REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE

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

AUTOR: PILLAJO MONTALVO ESTEBAN PATRICIO

DIRECTOR: MSC. XAVIER MAURICIO REA PEÑAFIEL

IBARRA – ECUADOR

2025

CERTIFICACION DEL DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

Ibarra, 26 de febrero de 2025

Msc Mauricio Rea Peñafiel

DIRECTOR DEL TRABAJO DE INTEGRACION CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integraccion Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f).....

MSC. MAURICIO REA PEÑAFIEL

Cc; 1002485744

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:	100389659-2		
APELLIDOS Y NOMBRES:	PILLAJO MONTALVO ESTEBAN PATRICIO		
DIRECCIÓN:	IBARRA, MEJÍA 1-70 Y MALDONADO		
EMAIL:	epatriciopm@hotmail.com		
TELÉFONO FIJO:	N/A	**TELÉFONO MÓVIL:**	0982236973

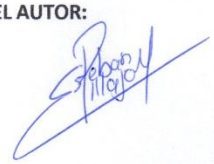
DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRRA NORTE
AUTOR (ES):	ESTEBAN PATRICIO PILLAJO MONTALVO
FECHA: DD/MM/AAAA	26/02/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[ ] **PREGRADO** [X] **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	Msc. Mauricio Rea Peñafiel

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 febrero de 2025

EL AUTOR:



.....
Nombre: Esteban Patricio Pillajo Montalvo

DEDICATORIA

Quiero dedicar este trabajo a mis padres que son un pilar fundamental durante toda la carrera estudiantil, de igual manera a los consejos y valores que me enseñaron a lo largo de este año de aprendizaje, mostrando su preocupación por seguir adelante en el camino de la vida. Siendo quienes me inspiraron a seguir adelante y nunca rendirme en el proceso de estudio, también una dedicatoria a mi hermano que me estuvo apoyando en todo momento y mencionando la importancia de adquirir nuevos conocimientos quién nunca se rindió de motivarme a culminar los estudios.

Dedicar esto a las personas quienes han estado durante el estudio universitario y maestría apoyándome, quienes me han brindado su apoyo emocional durante mi vida, en la formación académica y profesional, quienes me aconsejaron que jamás me diera por vencido, también a quienes me aconsejaron en todo momento para culminar este proyecto que empecé y que conocen que soy una persona con gran potencial.

AGRADECIMIENTOS

Agradezco a mis padres quienes han sido un pilar fundamental a nivel profesional, por siempre ayudarme a ver la vida profesional como un reto cada día para cumplir mis metas, por todo el apoyo económico y material que han brindado para iniciar sin preocupaciones el estudio de la maestría.

Además, agradezco a los profesores quienes me han inculcado sus conocimientos dentro de la carrera, las nuevas oportunidades, habilidades que se fue desarrollando en el año de estudio, que me han demostrado que puedo llegar a ser un gran profesional centrado y enfocado en cumplir mis metas personales.

ÍNDICE DE CONTENIDO

RESUMEN 12
ABSTRACT 13
CAPITULO I 14
1. EL PROBLEMA 14
1.1. Problema de investigación 14
1.2. Interrogantes de la investigación 18
1.3. Objetivos de la investigación 18
1.4. Hipótesis de trabajo 19
1.5. Hipótesis alternativa 20
1.6. Categorización de variables 20
1.7. Justificación 22
CAPITULO II 24
2. MARCO REFERENCIAL 24
2.1. Antecedentes 24
2.2. Marco teórico 26
2.2.1. Metodología de análisis y gestión de riesgos 26
2.2.1.1. NIST SP 800-30 26
2.2.1.2. CRAMM 27
2.2.1.3. MAGERIT 28
2.2.2. Activos de la información 35
2.2.3. Amenazas y vulnerabilidades 37
2.2.4. Evaluación de riesgo 41
2.2.5. Controles de la norma ISO/IEC 27001:2022 42
2.2.6. Política de seguridad de la información 43
CAPITULO III 46
3. MARCO METODOLÓGICO 46
3.1. Descripción del área de estudio / Descripción del grupo de estudio 46
3.2. Enfoque y tipo de investigación 46
3.3. Procedimiento de investigación 48
3.4. Consideraciones bioéticas 51

CAPITULO IV 53
4. MARCO ADMINISTRATIVO 53
4.1. Identificación de servicios y sistemas 53
4.2. Identificación de criterios de valoración 59
4.3. Niveles de riesgo para los activos 61
4.4. Estimación de amenazas y vulnerabilidades 62
4.5. Identificación de activos de la información 63
4.6. Valoración de los activos 66
4.7. Evaluación de riesgos 67
4.8. Declaración de aplicabilidad 71
4.9. Tratamiento de Riegos, después de la evaluación de riesgos 76
4.10. Diseño de Política de Seguridad de la Información 81
CAPITULO V 83
5. PROPUESTA 83
5.1. Evaluación de Política de Seguridad de la Información 83
5.2. Informe de resultados de la evaluación 85
5.3. Diseño de la política de seguridad de la información 87
CAPITULO VI 88
6. CONCLUSIONES Y RECOMENDACIONES 88
REFERENCIAS 91
ANEXOS 93

Índice de Tablas

Tabla 1. Objetivos de la metodología MAGERIT 29
Tabla 2. Propiedades principales y derivadas de la Seguridad de la Información 29
Tabla 3. Análisis de sistema 31
Tabla 4. Objetivos del Libro II "Catálogo de elementos" 34
Tabla 5. Ítems de catálogo de objetos 34
Tabla 6. Tipos de activos 35
Tabla 7. Catálogo de amenazas 37
Tabla 8. Análisis mediante tablas 41
Tabla 9. Grupos en los que se clasifican los controles 43
Tabla 10. Puertos y servicios de la dirección IP escaneada 54
Tabla 11. Puertos y servicios de la dirección IP de laptop de Oficial de Seguridad de la Información 55
Tabla 12. Puertos y servicios del DVR 56
Tabla 13. Puertos y servicios del DVR (segundo piso) 57
Tabla 14. Lista de puertos y servicios del Servidor de pruebas 58
Tabla 15. Lista de puertos y servicios del responsable de área de tecnología 58
Tabla 16. Puertos y servicios del switch 59
Tabla 17. Criterio de valoración de activo en la confidencialidad 59
Tabla 18. Criterio de valoración de activo en la integridad 60
Tabla 19. Criterio de valoración de activo en la disponibilidad 60
Tabla 20. *Tabla de referencia para evaluación de activo* 61
Tabla 21. Nivel de riesgo 61
Tabla 22. Estimación de amenazas 62
Tabla 23. Estimación de vulnerabilidades 63
Tabla 24. Inventario de activos del Área de TI 63
Tabla 25. Valoración de activos 66
Tabla 26. Evaluación de riesgos 68
Tabla 27. Declaración de aplicabilidad de Seguridad de la Información Norma ISO 27001:2022 72
Tabla 28. Tratamiento de riesgos de los activos de la información 77

Tabla 29. Grupo de evaluadores que participaron en la validación del modelo 83
Tabla 30. Escala para el análisis del chequeo de la política de seguridad de la información 84
Tabla 31. Resultados de juicio de expertos 85
Tabla 32. Lista de chequeo de evaluación de expertos 109

Índice de Figuras

Figura 1. Participación de las entidades por segmento en el estudio de seguridad y Ciberseguridad 15
Figura 2. Metodologías y procedimientos relacionados a Seguridad de la Información y Ciberseguridad 16
Figura 3. Variable dependiente 21
Figura 4. Variable Independiente 21
Figura 5. ISO 31000 - Marco de trabajo para la gestión de riesgos 28
Figura 6. Ciclo PDCA 33
Figura 7. Metodología de evaluación de riesgo 47
Figura 8. Escaneo de red de la central telefónica 54
Figura 9. Escaneo de red de laptop de Oficial de Seguridad de la Información 55
Figura 10. Escaneo de red de DVR (cámara de video primer piso) 55
Figura 11. Escaneo de red de DVR (cámaras de video segundo piso) 56
Figura 12. Escaneo de red, dirección IP de Servidor de pruebas 57
Figura 13. Escaneo de red de laptop de responsable del área de tecnología 58
Figura 14. Escaneo de red de switch 58

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE

Autor: Pillajo Montalvo Esteban Patricio

Tutor: Msc. Xavier Mauricio Rea Peñafiel

Año: 2024

RESUMEN

La Cooperativa de Ahorro y Crédito Rural Sierra Norte enfrenta nuevos desafíos en la implementación de la seguridad de la información principalmente porque debe proteger los datos personales de sus clientes. Entre las principales amenazas detectadas son: el ingreso a sitios web que pueden tener malware, desactualización de parches de seguridad en los equipos informáticos, inseguridad física, uso inadecuado del equipo informático, correos maliciosos, entre otros riesgos a la seguridad de la información. Es trabajo propone la implementación de políticas de seguridad dentro del área de TI de la cooperativa para disminuir las vulnerabilidades existentes en sus aplicaciones con base en la norma ISO/IEC 27001:2022. Se adoptó un enfoque de investigación cualitativa, mediante el juicio de expertos que evaluaron las políticas definidas en distintas fases establecidos por la metodología MAGERIT. Los resultados obtenidos a través de una lista de chequeo realizada por 3 expertos en seguridad de la información, muestran que están dentro del rango: Totalmente de acuerdo (TDA) con un valor de 4,55 sobre 5,00 puntos. Se concluye que la propuesta cumple con las normas y regulaciones que necesitaba la cooperativa para identificar los riegos y vulnerabilidades de los activos de la información.

Palabras clave: Política de seguridad de la información, activos de la información, vulnerabilidades, riesgo.

ABSTRACT

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTATION OF INFORMATION SECURITY POLICIES IN THE IT AREA BASED ON THE ISO/IEC 27001:2022 STANDARD. CASE STUDY: SAVINGS AND CREDIT COOPERATIVE SIERRA NORTE RURAL

Author: Pillajo Montalvo Esteban Patricio

Tutor: Msc. Xavier Mauricio Rea Peñafiel

Year: 2024

The Sierra Norte Rural Savings and Credit Cooperative faces new challenges in the implementation of information security mainly because it must protect the personal data of its clients. Among the main threats detected are: access to websites that may have malware, outdated security patches on computer equipment, physical insecurity, inappropriate use of computer equipment, malicious emails, among other risks to information security. This work proposes the implementation of security policies within the cooperative's IT area to reduce existing vulnerabilities in its applications based on the ISO/IEC 27001:2022 standard. A qualitative research approach was adopted, through the judgment of experts who evaluated the policies defined in different phases established by the MAGERIT methodology. The results obtained through a checklist carried out by 3 information security experts show that they are within the range: Totally agree (TDA) with a value of 4.55 out of 5.00 points. It is concluded that the proposal complies with the rules and regulations that the cooperative needed to identify the risks and vulnerabilities of the information assets.

Keywords: Information security policy, information assets, vulnerabilities, risk.

CAPITULO I

1. EL PROBLEMA

1.1. Problema de investigación

Ante la evolución tecnológica y las nuevas amenazas que se presentan en los ataques a la red de empresas, instituciones privadas y públicas que tienen información sensible de las personas, se ha venido proponiendo el uso de los Sistemas de Gestión de Seguridad de la Información (SGSI)

La Norma ISO/IEC 27001:2022 tiene como objetivo establecer los requisitos para la implementación, mantenimiento y mejora continua de un SGSI. Según De La Cruz Rodríguez, G., Méndez Fernández, A., & Méndez Fernández, R. (2023, pág. 233)., mencionan que la norma implementada de forma correcta es fundamental y es una de las más aplicadas en el momento de llevar a cabo el proceso de seguridad de la información.

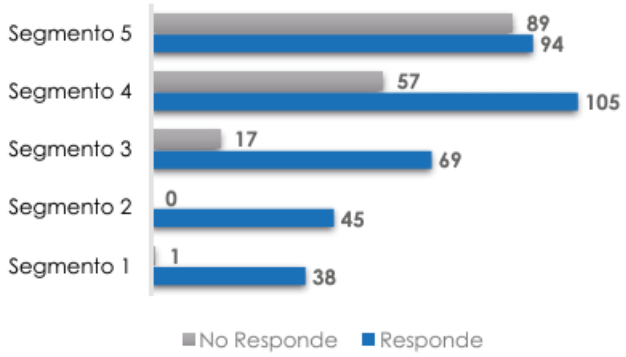
Así mismo, para implementar un SGSI, se han utilizado las normas ISO/IEC 27000, dentro de las cuales se destaca el estándar 27001. Según Calder, A., & Watkins, S. (2008)., la certificación ISO 27001 en una institución indica a los clientes actuales y potenciales que la organización ha desarrollado o está en proceso de desarrollar procesos de seguridad de la información, lo cual contribuye a fortalecer la confianza en la entidad.

Según los planteamientos de Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021)., la adopción de un estándar internacional permite a las organizaciones tener una base

uniforme y confiable. Su implementación está diseñada para ser aplicable a organizaciones de cualquier tipo, naturaleza o tamaño; este enfoque busca establecer la consistencia y la confiabilidad en diversas áreas, independiente de cada entidad.

Hay que mencionar, además que, en Ecuador la Superintendencia de Economía Popular y Solidaria (SEPS), en una encuesta realizada en agosto de 2021 “Encuesta estado y realidad de los servicios digitales y seguridad de la información en el SFPS 2021” donde muestra resultados que las cooperativas tienen iniciativas internas para la seguridad de la información y ciberseguridad, ver Figura 1, considerando un total de 516 que representan el 68% de entidades distribuidas por segmento (2021, pág. 40) .

Figura 1. *Participación de las entidades por segmento en el estudio de seguridad y Ciberseguridad*



Fuente: Superintendencia de Economía Popular y Solidaria (2021, pág. 41)

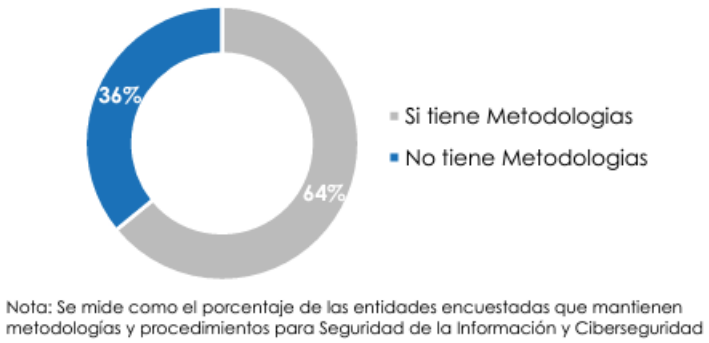
Obtenida de: https://www.seps.gob.ec/wp-content/uploads/Formato-DNIC-Estudio-de-servicios-financieros-digitales-y-seguridad-informacion-1.pdf

En la Figura 1, se presentan los resultados sobre una encuesta realizada por las cooperativas, mismas que dieron respuesta al envío masivo de correos electrónicos, denominado “mailing institucional”.

En el mismo informe de la SEPS, se muestran las respuestas sobre si tienen implementado una metodología y procedimientos para controlar los problemas que pueden ser relacionados con la seguridad de la información y ciberseguridad, como se indica en la Figura 2.

Figura 2. *Metodologías y procedimientos relacionados a Seguridad de la Información y Ciberseguridad*

(Superintendencia de Economía Popular y Solidaria, 2021)



Fuente: Superintendencia de Economía Popular y Solidaria (2021, pág. 44)

Obtenida de: https://www.seps.gob.ec/wp-content/uploads/Formato-DNIC-Estudio-de-servicios-financieros-digitales-y-seguridad-informacion-1.pdf

En la figura anterior, se puede indicar que el apoyo e interacción de alta dirección de las entidades es fundamental para un exitoso programa de Seguridad de la Información y Ciberseguridad (pág. 44).

Por otro lado, en la Cooperativa de Ahorro y Crédito (COAC) Rural Sierra Norte, no se tiene un SGSI. De acuerdo con lo mencionado por la SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) en su “RESOLUCIÓN No. SEPS-IGS-

IGT-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002", en el Artículo 10 indica que "Las entidades, empresas y la CONAFIPS que conforma este régimen, deberán implementar y mantener 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 legal vigente" (2022, pág. 7).

