

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría

Tema:

"Auditoría del sistema de información a la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda."

Autora: Henríquez Cisneros, Nathaly Estefanía

Tutora: Dra. Jiménez Estrella, Patricia Paola. Mg

Ambato-Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella. Mg con cédula de ciudadanía No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: **"AUDITORÍA DEL SISTEMA DE INFORMACIÓN A LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA."** desarrollado por Nathaly Estefania Henriquez Cisneros, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, agosto 2024

TUTORA



Dra. Patricia Paola Jiménez. Mg

C.C. 180293423-0

AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Nathaly Estefania Henriquez Cisneros con cédula de ciudadanía No. 180451368-5, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"AUDITORÍA DEL SISTEMA DE INFORMACIÓN A LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA."**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este proyecto integrador.

Ambato, agosto 2024

AUTORA



.....

Nathaly Estefania Henriquez Cisneros

C.C. 180451368-5

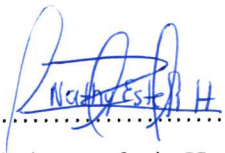
DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto de investigación, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, agosto 2024

AUTORA



.....

Nathaly Estefania Henriquez Cisneros

C.C. 180451368-5

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"AUDITORÍA DEL SISTEMA DE INFORMACIÓN A LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA."**, elaborado por Nathaly Estefania Henriquez Cisneros, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, agosto 2024

Dra. Tatiana Valle Ph. D.
PRESIDENTE

Dr. Edisson Coba. Mg
MIEMBRO CALIFICADOR

Dr. Carlos Barreno. Mg
MIEMBRO CALIFICADOR

DEDICATORIA

Dedico este proyecto de titulación a mi madre, por ser el pilar de mi vida, mi razón de ser, quien siempre confió en mí, y estuvo a mi lado brindándome apoyo y amor incondicional, así logró que no me rinda y siga adelante, ella es lo más valioso de mi vida.

A mi abuelita que desde el cielo me cuida y sé que estaría orgullosa de todo lo que he logrado.

A mi abuelito por su cariño, por confiar en mis capacidades y brindarme su apoyo.

Nathaly Estefania Henriquez Cisneros

AGRADECIMIENTO

A la Universidad Técnica de Ambato, por abrirme sus puertas y darme la oportunidad de pertenecer a tan prestigiosa institución.

A los docentes de la Facultad de Contabilidad y Auditoría, especialmente a mi tutora la Dra. Patricia Jiménez, por compartir sus conocimientos, y brindarme su guía en el proceso de realización de este proyecto.

A la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda., por permitirme realizar mi proyecto de titulación, bridándome los recursos necesarios durante todo el proceso.

Nathaly Estefania Henriquez Cisneros

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PÁGINA**

A. PÁGINAS PRELIMINARES

PORTADA i
APROBACIÓN DEL TUTOR ii
AUTORÍA DEL TRABAJO DE TITULACIÓN iii
DERECHOS DE AUTOR iv
APROBACIÓN DEL TRIBUNAL DE GRADO v
DEDICATORIA vi
AGRADECIMIENTO vii
ÍNDICE GENERAL DE CONTENIDOS viii
ÍNDICE DE TABLAS xi
ÍNDICE DE ILUSTRACIONES xii
RESUMEN EJECUTIVO xiv
ABSTRACT xv

B. CONTENIDOS

CAPÍTULO I 1
MARCO TEÓRICO 1
1.1 Introducción **1**
1.1.1 Antecedentes del proyecto integrador 1
1.1.1.1 Historia de la empresa 1
1.1.1.2 Detalles estratégicos 2
1.1.1.3 Estructura organizacional 2
1.1.1.4 Detalles de operación 4
1.1.1.5 Detalles legales 4
1.1.1.6 Marcas y logos 4
1.1.2 Descripción del entorno 5
1.1.2.1 Auditoría informática en el entorno organizacional 5
1.1.2.2 Auditoría de sistemas de información en el sector cooperativo ecuatoriano 6
1.1.2.3 Los sistemas de información en la Cooperativa Kullki Wasi Ltda. 7

1.1.3 Justificación 8
1.1.4 Objetivos 9
1.4.1 Objetivo general 9
1.4.2 Objetivos específicos 9
1.5 Revisión de la literatura 10
1.5.1 La teoría de sistemas y la auditoría de sistemas de información 10
1.5.2 Auditoría 10
1.5.2.1 Tipos de auditoría 11
1.5.3 Control interno 12
1.5.4 Tecnologías de la información 13
1.5.5 Sistemas de información 14
1.5.6 Sistema informático 14
1.5.7 Controles para la seguridad física del área de sistemas 14
1.5.8 Controles para la seguridad lógica de los sistemas 15
1.5.9 Controles para la seguridad de la base de datos 16
1.5.10 Auditoría a los sistemas de información 16
1.5.11 Fases de una auditoría a los sistemas de información 17
1.5.12 Activos de información 17
1.5.13 Amenaza, vulnerabilidad y riesgo 18
1.5.14 Normas Internacionales de Auditoría 18
1.5.15 Normas de Control Interno 19
1.5.16 Normas ISO 19
1.5.17 Modelo COSO ERM 20
1.5.18 Marco de Referencia COBIT 21
CAPÍTULO II 22
METODOLOGÍA 22
2.1 Descripción de la metodología 22
2.1.1 Unidad de análisis 22
2.1.2 Fuentes y técnicas de recolección de información 22
2.1.2.1 Fuentes de información primaria 22
2.1.2.2 Fuentes de información secundaria 28
2.1.3 Fases del desarrollo 28
2.1.3.1 Criterios para la fase de planificación 29

2.1.3.2 Criterios para la fase de ejecución 30
CAPÍTULO III 37
DESARROLLO 37
3.1 Resultado 37
3.1.1 Planificación 37
3.1.1.1 Memorándum 37
3.1.1.2 Programa de auditoría 39
3.1.1.3 Guía de visita previa 40
3.1.1.4 COSO ERM 40
3.1.2 Fase de Ejecución 41
3.1.2.1 NORMAS ISO/IEC 27000 Evaluación a los activos de información 41
3.1.2.2 Evaluación de los procesos catalizadores con el Marco de Referencia COBIT 5. 48
3.1.3 Comunicación de resultados 65
3.1.3.1 Reporte preliminar de auditoría 65
3.1.3.2 Informe de auditoría 67
3.1.3.3 Resultados del examen 70
3.1.4 Manual de políticas de seguridad 101
3.1.5 Matriz de seguimiento y monitoreo 109
3.1.5.1 Instrucciones para utilización de la matriz de seguimiento y monitoreo. 109
CAPÍTULO IV 114
CONCLUSIONES Y RECOMENDACIONES 114
4.1 Conclusiones 114
4.2 Recomendaciones 115
C. MATERIAL DE REFERENCIA
REFERENCIAS BIBLIOGRÁFICAS 117
ANEXOS 122

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

Tabla No.1 Tipos de Controles 13
Tabla No.2 Importancia de los sistemas de información 14
Tabla No.3 Áreas que abordan la auditoría a los sistemas de información 16
Tabla No.4 Fases de auditoría al sistema de información 17
Tabla No.5 Activos de Información 18
Tabla No.6 Normas Internacionales de Auditoría 18
Tabla No.7 Normas de Control Interno 19
Tabla No.8 Principales Normas ISO para el sistema de seguridad de información .. 20
Tabla No.9 Personas entrevistadas y encuestadas 23
Tabla No.10 Guion de entrevista 23
Tabla No.11 Preguntas de la entrevista 24
Tabla No.12 Preguntas de la lista de verificación 25
Tabla No.13 Verificación de los procesos a ser evaluados 26
Tabla No.14 Preguntas del cuestionario COSO ERM 2017 27
Tabla No.15 Fases de auditoría 28
Tabla No.16 Medición de confianza y riesgo 29
Tabla No.17 Criterios de calificación de los componentes 30
Tabla No.18 Criterios de confidencialidad 30
Tabla No.19 Criterios de Integridad 30
Tabla No.20 Criterios de Disponibilidad 31
Tabla No.21 Nivel de Tasación 31
Tabla No.22 Valoración de controles de los activos 32
Tabla No.23 Valoración de la probabilidad de ocurrencia de riesgos 32
Tabla No.24 Valoración de impacto de ocurrencia de riesgos 33
Tabla No.25 Nivel del riesgo 33
Tabla No.26 Procesos evaluados de COBIT 34
Tabla No.27 Niveles de capacidad de los procesos 36
Tabla No.28 Niveles de madurez de los procesos 36
Tabla No.29 Matriz de supervisión y monitoreo 109

ÍNDICE DE ILUSTRACIONES

CONTENIDO **PÁGINA**

Ilustración No. 1 Organigrama estructural 3
Ilustración No. 2 Logo de la cooperativa 4
Ilustración No. 3 Ubicación de la cooperativa 5
Ilustración No. 4 Funciones de Auditoría 11
Ilustración No. 5 Objetivo de auditoría 11
Ilustración No. 6 Tipos de auditoría 12
Ilustración No. 7 Características del control interno 12
Ilustración No. 8 Evolución de las TI 13
Ilustración No. 9 Sistema Informático 14
Ilustración No. 10 Controles para la seguridad física del área de sistemas 15
Ilustración No. 11 Controles para la seguridad lógica del área de sistemas 15
Ilustración No. 12 Controles para la seguridad de las bases de datos 16
Ilustración No. 13 Amenaza, vulnerabilidad y riesgo 18
Ilustración No. 14 Características del COSO ERM 20
Ilustración No. 15 Modelo de Referencia de Procesos de COBIT 5 21
Ilustración No. 16 Memorándum de planificación 37
Ilustración No. 17 Programa de auditoría 39
Ilustración No. 18 Guía de visita previa 40
Ilustración No. 19 Nivel de confianza y riesgo 40
Ilustración No. 20 Nivel de madurez y eficiencia del control interno 41
Ilustración No. 21 Nivel de tasación o criticidad de los activos de información 42
Ilustración No. 22 Principio #1 Confidencialidad 43
Ilustración No. 23 Principio #2 Integridad 43
Ilustración No. 24 Principio #3 Disponibilidad 44
Ilustración No. 25 Evaluación de riesgos de los Activos 45
Ilustración No. 26 Controles y políticas de seguridad de los activos 46
Ilustración No. 27 Periodicidad o frecuencia de controles 47
Ilustración No. 28 Evaluación del Marco de Referencia COBIT 5 49
Ilustración No. 29 EDM03 “Asegurar la Optimización del riesgo” 50
Ilustración No. 30 EDM04 “Asegurar la Optimización de Recursos” 51

Ilustración No. 31 APO01 “Gestionar el Marco de Gestión de TI” 52
Ilustración No. 32 APO02 “Gestionar la Estrategia” 53
Ilustración No. 33 APO04 “Gestionar la Innovación” 54
Ilustración No. 34 APO04 “Gestionar los Recursos Humanos” 55
Ilustración No. 35 APO09 “Gestionar los acuerdos de servicio” 56
Ilustración No. 36 APO11 “Gestionar la Calidad” 57
Ilustración No. 37 APO12 “Gestionar el Riesgo” 58
Ilustración No. 38 APO13 “Gestionar la Seguridad” 59
Ilustración No. 39 BAI02 “Gestionar la Definición de Requisitos” 60
Ilustración No. 40 BAI09 “Gestionar los Activos” 61
Ilustración No. 41 DSS01 “Gestionar Operaciones” 62
Ilustración No. 42 DSS04 “Gestionar la Continuidad” 63
Ilustración No. 43 DSS05 “Gestionar Servicios de Seguridad” 64
Ilustración No. 44 MEA02 “Supervisar, Evaluar y Valorar el Sistema de Control Interno” 65
Ilustración No. 45 Informe preliminar de auditoría 66
Ilustración No. 46 Informe general 68
Ilustración No. 47 Ejemplo de utilización de la matriz de seguimiento 111
Ilustración No. 48 Matriz de supervisión y monitoreo 112

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "AUDITORÍA DEL SISTEMA DE INFORMACIÓN A LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA."

AUTORA: Nathaly Estefania Henriquez Cisneros

TUTORA: Dra. Patricia Paola Jiménez E., Mg

FECHA: Agosto 2024

RESUMEN EJECUTIVO

El siguiente proyecto integrador se lo realizó en la Cooperativa de Ahorro y Crédito Kulkki Wasi Ltda. tuvo por objetivo realizar una auditoría del sistema de información para la evaluación de su nivel de confianza en la seguridad y confiabilidad. Se realizo la evaluación del control interno con el marco de referencia COSO ERM 2017 que se relaciona a la gestión de riesgos en la información. De igual manera se aplicó los criterios de la norma ISO/IEC 27001 para la evaluación de los activos de información. En cuanto al gobierno y gestión de las tecnologías de información, se utilizó la metodología COBIT 5 que permitió determinar los niveles de capacidad y madurez, así como las metas objetivo de los procesos, teniendo una visión clara del estado actual de la cooperativa y contribuir a la propuesta de mejoras al tratamiento de la información y las tecnologías de la información. Entre los principales resultados se menciona que existe un buen nivel de madurez en control interno, logrando un cumplimiento básico-táctico, protegiendo sus activos de información y gestionando sus tecnologías de información. Aun así, hay amenazas que se pueden materializar, por lo cual se establecieron políticas destinadas a gestionar de manera efectiva la seguridad de los activos de información principalmente enfocadas a la utilización del software contable.

PALABRAS DESCRIPTORAS: AUDITORÍA, SISTEMA DE INFORMACIÓN, ACTIVOS DE INFORMACIÓN, CONTROL INTERNO, RIESGOS.

TECHNICAL UNIVERSITY OF AMBATO

FACULTY OF ACCOUNTING AND AUDITING

ACCOUNTING AND AUDITING CAREER

TOPIC: "AUDIT OF THE INFORMATION SYSTEM OF THE KULLKI WASI LTDA SAVINGS AND CREDIT COOPERATIVE"

AUTHOR: Nathaly Estefania Henriquez Cisneros

TUTOR: Dra. Patricia Paola Jiménez E., Mg

DATE: August 2024

ABSTRACT

The following integrative project was carried out in the Kulkki Wasi Savings and Credit Cooperative Ltda. Its objective was to carry out an audit of the information system to evaluate its level of confidence in security and reliability. The evaluation of internal control was carried out with the COSO ERM 2017 reference framework that is related to information risk management. Likewise, the criteria of the ISO/IEC 27001 standard were applied for the evaluation of information assets. Regarding the governance and management of information technologies, the COBIT 5 methodology was used to determine the levels of capacity and maturity as well as the objective goals of the processes, having a clear vision of the current state of the cooperative and contributing to the proposal for improvements to the processing of information and information technologies. Among the main results, it is mentioned that there is a good level of maturity in internal control, achieving basic-tactical compliance, protecting its information assets and managing its information technologies. Even so, there are threats that can materialize, which is why policies were established to effectively manage the security of information assets mainly focused on the use of accounting software.

KEYWORDS: AUDIT, INFORMATION SYSTEM, INFORMATION ASSETS, INTERNAL CONTROL, RISKS.

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes del proyecto integrador

4.5.4.4 Historia de la empresa

Como se describe en la página web de la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. (2024), su trayectoria se remonta desde el año 2003, gracias a la idea visionaria del Lic. Juan Andagana e indígenas de Chibuleo, Salasaca y Pilahuin de la provincia de Tungurahua. A finales del año 2002, se reúnen en la ciudad de Ambato varios dirigentes de los Pueblos mencionados, con la finalidad de conformar una cooperativa de ahorro y crédito que en lo posterior llevaría el nombre de KULLKI WASI Ltda. «La casa de dinero», esta institución conformada por doce personas y liderado por Lic. Juan Andagana en calidad de gerente y presidente de Consejo de Administración, el Dr. Manuel Caizabanda lograron fortalecer su pensamiento visionario en una realidad.

El 23 de enero del año 2003 fue legalizada mediante acuerdo ministerial número 002-SDRCC, emitido por parte del Ministerio de Bienestar Social 6582 y, mediante resolución número SEPS-ROEPS-2013-000266 de la Superintendencia de Economía Popular y Solidaria la cual, aprobó con observaciones la adecuación de su estatuto social, a la Ley Orgánica de la Economía Popular y Solidaria. Se realizó varias reuniones en diferentes casas y comunidades como Chibuleo, Salasaca y Pilahuín.
La institución se encuentra en el segmento UNO, en lo que respecta a requerimientos de los entes como la Superintendencia de Economía Popular y Solidaria, cumpliendo con rigurosidad conforme lo disponen, con el apoyo del Consejo de Administración y Vigilancia, quienes permanente controlan a todos los departamentos que cumplan con su rol asignado (Superintendencia de Economía Popular y Solidaria, 2024).

El Lic. Mg. Juan Andagana, Gerente General de la Institución, lleno de vivencias, ha sido un visionario en el mundo de las finanzas que se ha entregado a la administración de la Cooperativa de Ahorro y Crédito de KULLKI WASI Ltda., ofreciendo su experiencia y transparencia para el crecimiento de los socios y clientes.

Hoy su oficina matriz se encuentra ubicada en las calles Martínez y Juan B. Vela esq. De la ciudad de Ambato. Cuenta con más de 65 000 socios y ocho agencias a escala nacional.

1.1.1.2 Detalles estratégicos

Los detalles estratégicos se obtuvieron de la página web de la cooperativa (Cooperativa de Ahorro y Crédito Kullki Wasi Ltda., 2024).

Misión

Fomentar el desarrollo de nuestros socios y clientes, brindando servicios financieros inclusivos, con transparencia, calidad, responsabilidad social y ambiental.

Visión

Ser una institución innovadora, reconocida, y con enfoque de calidad.

