UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)"

Trabajo de titulación previo a la obtención del título en Magister en Computación con Mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR:

Jefferson Esteban Andrade Pijuango

DIRECTOR:

Marco David Revelo Aldás PhD (C)

Ibarra – Ecuador 2026

AGRADECIMIENTO

Agradezco a Dios por haberme dado la oportunidad de culminar esta importante etapa en mi vida profesional, también a mi familia, profesores y directores por su apoyo en el desarrollo de mi trabajo de titulación.

DEDICATORIA

Quiero dedicar este trabajo de titulación a mi familia, quienes han sido los pilares fundamentales que me han inspirado en la búsqueda de nuevos propósitos y retos profesionales.

Ibarra, 06 de mayo de2026

Dr. Jorge Gordón
Decano (e)
Facultad de Posgrado

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)" del maestrante Jefferson Esteban Andrade Pijuango, de la Maestría en Computación mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director	Revelo Aldás Marco PhD (C)	Validar únicamente en FirmaEC. Firmado electrónicamente por: MARCO DAVID REVELO ALDAS
Asesor	Msc. Rea Peñafiel Mauricio	Validar únicamente en FirmaEC. Firmado electrónicamente por: XAVIER MAURICIO REA PENAFIEL

UNIVERSIDAD TÉCNICA DEL NORTE

DIRECCIÓN DE BIBLIOTECA

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	
APELLIDOS Y NOMBRES:	Andrade Pijuango Jefferson Esteban

DATOS DE LA OBRA	
TÍTULO:	Implementación de una metodología para la evaluación de controles de seguridad de la información alineada con la normativa 2022-002 de la Superintendencia de Economía Popular y Solidaria (SEPS)
AUTOR (ES):	Andrade Pijuango Jefferson Esteban
FECHA: DD/MM/AAAA	28/05/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en Computación con Mención en Seguridad Informática
DIRECTOR /ASESOR:	Revelo Aldás Marco David PhD (C) Msc. Rea Peñafiel Xavier Mauricio

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 28 días del mes de mayo de 2026

EL AUTOR:

JEFFERSON ESTEBAN ANDRADE PIJUANGO

Firmado digitalmente por JEFFERSON ESTEBAN ANDRADE PIJUANGO
Fecha: 2026.05.28 08:53:09 -05'00'

Nombre: Andrade Pijuango Jefferson Esteban

ÍNDICE DE CONTENIDOS

RESUMEN 9
ABSTRACT 10
CAPÍTULO I 11
1. EL PROBLEMA 11
1.1. Planteamiento del problema 11
1.2. Formulación del problema 13
1.3. Interrogantes de la investigación 13
1.4. Objetivos de la investigación 13
1.4.1. Objetivo general 13
1.4.2. Objetivos específicos 14
1.5. Hipótesis de trabajo 14
1.6. Hipótesis alternativa 14
1.7. Categorización de variables 14
1.8. Justificación 15
CAPÍTULO II 17
2. MARCO REFERENCIAL 17
2.1. Antecedentes 17
2.2. Marco Teórico 21
2.2.1. Seguridad de la Información 21
2.2.3. Evaluación de la Seguridad de la Información 24
2.2.4. Marcos de evaluación de Seguridad de la Información 24
2.3. Marco Legal 30
CAPÍTULO III 31
3. MARCO METODOLÓGICO 31
3.1. Descripción del área de estudio 31
3.2. Enfoque y tipo de investigación 31
3.3. Procedimiento de investigación 32
3.4. Consideraciones bioéticas 33
4. RESULTADOS 34
4.1. Revisión documental y normativa 34
4.1.1. Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 34

4.1.2. Revisión a la NORMA ISO/IEC 27001 37
4.1.3. Revisión a la NORMA ISO/IEC 27004 39
4.1.4. Revisión del estándar NIST 800-53A 42
4.2. Desarrollo de la metodología 44
4.2.1. Introducción 45
4.2.2. Antecedentes 45
4.2.3. Objetivo General 46
4.2.4. Objetivos Específicos 46
4.2.5. Alcance 46
4.2.6. Participación de las partes interesadas 47
4.2.7. Características generales de la medición 48
4.2.8. Tipos de medidas 51
4.2.9. Proceso de medición 54
4.3. Validación e implementación 77
4.3.1. Contexto del plan piloto 77
4.3.2. Etapa 1: Planificación de la Evaluación 77
4.3.3. Etapa 2: Definición del procedimiento de medición 83
4.3.4. Etapa 3: Monitorear y medir 83
4.3.5. Etapa 4: Análisis de resultados 83
4.3.6. Etapa 5: Clasificación de efectividad de los controles 84
4.3.7. Etapa 6: Revisar y mejorar 84
4.3.8. Etapa 7: Retener y comunicar información 85
5. CONCLUSIONES Y RECOMENDACIONES 88
5.1. Conclusiones 88
5.2. Recomendaciones 89
REFERENCIAS 90
ANEXOS 94
Anexo A. Solicitud para realizar tesis de grado 94
Anexo B. Formularios de recopilación y análisis de información del plan piloto. 95
Anexo C. Constancia de validación de expertos 103

ÍNDICE DE TABLAS

Tabla 1. Cuadro comparativo Antecedentes 20
Tabla 2. Comparación de normas, guías metodológicas 29
Tabla 3. Clasificación de controles (SEPS 2022-002) 36
Tabla 4. Revisión a la NORMA ISO/IEC 27001 37
Tabla 5. Revisión a la NORMA ISO/IEC 27004 39
Tabla 6. Revisión del estándar NIST 800-53A 42
Tabla 7. Necesidad de información 55
Tabla 8. Métodos de evaluación 58
Tabla 9. Definición de la medida 58
Tabla 10. Ejemplo - Definición de la medida 60
Tabla 11. Priorización de implementación 61
Tabla 12. Ejemplo - Priorización de implementación 61
Tabla 13. Herramientas de soporte 65
Tabla 14. Ejemplo - Formulario de recopilación y análisis de información 65
Tabla 15. Validación de datos 70
Tabla 16. Evaluación de los criterios 71
Tabla 17. Ejemplo - Consolidación de resultados y análisis 72
Tabla 18. Análisis de causas 72
Tabla 19. Niveles de clasificación de controles 73
Tabla 20. Matriz de decisión 74
Tabla 21. Ejemplo - Clasificación de controles 74
Tabla 22. Ejemplo - Clasificación de controles 75
Tabla 23. Plan Piloto - Definición de medida MED-SI-001 78
Tabla 24. Plan Piloto - Definición de medida MED-SI-002 79
Tabla 25. Plan Piloto - Definición de medida MED-SI-004 80
Tabla 26. Plan Piloto - Priorización de implementación 82
Tabla 30. Plan Piloto - Análisis de resultados 83
Tabla 31. Plan Piloto - Análisis de Causas 83
Tabla 32. Plan Piloto - Clasificación de efectividad de los controles 84
Tabla 33. Plan Piloto - Retención y comunicación de información 85

ÍNDICE DE FIGURAS

Figura 1. Verificación IEEE Explore 17
Figura 2. Proceso de evaluación NIST SP 800-53A 26
Figura 4. Avance de una medida de desempeño 52
Figura 5. Medida de desempeño resultante 52
Figura 6. Medida de eficacia en la gestión de vulnerabilidades 53
Figura 7. Medida de eficacia para exposición del riesgo 54
Figura 8. Diagrama de flujo del proceso de medición 54
Figura 9. Plan Piloto - Repositorio de Medición y Evidencias 86

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)

Autor: Andrade Pijuango Jefferson Esteban

Tutor: Revelo Aldás Marco PhD (C)

Año: 2026

RESUMEN

El presente estudio se enfoca en la evaluación de controles de seguridad y mejora en la gestión de riesgos del Sistemas de Gestión de Seguridad de la Información (SGSI), especialmente en las instituciones reguladas por la Superintendencia de Economía Popular y Solidaria (SEPS). Para lo cual se ha desarrollado una metodología basada en estándares como ISO/IEC 27001, ISO/IEC 27004, NIST SP 800-53A y COBIT 2019.

El objetivo principal de este estudio es implementar esta metodología para evaluar controles y fortalecer el cumplimiento normativo.

Para lo cual la implementación se estructuró en tres fases, en primer lugar, se realizó un análisis de estándares reconocidos y el marco regulatorio, en segundo lugar, se diseñó la metodología e instrumentos de evaluación considerando el análisis previo y finalmente, se implementó la propuesta metodológica mediante un plan piloto en una cooperativa de ahorro y crédito.

Los resultados obtenidos de tres medidas y validados por el responsable de Seguridad de la Información de la cooperativa, demuestran que la metodología permite medir el desempeño y la efectividad de los controles a través de indicadores basados en evidencia, demostrando su alineación con la normativa vigente y su aplicabilidad en el contexto del Sector Financiero Popular y Solidario.

Palabra clave: Evaluación de controles de seguridad, medición del SGSI.

ABSTRACT

This study focuses on the evaluation of security controls and the improvement of risk management within the Information Security Management System (ISMS), particularly in institutions regulated by the Superintendence of Popular and Solidarity Economy (SEPS). To this end, a methodology has been developed based on recognized standards such as ISO/IEC 27001, ISO/IEC 27004, NIST SP 800-53A, and COBIT 2019.

The implementation on the methodology was structured in three phases. First, an analysis of recognized standards and the regulatory framework was carried out. Second, the methodology and evaluation instruments were designed based on this analysis. Finally, the methodology was implemented through a pilot plan in a financial institution.

The results from three measurements, validated by the Security Officer of the evaluated entity, demonstrate that the methodology allows measuring the performance and effectiveness of controls thru evidence-based indicators, showing its alignment with current regulations and its applicability in the context of the Popular and Solidarity Financial Sector.

Keywords: Assessing Security Controls, ISMS Measurement.

CAPÍTULO I

1. EL PROBLEMA

1.1. Planteamiento del problema

Las entidades del Sector Financiero Popular y Solidario (SFPS) reguladas por la Superintendencia de Economía Popular y Solidaria (SEPS), registran un papel fundamental en la inclusión financiera del país. Según datos de TI AHORA (2021), hasta junio de 2021 este sector contaba con aproximadamente 3812 puntos de atención a nivel nacional, abarcando al menos el 62% de la población económicamente activa, asimismo el Instituto Nacional de Estadística y Censos (INEC) señala que el 55.3% de la población ecuatoriana mantiene relación con estas entidades, lo que evidencia su importancia en la economía y desarrollo social.

Sin embargo, el crecimiento del SFPS y la transformación digital ha incrementado la complejidad de los entornos tecnológicos, exponiendo a las organizaciones a nuevas amenazas que pueden comprometer la seguridad de la información (Hernández, 2022), en consecuencia, las entidades del sector deben diseñar planes de mitigación ante desastres impulsar iniciativas para proteger la integridad, confidencialidad y disponibilidad de la información.

En este escenario, el sector financiero en general se encuentra expuesto a amenazas; como la filtración de datos, ataques de malware, phishing, denegación de servicios (DoS), suplantación de identidad; además, se identifican vulnerabilidades críticas relacionadas con la insuficiencia de respaldos, fallas en las configuraciones en equipos de seguridad y ausencia de auditorías de seguridad de la información (Okoye, 2024). Estos hallazgos ponen en evidencia una brecha significativa en el nivel de preparación de controles, así como debilidades en la capacidad del personal para enfrentar incidentes de seguridad.

Lee et al. (2023) señalan que, pese a esfuerzos realizados por las organizaciones, persiste la ausencia de métricas de evaluación sistemáticas adaptadas para medir la resiliencia frente a ataques de seguridad, describen marcos estructurados con aspectos clave para evaluarla e implementarla, sin embargo, se centran en aspectos técnicos, lo que dificulta evaluar efectivamente dimensiones a las que se encuentran diversas organizaciones.

De la misma forma Marican et al. (2023) evidencia la ausencia de marcos integrales de evaluación de madurez en ciberseguridad para organizaciones relativamente jóvenes que sustentan sus servicios en fuentes tecnológicas, destacando de la misma forma la dificultad para justificar adecuadamente las inversiones necesarias para mitigar riesgos cibernéticos en constante evolución. En este sentido resulta fundamental que las entidades fortalezcan sus capacidades de obtener información orientada al desempeño de su seguridad y la toma de decisiones sustentada en evidencias.

En el ámbito regulatorio, la SEPS a través de la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 realizada en el 2022, define los niveles mínimos requeridos para la gestión de seguridad de la información que las entidades del sector deben definir e implementar para resguardar la información institucional. No obstante, Cadena (2025) señala una brecha en la literatura sobre como la seguridad de la información incide en la eficiencia operativa, asimismo Ramírez (2025), en un estudio sobre entidades del mismo sector, reporta que el 64% de responsables de la seguridad considera sus controles eficaces, evidenciando evaluaciones subjetivas de efectividad, limitando decisiones basadas en evidencia sólida.

El estudio “Estado Actual de la Ciberseguridad” de IT Ahora y Deloitte (2024) evidencia en el sector privado, una disminución de prácticas de evaluación de madurez respecto a 2023, reflejando debilidades en la gestión de riesgos y en la medición de controles. En cuanto a inversión en ciberseguridad, el 64% de las instituciones a nivel global se basan en la evaluación de madurez del SGSI, frente al 19% en el SFPS.

Adicionalmente, el estudio de IT Ahora y Deloitte (2024) mediante encuestas aplicadas a diversas instituciones evaluando capacidades organizacionales y gestión de riesgos, entre los principales hallazgos destaca la falta de capacitación interna y de talento especializado, sin embargo, se evidencia un mayor interés estratégico por parte de las juntas directivas. A pesar de ello los niveles de madurez en ciberseguridad en el país se mantiene por debajo del promedio global, evidenciando brechas asociadas al uso limitado de herramientas, deficiencias en la gestión de riesgos y el incumplimiento normativo (IT Ahora, 2025).

En conjunto, estos elementos evidencian la necesidad de fortalecer los mecanismos de evaluación de los controles de seguridad, orientándolos hacia enfoques medibles y alineados con la normativa vigente.

1.2. Formulación del problema

La brecha existente entre la gestión de riesgos, la implementación de controles de seguridad de la información y la capacidad institucional para evaluar su efectividad y elevar la madurez de gestión de ciberseguridad, originada por la falta de instrumentos alineados con la normativa SEPS 2022-002, limita la identificación oportuna de vulnerabilidades y debilita la toma de decisiones basada en evidencia.

1.3. Interrogantes de la investigación

En este sentido, la presente investigación se formula a partir de las siguientes preguntas:

¿Cuáles son los requisitos y lineamientos establecidos en la normativa 2022-002 de la Superintendencia de Economía Popular y Solidaria (SEPS) y qué debe considerarse para la evaluación de los controles de Seguridad de la Información en las instituciones del sector financiero popular y solidario?

¿Cómo diseñar una metodología de evaluación que permita medir de manera objetiva la efectividad de los controles de Seguridad de la Información, en concordancia con los criterios definidos en la norma 2022-002 de la SEPS?

¿En qué medida la metodología propuesta resulta aplicable y efectiva al ser implementada mediante un caso de estudio o prueba piloto en una institución del sector económico popular y solidario?

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Implementar una metodología integral para la evaluación de controles de seguridad de la información, que permita fortalecer la gestión de riesgos y asegurar el cumplimiento normativo en las instituciones del sector de la economía popular y solidaria bajo la normativa 2022-002 de la SEPS.

1.4.2. Objetivos específicos

Analizar la normativa 2022-002 de la SEPS para identificar los requisitos y lineamientos específicos aplicables a la evaluación de controles de Seguridad de la Información en las instituciones del sector económico popular y solidario.

Diseñar una metodología de evaluación detallada que permita medir la efectividad y el nivel de cumplimiento de los controles de Seguridad de la Información basada en los criterios establecidos en la normativa vigente 2022-002 de la SEPS.

Validar la aplicabilidad y efectividad de la metodología propuesta, mediante su implementación en un caso de estudio o prueba piloto en una institución del sector de la economía popular y solidaria.

1.5. Hipótesis de trabajo

Al implementar una metodología integral para la evaluación de controles de seguridad de la información, se fortalecerá la gestión de riesgos y se asegurará el cumplimiento normativo en las instituciones del sector de la economía popular y solidaria bajo la normativa 2022-002 de la SEPS.

1.6. Hipótesis alternativa

La no implementación de una metodología integral para la evaluación de controles de seguridad de la información, debilitará la seguridad y el cumplimiento normativo en las instituciones del sector de la economía popular y solidaria bajo la normativa 2022-002 de la SEPS.

1.7. Categorización de variables

Las variables que se derivan de la hipótesis planteada son:

Variable independiente: Metodología integral para la evaluación de controles de seguridad de la información.

Variable dependiente: Gestión de riesgos y cumplimiento normativo en las instituciones del sector de la economía popular y solidaria bajo la normativa 2022-002 de la SEPS.

1.8. Justificación

La SEPS, mediante la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 (SEPS 2022-002), establece los lineamientos para la gestión de la seguridad de la información aplicables a las entidades del SFPS. Esta normativa define los niveles mínimos que deben implementarse para resguardar y proteger la información institucional, garantizando su confidencialidad, integridad y disponibilidad.

En este marco, las instituciones reguladas están obligadas a implementar todo lo relacionado con un SGSI, que contemple un esquema de gobierno, responsabilidades, la adopción de medidas, mecanismos de protección y la ejecución de evaluaciones periódicas orientadas a determinar su efectividad y grado de cumplimiento.

Entre los controles mínimos exigidos se incluyen, definición de políticas, de procesos y procedimientos, asignación de roles y responsabilidades, la realización de auditorías informáticas y pruebas de penetración, gestión de riesgos, evaluación de controles, implementación de planes de contingencia y continuidad del negocio, cifrado de la información, gestión de accesos, configuraciones y cambios, así como, el monitoreo y la detección de eventos de seguridad, entre otros.

Adicionalmente, la normativa establece que la gestión de riesgos debe contemplar la clasificación de activos, descripción y determinación del riesgo, la implementación de los controles, la evaluación de efectividad de los controles y el tratamiento de riesgo, considerando criterios alineados con estándares como la ISO/IEC 27000.

A partir del año 2022, la normativa entre en vigencia, por lo tanto, la SEPS realiza auditorias de control para determinar el cumplimiento, emitir observaciones o recomendaciones y en el caso de no cumplir pueden estar sujetas a sanciones.

Pase a la existencia de este marco regulatorio, diversas entidades del sector presentan limitaciones en la implementación y, principalmente, en la evaluación de los controles de seguridad para la gestión adecuada de riesgos. Estas deficiencias se asocian, en gran medida, a la ausencia de metodologías estructuradas que permitan medir de manera objetiva la efectividad y cumplimiento de los controles (Revista IT, 2024). De esta manera la identificación oportuna de vulnerabilidades se ve debilitada y se

incrementa la exposición a incidentes de seguridad, lo que pondría en riesgo la continuidad operativa, la confianza de los socios y la protección de los datos personales, tal como se establece también en la Ley Orgánica de Protección de Datos Personales (2021).

Frente a esta situación, se justifica la necesidad de desarrollar una metodología alineada a la normativa vigente, que permita evaluar el nivel de cumplimiento y la efectividad de los controles de seguridad en las organizaciones del SFPS. Esta propuesta se basa en un enfoque estructurado para identificar brechas, que acciones de mejora deben realizarse y como se puede fortalecer la gobernanza de la seguridad de la información, todo bajo un enfoque basado en la gestión de riesgos.

Impacto Técnico

La implementación de esta propuesta tendrá un impacto técnico al optimizar la protección de los activos de información, al contribuir con el cumplimiento normativo y la adecuada gestión de riesgos.