La seguridad de la información en la COAC Rural Sierra Norte es un aspecto fundamental para mejorar la gestión del entorno tecnológico y la información crucial para la toma de decisiones que se maneja en la institución.

La cooperativa está en constante crecimiento, sin embargo, en el área de Tecnologías de Información (TI) se ha identificado la falta de protección y restricción en la navegación web a diferentes sitios. El área de TI tiene un servidor físico, dos portátiles, red interna inalámbrica, que están interconectados y con suministro de internet a las seis (6) departamentos administrativos y al sistema de circuito de cámaras (CCTV). Entre las principales amenazas detectadas son el ingreso a sitios web que pueden tener malware y pueden colocar la cuenta de usuario en los mismos, desactualización de parches de seguridad en los equipos informáticos, inseguridad física, uso inadecuado del equipo informático, correos maliciosos, entre otros.

De acuerdo a un reporte emitido por el Área de TI durante el año 2023, se ha verificado que la cooperativa ha sufrido estos ataques a su información como transacciones no autorizadas por mal uso de contraseñas de sus empleados, además los aplicativos que se encuentran en un sitio web, tienen diferentes vulnerabilidades como el no tener configurados

los dominios y el acceso se lo hace por direcciones IP, la falta de un control de acceso robusto por contraseñas deficientes lo que aumenta el riesgo de ataques externos.

1.2. Interrogantes de la investigación

¿Qué tipo de metodología se emplear para identificar los activos de la información de la Cooperativa?

¿Cuáles son las amenazas a las que puede estar expuesta la información que se encuentra en los activos?

¿Qué ventajas tiene emplear una política de seguridad de la información y planificar una evaluación de los riesgos sobre los activos?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Implementar políticas de seguridad en el área de TI de la Cooperativa de Ahorro y Crédito Rural Sierra Norte para disminuir las vulnerabilidades existentes en sus aplicaciones con base en la norma ISO/IEC 27001:2022.

1.3.2 Objetivos específicos

Crear un inventario de activos de información de acuerdo con su función y nivel, para facilitar el reconocimiento de las vulnerabilidades y riesgos que están dentro del área de Tecnología de Información de la Cooperativa de Ahorro y Crédito Rural Sierra Norte.

Evaluar los riesgos de los activos de la información en base a la norma ISO/IEC 27001:2022 y la metodología Magerit.

Diseñar una Política de Seguridad de la Información en el área de TI de la Cooperativa que garantice la confidencialidad, integridad y disponibilidad de la información.

Evaluar la efectividad de las políticas de seguridad mediante la matriz de tratamiento de riesgos y de control aplicadas en el caso de estudio.

1.4. Hipótesis de trabajo

La implementación de políticas de seguridad en el área de TI de la Cooperativa de Ahorro y Crédito Rural Sierra Norte permitirá disminuir las vulnerabilidades existentes en sus aplicaciones con base en la norma ISO/IEC 27001:2022.

1.5. Hipótesis alternativa

La implementación de políticas de seguridad en el área de TI de la Cooperativa de Ahorro y Crédito Rural Sierra Norte no permitirá disminuir las vulnerabilidades existentes en sus aplicaciones con base en la norma ISO/IEC 27001:2022.

1.6. Categorización de variables

Variable independiente: Implementación de política de seguridad en el área de TI de la información con base en la norma ISO/IEC 27001:2022 para la COAC Rural Sierra Norte.

Variable dependiente: Vulnerabilidades existentes en sus aplicaciones.

Figura 3. *Variable dependiente*

Fuente: Elaboración propia

Figura 4. *Variable Independiente*

Fuente: Elaboración propia

1.7. Justificación

La Norma ISO/IEC 27001:2022 tiene como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de la información, en sus objetivos la norma tiene presente la implementación, mejora y algunos controles asociados para corregir la gestión de la seguridad de la información.

Hay que mencionar, además que, la norma hace hincapié en la Política de Seguridad que nos permitirá ser un marco referencial para los objetivos que se van a declarar, desarrollando un marco de actuación apropiado para salvaguardar la información de la institución, además ayudará a la mejor adaptación de la institución, mejorará la comunicación dentro de la institución y las partes interesadas en conocer de forma continua como va corrigiendo los que se desea conseguir con la seguridad de la información.

La SEPS (2022) ha planteado ir realizando un SGSI dentro de las instituciones financieras, por lo tanto, el presente estudio permitirá contribuir con este objetivo. No solo se abordará vulnerabilidades y amenazas de la seguridad de la información, también sentará bases para fortalecer la eficiencia en el ámbito de tratamiento de riesgos. Además de mantener la confidencialidad, integridad y disponibilidad de toda la información que se maneja dentro de la cooperativa, además de mejorar el funcionamiento y capacitar a los trabajadores que pueden tener al manejar la información.

Para la evaluación de riesgo, la cooperativa considerará algunos activos en el área de TI que ayudarán a mejorar cada momento ante algunas amenazas, vulnerabilidades que

puedan repetirse en un activo de la información, y también considerará que se realizará un tratamiento del riesgo que ayuda a optimizar el riesgo y se tendrá la información presente ante problemas que se puedan dar a futuro.

La mejora en la gestión de seguridad de la información en la COAC Rural Sierra Norte, contribuirá a crear un mejor entorno en el área de TI, más seguro, confiable para los clientes existentes y potenciales.

El Plan Nacional de Desarrollo 2017–2021 de Ecuador, elaborado por la Secretaría Nacional de Planificación y Desarrollo (SENPLADES) y vigente durante ese período, estableció diversos objetivos. El Objetivo 9 se centra en "Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo".

Este objetivo busca fortalecer la presencia y posición de Ecuador tanto a nivel regional como internacional, en la Política 9.3 se hace mención en "Crear y fortalecer los vínculos políticos, sociales, económicos, turísticos, ambientales, académicos y culturales, y las líneas de cooperación para la investigación, innovación y transferencia tecnológica con socios estratégicos de Ecuador."

CAPITULO II

2. MARCO REFERENCIAL

2.1. Antecedentes

La investigación tecnológica y la constante evolución de las redes y la tecnología han dado lugar a la existencia de muchas vulnerabilidades que, en ocasiones, no se ha dado importancia como se lo merece frente a las amenazas potenciales que están asociadas a ciberataques.

En el ámbito tecnológico empresarial, institucional y organizacional, la actualización tanto del hardware como del software en los servidores debe ser una práctica común. Sin embargo, la difusión de los nuevos ciberataques en redes y la falta de revisión de parches en los servidores, pueden exponer a estas entidades.

De la misma forma, la información gestionada por las empresas es de sensibilidad completa. En este contexto, según lo señalado por Vega Briceño, E. (2021), la seguridad de la información desempeña un papel crucial en los aspectos de nuestra sociedad hiperconectada; esto atribuye a la adopción generalizada de la tecnología de información y comunicación. Las observaciones de Vega Briceño ilustran el papel fundamental de la seguridad de la información en la sociedad actual.

Calder, A., & Watkins, S. (2019), destacan que los activos de la información gestionados y controlados en las empresas son claves para la competitividad y supervivencia

a largo plazo tanto de las corporaciones como de las economías enteras. Esto implica que la responsabilidad de salvaguardar los activos de la información integrados en los activos físicos de una empresa, son la responsabilidad del gobierno corporativo.

En un estudio realizado en Bolivia por Vega Velasco, W. (2008), se indica que no solo se requiere comprender y conocer las amenazas a las que está expuesta la información y los recursos de una organización, sino también identificar su origen, ya sean internas o externas a la organización. Para comprender mejor la necesidad de tomar conciencia no solo de las amenazas y las vulnerabilidades existentes. Además de ajustarse al modelo de trabajo actual, mientras se busca constantemente mejorar y adaptarse con el tiempo.

Actualmente en Ecuador, varias empresas han adoptado estrategias para mejorar la atención al cliente y captar su interés, implementando un sistema de gestión que garantice la protección de la información personal, se ha propuesto la implementación de un SGSI como medida para mantener la integridad y confidencialidad de los datos de los clientes.

En la provincia de Cañar, un estudio enfocado en cooperativas de ahorro y crédito de segmento 3. En el análisis del cumplimiento de las políticas de seguridad de la información realizado por Guamán, A., Cárdenas Muñoz., J, V. (2022), se observó que algunas de las cooperativas evaluadas no implementan en su totalidad dichas políticas. Esto señala una falta de cumplimiento con todos los requerimientos y controles que se pueden emplear dentro de su organización, sugiriendo la posibilidad de que la información puede ser vulnerable a manipulaciones por parte de terceros.

Para minimizar el riesgo, algunas cooperativas han adoptado la Metodología MAGERIT, en este caso nos proporciona una forma de identificar las amenazas de los mayores desafíos en la protección de datos o información. Según Miranda Jiménez, J, N., (2021), la evaluación de riesgos resulta un impacto sobre los activos, facilitando el proceso mediante una matriz. En este escenario, se recurre al Esquema Gubernamental de Seguridad de la Información V2 (EGSI V2), que permite visualizar y comprender la definición de una matriz de evaluación de riesgo, considerando los activos ya identificados dentro de la institución.

2.2.Marco teórico

2.2.1. Metodología de análisis y gestión de riesgos

2.2.1.1.NIST SP 800-30

La *National Institute of Standards and Technology* (NIST, por sus siglas en inglés) es una agencia del gobierno de Estados Unidos que está encargada de desarrollar y promover estándares, medidas y tecnologías con la finalidad de mejorar la seguridad y la competitividad. Según Nebreda, P., (2023) la NIST trabaja en las áreas como tecnología de la información, ciberseguridad, metrología, ingeniería, manufactura y ciencias materiales.

El propósito directo de la NIST con la publicación especial (SP, por Special Publication) 800-30, es brindar orientación para realizar evaluaciones de riesgos en instituciones u organizaciones de los sistemas de información. De igual manera, está orientada a la identificación de factores de riesgo específicos para monitorear de manera

continua, de modo que pueden controlar de manera continua si los riesgos han aumentado a niveles superiores.

2.2.1.2.CRAMM

CRAMM (CCTA Risk Analysis and Management Method, Por sus siglas), es un método de análisis y control de riesgos que permite identificar, medir y reducir al mínimo los ataques a las que puede estar expuesta las organizaciones cada día.

Según Tejena Macías, M., (2018) resalta que CRAMM realiza un análisis cuantitativo y cualitativo por lo que se considera como una metodología mixta y se apoya de una herramienta de gestión, lo que permitirá a la institución u organización tener una visión más clara y priorizada de las amenazas que se puedan tener, los mismos que pueden ir afectando a los recursos y continuidad del negocio.

Para la implementación de CRAMM, hay que tomar en cuenta un adecuado análisis de riesgo que son:

- Amenazas
- Vulnerabilidades
- Riesgos
- Contramedidas,
- Implementación
- Auditoría

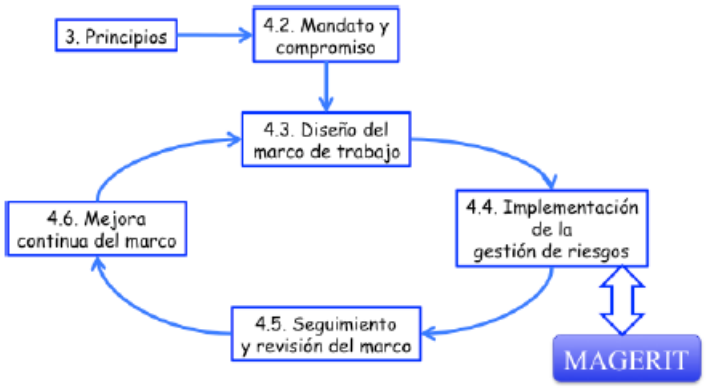
Lo cual permite tener un mejor resultado y asegura la continuidad del negocio.

2.2.1.3.MAGERIT

MAGERIT (por sus siglas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) la metodología es de carácter público que se puede utilizar de forma libremente ya que no requiere autorización previa es muy compatible con la norma ISO/IEC 27001:2022.

La metodología siguiendo la normativa ISO 31000, MAGERIT responde a la sección 4.4 “Implementación de la Gestión de los Riesgos” donde se hace mención a la implementación al Proceso de Gestión de Riesgos dentro de un marco de trabajo como se muestra en la Figura 5.

Figura 5. *ISO 31000 - Marco de trabajo para la gestión de riesgos*



Fuente: Ministerio de Hacienda y Administraciones Públicas (2012, pág. 7)

Además, para el Ministerio de Hacienda y Administraciones Públicas (2012), MAGERIT tiene 4 objetivos identificables como se muestra en la Tabla 1:

Tabla 1. *Objetivos de la metodología MAGERIT*

Objetivos Directos	Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
	Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
	Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
Objetivos Indirectos	Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Fuente: Elaboración propia

Obtenida de: Ministerio de Hacienda y Administraciones Públicas, Libro I, (2012, pág. 8)

La seguridad que se considera dentro de MAGERIT la define como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad, ver Tabla 2.

Tabla 2. *Propiedades principales y derivadas de la Seguridad de la Información*

Propiedades		**Descripción**	**Incumplimiento**
Principales	**Disponibilidad**	o disposición de los servicios a ser usados cuando sea necesario.	La falta de disponibilidad puede ocasionar la suspensión o interrupción del

			servicio, misma que influye de forma directa a la productividad.
	Integridad	o mantenimiento de las características de completitud y corrección de los datos.	La información puede verse manipulada, corrupta o incompleta, esto afecta directamente al verdadero desempeño de las funciones en la organización
	Confidencialidad	o que la información llegue solamente a las personas autorizadas.	Pueden darse fugas o filtraciones de la información, así como accesos no autorizados. Incumpliendo las leyes, compromisos contractuales relativos a la custodia de los datos.
Derivadas	**Autenticidad**	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.	Manipulación del contenido original de los datos. El acceso de los usuarios a los servicios, en este caso, la suplantación de identidad.

	Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.	Relacionada con los registros todas las actividades ejecutadas, en el caso de incidentes es esencial para encontrar los responsables

Fuente: Elaboración propia

Obtenido de: Ministerio de Hacienda y Administraciones Públicas, Libro I, (2012, pág. 9)

Estas propiedades pueden ser utilizadas en algún momento, en el caso de ocurrir un evento, se deben asignar recursos para obtenerlas. En esta actividad es donde se destinan las metodologías de análisis y gestión de riesgos.

También en el libro I de MAGERIT, se define el **riesgo** como un grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la institución u organización, es así que se muestra en la Tabla 3, un análisis de sistema para saber en qué medida los activos pueden estar en peligro. (Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 9)

Tabla 3. *Análisis de sistema*

Análisis de sistema	
Análisis de riesgo	Es un proceso sistemático, con la finalidad de estimar la magnitud de los riesgos a los que pueden estar expuesta una institución u organización.

Tratamiento de los riesgos	Para el tratamiento hay múltiples formas: • Evitar las circunstancias que pueden provocarlo. • Reducir las posibilidades de que ocurra. • Acotar las consecuencias. • Compartirlo con otra institución u organización. • Aceptar que pudieran ocurrir, previniendo recursos para su actuación en caso de que sea necesario.

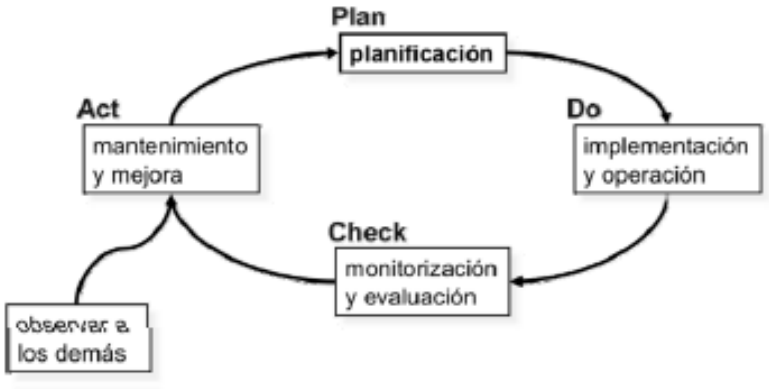
Fuente: Elaboración propia

Obtenida de: Ministerio de Hacienda y Administraciones Públicas, Libro I, (2012, págs. 9-10)

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, la fase de tratamiento de riesgo estructura acciones que se pueden explicar en materia de seguridad para satisfacer las insuficiencias que han sido detectadas en la fase previa del análisis.

