como: nombre del riesgo, calificación de la frecuencia y el impacto, descripción, proceso y activo asociado, criticidad, gestión que incluye el tratamiento de los riesgos a través de controles que ayuden a mitigar su probabilidad de ocurrencia y su impacto, así como la definición y creación de planes de acción con actividades y responsables específicos.

Para llevar a cabo la gestión de los activos de información y sus riesgos de manera eficiente, una buena práctica es apoyarse en herramientas tecnológicas que faciliten esta labor, reduciendo la operatividad y así mismo, las imprecisiones o errores que se puedan llegar a cometer.

2.3.2 Amenazas en Seguridad Informática.

A medida que las empresas dependen cada vez más de su infraestructura, su exposición a las amenazas cibernéticas se expande. La introducción de la computación en la nube, los dispositivos móviles, el internet y otros dispositivos han creado numerosos riesgos potenciales mediante los cuales un actor de amenazas cibernéticas puede atacar a una organización.

Como resultado, el panorama de amenazas se ha expandido significativamente. Los principales tipos de amenazas de ciberseguridad a las que se enfrentan las empresas hoy en día incluyen malware, ingeniería social, exploits de aplicaciones web, ataques a la cadena de suministro, ataques de denegación de servicio y ataques de intermediario. (Check, 2024)

Malware: Software malicioso que se ejecuta sin autorización del usuario y que perjudica el sistema o al usuario. El malware generalmente puede dañar, alterar o destruir computadoras y sistemas informáticos, este tiene varias características: se ejecuta de manera discreta sin autorización del usuario, ejecuta funciones perjudiciales para el usuario o el sistema se aprovecha de las vulnerabilidades del software infectando computadoras a través de sitios web. Algunos de los tipos de malware más comunes incluyen:

1. **Ransomware:** Es un tipo de malware o código malicioso que cifra los archivos imposibilitando la utilización de los equipos o sistemas que infecta, el operador del ransomware toma el control del equipo o sistema infectado y lo secuestra de varias maneras cifrando la información, bloqueando la pantalla. El usuario se convierte en víctima de una extorsión y para recuperar el normal funcionamiento del dispositivo o sistema se le pide un rescate económico.
2. **Caballo de Troya:** El malware troyano es un software malicioso que se disfraza de programa legítimo, este tiene como finalidad engañar a los usuarios para que sean ejecutados en sus sistemas, una vez descargado y ejecutado este troyano ejecuta su funcionalidad maliciosa interrumpiendo sistemas, robando datos e instalando puertas traseras.
3. **Spyware:** Código diseñado para infiltrarse en un dispositivo sin el conocimiento ni la autorización del usuario, este tipo de software tiene el propósito de recopilar información sensible y enviarla a terceros, su característica principal es de recolectar datos como: credenciales de acceso, historial de navegación, información financiera, registros de teclado e incluso grabaciones de audio o video en algunos casos.

   Este software puede instalarse a través de diversas técnicas como: descargas no autorizadas, en adjuntos de correos electrónicos fraudulentos, aplicaciones aparentemente legítimas, software desactualizado y vulnerabilidades en el sistema operativo.

   El impacto de este código va desde el robo de identidad, el espionaje, fraude financiero y la violación de la privacidad; para mitigar estos riesgos, es

fundamental contar con buenas prácticas de ciberseguridad, software de seguridad actualizado y evitar descargas de fuentes no confiables.

4. **Ingeniería social:** Los ataques utilizan trucos, coerción y otras formas de manipulación psicológica para lograr que el objetivo haga lo que el atacante quiere. Algunos ejemplos de tácticas comunes de ingeniería social incluyen:
    a. **Phishing:** Los ataques de phishing utilizan técnicas de ingeniería social para intentar engañar al destinatario para que realice una acción que beneficie al atacante. Los mensajes de phishing (enviados por correo electrónico, redes sociales, aplicaciones de comunicaciones corporativas u otras plataformas de mensajería) generalmente están diseñados para engañar a un objetivo para que haga clic en un enlace malicioso, abra un archivo adjunto malicioso o entregue información confidencial, como credenciales de inicio de sesión.
5. **Inyección SQL:** Técnica que permite al atacante inyectar código SQL malicioso en una aplicación web para manipular la base de datos, el atacante atacante puede utilizar la inyección SQL para robar información confidencial, modificar datos o incluso obtener acceso al servidor de la base de datos.
6. **Ataques DoS:** Estos ataques de denegación de servicio (DoS) están diseñados para interrumpir la disponibilidad de un recurso o servicio, los atacantes inundan el servidor con solicitudes de tráfico, lo que hace que el servidor se sature y deje de responder a las solicitudes legítimas.
7. **Explotación de vulnerabilidades:** Es el uso de código malicioso para aprovechar una debilidad en un sistema informático o en una red, esto puede permitir a los atacantes obtener acceso no autorizado a los datos, sistemas o daño a la imagen de una organización existen varios tipos de explotación de vulnerabilidades: de aplicación; relacionadas con errores de programación, de red; debido a la mala configuración de protocolos, firewall y servicios en la infraestructura, de servidor; relacionada con la mala configuración, de software y hardware.

2.3.3 Estándares de seguridad

Son técnicas generalmente establecidas que buscan proteger el entorno cibernético de una organización, ambiente que incluye a los usuarios, dispositivos, redes, procesos, software, información almacenada o en tránsito, aplicaciones, servicios y sistemas que se conectan de manera directa o indirecta a la red.

Norma ISO 27001. La norma ISO 27001 según el portal AqaEcuador (2022) es parte de la familia de normas ISO / IEC 27000, que es un conjunto de estándares realizados por ISO (Organización Internacional de Normalización o Estandarización) o IEC (Comisión Electrotécnica Internacional), centrados en ayudar a las organizaciones a mantener seguros los activos de información de sus empresas, ya sean estas grandes o pequeñas.

Las normas ISO 27000 permiten a las organizaciones gestionar los riesgos de seguridad de la información tales como: información financiera, propiedad intelectual, detalles de los empleados o información que le haya sido confiada por terceros ("ISO/IEC 27001 Information security management" 2018).

La familia de normas ISO 27000 consta de 39 normas, de manera particular para el sector financiero (EGS , 2024). Se pondrá énfasis en tres de ellas la ISO 27001, ISO 27002 e ISO 27015.

La norma ISO 27001, también es una norma nacional aprobada por el INEN con el nombre: NTE INEN-ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información – requisitos; esta es una norma certificable como empresa y/o como proceso, para garantizar la seguridad de la información en una empresa (INEN 2017a,1).

Norma ISO 27002. La norma ISO 27002, que también consta como norma nacional con el nombre: NTE INEN-ISO/IEC 27002:2013, código de práctica para los controles de seguridad de la información, establece las directrices para la seguridad de la información en las organizaciones, así como las prácticas de gestión de seguridad de la información incluyendo: la selección, la implementación y la gestión de los controles; todo esto siempre teniendo en consideración el entorno de riesgos de seguridad de la información de la organización que la está adoptando (INEN 2017b, 1).

Norma ISO 27015. Según el portal PMG (2024) La norma ISO 27015 tiene como nombre: Directrices de gestión de seguridad de la información para los servicios financieros, también ha sido adoptada por el INEN como normativa nacional; esta tiene la particularidad

de complementarse y sumarse a los controles de seguridad de la información definidos en la norma ISO 27002, para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros (INEN 2016a, 1).

Uno de los principales objetivos de la ISO 27001 es alinearse al propósito del negocio cubriendo el eje de seguridad de la información, independientemente del tamaño de la empresa o industria; esto se lo consigue con la implementación de un Sistema Gestor de Seguridad de la Información, sus siglas SGSI, cuyo principal propósito es disminuir la posibilidad de ocurrencia de un incidente de seguridad de la información, y, en caso de que el incidente acontezca, permitir la minimización del impacto en la operación de la empresa.

El Sistema Gestor de Seguridad de la Información (SGSI) permite a una empresa o industria, el mejoramiento de la postura de seguridad digital, una mayor claridad en la inversión en seguridad de la información, un aumento de la credibilidad dentro de su segmento de acción, así como la gestión del riesgo desde la perspectiva de la seguridad de la información.

La norma ISO 27001 es una norma técnica, que no solo se aplica a los procesos de las empresas de tecnología, sino también a los activos y procesos tecnológicos relacionados al núcleo de cualquier tipo de negocio, de cualquier empresa o industria; de esta manera se podrán considerar enfoques diferentes, de acuerdo con el giro del negocio, para lograr los procedimientos seguros y obligatorios para todas las actividades de gestión de la seguridad de la información. (INEN 2017a, 2).

La norma ISO 27001 considera dentro de la planificación de la seguridad de la información, la necesidad de definir dónde se encuentra la responsabilidad de seguridad de la información dentro de la organización, para que los comités y los órganos de revisión estén en un lugar administrativamente adecuado para cumplir y satisfacer los requerimientos del Sistema Gestor de Seguridad de la Información (SGSI).

La norma ISO 27001 exige que los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes de seguridad de la información, sus responsabilidades y compromisos, también asegura que estén equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal y para reducir el riesgo.

Según (Lopez, 2005) se debe proporcionar un nivel adecuado de conocimiento, educación y capacitación a todos los empleados, contratistas y usuarios de terceros, en

procedimientos de seguridad y uso correcto de las instalaciones, así como en el procesamiento de la información, todo esto enfocado a minimizar los posibles riesgos de seguridad. Se debe establecer un proceso disciplinario formal para manejar infracciones de seguridad.

La norma ISO 27001 acoge el modelo "Planificar, Hacer, Verificar, Actuar" (PHVA), que se emplea para estructurar todos los procesos del SGSI, según se puede apreciar en el siguiente gráfico, en el que se ilustra cómo un Sistema de Gestión de Seguridad de la Información (SGSI), toma como entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen con esos requisitos y expectativas.

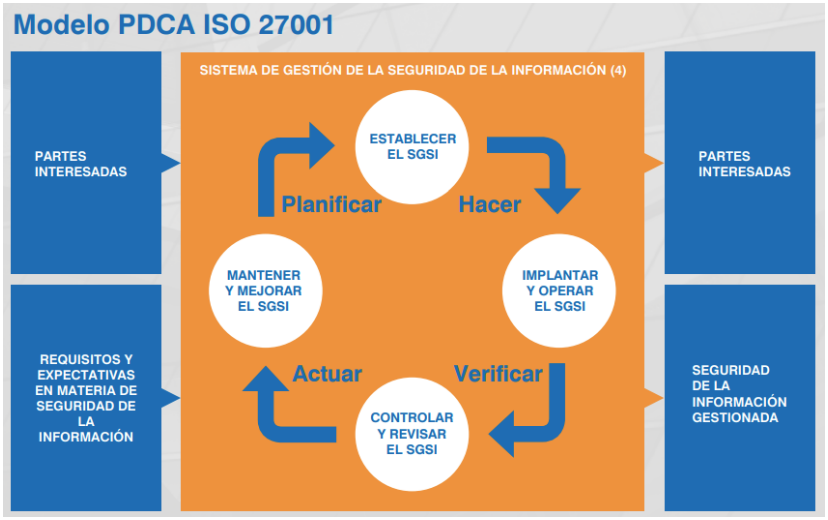

Figura 3 Modelo PHVA para ISO 27001 Modelo PHVA Norma ISO 27001. Tomada de clases/1889-iso/28231-terminos-y-definiciones, 2022, https://platzi.com

2.3.4 Riesgos.

En la era de la información y la digitalización, la seguridad de la información se ha convertido en un aspecto crítico para las organizaciones en todos los sectores, la protección de los activos de información contra amenazas y riesgos se ha vuelto fundamental para garantizar la continuidad del negocio, preservar la confianza de los clientes y cumplir con las regulaciones y normativas aplicables, en este contexto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se ha convertido en una estrategia esencial para las organizaciones que buscan fortalecer su seguridad y mitigar los riesgos asociados con la gestión de la información.

Identificar los riesgos. La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información para establecer y mantener los criterios de riesgo del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo criterios de aceptación del riesgo, criterios para realizar evaluaciones de riesgos de seguridad de la información, asegurar que las evaluaciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y resultados comparables. De igual manera identificar los riesgos del Sistema de Gestión, aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información en el ámbito del Sistema de Gestión de Seguridad de la Información (SGSI).

Analizar y evaluar los riesgos. Es fundamental investigar y analizar los diferentes riesgos que pueden suscitarse y que afecten los procesos que se llevan a cabo en la institución, y más aún si dichos procesos cuentan con información relevante.

El objetivo del análisis de riesgos es determinar si un riesgo es aceptable o quebranta las normas institucionales, para lo cual se definirá una metodología a través de la cual se analizará y evaluará los riesgos existentes. Dicha evaluación se basa en un método cualitativo en la que se detallan los activos de la institución, se identifican las amenazas relacionadas con cado uno de ellos y la posibilidad de que dichas amenazas se cumplan (Turner, 2024).

2.3.5 Marco legal

2.3.6 Constitución de la República del Ecuador

En la Carta Magna se establece de manera clara la organización del estado y los derechos de las personas. **Art. 66.- Se reconoce y garantizará a las personas:** "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información (Asamblea Constituyente , 2008).

2.3.7 Ley de Protección de Datos Personales (LOPDP)

Ámbito de aplicación integral:

Art. 1.- ***Objeto y finalidad.*** El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Art. 37.- ***Seguridad de datos personales.*** El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales (Asamblea Nacional d. E., 2021).

2.3.8 Código Orgánico Integral Penal (COIP)

En el Código Orgánico Integral Penal se destacan principalmente, dos artículos: **Art. 178.- Violación a la intimidad.** Establece sanciones para quien, sin autorización, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, vulnerando la privacidad de la información.

Art. 230.- Interceptación ilegal de datos. Tipifica los delitos informáticos, entre los que se incluyen conductas como el acceso no autorizado a sistemas informáticos, la manipulación, alteración o destrucción de datos, lo que afecta directamente la seguridad de la información (Asamblea Nacional, 2021).

2.3.9 Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (Ley SNDP)

En la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos se debaten temas de seguridad de la información en los siguientes artículos:

Art. 4.– Responsabilidad de la información. Establece que las instituciones tanto públicas como privadas que administran bases o registros de datos públicos son responsables de la integridad, protección y control de la información. Es decir, garantizan la veracidad, autenticidad, custodia y conservación adecuada de los datos.

Art. 26.– Seguridad. Aquí se dispone que toda base de datos informática debe contar con un archivo de respaldo y cumplir con los estándares técnicos y un plan de contingencia que evite la caída del sistema, el robo, la modificación o cualquier alteración que pueda afectar la información pública.

De igual manera en algunos documentos se hace mención al Artículo 6.- "Accesibilidad y confidencialidad, que establece que los datos de carácter personal como, por ejemplo: información íntima, de salud, son confidenciales y solo podrán ser accesibles con autorización expresa del titular, por mandato legal o mediante orden judicial" (Asamblea, 2017)."

2.3.10 Regulaciones de la Superintendencia de Economía Popular y Solidaria (SEPS)

Norma de control respecto a la Seguridad de la Información en las entidades del Sector Financiero, Popular y Solidario bajo control de la SEPS, **Art. 2.- "Objeto.** La presente norma tiene como objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas deben definir e implementar con el fin de resguardar y proteger sus activos de información preservando su confidencialidad, disponibilidad e integridad." (Margarita, 2022).

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Enfoque y Tipo de Investigación

Para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) y para profundizar en la valoración y determinación de los riesgos, se requiere aplicar una combinación de métodos de investigación cuantitativos y cualitativos (Hernández , Férnandez, & Baptista , 2014), situación que nos convoca a obtener una comprensión más completa de los aspectos técnicos y humanos relacionados con la seguridad de la información. Por lo manifestado en líneas anteriores, se describen brevemente ambos enfoques:

3.1.1 Método Cuantitativo:

Se centra en la recopilación y el análisis de datos numéricos para obtener conclusiones objetivas y medibles, en el contexto de un SGSI este enfoque implica el uso de métricas y mediciones para evaluar aspectos específicos de la seguridad de la información.

Algunos ejemplos de métodos cuantitativos en esta investigación incluyen:

1. **Análisis estadístico:** Recopilación de datos numéricos sobre incidentes de seguridad, vulnerabilidades, tiempos de respuesta, entre otros. Permite realizar análisis estadísticos para identificar patrones, tendencias y correlaciones.
2. **Encuestas estructuradas:** Se pueden recopilar datos cuantitativos sobre la percepción de los trabajadores, socios o clientes con respecto a la seguridad de la información; estas encuestas pueden incluir preguntas de opción múltiple o escalas de calificación para obtener datos cuantificables.
3. **Evaluación de riesgos** cuantitativos: Se pueden utilizar métodos cuantitativos, como el análisis de costo beneficio o el análisis cuantitativo del riesgo para evaluar los riesgos asociados con los activos de información y determinar la prioridad de los controles de seguridad.

3.1.2 Método Cualitativo:

Enfocado en la comprensión profunda y en la interpretación de los fenómenos a través de descripciones detalladas, narrativas y análisis subjetivos, en el contexto de un Sistema de Gestión, este enfoque permite explorar las percepciones, actitudes y comportamientos de las personas involucradas en el sistema de seguridad de la información. Algunos ejemplos de métodos cualitativos relevantes para esta investigación son:

1. **Entrevistas en profundidad:** Las entrevistas cualitativas permiten recopilar información detallada sobre las experiencias, conocimientos y opiniones de los participantes clave, como el

personal de seguridad, los gerentes o los usuarios finales. Estas entrevistas pueden proporcionar perspectivas ricas y contextualizadas sobre los desafíos y las prácticas de seguridad.

2. **Grupos de discusión:** Los grupos de discusión cualitativos reúnen a un grupo de personas con experiencia en seguridad de la información para debatir temas específicos. Esto permite obtener una comprensión más amplia de las percepciones colectivas, las normas sociales y las dinámicas grupales relacionadas con la seguridad.

3. **Análisis de documentos y políticas:** El análisis cualitativo de documentos, como políticas de seguridad, informes de incidentes o comunicaciones internas, ayuda a comprender los enfoques y las prácticas existentes en materia de seguridad de la información. Este análisis puede revelar brechas, desafíos y oportunidades de mejora.

La combinación de métodos cuantitativos y cualitativos en la investigación de un SGSI nos permite obtener una visión completa y equilibrada de la seguridad de la información, abordando tanto los aspectos técnicos como los humanos involucrados en el sistema. Esta aproximación multidimensional ayuda a comprender mejor los desafíos, identificar soluciones efectivas y tomar decisiones informadas para fortalecer la seguridad de la información en la organización.

3.2 Procedimiento de investigación

Fase 1: Inventario de activos

El propósito de haber realizado el levantamiento del inventario de activos, fue recopilar información relevante que me ha permitido describir de manera plena los activos institucionales, de tal forma, que, al realizar una consulta, ésta refleje la condición real del bien (Cooperativa de Ahorro y Crédito Tulcán, 2024), de manera que permita la toma de decisiones pertinentes para el caso; para la ejecución de esta actividad se ha realizado un trabajo en diferentes etapas, las mismas que me permito detallar a continuación:

Planificación: Se ha definido el alcance y los objetivos del inventario de activos determinando qué activos se debe incluir en el inventario como: elementos físicos, software, documentos, servicios, personas, instalaciones, hardware, todos aquellos activos que generan valor en la organización, levantamiento de información realizada de manera manual con el apoyo del personal encargado del área tecnológica y de captaciones.

Recopilación de información: Constatación física realizada en el área para recabar toda la información relevante sobre los activos que se incluirán en el inventario. Para la ejecución de esta actividad se ha presentado la matriz, a los funcionarios del área de

Captaciones, con los campos a ser llenados de cada activo. Específicamente se ha dado importancia a las características como: nombre del activo, número de serie, descripción, ubicación, estado, valor y cualquier otra información útil que se ha podido identificar.

Con los pasos realizados anteriormente, se ha logrado conseguir la actualización del inventario de los activos documento impregnado en formato digital, actividad que nos ha ayudado a identificar de manera general los activos que dispone la Cooperativa de Ahorro y Crédito "Tulcán Ltda.".

Fase 2: Clasificación de activos

Se ha realizado la clasificación y valoración de los activos, proceso crucial que ha ayudado al área tecnológica y a la organización a determinar el valor de los activos existentes, proceso que ha servido para determinar el valor actual de un activo, ya sea tangible o intangible. Una vez que se ha efectuado esta clasificación y valoración, se ha comprendido el valor de cada uno de los activos para en lo posterior tomar decisiones informadas basadas en la información obtenida, esto implica analizar varios factores que contribuyen al valor del activo.

Fase 3: Valoración de riesgos

Se han aplicado actividades documentadas para establecer los principios, objetivos y directrices generales para garantizar la seguridad de la información a nivel de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", el objetivo de esta valoración ha sido identificar y posteriormente designar responsabilidades claras y específicas a cada uno de los custodios responsables de la gestión de seguridad de la información y más usuarios que hacen uso de la información.

Fase 4: Evaluación del sistema de Gestión de Seguridad

Para la evaluación del Sistema de Gestión de Seguridad de la Información (SGSI) se han ejecutado actividades preliminares coordinadas con diferentes áreas a fin de comprobar el desempeño, rendimiento o efectividad de la implementación del SGSI, actividad ejecutada en el edificio Matriz de la Cooperativa "Tulcán Ltda.", evaluación realizada para obtener una visión objetiva de los resultados de la implementación con acercamientos con el personal del área de auditoría interna para revelar el cumplimiento de los requisitos de la norma de la seguridad de la información.

Definir el alcance del SGSI. Ha sido determinado de acuerdo a las características que se tienen en la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", siendo éstas las que cubren cada uno de los aspectos involucrados tales como: recursos, activos, procesos, etc.

La definición del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) es una de las más importantes decisiones en todo el proceso de esta Entidad Financiera.

Su magnitud está en la decisión de la autoridad general de la entidad financiera y sus cuerpos colegiados.

Con el crecimiento tecnológico en las organizaciones, el procesamiento de la información a través de las plataformas digitales, cada vez se incrementa debido al uso masivo por parte de las personas, quienes actualmente utilizan estos medios como una nueva cultura para gestionar las transacciones financieras en la medida en que lo requieren.

Esto ha demandado a las organizaciones a disponer de todas las garantías que permitan procesar las transacciones de manera segura y confiable apoyadas en procesos y normas de seguridad internacionales para garantizar la confidencialidad, disponibilidad e integridad de la misma.

En este caso, las organizaciones del sector financiero y sus activos de información ya sean estos físicos o digitales, enfrentan creciente y constantes amenazas que buscan comprometer su integridad y funcionamiento, entre estas se encuentran fraudes asistidos por dispositivos informáticos, espionaje, sabotaje, vandalismo, fenómenos naturales, descuido, desconocimiento o mal uso del tratamiento de la información por parte de las personas. Muchas de las amenazas provienen de ingenieros sociales, hackers, empleados desvinculados, errores operativos, entre otros, que buscan dañar la integridad de una organización.

Por ello la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Cooperativa de Ahorro y Crédito “Tulcán Ltda.” permitirá establecer de forma integrada las medidas de protección asegurando la identificación, valoración y gestión de los activos de información y los riesgos asociados en función del impacto que representen para la organización en los diferentes entornos operativos ya sean estos físicos o digitales a través del uso de los sistemas de información digital, mitigando las posibles vulnerabilidades que pudieren existir dentro de la organización, entorno a la gestión de la información y la infraestructura utilizada para el mismo fin.