Valores

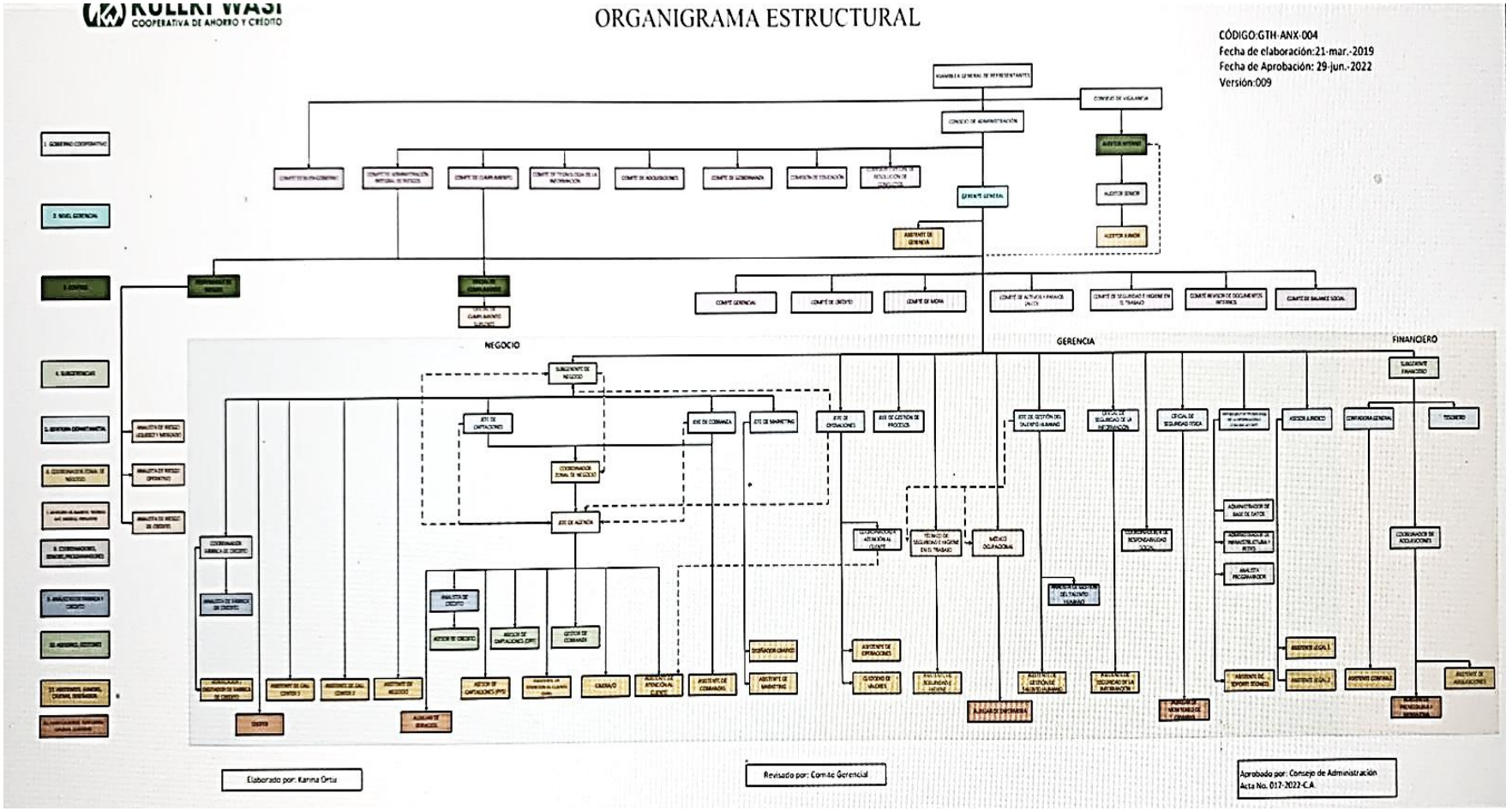
El personal que conforma la Cooperativa de Ahorro y Crédito de KULLKI WASI Ltda., cuenta con valores éticos son disciplina, honestidad, compromiso, trabajo en equipo, respeto a la naturaleza, pasión, respeto, solidaridad, con los cuales han brindado atención de calidad a sus clientes.

1.1.1.3 Estructura organizacional

En la Cooperativa de Ahorro y Crédito de KULLKI WASI Ltda. se destaca un definido sistema jerárquico, lo cual le posibilita tener una visión perspicaz de las diligencias designadas a los diferentes departamentos, de esta manera da paso a la competitividad y se puede tomar decisiones adecuadas para el desarrollo de sus actividades, se presenta su organigrama para mayor comprensión:

Ilustración 1

Organigrama estructural



Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. (2024)

1.1.1.4 Detalles de operación

El giro de la Cooperativa de Ahorro y Crédito de Kullki Wasi Ltda., se centra en la intermediación financiera mediante la captación de los ahorros a la vista, depósitos a plazo fijo, acceso a créditos y servicios cooperativos los cuales apoyan al desarrollo socioeconómico de la población. Brinda también ahorros a domicilio para las personas que no puedan salir de su hogar o de las oficinas, para lo cual el asesor de captación visita al cliente; apertura de cuentas para niños (Hormiguitas) con un valor de USD 3. Cuentan también con un plan de ahorro plus, con depósito inicial de USD 20 bajo el compromiso de un ahorro mensual por parte de los solicitantes, seguro exequial, seguro de desgravamen, tarjeta de débito 'DE UNA' y cajeros automáticos en todo el país. Adicionalmente brinda paso del bono de desarrollo humano, giros a través de Western Unión, cobro de RISE-SRI, cobro de SOAT, pago de servicios básicos, entre otros (Cooperativa de Ahorro y Crédito Kullki Wasi Ltda., 2024).

1.1.1.5 Detalles legales

La Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. (2024) se encuentra sujeta a las siguientes disposiciones legales:

- Ley Orgánica de Economía Popular y Solidaria
- Código de Trabajo
- Ley de Seguridad Social
- Ley Orgánica de Régimen Tributario
- Código Tributario
- Reglamento a la Aplicación de la Ley de Régimen Tributario

1.1.1.6 Marcas y logos

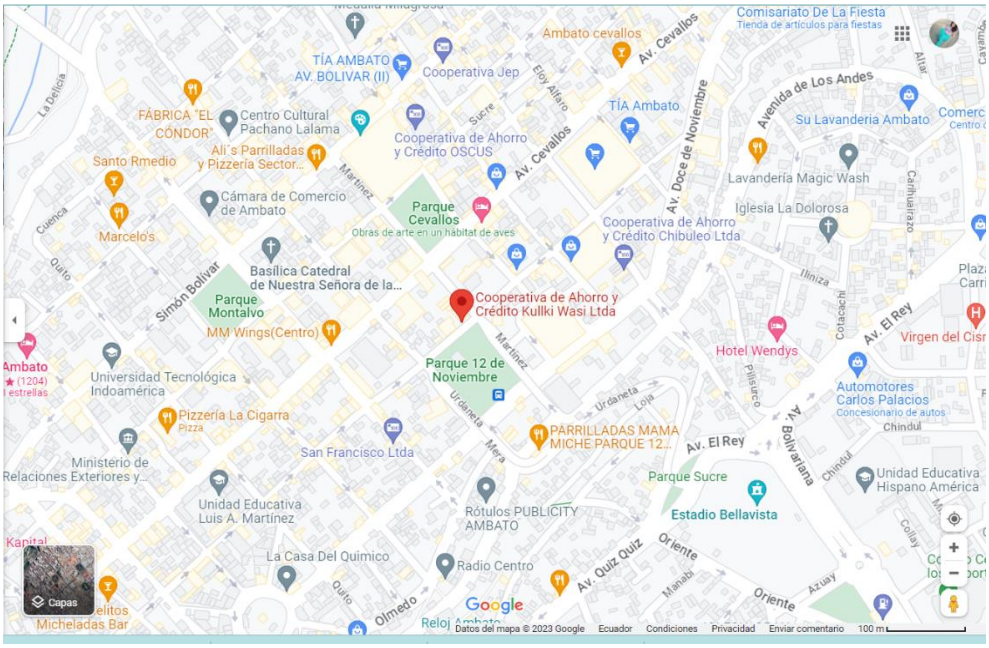
Ilustración 2

Logo de la cooperativa

Fuente: Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. (2024)

Ilustración 3

Ubicación de la cooperativa



Fuente: Google Maps (2024)

1.1.2 Descripción del entorno

4.5.4.4 Auditoría informática en el entorno organizacional

La auditoría de sistemas dentro del panorama global actual emerge como un componente esencial tanto en gestión, mejora y protección de los recursos como en la eficiencia del nivel directivo en las organizaciones (Martínez, Blanco, & Loy, 2012). En un entorno cambiante el éxito de las organizaciones se relaciona con su habilidad para manejar los riesgos a medida que las empresas incrementan su dependencia de la información que manejan para su ventaja competitiva (Arcentales & Caycedo, 2017). De esta manera es de suma importancia que la tecnología en las empresas esté en constante supervisión y control mediante una auditoría y así evitar muchas problemáticas.

La auditoría de sistemas de información ha sido reconocida a nivel mundial tanto en el ámbito público como privado, adoptando así normas y estándares internacionales. Siguiendo a Vecino (2017) menciona en marcos de referencia a ITIL (Information Technology Infrastructure Library), COBIT 5 (Control Objectives for information and related Technologies), normas ISO (International Organization for Standardization),

las cuales proporcionan directrices y mejores prácticas ayudando a todo tipo de organización a mejorar procesos de auditoría y proteger sistemas de información.

Es importante mencionar que el entorno caracterizado por la rápida evolución tecnológica enfrenta desafíos constantes, por la necesidad de adaptarse a nuevos entornos, siendo esencial la preservación de la privacidad de datos y gestión de riesgos como el hacking ético, el cibercrimen. Estos aspectos requieren una atención continua por los auditores informáticos, la adopción de regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea el cual ha apoyado en gran magnitud a extender la complejidad y el alcance que se obtiene en las auditorias informáticas, obteniendo un enfoque integrado entre auditores, equipos tecnológicos y demás partes importantes (Beltrán, 2018). La auditoría informática a nivel mundial se presenta como un campo vital para asegurar confianza, seguridad y eficacia en los sistemas de información, así como menciona Salgado et al. (2017) que si la función informática deja de funcionar correctamente afectaría total o parcialmente la operación de una organización, para lo cual es muy importante establecer controles, políticas, procesos, asegurando los activos, definiendo la gestión tecnológica para que la empresa rinda de la mejor manera en sus actividades.

1.1.2.2 Auditoría de sistemas de información en el sector cooperativo ecuatoriano

En la actualidad, en Ecuador los procesos se realizan de manera más fácil, con mayor comunicación gracias a la tecnología, sin embargo, esto ha causado un gran número de delitos cibernéticos y fraudes (Saltos, Rovalino, & Pazmiño, 2021). Con respecto al sector financiero, centrándose en las cooperativas de ahorro y crédito siguiendo a Zhañay, Erazo, & Narváez (2019) como las cooperativas cada vez dependen más de la tecnología de la información para gestión de sus operaciones diarias, son muy propensas a los ataques y pérdidas de información porque manejan muchos activos de información.

Se determinó que la auditoría de sistemas de información es esencial ya que brinda seguridad a la información y a los equipos informáticos de las cooperativas, según Pérez (2018), la importancia de la seguridad de la información es crucial y por ello

dentro de las cooperativas deben contar con personal capacitado en su gestión. En Ecuador si hay personal calificado en los campos de la tecnología informática, ciberseguridad y auditoría de sistemas, pero como menciona Rocha (2011), siempre se requiere que existan más expertos por la gran cantidad de delitos comunes en éstas áreas, para disminuir en gran medida las vulnerabilidades y evitar que se susciten las amenazas. La mayoría de las cooperativas en Ecuador no le dan el grado de importancia a tener un auditor informático y es por ello que tienen grandes problemáticas, ya que, se tiene activos críticos que requieren una auditoría regular y así mantener la seguridad en sus sistemas.

De acuerdo con Albarracín et al. (2021) las cooperativas pueden beneficiarse de la adopción de buenas prácticas en auditoría de sistemas de información, establecimiento de medidas de seguridad según los riesgos y la ejecución de pruebas de vulnerabilidad.

1.1.2.3 Los sistemas de información en la Cooperativa Kullki Wasi Ltda.

Se hace énfasis a las auditorías de sistemas de información, realizadas por la SEPS (Superintendencia de Economía Popular y Solidaria), la misma que exige que se contrate un auditor informático interno, para que exista un control y evaluación tanto de los equipos informáticos como la información que manejan los mismos. Esto es importante ya que la cooperativa tiene varios departamentos, los cuales manejan información relevante día a día de sus socios y se debe asegurar la integridad, confiabilidad en la información que se procesa diariamente para cumplir objetivos de la cooperativa, así como la protección de datos evitando hackeos, robos de información, entre otros riesgos a los que se expone. A pesar de contar con un departamento de seguridad de la información, la cooperativa necesitó una auditoría para mayor seguridad y de esta manera según las vulnerabilidades encontradas, proteger los aspectos más críticos, sin que se susciten los riesgos, cuidando a la alta gerencia.

La cooperativa Kullki Wasi Ltda., opera en un entorno que combina tanto el aspecto tradicional de las finanzas cooperativas como la innovación tecnológica para satisfacer las necesidades de sus socios. Ha realizado inversiones en tecnología para mejorar sus servicios financieros, sin embargo, como mencionó Bombón (2024) Ing. en Sistemas

de la Información en la cooperativa, en muchas organizaciones del sector estas tecnologías enfrentan desafíos de mantenerse actualizadas, debido a que no están exentas de amenazas tanto externas como internas.

Con la auditoría de sistemas de información se identificó los problemas que tienen con la infraestructura tecnológica y más aspectos relevantes que llevan a interrupciones del servicio en transacciones, afectando así la satisfacción del cliente, la operatividad de la cooperativa y la eficiencia y eficacia en el servicio ofertado.

1.1.3 Justificación

La auditoría de sistemas de información es un aspecto muy importante dentro de toda organización incluyendo las cooperativas donde se necesita realizar un examen destinado a revisar, evaluar cómo se están administrando actualmente los sistemas y controles desarrollados en los mismo, en efecto, en el estudio de Tejeda (2020) ésta revisión y evaluación de los sistemas de información que procesan información incluye todas las interfases que hacen potencial su funcionamiento, y son: software, hardware, comunicaciones, recurso humano, políticas, procedimientos, normativas internas y controles de seguridad.

Las TIC, en la actualidad, se encuentran en todas partes, las tecnologías de la información y comunicación la ocupan las personas y empresas ante la necesidad que tienen diariamente para revisar su correo electrónico, hablar por teléfono, monitorear las redes sociales, chatear con amigos, etcétera. Según Téllez Barrientos et al. (2016) los sistemas de información ayudan a cumplir los objetivos organizacionales, de esta manera, asegura la integridad, disponibilidad y confidencialidad de la información, mediante controles adecuados y recomendaciones de seguridad.

Se debe tener en cuenta que en las cooperativas de ahorro y crédito invierten en tecnología informática, no es solo por tenerla, sino que invierten en ella para apoyar a los objetivos de la organización fundamentados en liderazgo, estructuras empresariales y los procesos que aseguran que la tecnología informática se encuentre centrada en el valor, riesgo y control, alrededor del ambiente tecnológico de la empresa.

Así mismo permite conocer los riesgos a los cuales está expuesta la información, amenazas, vulnerabilidades en el sistema, como en los demás activos de información (Díaz Varela, 2020), en los cuales se pueden implantar medidas correctivas.

De esta manera, en el presente trabajo se aplicará la auditoría a los sistemas de información con la finalidad de buscar soluciones a varias problemáticas que se pueden suscitar dentro del campo de los sistemas de información, dichas soluciones permitirán el cumplimiento de los objetivos que tiene la entidad, en donde se reflejará como sus resultados generan e incorporan valor a la gestión gerencial, pues se detallará como la misma se constituye en insumo primordial para la toma de decisiones, amén de contribuir decididamente al fortalecimiento del SCI (Llumiguano Poma et al., 2021).

Para el trabajo se cuenta con la suficiente disponibilidad de información y asesoría dentro de la organización, así será factible el estudio teniendo en cuenta también que en el aspecto tecnológico se utilizará herramientas básicas como Word y Excel.

Al llevar a cabo una auditoría a los sistemas de información en la Cooperativa Kullki Wasi Ltda., siendo una necesidad de la cooperativa en la actualidad según Marcelo Herrera (2023) quien en su calidad de oficial de seguridad de la información, supo manifestar que la cooperativa necesita un auditor interno en el área de sistemas de la información, se aportaría de manera significativa con el aporte de los hallazgos para la toma de decisiones en la Gerencia y esto aporte al desarrollo de las actividades en los diferentes departamentos.

1.1.4 Objetivos

1.4.1 Objetivo General

Realizar una Auditoría del sistema de información en la Cooperativa Kullki Wasi Ltda., para la evaluación de su nivel de confianza en la seguridad y confiabilidad.

1.4.2 Objetivos Específicos

- Elaborar la planificación de auditoría a los sistemas de información para la determinación de los niveles de riesgo y enfoque de auditoría.

- Ejecutar la auditoría a los sistemas de información para la evaluación de los procesos en el nivel de informatización y tratamiento de los datos verificando los controles en el procesamiento y sistemas de seguridad
- Comunicar los resultados de la auditoría a los sistemas de información a través del informe para la toma de decisiones de la alta gerencia.

1.5 Revisión de la literatura

1.5.1 La teoría de sistemas y la auditoría de sistemas de información

La teoría de sistemas afirma que las características de un sistema no pueden describirse en elementos separados, sino más bien como un conjunto, por lo que, de no ser así no existiría una comprensión de todas las partes de un sistema (Bertalanffy, 1989). De esta forma, esta teoría posibilita que la auditoría de sistemas lleve a cabo un análisis global sin perder cada particularidad y dando el grado de importancia a las vulnerabilidades, amenazas, riesgos y controles dentro de la entidad.

En el presente proyecto se pretende examinar las amenazas a las que se encuentra expuesta la información de la cooperativa y el tránsito de la misma entre departamentos, verificando el cumplimiento de los controles y normativas que incluyen la seguridad de sus activos de información para una correcta administración de los riesgos tecnológicos que pueden causar un daño al sistema de seguridad de la información afectando su integridad, disponibilidad y confidencialidad.

1.5.2 Auditoría

La auditoría comprende un proceso de confirmación o comprobación del cumplimiento de actividades, según Zambrano et al. (2021) afirman que a la auditoría se la relaciona con la verificación, revisión de los procesos los cuales pueden llegar a ser financieros, económicos, gestión, operacional y administrativos.

Ilustración 4

Funciones de Auditoría

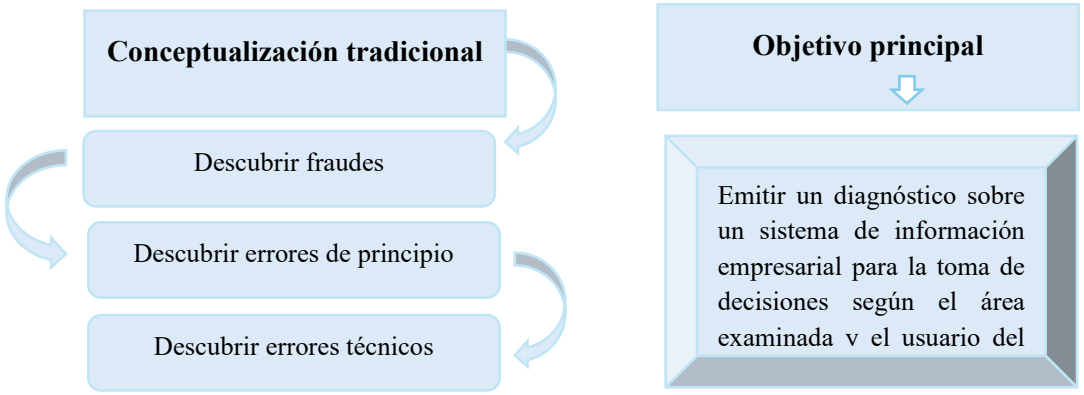
Funciones de la Auditoría	Evaluar la eficacia de las políticas y métodos empleados por la entidad, detactando cualquier desviación respecto a lo planeado.
	Recomendar las acciones pertinentes para corregir o mejorar ciertas actividades según sea necesario.

Fuente: Villardefrancos & Rivera (2006)
Elaborado por: Henriquez (2024)

Para Villardefrancos & Rivera (2006) la auditoría representa una herramienta tanto de revisión, supervisión aportando a crear una cultura de disciplina en la organización, de esta manera permitiendo descubrir vulnerabilidades o fallas que presenten. Es así que la auditoría según Manrique (2019) se puede aplicar en todo tipo de entidades con el mismo propósito de detallar en un informe de auditoría todas las inconsistencias encontradas exponerlas como hallazgos y redactar recomendaciones.