Es por eso que los sistemas de gestión de la seguridad de la información (SGSI), en especial la norma ISO/IEC 27001:2022, formalizan cuatro etapas como se muestra en la Figura 6.

Figura 6. *Ciclo PDCA*



Fuente: Ministerio de Hacienda y Administraciones Públicas, Libro I, (2012, pág. 11)

El ciclo mencionado en la Figura 6., la fase de "**Plan: planificación"**, es donde hace parte el análisis de riesgo, también se toman las decisiones de tratamiento, mismas que se materializan en la etapa de **"Do: implementación y operación",** en la etapa **"Check: monitorización y evaluación"** que se despliegan elementos que permitan monitorizar las medidas escogidas para poder evaluar la efectividad y la fase de **"Act: mantenimiento y mejora",** hace mención a la actuación en consecuencia que se hace, conjuntamente con las mejoras continuas. (Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 11)

En el Libro II que publicó el Ministerio de Hacienda y Administraciones Públicas (2012), de nombre "Catálogo de elementos" tiene como objetivos, ver Tabla 4:

Tabla 4. *Objetivos del Libro II "Catálogo de elementos"*

Objetivos de Libro II	
1	Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2	Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Fuente: Elaboración propia

Obtenida de: Ministerio de Hacienda y Administraciones Públicas, Libro II, (2012, pág. 6)

Como lo confirma el Ministerio de Hacienda y Administraciones Públicas en los objetivos mencionados anteriormente en la Tabla 4., y reconociendo la rápida evolución tecnológica se describe a continuación un catálogo de los objetos donde marca algunas reglas como se muestra en la Tabla 5.

Tabla 5*. Ítems de catálogo de objetos*

Ítems de Catálogo de Objetos	
Tipos de activos	Pueden aparecer nuevos tipos de activos continuamente.
Dimensiones de valoración	En algunos casos puede surgir dimensiones específicas, pero en la certidumbre debe estar recogido lo esencial.
Criterios de Valoración	Tener en cuenta la estimación que puede existir por parte de los expertos, marcando una primera pauta de homogeneidad. La principal idea que se puede tener es la valorización de las dimensiones, pero, ideando relaciones entre dichas dimensiones.

Amenazas	Hay que reconocer que algunas amenazas son significantes sobre los sistemas.
Salvaguardas	Se tratan como una identificación de necesidades por los responsables de los sistemas de información, debido a cierto nivel de complejidad de los diferentes productos y tecnologías, que los auditores de sistemas tratan como controles de eficacia y eficiencia.

Fuente: Elaboración propia

Obtenido de: Ministerio de Hacienda y Administraciones Públicas (2012, pág. 6)

2.2.2. Activos de la información

Los tipos del activo es una información que debe estar documentada por el interés de valorar el criterio de amenazas potenciales y salvaguardas apropiadas al activo.

Magerit clasifica los activos dentro de una jerarquía, que se determina cada uno un código que para el Ministerio de Hacienda y Administraciones Públicas refleja una posición jerárquica, donde se menciona un nombre y una pequeña pero breve descripción de las características que recoge, ver Tabla 6.

Tabla 6. *Tipos de activos*

Tipos de activos		
Nombre	**Código**	**Descripción**
Activos esenciales	essential	Marcan requisitos de seguridad para todos los demás componentes del sistema.

Arquitectura del sistema	arch	Son elementos que permiten estructurar el sistema, la arquitectura interna y sus relaciones con el exterior.
Datos / Información	D	Son el corazón de la organización para prestar sus servicios.
Claves criptográficas	K	Se emplea para proteger el secreto e identificar a las partes. Son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.
Servicios	S	Función que satisface una necesidad.
Software – Aplicaciones informáticas	SW	Denominado programas, aplicativos, desarrollos, etc., se refiere a las treas que han sido automatizadas para su desempeño por un equipo informático.
Equipamiento informático (Hardware)	HW	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Rede de comunicaciones	COM	Instalaciones delicadas como servicios de comunicaciones contratados a terceros, centrándose en que son medios de transporte que llevan daros de un sitio a otro.
Soportes de información	Media	Dispositivos físicos que permiten almacenar información permanente.
Equipamiento auxiliar	AUX	Equipos que sirven de soporte a los sistemas informáticos.
Instalaciones	L	Lugares donde se hospedan los sistemas de información y comunicación.
Personal	P	Las personas relacionadas con los sistemas de información.

Fuente: Elaboración propia

Obtenido de: Ministerio de Hacienda y Administraciones Públicas, Libro II, (2012, págs. 7-13)

2.2.3. Amenazas y vulnerabilidades

La amenaza según el Ministerio de Hacienda y Administraciones Públicas, Libro I, (2012, pág. 27), lo define como una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

A continuación, se presenta un catálogo de amenazas, como se muestra en la Tabla 7, posibles que se pueden dar sobre los activos de un sistema de información:

Tabla 7. *Catálogo de amenazas*

Catálogo de amenazas		
Categoría	**Código**	**Tipo de amenaza**
Desastres naturales	N	Fuego
		Daños por agua
		Desastres naturales
De origen industrial	I	Fuego
		Daños por agua
		Desastres industriales
		Contaminación mecánica
		Contaminación electromagnética
		Avería de origen físico o lógico
		Corte del suministro eléctrico
		Condiciones inadecuadas de temperatura o humedad
		Fallo de servicios de comunicaciones
		Interrupción de otros servicios y suministros esenciales

		Degradación de los soportes de almacenamiento de la información
		Emanaciones electromagnéticas
Errores y fallos no intencionados	E	Errores de los usuarios
		Errores del administrador
		Errores de monitorización
		Errores de configuración
		Deficiencias en la organización
		Difusión de software dañino
		Errores de [re-]encaminamiento
		Errores de secuencia
		Escapes de información
		Alteración accidental de la información
		Destrucción de información
		Fugas de información
		Vulnerabilidades de los programas (software)
		Errores de mantenimiento / actualización de programas (software)
		Errores de mantenimiento / actualización de equipo (hardware)
		Caída del sistema por agotamiento de recursos
		Pérdida de equipos
		Indisponibilidad del personal
Ataques intencionados	A	Ataques intencionados
		Manipulación de los registros de actividad (log)
		Manipulación de la configuración
		Suplantación de la identidad del usuario
		Abuso de privilegios de acceso

		Uso no previsto
		Difusión de software dañino
		[Re-]encaminamiento de mensajes
		Alteración de secuencia
		Acceso no autorizado
		Análisis de tráfico
		Repudio
		Interceptación de información (escucha)
		Modificación deliberada de la información
		Destrucción de información
		Divulgación de información
		Manipulación de programas
		Manipulación de equipos
		Denegación de servicio
		Robo
		Ataque destructivo
		Ocupación enemiga
		Indisponibilidad del personal
		Extorsión
		Ingeniería social (picaresca)

Fuente: Elaboración propia

Obtenida de: Ministerio de Hacienda y Administraciones Públicas, Libro II, (2012, págs. 25-47)

De igual manera en MAGERIT se muestra una pequeña descripción de algunas las amenazas.

Según Ortiz Lazo, J., Vizñay Duran, J., define a las vulnerabilidades como acciones inseparables a los activos que proveen las amenazas que se pueden materializar y llevar a los

activos a ser vulnerables, mientras las amenazas están presentes, pero sin la identificación de las posibles vulnerabilidades no se podrán ocasionar ningún impacto. (2019, pág. 179)

En el formato que se va a emplear del EGSI V2, se muestra en el "Cuadro resumen catalogo amenazas comunes (EGSI-V2)" muestra ejemplos de amenazas y vulnerabilidades que pueden existir.

De igual manera existen herramientas que nos brinda Kali Linux (distribución basada en Debian GNU/Linux diseñada para la auditoría y seguridad informática) entre estas se encuentran:

- **nmap:** Para Chamorro Pantoja, A & Pupiales Chacón, S., (2021, pág. 119) es un mapeador de redes que se utiliza en la detección de redes y auditoría, inventarios de red, gestión y actualización de programas y monitoreo de actividad del host de servicio.
- **Wireshark:** Según Chamorro Pantoja, A & Pupiales Chacón, S., (2021, pág. 120) permite ver lo que sucede en la red, además es una excelente aplicación que ayuda en los problemas de red, estudio de comunicaciones y facilita las opciones de administración para realizar un análisis de tráfico.

2.2.4. Evaluación de riesgo

Para la evaluación de riesgos el Libro III de MAGERIT nos muestra una guía de técnicas, que ayudará a ver cuáles técnicas pueden ser empleadas en el análisis y gestión de riesgos.

El Ministerio de Hacienda y Administraciones Públicas, Libro III, (2012, pág. 6), hace mención del análisis mediante tablas donde se muestra en la Tabla 8, para calificar el valor de los activos para conocer la magnitud del impacto y del riesgo.

Tabla 8. *Análisis mediante tablas*

Impacto	Código	Valor
MUY ALTO	MA	5
ALTO	A	4
MEDIO	M	3
BAJO	B	2
MUY BAJO	MB	1

Fuente: Elaboración propia

Obtenido de: Ministerio de Hacienda y Administraciones Públicas, Libro III, (2012, pág. 6)

Este modelo que se presenta, en la Tabla 8, se puede reducir a 3, en este caso sería Alto, Medio y Bajo, esta forma es la que nos presenta el formato de evaluación de riesgo del EGSI V2.

Para conocer el riesgo, al que se pueden ver afectados los activos por sus diferentes vulnerabilidades, se utiliza la siguiente fórmula matemática:

$$Impacto \times Probabilidad \times Valor\ Activo = \boldsymbol{Riesgo}$$

El impacto según el EGSI V2 son las consecuencias o efectos que puede ocasionar la materialización del riesgo al proceso y por ende a la institución; valorando la confidencialidad, integridad y disponibilidad de la información

La probabilidad es la medida para estimar la ocurrencia del riesgo y el valor del activo se lo realiza en cuando a la confidencialidad, integridad y disponibilidad en la que se puede ver afectada.

La importancia de la evaluación de riesgos permite a las organizaciones priorizar los esfuerzos de protección y la asignación de recursos de manera efectiva, la forma que utiliza el EGSI V2 es la realización de un cálculo con los valores que se muestran en la Tabla 8, dentro del formato se puede realizar la evaluación y ver el control que se llevará a cabo.

2.2.5. Controles de la norma ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 presenta el **Anexo A** que nos ayuda como una guía para implementar controles de seguridad específicos. De igual manera, especifica que para su aplicación va a depender si la organización realmente los necesita o no, en el caso de que no necesita implementar algunos controles establecidos en la norma.

La norma presenta en el Anexo A una clasificación de los noventa y tres (93) controles, ver Anexo II, que se dividen en cuatro (4) grupos, que se presenta los grupos en la Tabla 9.

Tabla 9. *Grupos en los que se clasifican los controles*

Controles	
Tipo	**Descripción**
Organizacionales	Todos los controles excepto aquellos que se refieren específicamente a personas, controles físicos y/o tecnológicos. Ejemplo: inadecuado espacio de trabajo
Personas	Controles de seguridad de la información respecto a las acciones que realizan las personas. Son las personas que se vinculan de algún modo con el SGSI de la organización.
Físicos	Controles que se aplican sobre objetos físicos. Ejemplo: equipos, anaqueles, libreros. Y que están considerados en el inventario de activos de la información.
Tecnológicos	Aplican sobre elementos tecnológicos: Ciberseguridad, tecnología de la información y comunicación. Ejemplo: detección de virus.

Fuente: Elaboración propia

2.2.6. Política de seguridad de la información

La implementación de la política de seguridad de la información va a ser una ayuda para el conocimiento de las amenazas internas que pueden existir dentro de la organización, la política de seguridad en sí es una declaración de las reglas que se deben respetar para acceder a la información y a los recursos. (Vega Velasco , 2008)

La política de seguridad de la información que se menciona dentro de la norma ISO/IEC 27001:2022, donde se menciona que la política es como el barco conductor de los objetivos, para la elaboración de los objetivos se puede apoyar en las preguntas:

- Qué se hará,
- Qué recursos son necesarios,
- Quién estará a cargo,
- Cuando culminará, y
- Cómo se evaluarán los resultados.

De igual manera, la política deberá ser documentada.

Los objetivos que se mencionan dentro de la política de seguridad de la información deben estar semejantes a la mejora continua, con la finalidad de evitar que las amenazas de los activos de información puedan efectuarse de manera recurrente.

Es necesario también contar con el conocimiento de quienes van a ser las partes interesadas y quienes pueden ser los responsables, debido a que los controles deberán cumplirse y dar tratamiento al riesgo.

Los controles que se pueden realizar son los siguientes:

1. Aceptación
2. Mitigación o modificación
3. Evitar
4. Transferir o distribución a terceros.

El formato que se usa para la política de seguridad de la información se encuentra en el EGSI V2, que actualmente tiene a la versión 2, pero en principios del mes de marzo, entró la versión 3 con la novedad de que falta los documentos de referencia.

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

La COAC Rural Sierra Norte se sitúa en la ciudad de Ibarra y provincia de Imbabura, de la parroquia El Sagrario, dirección Chica Narváez y Pedro Moncayo, a media cuadra del Obelisco de Ibarra, asentada en el sector urbano.

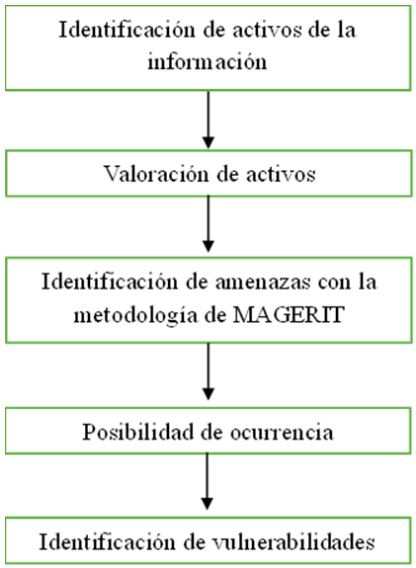
En la institución financiera, cuenta con dos (2) funcionarios en el área de TI, un (1) funcionario como auditor informático, dispone de un (1) servidor físico en un CPU, dos (2) portátiles, red interna inalámbrica, mismos que se encuentra interconectados y con el suministro de internet a las seis (6) departamentos administrativos, cuenta con un sistema de circuito cerrado (CCTV).

3.2. Enfoque y tipo de investigación

Es fundamental investigar y analizar los riesgos que pueden suscitarse y que puedan afectar los procesos de la cooperativa. El objetivo de la evaluación de los riesgos es determinar si los riesgos son aceptables o infringe las normas institucionales, para lo cual se definió una metodología por la cual se analizará y evaluará los riesgos que existente actualmente.

La investigación propuesta se contextualiza con el enfoque cualitativo, basado en la aplicación de una encuesta al personal del área de TI, además de identificar las amenazas relacionadas con cada uno de los activos de la información y la posibilidad de que dichas amenazas se cumplan. Adicionalmente se propone como técnica de validación el juicio de expertos, para determinar su criterio con respecto a la propuesta de políticas de seguridad de la información y con ello establecer si se cumple la hipótesis de trabajo planteada.

Figura 7. *Metodología de evaluación de riesgo*



Fuente: Elaboración propia

3.3.Procedimiento de investigación

El presente estudio se realizará de acuerdo con las siguientes fases:

Fase 1: Identificación de los activos de la información

Para el presente estudio se efectuó la identificación de los activos; se realizó una revisión del libro II de MAGERIT que presenta un catálogo de activos, ver Tabla 6, para la clasificación se tendrá la opción de visitar a la cooperativa de ahorro y crédito para conversar con el Responsable del Área de Tecnología con la finalidad de tener en claro cuales activos van a ser identificados para su valoración y evaluación.

Para la valoración de los activos de la información se utilizó un enfoque cualitativo, en este caso se presenta un formato establecido por el EGSI V2, en el documento se muestra una forma de valorar el activo en base a la Confidencialidad, Integridad y Disponibilidad (por sus palabras en inglés, *Confidentiality, Integrity, Availability*, más conocido como CIA),

La fórmula para obtener el valor del activo es la siguiente:

$$\frac{valor\ confidencialidad\ + valor\ integridad + valor\ disponibilidad}{3} = Valor\ de\ activo$$

Una vez que tenemos la valoración del activo en cuanto al impacto que puede tener en la confidencialidad, integridad y disponibilidad, ver Tabla 11, podemos avanzar a la siguiente fase.