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) puede ser aplicado a toda la organización, parte de ella, o simplemente un proceso o un sistema de información, poniendo mayor énfasis a los temas que a continuación se detalla:

Control de activos. Implementar un control efectivo de todos los activos con los que cuenta la cooperativa, contribuirá a una gestión más eficiente de la seguridad de la información, además establecer responsabilidades claras al personal que hace uso de cada una de los activos, abordando adecuadamente las vulnerabilidades y riesgos dentro de la institución financiera.

Control de recursos humanos. Un control adecuado y capacitaciones oportunas dentro de la institución financiera, así como el compromiso del recurso humano ayudará a que exista un mejor control de la seguridad de la información, como una mejor gestión en los recursos durante el periodo laboral o culminación del mismo.

Gestión de acceso. Un mejor control y una adecuada verificación previo a ingresar, así como el control de acceso a cualquiera de los recursos de la institución financiera ayudará a la integridad y confianza de la información.

Control de las operaciones y comunicación. Garantizar la comunicación y la funcionalidad de los sistemas de información, disponibilidad de servicios las veinte y cuatro horas ante cualquier eventualidad que pudiera suscitarse dentro de la institución financiera ya sea por factores externos o internos.

3.3 Consideraciones Bioéticas

Las Normas ISO, al ser consideradas un estándar internacional, que establecen los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información, nos deriva a no profundizar ni a enfocarnos en las consideraciones bioéticas por la aplicación de normativa y técnicas, tema que está más relacionado con aspectos técnicos y de seguridad informática en el ámbito cooperativo y financiero del país. No obstante, se puede considerar aspectos bioéticos de importancia relacionados con la seguridad de los datos, el impacto generado con los funcionarios, socios y clientes.

Seguridad de los datos. La implementación de un SGSI generalmente implica proporcionar capacitación y conciencia en seguridad de la información a los trabajadores, ayudando a aumentar su conocimiento sobre las amenazas y los riesgos de seguridad, permitiéndoles comprender cómo sus acciones pueden afectar la seguridad de la información de la Cooperativa. Los trabajadores se vuelven más conscientes de prácticas seguras, como el manejo adecuado de contraseñas, la navegación de páginas en internet, uso de redes seguras y la protección de la información confidencial.

Impacto generado con los funcionarios. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) puede influir en la cultura organizacional en lo que respecta a la seguridad de la información, esto va a fomentar una mayor conciencia y valoración de la seguridad en todos los niveles de la organización; los funcionarios empezarán a ver a la seguridad de la información como una responsabilidad compartida para adoptar prácticas seguras como parte de su cultura laboral.

Impacto con socios y clientes. El socio no percibe los cambios internos en aspectos tecnológicos, simplemente con el uso permanente y estable de los servicios en todos los canales que brinda la entidad cooperativa, siente confianza y estabilidad al transaccionar, situación que se generaliza con todas las personas que en la actualidad interactúan en las plataformas tecnológicas del sistema financiero nacional y mundial.

CAPÍTULO IV

4 DESARROLLO

4.1 Antecedentes de la Cooperativa

El objetivo principal de la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", es promover el bienestar financiero de sus socios mediante la presentación de servicios de ahorro, crédito y otros productos financieros accesibles según las aspiraciones económicas y sociales (Cooperativa de Ahorro y Crédito Tulcán, 2024).

4.2 Visión

Hasta el año 2024 consolidaremos la calificación de riesgos AA+ para ubicarnos entre las tres mejores cooperativas calificadas, con un crecimiento de al menos 40% en activos; salud financiera adecuada; satisfacción de nuestros socios y clientes e innovación tecnológica segura.

4.3 Misión

Somos una Institución de intermediación financiera, que brinda productos y servicios cooperativos con responsabilidad social, talento humano comprometido e infraestructura tecnológica; que promueve la inclusión financiera y el desarrollo sostenible de nuestros grupos de interés.

4.4 Estructura organizacional

Posterior a las entrevistas que se realizaron con los representantes de la entidad se facilitó el siguiente organigrama que se muestra continuación.

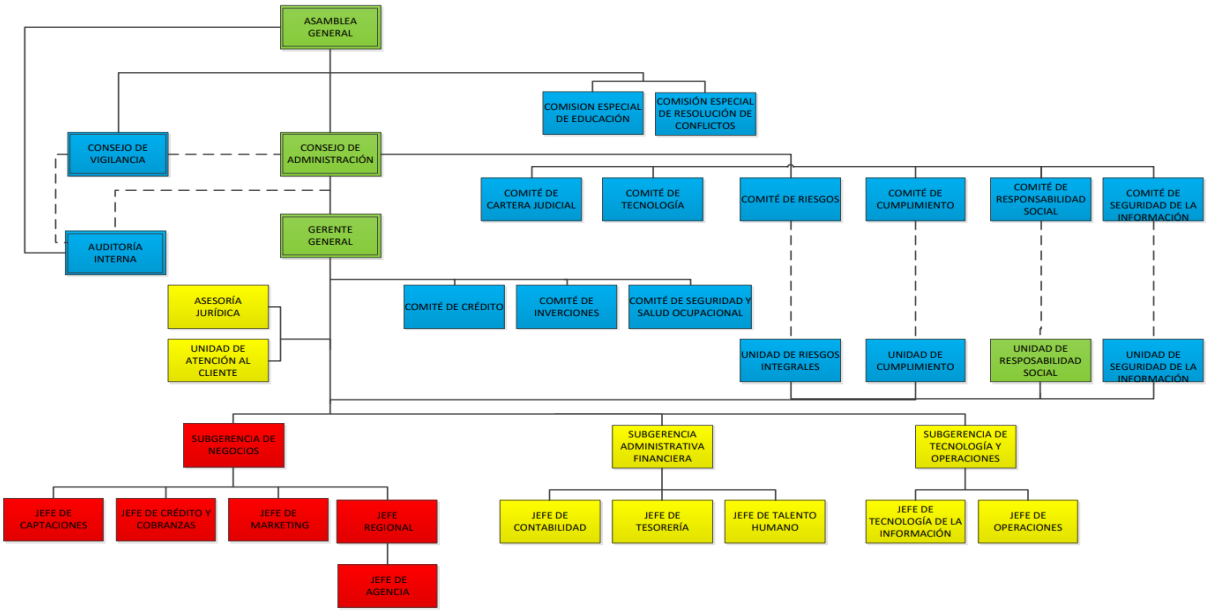

Figura 4 Estructura organizacional Cooperativa de Ahorro y Crédito "Tulcán Ltda."

4.4.1 Organigrama del Área de Captaciones.

La Cooperativa de Ahorro y Crédito "Tulcán Ltda.", presta servicios de índole financiera desde su edificio matriz en la ciudad de Tulcán, edificio ubicado en las calles Sucre y Atahualpa, que dispone de un área específica donde funciona el Área de Captaciones, espacio laboral asistido de dos funcionarios quienes realizan tareas de identificar y atraer nuevos clientes interesados en productos financieros como cuentas de ahorro, depósitos a plazo fijo y todo lo referente a inversiones de fondos. Entre las diferentes actividades que se realiza en el área se tiene:

- Elabora el plan operativo del área de captaciones, analizando los requerimientos de los socios, analizando los productos y servicios, para determinar los objetivos estratégicos del área de captaciones.
- Plantear estrategias y acciones encaminadas a mejorar las captaciones de ahorros a la vista, DPF, y servicios, con el fin de obtener la liquides necesaria.
- Realiza la promoción de productos y servicios financieros, visitando medios de comunicación, instituciones financieras, públicas, grupos organizados personas naturales, para captar nuevos socios o clientes

Desde este espacio se brinda, de manera permanente, soporte y cobertura a las 16 agencias ubicadas en las Provincias: Imbabura, Pichincha, Tungurahua, Chimborazo y Bolívar, y, por supuesto en Carchi, llegando con servicios financieros acorde a las tecnologías actuales.

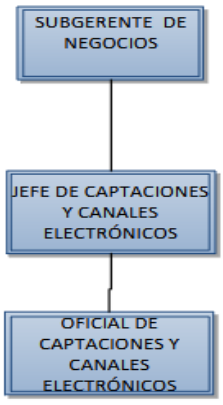

Figura 5 Organigrama del área de captaciones.

4.4.2 Estado actual de la seguridad

Para comprender el estado actual de la seguridad en la Cooperativa, con el objeto de determinar la situación que presenta la entidad frente a la implementación de un Sistema de Gestión de Seguridad de la Información basado en norma ISO/IEC 27001:2013.

En términos generales se pudo identificar los siguientes escenarios.

- La Cooperativa dispone un área de Seguridad de la Información para la implementación de controles de seguridad.
- Se cuenta con una intranet para la publicación de la Gestión documental de los diferentes procedimientos
- La Gerencia mantiene una cooperación y da la importancia necesaria de los procesos de seguridad.
- Existen controles mínimos para la gestión de administración de información física y digital (file de documentos de clientes, reportes, matrices de clientes).

Luego de haber realizado el análisis del estado de la situación actual de la seguridad de la información de la Cooperativa, a continuación, se presenta el detalle de los resultados para determinar el grado de cumplimiento con respecto a la norma internacional ISO/IEC 27001:2013.

Se evaluó cada uno de los requerimientos de los dominios de la norma y se asigna un 0% si no cumple y un 100% si cumple.

Con base en los resultados obtenidos a continuación, se presentan los resultados generales de cumplimiento de la norma ISO 27001:2013

Tabla 1 Requerimientos de los dominios de la norma

Dominio	Puntaje
4. Contexto de la organización	25%
5. Liderazgo	25%
6. Planificación	25%
7. Soporte	29%
8. Operación	0%
9. Evaluación del desempeño	13%
10. Mejoramiento	0%
PROMEDIO	***18%***

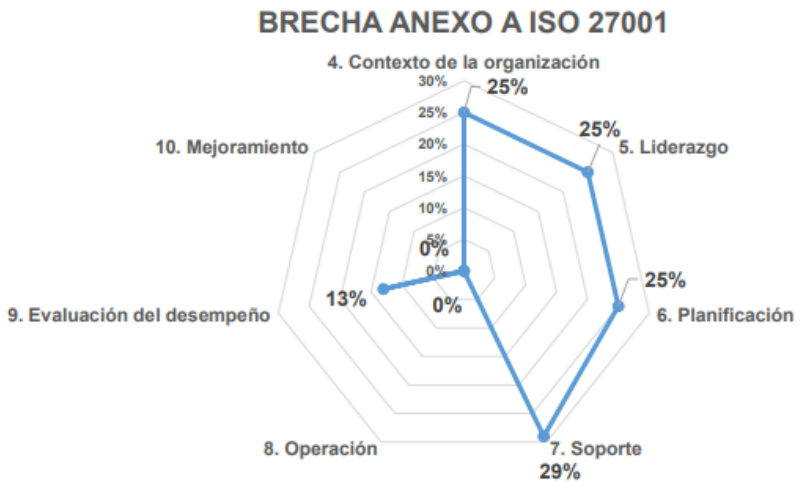

Figura 6 Brecha entre los requerimientos de los dominios de la norma

4.4.3 Estado actual de los Activos del Área de Captaciones

Con los datos obtenidos en la matriz de calor se generó los siguientes gráficos en los cuales se puede observar la distribución de riesgo en los activos que posee el área de Captaciones de la Cooperativa.

Tabla 2 Distribución de riesgos en los activos, área de Captaciones

TIPO ACTIVO	NRO. ACTIVOS
Actividades Procesos	**76**
Información	**11**
Instalaciones	**1**
Personas	**14**
Software	**47**
Total, general	**149**

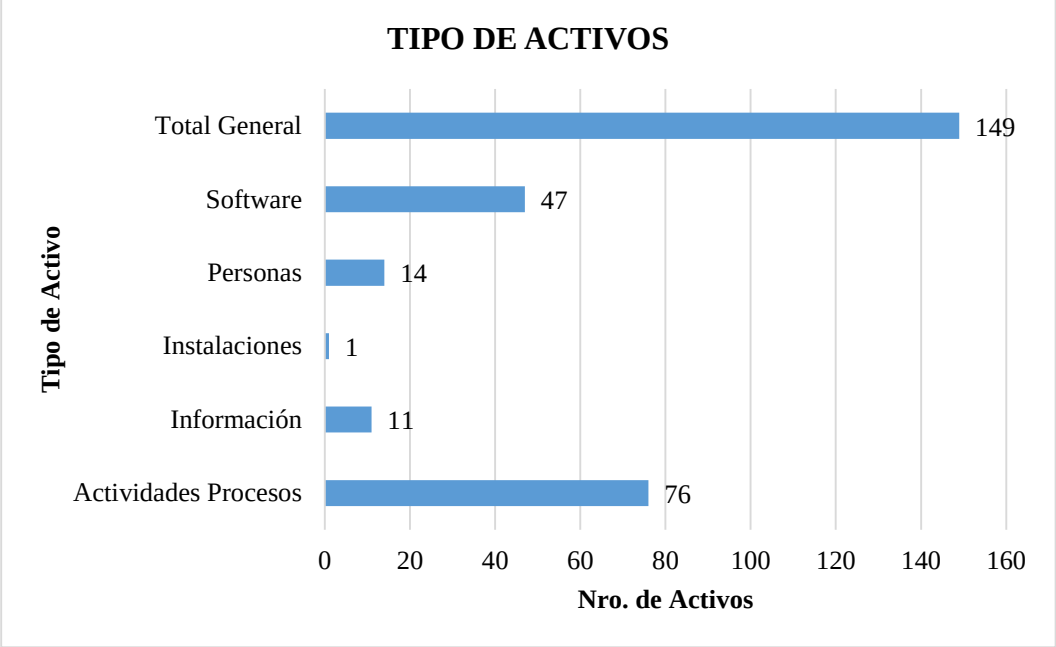

Figura 7 Distribución de riesgo en los activos, área de Captaciones

Detalle de análisis de los riesgos de los activos de información analizados

Se realizó el análisis inicial para identificar el riesgo inherente, es decir el que se concibe por la naturaleza de las actividades de los procesos que se realizan y que se evalúa antes de la aplicación de controles.

A continuación, el detalle del análisis realizado:

Captaciones

Tabla 3 Análisis inicial para identificación de riesgos

Vulnerabilidad	Nro. Activos
Acceso a sistema denegado	**2**
Demora en proceso operativo	**20**
Documentación falsa	**1**

Vulnerabilidad	Nro. Activos
Documentación errónea	**23**
Documentación no clasificada	**2**
Documento indisponible	**1**
Error en proceso operativo	**6**
Información errónea	**25**
Información no conocida por el cliente	**1**
Perdida de documentos	**9**
Recepción de documentos falsos	**6**
Registro de datos erróneos	**1**
Servicio Indisponible	**4**
Sistema financiero colapsado	**48**
Total General	**149**
Abuso de derechos	**2**
Ausencia de personal	**20**
Denegación del servicio por error	**3**
Falla del servicio	**1**
Falta de capacitación en procesos	**6**
Fuga de información por error	**3**
Hurto de medios o documentos	**9**
Ingreso de datos falsos	**6**
Modificación de la información	**27**
Modificación mal intencionada	**24**
Saturación del sistema de información	**48**
Total General	**149**

Tabla 4 Análisis Riesgo de activos

Riesgo	Nro. Activos
Alto	36
Bajo – Muy bajo	84
Medio	29
Total General	**149**

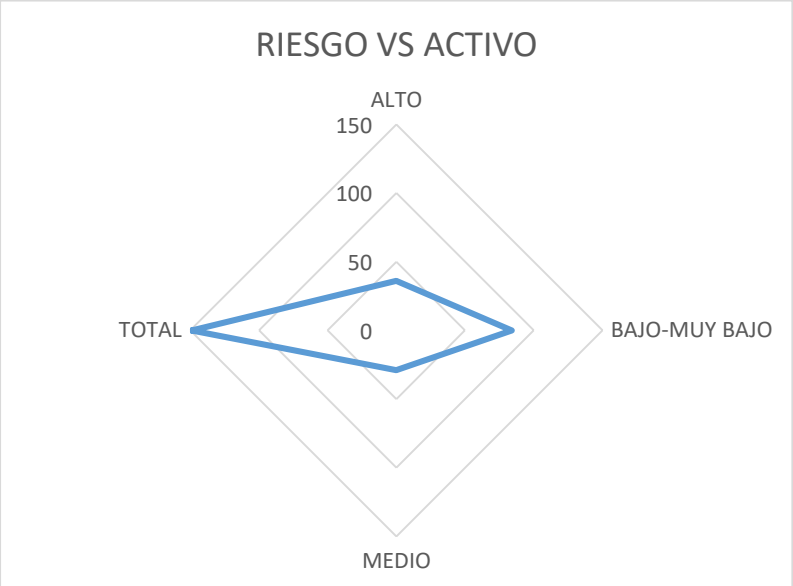

Figura 8 Evaluación de riesgo versus activo

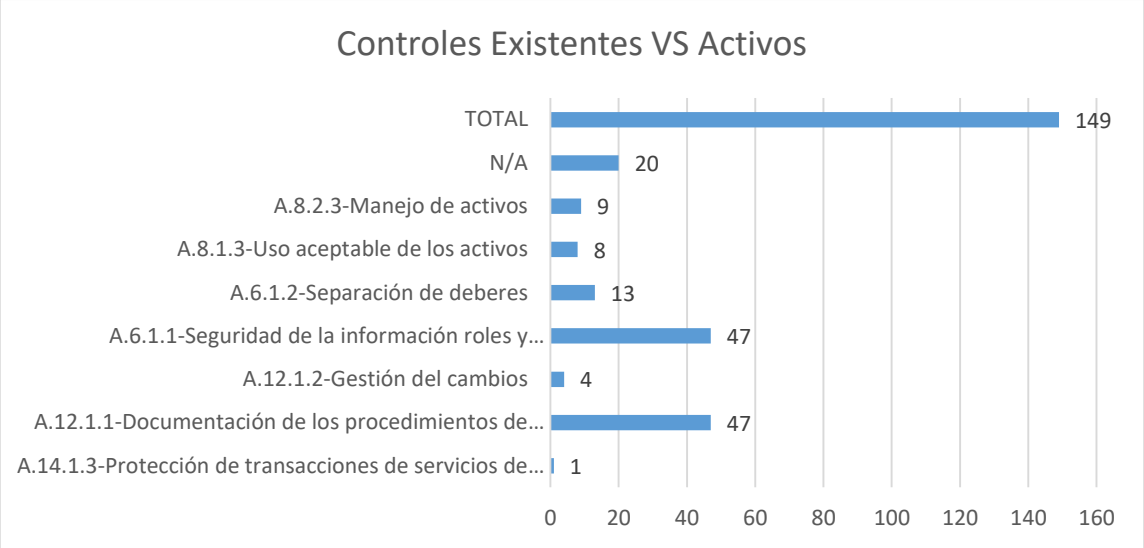

Figura 9 Análisis funciones de control existente para activos

4.5 Nivel de Cumplimiento Detallado – ISO 27002

Para la evaluación sobre los controles de seguridad de la información respecto de la norma internacional ISO/IEC 27002 se aplicó la siguiente nomenclatura de evaluación indicando que los porcentajes que se verifiquen corresponden a valores aproximados

Nomenclatura de evaluación	Porcentaje aproximado
	0% - 20%
	21% - 40%
	41% - 60%
	61% - 80%
	81%-100%

Figura 10. Nomenclatura necesaria para la evaluación

Para a medición de la efectividad de los controles de seguridad implementados se tomó como referencia la siguiente tabla de datos:

Efectivo	Efectivo No Formalizado	Inefectivo prueba	Infectivo diseño	Control No Existente
a) Control existente bien diseñado, ejecutado adecuadamente	a) Control existente bien diseñado, ejecutado adecuadamente	a) Control existente bien diseñado	a) Diseño del control existente, no permite mitigar adecuadamente el riesgo	a) No se ha diseñado algún control
b) Periodicidad establecida, minimizando exposición al riesgo	b) Periodicidad establecida, minimizando exposixión al riesgo	b) Formalizado en norma	b) Control débil, requiriendo acciones correctiva	b) El control diseñado falla continuamente, por tanto no mitiga el riesgo relacionado
c) Formalizado en norma	c) No formalizado	c) No es ejecutado adecuadamente: Falla en un número limitado de oportunidades y/o sin la periodicidad establecida		

Figura 11. Rangos de efectividad en los controles de seguridad implementados

Donde:

Efectivo= E, Efectivo No Formalizado

Inefectivo Prueba = IP

Inefectivo = ID

Control No Existente= CNE

Para la evaluación de la efectividad de los controles de seguridad se tomó en cuenta los literales de cada ítem de efectividad de la tabla de datos (Evaluación de efectividad).