Ilustración 5

Objetivo de auditoría



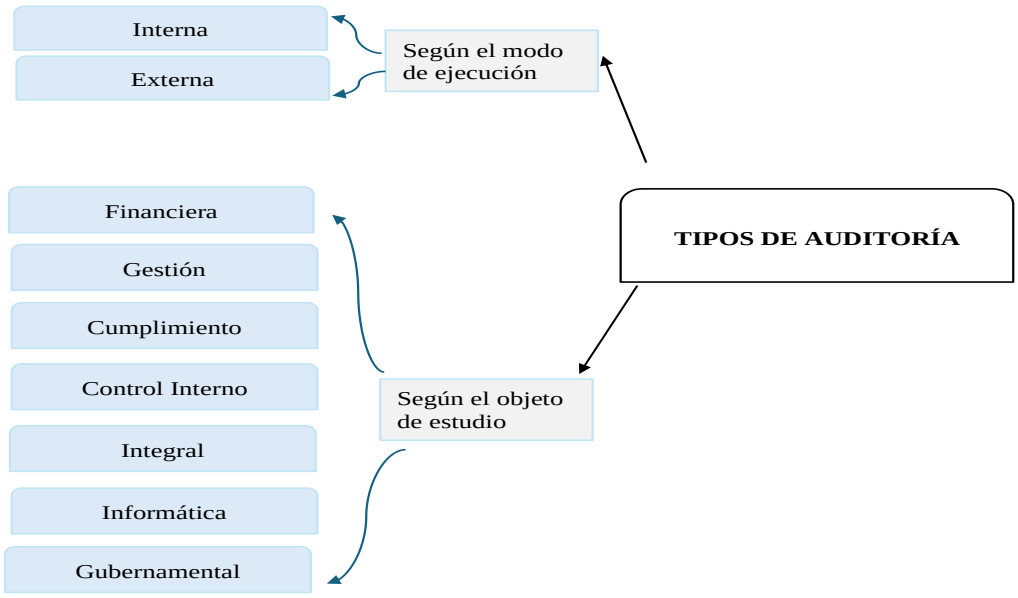
Fuente: Biler (2017)
Elaborado por: Henriquez (2024)

1.5.2.1 Tipos de auditoría

La auditoría según Montilla & Herrera (2006) se puede clasificar según el modo de ejecución y según el objeto de estudio, tal y como se presenta en la ilustración 6.

Ilustración 6

Tipos de auditoría



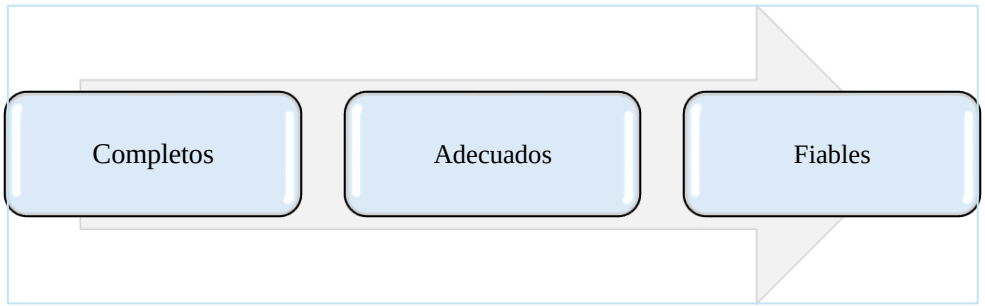
Fuente: Adaptado de Montilla & Herrera (2006)
Elaborado por: Henriquez (2024)

1.5.3 Control interno

El control interno comprende la acción o actividad de prevención y corrección de los errores con el fin de garantizar una seguridad adecuada en el logro de los objetivos de la organización, relativos a todo tipo de información, eficiencia y eficacia de operaciones y cumplimiento de disposiciones legales (Téllez et al., 2016). Los controles internos cuando se implementan deben tener las siguientes características:

Ilustración 7

Características del control interno



Fuente: Téllez et al. (2016)
Elaborado por: Henriquez (2024)

Existen tipos de controles internos que una empresa debe tener para ofrecer una seguridad razonable de que los recursos estén protegidos y los objetivos de la

institución sean alcanzados, siguiendo a Amezcua Luján & Santoyo Telles (2021) son los detallados a continuación:

Tabla 1

Tipos de Controles

TIPOS DE CONTROLES		
Preventivos	**Detectivos**	**Correctivos**
Previenen, tratan de evitar que ocurra el hecho.	Detectan errores, aparecen en caso de no funcionar correctamente los controles preventivos.	Ayudan a corregir errores que impidan se desarrolle con normalidad las actividades.

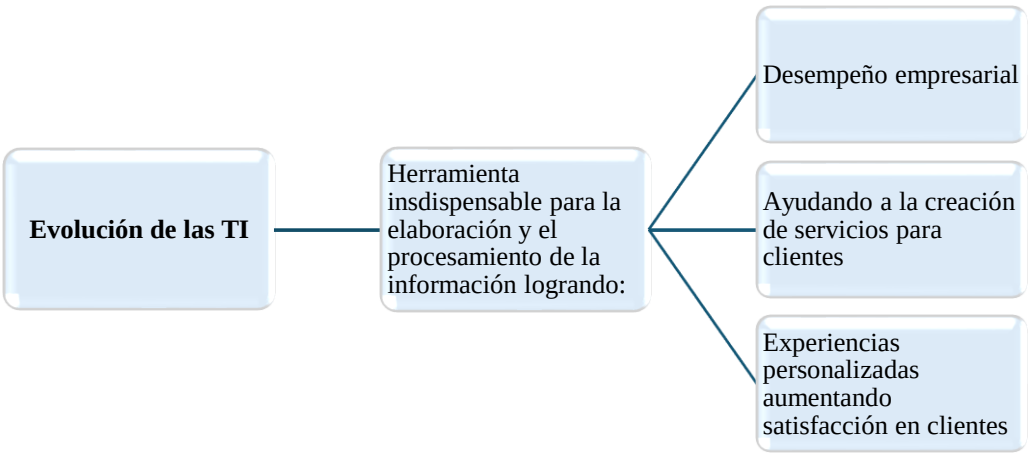
Fuente: Adaptado de Amezcua Luján & Santoyo Telles (2021)
Elaborado por: Henriquez (2024)

1.5.4 Tecnologías de la información

Las TI son un conjunto de tecnologías engloban todos los dispositivos desarrollados por el ser humano que posibilitan la producción, recuperación o transmisión de información de forma rápida, eficiente y a gran escala, Sánchez (2012) menciona que las TI son necesarias para la gestión y transformación de la información, destacando el uso de computadoras y software que permiten crear, modificar, almacenar, proteger y recuperar dicha información.

Ilustración 8

Evolución de las TI



Fuente: Arbeláez, (2014)
Elaborado por: Henriquez (2024)

1.5.5 Sistemas de información

Dentro del ámbito empresarial los sistemas de información son muy relevantes, así como menciona Abrego Almazán et al. (2017) los sistemas de información ofrecen grandes oportunidades de éxito en las entidades ya que reúnen, procesan, distribuyen y comparten datos de manera oportuna y de forma integrada.

Tabla 2

Importancia de los sistemas de información

Proceso	Importancia
Optimización de los procesos	Mayor eficiencia y reducción de costos
Toma de decisiones	Herramientas poderosas para el análisis de datos
Comunicación	Mejor comunicación, permitiendo
Competitividad	Permite responder ante cambios en el mercado

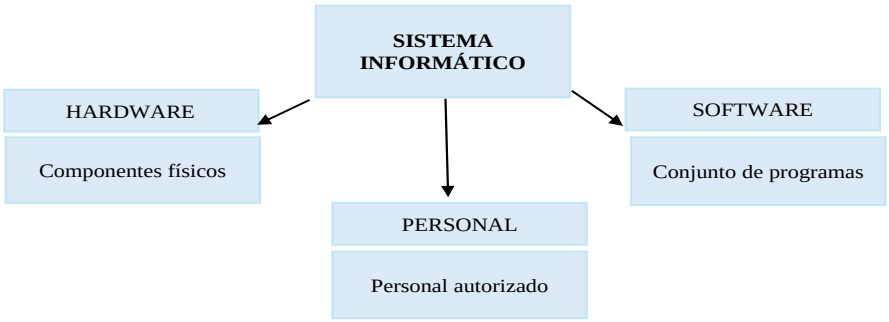
Fuente: Abrego Almazán et al. (2017)
Elaborado por: Henriquez (2024)

1.5.6 Sistema informático

El sistema informático es el que permite el almacenamiento y procesamiento de información y está conformado por: hardware, software y personal (Sepúlveda et al., 2008)

Ilustración 9

Sistema Informático



Fuente: Sepúlveda et al., (2008)
Elaborado por: Henriquez (2024)

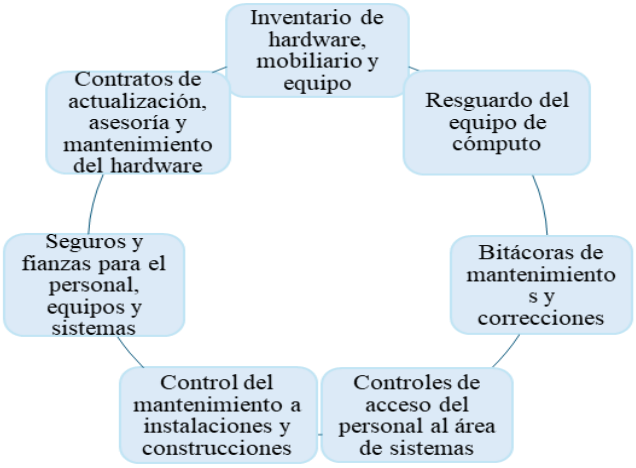
1.5.7 Controles para la seguridad física del área de sistemas

Como ya se mencionada es esencial establecer medidas de control para garantizar la seguridad física en el área de sistemas, como menciona Muñoz Razo (2002) estos controles tienen como objetivo proteger los activos tangibles de la empresa. En este

contexto particular, se trata de implementar medidas para protección y resguardo de equipos de cómputo, mobiliario y otros componentes ubicados en dicha área.

Ilustración 10

Controles para la seguridad física del área de sistemas



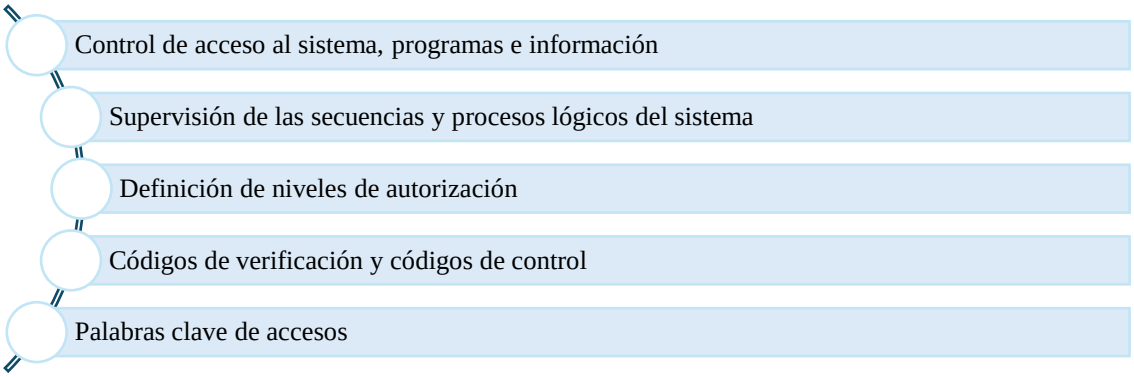
Fuente: Muñoz (2002)
Elaborado por: Henriquez (2024)

1.5.8 Controles para la seguridad lógica de los sistemas

Así como la seguridad física es importante dentro de las entidades Muñoz Razo (2002) también menciona que la seguridad lógica es importante, porque mediante ella se puede proteger los activos intangibles.

Ilustración 11

Controles para la seguridad lógica del área de sistemas



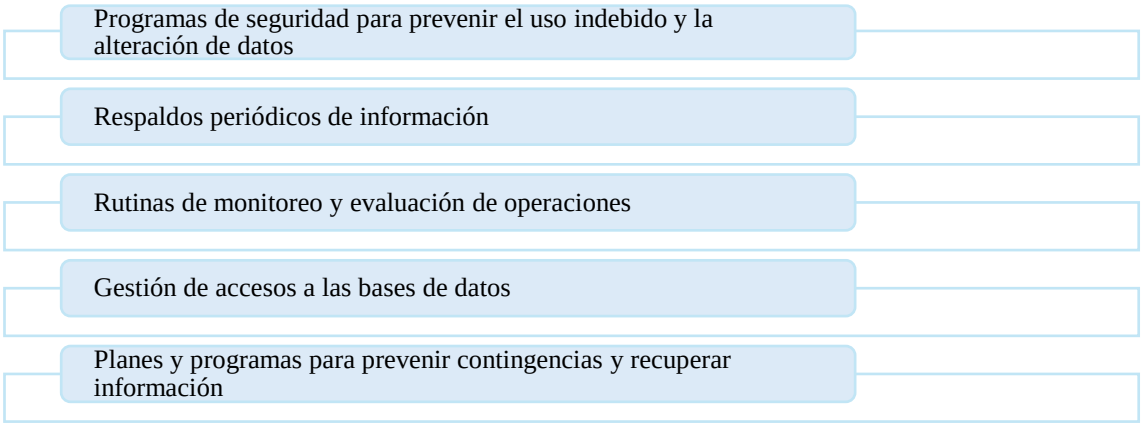
Fuente: Muñoz (2002)
Elaborado por: Henriquez (2024)

1.5.9 Controles para la seguridad de la base de datos

La base de datos debe estar resguardada porque dentro de ella se encuentra información muy valiosa y por ende como menciona Muñoz Razo (2002) se tiene una lista de controles que debe ser efectuados si se quiere proteger la base de datos.

Ilustración 12

Controles para la seguridad de las bases de datos



Fuente: Muñoz (2002)
Elaborado por: Henriquez (2024)

1.5.10 Auditoría a los sistemas de información

La auditoría a los sistemas de información se asocia con pruebas de control y seguridad de la información, abordando varias áreas, como menciona Bailon Lourido (2019) destaca las áreas que abordan la auditoría a sistemas de información:

Tabla 3

Áreas que abordan la auditoría a los sistemas de información

Áreas que abordan la auditoría a los sistemas de información	
Administración de recursos TI:	Asegurando que la organización emplee la TI de manera rentable, teniendo en cuenta los requisitos de automatización y la adaptación a los cambios ambientales que puedan surgir.
Seguridad Física y Seguridad de Información	Asegura que el entorno en el que operan los sistemas preserva su confidencialidad, integridad y fiabilidad.
Mantenimiento y desarrollo de los sistemas de información:	Garantiza la disponibilidad de los sistemas.
Continuidad de SI:	Minimiza la probabilidad de incidencias en los sistemas de información, garantizando que, en caso de alguna adversidad, la organización pueda reanudar sus operaciones de manera efectiva.

Fuente: Adaptado de Bailon Lourido (2019)
Elaborado por: Henriquez (2024)

1.5.11 Fases de una auditoría a los sistemas de información

Dentro de las fases de la auditoría encontramos la planificación, ejecución, informe y seguimiento y monitoreo de la auditoría informática, las mismas que según Castello (2017) son detalladas a continuación:

Tabla 4

Fases de auditoría al sistema de información

FASES DE AUDITORÍA	CONCEPTO
Planificación	1. Familiarización y comprensión de la organización 2. objetivos y alcance de la auditoria 3. Examen preliminar de control interno 4. Evaluación de los riesgos y la importancia 5. Planificación específica de la auditoría 6. Creación del programa de auditoría
Ejecución	Se recopila información necesaria en documentos y evidencias que permiten al auditor evidenciar sus comentarios, sugerencias y recomendaciones con respecto al manejo y administración de TI.
Informe	Proceso de finalización de auditoría se elabora el informe donde se detalla conclusiones, recomendaciones, comentarios para que en este caso la cooperativa tome acciones ante lo que se expone en el informe.
Seguimiento y monitoreo	Se realiza un seguimiento del cumplimiento de las recomendaciones que se dictaron en el informe.

Fuente: Adaptado de Castello (2017)
Elaborado por: Henriquez (2024)

Por otra parte según Díaz Varela (2020) indica que el esquema fundamental de un plan de auditoría para el área de sistemas de información sugiere un enfoque que evalúa los estándares de información, incluyendo aquellos relacionados con la seguridad y la excelencia. Se examinan recursos que abarcan la tecnología de la información, y se lleva a cabo una evaluación teniendo en cuenta la interacción entre procesos y organización.

1.5.12 Activos de información

Los activos de información son todas las herramientas, utilidades, que participan el desarrollo, la transmisión y recepción de la información que tenga valor dentro de una

organización (Colina & Túa, 2020). En la tabla se presentan algunos ejemplos de recursos de información.

Tabla 5

Activos de Información

ACTIVO	DESCRIPCIÓN
Software Contable	Sistema integrado para la organización contable, financiera, administrativa de una empresa tiene varios módulos.
Empleados	Personas que cumplen una función dentro de la organización.
Equipos de usuario final propiedad de la empresa	Computadoras, monitores, impresoras, teléfonos y otros tipos de dispositivos del usuario final considerado como activo de TI.

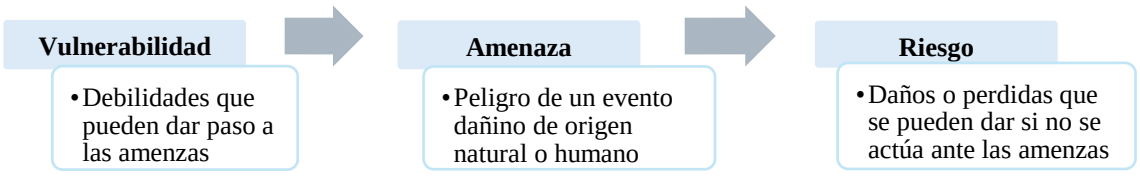
Fuente: Elaboración propia

1.5.13 Amenaza, vulnerabilidad y riesgo

Existe una estrecha relación entre la amenaza, vulnerabilidad y riesgo que de describen a continuación.

Ilustración 13

Amenaza, vulnerabilidad y riesgo



Fuente: Reyes et al. (2017)
Elaborado por: Henriquez (2024)

1.5.14 Normas Internacionales de Auditoría

Las Normas Internaciones de Auditoría (NIA) son un conjunto de directrices definidas por la Federación Internacional de Contadores que se aplican para garantizar la consistencia y precisión de las auditorías realizadas por los contadores. (Herrera, 2017).

Tabla 6

Normas Internacionales de Auditoría

Normas Internacionales de Auditoría	
NIA 300	Planificación de Auditoría.
NIA 401	Auditoria en un ambiente de sistemas de información por computadora.
NIA 500	Evidencia de Auditoría.

NIA 700	Formación de la opinión y emisión del informe de Auditoría.