Impacto Institucional

Asimismo, su carácter replicable y escalable permitirá su aplicación en otras entidades del sector financiero, lo que contribuye a elevar el nivel de madurez de la seguridad de la información a escala nacional.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1. Antecedentes

Con el propósito de determinar los estudios relacionados con la presente propuesta metodológica, se llevó a cabo una revisión de la literatura preliminar orientada a identificar trabajos o publicaciones relacionados con la evaluación de los controles de seguridad de la información. Para ello, se planteó una estrategia de búsqueda en la siguiente interrogante de investigación:

¿Cómo medir la efectividad de los controles de seguridad implementados?

Para obtener artículos relacionados a esta interrogante, se estableció la siguiente cadena de búsqueda ((("All Metadata":methodology for the evaluation) AND ("All Metadata":information security controls))), la cual fue ejecutada en la base de datos IEEE Xplore (IEEEX), obteniendo como resultado un total de 70 publicaciones entre revistas y conferencias como se muestra en la Figura 1. A partir de este conjunto inicial, se seleccionaron los estudios más relevantes en función de su aporte metodológico y pertinencia.

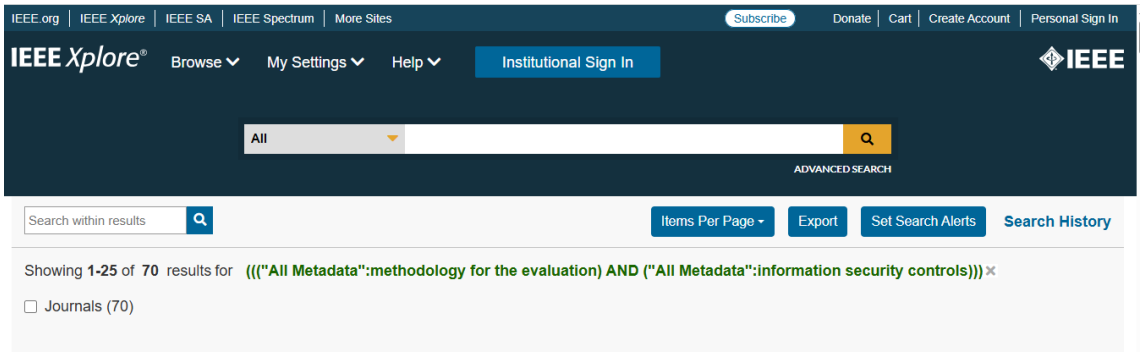


Figura 1. Verificación IEEE Explore

Fuente: Propia

Los resultados evidencian diversas aproximaciones a la evaluación de controles de seguridad.

Jung et al. (2023) destacan el incremento de ciberataques en sistemas de control industrial, así como también la importancia de la aplicación de controles de ciberseguridad y la evaluación de la seguridad contra distintas amenazas, ya que estos

ataques en el sector industrial pueden causar pérdidas económicas, como humanas. Por tanto, la aplicación de controles de seguridad y evaluación rutinaria de la operación correcta, es indispensable para mitigar estas amenazas, sin embargo, se considera que los recursos en ciberseguridad son limitados.

Para superar dichas limitaciones Jung et al. (2023) mencionan la necesidad de identificar los controles de seguridad más eficaces para optimizar la asignación de recursos. En este contexto, realizan un análisis comparativo de los resultados obtenidos al aplicar y evaluar controles de seguridad, permitiendo establecer criterios más precisos y sustentados.

Por su parte, Ko et al. (2025) desarrollan un marco metodológico basado en indicadores clave de desempeño (KPI) para evaluar la ciberresiliencia en sistemas marítimos. Para el logro de su estudio analizan marcos como UR E26, NIST CSF y MITRE CREF, dando como resultado siete dominios de evaluación: Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar y Adaptar, así como el diseño de 18 KPI medibles utilizando metodologías SMART, abarcando aspectos técnicos, de gestión y operativos de buques.

En el trabajo de estudio de Marican et al. (2023) se menciona la falta de un marco integral para evaluar la madurez en ciberseguridad en empresas tecnológicas que prestan servicios a grandes organizaciones gubernamentales y financieras. Basándose en 24 artículos, concluye que estos pequeños proveedores tecnológicos se encuentran en una situación vulnerable, ya que sus directivos no disponen de información confiable sobre su nivel de madurez en ciberseguridad, por lo que limita tomar decisiones ligadas a evaluaciones y dificulta justificar sus inversiones en seguridad para la gestión adecuada del riesgo.

Así mismo Marican et al. (2023) consideran que los marcos existentes de evaluación utilizados por los profesionales no son adecuados para implementaciones de forma ágil y eficiente en empresas relativamente pequeñas.

Por su parte Hadi et al. (2024) proporcionan instrumentos y conocimiento necesarios para gestionar eficazmente las complejidades de la ciberseguridad, así como de un sistema de puntuación y ponderación para evaluar herramientas de ciberseguridad

de código abierto en seis capas de defensa, el resultado revela que al proporcionar un marco claro para seleccionar los mecanismos y controles más adecuados no solo facilita la toma de decisiones rápida, sino que también ayuda a las partes interesadas a comprender las fortalezas y debilidades relacionadas con la seguridad de la información.

De acuerdo a Moreira et al. (2021), las organizaciones enfrentan ciberataques con una frecuencia de 39 segundos, demostrando la necesidad de implementar controles de seguridad eficaces y fortalecer procesos de análisis de riesgos, si bien los marcos como NIST proporcionan lineamientos para gestión de la seguridad, estos no indican con claridad como iniciar el plan de gestión de controles, para ello desarrollan un caso de estudio basado en el método Decisión Multicriterio Constructivista (MCDM-C) sobre los controles de detección de incidentes NIST en una institución financiera, en consecuencia el estudio demuestra la eficacia de cada control para mitigar riesgos, considerando el contexto organizacional, facilitando la elaboración de planes de riesgos basados en los datos obtenidos.

El estudio realizado por Zhuo y Jin (2025) se centra en el sector sanitario, donde la seguridad de la información desempeña un papel fundamental en el desarrollo económico, social y tecnológico, para ello resulta esencial garantizar la solidez y fiabilidad de los sistemas, de tal manera se establece un caso de estudio para evaluar y clasificar diversas políticas de seguridad de la información hospitalaria mediante técnicas de Toma de Decisiones Multicriterio (MCDM). Este enfoque identifica múltiples factores relevantes que influyen en la eficacia de los controles de seguridad, así como proponer recomendaciones de mejora. Los resultados obtenidos evidencian que el modelo propuesto proporciona una evaluación precisa y fiable, fortaleciendo los procedimientos.

Por otro lado, estudios como el de Kudriavtseva (2024) se centran en la seguridad de los sistemas de software, en este caso se propone un marco de evaluación orientado a identificar vulnerabilidades desde las primeras etapas del ciclo de desarrollo, con el fin de facilitar la corrección posterior. No obstante, garantizar que el software se mantenga seguro resulta complejo debido a la naturaleza multidimensional de seguridad. Frente a este desafío, se propone un marco de evaluación que integra métricas de seguridad con los modelos mentales de expertos en desarrollo seguro, incorporando un factor humano en el proceso de evaluación.

Conclusión de la revisión de literatura

Tabla 1. Cuadro comparativo Antecedentes

Articulo No.	Autor/es	Enfoque	Método de evaluación	Resultados	Limitaciones
1	Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T. (2023).	Evaluación de controles en centrales nucleares.	Proceso de ingeniería de ciberseguridad industrial TAM (Technical Assessment Methodology)	Identifica controles efectivos	Demanda alto conocimiento técnico
2	Ko, A., Lee, J. H., & Seo, J. T. (2025).	Evaluación de ciberresiliencia de buques marítimos	Framework basado en indicadores KPI y SMART	Mejora gestión de ciberresilien cia	Dependencia de la formulación de KPI
3	Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023)	Madurez de ciberseguridad en startups	Revisión sistémica de la literatura SLR	Justifica falta de frameworks completos	No desarrolla framework
4	Hadi, H. J., Ahmad, N., Aziz, K., Cao, Y., & Alshara, M. A. (2024).	Defensa multinivel con herramientas open-source	Defensa multinivel por capas de herramientas de ciberseguridad	Modelo de defensa escalable	Demanda conocimiento técnico e integración de las herramientas
5	Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., De Sousa Júnior, R. T., & Nunes, R. R. (2021).	Evaluación de controles NIST	Método multicriterio constructivista MCDA-C	Fortalece la toma de decisiones	Dependencia de criterios de expertos

6	Zhuo, P., & Jin, L. (2025)	Evaluación de controles de seguridad hospitalaria	Conjunto difuso de imágenes de disco D-PFS y Evaluación del Producto de Suma Agregada Ponderada WASPAS	Aumenta la precisión 18.5 % y reduce ambigüedad un 30%	Complejidad matemática y del enfoque hospitalario
7	Kudriavtseva, A. (2024)	Evaluación de seguridad de software	Framework basado en métricas y modelos mentales	Evaluación realista que incluye percepción de expertos de seguridad	La percepción puede generar imprecisiones

Fuente: Elaboración propia

2.2. Marco Teórico

2.2.1. Seguridad de la Información

Constituye un pilar fundamental en la gestión de la información en las organizaciones, ya que demanda de estrategias, medidas y controles diseñados e implementados para proteger los activos de información contra amenazas crecientes de carácter interno o externo (Pérez Rodríguez, 2025). Este concepto se basa en los principios de confidencialidad, integridad y disponibilidad (CIA).

La confidencialidad garantiza que la información sea accesible únicamente a personas autorizadas, la integridad asegura su exactitud y completitud, y la disponibilidad permite que los usuarios autorizados accedan a la información y a los activos relacionados cuando lo requieran.

En la actualidad, debido a la digitalización las organizaciones se ven obligadas a adoptar políticas de seguridad de la información alineadas con normativas como ISO/IEC 27001, a fin de establecer un marco para mitigar riesgos y asegurar la continuidad organizacional (Folorunso et al., 2024). No obstante, como se evidencia en los antecedentes de la investigación, uno de los principales desafíos es ampliar la capacidad para evaluar la eficacia real de los controles y medidas implementadas.

Seguridad Informática

La seguridad informática comprende el conjunto de medidas técnicas destinadas a impedir operaciones no autorizadas sobre un sistema o red informática, para salvaguardar la información, así como la confidencialidad, autenticidad e integridad. Así mismo busca fortalecer la operatividad de los sistemas y bloquear accesos no autorizados. (Cortez, 2024)

Los objetivos de seguridad informática según Cortez (2024) son:

- Garantizar la adecuada utilización de los recursos y aplicaciones del sistema.
- Limitar pérdidas y lograr una rápida recuperación del sistema en casos emergentes
- Gestionar y detectar los riesgos y posibles amenazas
- Cumplir con el marco legal y los requisitos regulatorios.

2.2.2. Sistemas de Gestión de Seguridad de la Información (SGSI)

Es un enfoque estructurado y continuo de políticas, procedimientos, recursos y actividades para proteger los activos de información de una organización frente a diversas amenazas (Pérez Rodríguez, 2025), además de proporcionar un marco de gestión, el SGSI fomenta una cultura organizacional enfocada a la seguridad, asegurando que la organización esté preparada para amenazas emergentes, mantener la confianza y cumplir obligaciones legales y regulatorias.

El ciclo de vida del SGSI se estructura en torno al modelo PDCA (Plan, Do, Check, Act), una metodología que fomenta la mejora continua en la gestión.

- **Planificar:** Definir políticas, objetivos y procesos.
- **Hacer:** Implementar controles y procedimientos.
- **Verificar:** Monitorear y evaluar el desempeño del SGSI.
- **Actuar:** Ejecutar acciones correctivas y de mejora continua.

Gestión del riesgo

Considerando que el riesgo se define como la posibilidad de que una amenaza explote una vulnerabilidad y genere pérdidas o daños en un activo de información, la

gestión de riesgo comprende el conjunto de actividades coordinadas orientadas para dirigir y controlar la organización frente a dichos riesgos. Su propósito esencial es establecer controles e indicadores que permitan gestionar adecuadamente los riesgos, contribuyendo a garantizar aspectos que permitan preservar los activos de información (Zevallos, M. 2019).

Activo de información

Un activo de información es cualquier recurso tangible o intangible que posee valor para una organización y que necesita ser protegido, un activo puede incluir desde datos confidenciales, documentos estratégicos y sistemas de información hasta el conocimiento de las personas (Pérez Rodríguez, 2025).

Controles de Seguridad de la Información

Los controles son medidas que reducen un riesgo, pueden ser de tipo técnico o administrativo para atacar las pérdidas y reducción de disponibilidad producidas por una amenaza (Cortés, 2022).

De acuerdo a la norma ISO/IEC 27001:2022 los controles se clasifican en:

- Controles organizativos
- Controles de personas
- Controles físicos
- Controles tecnológicos

Evaluación de controles de seguridad

La evaluación de controles de seguridad es un proceso sistemático que permite determinar si los controles están diseñados, implementados y operando de manera efectiva.

Por su parte la guía NIST SP 800-115 indica que la evaluación implica el uso de técnicas como pruebas técnicas, revisión de documentos y entrevistas. Este enfoque resalta que la evaluación debe sustentarse en evidencia verificable y en la observación directa de cómo funcionan realmente los controles de seguridad. Además, la NIST SP 800-53A Rev. 5 proporciona un enfoque estructurado de métodos para examinar, entrevistar responsables y probar los controles, permitiendo validar su eficacia.

Una evaluación efectiva no se limita a verificar la existencia de los controles, sino que debe considerar su desempeño, la evidencia de su aplicación y su alineación con los requisitos normativos (Calder y Watkins, 2019).

2.2.3. Evaluación de la Seguridad de la Información

La medición del desempeño de la seguridad de la información es un elemento esencial del SGSI, de acuerdo a la ISO/IEC 27001:2022 en su cláusula 9 denominada Evaluación del desempeño, las organizaciones deben realizar actividades de monitoreo, medición, análisis y evaluación con el fin de determinar la eficacia de sus controles de seguridad.

La medición debe contemplar los siguientes aspectos:

- Definición de métodos para el seguimiento, medición, análisis y evaluación
- Ejecución de métodos validados para obtener resultados comparables y reproducibles
- Determinación de los periodos de medición
- Asignación de responsables de supervisar y medir
- Cuando se analizará y evaluará los resultados de la medición
- El establecimiento de criterios claros para el análisis de dichos resultados

Toda la información recopilada en el proceso debe ser almacenada y disponible como prueba de los resultados.

2.2.4. Marcos de evaluación de Seguridad de la Información

Existen diversos marcos de evaluación, entre los analizados en el presente estudio se encuentran NIST SP 800-53A, ISO/IEC 27004:2016 y COBIT 2019.

ISO/IEC 27004: Medición de la seguridad de la información

La ISO/IEC 27004:2016 ofrece directrices para supervisar, medir, analizar y evaluar la gestión de la seguridad de la información, con el objetivo de facilitar a las empresas a verificar la efectividad del SGCI y el cumplimiento de la norma ISO/IEC 27001. Beneficia a las organizaciones a realizar una rendición de cuentas transparente y una mejor toma de decisiones basada en datos cuantitativos.

El proceso de medición de la norma se compone de cinco características clave:

1. **Enfoque en la Necesidad de Información**

La norma indica que intentar medir demasiados atributos o los irrelevantes es demasiado complicado, costoso y contraproducente, por ello inicialmente la organización debe determinar qué desea lograr con la evaluación para identificar las necesidades de información, ya que a posterior las medidas van a ir ligadas a estas necesidades para evitar información innecesaria.

2. **Qué Supervisar vs Qué Medir**

La supervisión se centra en determinar el estado de un sistema, proceso o actividad como la gestión de incidentes, vulnerabilidades, registros de acceso (firewall), concienciación del personal, entre otros. Estas actividades proporcionan datos estadísticos y sustentan otras medidas. Por su parte la medición es la actividad para determinar un valor, o tendencia en el rendimiento o la eficacia. Determinando áreas de mejora que se pueden aplicar a procesos del SGSO como liderazgo, planificación, auditoría y a los controles.

3. **Temporalidad y Validez de los Resultados**

Todos los resultados deben ser validados, para lo cual implica que sean comparables y reproducibles.

4. **Roles y Responsabilidades**

Según el tamaño de la organización se pueden definir los siguientes roles:

- **Cliente de medición:** dirección que solicita la información (necesidad de información)
- **Planificador:** vincula atributos medibles con la necesidad de la información
- **Titular de la información:** Propietario de los datos
- **Analista y comunicador:** Procesa los datos y comunica resultados

5. Tipos de Medidas

La norma clasifica las medidas en dos tipos:

- **Medidas de rendimiento**: expresan resultados en términos de cumplimiento de actividades planificadas, como el porcentaje de portátiles con cifrado o asistencia a reuniones.
- **Medidas de eficacia**: expresan el efecto de las actividades sobre objetivos de seguridad, como el ahorro de costos por reducción de incidentes o grado de confianza del cliente.

El proceso de medición es por etapas, iniciando con la identificación de necesidades de información, creación de medidas, establecimiento de procedimientos para la medición, supervisión, análisis y evaluación para reiniciar el ciclo con la mejora continua.

NIST SP 800-53A: Evaluación de controles de seguridad

La publicación NIST SP 800-53A (2022) propone un marco de evaluación flexible y repetible diseñado para determinar la efectividad de los controles de seguridad y privacidad en los sistemas organizacionales, este método no solo se limita a una simple lista de verificación, sino que se integra en todo el ciclo de vida del desarrollo del sistema.

El objetivo principal es compilar evidencias para demostrar que los controles están correctamente aplicados, funcionan como se espera y producen los resultados deseados, cada procedimiento de evaluación incluye objetos, métodos y objetivos específicos, cada método puede ser ajustado por su rigor y alcance permitiendo establecer el nivel de esfuerzo previamente.

El proceso consta de cuatro pasos fundamentales:



Figura 2. Proceso de evaluación NIST SP 800-53A

Fuente: NIST SP 800-53A

- Preparación: Identificación de objetos, alcance, recursos y selección de evaluaciones.
- Desarrollo del plan: Selección de controles a evaluar, procedimientos, adaptación, optimización de los procedimientos y definición de parámetros (ODP)
- Realización de evaluaciones: Ejecución de los métodos definidos de evaluación y recopilación de hallazgos como satisfechos o no satisfechos, así como también el análisis de causa raíz.
- Análisis de resultados: Los responsables analizan los informes de evaluación y la documentación necesaria para determinar los pasos apropiados para responder a las debilidades.

COBIT: Gobierno y Gestión de TI

Cobit 2019 es una guía de mejores prácticas y un marco de trabajo para el gobierno de la información y la tecnología, el cual abarca una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, marco de trabajo, objetos de control, mapas de auditoría, instrumentos de implementación, evaluación y una guía técnica de gestión. (Torres H., 2021)

Este marco definido por ISACA (2018) principalmente se fundamenta en diferenciar entre gobierno y gestión, donde el gobierno es responsabilidad de la alta dirección representada por la junta directiva, y se enfoca en evaluar, dirigir a la organización, lo cual se encuentra estructurado en el dominio (EDM), por su parte la Gestión es responsabilidad de la gerencia ejecutiva y comprende la planificación, construcción, ejecución y supervisión de las actividades para cumplir los objetivos organizacionales, estas funciones se organizan en los dominios:

- APO: enfocado a la planificación y organización
- BAI: enfocado en la construcción e implementación de soluciones
- DSS: enfocado a la operación y prestación de servicios
- MEA: encargado del monitoreo, evaluación y mejora continua

El dominio MEA es un componente crítico de retroalimentación dentro del ciclo de gestión de COBIT 2019, mientras que los dominios APO, BAI y DSS se enfocan en

planificar, construir y entregar soluciones. MEA tiene la función de verificar si esas actividades realmente cumplen con los objetivos y requisitos.