Fase 2: Evaluación de riesgos de los activos

Con la identificación y valoración de los activos de la información, continuamos con la fase de evaluación, que en este caso se utilizó el valor de activos que obtuvimos en la fase 1, debemos tomar en cuenta la evaluación que se puede tener en el activo, ver Tabla 14, una vez que obtenemos todos los valores.

Posteriormente se utilizó el nivel de amenazas, ver Tabla 11, y nivel de vulnerabilidades, ver Tabla 12, para realizar la valoración respectiva y conocer el **cálculo de evaluación de riesgo.**

Para el conocimiento del cálculo de evaluación riesgo, se tiene la siguiente fórmula.

$$Impacto\ de\ CID \times Nivel\ de\ amenaza\ \times Nivel\ de\ vulnerabilidad\ = Evaluación\ Riesgo$$

Una vez realizado el cálculo de evaluación riesgo, tomamos en cuenta el nivel de riesgo como se muestra en la Tabla 15. Con la evaluación de riesgo se obtuvo más información de los activos y se conoció los controles que nos brinda la norma ISO/IEC 27001:2022. En el "Anexo A" se puede colocar una fecha para la posible revisión y evaluación de que el riesgo pueda haber sido, aceptado, mitigado, transferido o evitado. Con lo siguiente, podemos diseñar una política acorde a los lineamientos para una evaluación aproximada.

Fase 3: Diseño política de seguridad de la información

Para la realización de la política de seguridad de la información, se tiene un formato de referencia, misma que nos brinda el EGSI V2 en concordancia con la norma ISO/IEC 27001:2022. Este formato nos ayudó al diseño de la política de seguridad con la finalidad de reconocer el tratamiento que se le deberá dar a cada uno de los activos con el riesgo que se tiene. Además, se hará hincapié sobre los tratamientos y fechas que deberán tomar en cuenta para los riesgos y observar si la política de seguridad deberá ir en mejora continua para su implementación en otras áreas que son de alta relevancia.

Este documento una vez revisado, deberá ser:

- Incluido o ser marco referencial para los objetivos
- Incluir un compromiso de satisfacer los requisitos del Sistema de Información
- Incluir el compromiso de mejora continua
- Documentado, comunicado y estar disponible.

Fase 4: Evaluación de la política de seguridad de la información

En esta fase, la política de seguridad deberá tomar en cuenta cuáles fueron los términos y valores del tratamiento de riesgos donde obtendremos los controles que se van a implementar.

De igual manera, la política de seguridad tiene como objetivo la mejora continua y se realizó una prueba a la implementación de control, conociendo que protocolos y mecanismos de evaluación para los riesgos que se pueden evidenciar en la fase 2, para cumplir con los objetivos que se plantearon.

Para la evaluación de la Política de Seguridad de la Información, se aplicó el método Delphi con el criterio de 3 expertos en el área de seguridad de la información.

3.4.Consideraciones bioéticas

Aunque el enfoque principal de este estudio está más relacionado con aspectos técnicos y de seguridad e la información, es importante reconocer y abordar las consideraciones bioéticas relacionadas con la privacidad, seguridad de los datos y el impacto sobre empleados y la comunidad en general.

Privacidad y Protección de Datos: El respeto a la privacidad del personal del área de TI con los datos que están manejando. Es importante garantizar que se respeten las normas

de privacidad y que se implementen medidas adecuadas para proteger la información personal de los empleados y clientes.

Seguridad de los Datos: Evitar el daño mediante implementación de medidas de seguridad robustas para proteger los datos contra accesos no autorizados o brechas de seguridad. Esto no solo protege los datos de la COAC Rural Sierra Norte, sino que también cumple con el principio de no causar daño.

Transparencia y Comunicación: Es muy importante informar al Responsable del Área de Tecnología y a las partes interesadas sobre los controles propuestos en la infraestructura de red, software y hardware. Esto puede ayudar a mejorar el manejo de la información para todos los empleados.

CAPITULO IV

4. MARCO ADMINISTRATIVO

4.1.Identificación de servicios y sistemas

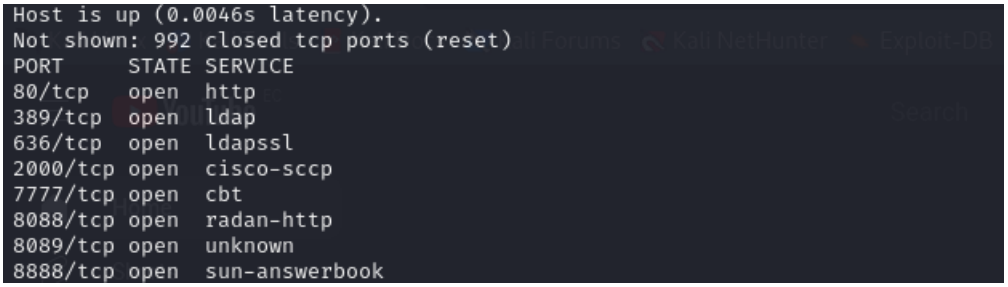
Se realizó una exploración a la red de la cooperativa de ahorro y crédito, con la finalidad de conocer cuales servicios se están ejecutando.

Para la exploración se ha utilizado la máquina virtual de Kali Linux, que nos permite utilizar la herramienta de **NMAP** que se la utiliza mediante comandos, misma que fue escogida anteriormente, si se desea utilizar con interfaz gráfica es la herramienta **ZENMAP**.

Para la obtención de las direcciones IP dentro de la red que se maneja en la cooperativa, se utilizó el siguiente comando con una IP de ejemplo **sudo nmap -O "192.168.1.0/24"**. Que se tiene como resultado las direcciones IP con los puertos, estado y servicio. En el área de estudio se realizó la identificación de las direcciones de los equipos que se manejan dentro del área de TI.

A continuación, se presenta el escaneo mediante nmap con las direcciones IP de la red de la cooperativa, con vista de los puerto, estado y servicios, de igual manera se muestra en tablas el puerto, servicio, protocolo, detalle. Como se muestra a continuación en la Figura 8-14, Tabla 11-17

Figura 8. *Escaneo de red de la central telefónica*



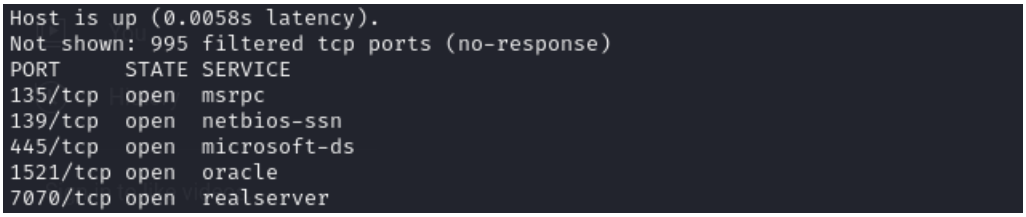
Fuente: Elaboración propia

Tabla 10. *Puertos y servicios de la dirección IP escaneada*

Listado de puertos y servicios			
Puertos	**Protocolo**	**Servicio**	**Detalle**
80	tcp	http	Protocolo de transferencia de hiper texto
389	tcp	ldap	Lightweight Directory Access Protocol
636	tcp	ldapssl	Lightweight Directory Access Protocol Sockets Security Layer
2000	tcp	cisco-sccp	Cisco SCCP
7777	tcp	cbt	Mesh
8088	tcp	radan-http	Resource Manager
8089	tcp	Virtualization Station (HTTPS)	Vitualization Station
8888	tcp	sun-answerbook	Puerto de Administración

Fuente: Elaboración propia

Figura 9. *Escaneo de red de laptop de Oficial de Seguridad de la Información*



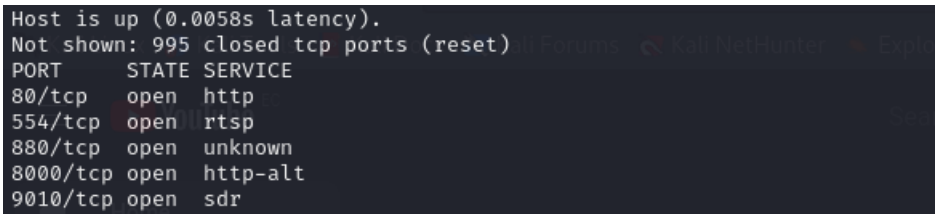
Fuente: Elaboración propia

Tabla 11. *Puertos y servicios de la dirección IP de laptop de Oficial de Seguridad de la Información*

Listado de puertos y servicios			
Puertos	**Protocolo**	**Servicios**	**Detalle**
135	tcp	msrpc	Microsoft RPC
139	tcp	netbios-ssn	Servicio de sesión
445	tcp	microsoft-ds	Microsoft-DS
1521	tcp	oracle	Base de datos Oracle
7070	tcp	realserver	Servidor multimedia

Fuente: Elaboración propia

Figura 10. *Escaneo de red de DVR (cámara de video primer piso)*



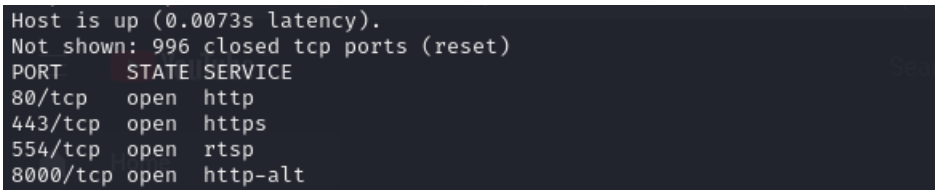
Fuente: Elaboración propia

Tabla 12. *Puertos y servicios del DVR*

Listado de puertos y servicios			
Puertos	**Protocolo**	**Servicios**	**Detalle**
80	tcp	http	Protocolo de transferencia de hiper texto
554	tcp	rtsp	Protocolo de transmisión en tiempo real
880	tcp	ipcserver	Router cisco
8000	tcp	http-alt	Estación de descarga
9010	tcp	sdr	Secure Data Replicator Protocol

Fuente: Elaboración propia

Figura 11. *Escaneo de red de DVR (cámaras de video segundo piso)*



Fuente: Elaboración propia

Tabla 13. *Puertos y servicios del DVR (segundo piso)*

Listado de puertos y servicios			
Puertos	**Protocolo**	**Servicios**	**Detalle**
80	tcp	http	Protocolo de transferencia de hiper texto
443	tcp	https	HTTPS (Hypertext Transfer Protocol over SSL/TLS) (Official)
554	tcp	Rtsp	Protocolo de transmisión en tiempo real
8000	tcp	http-alt	Estación de descarga

Fuente: Elaboración propia

Figura 12. *Escaneo de red, dirección IP de Servidor de pruebas*

Fuente: Elaboración propia

Tabla 14. *Lista de puertos y servicios del Servidor de pruebas*

Listado de puertos y servicios			
Puerto	**Protocolo**	**Servicio**	**Detalle**
135	tcp	msrpc	Microsoft RPC
139	tcp	netbios-ssn	Servicio de sesión
445	tcp	microsoft-ds	Microsoft-DS
3389	tcp	ms-wbt-server	Protocolo de escritorio remoto

Fuente: Elaboración propia

Figura 13. *Escaneo de red de laptop de responsable del área de tecnología*

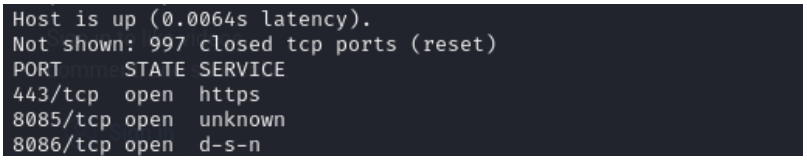
Fuente: Elaboración propia

Tabla 15. *Lista de puertos y servicios del responsable de área de tecnología*

Listado de puertos y servicios			
Puerto	**Protocolo**	**Servicio**	**Detalle**
135	tcp	msrpc	Microsoft RPC
139	tcp	netbios-ssn	Servicio de sesión
445	tcp	microsoft-ds	Microsoft-DS

Fuente: Elaboración propia

Figura 14. *Escaneo de red de switch*



Fuente: Elaboración propia

***Tabla* 16.** *Puertos y servicios del switch*

Listado de puertos y servicios			
Puertos	**Protocolo**	**Servicios**	**Detalle**
443	tcp	https	HTTPS (Hypertext Transfer Protocol over SSL/TLS) (Official)
8085	tcp	irdmi	EMC2 (Legato) Networker or Sun Solcitice Backup (Official)
8086	tcp	d-s-n	Distributed SCADA Networking Rendezvous Port

Fuente: Elaboración propia

4.2.Identificación de criterios de valoración

Para la valoración de los criterios que van a tener impacto sobre los activos de la información, se realiza una perspectiva desde el criterio de la confidencialidad, integridad y disponibilidad, como se muestra la Tabla 18, 19 y 20, estos criterios ayudan a tener idea de los términos de pérdida.

Tabla 17. *Criterio de valoración de activo en la confidencialidad*

Valoración del impacto en términos de la perdida de la confidencialidad	**Criterio**
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución. Ejemplo: Divulgación de información confidencial o sensible.

Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución. Ejemplo: Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución. Ejemplo: Divulgación de información pública.

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

Tabla 18. *Criterio de valoración de activo en la integridad*

Valoración del impacto en términos de la perdida de la integridad	Criterio
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

Tabla 19. *Criterio de valoración de activo en la disponibilidad*

Valoración del impacto en términos de la perdida de disponibilidad	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

4.3.Niveles de riesgo para los activos

Una vez realizada la valoración de los activos, se procede al diseño de la tabla para la evaluación de los activos bajo los niveles de confidencialidad, integridad y disponibilidad, ver Tabla 21, en la tabla se puede observar en qué tipo de rango puede estar evaluado el activo y entre que valores de nivel de riesgos pueden estar los activos como se muestra en la Tabla 22.

Tabla 20. *Tabla de referencia para evaluación de activo*

Tabla de evaluación del activo										
Nivel de Amenaza		Bajo (1)			Medio (2)			Alto (3)		
Nivel de Vulnerabilidades		Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)
Valor del impacto en términos de la pérdida de (CID) en los activos	Bajo (1)	1	2	3	2	4	6	3	6	9
	Medio (2)	2	4	6	4	8	12	6	12	18
	Alto (3)	3	6	9	6	12	18	9	18	27

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

Tabla 21. *Nivel de riesgo*

Nivel de Riesgo		
1	3	BAJO
4	8	MEDIO
9	27	ALTO

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

4.4.Estimación de amenazas y vulnerabilidades

Ayuda a la identificación de qué rango puede tener una amenaza y vulnerabilidad que puede afectar a los activos de la información. De igual manera nos muestra una explicación del nivel que pueden tener las amenazas y vulnerabilidades con sus respectivos valores. Ver Tabla 23 y 24.

Tabla 22. *Estimación de amenazas*

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque	desastres naturales
No aplica (0)				

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

Tabla 23. *Estimación de vulnerabilidades*

Nivel de vulnerabilidad	Criterio	Ejemplo
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Fuente: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

4.5.Identificación de activos de la información

En el área de TI, los activos de la información que forman parte de todos los procesos que se llevan a cabo dentro de la Cooperativa, existen diferentes tipos de activos informáticos, sistema de información, software y los tipos físicos.