Fuente: Adaptado de Herrera (2017)
Elaborado por: Henriquez (2024)

1.5.15 Normas de Control Interno

Dentro del Acuerdo 004 propuesto por Contraloría General del Estado (2023) donde constan normas de control interno, existe una sección referente a las tecnologías de la información detalladas a continuación:

Tabla 7

Normas de Control Interno

Tecnologías de la información	
410-01	Organización de la unidad de tecnologías de la información y comunicaciones
410-02	Comité de Tecnologías de la Información y Comunicaciones
410-03	Segregación de funciones
410-04	Plan estratégico y operativo de tecnologías de la información y comunicaciones
410-05	Políticas y procedimientos
410-06	Clasificación y arquitectura de la información
410-07	Administración de proyectos tecnológicos
410-08	Desarrollo, mantenimiento y adquisición de software de aplicación
410-09	Adquisiciones de infraestructura tecnológica
410-10	Mantenimiento, actualización y control de la infraestructura tecnológica
410-11	Seguridad de tecnología de información
410-12	Plan de contingencias
410-13	Administración de soporte de tecnología de información
410-14	Monitoreo y evaluación de los procesos y servicios
410-15	Portal web, servicios telemáticos e internet
410-16	Capacitación relacionada a las tecnologías de la información y comunicaciones
410-17	Firmas electrónicas

Fuente: Adaptado de Contraloría General del Estado (2023)
Elaborado por: Henriquez (2024)

1.5.16 Normas ISO

Las Normas ISO (International Organization for Standardization) constituyen un conjunto de pautas mundiales diseñadas para asistir a las organizaciones en la implementación de uniformidad en términos de administración, procedimientos y excelencia (Yánez & Yánez, 2012).

Las normas ISO/IEC 27000 ofrecen una serie de recomendaciones encaminadas a las buenas prácticas en relación del Sistema de Gestión de Seguridad de la Información para la mejora continua y mitigación de riesgos, las mismas pueden ser aplicadas en cualquier organización (Baena et al., 2019).

Tabla 8

Principales Normas ISO para el sistema de seguridad de información

Normas para la seguridad de la información	
ISO 27001	Sistemas de gestión de seguridad de la información.
ISO 27002	Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información.
ISO 27005	Seguridad de la información, ciberseguridad y protección de la privacidad: directrices para la gestión de riesgos de seguridad de la información".
ISO 27007	Guía para la auditoría de seguridad de la información.
Norma para la gestión del riesgo	
31000	Gestión del riesgo
Norma para la evaluación del sistema de calidad de los procesos	
15504	Niveles de capacidad de los procesos

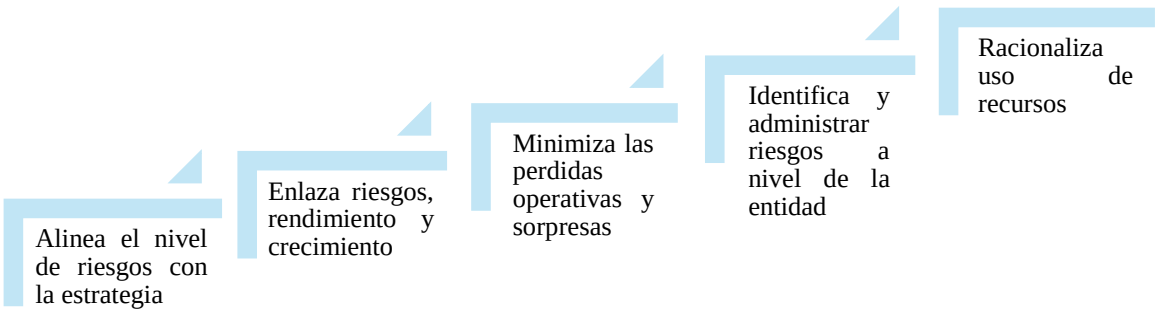
Fuente: Adaptado de Organización Internacional de Normalización (2008)
Elaborado por: Henriquez (2024)

1.5.17 Modelo COSO ERM

El COSO ERM actúa como facilitador del proceso de gestión de riesgos, según Sánchez Sánchez (2016) este permite a los directivos de las organizaciones operar de manera más efectiva en un entorno caracterizado por la incertidumbre.

Ilustración 14

Características del COSO ERM



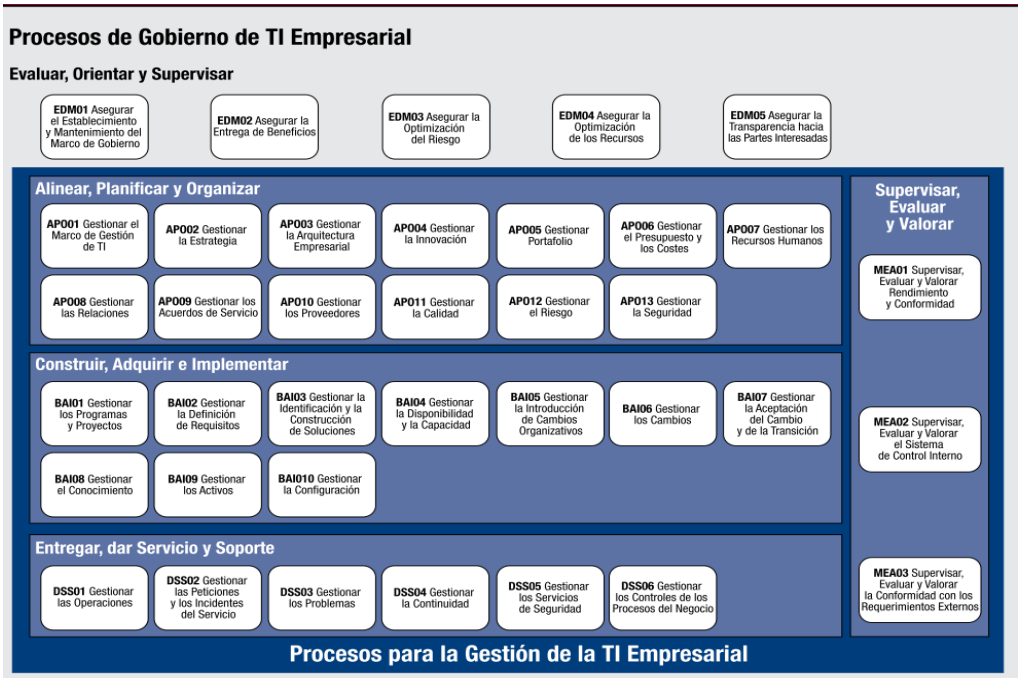
Fuente: Sánchez (2016)
Elaborado por: Henriquez (2024)

1.5.18 Marco de Referencia COBIT

COBIT (Control Objectives for Information and related Technology) es un marco de gestión y gobernanza de TI cuyo objetivo es ayudar a las organizaciones a desarrollar, organizar y gestionar sus estrategias de TI para alinearlas con sus objetivos empresariales y maximizar el valor de las inversiones tecnológicas. Según ISACA (2012) proporciona un conjunto integral de herramientas, prácticas, principios y modelos; COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales, dentro de los cuales se encuentran procesos; dentro de ellos se definen prácticas clave como se muestra en la siguiente ilustración.

Ilustración 15

Modelo de Referencia de Procesos de COBIT 5



Fuente: ISACA (2012)
Elaborado por: Henriquez (2024)

CAPITULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Unidad de análisis

Para el presente proyecto integrador se utilizó como unidad de análisis a la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. ubicada en la provincia de Tungurahua cantón Ambato. Su edificio matriz está en las calles Juan B. Vela y Martínez esq. Se extrajo información principalmente del departamento de sistemas de la información y seguridad de la información.

Para la ejecución de la auditoría se elaboró hojas de trabajo, con referencia a la información del sistema de información de la cooperativa, así como también activos de información, vulnerabilidades, amenazas y riesgos, con lo cual se obtuvo hallazgos que permitieron identificar diferentes falencias los cuales se presentaron para que tanto la gerencia como los directores departamentales tomen decisiones acertadas, y ayuden para el crecimiento y bienestar de la entidad.

2.1.2 Fuentes y técnicas de recolección de información

2.1.2.1 Fuentes de información primaria

Para el presente proyecto integrador se utilizaron como fuente primaria los datos recopilados a través de entrevistas realizadas al personal de la cooperativa, para lo cual se aplicó la técnica de la entrevista al Ing. en sistemas de información quien es el encargado de gestionar el área de TI, que a su vez proporcionó información relevante del sistema de información y al jefe de seguridad de la información, quién proporcionó información sobre activos de información y seguridad de estos, de igual manera se entrevistó al gerente para obtener información general sobre la gestión de la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda.

Tabla 9 Personas entrevistadas y encuestadas

Personas entrevistadas y encuestadas

Nombres	Cargo	Departamento
Juan Andagana	Gerente	Gerencia General
Víctor Bombón	Ingeniero en sistemas de información	Sistemas de información
Marcelo Herrera	Oficial en seguridad de la información	Seguridad de la información
Lorena Chaquinga	Directora de riesgos	Riesgos
Karina Ortiz	Directora de procesos	Procesos
Frank Cañizares	Director de talento humano	Talento Humano
Miriam Bautista	Directora de Operaciones	Operaciones

Elaborado por: Henriquez (2024)

Entrevista. – La entrevista se realizó al señor gerente el 22 de abril de 2024 a las 15:30 de forma presencial en las oficinas de la cooperativa Kullki Wasi Ltda., por medio del guion de entrevista que permitió recopilar información general de la cooperativa.

Guion de entrevista. – Se estructuraron 11 preguntas con respuestas abiertas referente a la información general de la cooperativa, permitiendo tener una visión global de aspectos importantes sobre la gestión de la misma.

Tabla 10

Guion de entrevista

	Preguntas de la entrevista	Tema
1.	¿La cooperativa dispone de un código de ética?	Ética y Socialización
2.	¿Si la respuesta fue afirmativa a la pregunta anterior comente si el código ha sido socializado entre sus empleados?	
3.	¿La cooperativa cuenta con estrategias y metas institucionales a corto o largo plazo?	Estrategias y Políticas Institucionales
4.	¿La cooperativa tiene definido políticas internas por departamento?	
5.	¿La cooperativa tiene un plan estratégico institucional o por departamentos?	
6.	¿La cooperativa evalúa el FODA institucional y con qué frecuencia lo realiza?	Evaluación y Análisis
7.	¿La cooperativa realiza evaluación de la eficiencia, eficacia, economía a través de indicadores?	
8.	¿Para el registro de sus transacciones operativas, la cooperativa utiliza un Software Contable? Señale el nombre de este.	
9.	¿Se mantienen reuniones frecuentes con el departamento de TI para evaluar las posibles amenazas, vulnerabilidad y riesgos a los que está expuesto la información de la cooperativa?	Gestión de TI y Seguridad Informática
10.	¿La gerencia tienen conocimiento completo sobre el plan de seguridad de la información que manejan los departamentos a cargo del gobierno y gestión de las TI?	
11.	¿La gerencia se ha involucrado en aportar acciones para el plan de contingencia sobre riesgos informáticos?	

Fuente: Muñoz (2002)
Elaborado por: Henriquez (2024)

Entrevista. - La entrevista se realizó al Ing. en sistemas el 23 de abril de 2024 a las 16:30 de forma presencial en las oficinas de la cooperativa Kullki Wasi Ltda., por medio del guion de entrevista que permitió recopilar información respecto al sistema de información.

Guion de entrevista. – Se estructuraron con 15 preguntas con respuestas abiertas referente a varios aspectos importantes a evaluar como son los activos de información, vulnerabilidades, amenazas, riesgos, donde se obtuvo información clara y precisa.

Tabla 11

Preguntas de la entrevista

	Preguntas	Tema
1.	¿Se ha realizado anteriormente auditorías de sistemas en la cooperativa	Auditoría de sistemas
2.	¿Tienen identificados los activos de información por departamentos?	Identificación y
3.	¿Realizan evaluaciones periódicas a los activos de información?	Evaluación de
4.	¿Cada qué tiempo evalúan los activos de información?	Activos de
5.	¿Cuáles son los activos de información más relevantes o críticos que se han identificado en el área tecnológica?	Información
6.	¿Cuáles son las vulnerabilidades, amenazas y riesgos del área de sistemas**?**	Vulnerabilidades,
7.	¿Evalúan las amenazas, vulnerabilidades y riesgos del sistema de información**?**	Amenazas y Riesgos
8.	¿El departamento tiene definido planes de contingencia contra riesgos informáticos?	Planes de Contingencia y
9.	¿Tienen definidos controles ante las amenazas que están expuestos los activos de información más importantes?	Gestión de Riesgos Informáticos
10.	¿Existen políticas específicas para la administración de activos de información en la cooperativa? ¿Cuáles son?	
11.	¿Existen el cumplimiento de políticas y procedimientos establecidos para los sistemas de información?	Políticas y procedimientos
12.	¿Realizan un seguimiento continuo a las políticas y procedimientos establecidos?	
13.	¿Cuáles son los medios de almacenamiento para los backups de las bases de datos de las herramientas informáticas que utiliza la cooperativa?	Seguridad de la Información y Almacenamiento
14.	¿Realizan un seguimiento a los controles implementados en seguridad de la información?	
15.	¿Evalúan niveles de madurez tanto en los riesgos como en la gestión y gobierno de las TI? ¿Qué procesos han evaluado?	Evaluación de COBIT

Fuente: Adaptado de Muñoz (2002)
Elaborado por: Henriquez (2024)

Adicionalmente, se aplicó la técnica de la observación a través de una lista de verificación como instrumento que permitió identificar in situ los procedimientos de control y la utilización de las tecnologías, así como factores importantes en la

seguridad de la información, y también una lista de verificación para verificar los procesos que serán evaluados en el marco de referencia COBIT, finalmente se evaluó mediante un cuestionario la información a través del método COSO ERM.

Observación. – La técnica de observación se realizó el 24 de abril de 2024 a las 15:00 de forma presencial en la cooperativa Kullki Wasi Ltda., por medio de una lista de verificación al Ing. en sistemas de información Víctor Bombón donde se anotó aspectos relevantes.

Lista de verificación. –Se realizó una lista de verificación con 12 preguntas para verificar el cumplimiento de una serie de aspectos relevantes para el buen desempeño empresarial.

Tabla 12

Preguntas de la lista de verificación

Preguntas	SI	NO	Observación
1. ¿La instalación de la red local es flexible y adaptable a las necesidades departamentales para la conexión de los equipos informáticos de la cooperativa?			
2. ¿Las direcciones IP's configuradas en la red permite dar seguimiento de las conexiones entrantes para su funcionamiento?			
3. ¿Existen niveles de acceso y seguridad en la red? ¿Cuáles son?			
4. ¿Evalúan las medidas preventivas o correctivas en caso de siniestros en el sistema contable?			
5. ¿Realizan respaldos o backups de la base de datos? ¿Con qué frecuencia?			
6. ¿Se verifica la vigencia de antivirus? ¿Con qué frecuencia?			
7. ¿Tienen controles en los procesos operativos? ¿Qué tipos de controles?			
8. ¿Manejan bitácoras de las revisiones que se hacen a los sistemas de información?			
9. ¿Tienen políticas de seguridad para el acceso a las instalaciones?			

10. ¿Cuentan con la señalética de emergencia y acceso a las instalaciones?	
11. ¿Tienen instaladas cámaras de seguridad en las áreas operativas de la cooperativa?	
12. ¿Cumplen con los parámetros establecidos en la normativa ISO 27000?	

Fuente: Adaptado de Muñoz, (2002)
Elaborado por: Henriquez (2024).

Observación. – La técnica de observación se realizó el 26 de abril de 2024 a las 15:30 de forma presencial en la cooperativa Kullki Wasi Ltda., por medio de una lista de verificación al Ing. en sistemas de información Víctor Bombón para verificación de los procesos a evaluar del COBIT.

Lista de verificación. –Se realizó una lista de verificación con 37 principios agrupados para verificar cuáles serán los procesos necesitan ser evaluados en el marco de referencia COBIT.

Tabla 13

Verificación de los procesos a ser evaluados

NIVELES DE MADUREZ				
	Descripción de los procesos	**SI**	**NO**	**Observación**
1	**EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno** Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.			
2	**EDM02 Asegurar la Entrega de Beneficios** Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.			
3	**EDM03 Asegurar la Optimización del Riesgo** Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.			
4	**EDM04 Asegurar la Optimización de Recursos** Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.			
5	**EDM05 Asegurar la Transparencia hacia las Partes Interesadas**			

	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas..

Fuente: ISACA (2012)
Elaborado por: Henriquez (2024)

Se evaluaron 16 principios en los cuales participaron 5 departamentos: departamento de sistema de información, seguridad de la información, riesgos, procesos, operaciones.

Evaluación. - Se realizó una evaluación al Ing. en sistemas y al Ing. en seguridad de la información el 26 de abril de 2024 a las 16:00 de forma presencial en las oficinas de la cooperativa Kullki Wasi Ltda., por medio de un cuestionario COSO ERM que permitió recopilar información respecto al control interno de las áreas de sistemas de información y seguridad de la información.

Cuestionario. – Se realizó un cuestionario con preguntas 55 preguntas estructuradas donde constan los 6 componentes sobre los sistemas de información, el control interno y lo referente a riesgos.

Tabla 14

Preguntas del cuestionario COSO ERM 2017

Preguntas sobre el Gobierno y cultura organizacional en el marco del COSO ERM 2017	Dimensión o categoría	SI	NO	N/A
¿Existen políticas que incluyan controles de TI?	Gobierno y cultura			
¿Se han definido, asignado y aceptado las responsabilidades de TI y de controles de TI				
¿Se dispone de especialistas con competencias en auditoría de TI (sea interna o externamente)?	Estrategias y objetivos			
¿Tiene en cuenta los riesgos relacionados a los factores internos y externos a los que se encuentra expuesta la empresa?				
¿Se han asegurado lógica y físicamente los equipos y herramientas de la infraestructura de TI?	Desempeño			
¿Se ha implementado una tecnología de filtros de seguridad conforme a la política de la empresa (por ejemplo, en lo lugares de conexiones externas, como Internet, y en los lugares donde se				

necesita una separación entre redes internas)?	
¿Se usan mecanismos de control para el acceso y la autenticación?	
¿Se ha implementado un software antivirus y se realiza su mantenimiento?	Revisión
¿Identifica información relevante y canales para la comunicación y divulgación interna y externa?	Información
¿Comunica internamente información relevante entorno a los riesgos relacionados con la empresa?	Comunicación y Reporte
¿Permiten las copias de seguridad resolver en un plazo satisfactorio las pérdidas de información o fallos a causa de la materialización de las amenazas?	Sistemas de Seguridad de información
¿Se llevan las copias de seguridad a dispositivos externos o en la nube?	

Fuente: Auditool (2024)
Elaborado por: Henriquez (2024)

2.1.2.2 Fuentes de información secundaria

Las fuentes secundarias fueron tomadas de la revisión de artículos científicos y textos sobre la auditoría de sistemas de información, así como la página web institucional.