MEA se estructura en los siguientes puntos clave:

1. Equilibrio entre rendimiento interno y cumplimiento externo
    a. Transparencia interna, utilizando métricas a evaluar si la Información y Tecnología contribuye valor al negocio (MEA01)
    b. Vigilancia de leyes, reglamentos y contratos (MEA03)
2. Transparencia como base de confianza (MEA02)
3. Necesidad de independencia en la gerencia (MEA04)

Los informes de rendimiento de MEA01 y los resultados de MEA04 son los argumentos principales para el objetivo de gobierno EDM.

Componentes de COBIT 2019

Los objetivos de gestión y gobierno de la organización deben adaptarse y mantener un sistema de algunos componentes. Estos componentes interactúan entre sí para tener un sistema de gobierno holístico para TI.

1. Procesos. - Describe las prácticas y actividades para lograr objetivos y producir resultados que apoyen a las metas de TI.
2. Estructuras organizacionales. – Representa las entidades clave encargadas de la toma de decisiones, adquiere un modelo de definición de roles RACI.
3. Elementos y flujos de información. - Recurso esencial que permite la toma de decisiones.
4. Personas, habilidades y competencias. – Comprende el capital humano necesario para ejecutar las actividades operativas y de gobierno.
5. Políticas y procedimientos. – Define las directrices formales que orientan la ejecución de actividades y procesos.
6. Cultura, ética y comportamiento. – Aborda la dimensión humana necesaria para que el sistema de gobierno sea efectivo y sostenible en el tiempo
7. Servicios, infraestructura y aplicaciones. – Provee los medios tecnológicos necesarios.

De acuerdo a los modelos desarrollados de gestión, cada componente está orientado a una norma o marco de estudio específico y en cada objetivo.

Cuadro comparativo

Tabla 2. Comparación de normas, guías metodológicas

Enfoque metodológico	**Propósito principal**	**Enfoque de evaluación**	**Fortalezas**	**Limitaciones**
ISO/IEC 27004	Establecer directrices para medir	Basado en indicadores.	Aporta objetividad, trazabilidad y soporte para mejora continua	Requiere que la organización tenga definidos objetivos, métricas y fuentes de datos confiables
NIST SP 800-53A	Proporcionar un marco estructurado para evaluar	Evalúa mediante entrevistas, pruebas y exámenes	Muy útil operativamente y documenta evidencia	Puede resultar exigente en tiempo, recursos y especialización técnica
COBIT 2019	Fortalecer el gobierno, control y monitoreo	Enfocado en procesos, gobierno y niveles de capacidad	Integra seguridad, riesgo, desempeño y gobierno	No está diseñado exclusivamente para seguridad de la información, por lo que se complementa con ISO y NIST

Fuente: Propia

La integración de ISO/IEC 27004, NIST SP 800-53A y COBIT 2019 permite sustentar el diseño de una metodología para la evaluación de controles de seguridad de la información alineada a la normativa SEPS 2022-002. En este contexto, ISO 27004 facilita la definición de indicadores para medir la efectividad, NIST SP 800-53A establece los procedimientos para evaluar los controles, y COBIT 2019 integra estos resultados en el gobierno de TI y la toma de decisiones, contribuyendo al fortalecimiento del SGSI y a la mejora continua en las organizaciones del sector financiero popular y solidario.

2.3. Marco Legal

Normativa SEPS 2022-002

La implementación de un SGSI en las entidades del SFPS está regulado por la Normativa SEPS-IGT-IGS-2022-002, emitida por la Superintendencia de Economía Popular y Solidaria, la cual establece un marco regulatorio exhaustivo para dichas entidades.

La normativa establece regímenes para aplicar exigencias proporcionales, así mismo define una jerarquía clara de responsabilidades que involucra desde el Consejo de Administración hasta el Oficial de Seguridad de la información y la formación del SGSI en base a la serie de estándares 27000.

A través del Anexo 1 de la normativa se establecen los controles mínimos que deben ser implementados, adicionalmente en el Anexo 2 se establece los lineamientos para la metodología de riesgos y la evaluación de efectividad de los controles implementados necesaria para su cumplimiento.

Ley Orgánica de Protección de Datos Personales (LOPDP)

De acuerdo a la Ley Orgánica de Protección de Datos Personales vigente del mayo del 2021 en su artículo 37 Seguridad de datos personales dispone a las organizaciones responsables o encargadas del tratamiento de datos personas deberán evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Descripción del área de estudio

La presente investigación se desarrollará en instituciones del SFPS en Ecuador, específicamente en una cooperativa de ahorro y crédito regulada por la SEPS. El objetivo de estas instituciones es prestar servicios financieros a sectores con acceso limitado a la banca tradicional, por lo que gestionan información sensible como datos privados de sus socios y clientes. La cooperativa seleccionada cuenta con una infraestructura tecnológica que incluye sistemas de gestión interna, estaciones de trabajo, redes de datos, y servicios digitales para sus socios y clientes.

En el contexto actual, estas entidades enfrentan una amplia variedad de amenazas a la seguridad de la información, como accesos no autorizados, malware, ingeniería social, y debilidades en la seguridad de los datos en reposo y en tránsito. Esta realidad obliga a contar con metodologías para evaluar la efectividad y fortalecer los controles de seguridad, de tal manera que aseguren también el cumplimiento de la normativa vigente SEPS 2022-002.

3.2. Enfoque y tipo de investigación

El enfoque de la investigación será mixto, ya que se integrarán elementos cuantitativos y cualitativos. El componente cuantitativo se empleará para medir la efectividad de los controles de seguridad implementados y evaluar el nivel de cumplimiento con los controles mínimos establecidos en la normativa SEPS 2022-002, a través de la aplicación de instrumentos de medición. Por su parte, el enfoque cualitativo permitirá analizar y conocer como están diseñados e implementados los controles y facilitar evidencia de cumplimiento o posibles debilidades.

La investigación desempeñada será de tipo proyectivo debido a que se contempla el diseño de una propuesta metodológica de evaluación de controles sustentada en un análisis previo del contexto, asimismo también un carácter evaluativo, ya que se analizará la aplicabilidad de la metodología mediante un estudio de caso piloto en una institución regulada por la SEPS.

3.3. Procedimiento de investigación

El procedimiento de investigación se desarrollará en tres fases relacionadas con los objetivos específicos del estudio:

Fase 1: Revisión documental y normativa

Técnicas: Revisión bibliográfica y análisis documental.

Instrumentos: Fichas de análisis documental.

Actividades:

- Análisis de la normativa SEPS 2022-002.
- Identificación de requisitos específicos relacionados con la evaluación de controles de seguridad de la información.
- Revisión de marcos internacionales como ISO/IEC 27001, 27004 y NIST para complementar la propuesta metodológica.

Fase 2: Diseño de la metodología

Técnicas: Análisis comparativo y modelado metodológico.

Instrumentos: Guía metodológica, checklist de evaluación.

Actividades:

- Elaboración de una propuesta metodológica que incluya criterios, indicadores, niveles de cumplimiento y herramientas de evaluación.

Fase 3: Validación e implementación de la metodología en un caso de estudio

Técnicas: Aplicación de encuestas, entrevistas y herramientas diseñadas.

Instrumentos: Cuestionarios estructurados, listas de verificación, matriz de evaluación.

Grupo de estudio: Personal del área de tecnologías de la información y responsables de seguridad de la información de una cooperativa regulada por la SEPS.

Actividades:

- Aplicación de la metodología en una cooperativa regulada por la SEPS.
- Levantamiento de información sobre el estado actual de los controles.
- Evaluación del grado de cumplimiento normativo y gestión de riesgos.

3.4. Consideraciones bioéticas

Esta investigación se desarrollará respetando los principios bioéticos de beneficencia, precaución, justicia, responsabilidad y autonomía. Se garantizará la confidencialidad y anonimato de los datos recolectados. Para ello:

Se solicitará consentimiento informado a todos los participantes antes de aplicar encuestas o entrevistas.

Se informará claramente sobre los objetivos de la investigación, el uso de los datos y el derecho a retirarse en cualquier momento sin consecuencia alguna.

Se obtendrán los permisos institucionales requeridos para la realización del estudio dentro de la cooperativa.

No se recopilará información sensible sin las debidas salvaguardas técnicas y legales, de acuerdo con la Ley Orgánica de Protección de Datos Personales (2021).

CAPÍTULO IV

4. RESULTADOS

4.1. Revisión documental y normativa

En esta fase se realiza un análisis de la normativa con base en la resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO, así como las fichas de análisis documental de las normas ISO/IEC 27001:2022, ISO/IEC 27004:2016 y estándar NIST SP 800-53A, para el diseño de la metodología, constituyendo una herramienta de evaluación de controles para las instituciones reguladas por la SEPS.

4.1.1. Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002

a) Objetivo y alcance normativo

Regular los niveles mínimos para la administración de la seguridad de la información que deben definir las entidades del sector financiero popular y solidario, CONAFIPS y sus proveedores, para resguardar la confidencialidad, integridad y disponibilidad de los activos de información.

b) Regímenes de aplicación

La norma define regímenes con obligaciones y niveles de control distintos, en primer lugar, el régimen general para las Cooperativas de ahorro y crédito segmentos 1 y 2, asociaciones mutualistas, CONAFIPS, en segundo lugar, el régimen especial la conforman Cooperativas del segmento 3 y el régimen simplificado instituciones pequeñas del segmento 4 y 5.

c) Estructura Organizacional

En el régimen general la estructura organizacional debe estar conformada por:

a. Consejo de administración o Directorio
b. Comité de Seguridad de la Información (CSI)
c. Gerencia General

d. Unidad o Departamento de Seguridad de la Información
e. Oficial de Seguridad de la Información

d) Gobierno y responsabilidades

En el régimen general y especial se exige un Comité de Seguridad de la Información presidido por el presidente del Comité de Administración Integral de Riesgos. Como miembros clave el Gerente General, Oficial de Seguridad de la Información, el responsable de tecnología, delegado de auditoría interna y opcionalmente un delegado del área de negocio. Así mismo la normativa determina las directrices del CSI, la conformación del Departamento de Seguridad de la información y la designación formal del Oficial de Seguridad de la Información.

e) Requisitos Obligatorios

a. Plan Estratégico de Seguridad de la Información
b. Plan de Recursos para seguridad de la información
c. Plan de Gestión de Riesgos de Seguridad de la Información
d. Plan de Concienciación y formación
e. Políticas, procesos, procedimientos, roles y responsabilidades
f. Controles mínimos de seguridad
g. Sistema de Gestión de Seguridad de la Información

f) Anexo 1 - Controles obligatorios de seguridad de la información

Además de los requisitos exigidos en la norma, se deben desarrollar e implementar los siguientes controles:

- Documentación de políticas, manuales, procesos y procedimientos.
- Gestión de activos de información.
- Gestión de riesgos.
- Control de acceso.
- Gestión de incidentes y continuidad.
- Gestión de proveedores.
- Respaldo y recuperación.
- Auditorias y remediación.

g) Anexo 2 – Consideraciones para la metodología de riesgos

a. Clasificación de activos de información
b. Gestión de riesgos
c. Descripción del riesgo
d. Determinación del riesgo inherente
e. Evaluación de la efectividad de los controles

La normativa clasifica los controles implementados de acuerdo con la siguiente tabla:

Tabla 3. Clasificación de controles (SEPS 2022-002)

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

Fuente: SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002

f. Medición del riesgo residual
g. Tratamiento del riesgo

h) Plazos de implementación

La norma establece plazos transitorios por segmento, los cuales ya se encuentran vencidos desde julio de 2023, por consiguiente, la institución regulatoria se encuentra en etapa de supervisión activa y verificación del cumplimiento del modelo, por lo que cualquier entidad que no tenga evidencia actualizada tiene el riesgo de observaciones.

i) Base normativa técnica y referencias

La resolución remite explícitamente a la serie ISO/IEC 27000 como marco de referencia para el diseño del SGSI, así como a normativas previas de la SEPS relativas a seguridad física, tecnológica y administración de riesgos operativos. Esto implica que la

implementación debe estar alineada con buenas prácticas internacionales y adaptada al tamaño de cada entidad.

j) Incumplimiento

No cumplir la normativa puede derivar en medidas administrativas, exigencia de medidas correctivas obligatorias

k) Consideraciones para el cumplimiento

- Realizar un análisis de la normativa SEPS en relación a la ISO 27001, con el fin de fortalecer el SGSI y cumplimiento normativo.
- Priorizar procesos, ejecutar pruebas de vulnerabilidades y mitigación de hallazgos.
- Establecer un calendario anual de evaluación de proveedores críticos.
- Mantener un registro de las evidencias de los controles implementados.

4.1.2. Revisión a la NORMA ISO/IEC 27001

Tabla 4. Revisión a la NORMA ISO/IEC 27001

FICHA DE ANÁLISIS DOCUMENTAL	
Título del documento	ESTANDAR INTERNACIONAL ISO/IEC 27001:2022
Autores	Organización Internacional de Normalización (ISO) Comisión Electrotécnica Internacional (IEC)
Palabras clave de búsqueda	Sistema de Gestión de la Seguridad de la Información
Palabras clave del documento	Seguridad de la Información
Referencia bibliográfica	Organización Internacional de Normalización. (2022). ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la intimidad - Sistemas de gestión de la seguridad de la información - Requisitos. https://www.iso.org/standard/82875.html
Descripción del aporte al tema de investigación	La norma constituye un marco de referencia fundamental para el diseño de la metodología de evaluación de controles de seguridad de la información, ya que establece los requisitos para desarrollar del SGSI, así como los principios

	para la gestión de riesgos, controles de seguridad de la información, medición de la seguridad y mejora continua. Su aporte radica en proporcionar directrices sobre el modelo (PDCA) Planificar, Hacer, Verificar y Actuar, adicional a través de la cláusula número 9 “Evaluación del desempeño” define los criterios que las organizaciones deben determinar para el monitoreo, medición, análisis y evaluación de la Seguridad. Además, la norma define los controles de seguridad necesarios del SGSI por medio del anexo A.
Conceptos abordados	1. Sistema de Gestión de Seguridad de la Información (SGSI) Preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de la su buena gestión. 2. Contexto de la organización Comprender el entorno interno y externo, las partes interesadas, sus necesidades y requisitos, que influyen en el SGSI. 3. Liderazgo y compromiso Implica que la alta dirección demuestre compromiso, establezca la política de seguridad, asigne responsabilidades y los recursos necesarios. 4. Evaluación y tratamiento del riesgo Proceso que una institución debe definir y aplicar para identificar, analizar, establecer controles, evaluar y tratar los riesgos con respecto a la confidencialidad, integridad y disponibilidad de la información. 5. Controles de seguridad de la información Medidas implementadas para gestionar los riesgos y proteger los activos de información. La ISO 27001:2022 remite a través de su anexo A establece controles organizados en cuatro aspectos: • Organizativo • Personas • Físicos

	• Tecnológico 6. Evaluación del desempeño Proceso de monitoreo, medición, análisis y evaluación que las organizaciones deben implementar para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI. Las organizaciones a su vez para determinar si se implementa y mantiene de manera efectiva el SGSI deben realizar auditorías internas a intervalos planificados. Finalmente, la alta dirección revisa el SGSI para garantizar la idoneidad, adecuación y eficacia continuas. 7. Mejora continua La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

Fuente: Propia

4.1.3. Revisión a la NORMA ISO/IEC 27004

Tabla 5. Revisión a la NORMA ISO/IEC 27004

FICHA DE ANÁLISIS DOCUMENTAL	
Título del documento	ESTANDAR INTERNACIONAL ISO/IEC 27001:2016
Autores	Organización Internacional de Normalización (ISO) Comisión Electrotécnica Internacional (IEC)
Palabras clave de búsqueda	Medición de la seguridad de la información
Palabras clave del documento	Medición del desempeño. Eficacia de controles. Indicadores de evaluación.
Referencia bibliográfica	Organización Internacional de Normalización. (2016). ISO/IEC 27004:2016 Tecnologías de la Información - Técnicas de Seguridad - Gestión de la Seguridad de la Información - Monitoreo, Medición, Análisis y Evaluación. https://www.iso.org/standard/64120.html

Descripción del aporte al tema de investigación	Las organizaciones, con el objetivo de salvaguardar la confidencialidad, integridad y confidencialidad de la información implementan un SGSI junto con las actividades para su mantenimiento, sin embargo, dichas actividades por si solas, no garantizan el cumpliendo de los objetivos de seguridad de la información. En este sentido la norma ISO/IEC 27004 establece directrices para monitorear, mediar y evaluar el desempeño del SGSI, así como para definir periodicidad, las responsabilidades y los enfoques orientados a determinar el desempeño y/o eficacia. Su principal aporte se centra en el modelo de medición propuesto en su anexo, el cual incluye un conjunto prediseñado de medidas que facilitan la evaluación de los controles implementados.
Conceptos abordados	1. Medición del desempeño y eficacia Facilita la definición de indicadores de cumplimiento y eficacia para cada control, generando evidencia objetiva para la evaluación. 2. Medidas de desempeño Permiten determinar el estado de implementación de procesos, procedimientos y controles. Identifica logro de planificaciones. 3. Medidas de eficacia Determinan si los controles evaluados funcionan según lo previsto y el impacto sobre los objetivos, permiten dar confianza de la gestión. 4. Monitoreo y Medición Permite diseñar procedimientos de evaluación, su aplicación periódica y sistémica, asegurando consistencia y trazabilidad de los resultados. 5. Gestión de riesgos A la evaluación de controles está vinculada a la priorización de riesgos, permitiendo que la medición se enfoque en los controles más críticos. 6. Mejora continua

	Enfoque basado en modelo PDCA permitiendo que los hallazgos de la evaluación sirvan para proponer mejoras y fortalecer la seguridad de la organización. 7. Beneficios de la evaluación Proporciona mayor responsabilidad, mejora de rendimientos, eficacia de cumplimiento y principalmente apoya a la toma de decisiones. 8. Qué monitorear • Procesos SGSI • Gestión de incidentes • Gestión de vulnerabilidades • Control de accesos 9. Qué medir • Eficacia de acciones correctivas • Reducción de riesgos • Competencia del personal 10. Proceso de medición • Identificar necesidades de información • Crear y mantener medidas • Establecer procedimientos • Monitorear y medir • Analizar resultados • Evaluar desempeño • Revisar y mejorar procesos 11. Cliente de medición Designación encargada de solicitar información sobre la eficacia del SGSI 12. Planificador de medición Encardado de traducir las necesidades de información en un modelo estructurado de medición. 13. Titular de la información

	Posee la información necesaria para alinear las medidas de seguridad. 14. Colector de información Unidad operativa que garantiza de integridad de los datos antes de ser transformados en indicadores de gestión. 15. Analista de información Responsable de transformar los datos brutos en reportes y gráficos gerenciales.