Detalle de avaluación en los aspectos de la normativa ISO 27002:

Nivel de cumplimiento de la ISO 27002		
DOMINIO	**Estado**	**Efectividad**
Políticas de seguridad de la información	◑	**IP:a,b,c**
Organización de la seguridad de la información	◑	**IP: a,b,c**
Seguridad de los recursos humanos	◕	**ENF: a,b**
Gestión de activos	◔	**CNE:a**
Control de acceso	◕	**ENF: a,b**
Criptografía	○	**CNE: a**
Seguridad física y del entorno	◕	**IP: a,b,c**
Seguridad de las operaciones	◑	**ENF: a,b**
Seguridad de las comunicaciones	◕	**ENF: a,b**
Adquisición, desarrollo y mantenimiento de los sistemas	◕	**ENF: a,b**
Relación con proveedores	◕	**ENF: a,b**
Gestión de incidentes de seguridad de la información	◑	**CNE: a**
Seguridad de la información -continuidad de negocio	◑	**CNE: a,b**
Cumplimiento	◑	**CNE:a.b**

Figura 12 Aspectos de cumplimiento de la norma ISO 27002

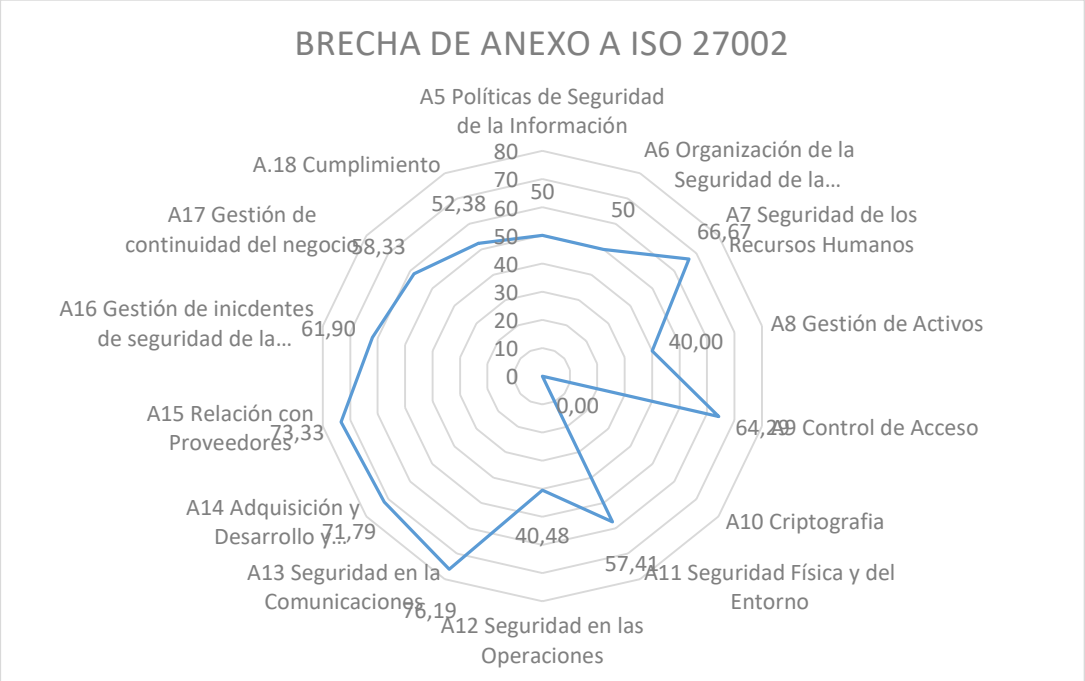

Figura 13 Relación entre los aspectos de cumplimiento de la norma ISO 27002

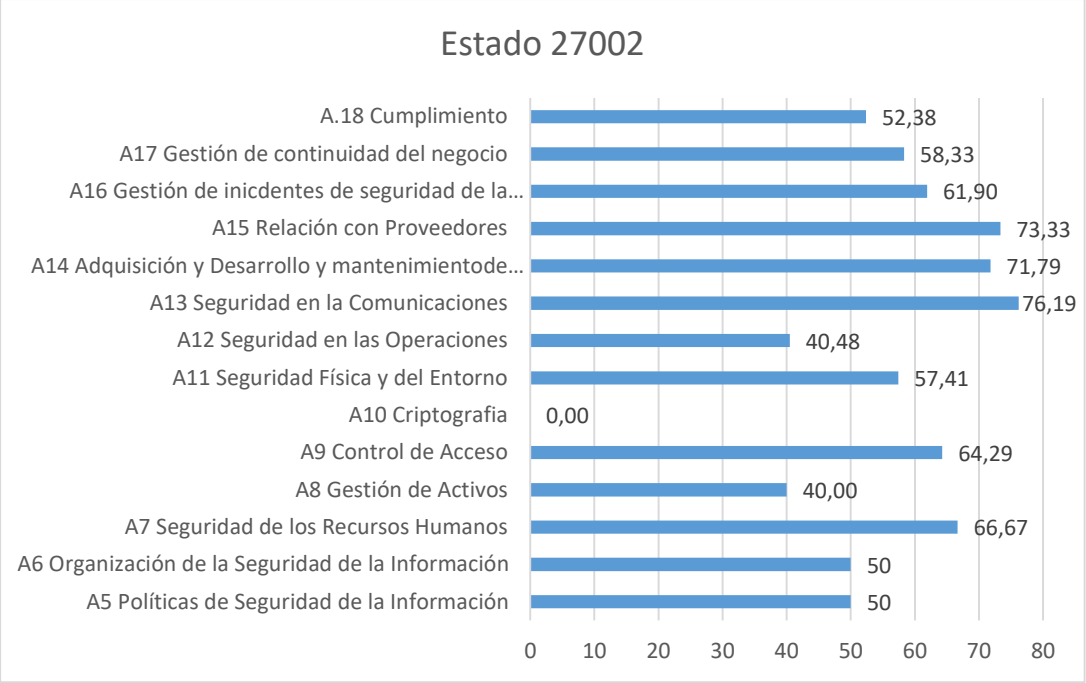

Figura 14 Madurez en aspectos de mejora

El nivel de madurez permite establecer las bases para la mejora continua del proceso de Seguridad de la Información de Cooperativa, e identificar las iniciativas de seguridad de la información, los cuales deberán estar alineadas al alcance de implementación del SGSI.

4.6 Diseño del sistema de gestión de seguridad de la información para el Área de Captaciones

4.7 Consideraciones Iniciales

Con el objetivo de determinar las partes interesadas, los requerimientos de este entorno a la implementación del Sistema de Gestión de Seguridad de la Información, en la Cooperativa se ha definido los siguientes grupos de interés los cuales se detalla a continuación.

4.8 Partes interesadas

- Comité de Seguridad de la Información
- Gerencia General
- Colaboradores
- Jefe de Seguridad de la Información.

4.9 Partes externas

- Superintendencia de Economía Popular y Solidaria SEPS
- Socios y Clientes

4.9.1 Recursos disponibles

Es la información que posee la cooperativa para el diseño del SGSI, como lo que se indica a continuación:

- **Procedimientos/Metodología/Instructivos/.** Es la línea que permitirá el desarrollo del SGSI, tomando en relación los incidentes de riesgos.
- **Apoyo de la Cooperativa.** Son todas las actividades y acciones por parte de la Cooperativa para la ejecución del SGSI
- **Documentación.** Son todos los datos proporcionados por la Cooperativa entre los cuales tiene:
    - Información de activos que tiene la Cooperativa.
    - Información de los eventos de seguridad de la información.
    - Información de vulnerabilidades y amenazas.

4.9.2 Metodología para la gestión de Riesgos

Luego de realizar el análisis de las diferentes metodologías existentes para la gestión de riesgos se llegó a determinar que para el caso de estudio aplicar en la "Cooperativa" se basara en la Metodología de MAGERIT (Análisis y Gestión de Riesgos de Seguridades de la Información), su enfoque está en la identificación, estimación y evaluación de los riesgos de seguridad de la información para definir un plan de tratamiento que se ajuste a los objetivos propuestos.

4.10 Inventario y Clasificación de Activos de Información

Un activo se considera a los elementos de una organización que se requieren para el correcto desarrollo de sus procesos, los cuales son objeto de análisis en la gestión de riesgos durante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa.

La protección de la información a los activos críticos y de alto valor para las organizaciones, se ha convertido en una actividad fundamental que se debe realizar con absoluta responsabilidad y conciencia, por lo cual es necesario definir una serie de medidas con base en los lineamientos definidos por la Alta Dirección o Gerencia, a través de la aplicación de la política de gestión de riesgos.

Esta fase del proyecto expone una guía para el Sistema de Gestión de Seguridad de la Información (SGSI) para la construcción y mantenimiento del inventario de activos, realizando la identificación, clasificación y valoración de los activos de información de Cooperativa "Tulcán Ltda.", con el fin de conocer el nivel de protección que debe ser aplicado frente a los

principios de disponibilidad, confidencialidad e integridad, alineados con las directrices y políticas de la Organización.

4.10.1 Identificación de los Activos de Información

La individualización de los activos de información de la Cooperativa en el área de Captaciones inicia con una revisión preliminar del listado de activos, objeto del alcance de este Proyecto. Se analiza el contexto de la Entidad, por medio de algunas entrevistas con los funcionarios responsables de los procesos, para analizar las actividades que definen los activos de información. Posteriormente se evalúa cada uno de los activos y su grado de impacto en la imagen de la Organización, la percepción de la Entidad en su propio entorno y la necesidad de tener siempre muy claro el concepto de imagen corporativa.

La información de los activos que será registrada en el inventario incluye:

Nº: Identificador del activo mediante un número secuencial para ordenar los activos de información.

Fecha actualización: Fecha en la cual se realiza el levantamiento de la información.

Proceso: Nombre del proceso agregador de valor.

Subproceso: Actividad operativa que se encuentra determinada en el flujo del proceso.

Activo: Nombre por el cual es conocido el activo según la actividad de proceso.

Ámbito: Grupo de los tipos de activos de información.

Descripción del activo: Descripción del activo de información en función de las actividades operativas del proceso.

Categoría: Clase donde se clasifica el activo de información.

Dependencias de activos: Cuando un activo dependa de otro para el procesamiento o alojamiento, esta casilla debe ser llenada para identificar dicho activo mencionándolo por su identificador (servidores de almacenamiento o procesamiento, equipos informáticos, equipos de comunicación, personas, sistemas de información, Internet, equipos de procesamiento de información y de servicios).

Entrada/ Salida/Otro

Entrada: Se lista todo aquel requerimiento de entrada necesario para la ejecución del proceso (las entradas pueden ser solicitudes, correos electrónicos, etc.).

Salida: Es el resultado obtenido luego de haber ejecutado el proceso en cuestión. Es posible que se tenga más de una salida en función de las actividades del proceso.

Otro: Son los activos de información que intervienen dentro del flujo del proceso como pueden ser: bases de datos, software de aplicación, equipos de cómputo, manuales, procesos, etc.

Tipo de activo

Tangible: Todo aquel activo que se encuentre físicamente disponible y sea palpable, como puede ser: guías y reglamentos, contratos, expedientes, notificaciones, papeles de trabajo, manuales de usuario, equipos de cómputo, servidores, discos ópticos, dispositivos magnéticos, etc.

Intangible: Todo aquel activo que no sea posible accederlo físicamente, como pueden ser: bases de datos, software de aplicación, software de sistema, correo electrónico.

Almacenamiento: Se especifica el nombre del lugar en donde es almacenado o resguardado.

Dueño del activo: Persona que actúa como dueño y responsable de la ejecución del proceso que determina las acciones que se realizan con el activo. Administra el inventario y clasificación del activo en función de su criticidad

Ejecutor el activo: Persona que ejecuta y da tratamiento a la información en función de las actividades del proceso.

Custodio del activo: Área donde reposa el activo de información.

Ubicación del activo: Sitio donde se encuentra alojado el activo de información para consulta o procesamiento del mismo.

Frecuencia de generación: Tiempo en el que el activo de información es generado o procesado.

Impacto:

Legal: Si el activo de información es comprometido o no se encuentra disponible.

Impacto Imagen: Si el activo de información se ve comprometido o no se encuentra disponible.

Impacto en la Pérdida de Confianza: Impacto en la pérdida de confianza ante el cliente, el contribuyente, empresas o instituciones con las cuales se intercambia información, por la imposibilidad para cumplir con los objetivos planteados si este activo de información se ve comprometido o no se encuentra disponible.

Disponibilidad: La importancia de la disponibilidad de los Activos de Información, se fundamenta en la importancia que esta tiene para la operación diaria, para su acceso por parte de los usuarios, contribuyentes, etc.

Integridad: En este criterio de clasificación, se debe evaluar el daño para la empresa causado por la pérdida de integridad de un activo de información (por ejemplo, equipos, sistemas o aplicaciones que parecen estar operando correctamente o información que es considerada correcta cuando no lo es).

Confidencialidad: Es la propiedad por la que se garantiza que la información es accesible solo al personal autorizado.

Importancia: La importancia de la disponibilidad de los Activos de Información, se fundamenta en la importancia que esta tiene para la operación diaria, para su acceso por parte de los usuarios, contribuyentes, etc.

Rango económico: Estimación cuantitativa del activo de información.

Agencia de acceso: Agencia donde pertenecen los usuarios funcionales que tiene acceso al activo de información.

4.10.2 Ámbito de los Activos de Información

Para iniciar con el inventario de los activos de información es importante determinar los tipos de activos de información que van a ser intervenidos.

Tabla 5 Ámbito de los Activo de Información (Autoría Propia)

ÁMBITO DEL ACTIVO	DESCRIPCIÓN
Actividades y procesos	Actividad específica para llevar a cabo una o varias actividades estrechamente relacionadas, que interactúan y que transforman elementos de entrada y los convierten en elementos de salida.
Información	Toda la información que sean de interés para la organización y que son indispensables para el cumplimiento de su misión y objetivos.
Instalaciones	Infraestructura física que soporta el funcionamiento de la entidad, por ejemplo, edificios, oficinas, muebles.
Hardware	Elementos y equipos electrónicos que soportan el procesamiento de la información
Software	Todos los aplicativos que contribuyen al procesamiento de la información, por ejemplo, sistemas operativos, herramientas de ofimática, aplicaciones del negocio, entre otras.
Redes	Abarca todos los equipos de telecomunicaciones usados para interconectar elementos y computadores físicamente separados en un sistema de información.
Personas	Consiste en todos los grupos de personas involucrados con el sistema de información, por ejemplo: los usuarios, personal de mantenimiento, desarrolladores, analistas, entre otros.

4.10.3 Clasificación de los activos de información

Tabla 6 Clasificación de los activos de información SGSI (Autoría Propia)

CRITERIO DE SEGURIDAD	DESCRIPCIÓN
CONFIDENCIALIDAD [C]	Con base en el marco legal y regulatorio que aplique para los procesos donde se encuentre involucrado el activo de información, se establece para que roles o funcionarios o grupos tengan permitido o no su acceso de lectura y que impacto tendría el incumplimiento de esta condición. Es decir que es una característica que indica que el activo sólo sea accedido por el personal, procesos o entidades que se encuentran autorizadas y con las autorizaciones adecuadas.
INTEGRIDAD [I]	Establecer cuál es el efecto de la modificación no autorizada de los datos del activo de información, que impacto tendría en los procesos donde se encuentra involucrado y a su vez que consecuencias tendría para la entidad. Es decir que es una condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, solo por el personal autorizado.
DISPONIBILIDAD [D]	Cuál es el efecto que se genera para la entidad cuando el activo de información no puede estar cuando se requiere; esto se determina por el tiempo que se puede esperar para que dicho activo de información pueda ser utilizado. Es una característica que indica que el activo debe ser oportuno, es decir que pueda ser consultado y usado por la persona, entidad o proceso cuando lo requiera.

4.10.4 Valoración de los Activos de Información

La valoración de los criterios para clasificar un activo de información frente a cada una de las propiedades de la seguridad de la información se presenta a continuación en una tabla para cada aspecto:

CRITERIO DE CONFIDENCIALIDAD

Tabla 7 Criterio de Confidencialidad SGSI (Autoría Propia)

CONFIDENCIALIDAD		
Valoración Cuantitativa	**Valoración Cualitativa**	**DESCRIPCIÓN**
1	Pública	Datos que son de acceso público y que por lo tanto no tienen requerimientos frente a la Confidencialidad. Están en esta clasificación los que son denominados como de carácter "Público", como dato Personal Público y como de tipo Publicable.
2	Uso Interno	Datos que son de uso interno de la entidad y que no deben ser conocidos por el público en general. Están en esta clasificación todos los documentos manejados en la operación diaria pero que no tengan el carácter de "reservado", los datos catalogados como "semiprivados" y los datos e información no publicable.
3	Uso Restringido	Corresponde a la información de carácter reservado. También se ubican en esta clasificación los datos catalogados como "privados".
4	Confidencial	La información catalogada como Restringida y Secreta. Los que representen Secreto comercial o estén amparados por el secreto profesional.

CRITERIO DE DISPONIBILIDAD

Tabla 8 Criterio de Disponibilidad SGSI (Autoría Propia)

DISPONIBILIDAD		
Valoración Cuantitativa	**Valoración Cualitativa**	**DESCRIPCION**
1	Muy bajo	Información cuya imposibilidad de acceso no afecta en forma significativa la operación de la entidad y puede no estar disponible por encima de dos semanas.
2	Bajo	Información cuya inaccesibilidad puede afectar la operación normal de la entidad, puede estar no disponible entre una semana y dos semanas **Indisponibilidad: Entre 1 y 2 semanas**
3	Medio	Información cuya imposibilidad de acceso de forma permanente durante un periodo comprendido entre 1 a 7 días podría ocasionar pérdidas significativas o sanciones a la entidad o los organismos de la función pública. **Indisponibilidad: Entre 1 y 7 días**
4	Alto	Información cuya imposibilidad de acceso por un periodo entre 1 hora y 1 día puede ocasionar pérdidas significativas o sanciones la entidad o los organismos de la función pública.
5	Crítico	Información cuya imposibilidad de acceso por menos de 1 hora ocasiona pérdidas significativas o sanciones a la entidad o los organismos de la función pública. **Indisponibilidad: menos de 1 hora**

CRITERIO DE INTEGRIDAD

Tabla 9 Criterio de Integridad SGSI (Autoría Propia)

INTEGRIDAD		
Valoración Cuantitativa	**Valoración Cualitativa**	**DESCRIPCIÓ**
1	Muy bajo	Información cuya modificación no autorizada puede repararse fácilmente, no se percibe ningún año, únicamente deterioros menores.
2	Bajo	Información cuya modificación no autorizada puede repararse. Se afecta solo una parte del proceso y no hay pérdida económica.
3	Medio	Información cuya modificación no autorizada es de difícil reparación, se afecta un único proceso y los daños no implican pérdidas económicas.
4	Alto	Información cuya modificación no autorizada podría no repararse, se afectan varios procesos misionales y los daños implican pérdidas económicas.
5	Crítico	Información cuya modificación afectan toda la organización y los daños son casi irreparables

4.10.5 Importancia de los Activos de Información.

La relevancia o criticidad del activo de información se obtiene por la media aritmética de los criterios de seguridad de la información evaluados Confidencialidad, Integridad y

Disponibilidad: de acuerdo con el valor obtenido se clasifican con una importancia Muy Bajo, Bajo, Medio, Alta o Crítico.

La siguiente tabla muestra la relevancia de un activo de información:

Tabla 10 Importancia del Activo de Información SGSI (Autoría Propia)

IMPORTANCIA DEL ACTIVO		
Valoración Cuantitativa	**Valoración Cualitativa**	**DESCRIPCIÓN**
1	Muy bajo	El activo no afecta procesos.
2	Bajo	El activo puede afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y no incurrirían en sanciones pecuniarias.
3	Medi	El activo puede afectar de forma parcial una operación o un proceso. Las pérdidas o afectación
4	Alt o	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectación causan sanciones.
5	Crítico	La organización se ve seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la organización y sus procesos.

Resumiendo lo antes mencionado, al realizar el cálculo de la media aritmética de las valoraciones de las propiedades de la seguridad de la información: Confidencialidad, Disponibilidad e Integridad, se halla el valor de la importancia de cada activo así:

Tabla 11 Resultados del cálculo de valoraciones SGSI (Autoría Propia)

CONFIDENCIALIDAD		DISPONIBILIDAD		INTEGRIDAD		IMPORTANCIA	
1	**Pública**	**1**	**Muy bajo**	**1**	**Muy bajo**	**1**	**Muy Bajo**
2	**Uso Interno**	**2**	**Baj**	**2**	**Baj**	**2**	**Baj**
3	**Uso Restringido**	**3**	**Medi**	**3**	**Medio**	**3**	**Medi**
4	**Confidencial**	**4**	**Alt**	**4**	**Alt**	**4**	**Alt**
		5	**Crític**	**5**	**Crítico**	**5**	**Critic0**

4.11 Identificación de Riesgos

En esta fase se trata de conocer el nivel de exposición de los activos de información o el nivel de inseguridad para el cumplimiento de los objetivos de la Cooperativa frente a las amenazas aplicables al entorno de trabajo de los procesos, es decir conocer los riesgos a los cuales se encuentra expuesto.

La clasificación se realiza en dos etapas:

Riesgo inherente:

Es aquel que por su naturaleza no se puede separar de la situación donde se presenta, es propio de las actividades que conlleva el proceso relacionado.

Riesgo residual:

Es el resultante después de los controles existentes, evaluando si el tratamiento es acorde al criterio de aceptación del responsable del riesgo, en caso contrario estos controles deben ser mejorados o cambiados según sea el caso.

El análisis de un control existente consiste en verificar si su aplicación modifica el riesgo acorde con el tratamiento esperado, esto ya que los controles son implementados en un momento determinado y con el paso del tiempo el cambio de las amenazas, el valor de los activos y el descubrimiento de vulnerabilidades puede cambiar la eficacia de un control.

El proceso de identificación de riesgos es el siguiente:

4.11.1 Identificación de Amenazas o Fuentes de Riesgos

Tomando como base los tipos de amenazas propuestos por ISO 27005, se analizan cuales aplican para cada activo.

• [D.] – Deliberadas: Corresponde a las acciones ejecutadas por personas que bajo diferentes motivaciones como pueden ser económicas, políticas, de reconocimiento, terrorismo o sabotaje, pretendan afectar la confidencialidad, integridad y/o disponibilidad de los activos de información de la organización.

• [A.] – Accidentales: Acciones ejecutadas involuntariamente debido a desconocimiento, descuido, cansancio o hechos fortuitos que puedan afectar la confidencialidad, integridad y/o disponibilidad de los activos de información de la organización.

• [E.] – Entorno: eventos cuyo origen se encuentra en los equipos, infraestructura, instalaciones, medio ambiente y que pueden llegar a afectar la confidencialidad, integridad y/o disponibilidad de los activos de información de la organización.

4.11.2 Identificación de Vulnerabilidades.

Para cada tipo de amenaza se orienta al funcionario responsable del proceso para conocer que vulnerabilidades pueden ser aprovechadas por dicha amenaza para

generar un escenario de riesgo por la pérdida de la confidencialidad, integridad o disponibilidad de la información de la entidad. Las amenazas y vulnerabilidades aplican de acuerdo con el tipo de activo.

4.11.3 Valoración de las Consecuencias

• Probabilidad

Para cada amenaza identificada, se analiza el número de veces que esta puede ocurrir en un lapso determinado. Se toma como base la guía de la siguiente tabla, sobre la base de las estadísticas existentes o el conocimiento y experiencia del funcionario responsable del proceso.

Tabla 12 Identificación de amenazas o fuentes de riesgos (Probabilidad) (Autoría Propia)

Valor cualitativo	Valor cuantitativo	PROBABILIDAD	PROBABILIDAD DE OCURRENCIA
Muy Frecuente (MF)	**4**	A diario	75% - 100%
Frecuente (F)	**3**	Una vez al mes	50% - 75%
Frecuencia Normal (FN)	**2**	Una vez al año	25% - 50%
Poca Frecuencia (PF)	**1**	Cada varios años	0% - 25%

Para el cálculo del riesgo residual esta probabilidad será considerada analizando los controles existentes, de tal manera que se analizará si cada control está cumpliendo con la función asignada para reducir la probabilidad de materialización de la amenaza al nivel que el riesgo resultante se encuentre dentro del NRA. Es importante considerar que los controles trabajan en conjunto para reducir la probabilidad de ocurrencia.

• Impacto o efecto

Para cada amenaza o fuente de riesgo que llegue a aprovechar la vulnerabilidad o causa identificada, considerando el contexto de la entidad, con el juicio del dueño del proceso que se está analizando se determina el efecto que tiene esta situación hipotética para la organización; para lo cual se ha definido la siguiente tabla:

Tabla 13 Análisis Valores e Impacto

Valor Cualitativo	Valor Cuantitativo	Impacto
Muy Bajo (MB)	1	Daño despreciable.
Bajo (B)	2	Daño menor para la empresa u organización.
Medio (M)	3	Daño importante para la empresa u organización.
Alto (A)	4	Daño grave para la empresa u organización.
Muy Alto (MA)	5	Daño muy grave para la empresa u organización.

Controles existentes vs los activos del área de Captaciones.

Anteriormente en el capítulo tres se indicó la situación actual de la seguridad en la que se encuentra la entidad, en la cual se pudo observar que las medidas de control que la entidad posee son mínimas y los planes para tratar los riesgos están en procesos de implementación o no posee por lo cual las amenazas pueden llegar a materializarse. A continuación, en la Tabla 14 se muestra los controles existentes en el área de Captaciones de la Cooperativa los cuales son utilizados por la misma para proteger sus activos ante las amenazas que puedan de alguna forma atentar contra la seguridad.