2.1.3 Fases del desarrollo

Tabla 15

Fases de auditoría

Objetivos	Fase o etapa	Descripción
Elaborar la planificación de auditoría al sistema de información para la determinación de los niveles de riesgo y enfoque de auditoría	Planificación	Para la planificación se recolecto la documentación preliminar mediante una visita previa a la cooperativa. Se aplicó una entrevista al gerente para determinar la situación estatutaria y organizativa de la institución y también una entrevista al Ing. en sistemas para obtener información relevante sobre el sistema de información. Finalmente, como resultado se obtuvo el memorando de planificación, la creación del programa de auditoría y el marco COSO ERM 2017.
Ejecutar la auditoría al sistema de información para la	Ejecución	Para la fase de ejecución se identificó y evaluó vulnerabilidades, amenazas y riesgos de los

evaluación de los procesos en el nivel de informatización y tratamiento de los datos verificando los controles en el procesamiento y sistemas de seguridad		activos de información, se utilizó el marco de referencia COBIT y se obtuvo papeles de trabajo y hallazgos.
Comunicar los resultados de la auditoría al sistema de información a través del informe para la toma de decisiones de la alta gerencia	Resultados	Para la fase de comunicación de los resultados se realizó un informe preliminar de auditoría con base a la ejecución de los procesos de auditoría de sistemas de información, se comunica a la gerencia y jefes departamentales de sistemas y seguridad de la información, como no existió cambios se emitió el informe final de auditoría, en el que se detalla los hallazgos conclusiones y recomendaciones.
Seguimiento a las recomendaciones	Seguimiento y monitoreo	Se elaboró una matriz de seguimiento a los controles y políticas de seguridad de la información para la mejora continua de los procesos que involucra a salvaguardar los activos de información.

Fuente: Elaboración propia

2.1.3.1 Criterios para la fase de planificación

Dentro de la planificación se realizó la recolección de información de cooperativa para la aplicación del marco de referencia COSO ERM 2017 para analizar los controles con el fin de conocer el nivel de confianza y riesgo.

Tabla 16

Medición de confianza y riesgo

Nivel de confianza		
BAJO	**MODERADO**	**ALTO**
5% - 50%	51% - 75%	76% - 95%
95% - 50%	49% - 25%	24% - 5%
ALTO	**MODERADO**	**BAJO**
Nivel de riesgo		

Fuente: COSO ERM (2017)
Elaborado por: Henriquez (2024)

Para realizar la evaluación del nivel de madurez y eficiencia del sistema de control interno se estableció criterios de calificación a cada uno de los componentes como se muestra en la tabla 17.

Tabla 17

Criterios de calificación de los componentes

CRITERIOS DE CALIFICACIÓN DE LOS COMPONENTES	
Efectivo	4.1-5.0
Cumplimiento básico- táctico	3.1-4.0
En proceso	2.1-3.0
Crítico y reactivo	1.1-2.0

Fuente: COSO ERM (2017)
Elaborado por: Henriquez (2024)

2.1.3.2 Criterios para la fase de ejecución

Para la fase de ejecución se aplicó las normas ISO/TEC 27000 para evaluar los activos de la cooperativa considerando los criterios de confidencialidad, integridad y disponibilidad para saber el valor del activo y su nivel de tasación y así la posible explotación de la vulnerabilidad.

Tabla 18

Criterios de confidencialidad

Valor del Activo	Confidencialidad
5 (Muy alto)	Solo el personal de alto rango tiene autorización para acceder a la información del activo, ya que su divulgación causaría daños irreparables en la empresa.
4 (Alto)	La información del activo está restringida y solo el personal designado tiene permiso para acceder a ella, siendo su divulgación un asunto grave para la empresa.
3 (Medio)	La información del activo se considera confidencial y solo el personal interno tiene la capacidad de acceder a ella, por lo que su divulgación tendría un impacto considerable en la empresa.
2 (Bajo)	La información del activo es de uso interno y solo el personal de ABC puede acceder a ella, por lo que su divulgación afectaría parcialmente a la empresa.
1 (Muy bajo)	La información del activo es de dominio público, accesible para cualquier persona, y no tendría ningún impacto en la empresa.

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 19

Criterios de Integridad

Valor del Activo	Integridad

5 (Muy alto)	El activo no puede experimentar pérdida o alteración alguna en sus componentes, ya que cualquier vulneración de su integridad sería irreversible para la empresa.
4 (Alto)	El activo puede tolerar una pérdida o alteración de hasta un 15% en sus componentes, lo que constituiría una violación seria para la empresa.
3 (Medio)	El activo puede soportar una pérdida o alteración de hasta un 50% en sus componentes, lo que afectaría significativamente a la empresa.
2 (Bajo)	El activo puede tolerar una pérdida o alteración de hasta un 85% en sus componentes, lo que afectaría parcialmente a la empresa.
1 (Muy bajo)	El activo puede tolerar una pérdida o alteración del 100% en sus componentes, sin impacto alguno.

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 20

Criterios de Disponibilidad

Valor del Activo	Disponibilidad
5 (Muy alto)	Se requiere que el activo no se esté indisponible, su falta afectaría irreparablemente a la empresa.
4 (Alto)	Se considera que el activo pueda estar indisponible máximo por una hora, su falta sería grave para la empresa.
3 (Medio)	Se considera que el activo pueda estar indisponible máximo por un día, pues su falta afectaría considerablemente a la empresa.
2 (Bajo)	Se considera que el activo pueda estar indisponible máximo por una semana, su falta afectaría parcialmente a la empresa.
1 (Muy bajo)	Se considera que el activo pueda estar indisponible por tiempo indefinido, su falta no tiene ningún impacto en la empresa.

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 21

Nivel de Tasación

Valor del Activo	Nivel de tasación
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 2.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy bajo

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Se evaluó también los controles que tiene la cooperativa ante los riesgos, como se muestra en la tabla 22.

Tabla 22

Valoración de controles de los activos

Valoración de controles de los activos			
Frecuencia de control	**Valores**	**Descripción**	**Guía**
Bajo	1	El nivel de control es bastante bajo, lo que permite que la empresa funcione, pero aumenta la posibilidad de que los riesgos se materialicen.	>1 año
Medio	2	Se implementa cierto grado de control, lo que permite que la empresa siga operando, pero podría haber efectos adversos en algunos procesos, como retrasos en actividades o errores.	>= 3 meses< 1 año
Alto	3	El control alcanza su máximo nivel, lo que resulta en una mínima incidencia de fallos en las actividades y el desarrollo empresarial.	< 3 meses

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 23

Valoración de la probabilidad de ocurrencia de riesgos

Valoración de la probabilidad de ocurrencia de riesgos		
Frecuencia del riesgo	**Valores**	**Descripción**
Bajo	1	Puede ocurrir al menos 1 vez en periodos mayores a 5 años
Moderado	2	Puede ocurrir al menos 1 vez en periodos de 1 a 5 años
Medio	3	Puede ocurrir al menos una vez al año
Alto	4	Puede ocurrir al menos una vez al mes
Muy alto	5	Puede ocurrir al menos una vez a la semana

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 24

Valoración de impacto de ocurrencia de riesgos

Frecuencia de riesgo	Valores	Descripción
Bajo	1	El nivel de impacto es mínimo, lo que permite que la empresa siga operando, aunque existe la posibilidad de que el riesgo se materialice.
Moderado	2	Se observa un cierto grado de impacto, lo que permite que la empresa continúe operando, pero puede haber obstáculos en algunos procesos, retrasos en actividades o errores.
Medio	3	El impacto es evidente, aunque la empresa puede seguir operando, existe una mayor probabilidad de enfrentar obstáculos en varios procesos, experimentar retrasos en actividades o cometer errores.
Alto	4	El impacto es significativo, lo que afecta las operaciones internas y puede resultar en la inactivación de procesos y la paralización de actividades.
Muy alto	5	El impacto es extremadamente grave, causando una interrupción severa en las operaciones internas, lo que lleva a la inactivación de procesos y la paralización total de actividades.

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Tabla 25

Nivel del riesgo

Nivel del riesgo	
Frecuencia del riesgo	**Calificación (Probabilidad*Impacto)**
Bajo	<3
Moderado	<5
Medio	<10
Alto	<20
Muy alto	>20

Fuente: ISO 27000 (2024)
Elaborado por: Henriquez (2024)

Luego se realizó el Marco de Referencia COBIT, según los requerimientos de la cooperativa solo se evaluaron algunos procesos presentados en la siguiente tabla.

Tabla 26

Procesos evaluados de COBIT

N.	PROCESOS	DESCRIPCIÓN
1	EDM03 Asegurar la Optimización del Riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.
2	EDM04 Asegurar la Optimización de Recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.
3	APO01 Gestionar el Marco de Gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.
4	APO02 Gestionar la Estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.
5	APO04 Gestionar la Innovación	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.
6	APO07 Gestionar los Recursos Humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.
7	AP009 Gestionar los acuerdos de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.
8	APO11 Gestionar la Calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

9	APO12 Gestionar el Riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
10	APO13 Gestionar la Seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.
11	BAI02 Gestionar la Definición de Requisitos	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.
12	BAI09 Gestionar los Activos	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia
13	DSS01 Gestionar Operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.
14	DSS04 Gestionar la Continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.
15	DSS05 Gestionar Servicios de Seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.
16	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

Elaborado por: Henriquez (2024)

Se evaluó las actividades que se encuentran dentro de las prácticas clave, para lo cual se debe detallar los niveles de capacidad de cada proceso para obtener el nivel de madurez.

Tabla 27

Niveles de capacidad de los procesos

NIVELES DE CAPACIDAD DE PROCESOS NORMAS ISO 15504		
NIVEL	**CRITERIO**	**DESCRIPCIÓN**
NIVEL 0	Incompleto	Falta de cualquier capacidad básica. Estrategia incompleta para abordar el propósito de gobierno y gestión la obtención de todas las practicas del proceso puede haberse definido o no.
NIVEL 1	Ejecutado	El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas.
NIVEL 2	Administrado	El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.
NIVEL 3	Establecido	El proceso logra su propósito de forma mucho más organizada utilizando activos. Los procesos por lo general están bien organizados.
NIVEL 4	Predecible	El proceso logra su propósito está bien definido y opera de acuerdo con los objetivos de rendimiento definidos
NIVEL 5	Optimizado	El proceso logra su propósito, está bien definido, Mejora continuamente para ayudar a alcanzar los objetivos actuales y futuros.

Fuente: ISO/IEC 15504 (2024)
Elaborado por: Henriquez (2024)

Tabla 28

Niveles de madurez de los procesos

NIVEL DE MADUREZ	NORMAS ISO 15504		NIVEL DE CAPACIDAD
SIGLAS	**DESCRIPCIÓN**	**VALORACIÓN**	
F	Completamente	>85%-100%	5
L	En gran medida	>50%-85%	3–4
P	Parcialmente	>15%-50%	1–2
N	No cumple	0%-15%	0

Fuente: ISO/IEC 15504 (2024)
Elaborado por: Henriquez (2024)

CAPÍTULO III

DESARROLLO

3.1 Resultado

3.1.1 Planificación

El presente proyecto integrador tuvo por objetivo realizar una Auditoría al sistema de información de la cooperativa Kullki Wasi Ltda. Ambato aplicando las fases correspondientes de la auditoría. Se mostrará el desarrollo de la Fase I de Planificación en la cual se obtuvo toda la información competente de la cooperativa para los análisis y conocimiento de su situación actual, para plantear soluciones.

3.1.1.1 Memorándum

Se realizo el memorándum de planificación de la auditoría, donde se asegura que la auditoría se lleve a cabo de manera eficiente y efectiva.

Ilustración 16

Memorándum de planificación

"NATEF"AUDITORES INDEPENDIENTES M.M

MEMORANDO DE PLANIFICACIÓN
PERIODO DEL AÑO 2024

Entidad : COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA.
Auditoria: AUDITORÍA DE SISTEMAS
Periodo: 2024

1. REQUERIMIENTO DE LA AUDITORIA

Informe de auditoría de sistemas

2. FECHA DE INTERVENCION	**Fecha estimada**
Marco de referencia COSO ERM 2017	09/05/2024
Aplicación normas ISO 27000	15/05/2024
Matriz de riegos	17/05/2024
Marco de referencia COBIT	20/05/2024

3. EQUIPO MULTIDISCIPLINARIO	
NOMBRE	**INICIALES**
Nathaly Estefania Henriquez Cisneros	NEHC

4. RECURSOS

Para la elaboración del proyecto integrador se contó con la participación de la Dra. Patricia Jiménez como tutora y mi persona Nathaly Henriquez estudiante de la Facultad de contabilidad y Auditoría, de la carrera de Contabilidad y Auditoría de la Universidad Técnica de Ambato

MATERIALES	
Hardware y Software	$100,00
Gastos de transporte	$100,00
Oficios	$50,00
Copias	$50,00
$	**300,00**

5. ENFOQUE DE LA AUDITORIA

5.1 Información general de la entidad auditada

-Misión

Fomentar el desarrollo de nuestros socios y clientes, brindando servicios financieros inclusivos, con transparencia, calidad, responsabilidad social y ambiental.

-Visión

Ser una instutición innovadora, reconocida, y con enfoque de calidad.

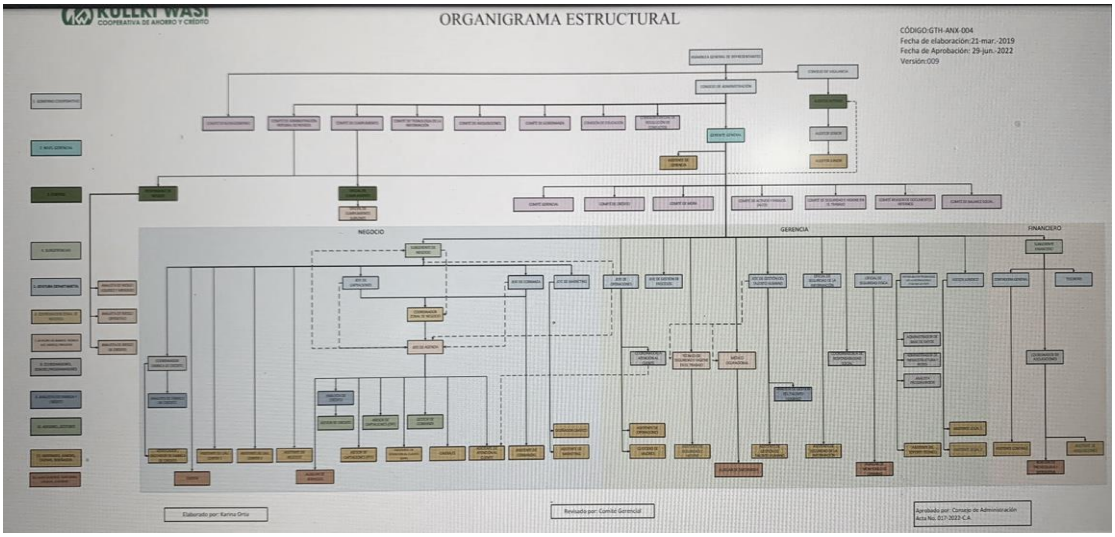
-Objetivo

Mejorar la calidad de vida de sus asociados; su accionar financiero está dirigido a lograr la sostenibilidad y crecimiento económico, promoviendo la inclusión social, compromiso, trabajo grupal, solidaridad y la confianza mutua entre socios y administradores con gestión responsable; a través de sus 19 Agencias ubicadas estratégicamente en las provincias de Tungurahua, Chimborazo, Bolívar, Cotopaxi, Pichincha, Santo Domingo, Guayas y Galápagos.

-Actividades Principales

Ahorros
Créditos
Inversiones

-Estructura orgánica



- Base Legal

- Ley orgánica de Economía Popular y Solidaria
- Código de Trabajo
- Ley de Seguridad Social
- Ley Orgánica de Régimen Tributario
- Código Tributario
- Reglamento a la Aplicación de la Ley de Régimen Tributario

5.2 Motivo de la auditoría

La auditoría esta direccionada al sistema de información de la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. Para recopilar información en cuanto al sistema de información

5.3 Enfoque a:

Auditoría al sistema de información de la Cooperativa de Ahorro y Crédito Kulkki Wasi Ltda.

5.4. Objetivos

Objetivo General

Realizar una Auditoría del sistema de información en la Cooperativa Kullki Wasi Ltda., para la evaluación de su nivel de confianza en la seguridad y confiabilidad.

Objetivos Específicos

• Elaborar la planificación de auditoría a los sistemas de información para la determinación de los niveles de riesgo y enfoque de auditoría.

• Ejecutar la auditoría a los sistemas de información para la evaluación de los procesos en el nivel de informatización y tratamiento de los datos verificando los controles en el procesamiento y sistemas de seguridad.

• Comunicar los resultados de la auditoría a los sistemas de información a través del informe para la toma de decisiones de la alta gerencia.

5.5. Alcance

Esta direccionado a los activos de información, vulnerabilidades, amenazas, riesgos, gobierno y gestión de las TI

5.6. Resumen de los Resultados de la Evaluación del Control Interno.

COMPONENTE	PONDERACIÓN TOTAL	CALIFICACIÓN TOTAL	NIVEL DE CONFIANZA %	NIVEL DE RIESGO %	SEMAFORIZACIÓN NIVEL DE CONFIANZA
GOBIERNO Y CULTURA	9	9	100,00%	0,00%	Alto
ESTRATEGIAS Y OBJETIVOS	5	3	60,00%	40,00%	Moderado
DESEMPEÑO	8	5	62,50%	37,50%	Moderado
REVISIÓN	8	8	100,00%	0,00%	Alto
COMUNICACIÓN Y REPORTE	7	5	71,43%	28,57%	Moderado
SEGURIDAD DE INFORMACIÓN	18	18	100,00%	0,00%	Alto

5.7. Grado del nivel de madurez y eficiecia del sistema de control interno			
DETERMINACIÓN DEL NIVEL DE MADUREZ Y EFICIENCIA DEL SISTEMA DE CONTROL INTERNO CALIFICACIÓN DE LOS COMPONENTES			
No.	**COMPONENTE**	**NIVEL DE MADUREZ**	**CALIFICACIÓN COMPONENTE**
1	GOBIERNO Y CULTURA ORGANIZACIONAL	4,78	EFECTIVO
2	ESTRATEGIAS Y OBJETIVOS	3,00	EN PROCESO
3	DESEMPEÑO	3,25	CUMPLIMIENTO BÁSICO -TÁCTICO
4	REVISIÓN	4,63	EFECTIVO
5	INFORMACIÓN, COMUNICACIÓN Y REPORTE	3,29	CUMPLIMIENTO BÁSICO -TÁCTICO
6	SISTEMAS DE SEGURIDAD DE INFORMACIÓN	4,44	EFECTIVO
	VALORACIÓN DEL COMPONETE	**3,90**	CUMPLIMIENTO BÁSICO -TÁCTICO
6 TRABAJO A REALIZAR EN LA FASE DE EJECUCIÓN			
6.1 TRABAJO A REALIZAR POR LOS AUDITORES EN LA FASE DE EJECUCIÓN			
Analisis de riesgos, vulnerabilidades y amenazas Marco de referencia COBIT			
7. COLABORACIÓN DE LA ENTIDAD AUDITADA			
7.1 Ingeniero encargados del departamento de TI			
Victor Bombón			
7.2 Ingeniero encargado del departamento de seguridad de la información			
Marcelo Herrera			
7.1 Ingeniera encargada del departamento de riesgos			
Lorena Chachinga			
7.1 Ingeniera encargada del departamento de procesos			
Karina Ortiz			
7.1 Ingeniera encargada del departamento de operaciones			
Miriam Bautista			

Elaborado por: Henriquez (2024)

3.1.1.2 Programa de auditoría

Se realizó el programa de auditoría detallando los procedimientos y técnicas utilizadas

Ilustración 17

Programa de auditoría

"NATEF"AUDITORES INDEPENDIENTES					P.A
PROGRAMA DE AUDITORÍA					
OBJETIVOS					
Evaluar el sistema de información de la entidad con apoyo del área de sistemas de información y seguridad de la información Aplicar marco de referencia COSO ERM 2017 Aplicar las normas ISO/IEC 27000 Delimitar niveles de riesgo en los activos de información Evaluar la gestión y gobierno de TIa con la metodología COBIT					
ALCANCE					
Evaluación a los activos de información, detectando vulnerabilidades, amenazas, previniendo los posibles riesgos que atenten al sistema de información Evaluación de la mejora continua ITIL,para la gestión de servicios de tecnologías de la información					
N.	**PROCEDIMIENTOS**	**TIPOS DE PROCEDIMIENTOS**	**TÉCNICA**	**ELABORADO POR**	**FECHA**
1	Levantamiento de activos de información	Pruebas de cumplimiento	Observación y verificación	NEHC	06/05/2024
2	Evaluación del control interno	Pruebas de cumplimiento	Cuestionario COSO ERM	NEHC	09/05/2024
3	Identificación de las vulnerabilidades, amenazas y riesgos de los activos de información	Pruebas sustantivas	Matriz evaluación ISO/IEC 27000	NEHC	15/05/2024
4	Evaluación de riesgos de activos de información	Pruebas sustantivas	Matriz de riesgo	NEHC	17/05/2024
5	Evaluación del nivel de madurez	Pruebas sustantivas	Marco de referencia COBIT	NEHC	20/05/2024

Elaborado por: Henriquez (2024)

3.1.1.3 Guía de visita previa

Se elaboró la guía de visita previa con la información general y de los departamentos de TI y seguridad de la información.