Fuente: Propia

4.1.4. Revisión del estándar NIST 800-53A

Tabla 6. Revisión del estándar NIST 800-53A

FICHA DE ANÁLISIS DOCUMENTAL	
Título del documento	NIST Special Publication 800-53A Revision 5
Autores	Instituto Nacional de Estándares y Tecnología
Palabras clave de búsqueda	Evaluación de controles de seguridad
Palabras clave del documento	Procedimientos de evaluación. Plan de evaluación. Nivel de aseguramiento. Controles de seguridad y privacidad.
Referencia bibliográfica	National Institute of Standards and Technology. NIST (2022). Assessing security and privacy controls in information systems and organizations (NIST Special Publication 800-53A Rev. 5). https://doi.org/10.6028/NIST.SP.800-53Ar5
Descripción del aporte al tema de investigación	El NIST SP 800-53A proporciona el marco metodológico base para: Diseñar procedimientos de evaluación de controles (qué, cómo y con qué evidencia evaluar). Facilitar el diseño de formatos y herramientas de evaluación en base a criterios estandarizados. Complementar el proceso de medición por medio de los tres métodos de evaluación como examinar, entrevistar y probar,

	así como también para recopilar las evidencias necesarias de cada control, y posteriormente realizar el análisis y determinar el cumplimiento en términos como: cumple, no cumple o cumple parcialmente.
Conceptos abordados	1. Evaluación de seguridad y privacidad Es la actividad o conjunto de actividades realizadas para determinar que los controles estén correctamente diseñados, desarrollados e implementados, y finalmente alineados con los objetivos de la gestión de riesgos. 2. Evaluación Proceso sistemático que determina si los controles están implementados correctamente, operan como se pretende y producen los resultados deseados con respecto a los requisitos de seguridad y privacidad. 3. Procedimiento de evaluación Un procedimiento de evaluación consiste en un conjunto de objetos de evaluación, cada uno con especificaciones, mecanismos, actividades y responsables definidos, así mismo el procedimiento comprende 3 métodos de evaluación, finalmente atributos de profundidad y cobertura de evaluación. 4. Métodos de evaluación Examinar: es la actividad de revisar documentos y configuraciones para entender cómo funcionan los controles. Entrevista: corresponde a las entrevistas, discusiones y otras actividades con los responsables para recopilar información clave de los controles evaluados. Probar: se trata de ejecutar procedimientos o aplicar herramientas tecnológicas para verificar que los controles operen como se espera. 5. Objetos de evaluación Son elementos específicos sobre los cuales se aplica un método de evaluación para obtener evidencia técnica o administrativa. 6. Atributos

	Son elementos esenciales de los métodos de evaluación que permiten definir el nivel de esfuerzo requerido, el grado de rigor aplicado y el alcance del procedimiento de evaluación. 7. Declaraciones de determinación Expresan el juicio del evaluador sobre si la evidencia demuestra que el control es satisfactorio, así como también definir subcategorías que indiquen las debilidades o deficiencias descubiertas. 8. Proceso de evaluación En el proceso se establecen 4 etapas Preparación: definición de alcance, objetivos y responsables de evaluación Desarrollo del plan: Selección y detalle de procedimientos y definición de parámetros ODP Conducción: Recopilación de hallazgos y análisis de causa raíz Análisis de Resultados: Desarrollo del informe de resultados, plan de acción e hitos. 9. Parámetros ODP Parámetros Definidos por la Organización (ODP) representan la parte variable de un control o mejora que la organización instancia durante el proceso de ajuste.

Fuente: Propia

4.2. Desarrollo de la metodología

La segunda fase de la investigación corresponde al diseño de la metodología para la evaluación de controles del Sistema de Gestión de Seguridad de la Información, en la cual se establecen los criterios de medición y evaluación, así como los indicadores de desempeño y eficacia derivados del proceso de evaluación. Asimismo, se define la clasificación de los niveles de cumplimiento y efectividad de los controles, junto con la descripción de los métodos, técnicas y herramientas empleadas para la recopilación, análisis y evaluación de la información.

A continuación, el contenido de la sección 4.2 corresponde al desarrollo de la metodología propuesta, la cual abarca su introducción, antecedentes, objetivos, alcance y generalidades, así como la planificación, medición, análisis, monitoreo y mejora del proceso de evaluación de controles de Seguridad de la Información.

4.2.1. Introducción

El presente documento establece la Metodología de Evaluación de Controles de Seguridad de la Información, la cual deberá ser aplicada de forma obligatoria dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de la Cooperativa de Ahorro y Crédito Atuntaqui.

La metodología se encuentra alineada con la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002, así como con las directrices de medición establecidas en la norma ISO/IEC 27004 y los métodos de evaluación definidos en NIST SP 800-53A.

Su propósito es establecer un marco estructurado, trazable y reproducible que permita evaluar de manera objetiva el desempeño y la efectividad de los controles de seguridad de la información, garantizando el cumplimiento normativo, la gestión de riesgos y la mejora continua del SGSI.

4.2.2. Antecedentes

Actualmente, la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 Norma de Control Respecto a la Seguridad de la Información, regula los niveles mínimos requeridos para la administración de la seguridad de la información en entidades y empresas del Sector Financiero Popular y Solidario (SFPS). Esta normativa obliga a definir, implementar y mantener controles orientados a resguardar la confidencialidad, disponibilidad e integridad de los activos de información. De igual manera, establece que estos controles deben ser revisados y evaluados de forma periódica, al menos una vez al año, para asegurar su efectividad y adaptación frente a cambios en el entorno, amenazas emergentes y evolución tecnológica.

En este contexto, la metodología que se desarrolla busca establecer un marco sistemático para la evaluación de controles de Seguridad de la Información, que permita medir tanto su desempeño como eficacia según corresponda y el nivel de cumplimiento de los requisitos normativos establecidos en la normativa. De esta manera, garantizar que las medidas implementadas no solo sean técnicamente efectivas, sino también conformes con las exigencias regulatorias aplicables, fortaleciendo la gestión de riesgos, la mejora continua y la resiliencia institucional frente a incidentes de seguridad de la información.

4.2.3. Objetivo General

Establecer una metodología para la evaluación de los controles del Sistema de Gestión de Seguridad de la Información (SGSI), que permita medir su desempeño y efectividad, asegurando la generación de información confiable para la toma de decisiones y promoviendo la mejora continua del sistema.

4.2.4. Objetivos Específicos

- *Definir el procedimiento de medición aplicable orientado a garantizar la validez de los resultados, así como su trazabilidad y reproducción.*
- *Establecer intervalos de seguimiento y medición de los procesos, asignando los roles responsables del monitoreo, medición, así como de la revisión y análisis de resultados.*
- *Demostrar el grado de cumplimiento de los controles frente a los lineamientos definidos en la normativa.*

4.2.5. Alcance

La presente metodología será de aplicación obligatoria para todos los controles de seguridad de la información implementados dentro del alcance del SGSI de la Cooperativa, en cumplimiento de lo dispuesto en la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 emitida por la Superintendencia de Economía Popular y Solidaria (SEPS).

La metodología establece los lineamientos para evaluar el grado de desempeño y efectividad de los controles de seguridad de la información, así como para evidenciar el cumplimiento de los requisitos regulatorios.

A través de su aplicación, la institución deberá:

- *Verificar que los controles contribuyan al logro de los objetivos de seguridad de la información.*
- *Generar información verificable que oriente a la identificación de brechas.*
- *Determinar la efectividad de los controles conforme a la clasificación determinada en la normativa.*
- *Apoyar la toma de decisiones dentro del proceso de gestión del riesgo, aportando datos objetivos y criterios claros para optimizar las acciones de mejora.*

En conjunto, este alcance asegura que la metodología no solo sirva como herramienta de verificación y control, sino también como un insumo estratégico para la mejora continua y la conformidad normativa vigente.

4.2.6. Participación de las partes interesadas

La presente metodología, apegada a los lineamientos de la norma ISO/IEC 27001 e incorporando las directrices de la ISO/IEC 27004, establece la participación activa de las partes interesadas en las actividades de medición de los controles del SGSI.

La inclusión de las partes interesadas garantiza que el proceso de medición cuente con el apoyo estratégico, técnico y operativo necesario para generar información confiable, objetiva y orientada a la mejora continua.

Definición de las partes interesadas

Las partes interesadas corresponden a los integrantes que conforman el Comité de Seguridad de la Información, principalmente:

- *Presidente del Comité de Administración Integral de Riesgos.*
- *Gerente General*
- *Responsable de Seguridad de la Información*
- *Responsable de Tecnología de la Información*

Responsabilidades

Comité de Seguridad de la Información: *Asegura la alineación del proceso de medición con los objetivos estratégicos institucionales y respalda la asignación de recursos.*

Responsable de Seguridad de la Información: *Implementa, supervisa y coordina el desarrollo e implementación de la metodología. Lidera el proceso de medición, valida la calidad de los recursos y comunica los hallazgos.*

Responsable de Tecnología de la Información: *Facilita la gestión de recursos tecnológicos y asegura que los procesos de medición se integren de manera adecuada con la infraestructura existente.*

4.2.6.1. Proceso de comunicación de actividades de medición

Para asegurar que el inicio y seguimiento de las actividades de medición tengan el apoyo estratégico y operativo necesario, se realizará el siguiente proceso:

- *Todas las partes interesadas serán informadas del objetivo, alcance, justificación de cada medición.*
- *La comunicación se la realizará antes del inicio de cada ciclo de medición.*
- *El responsable de la comunicación es el Responsable de Seguridad de la Información*
- *Se registrará la comunicación de recepción y conformidad por cada parte interesada, así como cualquier retroalimentación recibida.*
- *Los medios de comunicación incluyen reuniones, y correos formales utilizando herramientas para presentación de datos como dashboards y reportes de planificación de medición.*
- *Toda evidencia de comunicación y confirmación se documentará y archivará para fines de auditoría y trazabilidad.*

4.2.7. Características generales de la medición

Enfoque basado en necesidades de información

Debido a la cantidad de atributos relacionados con la seguridad de la información que se puede medir, la supervisión y medición debe enfocarse en aquellos que proporcionan datos útiles para determinar si los controles son eficaces y cumplen con los objetivos establecidos.

Considerar que no todo puede o debe medirse, ya que la medición excesiva es costosa, compleja y puede ocultar información relevante.

¿Qué supervisar?

La supervisión tiene como objetivo vigilar y conocer el estado de los sistemas, procesos y actividades clave del SGSI para dar respuesta a una necesidad de información. Los principales elementos que se puede supervisar son:

- *Implementación de los procesos del SGSI*
- *Gestión de incidentes de seguridad de la información*
- *Gestión de vulnerabilidades*
- *Gestión de configuración*
- *Concienciación y formación en seguridad*
- *Control de acceso y registro de eventos*
- *Auditorías internas y externas*
- *Evaluación y tratamiento de riesgos*
- *Gestión de riesgos de terceros*
- *Gestión de continuidad del negocio*
- *Seguridad física y ambiental*

Las actividades de supervisión producen información que puede permitir determinar si un riesgo se materializó, y tomas decisiones tempranas para mitigarlos, así mismo es importante mencionar que existen controles de seguridad con el propósito de supervisar como logs, alertas de seguridad, entre otros.

¿Qué medir?

La medición se enfoca en evaluar el desempeño y la eficacia de los controles y procesos del SGSI mediante indicadores y medidas, que permitan detectar oportunidades de mejora. La medición convierte los datos en información útil para apoyar la toma de decisiones.

Los procesos y actividades que pueden ser medidos son:

Eficacia de los controles de seguridad de la información:

- *Grado en que los controles reducen la probabilidad y el impacto de incidentes.*
- *Tiempo de detección y respuesta ante eventos de seguridad.*

Capacitación y concienciación en seguridad:

- *Nivel de adquisición de competencias mediante encuestas o cuestionarios posteriores a la formación.*

Gestión de riesgos:

- *Reducción del nivel de riesgo residual tras la implementación de controles.*

Indicadores de continuidad y seguridad física:

- *Resultados de pruebas de continuidad del negocio.*
- *Número de incidencias detectadas en sistemas de control de acceso físico.*

La medición no se limita a los indicadores presentados.

Frecuencia de medición y análisis

La frecuencia de medición y análisis de la información se debe realizar de acuerdo a las políticas contenidas en el "Manual de Políticas de Seguridad de la Información" y procedimientos establecidos en el "Manual de Gestión de Seguridad de la Información", considerando también la naturaleza de los datos, su ciclo de vida y el nivel de validez requerido. Antes de proceder al análisis, se debe recolectar un volumen suficiente de datos que permita obtener resultados significativos. Los plazos y la frecuencia de estas actividades pueden ajustarse según cambios tecnológicos, regulatorios o del entorno, garantizando que la medición se mantenga pertinente y actualizada.

Roles y responsabilidades de medición

Es importante asignar roles y responsabilidades claras en todo el proceso de supervisión y medición. Entre los principales roles se encuentran:

Cliente de medición. - *corresponde al Comité de Seguridad de la Información u otras partes que solicitan o requieren información de eficiencia y eficacia relacionada con el SGSI.*

Planificador de medición y gestor de datos. - *persona o unidad que define, diseña y valida las medidas de desempeño y eficacia, asegurando su alineación con los requerimientos del cliente de medición y verificando que sean adecuadas, consistentes y efectivas.*

Titular de la información. - *persona o unidad propietaria de la información responsable de proporcionar los datos.*

Colector y analista de información. – *persona o unidad responsable de recopilar registrar, almacenar, analizar los datos y comunicar los resultados.*

4.2.8. Tipos de medidas

Para evaluar el desempeño y la eficacia, se establecen dos tipos de medidas:

4.2.8.1. Medidas de desempeño

Se usan para demostrar el grado de implementación de procesos, procedimientos y controles del SGSI, mostrando si las actividades se han realizado según lo planificado.

Características

- *Demuestran el progreso en la implementación del SGSI*
- *Utilizan datos de registros, actas, planes de proyectos, asistencia, herramientas automatizadas, etc.*
- *Permiten determinar áreas que necesitan mejorar, incluso después de alcanzar los objetivos*
- *Se pueden recopilar y analizar automatizada para reducir errores humanos y esfuerzo.*

Ejemplo:

Medir el porcentaje de portátiles con cifrado completo del disco. Inicialmente, los resultados podrían ser menores al 100%. Al alcanzar y mantener el 100% de portátiles con cifrado se puede concluir que el control está plenamente implementado.



Figura 3. *Avance de una medida de desempeño*
Fuente: Propia



Figura 4. *Medida de desempeño resultante*
Fuente: Propia

Indicador sugerido: *Porcentaje de controles de seguridad implementados frente a los planeados en función del tiempo.*

4.2.8.2. Medidas de eficacia

Las medidas de eficacia se centran en evaluar el impacto real de los controles y actividades del SGSI sobre los objetivos de seguridad de la información. Estas medidas determinan si las acciones previstas logran los resultados deseados.

Características

- *Determinan si las actividades implementadas logran los objetivos de seguridad.*
- *Combinan datos de supervisión automatizada con información manual sobre la actividad del SGSI.*
- *Pueden incluir medidas de costos, nivel de confianza de clientes, reducción de incidentes y exposición al riesgo.*
- *Ayudan a la toma de decisiones estratégicas y a la gestión de riesgos.*

Ejemplo:

Medir la disminución progresiva en el inventario de vulnerabilidades identificadas y no corregidas en los activos críticos de la organización. La medida se calcula en función del número total de vulnerabilidades reportadas por las herramientas de gestión de vulnerabilidades frente al número de vulnerabilidades que permanecen sin aplicar parches dentro de los plazos definidos por la política de seguridad.

Este indicador permite evaluar la exposición residual al riesgo y la capacidad del proceso de gestión de parches para mitigar amenazas de manera oportuna.

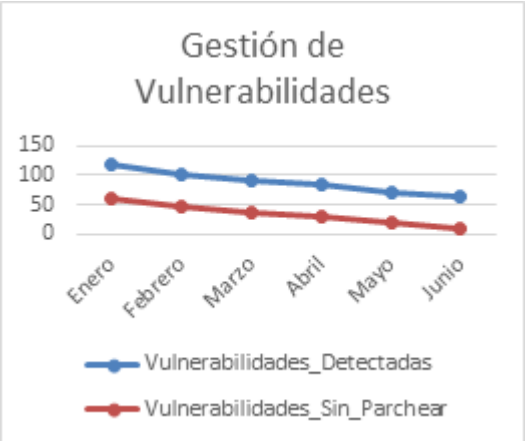


***Figura 5**. Medida de eficacia en la gestión de vulnerabilidades*

Fuente: Propia

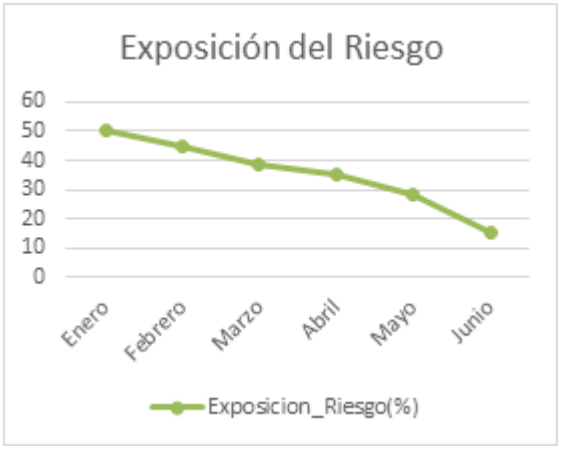


***Figura 6**. Medida de eficacia para exposición del riesgo*

Fuente: Propia

4.2.9. Proceso de medición

El proceso general de medición y evaluación de controles de seguridad de la información corresponde a las siguientes actividades.

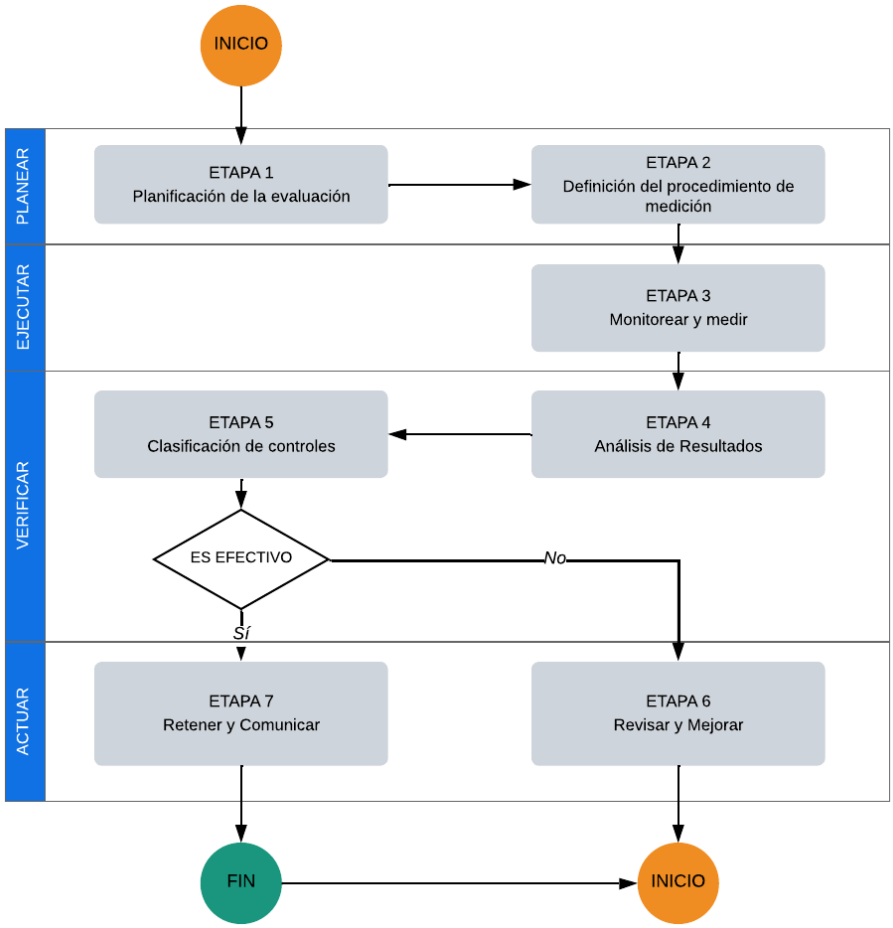


***Figura 7**. Diagrama de flujo del proceso de medición*

Fuente: Propia

El proceso sigue una lógica secuencial de evaluación de efectividad, en el cual incorpora un punto de decisión clave asegurando su alineación con el enfoque de mejora continua del SGSI.