Tabla 14 Identificación de amenazas o fuentes de riesgos (Impacto o efecto) (Autoría Propia)

Controles ISO 27002:2013	Controles Distribuidos en los activos del área de Captaciones
A.14.1.3-Protección de transacciones de servicios de aplicaciones	1
A.12.1.1-Documentación de los procedimientos de operación	47
A.12.1.2-Gestión de los cambios	4
A.6.1.1-Seguridad de la información roles y responsabilidades	47
A.6.1.2-Separación de deberes	13
A.8.1.3-Uso aceptable de los activos	8
A.8.2.3-Manejo de activos	9
N/A	20
TOTAL	**149**

Estimación de Riesgos

La estimación del riesgo permite determinar aquellos riesgos cuya materialización afectaría en mayor o menor porcentaje sobre los activos de una empresa u organización. De tal manera que todos los riesgos deben ser analizados cuidadosamente mediante la aplicación de buen juicio y sentido común.

Dependiendo del nivel con el que sea catalogado el riesgo, requerirá mayor o menor atención

por parte de los respectivos responsables dueños de los procesos agregadores de valor para lograr mitigarlos en un porcentaje aceptable que garantice que su materialización no influya sobre los activos.

Para realizar la estimación del riesgo es necesario utilizar las valoraciones tanto de las vulnerabilidades como de los impactos anteriormente efectuados, ya que ambos valores permiten determinar el valor del riesgo.

Para visualizar con mayor facilidad la representación del riesgo, es necesario aplicar una técnica matricial, la cual consiste en ubicar los niveles de las vulnerabilidades en las filas de la matriz, mientras que en las columnas se ubicarán los niveles de los impactos definidos anteriormente. A continuación, se muestra la respectiva matriz cualitativa que permite determinar el riesgo:

Tabla 15 Representación del riesgo, matriz de vulnerabilidades

RIESGO		VULNERABILIDAD			
		Poco Frecuente (**PF**)	Frecuencia Normal (**FN**)	Frecuente (**F**)	Muy Frecuente (**MF**)
IMPACTO	Muy alto (**MA**)	A	MA	MA	MA
	Alto (**A**)	M	A	MA	MA
	Medio (**M**)	B	M	A	MA
	Bajo (**B**)	MB	M	M	A
	Muy Bajo (**MB**)	MB	MB	B	M

En la siguiente tabla se muestra la respectiva matriz cuantitativa asociada a la matriz cualitativa anteriormente definida, en la cual el riesgo está determinado por el producto entre el impacto y la probabilidad de ocurrencia (vulnerabilidad), como se puede observar a continuación.

Por lo tanto:

Riesgo = Impacto * Probabilidad de Ocurrencia (vulnerabilidad)

Tabla 16 Matriz impacto y probabilidad de ocurrencia

RIESGO		VULNERABILIDAD			
		1	2	3	4
IMPACTO	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Además, es necesario establecer una matriz que asocia tanto la valoración cuantitativa y cualitativa para relacionar los valores obtenidos una vez que se ha determinado el riesgo. Esto con el propósito de tomar en cuenta aquellos que tengan alta importancia y requieran de mayor atención para ser tratados. A continuación, en la siguiente tabla se muestra la respectiva matriz que permite determinar la clase riesgo:

Tabla 17 Matriz para determinar la clase de riesgo

Clase	Valoración Cualitativa	Valoración Cuantitativa
Crítico	Muy alto	10 a 20
Grave	Alto	5 a 9
Moderado	Medio	4 a 6
Despreciable	Bajo y Muy Bajo	1 a 3

4.12 Evaluación de Riesgos

En esta sección se procederá a evaluar los riesgos en base a la metodología seleccionada, previo a eso, a continuación, se realizará una breve descripción de la Matriz de Evaluación de Riesgos de cada una de las columnas que componen el cuadro de evaluación de riesgos.

Descripción:

Nº: Número de fila.

Tipo de Amenaza: Las amenazas se clasifican por tipos. Algunos tipos de amenazas fueron tomadas del Anexo C de la norma ISO 27005.

Nombre del activo: Nombre del activo crítico de información.

Amenaza: Es un evento que puede desencadenar un incidente, produciendo daños materiales o inmateriales a los activos.

Vulnerabilidad: Las vulnerabilidades son puntos débiles que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza.

Integridad: Propiedad de proteger la exactitud y completitud de la información y cuyo valor va de 1 – 5.

Confidencialidad: Propiedad por la cual la información no se pone a disposición de usuarios no autorizados y cuyo valor va de 1 – 5.

Disponibilidad: Propiedad por la cual la información debe ser accesible en cualquier momento que el usuario autorizado lo requiera y cuyo valor va de 1 – 5.

Impacto: Es la materialización de una amenaza sobre un activo. De acuerdo al criterio

de los autores el impacto se determina mediante el promedio entre la integridad, confidencialidad y disponibilidad. Si el promedio resultante es un número decimal entonces aproximarlo al entero más cercano.

Probabilidad de Ocurrencia: Es la frecuencia con la cual una vulnerabilidad puede ser aprovechada por una amenaza y cuyo valor va de 1 – 4.

Riesgo: Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él, causando daños a la organización. El riesgo es el producto entre el impacto y la probabilidad de ocurrencia.

4.12.1 Análisis de los Datos Obtenidos

Con los datos obtenidos en la matriz de inventario de activos y matriz de riesgos calor se generó los siguientes gráficos en los cuales se puede observar la distribución de riesgo en los activos del área de Captaciones de la Cooperativa.

Tabla 18 Distribución de Activos

Tipo de Activo	Número de Activo
Actividades Procesos	10
Información	3
Software	7
Total, general	**20**

Tabla 19 Activo por riesgo

Riesgo	Nro de Activo por Riesgo
A	1
MB	8
M	8
MA	3

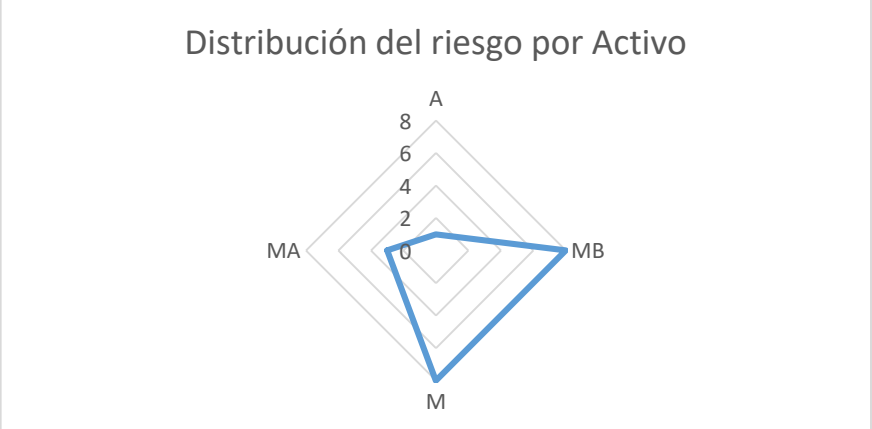

Figura 15 Evaluación de riesgo versus activo

4.12.2 Salvaguardas

En la seguridad de la información una salvaguarda es una medida de protección que se utiliza para resguardar y proteger la información de amenazas como el acceso no autorizado o la fuga de datos, estas salvaguardas pueden ser de tipo: administrativo, técnico o físico, a continuación se detallan algunos ejemplos: contraseñas seguras, encriptación, restricciones de gestión, seguridad del personal, y seguridad a estructuras físicas, áreas y dispositivos, el objetivo de estas contramedidas es para garantizar la confidencialidad, integridad y disponibilidad de la información.

4.12.3 Análisis de los Datos Obtenidos

Evaluación frente a Niveles de Riesgo Aceptables (NRA):

Identificado el nivel del riesgo, se lleva a cabo la evaluación del mismo para definir su tratamiento y para esto es necesario aplicar el Criterio de Aceptación de Riesgo que refleja la posición la organización y el manejo que se debe dar ante cada riesgo identificado.

Criterio de Aceptación del Riesgo:

Se establece para los niveles de riesgo definidos, es decir: bajo, moderado, alto y extremo, cuáles son aceptados por la organización con base en la estrategia de riesgo y la aprobación de la Gerencia General. De esta forma para los niveles de riesgo que no sean aceptados se debe definir un Tratamiento de Riesgos.

Tratamiento de Riesgos

Una vez que se han identificado, analizado y evaluado los riesgos a los que están expuestos los activos de la organización, la Administración y los responsables de dichos activos podrán tener una visión más clara y general sobre aspectos que deben ser considerados para evitar posibles daños y perjuicios.

De tal manera que, al contar con la estimación de riesgos anteriormente realizada, se podrá efectuar una evaluación general respecto a los controles y políticas que deben ser implementados para gestionar, corregir, controlar y mitigar los riesgos, garantizando de esta manera que dichos riesgos no persistan y proporcionar una mejoría considerable en el aspecto de seguridad de la información dentro de la organización.

La norma NTE INEN-ISO/IEC 27005 nos presenta diversas maneras para realizar el tratamiento de riesgos, dentro de las cuales tenemos: evitar el riesgo, reducir el riesgo, retener o aceptar el riesgo y transferir el riesgo.

Para visualizarlo de mejor manera, se presenta la forma en que se realiza la gestión de riesgos, en la que se encuentra incluido el tratamiento de riesgos:

Previo a la definición e implementación de los controles necesarios para realizar la correspondiente gestión de riesgos; se procederá con la elección del tipo de tratamiento que se les dará a los riesgos identificados con anterioridad.

A partir de la descripción de los tratamientos mencionados que nos ofrece la norma NTE INENISO/IEC 27005 y la descripción de estos que nos ofrece la metodología MAGERIT se ha realizado una adaptación para obtener una definición de los tratamientos más precisa al combinar ambas descripciones. Por tal razón, a continuación, se describen los diferentes tratamientos, como se indica en la siguiente figura.

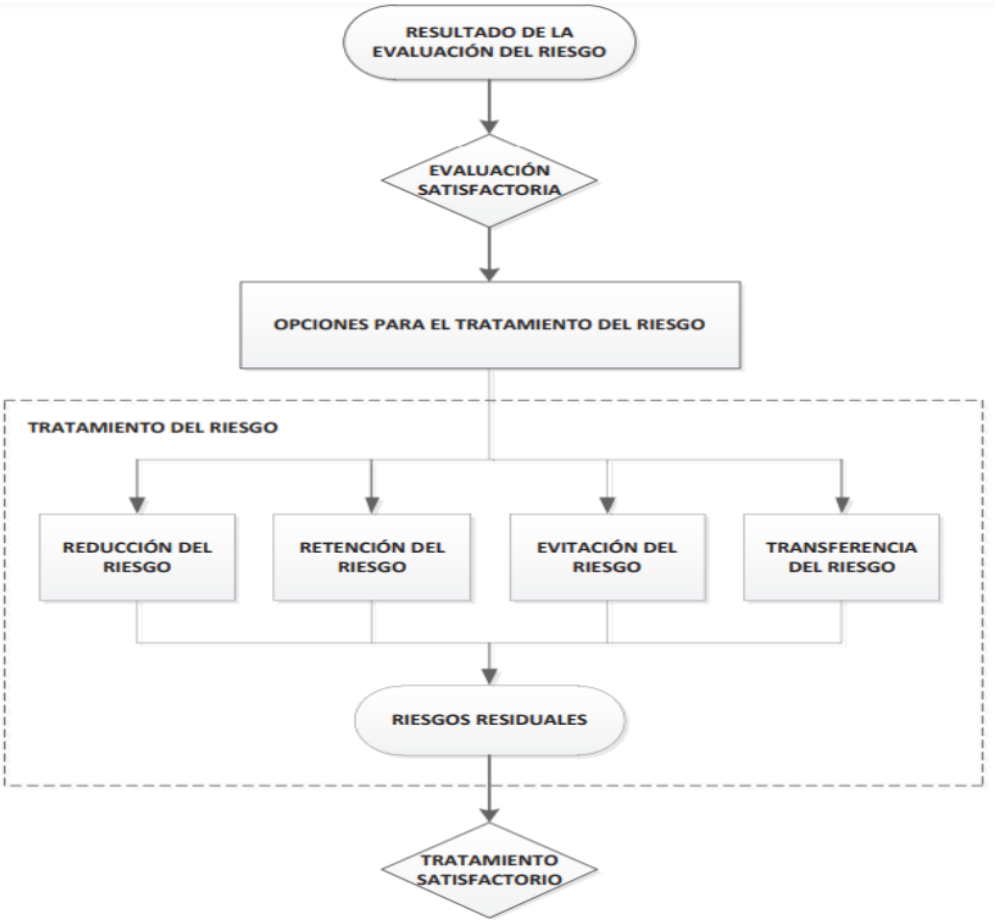

Figura 16 Actividades para el tratamiento de los riesgos

Previo a la definición e implementación de los controles necesarios para realizar la correspondiente gestión de riesgos; se procederá con la elección del tipo de tratamiento que se les dará a los riesgos identificados con anterioridad.

A partir de la descripción de los tratamientos mencionados que nos ofrece la norma NTE INEN ISO/IEC 27005 y la descripción de los mismos que nos ofrece la metodología MAGERIT se ha realizado una adaptación para obtener una definición de los tratamientos más precisa al combinar ambas descripciones. Por tal razón, a continuación, se describen los diferentes tratamientos:

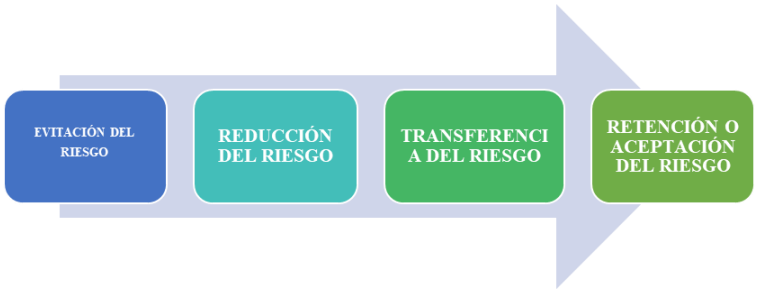

Figura 17 Control continuo de los indicadores de evaluación de impacto

Una vez determinados los riesgos con sus respectivos niveles de incidencia de acuerdo con los criterios anteriormente; es necesario establecer las políticas y controles adecuados para realizar la gestión de riesgos y la gestión de seguridad correspondientes a lo largo del tiempo, con la finalidad de garantizar que los riesgos hallados no persistan dentro de la organización.

La definición de políticas y controles conforman el primer paso hacia el objetivo de incrementar la seguridad de la información dentro de un ambiente tecnológico de la información. Para realizar la gestión de riesgos correspondiente, es necesario elegir el tipo de tratamiento que se le dará a uno o varios riesgos dependiendo de su criticidad, ya que es posible combinar los diferentes tratamientos de riesgos, con la finalidad de facilitar su gestión. Por tal razón, a los riesgos catalogados como moderados (4-6) y despreciables (1-3) se les aplicará el tratamiento de "Retención o Aceptación del Riesgo" por parte de la organización.

Para los riesgos con una valoración considerable y que han sido catalogados como críticos (10 - 20) y graves (5 - 9), a los cuales se les aplicará el tratamiento de "Reducción del Riesgo"; para tal propósito, se utilizarán las políticas y controles que constan en la norma NTE INEN-ISO/IEC 27001. La matriz de evaluación de riesgos consta de las siguientes columnas:

Nº: Número de fila

Nombre del activo: Nombre del activo crítico de información.

Amenaza: Es un evento que puede desencadenar un incidente, produciendo daños materiales o inmateriales a los activos.

Vulnerabilidad: Las vulnerabilidades son puntos débiles que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza.

Impacto: Es la materialización de una amenaza sobre un activo. De acuerdo al criterio de los autores el impacto se determina mediante el promedio entre la integridad, confidencialidad y disponibilidad. Si el promedio resultante es un número decimal entonces aproximarlo al entero más cercano.

Probabilidad de Ocurrencia: Es la frecuencia con la cual una vulnerabilidad puede ser aprovechada por una amenaza y cuyo valor va de 1 – 4.

Riesgo: Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él, causando daños a la organización. El riesgo es el producto entre el impacto y la probabilidad de ocurrencia.

Opción de Tratamiento: La opción de tratamiento de riesgo se determina mediante el valor cuantitativo del riesgo. Si el valor del riesgo es de 1-3 y de 4- 6 entonces la opción de tratamiento será "Retención o Aceptación del Riesgo" y si el valor del riesgo es de 5-9 y de 10-20 entonces la opción de tratamiento será "Reducción del Riesgo".

Controles Seleccionados: Los controles seleccionados han sido tomados de la norma ISO 27001. A cada vulnerabilidad le corresponde de uno a varios controles dependiendo del caso, obviamente los controles seleccionados deben estar relacionados con la vulnerabilidad.

4.12.4 Objetivos de control y controles

Posterior a obtener los resultados los resultados de evaluación de riesgos y verificado el nivel de impacto y riesgos a los que se tiene expuestos los activos y luego de analizar las opciones de tratamiento adecuados para mitigar los riesgos. La mayoría de las amenazas que se han podido evidenciar pueden ser tratadas mediante la reducción de los niveles de riesgo por lo cual se seleccionaron los objetivos de control y controles que se encuentran en la ISO 27002:2013. En la Tabla 20 se muestran cuáles son los controles para implementar.

Tabla 20 Controles para implementar ISO 27002

Controles ISO 27002	Controles Para Implementar
CONTROL CORRECTIVO	4
A.12.1.1-Documentación de los procedimientos de operación	2
A.6.1.1-Seguridad de la información roles y responsabilidades	1
A.6.1.2-Separación de deberes	1
CONTROL PREVENTIVO	8
A.12.1.1-Documentación de los procedimientos de operación	6
A.6.1.1-Seguridad de la información roles y responsabilidades	1
A.6.1.2-Separación de deberes	1
NO APLICA CONTROL	
(en blanco)	0
Total general	**12**

4.12.5 Matriz de Declaración de aplicabilidad de los controles

La siguiente tabla constituye la declaración de aplicabilidad para el SGSI de la Cooperativa, aquí se detallan los controles de seguridad que son aplicados a los objetivos de información en función del alcance de implementación o actualización del SGSI.

Tabla 21 Matriz de Declaración de Aplicabilidad de Controles

Sección	Dominio, objetivos de control y Controles	Aplicabilidad	Justificación	Recomendación implementación
A.12.1.1	Documentación de los procedimientos de operación	Aplica	Se deben preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación de información, como procedimientos de inicio y cierre de sesión de computadores, respaldo, mantenimiento de equipos, manejo de medios, salas de computación y administración y seguridad de manejo de correo. Dichos procedimientos deben estar vigentes y puestos a disposición de todos los usuarios que los necesiten.	a) la instalación y configuración de sistemas; b) el tratamiento y manipulación de la información tanto automatizada como manual; c) las copias de respaldo; d) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos más tempranos de comienzo y más tardíos de finalización posibles de cada tarea; f) los contactos de soporte y escalado, incluyendo contactos de soporte externo, para el caso de dificultades operacionales o técnicas inesperadas; h) el reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema; i) la gestión de pistas de auditoría y de la información del registro de sistemas (véase 12.4); j) los procedimientos de monitorización.
A.6.1.1	Seguridad de la información roles y responsabilidades	Aplica	Es necesario que los colaboradores de la Cooperativa conozcan sus roles y responsabilidades relacionadas con la seguridad de la información para la correcta operación del SGSI, por tanto, es importante que la Gerencia General respalde activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Cooperativa.	Generar roles y responsabilidades para la operación del SGSI, por tanto, es importante que la Gerencia General respalde activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Cooperativa. La Cooperativa debe en su política general de seguridad de la información establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma velar por mantener protegido su información mediante la revisión del sistema de gestión, mantenimiento, difusión y cumplimiento de los principios de seguridad de la información. Definir y verificar las responsabilidades del rol de líder de seguridad, quien será el responsable por el SGSI.

Sección	Dominio, objetivos de control y Controles	Aplicabilidad	Justificación	Recomendación implementación
A.6.1.2	Separación de deberes	Aplica	Se deben separar claramente los deberes para los roles establecidos, con el fin de que no se presenten conflictos de responsabilidades entre las áreas de la Cooperativa que tienen acceso a los activos de información para que realicen un uso debido de los mismos.	Análisis de la descripción de los cargos para identificar actividades que no cuenten con chequeo cruzado, para que se implementen. Formalización de la asignación de nuevas actividades a los funcionarios correspondientes. Identificación de actividades de revisión, aprobación, ejecución y auditoría en un mismo cargo para definir su separación

Evaluaciones:

Corresponde a los exámenes que serán desplegados a los funcionarios de la Institución de acuerdo con los módulos interactivos notificados a los usuarios, esto permitirá establecer los conocimientos que tiene los usuarios en temas de seguridad de la información para determinar si los niveles de concienciación se encuentran dentro de las expectativas deseadas.

4.12.6 Proceso Agregador de Valor

De acuerdo con el alcance de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) el proceso agregador de valor que será intervenido para la identificación, inventario y clasificación de los activos de información será:

4.12.7 Gestión de Captaciones

4.12.7.1 Área de Intervención y Análisis

Las áreas con las cuales se va a establecer las sesiones de trabajo serán de acuerdo con el alcance establecido en el análisis de los procesos agregadores de valor que se tenga por objetivo identificar, inventariar y clasificar los activos de información.

4.12.7.2 Roles y Responsabilidades del Propietario del Activo de Información

En la Cooperativa el rol de propietario del activo de información será asumido por el usuario funcional dueño del proceso agregador de valor y quienes intervienen en las diferentes actividades de su ejecución.

El propietario del activo de información tendrá como responsabilidades las siguientes actividades:

- Responsable del activo de información en su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda.
- Velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad, confidencialidad e integridad.
- Determinar el valor que el activo tiene para la institución.
- Responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de esta.
- Documentar y mantener actualizada la clasificación efectuada
- Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencias.

- Proporcionar toda la información concerniente a los procesos agregadores de valor en función de los flujos operativos prestablecidos con el fin de inventariar y clasificar los activos de información.

4.12.7.3 Diseño de las políticas

Forman parte integral de la Política de Seguridad de la Información, todas aquellas directrices que, por su tema particular, requieren un mayor nivel de detalle y especialización para su definición, las cuales son elaboradas y mantenidas por el departamento de Tecnologías de la Cooperativa.

Acorde a la norma ISOIEC NTC 27001, la cooperativa debe tener en operación las siguientes políticas obligatorias para cumplir con los requisitos de seguridad de la información, excepto si alguna de ellas está excluida en la declaración de aplicabilidad.

Las políticas mínimas requeridas en la norma ISO 27001 deben ser documentadas, aprobadas, publicadas y comunicadas a las partes interesadas.

A continuación, se muestra el resumen de las políticas y su estructura respecto a la política principal de la seguridad de la información.

Figura 18 Política de seguridad de la Información ISO 27001

4.13 Resultados para la identificación, valoración y mitigación de riesgos en activos de información utilizando la metodología MAGERIT.

Entre los aspectos claves para el desarrollo del proyecto es la investigación enfocada en establecer procedimientos para la identificación de riesgos en los activos de información en

la Cooperativa de Ahorro y Crédito “Tulcán Ltda.”, garantizando el cumplimiento de las normas y políticas de seguridad de la información.

Con la finalidad de identificar los riesgos, y definir actividades de mitigación, se aplicará la metodología Magerit, posteriormente se utilizará un procedimiento bien estructurado que garantice la estabilidad y efectividad en la gestión de riesgos, enfoque que nos permitirá identificar vulnerabilidades, priorizarlas y actuar de manera proactiva buscando reducir su impacto.