Ilustración 18

Guía de visita previa

"NATEF"AUDITORES INDEPENDIENTES	P.A
FASE I PLANIFICACIÓN **GUÍA DE VISITA PREVIA**	
1. INFORMACIÓN GENERAL	
1.1 Entidad	Cooperativa Kullki Wasi Ltda.
1.2 N.RUC	1891710255001
1.3 Dirección de la entidad	Q95F+29C, Juan B. Vela y Martínez (Esquina), Ambato 180150
1.4 Correo electronico de la entidad	jandagana@hotmail.com
1.5 Visita	30 de abril de 2024
1.6 Entrevistados	Victor Bombon Marcelo Herrera
1.7 Entrevistador	Nathaly Henriquez
2. Información de los departamentos	
El departamento de sistemas de la información se encarga de controlar y dirigir las actividades encargadas del tratamiento de la información, redes de comunicación con acceso a los sistemas, mantenimiento a todos los componentes que son parte del sistema informático. El departamento de seguridad de la información encargado de todo lo competente con la seguridad de los activos de información, gestión de riesgos, proporciona liderazgo garantizando la confidencialidad, integridad y disponibilidad de sus recursos de información, detección y respuesta a incidentes.	

Elaborado por: Henriquez (2024)

3.1.1.4 COSO ERM

Para la evaluación del control interno, sus estrategias y la seguridad de la información, se utilizó el marco de referencia COSO ERM 2017. La información se recopiló del área de informática basándose en el sistema de información existente. Se elaboraron un total de 55 preguntas vinculadas a los principios y componentes del marco, lo que permitió cuantificar y medir el nivel de riesgo y confianza en el área de informática.

Ilustración 19

Nivel de confianza y riesgo

NIVEL DE CONFIANZA Y NIVEL DE RIESGO					
COMPONENTE	**PONDERACIÓN TOTAL**	**CALIFICACIÓN TOTAL**	**NIVEL DE CONFIANZA %**	**NIVEL DE RIESGO %**	**SEMAFORIZACIÓN NIVEL DE CONFIANZA**
GOBIERNO Y CULTURA	9	9	100,00%	0,00%	**Alto**
ESTRATEGIAS Y OBJETIVOS	5	4	60,00%	40,00%	**Alto**
DESEMPEÑO	8	6	75,00%	25,00%	**Moderado**
REVISIÓN	8	8	100,00%	0,00%	**Alto**
COMUNICACIÓN Y REPORTE	7	5	71,43%	28,57%	**Moderado**
SISTEMAS DE SEGURIDAD DE INFORMACIÓN	18	18	100,00%	0,00%	**Alto**

Elaborado por: Henriquez (2024)

Luego, se determinó el nivel de madurez y eficiencia de control interno de los componentes del COSO ERM 2017. Se puede mencionar que el componente gobierno y cultura organizacional alcanza un mayor nivel de madurez calificado con el 4,78 siendo efectivo, mientras que el componente estrategias y objetivos es menos eficiente alcanzando un nivel de madurez de 3, lo que significa que se encuentra en un nivel en proceso, de esta manera el promedio de los componentes para el nivel de madurez general es 3,90 lo cual indica que está ubicada en un nivel de cumplimiento básico táctico, por ende los procedimientos del Gobierno Corporativo no están documentados de manera adecuada pero se ejecutan en la operación diaria y el seguimiento de los procedimientos depende de la iniciativa de cada individuo y es poco probable que las posibles no conformidades sean detectadas.

Ilustración 20

Nivel de madurez y eficiencia del control interno

DETERMINACIÓN DEL NIVEL DE MADUREZ Y EFICIENCIA DEL SISTEMA DE CONTROL INTERNO CALIFICACIÓN DE LOS COMPONENTES			
No.	**COMPONENTE**	**NIVEL DE MADUREZ**	**CALIFICACIÓN COMPONENTE**
1	GOBIERNO Y CULTURA ORGANIZACIONAL	4,78	EFECTIVO
2	ESTRATEGIAS Y OBJETIVOS	3,00	EN PROCESO
3	DESEMPEÑO	3,25	CUMPLIMIENTO BÁSICO -TÁCTICO
4	REVISIÓN	4,63	EFECTIVO
5	INFORMACIÓN, COMUNICACIÓN Y REPORTE	3,29	CUMPLIMIENTO BÁSICO -TÁCTICO
6	SISTEMAS DE SEGURIDAD DE INFORMACIÓN	4,44	EFECTIVO
	VALORACIÓN DEL COMPONETE	**3,90**	CUMPLIMIENTO BÁSICO -TÁCTICO

Elaborado por: Henriquez (2024)

3.1.2 Fase de Ejecución

3.1.2.1 NORMAS ISO/IEC 27000 Evaluación a los activos de información

La realización de estas evaluaciones proporciona un conocimiento más detallado del nivel de tasación de los activos de la empresa, identificando cuáles son los más críticos y estableciendo medidas para minimizar y mitigar riesgos. Los tipos de activos de información se valoraron utilizando los criterios en función de los principios que menciona la norma en lo que respecta a confidencialidad, integridad y disponibilidad.

Posteriormente, se promediaron estos valores para obtener el valor total del activo o su nivel de tasación (importancia), obteniendo así los activos más relevantes o críticos de la cooperativa.

Ilustración 21

Nivel de tasación o criticidad de los activos de información

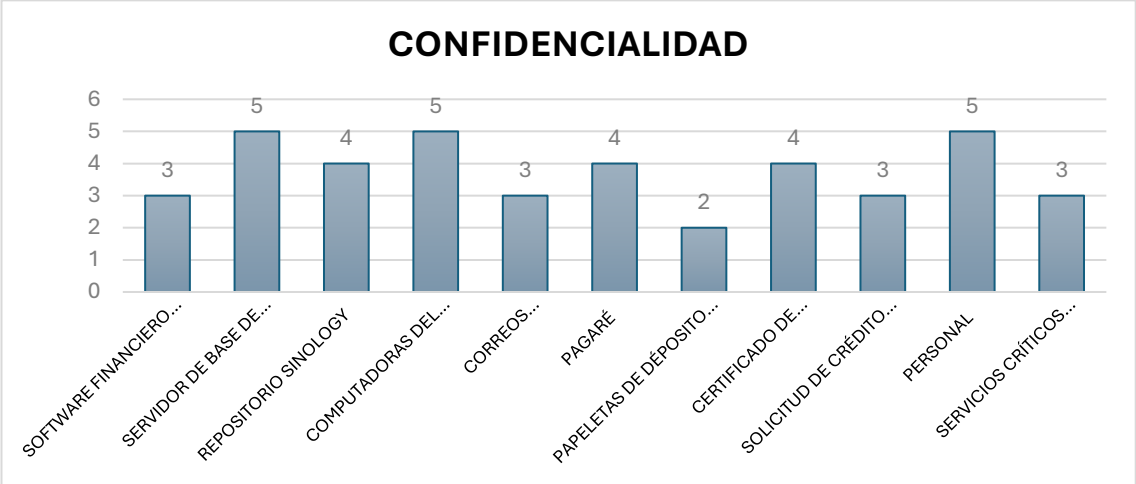
NIVEL DE TASACIÓN O CRITICIDAD ACTIVOS DE INFORMACIÓN						
TIPO DE ACTIVO	**NOMBRE DEL ACTIVO**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**VALOR**	**NIVEL DE TASACIÓN**
SOFTWARE	SOFTWARE FINANCIERO SOFTBANK	3	5	5	4,33	**MUY ALTO**
	SERVIDOR DE BASE DE DATOS	5	5	5	5,00	**MUY ALTO**
	REPOSITORIO SINOLOGY	4	5	5	4,67	**MUY ALTO**
ELECTRÓNICO	COMPUTADORAS DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN	5	5	5	5,00	**MUY ALTO**
	CORREOS ELECTRÓNICOS CON NIVEL DE AUTORIZACIÓN	3	5	5	4,33	**MUY ALTO**
	PAGARÉ	4	5	5	4,67	**MUY ALTO**
	PAPELETAS DE DÉPOSITO LLENAS	2	3	3	2,67	**MEDIO**
	CERTIFICADO DE DEPÓSITO A PLAZO LLENO	4	5	5	4,67	**MUY ALTO**
	SOLICITUD DE CRÉDITO LLENA	3	5	4	4,00	**ALTO**
PERSONAS	PERSONAL	5	4	4	4,33	**MUY ALTO**
SERVICIOS	SERVICIOS CRÍTICOS OFRECIDOS	3	4	5	4,00	**ALTO**

Elaborado por: Henriquez (2024)

En relación con el principio de la Confidencialidad, se pudo observar que el servidor de la base de datos, las computadoras del área de seguridad de la información son de suma importancia y por ende estos activos deben conservarse protegidos contra el acceso no autorizado, identificar oportunamente las vulnerabilidades y amenazas así como asegurar que solo las personas, procesos o sistemas autorizados tengan acceso a los mismos, considerado que el personal de la cooperativa debe comprometerse con el acuerdo de confidencialidad que es muy importante, con ello se garantiza que los datos de la institución se conserven protegidos, evitando así su divulgación no autorizada.

Ilustración 22

Principio #1 Confidencialidad

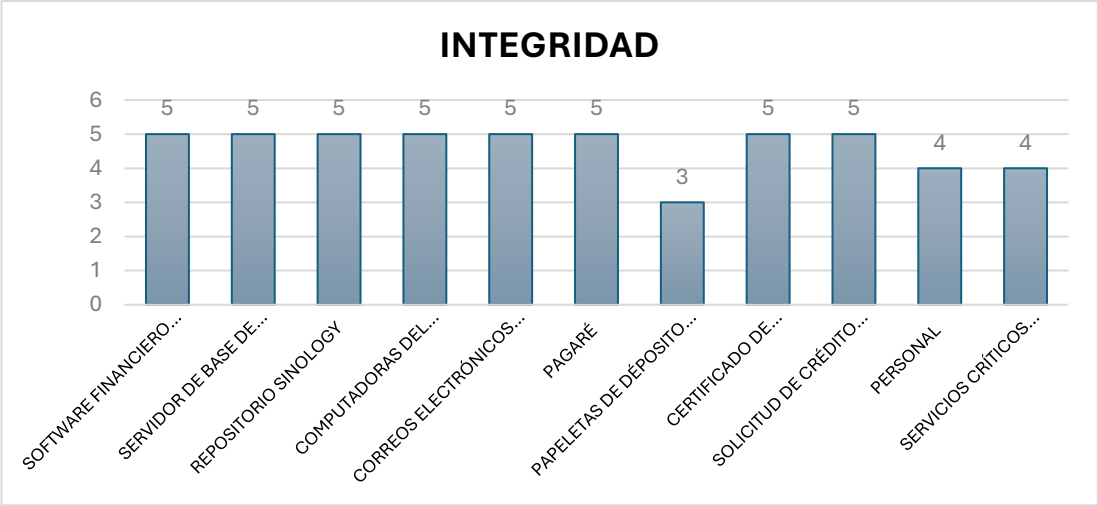


Elaborado por: Henriquez (2024)

Con respecto al principio de la Integridad, se pudo observar que la mayoría de los activos de la cooperativa no pueden tolerar una alteración o modificación de estos, ya que afectaría de manera considerable al proceso. La Integridad asegura que los datos y los sistemas de información se mantengan precisos, completos y sin alteraciones no autorizadas. Esto es crucial para garantizar que la información sea confiable y útil para la toma de decisiones adecuadas y las operaciones comerciales.

Ilustración 23

Principio #2 Integridad

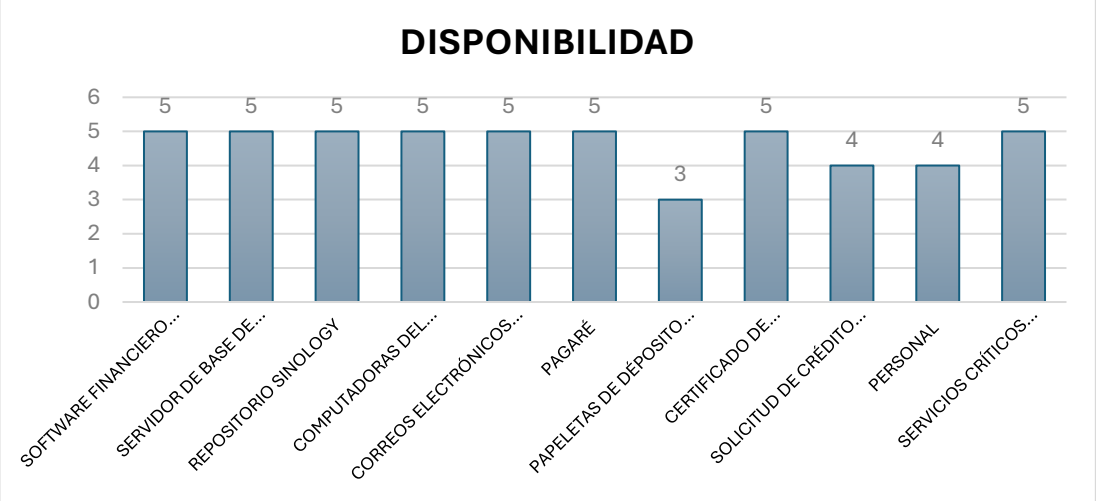


Elaborado por: Henriquez (2024)

Conforme al principio de la Disponibilidad, se determinó que la mayoría de los activos de la empresa deben estar siempre completamente disponibles. Si alguno de estos fallara, comprometería las actividades diarias de la entidad. La falta de disponibilidad de los activos de información puede provocar retrasos en el trabajo, interrupciones en los procesos cotidianos de la cooperativa y una disminución de la calidad del servicio, afectando así la capacidad de la organización para satisfacer las demandas de manera oportuna y eficiente.

Ilustración 24

Principio #3 Disponibilidad



Elaborado por: Henriquez (2024)

Luego, se realizó una evaluación de riesgos a los activos donde se evaluó la probabilidad de ocurrencia de las amenazas y el impacto, para obtener el riesgo y se calificó al riesgo en niveles bajo, moderado, medio, alto, muy alto, de esta manera se obtuvo como resultado los activos con nivel de riesgo más elevado, por consiguiente, los que se deben ser protegidos y controlados según el tratamiento al riesgo.

Ilustración 25

Evaluación de riesgos de los Activos

NIVEL DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN								
ACTIVO	VULNERABILIDAD	AMENAZA	RIESGO	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO	EVALUACIÓN DEL RIESGO (PROBABILIDAD DE OCURRENCIA*IMPACTO)	NIVEL DEL RIESGO
Software financiero Softbank	Desactualización de la información de la base de datos	Toma de decisiones ineficaces	R1	Riesgo operativo	2	5	10	ALTO Ψ
Servidor de la base de datos	Monitoreo y auditoría insuficientes	Los atacantes actúan sin ser detectados	R2	Robo de información	1	5	5	MEDIO
Repositorio Sinólogy	Falta de control al momento de compartir la información	Fuga de información	R3	Envío de la información a personas que no pertenecen a la cooperativa	2	5	10	ALTO Ψ
Computadoras del área de seguridad de la información	Falta de la instalación o desactualización de los software de seguridad en el equipo	Infección de virus en el equipo	R4	Pérdida de información	3	1	3	MODERADO
Correos electrónicos con nivel de autorización	Falta de controles de autentificación de usuarios en correos	Suplantación de identidad	R5	Comprometer los servidores de microsoft	1	3	3	MODERADO
Certificado de depósito a plazo lleno	Descuido en el proceso de apertura de póliza	Fraude	R6	Pérdida económica para la cooperativa	1	5	5	MEDIO
Pagaré	Falta de procedimientos para el llenado del pagaré	Intento de cobro del pagaré Fraude						
Solicitud de crédito llena	Falta de verificación de datos personales	Suplantación de identidad del cliente						
Personal	Falta de ética del empleado	Ingreso de información incorrecta en el Core financiero						
Servicios críticos ofrecidos	Fallos en los sistemas operativos de la entidad	Riesgo legal, corrido de fondos (retiros de efectivo y polizas)						
Papeletas de depósito llenas	Descuido en la verificación en ventanilla de las papeletas de depósito ingresadas	Fraude	R7	Saldos inconsistentes en estados de cuenta de socios	1	3	3	MODERADO

Elaborado por: Henriquez (2024)

Según los controles que manejan en la cooperativa, se estableció las políticas de seguridad, para proporcionar un marco estructurado y coherente que permita proteger los activos de información de la organización

Ilustración 26

Controles y políticas de seguridad de los activos

CONTROLES Y POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN			
ACTIVO	**N. CONTROLES**	**CONTROLES**	**POLÍTICA DE SEGURIDAD**
Software financiero Softbank	3	Firewall perimetral Software para prevención de fuga de infomación Firewall de aplicaciones	Protección y respaldo de información Bitácora de accesos
Servidor de la base de datos			
Personal	1	Capacitaciones periodicas al personal de la cooperativa	Plan de Educación y concientización del usuario en seguridad de la información
Repositorio Sinólogy	5	Firewall perimetral Software para prevencion de fuga de infomación Firewall de aplicaciones Antivirus EDR (Detección y respuesta de Endpoint)	Protección contra software malicioso Bloqueos de sesión
Computadoras del área de seguridad de la información			
Correos electrónicos con nivel de autorización	4	Firewall perimetral Software para prevencion de fuga de infomación Firewall de aplicaciones Controles implementados en los servidores de microsoft	Protección contra software malicioso Bloqueos de sesión
Certificado de depósito a plazo lleno	2	Bobedas o armarios de seguridad Sistema CCTV sistema de circuito cerrado de televisión	Acceso y control a instalaciones físicas y sistemas de red
Pagaré			
Solicitud de crédito llena	2		
		Archivero del personal de la cooperativa	Gestión de archivos físicos Registro histórico de actividades
Servicios críticos ofrecidos	5	Firewall perimetral Software para prevencion de fuga de infomación Firewall de aplicaciones Antivirus EDR (Detección y respuesta de Endpoint)	Registro histórico de actividades
Papeletas de depósito llenas	1	Sistema CCTV sistema de circuito cerrado de televisión	Acceso y control a instalaciones físicas y sistemas de red

Elaborado por: Henriquez (2024)

Luego, se determinó la periodicidad o frecuencia de control el cual debe estar a cargo de los departamentos de tecnologías y seguridad de la información.