4.2.9.1. Etapa 1: Planificación de la Evaluación

La etapa de planificación constituye el punto de partida del proceso de medición, cuyo propósito es establecer un modelo estructurado, trazable y reproducible.

a) Identificación de necesidades de información

Inicialmente se deberá identificar las necesidades de información que permite determinar qué aspectos del SGSI requieren ser medidos para evaluar los controles del SGSI.

Las necesidades pueden establecerse a partir de:

- *Partes interesadas (SEPS, auditorías, alta gerencia)*
- *Dirección estratégica de la institución*
- *Políticas y objetivos de seguridad de la información*

Para definir una necesidad de información, se debe revisar previamente el marco de políticas y objetivos de seguridad, así como los controles implementados, los requisitos legales, regulatorios, contractuales y los resultados de la gestión de riesgos.

Con base al análisis, las necesidades de información deben orientarse a determinar:

- *Si los controles están implementados y operan correctamente.*
- *Si se cumplen las obligaciones normativas y regulatorias.*
- *Si los riesgos están siendo gestionados de manera efectiva.*
- *Si la información generada permite apoyar la toma de decisiones de la alta dirección.*

Ejemplo práctico:

Tabla 7. *Necesidad de información*

ID	Necesidad de información
NI-001	Determinar si las políticas de seguridad de la información están definidas, aprobadas y alineadas a los objetivos estratégicos de la institución

Fuente: Propia

b) Creación y mantenimiento de medidas

Las medidas de seguridad de la información deberán ser creadas inicialmente y mantenidas de forma continua, con el fin de asegurar que respondan de manera efectiva a las necesidades de la información identificadas.

Las medidas deberán revisarse y, de ser necesario, actualizarse cuando se produzcan cambios significativos en el entorno del SGSI, como:

- *Cambios en el alcance del SGSI*
- *Modificaciones en la estructura organizacional*
- *Cambios en las partes interesadas, incluyendo roles, responsabilidades y participantes.*
- *Cambios en los objetivos institucionales*
- *Nuevos requisitos legales y regulatorios*
- *Logros sostenidos en varios ciclos de medición*
- *Implementación, modificación o retiro de tecnologías y sistemas de procesamiento de la información.*

La actualización debe priorizar la reutilización y adaptación de medidas existentes

c) Desarrollar o actualizar medidas

El desarrollo o actualización documenta las medidas de seguridad de la información que permiten evaluar de forma objetiva el desempeño y la efectividad de los controles, asegurando su alineación con las necesidades de información previamente identificadas.

Los principios que deben considerarse son:

- *Derivarse directamente de una necesidad de información*
- *Las medidas pueden requerir nuevas fuentes o mecanismos de medición*
- *Mejora o ajuste de medidas existentes*
- *Cada medida debe definirse con suficiente detalle para garantizar*
    - *Implementación consistente*
    - *Evaluación objetiva*
    - *Repetibilidad*
    - *Trazabilidad*

El proceso consiste en identificar las fuentes de datos, definir las consideraciones relevantes, integrar el método de evaluación y establecer la definición estructurada de la medida.

1) Identificación de fuentes de datos

Identificar y analizar las fuentes de datos que permitan sustentar cada medida. Estas pueden ser internas o externas, entre las cuales pueden ser:

- *Registros técnicos (logs, SIEM, escaneos de vulnerabilidades)*
- *Estadísticas de capacitación y concientización*
- *Resultados de encuestas*
- *Estadísticas de incidentes de seguridad*
- *Informes de auditoría interna/externa*
- *Resultados de pruebas de continuidad del negocio*

Es importante validar que los datos sean confiables, disponibles, trazables y verificables.

2) Consideraciones de implementación

Las medidas deben ser seleccionadas y diseñadas considerando los siguientes aspectos:

- *Facilidad de recopilación de datos*
- *Disponibilidad de recursos humanos y tecnológicos*
- *Costo de implementación y análisis*
- *Facilidad de implementación*

- *Utilidad para la toma de decisiones*

3) Integración de métodos de evaluación

Cada medida deberá definir el método mediante el cual será evaluada, en la siguiente tabla se determinan los métodos de evaluación.

Tabla 8. *Métodos de evaluación*

Método	***Descripción***	***Aplicación***
Examinar	*Revisión documental y técnica*	*Políticas, procedimientos, logs*
Entrevistar	*Validación con personal*	*Roles, responsabilidades, ejecución*
Probar	*Verificación técnica del control*	*Pruebas de seguridad, accesos, respaldos*

Fuente: NIST SP 800-35A

4) Definición estructural de la medida

Cada medida deberá documentarse mediante la siguiente ficha basada en la ISO/IEC 27004:2016:

Tabla 9. *Definición de la medida*

Definición de la medida	
ID de la medida	*Identificador alfanumérico único que permita su trazabilidad y control de versiones (Ej.: MED-SI-001)*
Necesidad de la información asociada	*Indica la necesidad de información que da origen a la medida (Ej.: NI-001)*
Control evaluado	*Cada medida deberá estar asociada a un control específico y, cuando aplique, al riesgo que se busca mitigar, garantizando la trazabilidad entre el control, el riesgo y la medición.*
Descripción de la medida	*Definición clara de la medida que puede ser expresada en términos como porcentaje, número de eventos, frecuencia o promedio (Ej.: Porcentaje de políticas revisadas).*

Fórmula o método de cálculo	*La formula define como se debe calcular la medida (Ej.:(Número de auditorias realizadas/Número de auditorías planificadas) *100)*
Objetivo o meta de la medida	*El objetivo de la medida es el resultado que se espera obtener al realizar la medición, puede expresarse como una meta específica, un valor numérico o un rango de referencia que indica si el resultado es adecuado (Ej. Verde: Si indicador>90%)*
Método de evaluación	*Determinar el o los procedimientos de evaluación a usar mediante la medición.* • *EXAMINAR: método que facilita la compresión, aclara información u obtiene evidencia mediante la revisión, inspección, estudio o análisis de documentales, controles, medidas de seguridad y acciones de gestión.* • *ENTREVISTA: método usado para facilitar la compresión, aclarar información u obtener evidencia a través de discusiones con los responsables de los procesos.* • *PROBAR: método que permite validar técnicamente el funcionamiento del control Ej. autenticación, respaldos, recuperación, análisis de vulnerabilidades, etc.*
Evidencia requerida	*Elementos encargados de demostrar y sustentar la evaluación, pueden facilitar la identificación de causas de resultados deficientes o brechas y aporta información al proceso, sirviendo como datos de entrada para la fórmula.*
Frecuencia de la medición	*Es necesario establecer la periodicidad con la que se debe recopilar y reportar los datos (Ej. mensual, trimestral, anual, etc.).*
Partes responsables	*Cada medida debe tener responsables para su ejecución, es mandatorio definición por lo menos al titular de la información, colector de información y cliente de medición.*
Fuente de datos	*Sistema, herramienta, registro o documento del cual se obtienen los datos (Ej.: SIEM, GLPI, Active Directory, reportes de auditoría, escáneres de vulnerabilidades, proveedores, áreas internas). Debe especificar si la fuente es interna o externa.*
Forma de presentación o informe	*Describe el formato del reporte final: texto, valor numérico, tabla, gráfico, tablero de indicadores (dashboard) u otro medio definido por el SGSI.*

Fuente: Propia

La validación de la documentación de medidas se evidenciará mediante la matriz de planificación de medidas. El cronograma de ejecución y responsables asignados.

Ejemplo práctico:

Tabla 10. Ejemplo - *Definición de la medida*

Definición de la medida	
ID de la medida	*MED-SI-001*
Necesidad de la información asociada	*NI -001.- Evaluar si las políticas de seguridad están definidas, aprobadas y alineadas a los objetivos estratégicos*
Control evaluado	*Políticas de Seguridad*
Descripción de la medida	*% de políticas formalizadas y alineadas*
Fórmula o método de cálculo	*(Políticas aprobadas y alineadas / Total políticas requeridas) x 100*
Objetivo o meta de la medida	*≥ 95%*
Método de evaluación	*EXAMINAR*
Evidencia requerida	*Documentos aprobados, actas*
Frecuencia de medición	*Anual*
Partes responsables	*Titular de la información: Jefe de Seguridad de la Información* *Colector de información: Jefe de Seguridad de la Información* *Cliente de medición: Comité de Seguridad de la Información*
Fuente de datos	*Repositorio documental (interno)*
Forma de presentación o informe	*Dashboard*

Fuente: Propia

5) Priorización de implementación

Asegurar que todas las medidas definidas se encuentren formalmente documentadas, organizadas y priorizadas, garantizando su implementación efectiva dentro del SGSI.

Todas las medidas deben consolidarse en un repositorio formal (matriz o catálogo de medidas), el cual debe contener los campos:

- *Identificación de la medida*
- *Medida (Declaración)*
- *Tipo de medida (desempeño / efectividad)*
- *Prioridad de implementación*

El enfoque de implementación de las medidas se realiza de forma secuencial, priorizando las medidas de desempeño orientadas a verificar que el control está definido e implementado y se ejecuta conforme a lo establecido ya que estas medidas constituyen la base del proceso de evaluación, posterior se implementan las medidas de efectividad orientadas a evaluar si el control reduce el riesgo asociado y cumple su propósito dentro del SGSI puesto que estas medidas se implementan cuando exista evidencia suficiente de que el control esta implementado.

Priorización de implementación

Tabla 11. *Priorización de implementación*

Criterio	***Prioridad***	***Implementación***
Requeridas por normativa o asociadas a riesgos críticos	*ALTA*	*Inmediata*
Relevantes para el seguimiento del SGSI	*MEDIA*	*Planificada*
De mejora continua o con baja disponibilidad de datos	*BAJA*	*Diferida*

Fuente: Propia

Ejemplo práctico:

Tabla 12. Ejemplo - *Priorización de implementación*

ID	Medida	Tipo de medida	Prioridad	Implementación
MED-SI-001	% políticas formalizadas	Desempeño	ALTA	Inmediata
MED-SI-002	% incidentes por falta de políticas	Efectividad	MEDIA	Posterior

Fuente: Propia

En importante considerar que no se debe implementar medidas de efectividad sin haber validado previamente la existencia y operación del control. En este sentido, la medición secuencial del desempeño y la efectividad garantiza una evaluación lógica, trazable y auditable.

4.2.9.2. Etapa 2: Definición del procedimiento de medición

Definir y estandarizar los procedimientos, formatos e instrumentos que serán utilizados para la medición de los controles de seguridad de la información, garantizando que su ejecución posterior se realice de forma consistente, repetible, trazable y auditable.

Esta etapa aplica a todas las medidas definidas y tiene como propósito preparar la ejecución de la medición.

1) Procedimiento general de medición

Se establece un procedimiento único para el SGSI que define la secuencia de ejecución de la medición, para lo cual se aplica conforme al siguiente flujo:

- *Recolección de datos*
- *Validación de información*
- *Evaluación de criterios*
- *Análisis de resultados*
- *Reporte de información*

2) Diseño de instrumentos de medición

Para la ejecución de las medidas se deberá contar con un instrumento estándar o formulario de recopilación y análisis de información alineado a la definición previa de la medida.

Las características del instrumento:

- *Permitir aplicar los métodos de evaluación (Examinar, Entrevistar, Probar)*
- *Incluye criterios de evaluación (S/P/N)*
- *Permite registrar evidencia*
- *Integra el cálculo de la medida*
- *Facilita la trazabilidad de la medición*

3) Uso del instrumento

Los lineamientos mínimos para asegurar la consistencia de la información serán:

- *Cada medida debe evaluarse mediante el formato definido*
- *No se podrá registrar cumplimiento sin evidencia verificable*
- *Se deberán utilizar únicamente fuentes de datos definidas en la medida*
- *La evaluación de criterios será objetiva (S/P/N)*
- *El cálculo deberá respaldar la fórmula establecida en la medida*

El uso del formulario de recopilación y análisis de información será obligatorio para la evaluación de todas las medidas definidas.

4) Lineamientos para la recolección de datos

La recolección de datos se realizará conforme a lo definido en cada medida, considerando:

- *Fuente de datos previamente establecida*
- *Frecuencia de medición definida*
- *Responsable asignado*
- *Evidencia requerida según método de evaluación*

5) Lineamientos para la validación de la información

El evaluador debe considerar controles mínimos de validación que deben aplicarse durante la ejecución:

- *Verificación de integridad de los datos*
- *Coherencia lógica de la información*
- *Correspondencia con la fuente definida*
- *Existencia de evidencia verificable*
- *Los datos validados podrán ser utilizados en el análisis.*

6) Lineamientos para la evaluación de criterios

La evaluación del control se realiza mediante la aplicación de criterios definidos en el formulario, registrando el resultado como:

- *S (Cumple)*
- *P (Cumple Parcialmente)*
- *N (No Cumple)*

Para las medidas de desempeño, los criterios deben orientarse a verificar la existencia y formalización del control, considerando como base los siguientes aspectos

- *El control se encuentra implementado(existe)*
- *Está documentado (políticas, procedimientos u otros documentos formales)*
- *Cuenta con aprobación formal por autoridad competente*
- *Alineado a la normativa aplicable (SEPS, ISO, normativa interna)*
- *Tiene un responsable definido*

7) Análisis de resultados

El análisis se realiza conforme a lo definido en el diseño de la medida mediante:

- *Aplicación de la fórmula establecida*
- *Obtención del resultado*
- *Comparación con el objetivo definido*

8) Uso del reporte de resultados

Los resultados obtenidos deben presentarse conforme a lo definido en la ficha de cada medida considerando:

- *Formato de reporte establecido*
- *Nivel de detalle requerido*
- *Destinatarios definidos*

9) Herramientas de soporte

Se deben utilizar herramientas que faciliten la ejecución del proceso considerando simplicidad y aplicabilidad.

Tabla 13. *Herramientas de soporte*

Uso	***Herramienta***
Evaluación	*Formulario / Excel*
Evidencia	*Repositorio documental*
Análisis	*Excel*
Visualización	*Dashboard*

Fuente: Propia

Ejemplo práctico:

Diseño del instrumento de medición en el que se incluye

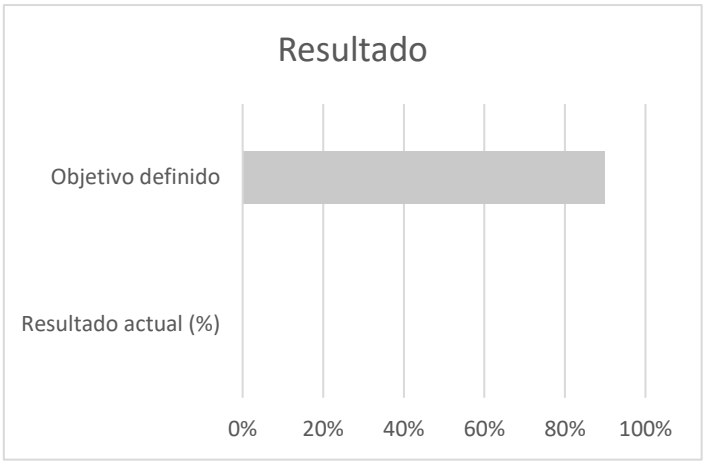
- *Información general de la medida*
- *Objetivo*
- *Métodos de evaluación*
- *Criterios y lineamientos de evaluación (S/P/N), registro de evidencia.*
- *Aplicación de la fórmula en función a los objetivos esperados*
- *Presentación del resultado conforme al formato establecido en la medida.*

Tabla 14. Ejemplo - *Formulario de recopilación y análisis de información*

Formulario de recopilación y análisis de información			
1. Información general			
Fecha de evaluación:	*11/03/2026*		
Evaluador:	*Jefferson Andrade*		
ID de la Medida:	*MED-SI-001*		
Control evaluado	*Políticas de Seguridad*		
Frecuencia	*Anual*		
Responsable / Entrevistado:	-		
Cargo:	*Jefe de Seguridad de la Información*		
2. Necesidad de la información			
Determinar si la entidad:			
Dispone de un marco integral de políticas de seguridad de la información que abarque todos los dominios establecidos por la normativa SEPS			
3. Métodos de evaluación aplicados			
Examinar	*• Inventario de políticas aprobadas y vigentes* *• Repositorio documental institucional* *• Historial de versiones.* *• Registros de difusión*		
Entrevistar	*• Responsable de Seguridad de la Información*		
4. Evaluación del marco general de políticas			
N	*Criterio de evaluación*	*Cumple (S/P/N)*	*Evidencia*
1	*¿Existe un marco formal que agrupe las políticas de seguridad de la información?*		

2	*¿Se designó responsable formal para el desarrollo, documentación y difusión?*		
3	*¿Las políticas están formalmente aprobadas por autoridad competente?*		
4	*¿Las políticas se encuentran vigentes?*		
5	*¿Se definen eventos de actualización como cambios normativos y regulatorios?*		
6	*¿Existe control de versiones?*		
7	*¿Las políticas están alineadas con los objetivos estratégicos institucionales?*		
8	*¿Las políticas están correctamente detalladas (no son genéricas)?*		
9	*¿Las políticas tienen coherencia con la normativa SEPS y otras regulaciones?*		

5. Evaluación de cobertura por dominio normativo			
¿Confirma que existen políticas formalmente documentadas, aprobadas y vigentes para los siguientes dominios?			
N	*Revisión por Dominio*	*Confirmación (S/P/N)*	*Evidencia (Políticas de Seguridad de la Información)*
1	*Seguridad de la información*		
2	*Clasificación de información*		
3	*Gestión de riesgos*		
4	*Control de accesos*		
5	*Gestión de incidentes*		
6	*Gestión de software*		
7	*Infraestructura tecnológica*		
8	*Seguridad RRHH*		
9	*Seguridad física*		
10	*Gestión con terceros*		
11	*Ciberseguridad*		
6. Fórmula o método de cálculo			
Fórmula de cálculo:		*Número de criterios y dominios cumplidos / Total de criterios y dominios evaluados x 100*	
Registro de datos			
Variable		*Resultado*	

Número de criterios y dominios evaluados	*20*
Número de criterios y dominios cumplidos	
Número de criterios y dominios no cumplidos	
Resultado actual (%)	*0%*
Objetivo definido	*90%*
7. Presentación de resultados	
Indicador porcentual de cumplimiento (Porcentaje de cobertura del marco de políticas de seguridad de la información respecto a los dominios exigidos por la normativa aplicable)	

Fuente: Propia

4.2.9.3. Etapa 3: Monitorear y medir

En esta etapa se aplica el formulario de recopilación y análisis de información definido previamente, con el fin de obtener resultados cuantificables sustentados en evidencia objetiva y verificable.

La medición de los controles de seguridad de la información se ejecuta mediante la recolección, validación, análisis y reporte de datos, asegurando que los resultados sean confiables, repetibles y útiles para la toma de decisiones.

Este proceso aplica a todas las medidas definidas (desempeño y efectividad), utilizando los instrumentos y lineamientos establecidos en la etapa de planificación.

a) Recolección de datos

Se obtiene la información desde las fuentes definidas en cada medida aplicando el formato de evaluación para recopilar las evidencias de acuerdo al tipo de medida como:

- *Documentos*
- *Registros*
- *Logs*
- *Entrevistas*
- *Pruebas*

Es importante utilizar las fuentes definidas en la medida, respetar la frecuencia y recopilar datos suficientes para análisis confiable.

b) Almacenamiento de la información

Los datos recopilados deben ser almacenados en repositorios o folders accesibles organizados por medida, fecha y evaluador, de modo que sea segura y trazable.

c) Validación de datos

Aplicación de la lista de verificación de datos.