Se ha definido ejecutar procedimientos específicos para este propósito, los cuales contienen el levantamiento de encuestas dirigidas a funcionarios/usuarios de la Cooperativa de Ahorro y Crédito “Tulcán Ltda.”. Con los resultados que arrojen éstas, conseguiremos identificar riesgos y vulnerabilidades aún no detectados.

Con la obtención de las respuestas, consecutivamente se establecerá una base sólida para el desarrollo de una gestión efectiva de los riesgos en el área de Captaciones; estas contestaciones proporcionarán información valiosa sobre los riesgos que los funcionarios consideren más relevantes.

El nivel de cumplimiento que posee la entidad sobre los requerimientos de seguridad que se plantea en el Anexo A de la norma ISO/IEC 27001 es bueno ya que la mayoría de los controles se encuentra en un porcentaje superior al 50% lo que implica que la entidad posee controles de seguridad implementados en políticas, procedimientos.

En el área de Captaciones se realizó la identificación de activos, para su posterior evaluación análisis de riesgos que permitió recomendar los diferentes controles, y; se espera que con el despliegue de este proyecto los niveles de cumplimiento sean los siguientes.

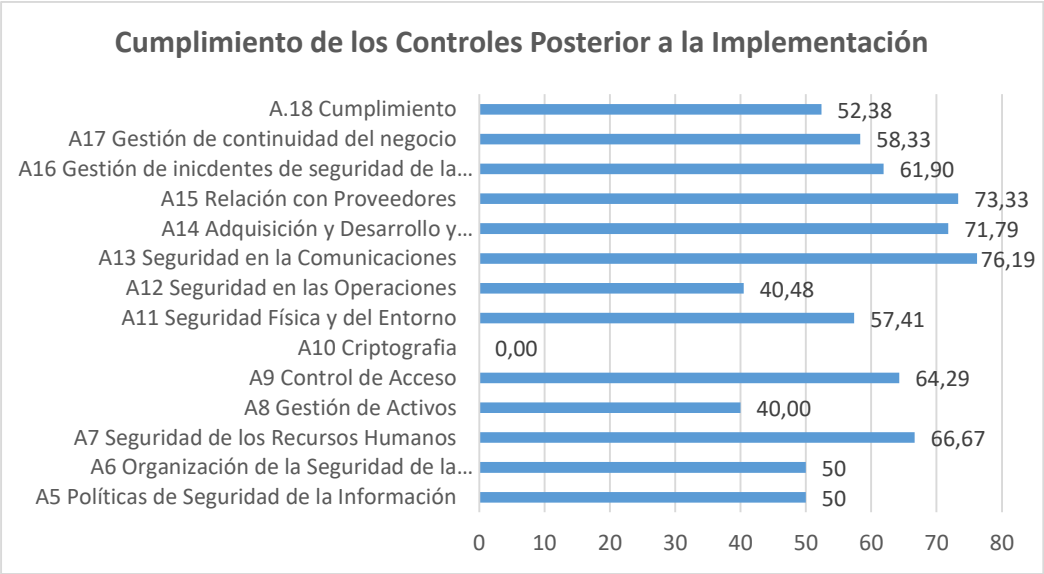

Figura 19 Niveles de cumplimiento en el control posterior a la implementación

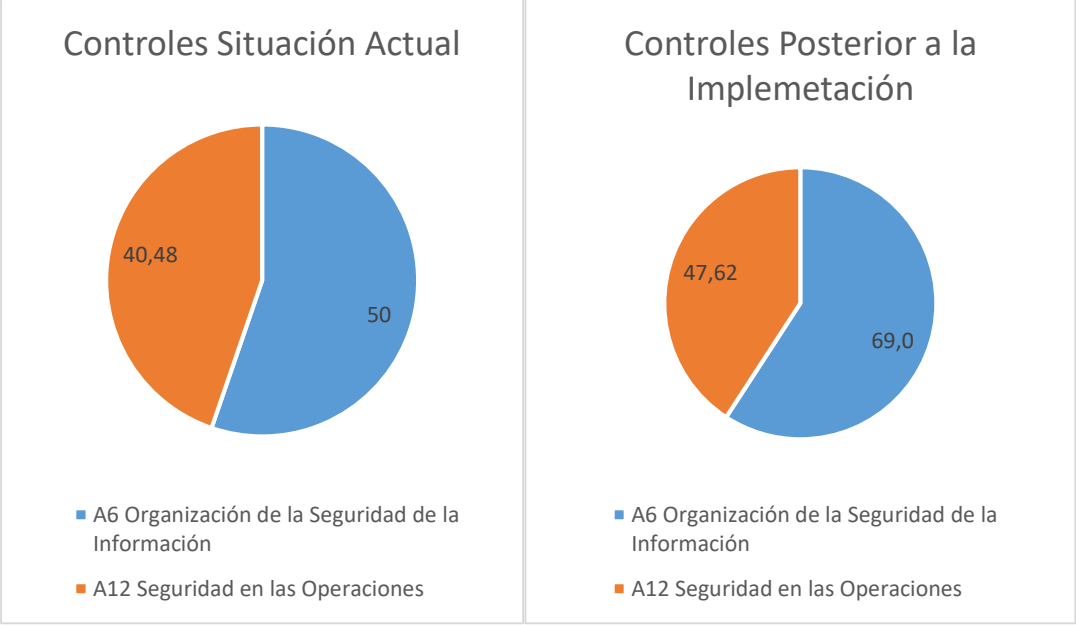

Figura 20 Diferencias en el control actual y posterior a la implementación

Mejora Continua

Esta fase corresponde a la entrega de los documentos descritos como entregables respecto de la implementación del SGSI y de la norma de control de seguridad emitida por el ente regulatorio SEPS.

El SGSI será actualizado y mejorado de forma permanente en los siguientes ámbitos de gestión:

- Aplicación de mejoras a través de la ejecución de los planes correctivos propuestos en las auditorias del SGSI.
- En los casos en que los funcionarios detecten o notifiquen situaciones que vulneren los esquemas de seguridad.
- Monitoreo permanente de la aplicación del plan de concienciación en temas de seguridad para los funcionarios.
- Validación del cumplimiento de las políticas y procedimientos entorno al SGSI.
- Monitoreo de ejecución del Plan Estratégico de Seguridad de la Información.

No conformidad y medidas correctivas

- La Cooperativa luego de haber realizado las revisiones del Sistema de Gestión de Seguridad de la Información validará los hallazgos detectados con el fin de mitigar las posibles vulnerabilidades en el caso de que existieran mediante la aplicación de planes correctivos. Cabe indicar que el despliegue de las medidas correctivas será aplicada previo la autorización de la Gerencia General.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El Sistema de Gestión de Seguridad de la Información – SGSI, es una de las mejores prácticas y herramientas que permite una adecuada gestión de los riesgos al interior de la Institución y el cumplimiento de la seguridad de la información bajo un marco de referencia que garantiza su gestión y continuidad a lo largo del tiempo.
- El SGSI se aborda efectivamente bajo una normativa reconocida como la ISO/IEC 27001 cuya implantación le asegura a la entidad, gozar de un correcto gobierno de seguridad de la información que garantiza la protección de los activos, mejorar el negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio.
- La correcta y continua gestión del SGSI se logra con la implantación correcta de políticas, proceso, procedimientos, una adecuada estructura organizacional, controles y lo más importantes con la concientización del recurso humano sobre la importancia de la seguridad de la Información, y contando especialmente con el apoyo total de la Alta Dirección.

Recomendaciones

- Verificar el cumplimiento de los requisitos legales y/o normativos en lo relacionado con la implantación de la seguridad de la información en la cooperativa, ejemplo de esto es la Norma ISO/IEC 27001, Ley de protección de datos.
- Hacer seguimiento a las acciones correctivas y preventivas que resultan de la detección de no conformidades en la gestión del sistema de seguridad de información al interior de la Cooperativa, con el objetivo de tomar correctas decisiones para las mejoras respectivas.
- Identificar el impacto y las acciones que se deben llevar a cabo sobre el SGSI por los posibles cambios que se establezcan en la entidad como por ejemplo cambio de personal clave, reestructuración de procesos, implantación de nuevas tecnologías, nuevas normas o leyes que inciden en el SGSI.
- Realizar el seguimiento a los controles que se encuentren implementados para mitigar los riesgos identificados en cada uno de los procesos y subprocesos que hacen parte del alcance del SGSI, con el fin de conocer y evaluar el índice de eficiencia y eficacia de los mismos, identificar aquellos riesgos, las causas y sus impactos cuyos controles

identificados no se han podido implementar, con el fin de tomar decisiones frente a los mismos.

- Al líder del área de seguridades de la información de esta Entidad Financiera identificar técnicas, productos o procedimientos que se puedan implementar en la organización con el fin de mejorar el desempeño y eficacia del Sistema de Gestión de Seguridad de la Información SGSI.

Tabulación de resultados

1. ***¿Conoce usted la existencia de políticas de seguridad de la información en la cooperativa? (Sí/No)***

Tabla 22 Pregunta 1

Respuesta	***Cantidad***	***Porcentaje***
Sí, en la Cooperativa tenemos políticas de seguridad de la información para proteger la información de nuestros socios.	*7*	*70%*
No conozco del tema de seguridad de información.	*3*	*30%*
Total	*10*	*100%*

Fuente: Autor

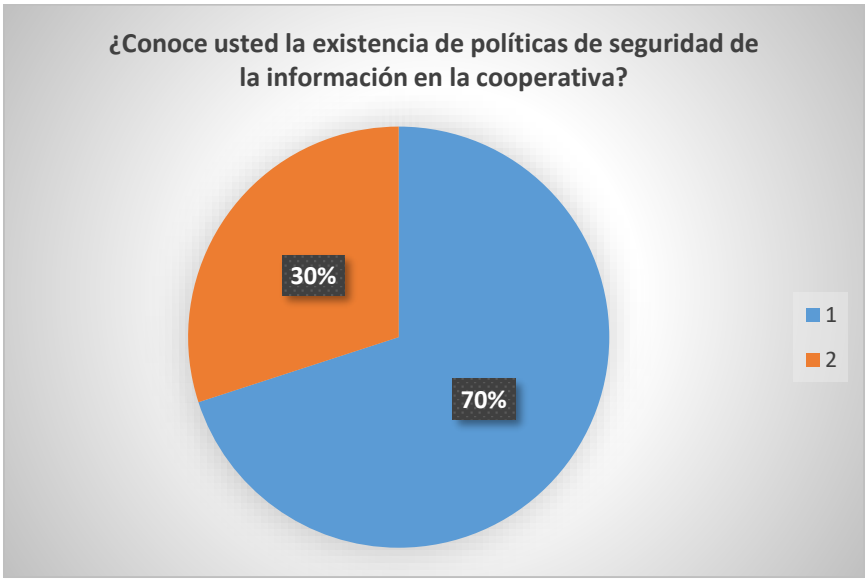

Figura 21 Resultados Pregunta 1

Interpretación: del total de entrevistados, (7) conocen la existencia de políticas de seguridad, aunque no a profundidad, este tema está ligado o relacionado a personas que trabajan de manera cotidiana al uso de computador y de sistemas, mientras que (3) son personas que trabajan en la cooperativa, pero en áreas donde no se utiliza de manera permanente el computador sin conocer sobre estas políticas.

Análisis: estas políticas de seguridad en el trabajo hacen que el funcionario tenga mucho cuidado con el uso de información externa y el uso de contraseñas inseguras.

2. ***¿Ha recibido capacitación en seguridad de la información en los últimos 12 meses? (Sí/No)***

Tabla 23 Pregunta 2

Respuesta	***Cantidad***	***Porcentaje***
No, no se ha recibido capacitación en temas de seguridad de información	*9*	*90%*
Si, estudio una maestría en seguridad y tengo capacitación permanente	*1*	*10%*
Total	*10*	*100%*

Fuente: Autor

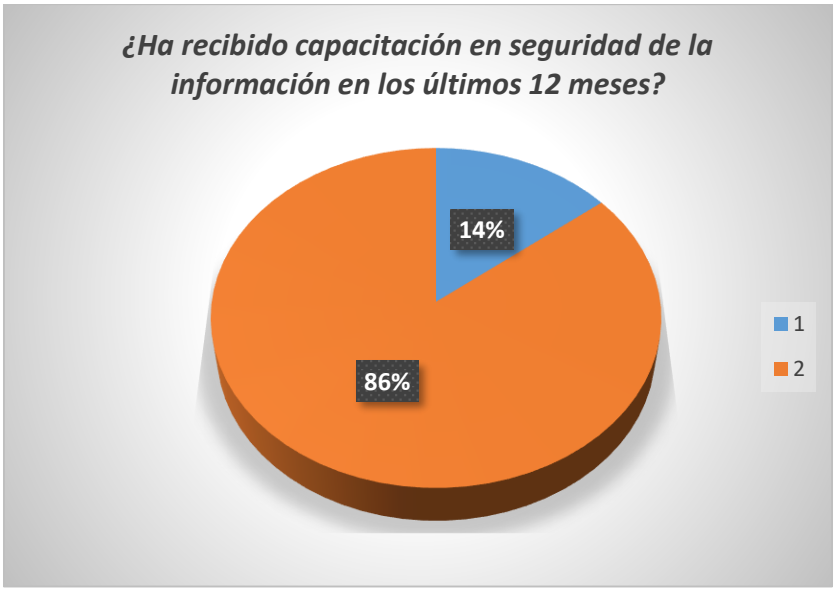

Figura 22 Resultados Pregunta 2

Interpretación: del total de entrevistados, nueve (9) manifiestan no haber sido capacitados en temas de seguridad de la información o ciberseguridad, mientras que un (1) encuestado comenta que actualmente cursa una maestría en ciberseguridad y conoce muy bien el manejo para mitigar los riesgos.

Análisis: la capacitación debería ser constante a funcionarios a través de cualquier medio, con esto en lo posterior se conseguiría disponer de un capital humano que conozca las estrategias al menos las básicas para minimizar los riesgos.

3. ¿Con qué frecuencia cambia sus contraseñas de acceso a los sistemas internos?

a) Cada mes b) Cada tres meses c) Cada seis meses o más d) Nunca

Tabla 24 Pregunta 3

Respuesta	***Cantidad***	***Porcentaje***
Cada mes	*1*	*10%*
Cada tres meses	*6*	*60%*
Cada seis meses	*3*	*30*
Nunca	*0*	*0*
Total	*10*	*100%*

Fuente: Autor

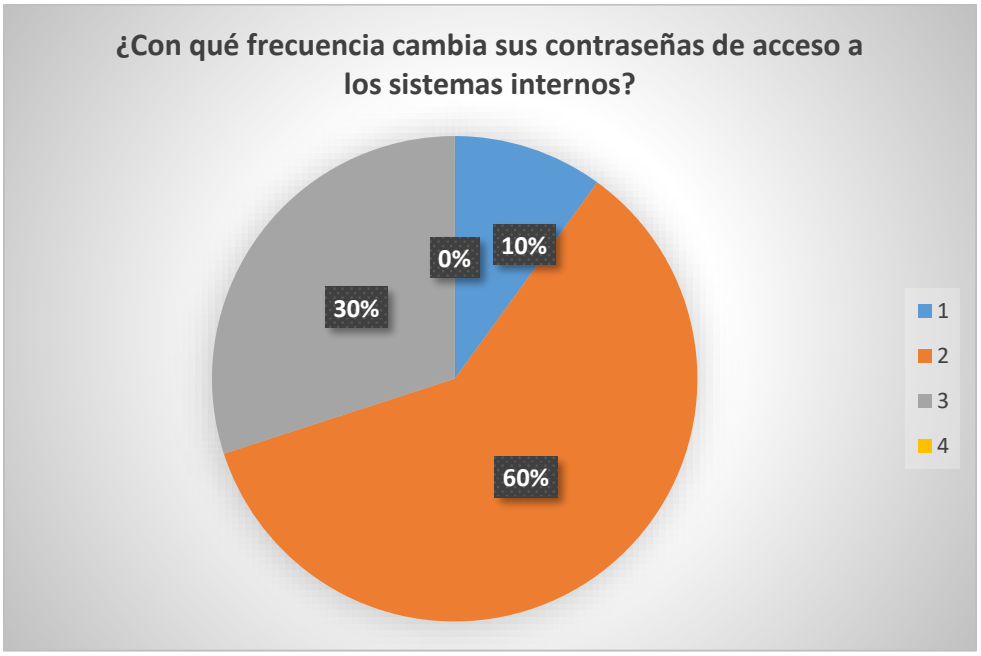

Figura 23 Resultados Pregunta 3

Interpretación: los usuarios comentan que cuentan con portales seguros que no necesitan cambiar de manera continua las contraseñas, esto debido a que tiene limitación en el uso del internet, por políticas internas una (1) persona cambia cada mes, seis (6) cada tres meses, tres (3) cada 6 meses y ninguna deja por tiempos largos la misma contraseña.

Análisis: el funcionario que labora de manera permanente conectado a la red tecnológica conoce de la importancia de tener seguridad en el uso de los programas informáticos es por eso que como política profesional los funcionarios optan por cambiar sus contraseñas de ingreso al dominio como de correos institucionales e ingreso a aplicativos.

4. ***¿Qué tan seguro considera que es el sistema informático de la cooperativa para proteger los datos de los clientes? (Escala de 1 a 5)***

1 2 3 4 5

(1, bueno – 5, malo).

Tabla 25 Pregunta 4

Respuesta	*Cantidad*	*Porcentaje*
1	*8*	*80%*
2	*2*	*20%*
3	*0*	*0*
4	*0*	*0*
5	*0*	*0*
Total	*10*	*100%*

Fuente: Autor

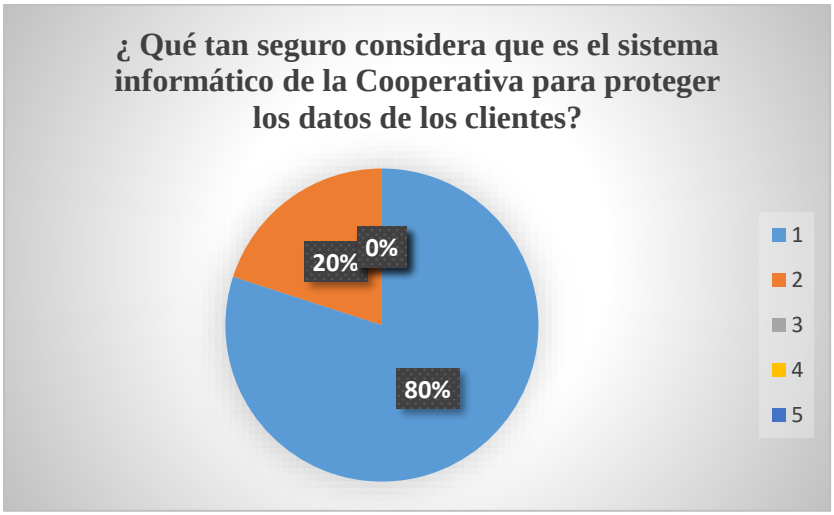

Figura 24 Resultados Pregunta 4

Interpretación. Hay mucha confianza en los sistemas que dispone la Cooperativa y más aún cuando hace dos años atrás se cambió el core financiero nuevo en su totalidad, esto les asevera a todos los trabajadores laborar en un entorno seguro, concluyendo que (8) personas confían a plenitud en la protección de los datos de los socios, mientras que (2) perciben que todavía falta muchas cosas por corregir en lo implementado.

Análisis. El funcionario siente seguridad al trabajar con información de socios, debido a que el sistema informático en general protege los datos sin destacar presencia de riesgos de manera permanente, esto en relación a las afectaciones que se conoce especialmente en los inconvenientes que se suscitan en entidades bancarias.

5. ***¿Ha detectado o ha sido víctima de algún incidente relacionado con la seguridad de la información (phishing, fuga de datos, accesos no autorizados, etc.)? (Sí/No)***

Tabla 26 Pregunta 5

Respuesta	*Cantidad*	*Porcentaje*
Sí	*1*	*10%*
No	*9*	*90%*
Total	*10*	*100%*

Fuente: Autor

Figura 25 Resultados Pregunta 5

Interpretación. Como funcionarios se percibe que es muy baja la incidencia de personas que sin autorización hagan mal uso de las herramientas informáticas que dispone esta entidad, al contrario, parece ser que el personal humano como parte de su formación y compromiso con la Institución no arremete en contra de la ella, exponiendo información sensible a personas externas a la Cooperativa.

Análisis. Afortunadamente en la Cooperativa se cuenta con medidas de seguridad que han ayudado, de alguna manera, a prevenir incidentes graves. Se ha identificado intentos de phishing y algunos accesos no autorizados, que han sido gestionados de inmediato, todo esto gracias a los controles de seguridad implementados, minimizando cualquier posible impacto.

6. ***¿Utiliza dispositivos personales para acceder a información confidencial de la cooperativa? (Sí/No)***

Tabla 27 Pregunta 6

Respuesta	***Cantidad***	***Porcentaje***
Sí	*0*	*0%*
No	*10*	*10%*
Total	*10*	*100%*

Fuente: Autor

Figura 26 (Autoría Propia) Pregunta 6

Interpretación. Las políticas internas emitidas por parte de la dirección de tecnologías son radicales en exigir el no uso de dispositivos electrónicos (tablets, teléfonos y computadores portátiles) para el manejo de aplicativos institucionales. En el caso de hacer uso existe un posible riesgo de acceder a información confidencial aumentando la vulnerabilidad de infección de virus o fuga de datos, todo esto conduciendo a sanciones internas o llamados de atención.

Análisis. En tiempo posterior, si en la Cooperativa se permite esta práctica, sería conveniente establecer controles adicionales, y, de paso, concienciar al personal sobre los riesgos, reconfirmando que la prohibición y el acceso de dispositivos personales reflejan un indicador positivo de una buena política de seguridad.

7. ***¿Cuál considera que es la principal amenaza para la seguridad de la información en la cooperativa?***

a) Uso inadecuado por parte de los empleados.

b) Ataques externos (hackers, malware).

c) Falta de capacitación en seguridad.

d) Falta de inversión en tecnología de seguridad.

Tabla 28 Pregunta 7

Respuesta	***Cantidad***	***Porcentaje***
Uso inadecuado por parte de los empleados.	*6*	*60%*
Ataques externos (Hacker, malware).	*1*	*10%*
Falta de capacitación en seguridad.	*3*	*30%*
Falta de inversión en tecnología de seguridad.	*0*	*0%*
Total	*10*	*100%*

Fuente: Autor

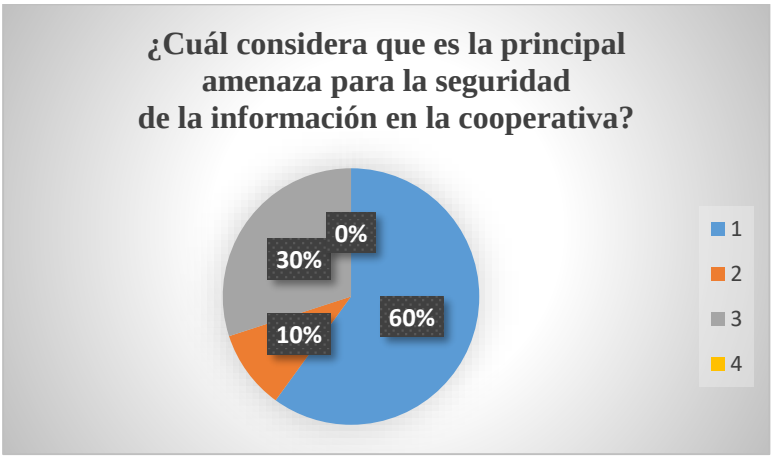

Figura 27 Resultados Pregunta 7

Interpretación. Las personas encuestadas coinciden que la vulnerabilidad más fuerte, en caso de incidentes, es la fuga de información del personal que labora o de las personas que por alguna razón fueron desvinculadas y conocen el manejo de los paquetes informáticos. Seis (6) personas consideran que la principal amenaza es el factor humano, mientras que una (1) persona cree que las herramientas tecnológicas externas pueden causar impacto en la

información y tres (3) se proyectan a creer que la capacitación será el puntal de defensa para enfrentar las amenazas.