Ilustración 27

Periodicidad o frecuencia de controles

FRECUENCIA DE CONTROLES			
CONTROL	**DESCRIPCIÓN**	**CALIFICACIÓN**	**FRECUENCIA DE CONTROL**
Firewall perimetral	Software de seguridad que se coloca en el borde de la red para monitorear y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas. Su función principal es prevenir accesos no autorizados y proteger la red interna de amenazas externas.	ALTO	Diario
Software para prevencion de fuga de infomación	También conocido como Data Loss Prevention (DLP), es una solución que detecta y previene la transferencia no autorizada de datos sensibles fuera de la red corporativa. Ayuda a asegurar que la información confidencial no se filtre o sea accesada por personas no autorizada	ALTO	Diario
Firewall de aplicaciones	Es un tipo de firewall que protege aplicaciones web al monitorear, filtrar y controlar las aplicaciones. Previene ataques específicos a aplicaciones	ALTO	Diario
Antivirus	Es un software diseñado para detectar, prevenir y eliminar malware, incluyendo virus, gusanos, troyanos y otros programas maliciosos. Protege los sistemas informáticos de infecciones y ayuda a mantener la integridad y seguridad de los datos.	ALTO	Diario
EDR (Detección y respuesta de endopint)	Es una solución de seguridad que monitorea y recopila datos de actividad en los endpoints (dispositivos finales) para identificar, detectar y responder a amenazas avanzadas. Proporciona visibilidad y análisis de incidentes de seguridad en tiempo real.	ALTO	Diario
Controles implementados en los servidores de microsoft	Se refiere a las medidas de seguridad configuradas en los servidores de Microsoft, configuraciones de seguridad, actualizaciones regulares, políticas de acceso y otras prácticas de seguridad recomendadas por Microsoft.	ALTO	Diario
Bobeda o armarios de seguridad	Instalaciones físicas diseñadas para almacenar y proteger documentos importantes, dispositivos de almacenamiento, y otros activos valiosos contra robo, daño o acceso no autorizado. Están construidos con materiales resistentes y a menudo cuentan con sistemas de seguridad avanzados.	ALTO	Diario
Sistema CCTV sistema de circuito cerrado de televisión	Es un sistema de videovigilancia que utiliza cámaras para transmitir imágenes a un conjunto específico de monitores. Se utiliza para monitorear áreas sensibles y aumentar la seguridad en instalaciones mediante la grabación y supervisión en tiempo real.	ALTO	Diario
Archivero del personal de la cooperativa	Muebles diseñados para organizar, almacenar y proteger documentos, archivos y otros materiales importantes en un entorno de oficina.	ALTO	Diario
Contratación de servicios de seguridad y vigilancia	Profesionales encargados de proteger personas, entorno de la entidad garantizando la seguridad y el orden.	ALTO	Diario
Capacitaciones periodicas al personal de la cooperativa	Programas de formación diseñados para mejorar las habilidades, conocimientos y competencias de los empleados, asegurando que puedan desempeñar sus funciones de manera efectiva y alineada con los objetivos de la cooperativa	MEDIO	Mensual

Elaborado por: Henriquez (2024)

3.1.2.2 Evaluación de los procesos catalizadores con el Marco de Referencia COBIT 5

En la cooperativa en lo que se refiere al gobierno y gestión de las TI existen dos departamentos encargados que son: departamento de TI y departamento de seguridad de la información quienes son los que evalúan los procesos y sus actividades, por lo cual en la visita realizada al revisar los 37 objetivos de control del marco de referencia Cobit 5 se concluyó que es necesario evaluar apenas 16 objetivos de control. El procedimiento al llevarse a cabo fue la identificación de los procesos a ser evaluados, las prácticas clave de gobierno y sus actividades calificando los niveles de capacidad, estableciendo el porcentaje de cumplimiento, los objetivos meta de las actividades y el objetivo meta del proceso.

Ilustración 28

Evaluación del Marco de Referencia COBIT 5

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso															
Práctica de Gobierno	**Entradas**		**Salidas**												
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	**De**	**Descripción**	**Descripción**	**A**											
	APO12.01	Factores y problemas de riesgos emergentes	Guías de apetito de riesgo	APO12.03											
			Niveles de tolerancia de riesgo aprobados	APO12.03											
	Fuera del Ámbito de COBIT	Principios de la gestión de riesgos de la empresa	Evaluación de las actividades de gestión de riesgo	APO12.01											
Actividades					**Nivel de capacidad / observado**										
1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).					4										
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.					3										
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.					4										
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.					3										
5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.					4										
6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.					3										

					Nivel de capacidad objetivo del proceso	4				
0-15%	*>15%-50%*	*>50%-85%*	*>85%*						*METAS NIVEL DE CUMPLIMIENTO OBJETIVO DE ACTIVIDADES*	
		67%			*NIVEL DE CUMPLIMIENTO*				*NIVEL DE CUMPLIMIENTO OBJETIVO*	
N	**P**	**L**	**F**		**VALOR**				**META**	**OBSERVACIÓN**
		70%			70%				L	SI CUMPLE
		70%			70%				L	SI CUMPLE
	50,00%				50%				L	NO SE CUMPLE φ
		70%			70%				L	SI CUMPLE
		80%			80%				L	SI CUMPLE
		60%			60%				L	SI CUMPLE
PROMEDIO	67%				**67%**					

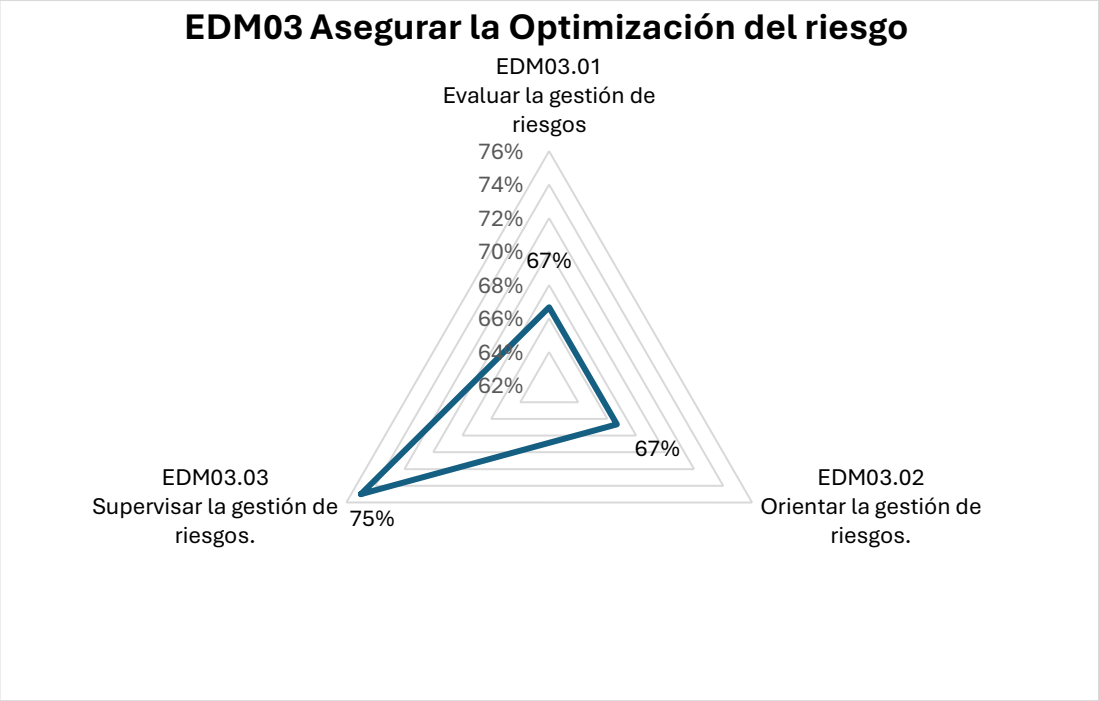
Elaborado por: Henriquez (2024)

3.1.2.2.1 EDM03 “Asegurar la Optimización del riesgo”

Mediante el análisis del dominio Evaluar, Orientar y Supervisar, el objetivo de control EDM03 “Asegurar la Optimización del riesgo”; dio como resultado que, la práctica clave de gobierno EDM03.03 Supervisar la gestión con el 75%, cumple con mayor nivel de capacidad en eficacia, seguida de las prácticas EDM03.01 Evaluar la gestión de riesgos y EDM03.02 Orientar la gestión de riesgos con el 67%. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definidos, encontrándose en un nivel 4.

Ilustración 29

EDM03 “Asegurar la Optimización del riesgo”



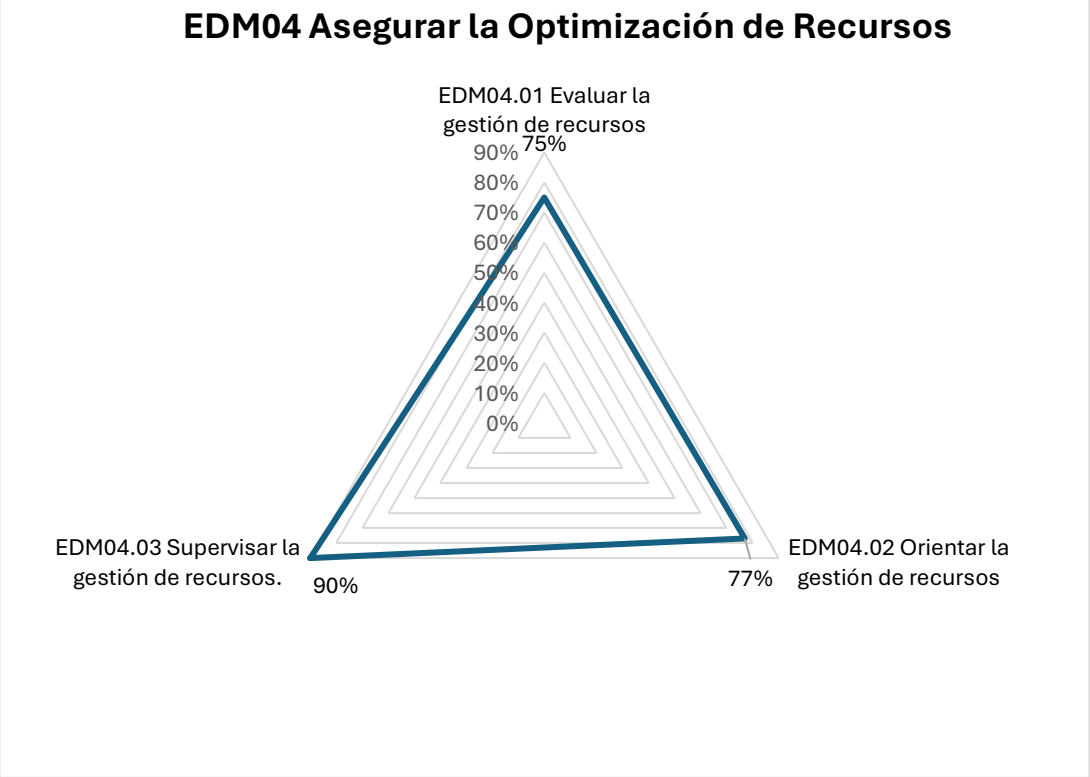
Elaborado por: Henriquez (2024)

3.1.2.2.2 EDM04 “Asegurar la Optimización de Recursos”

Mediante el análisis del dominio Evaluar, Orientar y Supervisar el objetivo de control EDM04 “Asegurar la Optimización de Recursos”; dio como resultado que, EDM04.03 Supervisar la gestión de recursos con el 90%, cumple con el mayor nivel de capacidad en eficacia, seguida de la práctica clave EDM04.02 Orientar la gestión de recursos con el 77%. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definidos, encontrándose en un nivel 4.

Ilustración 30

EDM04 "Asegurar la Optimización de Recursos"



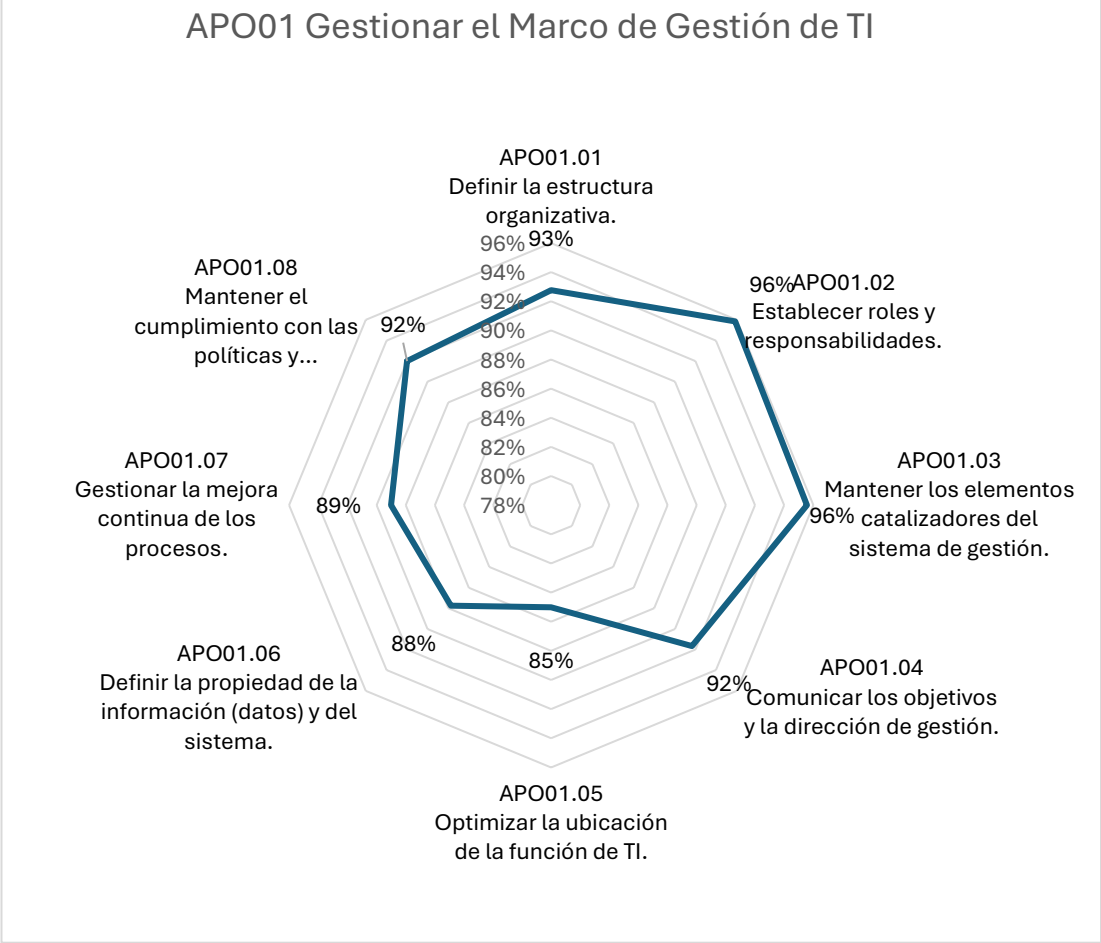
Elaborado por: Henriquez (2024)

3.1.2.2.3 APO01 "Gestionar el Marco de Gestión de TI"

Mediante el análisis del dominio Evaluar, Orientar y Supervisar, el objetivo de control APO01 "Gestionar el Marco de Gestión de TI"; dio como resultado que, APO01.02 Establecer roles y responsabilidades y el APO01.03 Mantener los elementos catalizadores del sistema de gestión con el 96%, cumplen con el mayor nivel de capacidad en eficacia, seguidos de los procesos APO01.04 Comunicar los objetivos y la dirección de gestión y APO01.08 Mantener el cumplimiento con las políticas y procedimientos con el 92%. El proceso se encuentra en optimización, mejora continuamente para ayudar a alcanzar los objetivos actuales y futuros, encontrándose en un nivel 5.

Ilustración 31 APO01 "Gestionar el Marco de Gestión de TI"

APO01 "Gestionar el Marco de Gestión de TI"



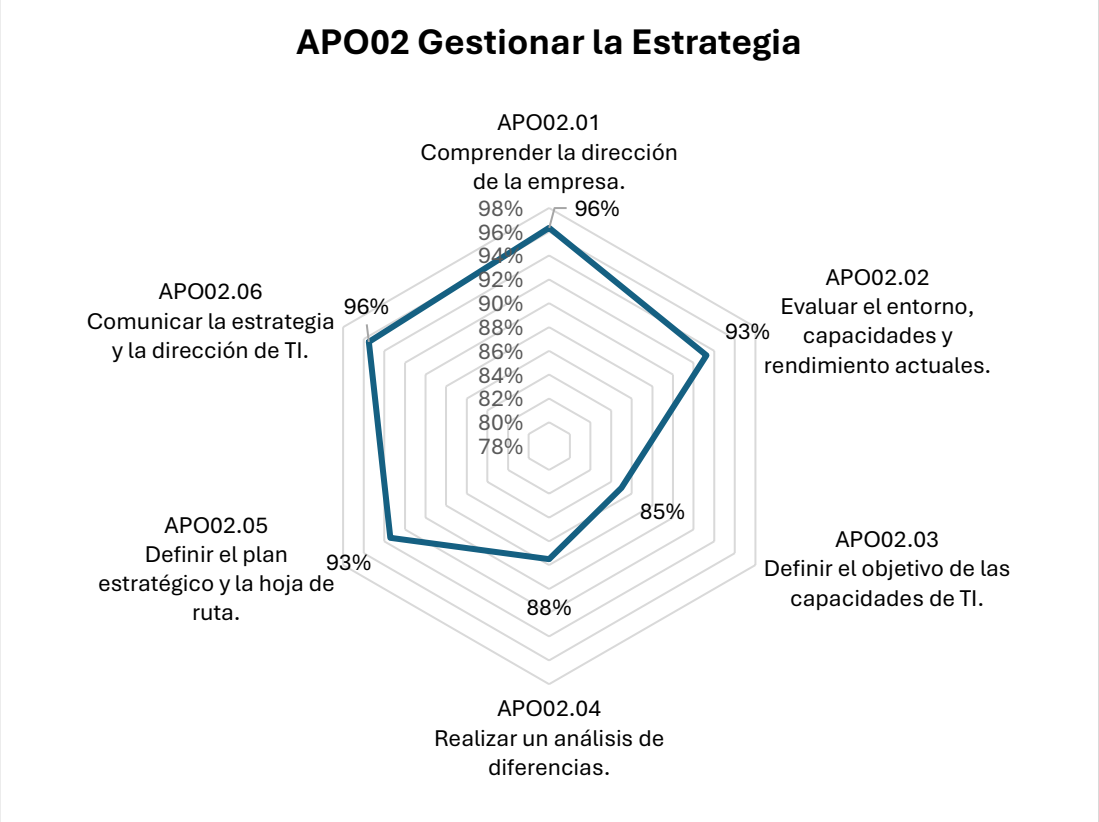
Elaborado por: Henriquez (2024)

3.1.2.2.4 APO02 "Gestionar la Estrategia"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO02 "Gestionar la Estrategia"; dio como resultado que, APO02.01 Comprender la dirección de la empresa y el APO02.06 Comunicar la estrategia y la dirección de TI con el 96% cumplen con el mayor nivel de capacidad en eficacia, seguidos de los procesos APO02.02 Evaluar el entorno, capacidades y rendimiento actuales y APO02.05 Definir el plan estratégico y la hoja de ruta con el 93%. El proceso se encuentra en optimización, mejora continuamente para ayudar a alcanzar los objetivos actuales y futuros, encontrándose en un nivel 5.