Tabla 24. *Inventario de activos del Área de TI*

Inventario de Activos de la Información	
Identificación del activo	Laptop de Oficial de Seguridad de la Información
Tipo de activo	Activo físico móvil
Descripción	Marca: Asus Modelo: F15 Procesador: Intel core i5 10ma Memoria: 16 GB RAM Almacenamiento: 500 GB SSD
Propietario	Oficial de Seguridad de la Información
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Servidor de pruebas
Tipo de activo	Activo físico

Descripción	Marca: S/N Modelo: S/N Procesador: Intel core i7 13va Memoria: 32GB RAM Almacenamiento: 1TB SSD
Propietario	Responsable del Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Laptop de Responsable del Área de Tecnología
Tipo de activo	Activo físico móvil
Descripción	Marca: Asus Modelo: Vivobook Procesador: Intel core i7 Memoria: 16 GB RAM Almacenamiento: 480 GB SSD
Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Sistema de circuito cerrado de televisión (cctv)
Tipo de activo	Activo físico
Descripción	Marca: Epcom Modelo: EV4004TURBO Almacenamiento: 1 TB
Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Central telefónica
Tipo de activo	Activo físico
Descripción	Marca: Grandstream network Modelo: UCM6202

Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Conjunto de 2 Switch
Tipo de activo	Activo físico
Descripción	Marca: Mikrotik Routerboard (10 puertos) y TP-Link (24 puertos)
Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Router para Banco Central
Tipo de activo	Activo físico
Descripción	Marca: Cloud Core Router Modelo: CCR1009-7G-1C-15 Puertos: 24-Port-Gigabit Switch
Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Core Financiero
Tipo de activo	Software
Descripción	VimaSistem (Sistema Financiero)
Propietario	Responsable de Área de Tecnología
Localización	Área de TI
Inventario de Activos de la Información	
Identificación del activo	Base de datos
Tipo de activo	Base de datos
Descripción	Oracle Respaldos elaborados por el Responsable de Área de Tecnología

Propietario	Administrador de core financiero y Responsable de Área de Tecnología
Localización	Área de TI

Fuente: Elaboración propia

4.6.Valoración de los activos

Para la evaluación de estos activos tenemos un rango de 1 a 3 para después obtener la valoración de los activos.

Tabla 25. *Valoración de activos*

Valoración de activos				
Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**TOTAL**
Laptop oficial de seguridad de la información	3	3	2	2,67
Servidor de pruebas	3	3	3	3
Laptop responsable de área de tecnología	3	3	2	2,67
Sistema de circuito cerrado de televisión (cctv)	3	3	3	3
Central telefónica	2	2	2	2,00
Switch	3	3	3	3,00

Router de Banco Central	3	3	3	3,00
Core financiero (Sistema Financiero)	3	3	3	3,00
Base de datos	3	3	3	3,00

Fuente: Elaboración propia

Lo siguiente es determinar los activos que tienen un valor mayor o igual a 2, que van a ser analizados en la evaluación de riesgos.

4.7.Evaluación de riesgos

Para el análisis de riesgo donde se coloca las amenazas y vulnerabilidades, donde se tiene que tomar en cuenta los factores que pueden estar expuestos dentro del área de TI.

En la evaluación de riesgos, el impacto es el resultado de la valoración del activo que se hizo anteriormente en la Tabla 25, posteriormente se realiza una evaluación donde se tiene un rango de 1 a 3 para mantener un nivel real de amenazas y vulnerabilidades. De igual manera, se pueden ver los controles que se tienen implementados y cuál va a ser el cálculo de la evaluación de riesgo y el nivel del riesgo que se tienen para los activos como se muestra en la Tabla 27.

Tabla 26. *Evaluación de riesgos*

Análisis de Riesgo				Evaluación de Riesgos					
				Impacto	Probabilidad		Controles implementados existentes	Cálculo de Evaluación de Riesgo	Nivel de Riesgo
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Laptop oficial de seguridad de la información	Hurto del equipo	Falta de seguridad física	2,67	3	3	Candado para laptop.	24,00	ALTO
		Incumplimiento de mantenimiento	Mantenimiento insuficiente		3	2	Control trimestral	16,00	ALTO
		Daño de disco de almacenamiento	Ausencia de equipo de reemplazo		3	3	Respaldo en la nube	24,00	ALTO
		Malware	Falta de antivirus		3	3	Antivirus Gravity Zone	24,00	ALTO
A2	Servidor	Almacenamiento sin protección	Hurto de respaldo	3,00	3	3	No existe control	27,00	ALTO
		Malware	Falta de antivirus		3	3	Antivirus BitDefender Gravity Zone	27,00	ALTO
			Falta de control de navegación web		2	3	Antivirus BitDefender Gravity Zone	18,00	ALTO
		Daño por inundación	Ubicación en área susceptible a inundación		3	3	Ninguno	27,00	ALTO
		Daño por suministro eléctrico	Red energética inestable		3	3	UPS	27,00	ALTO
A3	Laptop responsable de	Hurto del equipo	Falta de seguridad física	2,67	3	3	Candado para laptop.	24,00	ALTO

	área de Tecnología	Incumplimiento de mantenimiento	Mantenimiento insuficiente		3	2	Control trimestral	16,00	**ALTO**
		Daño de disco de almacenamiento	Ausencia de equipo de reemplazo		3	3	Respaldo en la nube	24,00	**ALTO**
		Malware	Falta de antivirus		3	3	Antivirus BitDefender Gravity Zone	24,00	**ALTO**
A4	**CCTV**	Mantenimiento de sistema del DVR	Falla de fecha y horas	3,00	2	2	Control de configuración con internet de fecha y hora	12,00	**ALTO**
		Daño de DVR	Falta de respaldos		3	3	Ninguno	27,00	**ALTO**
		Daño de cámaras	Mal color de imagen		2	2	No tienen cámaras de respaldo	12,00	**ALTO**
			Baja resolución		3	3	Ninguno	27,00	**ALTO**
		Ubicación	Falta de mejor enfoque de visualización		3	3	Ubicación estratégica	27,00	**ALTO**
A5	**Central Telefónica**	Pérdida de conexión de red	Configuración inadecuada	2,00	2	2	Ninguno	8,00	**MEDIO**
			Corte de llamadas		2	2	Ninguno	8,00	**MEDIO**
A6	**Switch**	Sobre calentamiento	Red energética inestable	3,00	3	3	Ninguno UPS en 3 meses	27,00	**ALTO**
		Pérdida o daño de equipo			3	3	Ninguno	27,00	**ALTO**
A7	**Router Banco Central**	Pérdida de conexión de red	Configuración inadecuada	3,00	3	3	Ninguno	27,00	**ALTO**
A8	**Core Financiero**	Pérdida de conexión de red	Lentitud de software	3,00	3	2	Cambio de proveedor	18,00	**ALTO**
		Robo de identidad	Divulgación de contraseñas		3	2	Control de 3 meses en	18,00	**ALTO**

							actualización de contraseña		
			Robo de información		3	3	Capacitación	27,00	**ALTO**
		Manipulación de software	Ausencia de copias de seguridad		3	3	Respaldo de seguridad que es automático	27,00	**ALTO**
		Fallas en el core financiero	Falta de pruebas		3	3	Pruebas de nuevos procesos en el servidor de pruebas previa implementación	27,00	**ALTO**
A9	**Base de datos**	Ransomware	Falta de encriptación	3,00	3	3	Control de encriptación del proveedor	27,00	**ALTO**
		Manipulación de software	Ausencia de copias de seguridad		3	3	Acceso de escritorio solo el proveedor.	27,00	**ALTO**

Fuente: Elaboración Propia

Obtenido de: Esquema Gubernamental de Seguridad de la Información, Formato-Referencial_Matriz-de-Evaluación-de-Riesgos-de-Seguridad-de-la-Información-EGSI-V2 (2019)

Una vez finalizada la evaluación y análisis de riesgos de los activos de la información de la COAC Rural Sierra Norte, se toma en cuenta a los activos con las valoraciones más altas que van a estar afectadas ante posibles daños y/o vulnerabilidades.

4.8.Declaración de aplicabilidad

Dentro de la SGSI, la declaración de aplicabilidad, que es un punto para la instauración con una alta escalabilidad dentro de la institución que se encuentra basada en las áreas que menciona la Norma ISO 27001:2022.

Para esto necesitamos apoyarnos en la Tabla 10., que nos indica por las áreas y los controles que se pueden implementar dentro del mismo. Esto nos permitirá ver cuál control se puede tomar en cuenta para mitigar, corregir, evitar o transferir el riesgo que se tiene en los activos de la información.

Los controles que se van a implementar dentro de la COAC Rural Sierra Norte están verificados con el Oficial de Seguridad de la Información y el Responsable del Área de Tecnología, que ayudará a la mejora continua de la institución con la Seguridad de la Información.

Tabla 27. *Declaración de aplicabilidad de Seguridad de la Información Norma ISO 27001:2022*

NRO	CONTROL	CONTROLES IMPLEMENTADOS	CONTROLES PARA TRATAMIENTO	JUSTIFICACIÓN
A.5	**Controles aplicables a la organización**			
5.1	Políticas para la seguridad de la información	SI	Política de seguridad de la información para la COAC Rural Sierra Norte	La creación de la política de la seguridad de información ayudará a la institución en el mejor manejo de los activos de la información, la revisión se la realizará con el Responsable del Área de Tecnología.
A.6	**Controles aplicables al Talento Humano**			
6.3	Toma de conciencia educacional y entrenamiento sobre la seguridad de la información	SI	Capacitación sobre la seguridad de la información	El previo conocimiento que se puede dar a las personas que trabajan con información de los socios.
A.7	**Controles físicos**			
7.1	Perímetros de seguridad física	NO	Mejora de seguridad en instalaciones donde se resguarda la información	Implementación de cámaras de seguridad en el área de TI.
7.2	Ingreso físico	SI	Mejor señalización	El uso de señalización para informar a las personas sobre el acceso restringido por el uso de servidores en la misma área,
7.3	Asegurar oficinas salas e instalaciones	SI	Compra de cámaras de seguridad	La previa visualización clara de las acciones de empleados, socios y terceras personas debe ser clara y ubicada en puntos estratégicos.

7.5	Protección contra amenazas físicas y ambientales	SI	Falta de UPS para computadoras	Ante los cortes de energía eléctrica, se necesita el previo uso de UPS para evitar daños en los equipos informáticos.
7.8	Ubicación y protección de los equipos	SI	Mejorar la posición de los equipos, mantener una protección de los equipos informáticos	El posicionamiento correcto de los equipos va a permitir que nadie puede ver o espiar los documentos o información que se está utilizando en ese momento.
7.10	Medios de almacenamiento	NO	Compra de discos duros externos	Los discos duros externos servirán para el respaldo de información y de grabaciones, de igual manera para el core financiero (base de datos).
7.11	Servicios de suministro de apoyo	SI	Compra de generador de energía	Los generadores de energía pueden facilitar la continuidad de negocio dentro de la cooperativa.
7.13	Mantenimiento de equipos	SI	Cronograma de mantenimiento de equipos en el área de TI	El mantenimiento de equipos es de suma importancia para su correcto funcionamiento.
A.8	**Controles tecnológicos**			
8.2	Derecho de acceso privilegiados	SI	Mejorar y definir los roles que se utilizan y sus opciones en el core financiero	La definición de los roles y el acceso que pueden tener en el core financiero ayudará a mantener la confidencialidad e integridad de los datos.

8.3	Restricción de acceso a la información	SI	Bloqueo de reportes a diferentes roles	Los reportes al no estar asignados por roles de una forma definitiva, puede evidenciar la falta de confidencialidad e integridad de datos.
8.5	Autenticación segura	SI	Capacitación de contraseñas seguras	El cambio de contraseña y conocimiento de cómo pueden ser más seguras.
8.7	Protección contra programas maliciosos (malware)	SI	Charla sobre la descargar o uso de dispositivos sin autorización del área de TI	El bloqueo de páginas web que permiten descargar software que no es permitido por el área de TI.
8.8	Gestión de vulnerabilidades técnicas	SI	Documentación de vulnerabilidades anteriores	El tener documentado las vulnerabilidades que han existido antes, puede ayudar a mejorar el funcionamiento en buscar la solución rápida.
8.9	Gestión de la configuración	SI	Implementación de documentación de cambios en el software para supervisión y control.	La documentación siempre ayudará a visualizar a los futuros ingenieros que puedan ingresar los cambios que se han implementado y resultado en buenas prácticas.
8.12	Prevención de fuga de datos	SI	Denegar el acceso a toda página web mediante aplicación	Controlar el acceso a la información confidencial y el acceso a los lugares donde se guardan los respaldos.

8.13	Copia de seguridad de la información	SI	Compra de medios de almacenamiento.	Las copias de seguridad ayudan a mantener la información respaldada cuando existan problemas de hardware o software.
8.29	Pruebas de seguridad en desarrollo y aceptación	SI	Utilización de servidor de pruebas para detectar fallas antes de la implementación	Las pruebas en los servidores ayudan a detectar fallas que pueden ser corregidas con la finalidad de tener el core financiero en buen funcionamiento.
8.33	Información de las pruebas	SI	Control y documentación de las pruebas realizadas en el core financiero	El control de todas las pruebas que se realiza previa a la implementación ayuda a verificar que problemas se deben solucionar.

Fuente: Elaboración propia

4.9.Tratamiento de Riegos, después de la evaluación de riesgos

El tratamiento de riesgos ayudará a mejorar el funcionamiento de la cooperativa sobre todo permite implementar controles en los activos de la información, de igual manera, brinda la mejora continua a toda la seguridad física del área de TI que tiene relación con el objetivo de la política de seguridad de la información que se implementará a futuro dentro de toda la cooperativa.

Los tratamientos implementados han sido aclarados con el Responsable del Área de Tecnología para que pueda ser aceptado e informado a todo el personal que resguarda información valiosa mediante el apoyo de una capacitación que va a servir como un nuevo aprendizaje sobre la importancia de la seguridad de la información, con la finalidad de ir realizando la capacitación a todo el personal. Los controles que se implementaran dentro de la cooperativa se las va a realizar en un tiempo planteado debido a los medios y recursos que se van a necesitar.

La Tabla 29, presenta los controles que se realizarán dentro del área de TI con la finalidad de mejorar el manejo de la información digital y físico, de igual forma, la Gerente General de la COAC Rural Sierra Norte tendrá el conocimiento de los controles que la Norma ISO/IEC 27001:2022 plantea y que servirán para mejorar el funcionamiento.

Tabla 28. *Tratamiento de riesgos de los activos de la información*

Análisis de Riesgos	Evaluación de Riesgos		Tratamiento de Riesgos							Riesgo residual
Nombre Activo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	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	
Laptop de Oficial de Seguridad de la Información	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.8 Ubicación y protección de los equipos	1	1	2,67	**BAJO**	**ACEPTABLE**
	16,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	2,67	**BAJO**	**ACEPTABLE**
	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.10 Medios de almacenamiento	1	1	2,67	**BAJO**	**ACEPTABLE**
	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.7 Protección contra programas maliciosos (malware)	1	1	2,67	**BAJO**	**ACEPTABLE**
Servidor de pruebas	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.1 Perímetros de seguridad física 7.2 Ingreso físico 7.3Asegurar oficinas, salas e instalaciones	1	1	3,00	**BAJO**	**ACEPTABLE**
	12,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.7 Protección contra programas maliciosos (malware)	1	1	3,00	**BAJO**	**ACEPTABLE**

	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.7 Protección contra programas maliciosos (malware)	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.5 Protección contra amenazas físicas y ambientales	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.11 Servicios de suministro de apoyo	1	1	3,00	**BAJO**	**ACEPTABLE**
Laptop de Responsable de Área de Tecnología	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.8 Ubicación y protección de los equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	16,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.10 Medios de almacenamiento	1	1	3,00	**BAJO**	**ACEPTABLE**
	24,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.7 Protección contra programas maliciosos (malware)	1	1	3,00	**BAJO**	**ACEPTABLE**
CCTV	12,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.10 Medios de almacenamiento	1	1	3,00	**BAJO**	**ACEPTABLE**
	12,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.8 Ubicación y protección de los equipos	1	1	3,00	**BAJO**	**ACEPTABLE**

Central Telefónica	4,00	**MEDIO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL PREVENTIVO**	8.9 Gestión de configuración	1	1	3,00	**BAJO**	**ACEPTABLE**
	8,00	**MEDIO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL PREVENTIVO**	8.8 Gestión de vulnerabilidades técnicas	1	1	3,00	**BAJO**	**ACEPTABLE**
Switch	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.13 Mantenimiento de equipos	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	7.5 Protección contra amenazas físicas y ambientales 7.8 Ubicación y protección de los equipos 7.11 Servicios de suministro de apoyo	1	1	3,00	**BAJO**	**ACEPTABLE**
Router Banco Central	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.9 Gestión de configuración	1	1	3,00	**BAJO**	**ACEPTABLE**
Core Financiero	18,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de configuración	1	1	3,00	**BAJO**	**ACEPTABLE**
	18,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	6.3 Toma de conciencia educacional y entrenamiento sobre la seguridad de la información. 8.5 Autenticación segura	1	1	3,00	**BAJO**	**ACEPTABLE**

	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	6.3 Toma de conciencia educacional y entrenamiento sobre la seguridad de la información. 8.12 Prevención de fuga de datos 8.3 Restricción de acceso a la información	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.13 Copia de seguridad de la información	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.29 Pruebas de seguridad en desarrollo y aceptación 8.33 Información de pruebas	1	1	3,00	**BAJO**	**ACEPTABLE**
Base de datos	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.12 Prevención de fuga de datos.	1	1	3,00	**BAJO**	**ACEPTABLE**
	27,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	8.13 Copia de seguridad de la información	1	1	3,00	**BAJO**	**ACEPTABLE**

Fuente: Elaboración propia

Una vez realizada la evaluación después de 4 meses, se realizó la nueva evaluación de riesgos que se presenta en la Tabla 29., se procedió al diseño de la Política de Seguridad de la Información para la COAC Rural Sierra Norte, detectando las mejoras continuas que se plantean en la institución.