Análisis. En el sector financiero cuando se presentan incidencias en las cooperativas o bancos, muchas veces se concluye que las personas en funciones, o desvinculadas, hacen mal uso de sus conocimientos tratando de manipular sistemas informáticos sensibles, muchas veces con la intención de conseguir recursos económicos o simplemente dañar la imagen institucional.

8. ***¿Cómo calificaría la protección de datos personales y financieros de los clientes en la cooperativa? (Escala de 1 a 5)***

1 2 3 4 5 (1, bueno – 5, malo).

Tabla 29 Pregunta 8

Respuesta	***Cantidad***	***Porcentaje***
1	*9*	*90%*
2	*1*	*10%*
3	*0*	*0%*
4	*0*	*0%*
5	*0*	*0%*
Total	*10*	*100%*

Fuente: Autor

Figura 28 Resultados Pregunta 8

Interpretación. Se concluye que se evidencia que los datos personales por parte de esta entidad financiera gozan de seguridad debido a que la información no está anclada a una sola persona, y que para ser divulgada se debe pasar por algunos filtros, situación que deriva a garantizar la protección de los datos, respuestas efectuadas por nueve (9) funcionarios, en tanto un (1) solo

funcionario compara la actividad de esta entidad con otras concluyendo que en todo el sistema financiero existen vulnerabilidad en el manejo de información.

Análisis. Se considera alta la calificación en la protección de datos debido a que es muy esporádico presenciar que algún socio o cliente, dé a conocer o exponga dificultades en el mal uso de sus datos.

9. ***¿Conoce Usted sobre incidentes tecnológicos en donde los socios han perdido dinero de sus cuentas? (Sí/No)***

Tabla 30 Pregunta 9

Respuesta	***Cantidad***	***Porcentaje***
Sí	*7*	*70%*
No	*3*	*30%*
Total	*10*	*100%*

Fuente: Autor

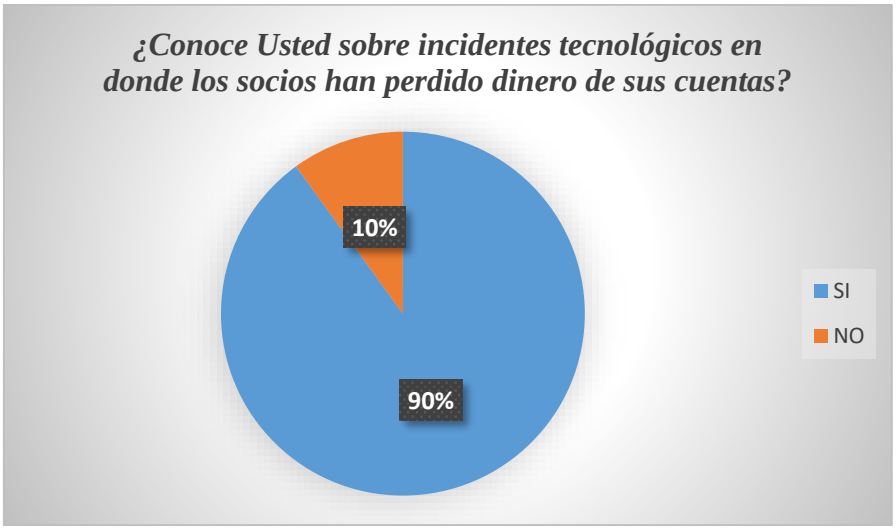

Figura 29 Resultados Pregunta 9

Interpretación. De las personas entrevistadas nueve (9) afirman que el sector cooperativo no es tan atractivo como el bancario, comparando que existen más incidencias de fuga de dinero, compras con tarjetas en el exterior, retiro en cajeros en bancos nacionales, mientras que sólo uno (1) desconoce de estos incidentes con los socios o las personas.

Análisis. La actividad cotidiana en el manejo de sistemas robustos que dispone esta entidad financiera hace que se conozca que es muy complicado pensar en que el dinero se pierda de las cuentas, los procesos diarios de cierres, las auditorias y los batchs que se ejecutan en planta central aseguran un manejo perfecto para resguardo del dinero que es de los clientes.

10. ¿Cree Usted que la Cooperativa cuenta con un sistema informático confiable para transaccionar? (Si/No)

Tabla 31 Pregunta 9

Respuesta	*Cantidad*	*Porcentaje*
Sí,	*10*	*100%*
No	*0*	*00%*
Total	*10*	*100%*

Fuente: Autor

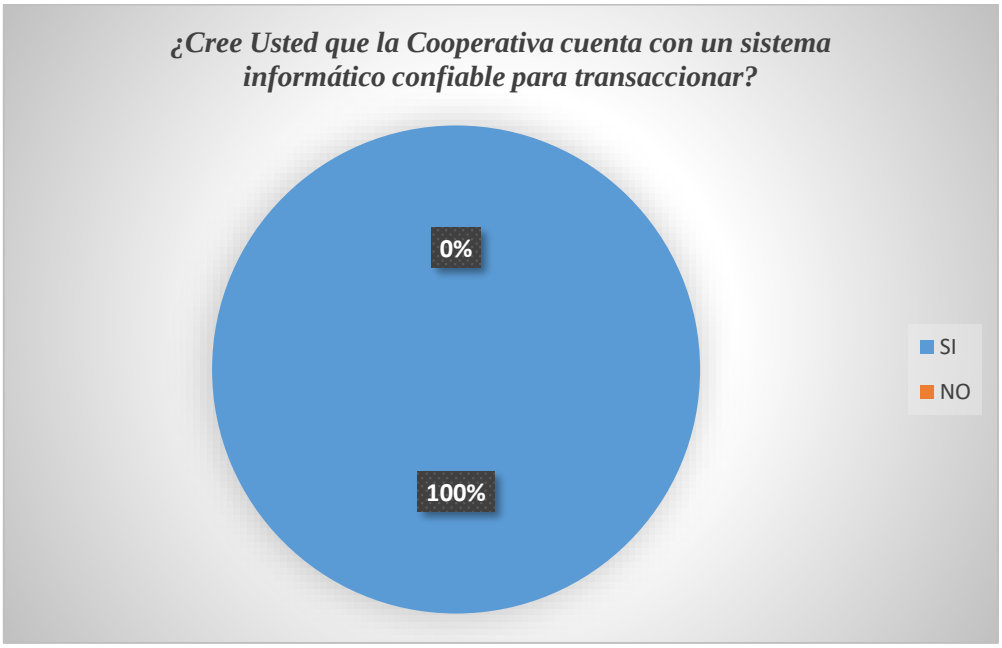

Figura 30 Resultados Pregunta 10

Interpretación. Las diez (10) personas hacen relación de que en esta entidad financiera no se evidencia de manera permanente socios con reclamos de perdida de información, dinero o documentos, procediendo a calificarlo, al sistema en general, como muy bueno.

Análisis. La percepción de los funcionarios sobre la confianza en el sistema informático para realizar transacciones es buena debido a la estabilidad, disponibilidad y eficiencia en todo momento, esto nos ha generado confianza a nosotros como empleados, reflejando seguridad en los socios al hacer uso de los cajeros automáticos, retiros en ventanilla, depósitos, depósitos a plazo fijo, etc.

Después de las encuestas levantadas a los funcionarios de Cooperativa de Ahorro y Crédito "Tulcán Ltda.", en concordancia con la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002; "*Art. 10.- Sistema de Gestión de Seguridad de la Información (SGSI).-* Las entidades, empresas y CONAFIPS que conforman el régimen de

cooperativas del segmento uno deberán implementar un SGSI orientado a garantizar la adecuada gestión de seguridad de la información, con base en la serie de estándares ISO/IEC 27000, y acorde a la normativa vigente, el mismo que establece el alcance del SGSI; deberán considerar:

1. Definición de tipos de información con criterios de integridad, confidencialidad y disponibilidad.
2. Identificación y clasificación de activos que debe contener:
    - personas.
    - procesos, agregadores de valor, catalogados como sensibles o críticos.
    - unidades intervinientes en los procesos.
    - infraestructura tecnológica.
    - ubicación física y puntos de atención.
    - relaciones con personas naturales y/o jurídicas que pudieren acceder a la información crítica o sensible.

Con los resultados obtenidos como base y en articulación con las áreas involucradas, se puede evaluar la efectividad o criticidad de las prácticas actuales de seguridad de la información, buscando proporcionar recomendaciones orientadas a su perfeccionamiento.

Mediante un análisis minucioso, y la elaboración de un plan de acción, la Cooperativa de Ahorro y Crédito “Tulcán Ldta.”, y en particular el área de Captaciones, puede fortalecer su postura de seguridad, optimizando la gestión de riesgos y garantizando una protección más efectiva de la información que abarca esta plaza, donde reposa información confidencial y sensible.

En honor a lo manifestado se detallan, los análisis que se han efectuado de acuerdo a la metodología Magerit.

- Listado y valoración de activos de la información.
- Análisis de riesgos.
    - Evaluación de riesgos.
    - Tratamiento de riesgos.
    - Cálculo de la valoración del impacto de los activos de información.

- Plan de tratamiento de riesgos.

Matriz de Activos de Información - Inventario y Clasificación

Versión	**1,0**
Fecha creación:	**16/3/2025**

No.	No. ACT		Fecha de Actualización	Proceso	Sub Proceso	Actvidad	Identificador del activo	Activo	Ámbito del activo (reclasificado)	Descripción del Activo	Categoría del activo	Dependencias de ac
1	A1	1	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_1	Recepción de requisitos	Actividades y procesos del negocio	Recepción de la información del socio/cliente	Documentación	Equipo de oficina, personas
2	A2	2	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_2	Validación de la información	Software	Verificación de la información receptada	Base de Datos	Equipo de oficina, personas, sistem
3	A3	3	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_3	Comunicación de información	Actividades y procesos del negocio	Comunicación del información al socio/cliente	Documentación	Equipo de oficina, personas, sistem
4	A4	4	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_4	Informar al oficial de cumplimiento	Actividades y procesos del negocio	Informa Oficial de Cumplimiento si consta en lista	Documentación	Equipo de oficina, personas, sistem
5	A5	5	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_5	Autorización Gerencia continuidad de ap	Actividades y procesos del negocio	Llenar ficha de Declaración sobre la condición de PEP	Documentación	Equipo de oficina, personas, sistem
6	A6	6	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_6	Verificar si consta en el Sistema	Software	Verifica con Nro. Cédula si consta en nuestro sistema	Base de Datos	Sistemas de Información
7	A7	7	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_7	Actualizar información del socio o cliente	Software	Actualizar información del socio o cliente en nuestro sistema	Base de Datos	Servidores de almacenimiento o pro
8	A8	8	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_8	Creación de clientes	Software	Ingreso de información en el sistema para creación de clientes o socios	Equipo Informático	Equipo informático, personas, servi almacenamiento
9	A9	9	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_9	Seleccionar el producto de ahorros	Software	Selección de producto de ahorro solicitado por el cliente	Servicio	Equipo de oficina, personas, sistem
10	A10	10	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_10	Impresión y legalización documentos	Actividades y procesos del negocio	Impresión y legalización documentos	Documentación	Equipo informático, personas
11	A11	11	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_11	Capturar, autorizar y asociar firmas	Software	Registro de firmas y asociar en nuestro sistema	Base de Datos	Equipo informático, personas, servi almacenamiento
12	A12	12	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_12	Escanear y legalizar contrato de seguro d	Actividades y procesos del negocio	Escanear y legalizar contrato de seguro de vida sino desea certificar oficio de operaciones	Aplicación	Equipo informático, personas
13	A13	13	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_13	Solicitud digital clientes que no desean se	Información	Solicitud digital clientes que no desean seguro de vida	Dispositivo de Almacenamiento	Sistemas de Información
14	A14	14	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_14	Notificación de la exclusión del débito	Actividades y procesos del negocio	Notificación al asistente de negocios la exclusión del débito	Documentación	Equipo informático, personas
15	A15	15	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_15	Retener la cédula de identidad hasta que	Información	Retener la cédula de identidad hasta que efectue la apertura de c	Documentación	personas
16	A16	16	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de cuentas de ahorros de personas naturales	ACT_P.CAP01_16	Validar depósitos iniciales y entrega de cé	Software	Validar depósitos iniciales y entrega de cédula al cliente	Base de Datos	Equipo informático, personas
17	A17	17	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_1	Asesorar al socio / cliente opciones de inv	Actividades y procesos del negocio	Asesorar al socio / cliente opciones de inversión	Documentación	Personas
18	A18	18	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_2	Ofrecer otras opciones de captación	Actividades y procesos del negocio	Ofrecer otras opciones de captación, obtener información del clie	Documentación	Personas
19	A19	19	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_3	Negociar condiciones, solicitar cédula	Actividades y procesos del negocio	Negociar condiciones, solicitar cédula y entregar requisitos	Documentación	Personas
20	A20	20	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_4	Coordinar la autorización de tasa	Actividades y procesos del negocio	Coordinar la autorización de tasa de acuerdo al nivel	Documentación	Equipo informático
21	A21	21	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_5	Revisar condiciones de negociación y au	Actividades y procesos del negocio	Revisar condiciones de negociación y autorizar incremento	Documentación	Equipo informático, personas
22	A22	22	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_6	Verificar con la cédula de socio o cliente	Software	Verificar con la cédula de socio o cliente si consta en listas de con	Base de Datos	Equipo informático, personas, servi almacenamiento o procesamiento
23	A23	23	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_7	Informar al socio si consta en lista para pr	Información	Informar al socio si consta en lista para presente certificación	Documentación	Equipo informático, personas, servi almacenamiento o procesamiento
24	A24	24	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_8	de Cumplimiento	Información	Informar vía correo electrónico al Oficial de Cumplimiento	Documentación	Equipo informático, personas
25	A25	25	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_9	Solicitar autorización a Gerencia General	Información	Solicitar autorización a Gerencia General y llenar ficha declaració	Documentación	Equipo informático, personas
26	A26	26	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_10	Verificar requisitos para DPF	Información	Verificar requisitos para DPF	Documentación	Personas
27	A27	27	1/1/2025	Gestión de Captaciones	Gestión de contratos de captaciones	Apertura de certificados de Depósito a Plazo Fijo	ACT_P.CAP02_11	Devolver documentos indicando las razo	Información	Devolver documentos indicando las razones	Documentación	Personas

Clasificiación de Información

Análisis de Riesgos							Evaluación de Riesgos					
							Impacto	Probabilidad				
Nro. Activo	Proceso Macro	Subprocesos	Nombre Activo	Tipo Activo-Ámbito	Vulnerabilidad	Amenaza	CID	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nro. Activo	Proceso Macro	Subprocesos	Nombre del Activo	Tipo Activo-Ámbito-reclasificado	Vulnerabilidad	Amenaza	CID	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
A1	Gestión de Captaciones	Gestión de contratos de captaciones	Recepción de requisitos	ActividadesProcesos	Recepción de documentos falso	Ingreso de datos falsos o corruptos	3,00	1	1	A.8.2.1-Clasificación de la información	3,00	BAJO-MUY BAJO
A2	Gestión de Captaciones	Gestión de contratos de captaciones	Validación de la información	Software	Información erronea	Modificación de la Información por Error	3,00	2	2	A.6.1.1-Seguridad de la información roles y responsabilidades	12,00	MUY ALTO
A3	Gestión de Captaciones	Gestión de contratos de captaciones	Comunicación de información	ActividadesProcesos	N/A	N/A	3,00			NA		
A4	Gestión de Captaciones	Gestión de contratos de captaciones	Informar al oficial de cumplimiento	ActividadesProcesos	Registro de datos erroneos	Modificación de la Información por Error	1,33	1	1	A.8.2.3-Manejo de activos	1,33	BAJO-MUY BAJO
A5	Gestión de Captaciones	Gestión de contratos de captaciones	Autorización Gerencia continuidad de apertura	ActividadesProcesos	Demora en proceso operativo	Ausencia de personal / Legalización de Documentación a destiempo	1,33	2	1	A.6.1.2-Separación de deberes	2,67	BAJO-MUY BAJO
A6	Gestión de Captaciones	Gestión de contratos de captaciones	Verificar si consta en el Sistema	Software	Error en proceso operativo	Falta de capacitación en procesos operativos	1,33	1	1	A.12.1.1-Documentación de los procedimientos de operación	1,33	BAJO-MUY BAJO
A7	Gestión de Captaciones	Gestión de contratos de captaciones	Actualizar información del socio o cliente	Software	Información erronea	Modificación de la Información por Error	1,67	2	2	A.12.1.1-Documentación de los procedimientos de operación	6,67	MEDIO
A8	Gestión de Captaciones	Gestión de contratos de captaciones	Creación de clientes	Software	Información erronea	Modificación de la Información por Error	1,67	1	1	A.6.1.1-Seguridad de la información roles y responsabilidades	1,67	BAJO-MUY BAJO
A9	Gestión de Captaciones	Gestión de contratos de captaciones	Seleccionar el producto de ahorros	Software	Error en proceso operativo	Falta de capacitación en procesos operativos	1,67	1	1	A.12.1.1-Documentación de los procedimientos de operación	1,67	BAJO-MUY BAJO
A10	Gestión de Captaciones	Gestión de contratos de captaciones	Impresión y legalización documentos	ActividadesProcesos	Perdida de documentos	Hurto de medios o documentos	2,00	2	1	A.12.1.1-Documentación de los procedimientos de operación	4,00	MEDIO
A11	Gestión de Captaciones	Gestión de contratos de captaciones	Capturar, autorizar y asociar firmas	Software	Error en proceso operativo	Falta de capacitación en procesos operativos	1,33	1	1	A.6.1.1-Seguridad de la información roles y responsabilidades	1,33	BAJO-MUY BAJO
A12	Gestión de Captaciones	Gestión de contratos de captaciones	Escanear y legalizar contrato de seguro de vida	ActividadesProcesos	Perdida de documentos	Hurto de medios o documentos	1,67	2	2	A.12.1.1-Documentación de los procedimientos de operación	6,67	MEDIO
A13	Gestión de Captaciones	Gestión de contratos de captaciones	Solicitud digital clientes que no desean seguro de vida	Información	Perdida de documentos	Hurto de medios o documentos	1,67	2	2	A.12.1.1-Documentación de los procedimientos de operación	6,67	MEDIO
A14	Gestión de Captaciones	Gestión de contratos de captaciones	Notificación de la exclusión del débito	ActividadesProcesos	Perdida de documentos	Hurto de medios o documentos	1,33	2	1	A.12.1.1-Documentación de los procedimientos de operación	2,67	BAJO-MUY BAJO
A15	Gestión de Captaciones	Gestión de contratos de captaciones	Retener la cédula de identidad hasta que efectue la apertu	Información	Perdida de documentos	Hurto de medios o documentos	1,33	2	1	A.12.1.1-Documentación de los procedimientos de operación	2,67	BAJO-MUY BAJO

Tablas de referencia | Instructivo | Evaluación de Riesgos | Opc. Tratamiento Riesgo | ControlesAnexoA | Tipo de amenazas | Valoración de Activos | **Análisis de Riesgos**

Tratamiento de Riesgos								Implementación de Control		
Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual	Actividades	Responsable	Entregables
Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual	Actividades	Responsable	Entregables
ACEPTAR	NO APLICA CONTROL	A.8.2.1-Clasificación de la información	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Segregar la funciones operativas del asistentes de nego	Jefe de Captaciones	Manual de funciones
MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.6.1.1-Seguridad de la información roles y responsabilidades	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones	Jefe de Captaciones	Manual y proceso actualizado
		A.12.1.1-Documentación de los procedimientos de operación						Actualización del proceso Actualización del manual de Captaciones	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	NO APLICA CONTROL	A.6.1.1-Seguridad de la información roles y responsabilidades						Actualización del proceso Actualización del manual de Captaciones	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	CONTROL CORRECTIVO	A.12.1.1-Documentación de los procedimientos de operación	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	NO APLICA CONTROL	A.8.1.3-Uso aceptable de los activos						Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12.1.1-Documentación de los procedimientos de operación	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	NO APLICA CONTROL	A.12.1.1-Documentación de los procedimientos de operación						Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	NO APLICA CONTROL	A.8.1.3-Uso aceptable de los activos						Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	A.12.1.1-Documentación de los procedimientos de operación	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	NO APLICA CONTROL	A.12.1.2-Gestión del cambios						Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12.1.1-Documentación de los procedimientos de operación	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12.1.1-Documentación de los procedimientos de operación	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	CONTROL CORRECTIVO	A.6.1.1-Seguridad de la información roles y responsabilidades	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado
ACEPTAR	CONTROL CORRECTIVO	A.6.1.2-Separación de deberes	1	1	3,00	BAJO-MUY BAJO	ACEPTABLE	Actualización del proceso Actualización del manual de Captaciones Socialización-Capacitación	Jefe de Captaciones	Manual y proceso actualizado

Tablas de referencia | Instructivo | Evaluación de Riesgos | Opc. Tratamiento Riesgo | ControlesAnexoA | Tipo de amenazas | Valoración de Activos | **Análisis de Riesgos**

CÁLCULO DE LA VALORACIÓN DEL IMPACTO DE LOS ACTIVOS DE INFORMACIÓN

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo (Ámbito)	Nombre de Activo	Descripción del activo	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
								C	I	D	VA
A1	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Recepción de requisitos	Recepción de la información del socio/cliente	Tangible	Archivo físico de cada Agencia	3	3	3	3.00
A2	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Validación de la información	Verificación de la información receptada	Intangible	Servidor del sistema financiero	3	3	3	3.00
A3	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Comunicación de información	Comunicación del información al socio/cliente	Intangible	Servidor del sistema financiero	3	3	3	3.00
A4	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Informar al oficial de cumplimiento	Informa Oficial de Cumplimiento si consta en lista	Intangible	Base de datos	2	1	1	1.33
A5	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Autorización Gerencia continuidad de apertura	Llenar ficha de Declaración sobre la condición de PEP	Tangible	Base de datos	2	1	1	1.33
A6	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Verificar si consta en el Sistema	Verifica con Nro. Cédula si consta en nuestro sistema	Intangible	Core Financiero	2	1	1	1.33
A7	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Actualizar información del socio o cliente	Actualizar información del socio o cliente en nuestro sistema	Intangible	Core Financiero	2	1	2	1.67
A8	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Creación de clientes	Ingreso de información en el sistema para creación de clientes o socios	Intangible	Core Financiero	2	1	2	1.67
A9	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Seleccionar el producto de ahorros	Selección de producto de ahorro solicitado por el cliente	Intangible	Core Financiero	2	1	2	1.67
A10	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Impresión y legalización documentos	Impresión y legalización documentos	Tangible	Archivo físico de cada Agencia	2	2	2	2.00
A11	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Capturar, autorizar y asociar firmas	Registro de firmas y asociar en nuestro sistema	Intangible	Archivo físico y core financiero	2	1	1	1.33
A12	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Escanear y legalizar contrato de seguro de vida	Escanear y legalizar contrato de seguro de vida sino desea notificar al jefe de operaciones	Tangible	Archivo físico	2	1	2	1.67
A13	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Solicitud digital clientes que no desean seguro de vida	Solicitud digital clientes que no desean seguro de vida	Intangible	Dispositivo de almacenamiento	2	1	2	1.67
A14	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Notificación de la exclusión del débito	Notificación al asistente de negocios la exclusión del débito	Intangible	equipo usuario	2	1	1	1.33
A15	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Retener la cédula de identidad hasta que efectue la apertura de cuenta en ventanilla	Retener la cédula de identidad hasta que efectue la apertura de cuenta en ventanilla	Tangible	N/D	2	1	1	1.33
A16	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Validar depósitos iniciales y entrega de cédula al cliente	Validar depósitos iniciales y entrega de cédula al cliente	Tangible	N/D	2	1	1	1.33
A17	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Asesorar al socio / cliente opciones de inversión	Asesorar al socio / cliente opciones de inversión	Intangible	Boveda de cada Agencia	2	1	1	1.33
A18	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Ofrecer otras opciones de captación	Ofrecer otras opciones de captación, obtener información del cliente y guardar digitalmente	Intangible	Boveda de cada Agencia	2	1	1	1.33
A19	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Negociar condiciones, solicitar cédula	Negociar condiciones, solicitar cédula y entregar requisitos	Intangible	Boveda de cada Agencia	2	1	1	1.33
A20	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Coordinar la autorización de tasa	Coordinar la autorización de tasa de acuerdo al nivel	Intangible	Boveda de cada Agencia	2	1	1	1.33
A21	Gestión de Captaciones	Gestión de contratos de captaciones	Actividades y procesos del negocio	Revisar condiciones de negociación y autorizar incremento	Revisar condiciones de negociación y autorizar incremento	Intangible	Boveda de cada Agencia	2	1	1	1.33
A22	Gestión de Captaciones	Gestión de contratos de captaciones	Software	Verificar con la cédula de socio o cliente si consta en listas de control	Verificar con la cédula de socio o cliente si consta en listas de control	Tangible	Boveda de cada Agencia	2	2	2	2.00
A23	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Informar al socio si consta en lista para presente certificación	Informar al socio si consta en lista para presente certificación	Intangible	Boveda de cada Agencia	3	2	2	2.33
A24	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Informar vía correo electrónico al Oficial de Cumplimiento	Informar vía correo electrónico al Oficial de Cumplimiento	Tangible	Boveda de cada Agencia	2	1	1	1.33
A25	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Solicitar autorización a Gerencia General	Solicitar autorización a Gerencia General y llenar ficha declaración PEP	Intangible	Boveda de cada Agencia	2	1	1	1.33
A26	Gestión de Captaciones	Gestión de contratos de captaciones	Información	Verificar requisitos para DPF	Verificar requisitos para DPF	Intangible	Boveda de cada Agencia	2	1	1	1.33

CAPITULO V
PROPUESTA

5.1 Determinación del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) para Cooperativa de Ahorro y Crédito "Tulcán Ltda."