Tabla 15. *Validación de datos*

Validación	***Descripción***
Integridad	*Datos completos*
Rango	*Valores dentro de límites establecidos*
Consistencia	*Coherencia entre datos*
Evidencia	*Soporte verificable*

Fuente: Propia

d) Evaluación de los criterios

Evaluar cada criterio del control previa revisión de las evidencias necesarias registrando de forma objetiva en el formulario de recopilación y análisis de información de la medida.

Tabla 16. *Evaluación de los criterios*

Valor	*Valor numérico*	*Significado*
S	*1*	*Cumple: El criterio cumple en su totalidad y existe evidencia objetiva, suficiente y verificable*
P	*0.5*	*Cumple parcialmente: El criterio se cumple de manera incompleta, presentando desviaciones, limitaciones o evidencia parcial*
N	*0*	*No Cumple: El criterio no se cumple o no existe evidencia que lo respalde*

Fuente: Propia

e) Cálculo de resultados

Mediante el formulario y la aplicación de la fórmula definida se determina el resultado de la evaluación, tomando en cuenta el objetivo planteado.

El resultado debe reflejar el desempeño o la efectividad del control.

4.2.9.4. Etapa 4: Análisis de resultados

Interpretar los resultados obtenidos en medición para determinar brechas, causas, y evaluar el estado real del control generando insumos para la toma de decisiones.

a) Consolidar resultados y comparar contra objetivos

Revisar los resultados de las medidas de desempeño y eficacia, posterior comparar cada resultado con la meta definida.

Cuando una medida no cumple su objetivo presenta una brecha.

Ejemplo práctico:

Tabla 17. Ejemplo - *Consolidación de resultados y análisis*

Medida	***Resultado***	***Objetivo***	***Estado***
MED-SI-001	*85%*	*90%*	*Brecha*
MED-SI-002	*100%*	*90%*	*Sin desviación*

Fuente: Propia

b) Identificar desviaciones

Identificar específicamente qué aspectos del control no están cumpliendo, es decir, donde se encuentra la falla.

Para lo cual se debe revisar criterios no cumplidos y determinar fallas puntuales como los siguientes:

- *Políticas no difundidas*
- *Falta de evidencia*
- *Controles no ejecutados*
- *Incumplimiento de periodicidad*

c) Análisis de causas

Identifica el origen de las desviaciones detectadas, es decir, porque ocurre el problema analizando el contexto del incumplimiento e identificar factores organizacionales u operativos definidos a continuación.

Tabla 18. *Análisis de causas*

Tipo	***Causa***
Gobierno	*Falta de responsable*
Políticas/Procesos	*Procedimientos inexistentes*
Operación	*No se ejecuta el control*
Diseño	*Control mal diseñado*
Cultura	*Falta de conocimiento*

Fuente: Propia

4.2.9.5. Etapa 5: Clasificación de efectividad de los controles

Determinar el nivel de efectividad de los controles de seguridad de la información, mediante la interpretación de los resultados obtenidos en las medidas de desempeño y, cuando corresponda, en las medidas de efectividad, evaluando su existencia, formalización, ejecución y capacidad para mitigar los riesgos asociados.

La clasificación constituye una actividad de interpretación final, la cual debe realizarse posterior al análisis de resultados, asegurando que la conclusión se base en:

- *Resultados cuantitativos obtenidos de las medidas*
- *Evidencia objetiva y verificable*
- *Identificación de brechas y causas*
- *Evaluación de la capacidad del control para mitigar el riesgo*

La clasificación se fundamenta en un enfoque secuencial basado en la medida de desempeño que permite verificar la existencia, implementación y formalización del control y la medida de efectividad que permite evaluar el funcionamiento real del control.

a) Niveles de clasificación

La clasificación del control se realiza considerando los siguientes niveles:

Tabla 19. *Niveles de clasificación de controles*

Nivel	***Clasificación***	***Descripción***
5	*Efectivo*	*El control existe, está formalizado, se ejecuta correctamente y mitiga riesgos*
4	*Efectivo no formalizado*	*El control existe y funciona adecuadamente, pero no se encuentra formalizado*
3	*Inefectivo(prueba)*	*El control existe y está formalizado, pero presenta fallas en su ejecución.*
2	*Inefectivo(diseño)*	*El control existe, pero su desempeño es inadecuado y no mitiga el riesgo*
1	*Control no existente*	*El control no ha sido implementado o no existe evidencia de su aplicación*

Fuente: Propia

b) Matriz de decisión

El enfoque de clasificación se determina respondiendo 4 preguntas secuenciales:

- *¿El control existe?*
- *¿Está formalizado?*
- *¿Se ejecuta correctamente?*
- *¿Cumple su propósito (mitiga el riesgo)?*

El flujo es consecuente de acuerdo a la siguiente tabla:

Tabla 20. *Matriz de decisión*

Paso	***Pregunta***	***Respuesta***	***Clasificación***
1	*¿El control existe?*	*NO*	*Control no existente*
2	*¿Está formalizado?*	*NO*	*Efectivo no formalizado*
3	*¿Se ejecuta correctamente?*	*NO*	*Inefectivo (prueba)*
4	*¿Cumple su propósito (mitiga el riesgo)?*	*NO*	*Inefectivo(diseño)*
Final	*Todas las anteriores son positivas*	*SI*	*Efectivo*

Fuente: Propia

Ejemplo práctico:

Caso 1:

Tabla 21. Ejemplo *- Clasificación de controles*

Medida	***¿El control existe?***	***¿Está formalizado?***	***¿Se ejecuta correctamente?***	***¿Cumple su propósito (mitiga el riesgo)?***	***Clasificación***
MED-SI-001	*SI*	*SI*	*NO*	*-*	*Inefectivo (prueba)*

Fuente: Propia

Clasificación: Inefectivo (prueba)

Caso 2:

Tabla 22. Ejemplo - *Clasificación de controles*

Medida	***¿El control existe?***	***¿Está formalizado?***	***¿Se ejecuta correctamente?***	***¿Cumple su propósito (mitiga el riesgo)?***	***Clasificación***
MED-SI-001	*SI*	*SI*	*SI*	*NO*	*Inefectivo (diseño)*

Fuente: Propia

Clasificación: Inefectivo (diseño)

4.2.9.6. Etapa 6: Revisar y mejorar

Asegurar la mejora continua del SGSI mediante la revisión de los resultados de medición, el análisis de lecciones aprendidas y la implementación de acciones de mejora sobre los controles, las medidas y el proceso de evaluación.

La mejora continua se basa en evidencia objetiva derivada del proceso de evaluación, para lo cual es indispensable:

a) Identificar lecciones aprendidas

Consiste en analizar los resultados obtenidos durante la evaluación para identificar oportunidad de mejora de los controles, procesos y método de medición.

b) Ajustes de medidas e indicadores

Corresponde a revisar la pertinencia, utilidad y aplicabilidad de las medidas definidas, ajustándoles en función a los resultados y la evolución del SGSI.

c) Actualización de controles

Consiste en fortalecer los controles de seguridad de la información en función de las brechas identificadas, asegurando su alineación con los riesgos y la normativa aplicable.

d) Mejora del proceso de medición

En necesario optimizar los mecanismos y análisis de datos para asegurar la calidad y confiabilidad de la información para:

- *Mejorar la recolección de datos*
- *Optimizar herramientas de medición*
- *Simplificar procesos operativos*
- *Fortalecer la trazabilidad de la información.*

4.2.9.7. Etapa 7: Retener y comunicar información

Con la finalidad de garantizar la trazabilidad, disponibilidad y comunicación efectiva de la información generada durante el proceso de evaluación del SGSI, y demostrando la información generada en las etapas:

- *Planificación*
- *Medición*
- *Análisis*
- *Clasificación*
- *Mejora continua*

El proceso de evaluación deberá mantener como mínimo los siguientes elementos en el repositorio definido para cada medida:

- *Matrices de evaluación de controles*
- *Formularios de recopilación y análisis de información*
- *Evidencias documentales y técnicas (logs, reportes, actas, capturas, etc.)*
- *Resultados de las medidas*
- *Clasificación de controles*
- *Registros de acciones de mejora*

La información deberá mantenerse disponible para fines de auditoría interna, externa y del organismo de control.

1. Presentación de reportes

La información generada como resultado del proceso de evaluación deberá ser presentada en formatos claros, comprensibles y alineados a las necesidades de las partes interesadas, a través de reportes ejecutivos que contengan, como mínimo:

- *Indicadores clave de desempeño*
- *Clasificación de la efectividad de los controles evaluados*
- *Recomendaciones estratégicas para el fortalecimiento y mejora continua*

4.3. Validación e implementación

4.3.1. Contexto del plan piloto

Con el propósito de validar la aplicabilidad y efectividad de la metodología propuesta, se lleva a cabo su implementación controlada en un caso de estudio o prueba polito real. Esta fase permite evidenciar que los criterios y fases definidas son claros, aplicables y consistentes.

A continuación, el contenido de la sección 4.3 corresponde a la aplicación de la metodología propuesta en la Cooperativa de Ahorro y Crédito Atuntaqui, institución del segmento 1, regulada por la Superintendencia de Economía Popular y Solidaria (SEPS).

4.3.2. Etapa 1: Planificación de la Evaluación

4.3.2.1. Identificación de la necesidad de la información

De conformidad con la normativa SEPS 2022-002, las instituciones del sector financiero popular y solidario deben implementar un conjunto de controles mínimos obligatorios relacionados con la gobernanza de la seguridad de la información y la gestión de riesgos.

En este contexto, y en función de la necesidad de desarrollar la ejecución del plan piloto, se establecen las siguientes necesidades de información:

***NI-001:** Determinar si la institución dispone de un marco integral de políticas de seguridad de la información que abarque los dominios establecidos por la normativa de*

la SEPS, y que dichas políticas se encuentren documentadas, formalizadas aprobadas, vigentes y alineadas con los objetivos.

NI-002: *Determinar si la institución realiza, con periodicidad anual, ejercicios prácticos y controlados de evaluación de seguridad (ethical hacking, pruebas de penetración u otras pruebas técnicas), que simulen escenarios reales de amenazas sobre infraestructura y aplicaciones críticas, y que sean ejecutadas por terceros independientes con experiencia acreditada.*

NI-004: *Determinar el grado en que las vulnerabilidades altas y críticas identificadas son remediadas dentro de los tiempos planificados, con el fin de evaluar la efectividad del proceso de gestión de vulnerabilidades y reducción del riesgo.*

4.3.2.2. Creación y mantenimiento de medidas

Una vez identificadas las necesidades de información y los lineamientos necesarios se establecen las siguientes medidas:

Tabla 23. Plan Piloto *- Definición de medida MED-SI-001*

Definición de la medida	
ID de la medida	*MED-SI-001*
Necesidad de la información asociada	*Determinar si la institución dispone de un marco integral de políticas de seguridad de la información que abarque los dominios establecidos por la normativa de la SEPS, y que dichas políticas se encuentren documentadas, formalizadas aprobadas, vigentes y alineadas con los objetivos.*
Control Evaluado	*Políticas de Seguridad de la Información*
Descripción de la medida	*Porcentaje de cobertura del marco de políticas de seguridad de la información respecto a los dominios exigidos por la normativa aplicable*
Fórmula o método de cálculo	*Número de criterios definidos y dominios de políticas de Seguridad de la Información cumplidos / Total de criterios definidos y dominios de políticas de Seguridad de la Información * 100*
Objetivo o meta de la medida	*Objetivo o meta de la medida* *Meta mínima >= 100% de cobertura normativa*

	Umbral aceptable >=90%
Método de evaluación	*EXAMINAR: Evidencia requerida* *ENTREVISTAR: Responsable de Seguridad de la Información*
Evidencia requerida	*Documentación de políticas aprobadas y vigentes* *Repositorio documental institucional* *Historial de versiones.* *Registro de difusión*
Frecuencia de medición	*Anual*
Partes responsables	*Titular de la información: Jefe de Seguridad de la Información* *Colector de información: Asistente de Seguridad de la Información* *Cliente de medición: Gerencia General / Comité de Seguridad de la Información*
Fuente de datos	*Repositorio documental institucional (interna).*
Forma de presentación o informe	*Indicador porcentual de cumplimiento*

Fuente: Propia

***Tabla 24. Plan Piloto** - Definición de medida MED-SI-002*

Definición de la medida	
ID de la medida	*MED-SI-002*
Necesidad de la información asociada	*Determinar si la institución realiza, con periodicidad anual, ejercicios prácticos y controlados de evaluación de seguridad (ethical hacking, pruebas de penetración u otras pruebas técnicas), que simulen escenarios reales de amenazas sobre infraestructura y aplicaciones críticas, y que sean ejecutadas por terceros independientes con experiencia acreditada.*
Control evaluado	*Gestión de vulnerabilidades*
Descripción de la medida	*Cumplimiento anual de la ejecución de pruebas técnicas de penetración*

Fórmula o método de cálculo	*Número de criterios cumplidos de la ejecución de pruebas técnicas de penetración / Total de criterios de la ejecución de pruebas técnicas de penetración * 100*
Objetivo o meta de la medida	*Objetivo o meta de la medida* *Optimo = 100%* *Aceptable > 90%*
Método de evaluación	*EXAMINAR: Evidencia requerida* *ENTREVISTAR: Oficial de Seguridad / Responsable de TI* *PROBAR: Validación de evidencia técnica inclinada en el informe*
Evidencia requerida	*Contrato con proveedor externo.* *Informe técnico de pentesting.* *Certificaciones del proveedor.* *Acta de recepción del servicio.* *Registro de presentación a la Gerencia General y Comité de administración de Riesgos Integrales* *Plan de mitigación de los hallazgos identificados*
Frecuencia de medición	*Anual*
Partes responsables	*Titular de la información: Jefe de Seguridad de la Información* *Colector de información: Asistente de Seguridad de la Información* *Cliente de medición: Gerencia General / Comité de Seguridad de la Información.*
Fuente de datos	*Reportes del proveedor externo (externa).* *Registro contractual (interna).* *Plan anual de seguridad (interna).*
Forma de presentación o informe	*Gráfico de barras para la presentación del cumplimiento del control*

Fuente: Propia

***Tabla 25. Plan Piloto** - Definición de medida MED-SI-004*

Definición de la medida	
ID de la medida	*MED-SI-004*
Necesidad de la información asociada	*Determinar el grado en que las vulnerabilidades altas y críticas identificadas son remediadas dentro de los tiempos planificados, con el fin de evaluar la efectividad del proceso de gestión de vulnerabilidades y reducción del riesgo.*
Control evaluado	*Gestión de vulnerabilidades*
Descripción de la medida	*Porcentaje de activos con vulnerabilidades altas y críticas remediadas dentro del tiempo planificado con respecto al total de vulnerabilidades altas y críticas detectadas.*
Fórmula o método de cálculo	*Número de activos con vulnerabilidades altas y críticas remediadas/Total de activos con vulnerabilidades altas y críticas detectadas x 100*
Objetivo o meta de la medida	*Meta ideal >90%* *Umbral aceptable >80%* *Nivel crítico < 80%*
Método de evaluación	*EXAMINAR: Evidencia requerida* *ENTREVISTAR: Responsable de Seguridad de la Información* *PROBAR: Ejecución del análisis de verificación retest*
Evidencia requerida	*Informe técnico de pentesting* *Informe técnico de retest* *Reporte y seguimiento de remediaciones*
Frecuencia de medición	*Semestral*
Partes responsables	*Titular de la información: Jefe de Seguridad de la Información* *Colector de información: Asistente de Seguridad de la Información* *Cliente de medición: Comité de Seguridad de la Información / Comité de Administración Integral de Riesgos*
Fuente de datos	*Reportes de pentest (interna/ externa)*

Forma de presentación o informe	*Tablero de tendencia por periodo*

Fuente: Propia

4.3.2.3. Priorización de implementación

Tabla 26. Plan Piloto - *Priorización de implementación*

ID	***Medida***	***Tipo de medida***	***Criterio de priorización***	***Prioridad***	***Implementación***
MED-SI-001	*Porcentaje de cobertura del marco de políticas de seguridad de la información respecto a los dominios exigidos por la normativa aplicable*	*DESEMPEÑO*	*Requeridas por normativa o asociadas a riesgos críticos*	*ALTA*	*Inmediata*
MED-SI-002	*Cumplimiento anual de la ejecución de pruebas técnicas de penetración*	*DESEMPEÑO*	*Requeridas por normativa o asociadas a riesgos críticos*	*ALTA*	*Inmediata*
MED-SI-004	*Determinar el grado en que las vulnerabilidades altas y críticas identificadas son remediadas dentro de los tiempos planificados, con el fin de evaluar la efectividad del proceso de gestión de vulnerabilidades y reducción del riesgo.*	*EFECTIVIDAD*	*Requeridas por normativa o asociadas a riesgos críticos*	*ALTA*	*Inmediata*

Fuente: Propia

4.3.3. Etapa 2: Definición del procedimiento de medición

El diseño de los formularios para la recopilación y análisis de información se presentan durante la ejecución del plan piloto (ver Anexo B).

4.3.4. Etapa 3: Monitorear y medir

La ejecución de los métodos de evaluación se desarrolla a partir de los formularios diseñados en la Etapa 2. (ver Anexo B).

4.3.5. Etapa 4: Análisis de resultados

***Tabla 27. Plan Piloto -** Análisis de resultados*

Medida	***Resultado***	***Objetivo***	***Estado***
MED-SI-001	*95%*	*100%*	*Brecha del 5%, dentro del umbral aceptable definido en la etapa 1 Creación y Mantenimiento de la medida (Tabla 21 – Plan Piloto - Definición de medida MED-SI-001)*
MED-SI-002	*100%*	*100%*	*Sin desviación*
MED-SI-004	*96%*	*90%*	*El resultado de la medición supera el objetivo establecido.*

Fuente: Propia

***Tabla 28. Plan Piloto -** Análisis de Causas*

Medida	***Desviación***	***Tipo***	***Causa***
MED-SI-001	*5%*	*Proceso*	*No se especifica en ninguna política la revisión cuando ocurran cambios normativos o estructurales que afecten su contenido* *Según el estándar internacional NIST se debe definir la frecuencia de revisión y eventos que requieran revisión y actualización, de acuerdo con la ISO/IEC 27001:2022 en las Clausula 5.2 y 10 se establece que la política debe: Mantenerse como información documentada, ser revisada cuando sea necesario, mantener sea adecuación, pertinencia y eficacia*

			La normativa vigente de la SEPS establece que las políticas deben estar actualizadas, se ajusten a cambios regulatorios y sean coherentes con disposiciones vigentes.