4.10. Diseño de Política de Seguridad de la Información

Para establecer la política de seguridad de la información es importante comprender todas las necesidades que están relacionadas con la gestión de la seguridad de la información en la COAC Rural Sierra Norte, misma que permitirá la implementación del SGSI.

Para el diseño de la Política de Seguridad de la Información, se ha utilizado los documentos de referencia del Esquema Gubernamental de Seguridad de la Información, que nos plantea los puntos importantes. También se ha realizado un estudio de los activos de la información dentro del Área de TI con la finalidad de tomar en cuenta los riesgos que pueden existir y cuales son los controles que se deben implementar dentro de los mismos.

4.10.1. Revisión de las Políticas de Seguridad de la Información

Dado que la entidad financiera no cuenta con un documento de política de seguridad de la información, como se mencionó anteriormente, no es posible obtener ni revisar las políticas vigentes dentro de la institución.

Una vez que se elabore la política de seguridad de la información, será necesario que el Área de TI y la Gerencia General se comprometan a realizar la revisión periódica de todas las políticas de seguridad, en especial énfasis en la política de seguridad de la información. Esto garantizará la efectividad y permitirá la mejora continua de cada una de las políticas.

CAPITULO V

5. PROPUESTA

5.1.Evaluación de Política de Seguridad de la Información

Se realizará uso del método Delphi para la evaluación, conformándose un grupo de informantes por tres (3) expertos por grado académico.

Tabla 29. *Grupo de evaluadores que participaron en la validación del modelo*

Nombre y Apellido	Profesión	Especialización	Cargo
Jhonatan Marcelo Domínguez Montalvo	Ingeniero en sistemas	Magister en seguridad informática	Jefe del Departamento de Tecnología de la Información
Jorge Armando Puga Placencia	Ingeniero en sistemas	Ingeniero en sistemas	Oficial de Seguridad Información
Carlos Andrés Manrique Cachimuel	Ingeniero en tecnologías de la información	Ingeniero en sistemas	Especialista de operaciones y seguridad de la información

Fuente: Elaboración propia

En la Tabla 30, se registran a los expertos que fijaron su perspectiva ante la coherencia de la Política de seguridad de la información con relación a la Norma ISO/IEC 27001:2022 y con el Esquema Gubernamental de Seguridad de la Información, y en este verificar el grado de alineamiento al alcance que se establece.

Ante eso fue necesario contactar a los expertos por correo electrónico e informar para dar un preámbulo del diseño de Política que va dirigido al área de TI, haciendo énfasis a la mejora de los niveles de riesgos de los activos de la información, en este caso, se realiza un resumen del planteamiento del problema.

En la Tabla 31, se presenta una escala que nos servirá para el chequeo de la política de seguridad de la información por parte de los expertos, como se muestra en la Tabla 30.

Tabla 30. *Escala para el análisis del chequeo de la política de seguridad de la información*

Calificación	Criterio de evaluación
Totalmente de acuerdo	Muy bueno (4,1 puntos a 5 puntos)
De acuerdo	Bueno (3,1 puntos a 4 puntos)
Neutral	Aceptable (2,1 puntos a 3 puntos)
En desacuerdo	Requiere atención (1,1 puntos a 2 puntos)
Totalmente en desacuerdo	Crítico 0,1 puntos a 1 puntos)

Fuente: Elaboración propia

Los resultados por parte de los expertos quienes realizaron la evaluación fueron registrados y tabulados para su análisis respectivo, ver Anexo IV.

5.2.Informe de resultados de la evaluación

Los resultados que se evidenciaron después de consultar con los expertos, ver Anexo IV, en la evaluación de la política de seguridad de la información son los siguientes:

Tabla 31. *Resultados de juicio de expertos*

ITEMS	TDA 5	DA 4	N 3	D 2	TD 1	TOTAL	PROMEDIO
1. Se plantea una norma para reconocer los activos de la información en toda la organización	2		1			13	4,33
2. Se facilita el reconocimiento de vulnerabilidades y amenazas asociadas a estos activos	1	2				13	4,33
3. Se establece una evaluación de riesgos de los activos de la información	1	2				13	4,33
4. ¿Esta evaluación se alinea con el Esquema Gubernamental de Sistemas de la Información y los requisitos de la ISO 27001:2022?	3					15	5,00
5. Se establecen claramente los roles y responsabilidades como lo menciona la Norma ISO/IEC 27001:2022	3					15	5,00
6. Se incluyen responsabilidades para salvaguardar la información en todos los niveles de la organización, incluyendo la alta dirección	3					15	5,00
7. El modelo de política propuesto sigue una secuencia lógica alineada con el ciclo PDCA	1	2				13	4,33

8. El modelo de política es claro y conciso		3				12	4,00
9. La política se adapta al contexto específico de la organización	3					15	5,00
10. Se establecen objetivos claros de seguridad de la información	2	1				14	4,66
11. La política refleja el compromiso de la alta dirección con la seguridad de la información	3					15	5,00
12. La política incorpora un enfoque basado en riesgos en todas las decisiones y procesos de seguridad	1	2				13	4,33
13. Se establece un proceso continuo de evaluación y tratamiento de riesgos	1	1	1			12	4,00
14. Se establecen procesos para la revisión y actualización regular de la política	1	2				13	4,33
TOTAL							**4.55**

Fuente: Elaboración propia

De acuerdo con los datos que se muestran al tener los resultados de la lista de chequeo realizada por los 3 expertos en seguridad de la información, se muestra que la calificación está dentro del rango Totalmente de acuerdo (TDA) con un valor de **4,55** sobre **5,00**.

Una vez realizada la validación de los expertos y teniendo los resultados presentes, se entregó los documentos a la cooperativa de ahorro y crédito con la finalidad de que puedan seguir con la implementación en las demás áreas y proceder con la evaluación de los riesgos en los

activos de la información de forma semestral para mantener un mejor control y tomar en cuenta la mejora continua.

5.3. Diseño de la política de seguridad de la información

Para el diseño de la política de seguridad de la información, se utilizó el formato de referencia del Esquema Gubernamental de Seguridad de la Información, al mismo que se le ha implementado unos literales que debería tener la política como son:

- **Normas de Aplicación:** menciona algunas normas que se utilizaron para dicha política y que pueden ayudar a la mejora continua de la política de seguridad de la información.

- **Excepciones y Sanciones:** que se deberá revisar para toda persona que incumpla las normas de la política, esto se deberá revisar en el reglamento interno de la institución.

Se presenta el diseño de la política de seguridad de la información en el Anexo V, para que se pueda revisar, ya que dicha política fue validada por tres (3) expertos.

CAPITULO VI

6. CONCLUSIONES Y RECOMENDACIONES

De acuerdo con los objetivos establecidos para el desarrollo de este trabajo, se concluye lo siguiente:

- Se realizó el inventario de activos de la información dentro del Área de Tecnología de Información, con el cumplimiento basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) donde se presenta un modelo de clasificación por la función y nivel que ayudó a facilitar su reconocimiento.
- Se aplicó la Metodología Magerit, comenzando con un análisis de los tipos de activos. Esta metodología facilitó el reconocimiento de las amenazas, lo que permitió una identificación más rápida de las vulnerabilidades y riesgos, además de aportar una evaluación más precisa de los riesgos, conforme a los requisitos de la Norma ISO/IEC 27001:2022. También se establecieron intervalos para la evaluación periódica de los activos. Además, mejoró la documentación y la comunicación, promoviendo la mejora continua.
- Se diseñó un formato de la Política de Seguridad de la Información destinado al área de TI de la Cooperativa de Ahorro y Crédito, basado en el formato del EGSI (Esquema Gubernamental de Seguridad de la Información V2). Este formato no solo facilitó al diseño de la política centrada en preservar la confidencialidad, integridad y disponibilidad, sino que también proporciona diversos formatos prácticos y asegura el cumplimiento de las Resoluciones planteadas por la SEPS (Superintendencia de Economía Popular y Solidaria).

- Se evaluó la Política de Seguridad de la Información para la cooperativa con tres (3) expertos que conocen sobre la seguridad de la información para valorar su nivel de aceptación, donde se pueden definir objetivos que ayudarán a extender la política a las demás áreas de la institución.
- De acuerdo con la hipótesis de trabajo planteada, y en base al resultado obtenido mediante el juicio de expertos se puede concluir que la implementación de políticas de seguridad en el área de TI de la Cooperativa de Ahorro y Crédito Rural Sierra Norte permitirá disminuir las vulnerabilidades existentes en sus aplicaciones con base en la norma ISO/IEC 27001:2022.

6.1.Recomendaciones

- Se recomienda la implementación de un plan de respuestas para la mejora continua dentro del área de TI debe darse de acuerdo con los riesgos que existen en los activos, la evaluación continua de los riesgos que pueden existir con el paso del tiempo, la capacitación sobre las normas de seguridad de la información que se deben tomar en cuenta para proteger los datos que maneja la cooperativa.
- Se recomienda la mejora continua del proceso de Política de Seguridad de la Información para las demás áreas de la cooperativa de ahorro y crédito, basándose en los procesos que son: planificar, actuar, verificar, hacer (Norma ISO/IEC 27001:2022).

- Se recomienda asignar claramente los roles y responsabilidades descritos en la política de seguridad de la información y la Resolución de la SEPS. Esta asignación es crucial para garantizar una gestión eficaz y organizada de la seguridad de la información, asegurando que cada aspecto de la seguridad de la información sea abordado de manera adecuada y eficiente.

REFERENCIAS

Calder, A., & Watkins, S. (2008). *IT governance : a manager's guide to data security and ISO 27001/ISO 27002* (4 ed.). Kogan Page Publishers. Retrieved from https://profsite.um.ac.ir/kashmiri/it_governance.pdf

Calder, A., & Watkins, S. (2019). *Information Security Risk Management for ISO 27001 / ISO 27002* (3 ed.). United Kingdom: IT Governance Publishing Ltd.

Chamorro Pantoja, A. D., & Pupiales Chacón, S. V. (2021). Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información. *(Tesis de ingeniería informática).* Universidad Politécnica Estatal del Carchi, Tulcán, Carchi, Ecuador. Retrieved from http://repositorio.upec.edu.ec/handle/123456789/1301

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105. doi:https://doi.org/10.1108/TQM-09-2020-0202

De La Cruz Rodriguez, G., Méndez Fernández, A., & Méndez Fernández, R. (2023, Agosto). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Una revisión sistemática. Innovación y Software, 4*(1), 219-236. Retrieved from https://revistas.ulasalle.edu.pe/innosoft

Esquema Gubernamental de Seguridad de la Información. (2019). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. Retrieved from Guías y formatos - EGSI: https://www.gobiernoelectronico.gob.ec/guias-y-formatos-egsi/

Guamán, A., & Cárdenas Munóz, J. V. (2022). Cumplimiento de las políticas de seguridad de información en las cooperativas de ahorro y crédito del cantón Cañar. *Pro Sciences: Revista de Producción, Ciencias e Investigación, 6*(43), 127-138. doi:https://doi.org/10.29018/issn.2588-1000vol6iss43.

Ministerio de Hacienda y Administraciones Públicas. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información.* Madrid, España.

Miranda Jiménez, J. N. (2021). Análisis de Tesis. *Mapeo Sistemático de Metodologías de Seguridad de la Información para el Control de la Gestión de Riesgos Informáticos.* Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, Guayas, Ecuador. Retrieved from https://dspace.ups.edu.ec/handle/123456789/20966

Nebreda, P. (2023, Junio 8). *¿Qué es el NIST y de qué se encarga?* Retrieved from Alice: https://alicebiometrics.com/que-es-el-nist-y-de-que-se-encarga/

Ortiz Lazo, J. E., & Vizñay Duran, J. K. (2019, Julio). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa

Sistelcel. *Polo del Conocimiento: Revista científico - profesional, 4*(7), 174-195. doi:10.23857/pc.v4i7.1029

Superintendencia de Economía Popular y Solidaria. (2021). *ENCUESTA ESTADO Y REALIDAD DE LOS SERVICIOS DIGITALES Y SEGURIDAD DE LA INFORMACIÓN EN EL SFPS 2021.* iT ahora La Revista Lider de tecnología. Retrieved from https://www.seps.gob.ec/wp-content/uploads/Estudio_SEPS_ITAhora.pdf

Superintendencia de Economía Popular y Solidaria. (2022). *SEPS-IGS-IGT-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.* Retrieved from Superintendencia de Economía Popular y Solidaria: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Tejena Macía, M. (2018, Abril). Análisis de riesgo en seguridad de la información. *Polo del Conocimiento, 3*(4), 230-244. doi:10.23857/pc.v3i4.809

Vega Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN* (1 ed.). Alicante: 3Ciencias. doi:https://doi.org/10.17993/tics.2021.4

Vega Velasco , W. (2008, Septiembre). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2*(2), 63-69. Retrieved from http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es

ANEXOS

Anexo I. Solicitud para realizar trabajo de grado

Ibarra, 12 de marzo de 2024

Dra. Myrian Cisneros
Gerente General
COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE

Estimada Doctora:

Yo, Pillajo Montalvo Esteban Patricio, con cédula de identidad Nº 100389659-2, estudiante de la Maestría en Computación con mención en Seguridad Informática, solicito a usted muy comedidamente, autorice a quién corresponda, para la realización del Trabajo de Investigación en su institución, con el tema: **"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE".**

Por la atención que se digne dar a la presente, le anticipo mis debidos agradecimientos.
Atentamente,