El alcance del SGSI deberá estar estructurado bajo el siguiente esquema.

5.1.1 Objetivo

Establecer el Plan de Implementación del Sistema de Gestión de Seguridad de la Información en la Cooperativa de Ahorro y Crédito "Tulcán Ltda.", basado en la norma ISO 27001 y alineado a los objetivos estratégicos institucionales, con la finalidad de proteger los activos de información de la Institución e infraestructura tecnológica.

5.1.2 Justificación

El establecimiento de un sistema de gestión de seguridad de la información (SGSI), permitirá asegurar que se implementen los controles de seguridad adecuados sobre la confidencialidad, disponibilidad e integridad de la información, protegiendo de esta forma la información de todas las partes interesadas, adicional a esto el cumplimiento de la norma SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 y la ISO 27001 permitirá establecer los marcos de seguridad que garanticen la seguridad de la información y su vez minimicen los riesgos de naturaleza no financiera derivados de un impacto por una gestión ineficaz de la misma.

5.1.3 Políticas de Seguridad

En el sistema de Gestión de Seguridad de la Información, una de fases importantes es la constitución de las políticas de seguridad de la información las mismas que se encuentran alineadas a los objetivos Institucionales de la Cooperativa.

También se constituirá la Política General de Seguridad de la Información que permitirá establecer los lineamientos generales del Sistema de Gestión de Seguridad de la Información.

5.1.4 Procedimientos de Auditorías

El procedimiento de revisión a través de auditorías permitirá establecer la consistencia y efectividad del Sistema de Gestión de Seguridad de la Información de acuerdo con los planes, procedimientos, registros y controles establecidos, si es conforme con los requisitos de la

norma ISO 27001: y es eficaz para satisfacer los requisitos relacionados con seguridad de la información.

De acuerdo con los informes que se generen en las auditorías se corroborará las regulaciones preestablecidas relacionadas con la norma ISO/IEC 27001 y los objetivos Institucionales de la Cooperativa.

5.1.5 Estructura Organizacional de la Seguridad de la Información

Con el objetivo de establecer una estructura de organización de la Seguridad de la Información alineados a las mejores prácticas internacionales (ISO 27001) y de acuerdo con la norma de control de seguridad de la información emitida por el ente regulatorio SEPS, deberá de existir un departamento de Seguridad de la Información que permita gestionar de forma transversal los diferentes lineamientos de la seguridad de la Cooperativa; así mismo el apoyo de la alta Gerencia, el mismo que se constituye un pilar fundamental para el buen desempeño de todas las fases de implementación del SGSI.

5.1.6 Gestión de Indicadores

- Los indicadores son parámetros generales que guían el proceso de evaluación de la eficiencia y eficacia del SGS.
- La efectividad del sistema es proporcional a la efectividad de los controles implementados en la Cooperativa, y los indicadores son el medio para obtener la información.
- En base a los resultados de los indicadores, es posible generar un informe del estado de la gestión de seguridad de la información.

5.1.7 Procedimiento de Revisión por la Alta Dirección

El Sistema de Gestión de Seguridad de la Información (SGSI) contempla una evaluación periódica, sistemática y estructurada a cargo de la Alta Dirección que permite asegurar una adecuada planeación y corrección de las desviaciones en el cumplimiento de los objetivos, y, como tal, incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la Entidad promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.

5.1.8 Gestión de Roles y Responsabilidades

La implementación del SGSI, y los procesos definidos en él, generará la necesidad de establecer roles y responsabilidades los cuales son necesarios para evitar riesgos de una gestión y ejecución de tareas de seguridad incorrectas. En este sentido una de las primeras tareas a realizar en la implementación del SGSI es conformar una estructura interna directamente responsable de la seguridad de la información, permitiendo la creación, mantenimiento, supervisión y mejora del SGSI.

5.1.9 Metodología de Análisis de Riesgos

La implementación del SGSI según la norma ISO/IEC 27001 requiere de un análisis de riesgos, con el fin de obtener una perspectiva objetiva de los peligros que pudiere enfrentar la Cooperativa, por ello la metodología de evaluación de los riesgos de seguridad de la información de la Cooperativa será Magerit. Los resultados del análisis de riesgos permitirán a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

5.1.10 Declaración de Aplicabilidad

La declaración de aplicabilidad es un requisito fundamental de la norma ISO/IEC 27001, ya que permitirá registrar y controlar las medidas de seguridad aplicadas en el Sistema de Gestión de Seguridad de la Información, ésta describe todos los controles de seguridad aplicables y los controles que no cumplen con los requisitos.

5.2 Medidas para abordar los riesgos y las oportunidades

En esta fase del SGSI la estrategia de evaluación de riesgos y la planificación para el tratamiento de los mismos de Seguridad de la Información, la estructura de ISO / IEC 27001 subdivide los riesgos en dos categorías durante la planificación:

a) riesgos y oportunidades relevantes para los resultados previstos del SGSI en su conjunto.

b) riesgos de seguridad de la información que se relacionan con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI.

La primera categoría debe manejarse de acuerdo con los requisitos especificados en ISO/IEC 27001.

Los riesgos que caen en esta categoría pueden estar relacionados con el SGSI en sí, la definición del alcance del SGSI, el compromiso de la alta dirección con la seguridad de la información, los recursos para operar el SGSI, etc. Las oportunidades que caen en esta categoría pueden ser oportunidades relacionadas con el resultado (s) del SGSI, el valor comercial de un SGSI, la eficiencia de los procesos operativos del SGSI y los controles de seguridad de la información, etc.

La segunda categoría comprende todos los riesgos que se relacionan directamente con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI.

5.3 Objetivos del Sistema de Seguridad de la Información y los Planes para lograrlo.

5.3.1 Objetivos del SGSI

Los objetivos planteados en la Política General de Seguridad de la Información están contemplados de la siguiente forma:

- Establecer las políticas, prácticas y lineamientos que permitan a la Cooperativa garantizar la adecuada protección de todos sus activos de información y prevenir la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.
- Asegurar que se proporcione una adecuada protección contra las amenazas a la información de la Cooperativa, garantizando así la Confidencialidad, Integridad y Disponibilidad de la información adecuada a las necesidades de la Institución.
- Asegurar que los activos de la Cooperativa estén protegidos y permanezcan disponibles.
- Asegurar que la Cooperativa implemente y mantenga el estándar mínimo de seguridad definido en las políticas de seguridad global de la Cooperativa o definido en cualquier normativa o política aplicable.
- Asegurar que la información de la Cooperativa, compartida con otras partes, esté protegida contra la divulgación no autorizada y se gestione de acuerdo con esta política.
- Asegurar que la Cooperativa implemente los requisitos de ISO.
- Velar por que todos los funcionarios, empleados y directivos conozcan y cumplan los requisitos legales y reglamentarios aplicables.
- Crear y mantener la conciencia de la gestión y del personal de la Cooperativa sobre la seguridad de la información, garantizando así que todos los empleados entiendan su

importancia para la Cooperativa y sus propias responsabilidades individuales en materia de seguridad.

• Asegurar que las personas que desempeñan funciones de seguridad identificadas reciban una formación especializada en consonancia con sus responsabilidades en materia de seguridad.

• Asegurar que todas las infracciones de seguridad de la información, reales o sospechosas sean reportadas e investigadas por el Departamento de Seguridad de la Información.

5.4 Mejora continua

Esta fase corresponde a la entrega de los documentos descritos como entregables respecto de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), y de la norma de control de seguridad emitida por el ente regulatorio -SEPS-.

- El Sistema de Gestión de Seguridad de la Información (SGSI) será actualizado y mejorado de forma permanente en los siguientes ámbitos de gestión:
- En los casos en que los funcionarios detecten o notifiquen situaciones que vulneren los esquemas de seguridad.
- Monitoreo permanente de la aplicación del plan de concienciación en temas de seguridad para los funcionarios.
- Validación del cumplimiento de las políticas y procedimientos entorno al SGSI.
- Monitoreo de ejecución del Plan Estratégico de Seguridad de la Información.
- Los controles de seguridad de la información que actualmente se están gestionando con el área de Captaciones de acuerdo con el Anexo A de la norma de control SEP-2022-022 pueden incrementarse o modificarse según la necesidad en que se lo requiera durante la implementación del SGSI.
- El Sistema de Gestión de Seguridad de la Información (SGSI), considerada una de las mejores prácticas y herramientas, permite la adecuada gestión de los riesgos al interior de la Institución y el cumplimiento de la seguridad de la información bajo un marco de referencia que garantiza su gestión y continuidad a lo largo del tiempo.
- El SGSI, efectivamente se aborda bajo una normativa reconocida como la ISO/IEC 27001, cuya implantación asegura a la Entidad gozar de un correcto gobierno de seguridad de la información que garantizará la protección de los activos, maximizar el retorno de las inversiones y asegurar la continuidad del negocio.

- El Sistema de Gestión de Seguridad de la Información (SGSI) se debe convertir al interior de la entidad en un proceso sistemático de revisión y mejora continua a través de herramientas como las auditorías internas de cumplimiento que garanticen la mantenibilidad del sistema.
- La correcta y continua gestión del SGSI se logra con la implantación correcta de políticas, procesos, procedimientos, una adecuada estructura organizacional, controles, y, lo más importantes, con la concientización del recurso humano acerca de la importancia de la seguridad de la Información, contando especialmente con el apoyo total de la Alta Dirección.

5.4.1 Documentos de referencia

- ✓ Constitución de la República del Ecuador.
- ✓ Plan de Gestión de Riesgos de Seguridad de la Información.
- ✓ Metodología de Gestión de Riesgos de Seguridad de la Información.
- ✓ Metodología de inventario y clasificación de los activos de información.
- ✓ Documento de Declaración de Aplicabilidad de los controles de Seguridad de la Información. según la Norma Internacional ISO 27002.
- ✓ Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.
- ✓ Ley de Protección de Datos.
- ✓ Metodología de Análisis y Gestión de Riesgos de los Sistema de Información.

Referencias

2700, I. (2005). *iso2700.es*. Obtenido de https://www.iso27000.es/iso27002_6.html

Alvarado, C. (10 de 01 de 2025). *gestion.pensemos.com*. Obtenido de gestion.pensemos.com: https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Ambato, U. T. (07 de 2015). *Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato*. Obtenido de Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato: https://repositorio.uta.edu.ec/items/53903a88-573e-4c7a-8e00-c500861ec811?utm_source=chatgpt.com

Ana, & Guzman , A. D. (02 de 2024). Jefa de Captaciones y medios electronicos. (A. López, Entrevistador)

Anton Peregrina, E. (10 de 10 de 2020). *Seguridad de la información: realidad o Utopia*. Obtenido de https://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia

AqaEcuador, & Aqa, E. (10 de 10 de 2022). *Sistemas de Gestión*. Obtenido de https://eqaecuador.com/iso-27001/?gad_source=1&gclid=CjwKCAjw48-vBhBbEiwAzqrZVOZobKZTq7XPyGTEwZG4lHlQR6Mvm9DRVhiz6grl7ZLm7_Tn84X2kRoCSsAQAvD_BwE

Asamblea Constituyente . (25 de 01 de 2008). *Constitución de la República del Ecuador*. Obtenido de Constitución de la República del Ecuador: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Asamblea Nacional. (17 de 02 de 2021). *CODIGO ORGANICO INTEGRAL COIP*. Obtenido de CODIGO ORGANICO INTEGRAL COIP: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Asamblea Nacional, d. E. (26 de 05 de 2021). *Ley de Proteccion de datos personales*. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asamblea, N. (29 de dic de 2017). *LEY ORGÁNICA DEL SISTEMA NACIONAL DE REGISTRO*. Obtenido de LEY ORGÁNICA DEL SISTEMA NACIONAL DE REGISTRO: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/01/LEY-ORGANICA-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf

Check, P. (2024). *Tipos de amenazas de ciberseguridad*. Obtenido de Tipos de amenazas de ciberseguridad: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

Cooperativa de Ahorro y Crédito Tulcán. (2024). Información Financiera. *Memoria Insitucional*, 5-6.

CYNTHUS. (10 de 10 de 2022). *Seguridad de la Informacion y Ciberseguridad* . Obtenido de https://www.cynthus.com.mx/iso-27002-diferencias-con-iso-27001/

EGS , I. G. (2024). *ISO 27015 para servicios financieros*. Obtenido de https://www.pmg-ssi.com/2014/03/iso-27015-para-servicios-financieros/

Electrónica, Administración. (2024). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Escuela Europa Excelencia. (2025). *Gestión de activos según ISO 27001: cómo administrar un inventario de activos*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2023/12/gestion-de-activos-segun-iso-27001-como-administrar-un-inventario-de-activos/

Gómez José María. (01 de 05 de 2023). *Reorientación estratégica de una empresa de servicios de seguridad de.* Obtenido de Reorientación estratégica de una empresa de servicios de seguridad de: https://repositorio.uasb.edu.ec/bitstream/10644/9328/1/T4086-MAE-Gomez-Reorientacion.pdf

Guerrero, S. (07 de 02 de 2025). *factorial.es*. Obtenido de factorial.es: https://factorial.es/blog/iso-27000/

Hernández , R., Férnandez, C., & Baptista , P. (04 de 2014). *El Porta de la Tesis*. Obtenido de https://recursos.ucol.mx/tesis/investigacion.php

Higuera, J. (02 de 2024). SGSI Coop Tulcan. (A. López, Entrevistador)

Higuera, J. (2025). *Plan Estratégico de Seguridad de la Información.*

Jhony, H. (2024). *Plan de gestion de riesgos de seguridad de la informacion.* Tulcan.

Lopez, A. (05 de 10 de 2005). *Iso27000.es*. Obtenido de https://www.iso27000.es/iso27002_7.html

López, N. A. (2005). *Iso 2700 es*. Obtenido de https://www.iso27000.es/

Lukas, A. (14 de 01 de 2015). *Diseño y estructura de una guía para la documentación de un Sistema de Gestión de la Seguridad de la Información con base en la norma Iso/IEC 27001:2005*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/16176/DISE%C3%91O%20Y%20ESTRUCTURA%20DE%20UNA%20GUIA.pdf?sequence=1

MAGERIT, V. (2012). *Metodología de análisis y Gestión de Riesgos de los sistemas de información.* Obtenido de Metodología de análisis y Gestión de Riesgos de los sistemas de información.: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Margarita Hernandez. (03 de 05 de 2022). *Superintendencia Economia Popular y Solidaria*. Obtenido de Superintendencia Economia Popular y Solidaria: https://www.seps.gob.ec/resoluciones-de-entidades-del-sector-financiero-popular-y-solidario/

Margarita, H. (03 de 05 de 2022). *Superintendencia Economia Popular y Solidaria*. Obtenido de Superintendencia Economia Popular y Solidaria: https://www.seps.gob.ec/resoluciones-de-entidades-del-sector-financiero-popular-y-solidario/

Mendoza, M. A. (05 de 04 de 2023). *welivesecurity*. Obtenido de https://www.welivesecurity.com/

Morales Alomoto, L. (24 de 10 de 2018). *"BALANCED SCORECARD PARA SEGURIDAD DE LA INFORMACIÓN*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/29216/1/Tesis_%20t1537msi.pdf

Pilla, Y. C. (10 de marzo de 2019). *Políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el departamento de tecnología de la cooperativa de ahorro y crédito San Francisco LTDA.* Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/34814

Pirani, A. (2024). *Guía para realizar la evaluación de riesgos*. Obtenido de Guía para realizar la evaluación de riesgos: https://www.piranirisk.com/es/academia/especiales/guia-para-realizar-la-evaluacion-del-riesgo

Porras Ruiz, M. A. (01 de 01 de 2019). *Sistema de Gestión de Seguridad de la Información para la Gestión de Riesgos en Axctivos de Inofrmacion*. Obtenido de https://journalprosciences.com/index.php/ps/article/view/527/576

Suarez, L. (06 de 2013). *Trabajo final de master*. Obtenido de https://openaccess.uoc.edu/bitstream/10609/23143/7/lsuarezsiTFM0613memoria.pdf

Suites, G. (2024). *¿Qué es la norma ISO 27001 y para qué sirve?* Obtenido de ¿Qué es la norma ISO 27001 y para qué sirve?: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Torres, E. (10 de marzo de 2022). *Repositorio Universidad Técnica de Ambato*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/34814/1/t1959si.pdf

Turner, B. (10 de 2024). *¿Qué es Análisis de Riesgos? Procesos, Tipos y Elementos* . Obtenido de ¿Qué es Análisis de Riesgos? Procesos, Tipos y Elementos : https://osheblog.com/es/analisis-de-riesgos/

wordpress.com. (5 de Octubre de 2020). *www.wordpresscom*. Obtenido de https://interpolados.wordpress.com/2020/10/05/magerit-3-0-el-analisis-y-el-tratamiento-de-los-riesgos-en-su-contexto/

Anexos

Preguntas para los trabajadores (empleados de la cooperativa) sobre la Seguridad de la información.

1. ¿Conoce Usted la existencia de políticas de seguridad de la información en la Cooperativa? (**Sí/No**)

   Si ( ) No ( )

2. ¿Recibió capacitación en seguridad de información en los últimos 12 meses? (**Sí/No**)

   Si ( ) No ( )

3. ¿Con qué frecuencia cambia sus contraseñas de acceso a los sistemas internos?

   a) Cada mes b) Cada tres meses c) Cada seis meses o más d) Nunca

4. ¿Qué tan seguro considera que es el sistema informático de la Cooperativa para proteger los datos de los clientes? (Escala de 1 a 5)

   1 2 3 4 5

5. ¿Ha detectado o ha sido víctima de algún incidente relacionado con la seguridad de la información (phishing, fuga de datos, accesos no autorizados, etc.)? (**Sí/No**).