Fuente: Propia

4.3.6. Etapa 5: Clasificación de efectividad de los controles

Tabla 29. Plan Piloto - *Clasificación de efectividad de los controles*

Medida	***¿El control existe?***	***¿Está formalizado?***	***¿Se ejecuta correctamente?***	***¿Cumple su propósito (mitiga el riesgo)?***	***Clasificación***
MED-SI-004	***SI*** *(Se determina la implementación a través de la medida de desempeño MED-SI-002)*	***SI*** *(Se detalla la evidencia en el formulario de recopilación y análisis de información MED-SI-002)*	***SI*** *(No presenta brechas o desviaciones en el análisis de resultados de la MED-SO-002)*	***SI*** *(Reduce el grado de riesgo al disminuir el número de activos con vulnerabilidades altas y críticas)*	***Efectivo***

Fuente: Propia

4.3.7. Etapa 6: Revisar y mejorar

a) Identificación de lecciones aprendidas

- *Falta de ejecución consistente de controles*
- *Debilidades en la gestión de cambios*
- *Limitada trazabilidad en algunos procesos*
- *Falta de estandarización en criterios de evaluación*

b) Ajustes realizados

- *Refinamiento de criterios de evaluación*

c) Mejora del proceso de medición

- *Se optimizó el proceso de medición en base a la experiencia del plan piloto*

Resultados:

- *Disminución del tiempo de evaluación fortaleciendo el **Formulario de recopilación y análisis de información**.*

d) *Conclusión del plan piloto*

- *Los resultados del plan piloto evidencian que la institución cuenta con un nivel adecuado de formalización de controles de seguridad de la información, sin embargo, se identifican oportunidades de mejora en su ejecución y efectividad, lo que justifica su implementación de acciones correctivas y el fortalecimiento del modelo de medición.*

4.3.8. Etapa 7: Retener y comunicar información

Durante la ejecución del plan piloto, se consolidó un repositorio estructurado por medida, con los siguientes resultados:

***Tabla 30. Plan Piloto -** Retención y comunicación de información*

Elemento	***Resultado***
Medidas	*3*
Controles evaluados	*2*
Formularios generados	*3*
Evidencias recopiladas	*23*
Registros de mejora generados	*1*

Fuente: Propia

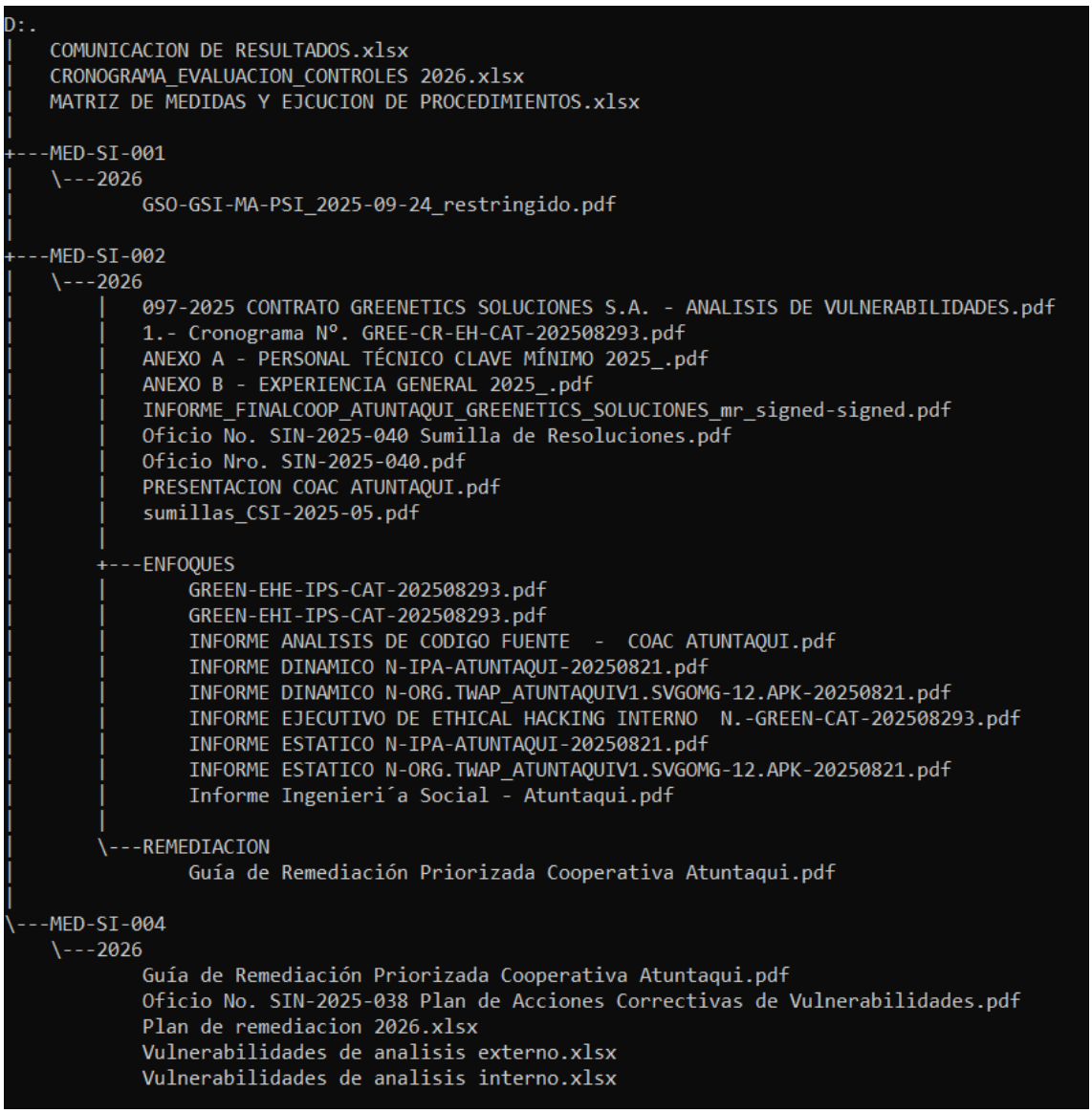


Figura 8. Plan Piloto - *Repositorio de Medición y Evidencias*

Fuente: Propia

La información generada durante el plan piloto evidenció la necesidad de establecer controles de gestión documental, considerando:

- *Organizado por:*
  - *ID de medida*
  - *Fecha de evaluación*
  - *Responsables*
- *Respaldo de información*
- *Integridad y disponibilidad de las evidencias*

4.3.8.1. Presentación

Con la finalidad de comunicar el proceso de evaluación de manera clara, estructurada y alineada a las necesidades de las partes interesadas se presenta lo siguiente:

a) Reporte ejecutivo

Contenido:

- *Indicadores clave de desempeño*
- *Indicadores de efectividad*
- *Clasificación de controles*
- *Brechas identificadas*
- *Recomendaciones estratégicas*

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

La investigación desarrollada permitió analizar los principales referentes teóricos relacionados con la evaluación de controles de seguridad de la información, identificando que los estándares proporcionan lineamientos complementarios para la implementación, medición y evaluación de controles dentro de un SGSI. Sin embargo, también se evidenció que, a pesar de contar con marcos sólidos, aún existe una brecha en la aplicación práctica, especialmente en lo relacionado con la medición de la eficacia de los controles.

El desarrollo de la metodología permitió establecer de forma clara un conjunto de fases, criterios y herramientas orientadas a evaluar y determinar el nivel de eficacia de los controles de seguridad de la información, alineadas tanto a estándares internacionales y normativos como SEPS 2022-002, e incorpora indicadores y criterios de evaluación que facilitan la obtención de resultados objetivos, lo que permite su aplicación y adaptación en distintas instituciones del sector.

La aplicación de la metodología, mediante la evaluación del control de políticas de seguridad de la información permitió evidenciar que la institución seleccionada cuenta con una estructura formal, documentada y alineada con la normativa SEPS 2022-002 alcanzando el 95% de desempeño, la brecha del 5% representa una oportunidad de mejora en la definición de eventos de actualización frente a cambios normativos y organizacionales.

La evaluación de efectividad de un control parte de una evaluación previa de desempeño, la cual debe demostrar su existencia y correcta ejecución, esto se reflejó a través del desempeño favorable del control de gestión de vulnerabilidades, posteriormente la remediación y el retest permitieron medir su efectividad alcanzando un 94%, al determinar el grado de vulnerabilidades corregidas conforme a la planificación el resultado confirma la adecuada implementación, formalización y ejecución del control, así como la reducción del nivel de riesgo.

5.2. Recomendaciones

Se recomienda socializar a los responsables de seguridad de la información y áreas involucradas del sector financiero popular y solidario en el uso de la metodología propuesta, con el fin de asegurar su correcta aplicación, interpretación de resultados y aprovechamiento como herramienta para la gestión efectiva de controles.

Asimismo, se sugiere fortalecer el proceso de medición de los controles de seguridad de la información mediante la aplicación del ciclo de mejora continua Planificar, Hacer, Verificar y Actuar (PDCA), conforme a lo establecido en la norma ISO/IEC 27001:2022, a fin de garantizar la evaluación sistemática y la optimización permanente de los controles implementados.

Finalmente, se recomienda a la Cooperativa de Ahorro y Crédito Atuntaqui formalizar, socializar e integrar la metodología dentro de su proceso de gestión de riesgos, con el objetivo de fortalecer su administración y obtener resultados precisos sobre la exposición al riesgo inherente de sus activos de información, permitiendo así orientar eficientemente los recursos hacia aquellos controles que, de acuerdo con el análisis, lo requieran prioritariamente.

REFERENCIAS

Cadena Oleas, B. N. (2025). La ciberseguridad como pilar en la transformación digital de las cooperativas de ahorro y crédito. https://doi.org/10.56519/tvh0dh66

Corozo, K. E. (2023). Modelo de evaluación madurez de gestión de seguridad de la información en centros de datos. https://doi.org/10.48190/cumbres.v9n1a3

Cortez C. M. (2024). Guía del docente. Seguridad de la información: (1 ed.). Tecnológico Universitario Espíritu Santo - TES. https://elibro.net/es/ereader/utnorte/284787?page=6

Cortés, J. M. (2024). Sistemas de gestión de seguridad de la información (ISO 27001:2022): (1 ed.). Editorial ICB. https://elibro.net/es/ereader/utnorte/283864?page=42

Ley Orgánica de Protección de Datos Personales. (2021). Asamblea Nacional. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Hadi, H. J., Ahmad, N., Aziz, K., Cao, Y., & Alshara, M. A. (2024). Cost-effective resilience: A comprehensive survey and tutorial on assessing open-source cybersecurity tools for multi-tiered defense. IEEE Access, 12, 194053–194076. https://doi.org/10.1109/ACCESS.2024.3510533

Hernández, M. (2022). Situación de los servicios financieros digitales, la seguridad de la información y ciberseguridad en el sector financiero popular y solidario. X-Pedientes Económicos, 6(14), 18–32.

Organización Internacional de Normalización. (2022). ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la intimidad - Sistemas de gestión de la seguridad de la información - Requisitos. https://www.iso.org/standard/82875.html

Organización Internacional de Normalización NIST. (2016). ISO/IEC 27004:2016 Tecnologías de la Información - Técnicas de Seguridad - Gestión

de la Seguridad de la Información - Monitoreo, Medición, Análisis y Evaluación. https://www.iso.org/standard/64120.html

IT Ahora. (2025, mayo 6). Cinco años de ciberseguridad en Ecuador: una mirada a las tendencias. IT Ahora. https://itahora.com/2025/05/06/cinco-anos-de-ciberseguridad-en-ecuador-una-mirada-a-las-tendencias/

IT Ahora, Deloitte. (2023). Estado Actual Ciberseguridad Ecuador 2023. https://content.bhybrid.com/publication/6bede106/mobile/

ISACA. (2018). COBIT 2019: Objetivos de gobierno y gestión. https://es.scribd.com/document/604524662/COBIT-2019

Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T. (2023). Controles de ciberseguridad en centrales nucleares mediante metodología de evaluación técnica. IEEE Access, 11, 15229–15241. https://doi.org/10.1109/ACCESS.2023.3244991

Kaspersky. (2023, agosto 23). Panorama de amenazas en América Latina 2023. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Ko, A., Lee, J. H., & Seo, J. T. (2025). KPI-based evaluation framework for cyber resilience of ships. IEEE Access, 13, 64226–64245. https://doi.org/10.1109/ACCESS.2025.3550501

Kudriavtseva, A. (2024). A software security evaluation framework. En 2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion) (pp. 150–152). https://doi.org/10.1145/3639478.3639796

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber security maturity assessment framework for technology startups: A systematic literature review. IEEE Access, 11, 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., De Sousa Júnior, R. T., & Nunes, R. R. (2021). Performance euation of cybersecurity controls of the NIST

framework using a constructivist multicriteria methodology. IEEE Access, 9, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178

National Institute of Standards and Technology. NIST (2022). Assessing security and privacy controls in information systems and organizations (NIST Special Publication 800-53A Rev. 5). https://doi.org/10.6028/NIST.SP.800-53Ar5

Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. International Journal of Science and Research Archive, 11(1), 1968–1983. https://doi.org/10.30574/ijsra.2024.11.1.0267

Pérez Rodríguez, (2025). Seguridad de la información y ciberseguridad en la empresa. Editorial ICB. https://elibro.net/es/ereader/utnorte/283847?page=10

Ramírez, A. del P., Urrutia, J. A., Lach, W. (2025). El control interno de las cooperativas de ahorro y crédito del segmento 4 de Chimborazo. Noesis. Revista Electrónica de Investigación, 7(1), 307–327. https://doi.org/10.35381/noesisin.v7i1.386

Revista IT & Consultora Deloitte. (2024). Estado actual de la ciberseguridad Ecuador 2024.

Superintendencia de Economía Popular y Solidaria. (2022). Norma de control para la gestión de la seguridad de la información en las entidades del sector financiero popular y solidario. Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002. https://www.seps.gob.ec

Torres, H. (2021). Propuesta de metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas. https://repositorio.ucenfotec.ac.cr/handle/123456789/383

Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. http://dx.doi.org/10.15381/rpcs.v2i2.17103

Zhuo, P., & Jin, L. (2025). Decision model for information security control assessment for hospitals using disc picture fuzzy information. IEEE Access, 13, 100307–100316. https://doi.org/10.1109/ACCESS.2025.3577220

ANEXOS

Anexo A. Solicitud para realizar tesis de grado

Atuntaqui, 06 de 05 del 2026

Magister
Jenny Maldonado
Gerente General
COOPERATIVA DE AHORRO Y CRÉDITO "ATUNTAQUI" LTDA.
Presente

Estimada Magister:

Yo, Jefferson Esteban Andrade Pijuango, con cédula de identidad N° 100365341-5, en calidad de estudiante de la Maestría en Computación con mención en Seguridad Informática, me permito solicitar de la manera más comedida se sirva autorizar a quien corresponda la aplicación de la propuesta metodológica orientada a fortalecer la gestión de Seguridad de la Información en la institución, derivada de mi trabajo de investigación con el tema: **"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)".**

En tal virtud, se adjunta la documentación que respalda la presente solicitud, consistente en el certificado de inicio y finalización de la maestría otorgado por la Facultad de Posgrado de la Universidad Técnica del Norte, el anteproyecto desarrollado y la certificación de aprobación del tema de investigación.

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

Atentamente,

JEFFERSON ESTEBAN ANDRADE PIJUANGO
Firmado digitalmente por JEFFERSON ESTEBAN ANDRADE PIJUANGO
Fecha: 2026.05.06 12:45:12 -05'00'

Ing. Jefferson Andrade
CI: 1003653415

Anexo B. Formularios de recopilación y análisis de información del plan piloto.

Formulario de recopilación y análisis de información			
1. Información general			
Fecha de evaluación:	11/03/2026		
Evaluador:	Jefferson Andrade		
ID de la Medida:	MED-SI-001		
Control evaluado	Políticas de Seguridad		
Frecuencia	Anual		
Responsable / Entrevistado:	Wilson Cardenas		
Cargo:	Jefe de Seguridad de la Información		
2. Necesidad de la información			
Determinar si la entidad:			
Determinar si la institución dispone de un marco integral de políticas de seguridad de la información que abarque los dominios establecidos por la normativa de la SEPS, y que dichas políticas se encuentren documentadas, formalizadas aprobadas, vigentes y alineadas con los objetivos.			
3. Métodos de evaluación aplicados			
Examinar	Documentación de políticas aprobadas y vigentes Repositorio documental institucional Historial de versiones. Registro de difusión		
Entrevistar	Responsable de Seguridad de la Información		
4. Evaluación del margo general de políticas (Fuente: Criterios de evaluación de la NIST 800-53A			
N	**Criterio de evaluación**	**Cumple (S/P/N)**	**Evidencia**
1	¿Existe un marco formal que agrupe las políticas de seguridad de la información?	S	Documento de Manual de Políticas de Seguridad de la Información (MPSI) Código GSO-GSI-MA-PSI, formalizado y publicado en el repositorio institucional.
2	¿Se designó responsable formal para el desarrollo, documentación y difusión?	S	Dentro del MPSI en la Política 2 se establece al Oficial de Seguridad de la Información como responsable de revisar y actualizar anualmente las políticas de Seguridad de la Información, mismas que deberán ser analizadas por el Comité de Seguridad de la Información, aprobadas por el Consejo de Administración y difundidas a todos los trabajadores.
3	¿Las políticas están formalmente aprobadas por autoridad competente?	S	Cumple un proceso de revisión por parte de Comité de Seguridad de la Información y aprobación por el Consejo de Administración.
4	¿Las políticas se encuentran vigentes?	S	Documento vigente desde el 24 de Septiembre del 2025con la certificación del Consejo de Administración de la Cooperativa, en sesión extraordinaria realizada en la fecha indicada, según Acta Nro. CAD-2025-34
5	¿Se definen eventos de actualización como cambios normativos y regulatorios?	N	

6	¿Existe control de versiones?	S	Control de versiones evidenciable a través del sistema WebCoop Módulo de Manuales de Procedimientos, así mismo el documento MPSU cuenta con un registro de cambios que detalla la versión, fecha, sección, tipo de cambio y responsable de la elaboración o actualización.
7	¿Las políticas están alineadas con los objetivos estratégicos institucionales?	S	Uno de los objetivos estratégicos institucionales es conservar un adecuado nivel de satisfacción del socio y cliente (interno y externo) para lo cual en el Capítulo IV. Alcance del Manual de Políticas de Seguridad de la Información establece mantener un adecuado cumplimiento de funciones y se encuentren a disposición de socios , clientes y terceros
8	¿Las políticas están correctamente detalladas (no son genéricas)?	S	Las políticas se encuentran correlacionadas de acuerdo a cada uno de los dominios contemplados para su implementación
9	¿Las políticas tienen coherencia con la normativa SEPS y otras regulaciones?	S	El documento presente el Marco Normativo y Referencial en su capitulo II, de esta manera abarca lineamientos con especto a la administración de riesgo operativo, control respecto a la Seguridad de la Información, seguridad en el uso de canales Electrónicos y su reforma pertinente.

5. Evaluación de cobertura por dominio normativo

¿Confirma que existen políticas formalmente documentadas, aprobadas y vigentes para los siguientes dominios?

N	**Revisión por Dominio**	**Confirmación (S/P/N)**	**Evidencia (Políticas de Seguridad de la Información)**
1	Seguridad de la información	S	Sección del Capítulo V Contexto de la Organización que contiene la Política General de Seguridad de la Información, Roles y Responsabilidades de Seguridad de la Información, Responsables de la información, entidades externas
2	Clasificación de información	S	Sección Gestión de los Activos, Políticas N 34, 35, 36 del MPSI
3	Gestión de riesgos	S	Sección Administración de la continuidad del negocio conforme a la Normativa de Gestión de Riesgo Operativo, Políticas N 74, 75, 76, 77.
4	Control de accesos	S	Sección de Control de Accesos del MPSI en las políticas N 49, 50, 51, así como también en el Capítulo IX Autenticación Segura - Control de Accesos, Gestión de accesos de usuarios, responsabilidades del usuario, Sistema de gestión de claves y Control de acceso a redes
5	Gestión de incidentes	S	Sección Administración de Incidentes de Seguridad, Políticas N 68, 69, 70, 71, 72, 73.
6	Gestión de software	S	Con respecto a dominio siguiente se gestiona dos perspectivas que comprenden la adquisición de software en la Política N 5, Protección Contra Software Malicioso en las Políticas N 145, 146, 147, la Instalación de Software en sistemas operativos en las políticas 176, 177, 178. Finalmente en la sección de gestión de cambios Política N 198. donde se indica que el software debe estar sujeto a un proceso de aceptación, donde se realizasen las pruebas respectivas que deben estar documentadas antes de entrar a producción.
7	Infraestructura tecnológica	S	Dominio contemplado en el capítulo VIII Controles Tecnológicos, que contempla Ciberseguridad, Gestión de Operaciones y comunicaciones, Configuraciones para Servidores y dispositivos de punto final de usuario.