Ing. Esteban Patricio Pillajo Montalvo
+593982236973

Anexo II. *Tabla de controles aplicables a la organización*

5		Controles aplicables a la organización	
1	5.1	Políticas para la seguridad de la información	**La política de seguridad de la información y políticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas tanto por el personal como por las partes interesadas pertinentes,** además revisadas en intervalos planificados y cuando ocurran cambios significativos.
2	5.2	Roles y responsabilidades en seguridad de la información	Los roles y responsabilidades de seguridad de la información **deben definirse y asignarse de acuerdo con las necesidades de la organización**
3	5.3	Segregación de funciones	Funciones en conflicto y áreas de responsabilidad en conflicto **deben** ser segregadas.
4	5.4	Responsabilidades de la dirección	**La dirección debe requerir a todo el personal** que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos de la organización.
5	5.5	Contacto con autoridades	**La organización debe establecer y mantener contacto con las autoridades pertinentes.**
6	5.6	Contacto con grupos especiales de interés	**La organización debe establecer y mantener contacto con grupos especiales de interés** u otros foros y asociaciones profesionales especializados en seguridad.
7	5.7	Inteligencia de amenazas	La información relacionada con las amenazas a la 8seguridad de la información **debe ser**

			recopilada y analizada para producir inteligencia sobre las amenazas
8	5.8	Seguridad de la información en Control la gestión de proyectos	La seguridad de la información **debe estar integrada en la gestión de proyectos.**
9	5.9	Inventario de información y control otros activos asociados	Un inventario de información y otros activos asociados, incluidos los propietarios, **debe ser desarrollado ymantenido**.
10	5.10	Uso aceptable de la información yotros activos Reglas para el uso aceptable y procedimientos para el asociado	Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe ser **identificadas, documentada e implementada.**
11	5.11	Devolución de activos	El personal y otras partes interesadas, según sea apropiado, **deben devolver todos los activos de laorganización en su posesión cuando cambien o terminen su empleo, contrato o acuerdo.**
12	5.12	Clasificación de la información	**La información debe ser clasificada** de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas pertinentes.
13	5.13	Etiquetado de la información	Un conjunto de procedimientos apropiado para el etiquetado de información **debe ser**

			desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.
14	5.14	Transferencia de información	**Deben existir reglas, procedimientos o acuerdos de transferencia de información** para todos los tipos de instalaciones para transferencia, dentro de la organización y entre la organización y otras partes.
15	5.15	Control de acceso	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados **deben establecerse e implementarse** en función de los requisitos del negocio y de seguridad de la información.
16	5.16	Gestión de identidades	El ciclo de vida completo de identidades debe ser gestionado.
17	5.17	Información de autenticación	La asignación y gestión de la información de autenticación **debe ser controlada por un proceso de gestión**, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
18	5.18	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados **deben ser aprovisionados, revisados, modificados y removidos en concordancia con la política** específica de la organización y las reglas para el control de acceso.
19	5.19	Seguridad de la información en las relaciones con los proveedores	**Deben definirse e implementarse procesos** y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios del proveedor.
20	5.20	Abordar la	Los requisitos de seguridad de la información

		seguridad de la información dentro de los acuerdos con proveedores	pertinentes **deben establecerse y acordarse** con cada proveedor en función el tipo de relación con el proveedor.
21	5.21	Gestión de la seguridad de la información en la cadena de suministros de las tecnologías de la información (TIC)	La organización **debe hacer seguimiento, revisar, evaluar y gestionar** periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
22	5.22	Seguimiento, revisión y gestiónde cambios en servicios de proveedores	La organización debe hacer seguimiento, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
23	5.23	Seguridad de la información en el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube **deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.**
24	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización **debe planificar y preparar la gestión de seguridad de la información los incidentes de seguridad de la información** definiendo, estableciendo y comunicando los procesos, las funciones y las responsabilidades de gestión de incidentes de seguridad de la información.
25	5.25	Evaluación y decisión sobre	La organización **debe evaluar los eventos de seguridad de la información** y decidir si se

		eventos de seguridad de la información	categorizan como incidentes de seguridad de la información.
26	5.26	Respuesta a incidentes de seguridad de la información	**Se debe responder a los incidentes de seguridad** de la información de acuerdo con los procedimientos documentados.
27	5.27	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido de los incidentes de seguridad de **la información debe utilizarse para fortalecer y mejorar** los controles de seguridad de lainformación.
28	5.28	Recolección de evidencia	La organización **debe establecer e implementar procedimientos** para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
29	5.29	Seguridad de la información durante una interrupción	La organización **debe planificar cómo mantener laseguridad de la información** en un nivel apropiado durante una interrupción.
30	5.30	Preparación de las TIC para la continuidad del negocio	La preparación de las TIC **debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad** del negocio y los requisitos de continuidad de las TIC.
31	5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Los requisitos legales, estatutarios, regulatorios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos **deben identificarse, documentarse y mantenerse actualizados.**
32	5.32	Derechos de la propiedad intelectual	La organización **debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.**

33	5.33	Protección de registros	Los registros **deben protegerse contra pérdida**, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
34	5.34	Privacidad y protección de la información de identificación personal (IIP)	La organización **debe identificar y cumplir los requisitos** relacionados con la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
35	5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, procesos y tecnologías, **debe revisarse de forma independiente** en intervalos planificados o cuando se produzcan cambios significativos.
36	5.36	Cumplimiento con políticas reglas y normas de seguridad de la información	**Se debe revisar periódicamente el cumplimiento** de la de la información de la organización, las políticas específicas,las reglas y las normas.
37	5.37	Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información **deben documentarse** y ponerse a disposición del personal que los necesite.
6		**Controles aplicables al Talento Humano**	
38	6.1	Selección	Los controles de verificación de antecedentes de todos los candidatos para convertirse en **personal deben llevarse a cabo antes de unirse a la organización** y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a

			la que se accede y a los riesgos percibidos.
39	6.2	Término y condiciones del empleo	Los acuerdos contractuales de empleo deben establecerlas responsabilidades del personal y de la organización con respecto a la seguridad de la información.
40	6.3	Toma de conciencia educacional y entretenimiento sobre la seguridad de la información	El personal de la organización y las partes interesadas pertinentes **deben recibir una adecuada concientización**, educación capacitación en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos, según sea pertinente para su función laboral.
41	6.4	Proceso disciplinario	**Se debe formalizar y comunicar** un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas pertinentes que hayan cometido una violaciónde la política de seguridad de la información.
42	6.5	Responsabilidades después del cese o cambio de empleo	Las responsabilidades y obligaciones en materia de seguridad de la información que siguen siendo válidos después del cese o cambio de empleo **deben definirse, aplicarse y comunicarse** al personal pertinente y otras partes interesadas.
43	6.6	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información **deben ser identificados, documentados, revisados regularmente** y firmados por el personal y otras partes interesadas pertinentes.
44	6.7	Trabajo remoto	**Se debe implementar medidas de seguridad**

			cuando el personal trabaja de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.
45	6.8	Reporte de eventos de seguridadde la información	**La organización debe proporcionar** un mecanismo para que el personal informe eventos de seguridad de la información observados o bajo sospecha a través de los canales apropiados de manera oportuna.
7		**Controles físicos**	
46	7.1	Perímetros de seguridad física	Los perímetros de seguridad **deben definirse y utilizarse para proteger las áreas que contienen información** y otros activos asociados.
47	7.2	Ingreso físico	Las áreas seguras **deben estar protegidas por controles** de entrada y puntos de acceso adecuados.
48	7.3	Asegurar oficinas, salas e instalaciones	Se **debe diseñar e implementar la seguridad física** para oficinas, salas e instalaciones.
49	7.4	Supervisión de la seguridad física	Las instalaciones **deben ser monitoreadas continuamente** para detectar accesos físicos no autorizados.
50	7.5	Protección contra amenazas físicas y ambientales	**Se debe diseñar e implementar protección contra amenazas físicas ambientales**, como desastres y naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
51	7.6	Trabajo en áreas seguras	**Deben diseñarse e implementarse medidas de seguridad** para trabajar en áreas seguras.
52	7.7	Escritorio y pantallas limpios	**Deben definirse y aplicarse adecuadamente reglas**, de papeles y medios de almacenamiento extraíbles y reglas de pantalla limpia en las instalaciones de procesamiento de información.
53	7.8	Ubicación y	Los equipos **deben estar ubicados de forma segura** y

		protección de los equipos	protegidos.
54	7.9	Seguridad de los activos fuera de las instalaciones	Los activos fuera del sitio **deben protegerse.**
55	7.10	Medios de almacenamiento	Los medios de almacenamiento **deben gestionarse a lo largo de su ciclo de vida de adquisición**, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación.
56	7.11	Servicios de suministro de apoyo	Las instalaciones de procesamiento de información **deben protegerse de cortes de energía** y otras interrupciones causadas por fallas en los servicios de suministro de apoyo.
57	7.12	Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo **deben protegerse contra interceptaciones, interferencias o daños.**
58	7.13	Mantenimiento de equipos	El equipo **debe mantenerse correctamente para asegurar la disponibilidad, integridad y confidencialidad** de la información
59	7.14	Eliminación segura o reutilización de los equipos.	Los elementos del equipo que contienen medios de almacenamiento **deben verificarse para asegurar que los datos sensibles y el software con licencia se hayan eliminado** o sobrescrito de forma segura antes de su eliminación o reutilización.
8		**Controles tecnológicos**	
60	8.1	Dispositivos terminales del usuario	La información almacenada, procesada o accesible a través de dispositivos terminales de usuario **debe protegerse.**
61	8.2	Derecho de acceso privilegiados	La asignación y el uso de derechos de acceso privilegiado **deben restringirse y administrarse**.

62	8.3	Restricción de acceso a la información	El acceso a la información y otros activos asociados **debe restringirse de acuerdo con la política** específica establecida sobre control de acceso
63	8.4	Acceso al código de fuente	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las librerías de software **debe administrarse adecuadamente**.
64	8.5	Autenticación segura	**Se deben implementar tecnologías** y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política específica sobre el control de acceso.
65	8.6	Gestión de la capacidad	El uso de recursos **debe monitorearse y ajustarse** de acuerdo con los requisitos y capacidad actuales y esperados.
66	8.7	Protección contra programas maliciosos (malware)	La protección contra programas maliciosos (malware) **debe implementarse y respaldarse** mediante la toma deconciencia adecuada del usuario.
67	8.8	Gestión de vulnerabilidades técnicas	**Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso**, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
68	8.9	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes **deben establecerse, documentarse, implementarse, monitorearse y revisarse.**
69	8.10	Eliminación de la información	La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento **debe eliminarse**

			cuando ya no sea necesaria.
70	8.11	Enmascaramiento de datos	El enmascaramiento **de datos debe utilizarse de acuerdo con la política específica de la organización** sobre control de acceso, otras políticas específicas relacionadas y los requisitos del negocio, teniendo en cuenta la legislación aplicable.
71	8.12	Prevención de fuga de datos	Las medidas de prevención de fuga de datos **deben aplicarse a los sistemas, redes y otros dispositivos** que procesan, almacenan o trasmiten información sensible.
72	8.13	Copia de seguridad de la información	Las copias de respaldo de la información, el software y los sistemas **deben mantenerse y probarse regularmente** de acuerdo con la política específica establecida sobre copias de seguridad
73	8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información **deben implementarse con suficiente redundancia** para cumplir con los requisitos de disponibilidad.
74	8.15	Registro	**Se deben producir, almacenar, proteger y analizar** los registros que guarden actividades, excepciones, fallas y otros eventos relevantes.
75	8.16	Actividades de monitoreo	Las redes, los sistemas y las aplicaciones **deben monitorearse para detectar comportamientos anómalos** y tomar acciones para evaluar posibles incidentes de seguridad de la información.
76	8.17	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización **deben sincronizarse para fuentes de tiempo aprobadas.**

77	8.18	Uso de programas de utilidad privilegiados	**Se debe restringir y controlar estrictamente el uso de programas de utilidad** que puedan anular los controles del sistema y de las aplicaciones.
78	8.19	Instalación de software en sistemas operativos	**Deben implementarse procedimientos** y medidas para gestionar de forma segura la instalación de software en sistemas operativos.
79	8.20	Seguridad de redes	Las redes y los dispositivos de red **deben protegerse, administrarse y controlarse** para proteger la información ensistemas y aplicaciones.
80	8.21	Seguridad de servicios de red	**Deben identificarse, implementarse y monitorearse losmecanismos de seguridad**, los niveles de servicio y los requisitos de servicio de los servicios de red.
81	8.22	Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información **deben estar segregados en las redes de la organización**.
82	8.23	Filtrado de la web	El acceso a sitios web externos **debe administrarse para reducir la exposición a contenido malicioso**.
83	8.24	Uso de criptografía	**Deben definirse e implementarse reglas para el uso eficaz de la criptografía**, incluida la gestión de claves criptográficas.
84	8.25	Ciclo de vida de desarrollo seguro	Los requisitos de seguridad de la información **deben identificarse, especificarse y aprobarse** al desarrollar o adquirir aplicaciones.
85	8.26	Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información **deben identificarse, especificarse y aprobarse** al desarrollar oadquirir aplicaciones.
86	8.27	Arquitectura de sistemas segurosy principios de ingeniería	Los principios de ingeniería de sistemas seguros **deben establecerse, documentarse, mantenerse** y aplicarse a cualquier actividad de desarrollo de sistema de información.
87	8.28	Codificación segura	Los principios de codificación segura **deben aplicarse**

			al desarrollo de software.
88	8.29	Pruebas de seguridad en desarrollo y aceptación	Los procesos de pruebas de seguridad **deben definirse e implementarse en el ciclo de vida del desarrollo.**
89	8.30	Desarrollo subcontratado	La organización **debe dirigir, monitorear y revisar** las actividades relacionadas con el desarrollo de sistemas subcontratados.
90	8.31	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción **deben** estar separados y protegidos.
91	8.32	Gestión de cambios	Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
92	8.33	Información de las pruebas	La información de las pruebas **debe seleccionarse, protegerse y gestionarse** adecuadamente.
93	8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos **deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.**

Anexo III. *Formato de evaluación de política*

Lista de chequeo para validar el nivel de coherencia y correspondencia de la política de seguridad de la información propuesta, en función del enfoque de la Norma ISO/IEC 27001:2022

Dirigido a:

Expertos en Seguridad de la Información

Esta check list que se presenta a continuación, tiene como finalidad de medir el nivel de coherencia de la política de seguridad de la información propuesta en función al enfoque de la Norma ISO/IEC 27001:2022, a quienes se les presenta en forma de entrevista que está compuesta de cinco (5) preguntas que permiten obtener la información para analizar el cumplimiento de los lineamientos de la política, con el fin de que este análisis permita conocer los resultados para mejorar algunos ítems en la política, de tal forma que el entorno llegue a ser satisfactorio y tenga resultados positivos tanto para la investigación como para el investigador.

Instrucciones:

1. Conteste colocando en cada sección de la pregunta una X (equis) rn la descripción que se aproxime a **su opinión y percepción.** Las descripciones que se encuentran para escoger son:

- Totalmente de acuerdo (TA)
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

2. Conteste todas las preguntas en orden después de analizar cada elemento.
3. Se garantiza la confidencialidad de la información proporcionada.
4. Use lápiz para que pueda borrar cualquier respuesta que desee cambiar.

Tabla 32. *Lista de chequeo de evaluación de expertos*

ITEMS	TDA	DA	N	D	TD	TOTAL	PROMEDIO
1. Se plantea una norma para reconocer los activos de la información en toda la organización							
2. Se facilita el reconocimiento de vulnerabilidades y amenazas asociadas a estos activos							
3. Se establece una evaluación de riesgos de los activos de la información							
4. ¿Esta evaluación se alinea con el Esquema Gubernamental de Sistemas de la Información y los requisitos de la ISO 27001:2022?							
5. Se establecen claramente los roles y responsabilidades como lo menciona la Norma ISO/IEC 27001:2022							
6. Se incluyen responsabilidades para salvaguardar la información en todos los niveles de la organización, incluyendo la alta dirección							
7. El modelo de política propuesto sigue una secuencia lógica alineada con el ciclo PDCA							
8. El modelo de política es claro y conciso							
9. La política se adapta al contexto específico de la organización							

10. Se establecen objetivos claros de seguridad de la información							
11. La política refleja el compromiso de la alta dirección con la seguridad de la información							
12. La política incorpora un enfoque basado en riesgos en todas las decisiones y procesos de seguridad							
13. Se establece un proceso continuo de evaluación y tratamiento de riesgos							
14. Se establecen procesos para la revisión y actualización regular de la política							

Escala utilizada para el análisis de la lista de chequeo

Calificación	Criterio de evaluación	Cuantitativa	Cualitativa
Totalmente de acuerdo	Muy bueno (4,1 puntos a 5 puntos)		
De acuerdo	Bueno (3,1 puntos a 4 puntos)		
Neutral	Aceptable (2,1 puntos a 3 puntos)		
En desacuerdo	Requiere atención (1,1 puntos a 2 puntos)		
Totalmente en desacuerdo	Crítico 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO:

ESPECIALIDAD

CÉDULA DE IDENTIDAD:

Por este medio, hago presente que realicé la revisión de la política de seguridad de la información propuesto para la Cooperativa de Ahorro y Crédito Rural Sierra Norte, elaborado por Ing Esteban Patricio Pillajo Montalvo – Cursando estudio de la Maestría en Computación con mención en Seguridad Informática de la Universidad Técnica del Norte, quién está realizando su tesis **"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE".**

Una vez indicadas las observaciones pertinentes y aclaradas considero que la política de seguridad de la información es **VÁLIDO** para su aplicación e implementación.

Ibarra, _____ días de _____ de 2024.

_____

Nombre y Apellido

C.I.