   Si ( ) No ( )

6. ¿Utiliza dispositivos personales para acceder a información confidencial de la cooperativa? (**Sí/No**)

   Si ( ) No ( )

7. ¿Cuál considera que es la principal amenaza para la seguridad de la información en la Cooperativa?

   a) Uso inadecuado por parte de los empleados

   b) Ataques externos (hackers, malware)

   c) Falta de capacitación en seguridad

   d) Falta de inversión en tecnología de seguridad

8. ¿Cómo calificaría la protección de datos personales y financieros de los clientes en la Cooperativa? (Escala de 1 a 5)

   1 2 3 4 5

9. ¿Conoce Usted de incidentes tecnológicos en donde los socios han perdido dinero de sus cuentas? (**Sí/No**)

   Si ( ) No ( )

10. ¿Cree Usted que la Cooperativa cuenta con un sistema informático confiable para transaccionar? **(Si/No).**

    Si ( ) No ( )

Anexo Aplicabilidad Controles ISO 27002:2013

ANEXO A - NTC-ISO-IEC 27002:2013

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
A.5	Política de Seguridad	A.5.1	Política de Seguridad de la Información	A.5.1.1	A.5.1.1-Políticas para la seguridad de la información
				A.5.1.2	A.5.1.2-Revisión de la política de seguridad de la información
A.6	Organización de la Seguridad de la Información	A.6.1	Organización interna	A.6.1.1	A.6.1.1-Seguridad de la información roles y responsabilidades
				A.6.1.2	A.6.1.2-Separación de deberes
				A.6.1.3	A.6.1.3-Contacto con las autoridades
				A.6.1.4	A.6.1.4-Contacto con grupos de interés especial
				A.6.1.5	A.6.1.5-Seguridad de la información en gestión de proyectos
		A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1	A.6.2.1-Política para dispositivos móviles
				A.6.2.2	A.6.2.2-Teletrabajo
A.7	Seguridad de los Recursos Humanos	A.7.1	Antes de asumir el empleo	A.7.1.1	A.7.1.1-Selección
				A.7.1.2	A.7.1.2-Términos y condiciones del empleo
		A.7.2	Durante la ejecución del empleo	A.7.2.1	A.7.2.1-Responsabilidades de la dirección
				A.7.2.2	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
				A.7.2.3	A.7.2.3-Proceso disciplinario
		A.7.3	Terminación o cambio de empleo	A.7.3.1	A.7.3.1-Terminación o cambio de responsabilidades de empleo
A.8	Gestión de Activos	A.8.1	Responsabilidad por los activos	A.8.1.1	A.8.1.1-Inventario de activos
				A.8.1.2	A.8.1.2-Propiedad de los activos
				A.8.1.3	A.8.1.3-Uso aceptable de los activos
				A.8.1.4	A.8.1.4-Devolución de activos
		A:8.2	Clasificación de la información	A.8.2.1	A.8.2.1-Clasificación de la información
				A.8.2.2	A.8.2.2-Etiquetado de la información
				A.8.2.3	A.8.2.3-Manejo de activos
		A.8.3	Manejo de Medios	A.8.3.1	A.8.3.1-Gestión de medios de soporte removibles
				A.8.3.2	A.8.3.2-Disposición de los medios de soporte
				A.8.3.3	A.8.3.3-Transferencia de medios de soporte físicos
A.9	Control de Acceso	A.9.1	Requisitos del Negocio para Control de Acceso	A.9.1.1	A.9.1.1-Política de control de acceso
				A.9.1.2	A.9.1.2-Acceso a redes y a servicios en red
		A.9.2	Gestión de acceso de usuarios	A.9.2.1	A.9.2.1-Registro y cancelación del registro de usuarios
				A.9.2.2	A.9.2.2-Suministro de acceso de usuarios

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
				A.9.2.3	A.9.2.3-Gestión de derechos de acceso privilegiado
				A.9.2.4	A.9.2.4-Gestión de información de autenticación secreta de usuarios
				A.9.2.5	A.9.2.5-Revisión de los derechos de acceso de usuarios
				A.9.2.6	A.9.2.6-Retiro o ajuste de los derechos de acceso
		A.9.3	Responsabilidades de los usuarios	A.9.3.1	A.9.3.1-Uso de información de autenticación secreta
		A.9.4	Control de Acceso a Sistemas y Aplicaciones	A.9.4.1	A.9.4.1-Restricción de acceso a información
				A.9.4.2	A.9.4.2-Procedimiento de ingreso seguro
				A.9.4.3	A.9.4.3-Sistema de gestión de contraseñas
				A.9.4.4	A.9.4.4-Uso de programas utilitarios privilegiados
				A.9.4.5	A.9.4.5-Control de acceso a códigos fuente de programas
A.10	Criptografía	A.10.1	Controles Criptográficos	A.10.1.1	A.10.1.1-Política sobre el uso de controles criptográficos
				A.10.1.2	A.10.1.2-Gestión de Llaves
A.11	Seguridad Física y del Entorno	A.11.1	Áreas Seguras	A.11.1.1	A.11.1.1-Perímetro de seguridad física
				A.11.1.2	A.11.1.2-Controles de acceso físico

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
				A.11.1.3	A.11.1.3-Seguridad de oficinas, recintos e instalaciones
				A.11.1.4	A.11.1.4-Protección contra amenazas externas y ambientales
				A.11.1.5	A.11.1.5-Trabajo en áreas seguras
				A.11.1.6	A.11.1.6-Áreas de carga, despacho y acceso público
		A-11.2	Equipos	A.11.2.1	A.11.2.1-Ubicación y protección de los equipos
				A.11.2.2	A.11.2.2-Servicios públicos de soporte
				A.11.2.3	A.11.2.3-Seguridad del cableado
				A.11.2.4	A.11.2.4-Mantenimiento de los equipos
				A.11.2.5	A.11.2.5-Retiro de activos
				A.11.2.6	A.11.2.6-Seguridad de los equipos y activos fuera de las instalaciones
				A.11.2.7	A.11.2.7-Disposición segura o reutilización de equipos
				A.11.2.8	A.11.2.8-Equipos de usuario desatendido
				A.11.2.9	A.11.2.9-Política de escritorio limpio y pantalla limpia
A.12	Seguridad de las Operaciones	A.12.1	Procedimientos Operacionales y Responsabilidades	A.12.1.1	A.12.1.1-Documentación de los procedimientos de operación

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
				A.12.1.2	A.12.1.2-Gestión del cambios
				A.12.1.3	A.12.1.3-Gestión de la capacidad
				A.12.1.4	A.12.1.4-Separación de los ambientes de desarrollo, pruebas y operación
		A.12.2	Protección Contra Códigos Maliciosos	A.12.2.1	A.12.2.1-Controles contra códigos maliciosos.
		A.12.3	Copias de Respaldo	A.12.3.1	A.12.3.1-Copias de respaldo de la información
		A.12.4	Registro y Seguimiento	A.12.4.1	A.12.4.1-Registro de eventos
				A.12.4.2	A.12.4.2-Protección de la información de registro
				A.12.4.3	A.12.4.3-Registros del administrador y del operador
				A.12.4.4	A.12.4.4-Sincronización de relojes
		A12.5	Control de Software Operacional	A.12.5.1	A.12.5.1-Instalación de software en sistemas operativos
		A.12.6	Gestión de la Vulnerabilidad Técnica	A.12.6.1	A.12.6.1-Gestión de las vulnerabilidades técnicas
				A.12.6.2	A.12.6.2-Restricciones sobre la instalación de software.
		A.12.7	Consideraciones sobre Auditorias de Sistemas de Información	A.12.7.1	A.12.7.1-Controles de auditorías de sistemas de información.
A.13	Seguridad de las Comunicaciones	A.13.1	Gestión de la Seguridad de las Redes	A.13.1.1	A.13.1.1-Controles de redes

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
				A.13.1.2	A.13.1.2-Seguridad de los servicios de red.
				A.13.1.3	A.13.1.3-Separación en las redes
		A.13.2	Transferencia de Información	A.13.2.1	A.13.2.1-Políticas y procedimientos de transferencia de información
				A.13.2.2	A.13.2.2-Acuerdos sobre transferencia de información
				A.13.2.3	A.13.2.3-Mensajes electrónicos
				A.13.2.4	A.13.2.4-Acuerdos de confidencialidad o de no divulgación
A.14	Adquisición, Mantenimiento y Desarrollo de Sistemas	A.14.1	Requisitos de seguridad de los sistemas de información	A.14.1.1	A.14.1.1-Análisis y especificación de requisitos de seguridad de la información
				A.14.1.2	A.14.1.2-Seguridad de servicios de las aplicaciones en redes públicas
				A.14.1.3	A.14.1.3-Protección de transacciones de servicios de aplicaciones
		A.14.2	Seguridad en los procesos de desarrollo y soporte	A.14.2.1	A.14.2.1-Política de desarrollo seguro
				A.14.2.2	A.14.2.2-Procedimientos de control de cambios en sistemas
				A.14.2.3	A.14.2.3-Revisión técnica de aplicaciones después de cambios en la

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
					plataforma de operaciones
				A.14.2.4	A.14.2.4-Restricciones en los cambios a los paquetes de software
				A.14.2.5	A.14.2.5-Principios de construcción de los sistemas seguros
				A.14.2.6	A.14.2.6-Ambiente de desarrollo seguro
				A.14.2.7	A.14.2.7-Desarrollo contratado externamente
				A.14.2.8	A.14.2.8-Pruebas de seguridad de sistemas
				A.14.2.9	A.14.2.9-Prueba de aceptación de sistemas
		A.14.3	Datos de prueba	A.14.3.1	A.14.3.1-Protección de datos de prueba
A.15	Relaciones con los Proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1	A.15.1.1-Política de seguridad de la información para las relaciones con proveedores
				A.15.1.2	A.15.1.2-Tratamiento de la seguridad dentro de los acuerdos con proveedores
				A.15.1.3	A.15.1.3-Cadena de suministro de tecnología de información y comunicación
		A.15.2	Gestión de la prestación de servicios de proveedores	A.15.2.1	A.15.2.1-Seguimiento y revisión de los servicios de los proveedores
				A.15.2.2	A.15.2.2-Gestión de cambios a los servicios de los proveedores

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
A.16	Gestión de Incidentes de Seguridad de la Información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	A.16.1.1-Responsabilidades y procedimientos
				A.16.1.2	A.16.1.2-Reporte de eventos de seguridad de la información
				A.16.1.3	A.16.1.3-Reporte de debilidades de seguridad de la información
				A.16.1.4	A.16.1.4-Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
				A.16.1.5	A.16.1.5-Respuesta a incidentes de seguridad de la información
				A.16.1.6	A.16.1.6-Aprendizaje obtenido de los incidentes de seguridad de la información
				A.16.1.7	A.16.1.7-Recolección de evidencia
A.17	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	A.17.1	Continuidad de Seguridad de la Información	A.17.1.1	A.17.1.1-Planificación de la continuidad de la seguridad de la información
				A.17.1.2	A.17.1.2-Implementación de la continuidad de la seguridad de la información
				A.17.1.3	A.17.1.3-Verificación, revisión y evaluación de la continuidad de la seguridad de la información

ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
		A.17.2	Redundancias	A.17.2.1	A.17.2.1-Disponibilidad de instalaciones de procesamiento de información
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1	A.18.1.1-Identificación de la legislación aplicable y de los requisitos contractuales
				A.18.1.2	A.18.1.2-Derechos de propiedad intelectual
				A.18.1.3	A.18.1.3-Protección de registros
				A.18.1.4	A.18.1.4-Privacidad y protección de información de datos personales
				A.18.1.5	A.18.1.5-Reglamentación de controles criptográficos
		A.18.2	Revisiones de seguridad de la información	A.18.2.1	A.18.2.1-Revisión independiente de la seguridad de la información
				A.18.2.2	A.18.2.2-Cumplimiento con las políticas y normas de seguridad
				A.18.2.3	A.18.2.3-Revisión del cumplimiento técnico

ANEXO A - NTC-ISO-IEC 27002:2013					
ID Dominio	Dominio	ID Objetivo de Control	Objetivo de Control	ID Control	Control
A.5	Política de Seguridad	A.5.1	Política de Seguridad de la Información	A.5.1.1	A.5.1.1-Políticas para la seguridad de la información
				A.5.1.2	A.5.1.2-Revisión de la política de seguridad de la información

A.6	Organización de la Seguridad de la Información	A.6.1	Organización interna	A.6.1.1	A.6.1.1-Seguridad de la información roles y responsabilidades
				A.6.1.2	A.6.1.2-Separación de deberes
				A.6.1.3	A.6.1.3-Contacto con las autoridades
				A.6.1.4	A.6.1.4-Contacto con grupos de interés especial
				A.6.1.5	A.6.1.5-Seguridad de la información en gestión de proyectos
		A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1	A.6.2.1-Política para dispositivos móviles
				A.6.2.2	A.6.2.2-Teletrabajo
A.7	Seguridad de los Recursos Humanos	A.7.1	Antes de asumir el empleo	A.7.1.1	A.7.1.1-Selección
				A.7.1.2	A.7.1.2-Términos y condiciones del empleo
		A.7.2	Durante la ejecución del empleo	A.7.2.1	A.7.2.1-Responsabilidades de la dirección
				A.7.2.2	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información
				A.7.2.3	A.7.2.3-Proceso disciplinario
		A.7.3	Terminación o cambio de empleo	A.7.3.1	A.7.3.1-Terminación o cambio de responsabilidades de empleo
A.8	Gestión de Activos	A.8.1	Responsabilidad por los activos	A.8.1.1	A.8.1.1-Inventario de activos
				A.8.1.2	A.8.1.2-Propiedad de los activos
				A.8.1.3	A.8.1.3-Uso aceptable de los activos
				A.8.1.4	A.8.1.4-Devolución de activos
		A:8.2	Clasificación de la información	A.8.2.1	A.8.2.1-Clasificación de la información
				A.8.2.2	A.8.2.2-Etiquetado de la información
				A.8.2.3	A.8.2.3-Manejo de activos
		A.8.3	Manejo de Medios	A.8.3.1	A.8.3.1-Gestión de medios de soporte removibles
				A.8.3.2	A.8.3.2-Disposición de los medios de soporte
				A.8.3.3	A.8.3.3-Transferencia de medios de soporte físicos
A.9	Control de Acceso	A.9.1	Requisitos del Negocio para Control de Acceso	A.9.1.1	A.9.1.1-Política de control de acceso
				A.9.1.2	A.9.1.2-Acceso a redes y a servicios en red
		A.9.2	Gestión de acceso de usuarios	A.9.2.1	A.9.2.1-Registro y cancelación del registro de usuarios
				A.9.2.2	A.9.2.2-Suministro de acceso de usuarios
				A.9.2.3	A.9.2.3-Gestión de derechos de acceso privilegiado
				A.9.2.4	A.9.2.4-Gestión de información de autenticación secreta de usuarios
				A.9.2.5	A.9.2.5-Revisión de los derechos de acceso de usuarios
				A.9.2.6	A.9.2.6-Retiro o ajuste de los derechos de acceso

		A.9.3	Responsabilidades de los usuarios	A.9.3.1	A.9.3.1-Uso de información de autenticación secreta
		A.9.4	Control de Acceso a Sistemas y Aplicaciones	A.9.4.1	A.9.4.1-Restricción de acceso a información
				A.9.4.2	A.9.4.2-Procedimiento de ingreso seguro
				A.9.4.3	A.9.4.3-Sistema de gestión de contraseñas
				A.9.4.4	A.9.4.4-Uso de programas utilitarios privilegiados
				A.9.4.5	A.9.4.5-Control de acceso a códigos fuente de programas
A.10	Criptografía	A.10.1	Controles Criptográficos	A.10.1.1	A.10.1.1-Política sobre el uso de controles criptográficos
				A.10.1.2	A.10.1.2-Gestión de Llaves
A.11	Seguridad Física y del Entorno	A.11.1	Áreas Seguras	A.11.1.1	A.11.1.1-Perímetro de seguridad física
				A.11.1.2	A.11.1.2-Controles de acceso físico
				A.11.1.3	A.11.1.3-Seguridad de oficinas, recintos e instalaciones
				A.11.1.4	A.11.1.4-Protección contra amenazas externas y ambientales
				A.11.1.5	A.11.1.5-Trabajo en áreas seguras
				A.11.1.6	A.11.1.6-Áreas de carga, despacho y acceso público
		A-11.2	Equipos	A.11.2.1	A.11.2.1-Ubicación y protección de los equipos
				A.11.2.2	A.11.2.2-Servicios públicos de soporte
				A.11.2.3	A.11.2.3-Seguridad del cableado
				A.11.2.4	A.11.2.4-Mantenimiento de los equipos
				A.11.2.5	A.11.2.5-Retiro de activos
				A.11.2.6	A.11.2.6-Seguridad de los equipos y activos fuera de las instalaciones
				A.11.2.7	A.11.2.7-Disposición segura o reutilización de equipos
				A.11.2.8	A.11.2.8-Equipos de usuario desatendido
				A.11.2.9	A.11.2.9-Política de escritorio limpio y pantalla limpia
A.12	Seguridad de las Operaciones	A.12.1	Procedimientos Operacionales y Responsabilidades	A.12.1.1	A.12.1.1-Documentación de los procedimientos de operación
				A.12.1.2	A.12.1.2-Gestión del cambios
				A.12.1.3	A.12.1.3-Gestión de la capacidad
				A.12.1.4	A.12.1.4-Separación de los ambientes de desarrollo, pruebas y operación
		A.12.2	Protección Contra Códigos Maliciosos	A.12.2.1	A.12.2.1-Controles contra códigos maliciosos.
		A.12.3	Copias de Respaldo	A.12.3.1	A.12.3.1-Copias de respaldo de la información
		A.12.4	Registro y Seguimiento	A.12.4.1	A.12.4.1-Registro de eventos

				A.12.4.2	A.12.4.2-Protección de la información de registro
				A.12.4.3	A.12.4.3-Registros del administrador y del operador
				A.12.4.4	A.12.4.4-Sincronización de relojes
		A12.5	Control de Software Operacional	A.12.5.1	A.12.5.1-Instalación de software en sistemas operativos
		A.12.6	Gestión de la Vulnerabilidad Técnica	A.12.6.1	A.12.6.1-Gestión de las vulnerabilidades técnicas
				A.12.6.2	A.12.6.2-Restricciones sobre la instalación de software.
		A.12.7	Consideraciones sobre Auditorias de Sistemas de Información	A.12.7.1	A.12.7.1-Controles de auditorías de sistemas de información.
A.13	Seguridad de las Comunicaciones	A.13.1	Gestión de la Seguridad de las Redes	A.13.1.1	A.13.1.1-Controles de redes
				A.13.1.2	A.13.1.2-Seguridad de los servicios de red.
				A.13.1.3	A.13.1.3-Separación en las redes
		A.13.2	Transferencia de Información	A.13.2.1	A.13.2.1-Políticas y procedimientos de transferencia de información
				A.13.2.2	A.13.2.2-Acuerdos sobre transferencia de información
				A.13.2.3	A.13.2.3-Mensajes electrónicos
				A.13.2.4	A.13.2.4-Acuerdos de confidencialidad o de no divulgación
A.14	Adquisición, Mantenimiento y Desarrollo de Sistemas	A.14.1	Requisitos de seguridad de los sistemas de información	A.14.1.1	A.14.1.1-Análisis y especificación de requisitos de seguridad de la información
				A.14.1.2	A.14.1.2-Seguridad de servicios de las aplicaciones en redes públicas
				A.14.1.3	A.14.1.3-Protección de transacciones de servicios de aplicaciones
		A.14.2	Seguridad en los procesos de desarrollo y soporte	A.14.2.1	A.14.2.1-Política de desarrollo seguro
				A.14.2.2	A.14.2.2-Procedimientos de control de cambios en sistemas
				A.14.2.3	A.14.2.3-Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones
				A.14.2.4	A.14.2.4-Restricciones en los cambios a los paquetes de software
				A.14.2.5	A.14.2.5-Principios de construcción de los sistemas seguros
				A.14.2.6	A.14.2.6-Ambiente de desarrollo seguro
				A.14.2.7	A.14.2.7-Desarrollo contratado externamente
				A.14.2.8	A.14.2.8-Pruebas de seguridad de sistemas

				A.14.2.9	A.14.2.9-Prueba de aceptación de sistemas
		A.14.3	Datos de prueba	A.14.3.1	A.14.3.1-Protección de datos de prueba
A.15	Relaciones con los Proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1	A.15.1.1-Política de seguridad de la información para las relaciones con proveedores
				A.15.1.2	A.15.1.2-Tratamiento de la seguridad dentro de los acuerdos con proveedores
				A.15.1.3	A.15.1.3-Cadena de suministro de tecnología de información y comunicación
		A.15.2	Gestión de la prestación de servicios de proveedores	A.15.2.1	A.15.2.1-Seguimiento y revisión de los servicios de los proveedores
				A.15.2.2	A.15.2.2-Gestión de cambios a los servicios de los proveedores
A.16	Gestión de Incidentes de Seguridad de la Información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	A.16.1.1-Responsabilidades y procedimientos
				A.16.1.2	A.16.1.2-Reporte de eventos de seguridad de la información
				A.16.1.3	A.16.1.3-Reporte de debilidades de seguridad de la información
				A.16.1.4	A.16.1.4-Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
				A.16.1.5	A.16.1.5-Respuesta a incidentes de seguridad de la información
				A.16.1.6	A.16.1.6-Aprendizaje obtenido de los incidentes de seguridad de la información
				A.16.1.7	A.16.1.7-Recolección de evidencia
A.17	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	A.17.1	Continuidad de Seguridad de la Información	A.17.1.1	A.17.1.1-Planificación de la continuidad de la seguridad de la información
				A.17.1.2	A.17.1.2-Implementación de la continuidad de la seguridad de la información
				A.17.1.3	A.17.1.3-Verificación, revisión y evaluación de la continuidad de la seguridad de la información
		A.17.2	Redundancias	A.17.2.1	A.17.2.1-Disponibilidad de instalaciones de procesamiento de información
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1	A.18.1.1-Identificación de la legislación aplicable y de los requisitos contractuales
				A.18.1.2	A.18.1.2-Derechos de propiedad intelectual
				A.18.1.3	A.18.1.3-Protección de registros
				A.18.1.4	A.18.1.4-Privacidad y protección de información de datos personales

				A.18.1.5	A.18.1.5-Reglamentación de controles criptográficos
		A.18.2	Revisiones de seguridad de la información	A.18.2.1	A.18.2.1-Revisión independiente de la seguridad de la información
				A.18.2.2	A.18.2.2-Cumplimiento con las políticas y normas de seguridad
				A.18.2.3	A.18.2.3-Revisión del cumplimiento técnico

Anexo. Solicitud para realizar tesis de grado.

Oficio N° UTN-AJLR-2024-002

Tulcán, 10 de diciembre de 2024

Doctor

Andrés Fabian Jácome Moreta

Gerente General de Cooperativa de Ahorro y Crédito Tulcán Ltda.

De mi consideración,

En mi condición de maestrante egresado de la Universidad Técnica del Norte, en la Maestría en Computación con Mención en Seguridad Informática, Cohorte III, y tras haber culminado en marzo la malla curricular de estudios, la universidad establece diversas opciones de titulación para completar el programa. En mi caso, y acorde con el desarrollo de las competencias declaradas y con la finalidad de apoyar con el fortalecimiento del área tecnológica de tan prestigiosa cooperativa, se ha tomado la decisión de desarrollar un informe de investigación o tesis con un enfoque específico en el área de seguridad de la información, este tema reviste una importancia crucial en el entorno actual, donde la protección de los datos y los sistemas tecnológicos se ha convertido en un pilar fundamental para garantizar la operatividad, la confianza y la continuidad de las organizaciones.

Por lo antes expuesto, me dirijo a usted de la manera más comedida y respetuosa para solicitar por su intermedio, al área o personal encargado de la información relacionada con el Sistema de Gestión de Seguridad de la Información, se me extienda la documentación relevante sobre el proceso mediante el cual fue implementado dicho sistema; solicitud que tiene como finalidad cumplir con los objetivos académicos planteados y desarrollar mi proyecto de titulación, siendo esta información clave y esencial para la continuidad y finalización esta maestría en curso.

Agradezco de antemano su colaboración y apoyo en este proceso académico, su contribución es vital para el desarrollo de una investigación robusta y significativa, que no solo ayudará a mi formación profesional, sino que también puede aportar valor a su organización mediante la identificación y mitigación de riesgos en sus activos de información.

La información proporcionada será utilizada exclusivamente con fines académicos y de investigación, garantizando su confidencialidad y uso ético conforme a las normas de seguridad y protección de datos vigentes.

Quedo a la espera de su pronta respuesta, y a su disposición para cualquier consulta adicional o coordinación necesaria.

Atentamente,

Ing. Andrés Javier López Ruano
Cédula de Identidad: 0401158985
Teléfono: 0980 519290
E-mail: ajlr_78@hotmail.com

COOPERATIVA DE AHORRO Y CRÉDITO TULCÁN LTDA
11- Dic-2024 11h45
PROSECRETARÍA

DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/ IEC 13335]: "característica/ propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Controles de seguridad: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También utilizado como sinónimo de salvaguarda o contramedida.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/ IEC 13335]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Impacto: El coste para la empresa de un incidente que puede o no ser medido en términos estrictamente financieros ejemplo, pérdida de reputación, implicaciones legales, etc.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [I SO/ I EC 13335]: propiedad/ característica de salvaguardar la exactitud y completitud de los activos.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite

probar la participación de las partes en una comunicación.

PDCA: Modelo de proceso basado en un ciclo continuo de las actividades de planificar

(establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/I EC 27002]: intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Según [ISOGuía73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Según [ISO/ IEC Guía 73: 2002] El riesgo que permanece tras el tratamiento del riesgo.

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [I SO/ IEC 27001]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

Sistema de Gestión de la Seguridad de la Información (SGSI): Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.