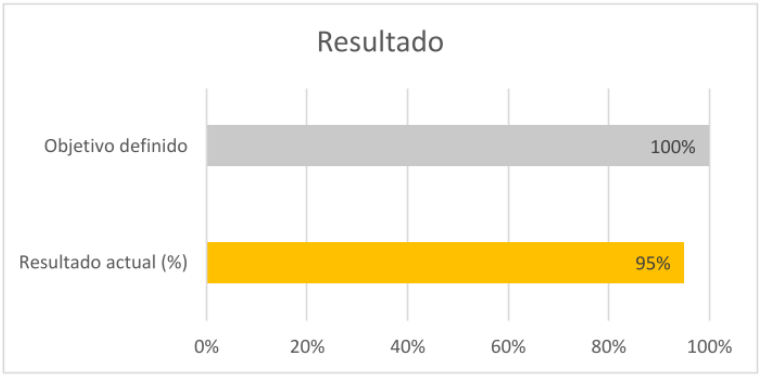
8	Seguridad RRHH	S	Dominio establecido en el capítulo VI Controles de Personas Antes del empleo, Durante el empleo, Faltas y Sanciones, Terminación o cambio de empleo
9	Seguridad física	S	Sección del Capítulo VII Controles físicos con contiene controles para Áreas Seguras, Monitoreo, Protección contra amenazas físicas y ambientales, emplazamiento y control de equipos.
10	Gestión con terceros	S	Sección de Seguridad de la información en las relaciones con los proveedores Políticas N 63.
11	Ciberseguridad	S	Sección establecida de Ciberseguridad, Gestión de Operaciones y Comunicaciones contemplado en el Capítulo VIII Controles Tecnológicos

6. Fórmula o método de cálculo	
Fórmula de cálculo:	Número de criterios definidos y dominios de políticas de Seguridad de la Información cumplidos / Total de criterios definidos y dominios de políticas de Seguridad de la Información * 100

Registro de datos	
Variable	**Resultado**
Número de criterios y dominios evaluados	20
Número de criterios y dominios cumplidos	19
Número de criterios y dominios no cumplidos	1
Resultado actual (%)	**95%**
Objetivo definido	**100%**

8. Presentación

Indicador porcentual de cumplimiento



JEFFERSON ESTEBAN ANDRADE PIJUANGO
Firmado digitalmente por JEFFERSON ESTEBAN ANDRADE PIJUANGO
Fecha: 2026.04.28 00:41:21 -05'00'

Jefferson Andrade
Evaluador

WILSON ANIBAL CARDENAS HERNANDEZ
Firmado digitalmente por WILSON ANIBAL CARDENAS HERNANDEZ
Fecha: 2026.04.28 08:22:32 -05'00'

Wilson Cárdenas
Jefe de Seguridad de la Información

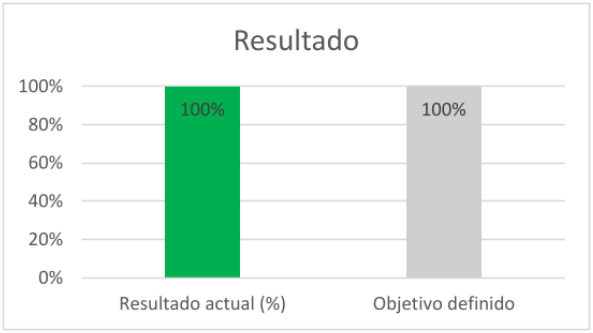
Formulario de recopilación y análisis de información	
1. Información general	
Fecha de evaluación:	11/03/2026
Evaluador:	Jefferson Andrade
ID de la Medida:	MED-SI-002
Control evaluado	Gestión de vulnerabilidades
Frecuencia	Anual
Responsable / Entrevistado:	Wilson Cardenas
Cargo:	Jefe de Seguridad de la Información
2. Objetivo	
Determinar si la institución realiza, con periodicidad anual, ejercicios prácticos y controlados de evaluación de seguridad (ethical hacking, pruebas de penetración u otras pruebas técnicas), que simulen escenarios reales de amenazas sobre infraestructura y aplicaciones críticas, y que sean ejecutadas por terceros independientes con experiencia acreditada.	
3. Métodos de evaluación aplicados	
Examinar	Contrato con proveedor externo. Informe técnico de pentesting. Certificaciones del proveedor. Acta de recepción del servicio. Registro de presentación a la Gerencia General y Comité de administración de Riesgos Integrales Plan de mitigación de los hallazgos identificados
Entrevistar	Responsable de Seguridad de la Información
Probar	Validación de evidencia técnica inclinada en el informe

4. Validación del cumplimiento del control (Fuente: Criterios de evaluación de la NIST 800-53A

N	Criterio de evaluación	Cumple (S/P/N)	Evidencia
1	¿La entidad ejecutó pruebas técnicas de seguridad durante el periodo evaluado?	S	Conforme a las disposiciones normativas se realizó el Análisis de Vulnerabilidades y Pruebas de penetración con la empresa externa Greenetics Soluciones S.A durante el año 2025 conforme el contrato N. 097-2025
2	¿Las pruebas fueron realizadas por un proveedor externo independiente?	S	De acuerdo al contrato N. 097-2025 se establece realizar el Análisis de Vulnerabilidades y Pruebas de penetración con la empresa externa Greenetics Soluciones S.A
3	¿El proveedor acredita experiencia comprobable en pruebas de seguridad?	S	A través del líder del proyecto presenta Certificados de experiencia como Consultor senior en seguridad informática en proyectos relacionados a Ethical Hacking, la información se encuentra detallada en el ANEXO A - PERSONAL TÉCNICO CLAVE MÍNIMO 2025 y ANEXO B - EXPERIENCIA GENERAL 2025
4	¿El proveedor cuenta con certificaciones técnicas relevantes?	S	Conforme al anexo ANEXO A - PERSONAL TÉCNICO CLAVE MÍNIMO 2025 los responsables del proyecto presentan Certificados de seguridad tales como Ethical Hacker, Offensive Security Wireless Professional, ISO IEC 27032, Herramientas como ARCSIGHT, SOCRADAR, ITIL FUNDATION 4.0, entre otros.
5	¿Existe contrato o documento formal que respalde el servicio prestado?	S	Mediante el contrato N. 097-2025 desde el 01 de julio de 2025 se autoriza legalmente la ejecución del proyecto "Análisis de vulnerabilidades y pruebas de penetración a activos de información de la Cooperativa de Ahorro y Crédito Atuntaqui Ltda."

6	¿El informe técnico final se encuentra formalmente emitido y firmado?	S	Mediante el informe final INFORME_FINALCOOP_ATUNTAQUI _GREENETICS_SOLUCIONES_mr_signed-signed se detallan los servicios adquiridos por la empresa contratada y aceptación del responsable interno del proyecto.
7	¿El informe identifica vulnerabilidades en infraestructura o aplicaciones?	S	Los resultados específicos en el INFORME_FINALCOOP_ATUNTAQUI _GREENETICS_SOLUCIONES_mr_signed-signed son presentados por componente, Evaluación externa, Evaluación Interna, Aplicación Móvil, Homebanking (Análisis de código), Ingeniería social.
8	¿Los resultados fueron presentados a la alta dirección o Comité de Seguridad?	S	Mediante en informe mensual del mes de Octubre mediante el Oficio Nro. SIN-2025-040 pág. 16 dirigido a la Gerencia General se presenta el Responsable de Seguridad de la Información dando a conocer la ejecución del proyecto, indicando generalmente los hallazgos obtenidos Adicionalmente de manera específica se da a conocer el informe de pruebas de vulnerabilidades de la plataforma Cooperativa Virtual y sitio web al Conté de Seguridad de la Información generando de esta forma la resolución : Resolución: CSI-2025-06-03 Una vez efectuada la revisión pertinente, se resuelve dar por conocido y aprobado el Informe de Análisis de Vulnerabilidades del Sitio Web y Cooperativa Virtual, conforme recomendación de Auditoría Externa AE-2025-00001 y resolución del Comité de Seguridad de la Información CSI-2025-05-03. el 23 de diciembre del 2025
5. Validación técnica del informe			
Se evidencia que se cumplió el ejercicio de análisis de vulnerabilidades			
N	**Criterio técnico**	**Cumple (S/P/N)**	**Evidencia**
1	El informe describe el alcance de las pruebas realizadas	S	De acuerdo al informe final INFORME_FINALCOOP_ATUNTAQUI _GREENETICS_SOLUCIONES_mr_signed-signed entregado se establece el alcance de los trabajos, indicando el número de activos evaluados sobre la infraestructura interna, externa, aplicaciones y usuarios finales.
2	El informe incluye metodología aplicada (OWASP, PTES, NIST u otra)	S	De acuerdo al informe final se aplican las metodologías OWAST v4.2, MITRE ARR&CK, NNIST SP-800-115, PTES
3	Se presentan evidencias técnicas de explotación de vulnerabilidades	S	Los enfoques: interno, externo, aplicaciones y usuarios presentan un informe en particular a detalle de los hallazgos y explotación de vulnerabilidades ejecutado. Se detallan los informes presentados: - GREEN-EHE-IPS-CAT-202508293 - GREEN-EHI-IPS-CAT-202508293 - INFORME ANALISIS DE CODIGO FUENTE - COAC ATUNTAQUI - INFORME DINAMICO N-IPA-ATUNTAQUI-20250821 - INFORME DINAMICO N-ORG.TWAP_ATUNTAQUIV1.SVGOMG-12.APK-20250821 - INFORME EJECUTIVO DE ETHICAL HACKING INTERNO N.-GREEN-CAT-202508293 - INFORME ESTATICO N-IPA-ATUNTAQUI-20250821 - INFORME ESTATICO N-ORG.TWAP_ATUNTAQUIV1.SVGOMG-12.APK-20250821 - Informe Ingeniería Social - Atuntaqui
4	Los hallazgos incluyen recomendación de mitigación	S	Dentro de los entregables del proveedor se incluye el documento Guía de Remediación Priorizada Cooperativa Atuntaqui

5	Existe clasificación de severidad (crítica, alta, media, baja)	S	Mediante la presentación "PRESENTACION COAC ATUNTAQUI" y documentación entregada por parte del proveedor se evidencian los Resultados del Ethical Hacking de hallazgos catalogados y diferenciados por nivel de riesgo, Bajo, Medio, Alto y Crítico. Adicional, todos son informes de evidencias citados presentan clasificación del riesgo por su criticidad.
6	Existe documentación formal de la entrega del análisis y ejecución del proyecto	S	Mediante la formalización del informe final INFORME_FINALCOOP_ATUNTAQUI _GREENETICS_SOLUCIONES_mr_signed-signed se evidencia la aceptación y constancia ratificando la responsabilidad de las partes, firmado el 6 de octubre del 2025
7	Se desarrolla un plan anual de remediación de los hallazgos obtenidos	S	Se desarrolla la planificación anual de remediación de vulnerabilidades mismo que es presentado al Comité de Seguridad de la Información el 23 de diciembre de 2025 generando la siguiente resolución: Resolución: CSI-2025-06-05 Una vez efectuada la revisión pertinente, se resuelve dar por conocido el Plan de Acciones Correctivas de Vulnerabilidades detectadas en el Test de Intrusión 2025, conforme recomendación No. AI-2025-00080 de Auditoría Interna.

6. Medición del indicador	
Fórmula de cálculo:	Número de criterios cumplidos de la ejecución de pruebas técnicas de penetración / Total de criterios de la ejecución de pruebas técnicas de penetración * 100
Registro de datos	
Variable	**Resultado**
Número de criterios evaluados	15
Número de criterios cumplidos	15
Número de criterios no cumplidos	0
Resultado actual (%)	**100%**
Objetivo definido	**100%**
8. Presentación	
Indicador porcentual de cumplimiento	

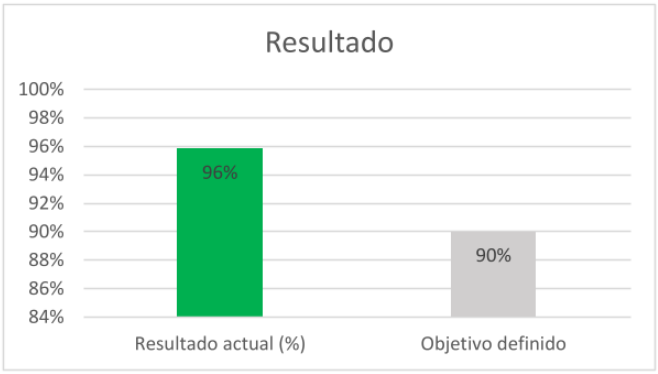
JEFFERSON ESTEBAN ANDRADE PIJUANGO
Firmado digitalmente por JEFFERSON ESTEBAN ANDRADE PIJUANGO
Fecha: 2026.04.28 00:42:17 -05'00'

Jefferson Andrade
Evaluador

WILSON ANIBAL CARDENAS HERNANDEZ
Firmado digitalmente por WILSON ANIBAL CARDENAS HERNANDEZ
Fecha: 2026.04.28 08:23:40 -05'00'

Wilson Cárdenas
Jefe de Seguridad de la Información

Formulario de recopilación y análisis de información			
1. Información general			
Fecha de evaluación:	27/04/2026		
Evaluador:	Jefferson Andrade		
ID de la Medida:	MED-SI-004		
Control evaluado	Gestión de vulnerabilidades		
Frecuencia	Semestral		
Responsable / Entrevistado:	Wilson Cardenas		
Cargo:	Jefe de Seguridad de la Información		
2. Necesidad de la información			
Determinar el grado en que las vulnerabilidades altas y críticas identificadas son remediadas dentro de los tiempos planificados, con el fin de evaluar la efectividad del proceso de gestión de vulnerabilidades y reducción del riesgo.			
3. Métodos de evaluación aplicados			
Examinar	Informe técnico de pentesting Informe técnico de retest Reporte y seguimiento de remediaciones		
Entrevistar	Responsable de Seguridad de la Información		
Probar	Ejecución de retest para conformar cierre de vulnerabilidades		
4. Evaluación del proceso de remediación de vulnerabilidades			
N	**Criterio de evaluación**	**Cumple (S/P/N)**	**Evidencia**
1	¿Las vulnerabilidades están clasificadas según criticidad (CVSS)?	S	De acuerdo a la revisión de los reportes Vulnerabilidades de analisis interno y externo se evidencia que cada vulnerabilidad cuenta está catalogada por su severidad, posee la descripción, resumen, remediación, puntuación base CVSS y el numero CVE
2	¿Existe una planificación de remediación de vulnerabilidades?	S	Conforme al Oficio No. SIN-2025-038 se formaliza el Plan de Acciones Correctivas de Vulnerabilidades
3	¿Se asignan responsables para la remediación?	S	Cada activo de información se encuentra asignado a un responsable, información detallada en el Oficio No. SIN-2025-038 Plan de Acciones Correctivas de Vulnerabilidades
4	¿Se realiza seguimiento del estado de las vulnerabilidades (retest)?	S	Se realiza el seguimiento del estado de las vulnerabilidades a traves del análisis de vulnerabilidades denominado retest.
5	¿Se valida técnicamente el nuevo analisis de vulnerabilidades (retest)?	S	De acuerdo al contrato N. 097-2025 se establece realizar el retest con la empresa externa Greenetics Soluciones S.A, durante la medida MED-SI-002 se validó la información documental del control evaluado.
6. Medición del indicador			
Fórmula de cálculo:	Número de activos con vulnerabilidades altas y críticas remediadas/Total de activos con vulnerabilidades altas y críticas detectadas x 100		
Registro de datos			
Variable	**Resultado**		

Número de activos con vulnerabilidades altas y críticas	24
Número de activos demediados	23
Periodo	Abril
Resultado actual (%)	**96%**
Objetivo definido	**90%**
8. Presentación	
Indicador porcentual de cumplimiento	

JEFFERSON ESTEBAN ANDRADE PIJUANGO
Firmado digitalmente por JEFFERSON ESTEBAN ANDRADE PIJUANGO
Fecha: 2026.04.28 00:43:03 -05'00'

Jefferson Andrade
Evaluador

WILSON ANIBAL CARDENAS HERNANDEZ
Firmado digitalmente por WILSON ANIBAL CARDENAS HERNANDEZ
Fecha: 2026.04.28 08:24:19 -05'00'

Wilson Cárdenas
Jefe de Seguridad de la Información

Anexo C. Constancia de validación de expertos

CONSTANCIA DE VALIDACIÓN DE EXPERTO

NOMBRE DEL EXPERTO: Roberto Santiago Portilla Proaño
ESPECIALIDAD: Seguridad Informática
CÉDULA DE IDENTIDAD: 1002433058

Por medio del presente, informo que realicé la revisión de la tesis con tema de **"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)"**, elaborado por el Ing. Jefferson Esteban Andrade Pijuango que cursó estudios de Maestría en el campo de COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA en la Universidad Técnica del Norte.

Una vez indicadas las observaciones pertinentes y aclaradas considero que la metodología propuesta es Valida para su aplicación e implementación.

Ibarra, 28 días de abril de 2026



Firmado digitalmente por Santiago Portilla
Fecha: 2026.04.28 10:30:22 -05'00'

NOMBRE: Ing. Santiago Portilla
CI: 1002433058

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Ing. Alex Eduardo Chuquín López
ESPECIALIDAD: Gobierno de TI y Seguridad de la Información
CÉDULA DE IDENTIDAD: 1003288477

Por medio del presente, informo que realicé la evaluación de la tesis con tema de **"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)"**, elaborado por el Ing. Jefferson Esteban Andrade Pijuango que cursó estudios de Maestría en el campo de COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA en la Universidad Técnica del Norte.

Se concluye que la metodología presenta una **EXCELENTE** concordancia, con objetivos claramente definidos y resultados consistentes, por lo cual, se considera procedente su implementación. Asimismo, permitirá a las instituciones del Sector Financiero Popular y Solidario fortalecer el cumplimiento de la normativa vigente, mediante el uso de indicadores de desempeño y efectividad del Sistema de Gestión de Seguridad de la Información.

Ibarra, 28 días de abril de 2026

Firmado electrónicamente por:
ALEX EDUARDO CHUQUIN LOPEZ
Validar únicamente con FirmaEC

Ing. Alex Eduardo Chuquín López
CI: 1003288477

CONSTANCIA DE VALIDACIÓN DE EXPERTO

NOMBRE DEL EXPERTO: Ing. Wilson Aníbal Cardenas Hernández
ESPECIALIDAD: Gestión de TI y Seguridad de la Información
CÉDULA DE IDENTIDAD: 1003090733

Por medio del presente, informo que realicé la revisión de la tesis con tema de **"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ALINEADA CON LA NORMATIVA 2022-002 DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS)"**, elaborado por el Ing. Jefferson Esteban Andrade Pijuango que cursó estudios de Maestría en el campo de COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA en la Universidad Técnica del Norte.

Tras la revisión de las observaciones emitidas y las aclaraciones presentadas, se determina que la metodología propuesta cumple con criterios de consistencia, aplicabilidad y rigor técnico, considerándose procedente su implementación en el área de Seguridad de la Información.

Ibarra, 28 días de abril de 2026



Ing. Wilson Aníbal Cardenas Hernández
CI: 1003090733