Anexo IV. *Evaluaciones por parte de los expertos*

Lista de Chequeo

ITEMS	TDA 5	DA 4	N 3	D 2	TD 1	TOTAL	PROMEDIO
1. Se plantea una norma para reconocer los activos de la información en toda la organización			X			3	
2. Se facilita el reconocimiento de vulnerabilidades y amenazas asociadas a estos activos		X				4	
3. Se establece una evaluación de riesgos de los activos de la información		X				4	
4. ¿Esta evaluación se alinea con el Esquema Gubernamental de Sistemas de la Información y los requisitos de la ISO 27001:2022?	X					5	
5. Se establecen claramente los roles y responsabilidades como lo menciona la Norma ISO/IEC 27001:2022	X					5	
6. Se incluyen responsabilidades para salvaguardar la información en todos los niveles de la organización, incluyendo la alta dirección	X					5	
7. El modelo de política propuesto sigue una secuencia lógica alineada con el ciclo PDCA		X				4	
8. El modelo de política es claro y conciso		X				4	
9. La política se adapta al contexto específico de la organización	X					5	

10. Se establecen objetivos claros de seguridad de la información	X					5	
11. La política refleja el compromiso de la alta dirección con la seguridad de la información	X					5	
12. La política incorpora un enfoque basado en riesgos en todas las decisiones y procesos de seguridad		X				4	
13. Se establece un proceso continuo de evaluación y tratamiento de riesgos			X			3	
14. Se establecen procesos para la revisión y actualización regular de la política		X				4	

Escala utilizada para el análisis de la lista de chequeo

Calificación	Criterio de evaluación	Cuantitativa	Cualitativa
Totalmente de acuerdo	Muy bueno (4,1 puntos a 5 puntos)	**4,29**	**TDA**
De acuerdo	Bueno (3,1 puntos a 4 puntos)		
Neutral	Aceptable (2,1 puntos a 3 puntos)		
En desacuerdo	Requiere atención (1,1 puntos a 2 puntos)		
Totalmente en desacuerdo	Crítico 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Ing. Jhonatan Dominguez M., MSc.

ESPECIALIDAD: Master en Seguridad Informática

CÉDULA DE IDENTIDAD: 1003183660

Por este medio, hago presente que realicé la revisión de la política de seguridad de la información propuesto para la Cooperativa de Ahorro y Crédito Rural Sierra Norte, elaboradopor Ing Esteban Patricio Pillajo Montalvo – Cursando estudio de la Maestría en Computacióncon mención en Seguridad Informática de la Universidad Técnica del Norte, quién está realizando su tesis **"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE".**

Una vez indicadas las observaciones pertinentes y aclaradas considero que la política de seguridad de la información es **VÁLIDO** para su aplicación e implementación.

Ibarra, 07 días de septiembre de 2024.

MSc. Jhonatan Dominguez M

C.I. 1003305008

Lista de Chequeo

ITEMS	TDA 5	DA 4	N 3	D 2	TD 1	TOTAL	PROMEDIO
1. Se plantea una norma para reconocer los activos de la información en toda la organización	X					5	
2. Se facilita el reconocimiento de vulnerabilidades y amenazas asociadas a estos activos	X					5	
3. Se establece una evaluación de riesgos de los activos de la información	X					5	
4. ¿Esta evaluación se alinea con el Esquema Gubernamental de Sistemas de la Información y los requisitos de la ISO 27001:2022?	X					5	
5. Se establecen claramente los roles y responsabilidades como lo menciona la Norma ISO/IEC 27001:2022	X					5	
6. Se incluyen responsabilidades para salvaguardar la información en todos los niveles de la organización, incluyendo la alta dirección	X					5	
7. El modelo de política propuesto sigue una secuencia lógica alineada con el ciclo PDCA	X					5	
8. El modelo de política es claro y conciso		X				4	
9. La política se adapta al contexto específico de la organización	X					5	
10. Se establecen objetivos claros de seguridad de la información		X				4	

11. La política refleja el compromiso de la alta dirección con la seguridad de la información	X					5	
12. La política incorpora un enfoque basado en riesgos en todas las decisiones y procesos de seguridad	X					5	
13. Se establece un proceso continuo de evaluación y tratamiento de riesgos	X					5	
14. Se establecen procesos para la revisión y actualización regular de la política	X					5	

Escala utilizada para el análisis de la lista de chequeo

Calificación	Criterio de evaluación	Cuantitativa	Cualitativa
Totalmente de acuerdo	Muy bueno (4,1 puntos a 5 puntos)	**4,86**	**TDA**
De acuerdo	Bueno (3,1 puntos a 4 puntos)		
Neutral	Aceptable (2,1 puntos a 3 puntos)		
En desacuerdo	Requiere atención (1,1 puntos a 2 puntos)		
Totalmente en desacuerdo	Crítico 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Ing. Carlos Manrique

ESPECIALIDAD: Ingeniero en Tecnología de la Información

CÉDULA DE IDENTIDAD: 1003305008

Por este medio, hago presente que realicé la revisión de la política de seguridad de la información propuesto para la Cooperativa de Ahorro y Crédito Rural Sierra Norte, elaboradopor Ing Esteban Patricio Pillajo Montalvo – Cursando estudio de la Maestría en Computacióncon mención en Seguridad Informática de la Universidad Técnica del Norte, quién está realizando su tesis **"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE".**

Una vez indicadas las observaciones pertinentes y aclaradas considero que la política de seguridad de la información es **VÁLIDO** para su aplicación e implementación.

Ibarra, 8 días de Septiembre de 2024.

Ing. Carlos Manrique

C.I. 1003305008

Lista de Chequeo

ITEMS	TDA 5	DA 4	N 3	D 2	TD 1	TOTAL	PROMEDIO
1. Se plantea una norma para reconocer los activos de la información en toda la organización	X					5	
2. Se facilita el reconocimiento de vulnerabilidades y amenazas asociadas a estos activos		X				4	
3. Se establece una evaluación de riesgos de los activos de la información		X				4	
4. ¿Esta evaluación se alinea con el Esquema Gubernamental de Sistemas de la Información y los requisitos de la ISO 27001:2022?	X					5	
5. Se establecen claramente los roles y responsabilidades como lo menciona la Norma ISO/IEC 27001:2022	X					5	
6. Se incluyen responsabilidades para salvaguardar la información en todos los niveles de la organización, incluyendo la alta dirección	X					5	
7. El modelo de política propuesto sigue una secuencia lógica alineada con el ciclo PDCA		X				4	
8. El modelo de política es claro y conciso		X				4	
9. La política se adapta al contexto específico de la organización	X					5	
10. Se establecen objetivos claros de seguridad de la información	X					5	

11. La política refleja el compromiso de la alta dirección con la seguridad de la información	X					5	
12. La política incorpora un enfoque basado en riesgos en todas las decisiones y procesos de seguridad		X				4	
13. Se establece un proceso continuo de evaluación y tratamiento de riesgos		X				4	
14. Se establecen procesos para la revisión y actualización regular de la política		X				4	

Escala utilizada para el análisis de la lista de chequeo

Calificación	**Criterio de evaluación**	**Cuantitativa**	**Cualitativa**
Totalmente de acuerdo	Muy bueno (4,1 puntos a 5 puntos)	**4,50**	**TDA**
De acuerdo	Bueno (3,1 puntos a 4 puntos)		
Neutral	Aceptable (2,1 puntos a 3 puntos)		
En desacuerdo	Requiere atención (1,1 puntos a 2 puntos)		
Totalmente en desacuerdo	Crítico 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Armando Puga

ESPECIALIDAD Oficial de Seguridad de la Información

CÉDULA DE IDENTIDAD: 1002279899

Por este medio, hago presente que realicé la revisión de la política de seguridad de la información propuesto para la Cooperativa de Ahorro y Crédito Rural Sierra Norte, elaborado por Ing Esteban Patricio Pillajo Montalvo – Cursando estudio de la Maestría en Computación con mención en Seguridad Informática de la Universidad Técnica del Norte, quién está realizando su tesis **"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TI CON BASE EN LA NORMA ISO/IEC 27001:2022. CASO DE ESTUDIO: COOPERATIVA DE AHORRO Y CRÉDITO RURAL SIERRA NORTE".**

Una vez indicadas las observaciones pertinentes y aclaradas considero que la política de seguridad de la información es **VÁLIDO** para su aplicación e implementación.

Ibarra, 4 días de Septiembre de 2024.

Jorge Armando Puga Placencia

C.I. 1002279899

Anexo V. *Diseño de política de seguridad de la información*

Antecedentes

La Seguridad de la Información ha tomado relevancia ante los nuevos ciberataques que se han desarrollo en el mundo digital, es por eso que las instituciones financieras, bancos, cooperativas, etc., han decidido implementar mejoras en la seguridad de todos los activos informáticos debido a que se tienen datos sensibles de muchas personas.

En la institución actualmente carece de una política de seguridad de la información documentada, aun así, se llevan a cabo algunos procesos para mantener a salvo la información, indicando que cumplen con normativas básicas, pero, esto no garantiza la apropiada seguridad para toda la información que se genera al ser una institución financiera.

Ante la **RESOLUCIÓN No. SEPS-IGS-IGT-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002** de la SEPS (Superintendencia de Economía Popular y Solidaria) donde se menciona la importancia de la implementación de las normas ISO/IEC 27001:2022, mismo que deberá estar aprobado y en proceso de implementación.

El propósito de esta política de alto nivel es definir el objetivo para el área de TI y las reglas básicas para la mejor gestión de la seguridad de la información, dentro de los principios que se van a implementar y contemplar para que se pueda cumplir la Confidencialidad, Integridad y Disponibilidad.

Política de Seguridad de la Información

Descripción de la Política

La máxima autoridad o el Oficial de Seguridad de la Información de la Cooperativa de Ahorro y Crédito Rural Sierra Norte, menciona la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.

Para la COAC Rural Sierra Norte, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

Esta política aplica para el Área de TI, que tiene como objetivo establecer los requisitos para proteger la información, los activos de la institución, mismos que sirven para dar soporte para la mayoría de los procesos que se llevan a cabo en la COAC Rural Sierra Norte, se aplica también a sus funcionarios, abonados, proveedores.

Objetivo

El objetivo principal de la presente Política es definir los principios y reglas básicas para la gestión de la seguridad de la información es **"Proteger, concientizar y mejorar continuamente la seguridad de la información de los activos informáticos que contienen datos personales de los socios que se encuentran en las bases de datos"**, de esta manera se evaluará y se sugerirá, actualizaciones, considerando los aspectos ambientales internos y externos, la disponibilidad de recursos, condiciones contractuales, reguladoras y legales, para la mejora continua de la Seguridad de la Información.

Dentro del área de TI se obtendrá, un progreso dentro de la implementación del Sistema de Gestión de Seguridad de la Información, manteniendo la Confidencialidad, Integridad y Disponibilidad, haciendo que la COAC Rural Sierra Norte alcance mejores niveles de seguridad.

Roles y Responsabilidades

Alta Gerencia o Gerente General de la COAC Rural Sierra Norte tendrá la responsabilidad de conocer las medidas que se van a implementar para gestionar la seguridad de la información en el área de TI.

El **Comité de Seguridad de la Información** (CSI – equipo directivo) serán los responsables de asegurar que la seguridad de la información se gestiona adecuadamente en el área de TI de la COAC Rural Sierra Norte. Al ser una entidad financiera la SEPS

(Superintendencia de Economía Popular y Solidaria) menciona que debe estar conformado por:

- Presidente del Comité de Administración Integral de Riesgos.
- Gerente General o representante legal.
- Oficial de Seguridad de la Información.
- Responsable del Área de Tecnología.
- Delegado de Auditoría Interna.

El **Oficial de Seguridad de la Información**, asesora al equipo directivo, proporcionando apoyo especializado al personal de la institución, garantizando que los informes sobre la situación de la seguridad de la información estén disponibles.

Responsable de Área de Tecnología es el que apoyará y solventará las dudas que puedan existir en el proceso de implementación del SGSI, además de garantizar que los funcionarios que están en su área protejan de forma correcta la información que se va a gestionar dentro del área.

El **Personal del Área de TI** realizan las operaciones de mantenimiento y gestión de servidores deberán mantener en funcionamiento y con los controles necesarios para evitar la divulgación, manipulación de datos una vez finalizada la jornada laboral, con la finalidad de evitar incidentes.

Alcance y usuarios

La Política de Seguridad de la Información, nos brindará un mejor entendimiento sobre los riesgos y oportunidades que se pueden brindar en la COAC Rural Sierra Norte, denotando que se mantiene actualizado la protección de los datos de los abonados, mismo que se deberán definir, aprobar por la gerencia, publicar, comunicar y conocer por todo el personal como las partes interesadas relevantes, además revisadas en intervalos planificados y cuando se den cambios significativos.

Los usuarios que van a tener acceso a la Política de Seguridad de la Información de la COAC Rural Sierra Norte en este caso van a ser:

- Comité de Seguridad de la Información
- Gerente de la COAC Rural Sierra Norte
- Oficial de Seguridad de la Información
- Responsable del Área de Tecnología
- Responsable de los activos de la información
- Socios
- Terceras personas

Comunicación de la Política

Para la comunicación de la política de seguridad de la información se utilizará primero una evaluación sobre el conocimiento previo del personal que trabaja en el área de TI y además, se tendrán capacitaciones a través de medios digitales como Zoom, Microsoft Teams o Google Meet, de esta manera se tendrá en cuenta cómo van a tomar la concientización de todos los datos e información que se manejan dentro de la COAC Rural Sierra Norte, también se coordinará para realizar una capacitación para las demás áreas en las otras agencias y oficinas.

También se podrá visualizar dentro del portal web de la COAC Rural Sierra Norte, la elaboración de material informativo donde se muestren mejor las explicaciones de la seguridad de la información que se aplicará en el área de TI que se puedan comunicar sobre la política que existe dentro la empresa.

Normas de aplicación

Dentro de las normas que se debe contemplar para que la política de Seguridad de la Información se pueda llevar a cabo son:

- Norma para la gestión y clasificación de los activos de la información (se puede utilizar MAGERIT).
- Norma para la gestión de incidentes de seguridad de la información.
- Norma y gestión para el control de acceso, perfiles y roles.

- Norma de control respecto de la seguridad física y electrónica.
- Norma para gestionar el respaldo y recuperación de información.
- Norma para la continuidad del negocio.
- Reglamento interno.

En este punto se pueden incluir normas que la institución considere necesario, con la finalidad de garantizar y preservar la seguridad de la información de los activos.

Excepciones y sanciones

Las sanciones que se pueden tener dentro de la COAC Rural Sierra Norte se deben revisar y actualizar con la implementación de la política de seguridad de la información, de esta manera ante los incumplimientos de los trabajadores en las áreas donde se deberá emitir un llamado de atención y en tal caso que siga sucediendo, se procederá a una sanción como lo menciona el Reglamento Interno de la Institución.

Documentos de referencia

- Superintendencia de Economía Popular y Solidaria (RESOLUCIÓN No. SEPS-IGS-IGT-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002)
- Cooperativa de Ahorro y Crédito Rural Sierra Norte
- Normas ISO/IEC 27001
- Manual de Seguridad Física

- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001

Terminología

Activo de la Información: elemento físico o digital que representa un valor para la empresa.

Comité de Seguridad de la Información (CSI): es el comité que tiene como objetivo garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la empresa.

Confidencialidad: Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Cooperativa de Ahorro y Crédito Rural Sierra Norte: cooperativa que brinda el servicio de ahorro y crédito a todos los usuarios que tengan necesidades financieras.

Disponibilidad: Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad no autorizada.

Incidente de Seguridad de la Información: ocurrencia de eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.

Integridad: Propiedad de proteger la precisión y completitud de los activos.

Oficial de Seguridad de la Información (OSI): Es el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimento del SGSI.

Historial de cambios

Versión	Fecha	Detalle de la modificación
1.0	15/05/2024	Modificación del documento
1.1	30/05/2024	Actualización de documento
1.2	20/06/2024	Implementación de correcciones
1.3	25/07/2024	Actualización de documento
1.4	07/08/2024	Revisión de documento
1.5	08/08/2024	Actualización de documento
1.6	18/08/2024	Revisión de documento
1.7	19/08/2024	Actualización de documento