Ilustración 32

APO02 "Gestionar la Estrategia"



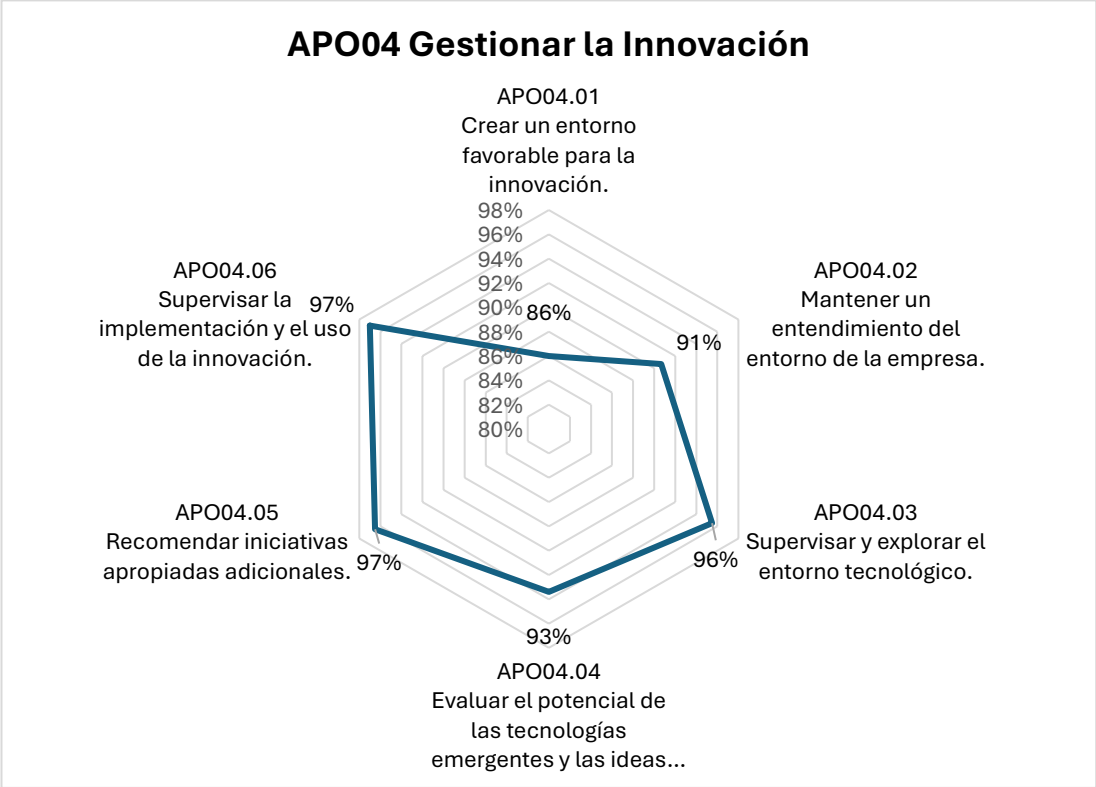
Elaborado por: Henriquez (2024)

3.1.2.2.5 APO04 "Gestionar la Innovación"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO04 "Gestionar la Innovación"; dio como resultado que, APO04.05 Recomendar iniciativas apropiadas adicionales y APO04.06 Supervisar la implementación y el uso de la innovación con el 97% cumplen con el mayor nivel de capacidad en eficacia. Las demás prácticas clave se encuentran en un nivel optimizado. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definido, encontrándose en un nivel 4.

Ilustración 33

APO04 "Gestionar la Innovación"



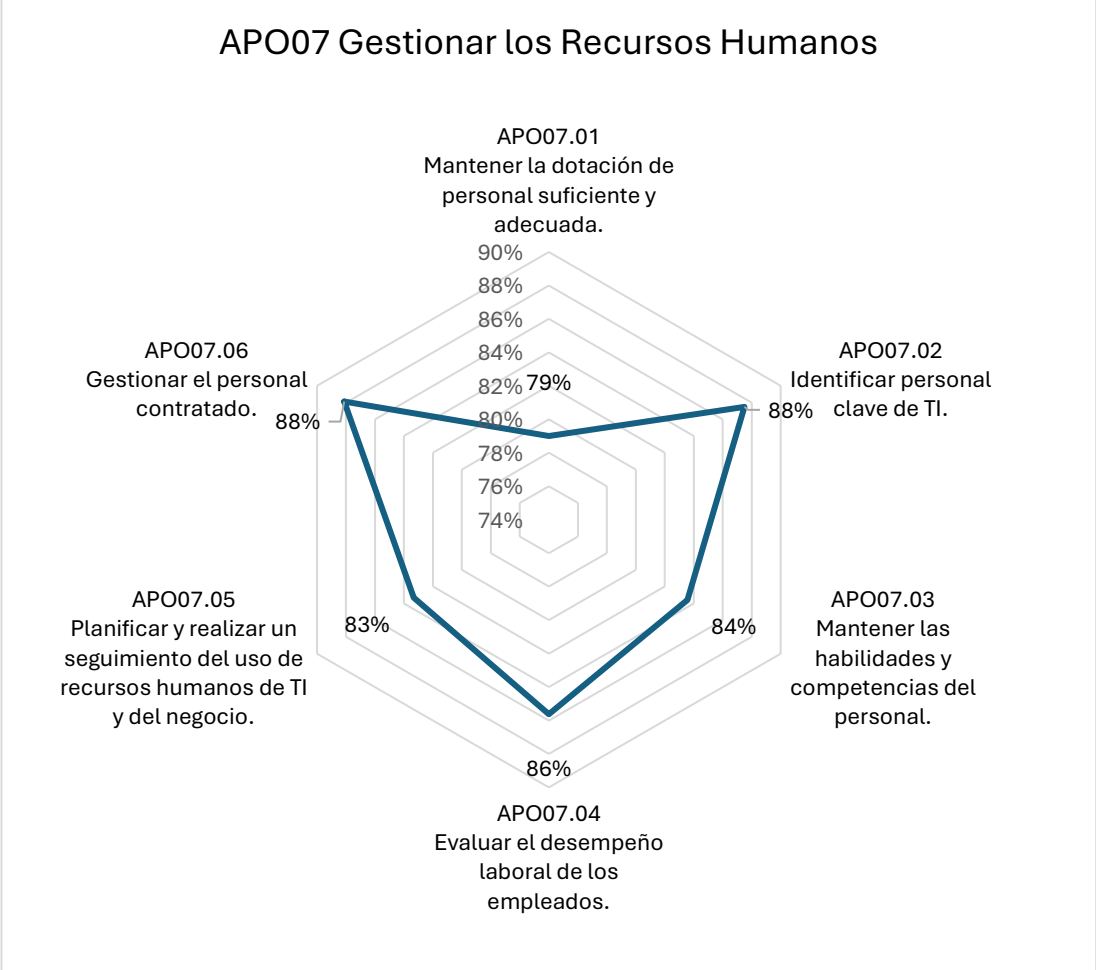
Elaborado por: Henriquez (2024)

3.1.2.2.6 APO07 "Gestionar los Recursos Humanos"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO04 "Gestionar los Recursos Humanos"; dio como resultado que, APO07.02 Identificar personal clave de TI y APO07.06 Gestionar el personal contratado con el 88% cumplen con el mayor nivel de capacidad en eficacia, seguido del proceso APO07.04 Evaluar el desempeño laboral de los empleados con el 86%. Las demás prácticas clave se encuentran en un nivel predecible. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definidos, encontrándose en un nivel 4.

Ilustración 34

APO04 "Gestionar los Recursos Humanos"



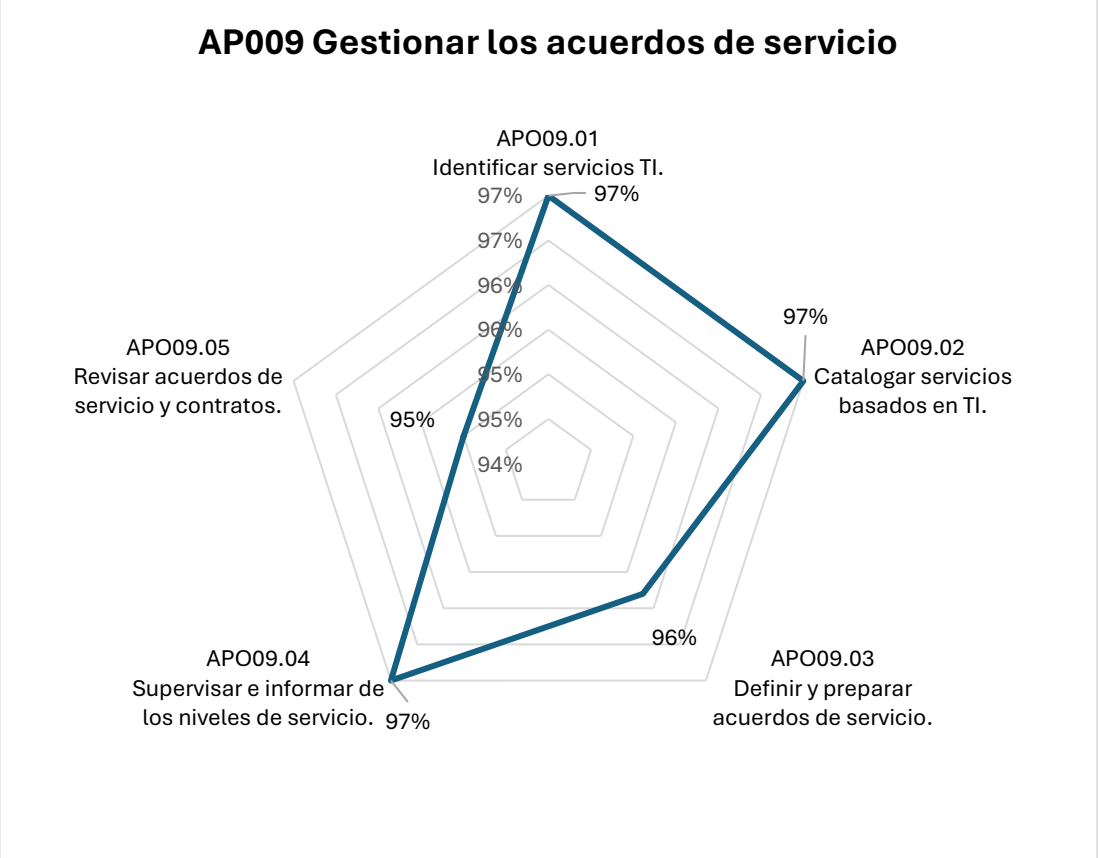
Elaborado por: Henriquez (2024)

3.1.2.2.7 AP009 "Gestionar los acuerdos de servicio"

Mediante el análisis del dominio Alinear, Planificar y Organizar en el proceso APO09 "Gestionar los acuerdos de servicio"; se menciona que todas las practicas clave contribuyen al cumplimiento de la meta objetivo debido a que sus evaluaciones se identifican entre el 95,96 y 97% lo que significa que están en un nivel 5, es decir su proceso se encuentra optimizado.

Ilustración 35

APO09 "Gestionar los acuerdos de servicio"



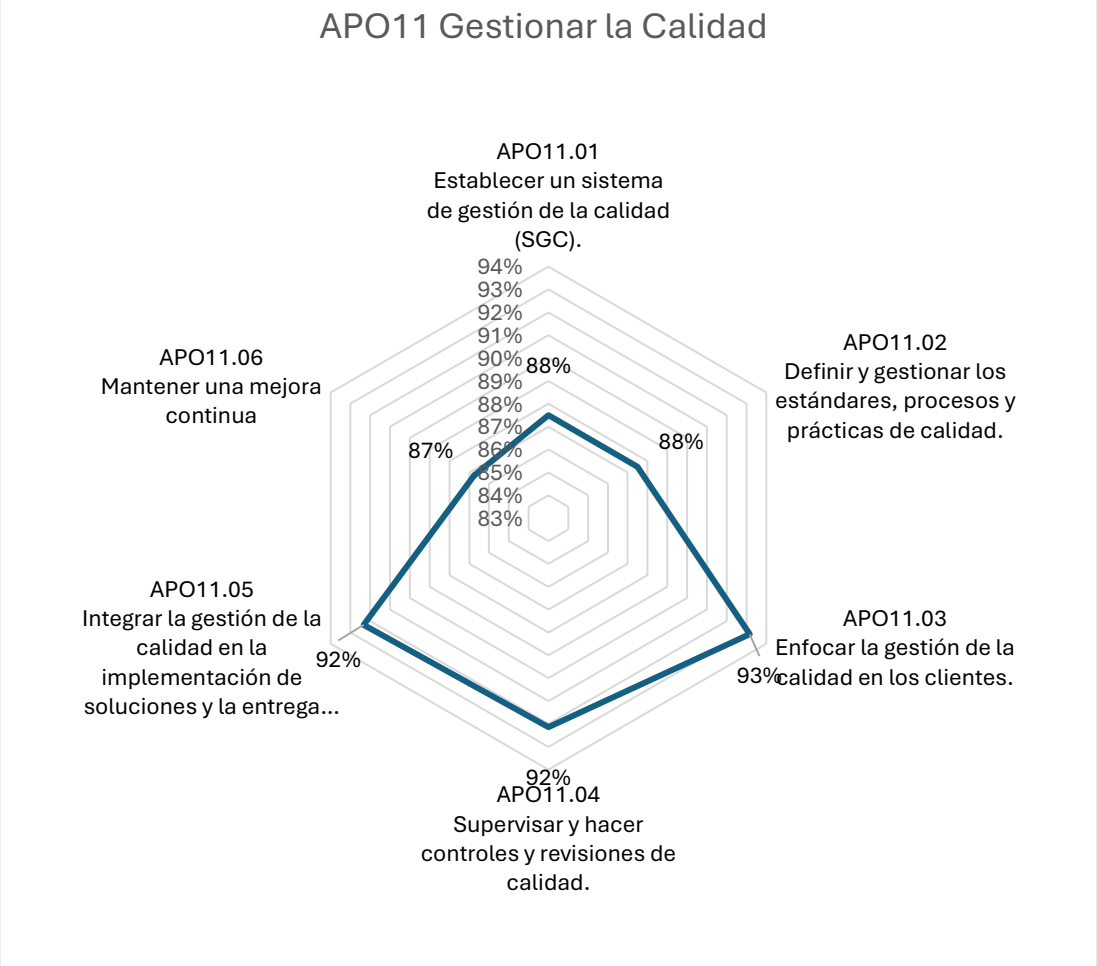
Elaborado por: Henriquez (2024)

3.1.2.2.8 APO11 "Gestionar la Calidad"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO11 "Gestionar la Calidad"; dio como resultado que, APO11.03 Enfocar la gestión de la calidad en los clientes con el 97% es la práctica clave con mayor nivel de capacidad en eficacia. Las demás prácticas clave se encuentran en un nivel optimizado. El proceso se encuentra en optimización, mejora continuamente para ayudar a alcanzar los objetivos actuales y futuro, encontrándose en un nivel 5.

Ilustración 36

APO11 "Gestionar la Calidad"



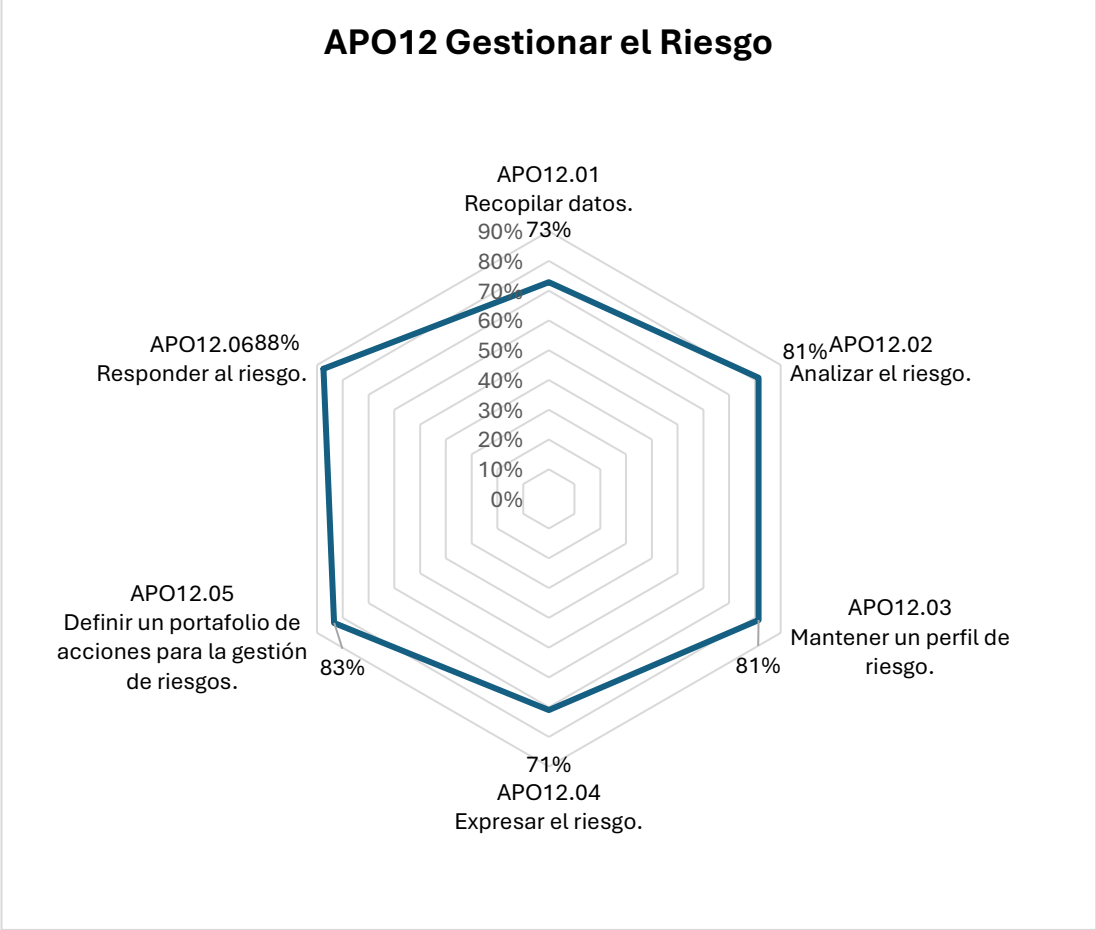
Elaborado por: Henriquez (2024)

3.1.2.2.9 APO12 "Gestionar el Riesgo"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO12 "Gestionar el Riesgo"; dio como resultado que, APO12.06 Responder al riesgo con el 88% cumple con mayor nivel de capacidad en eficacia, seguido del proceso APO12.05 Definir un portafolio de acciones para la gestión de riesgos con el 83%. Las demás prácticas clave se encuentran en un nivel establecido. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definidos, encontrándose en un nivel 4.

Ilustración 37

APO12 "Gestionar el Riesgo"



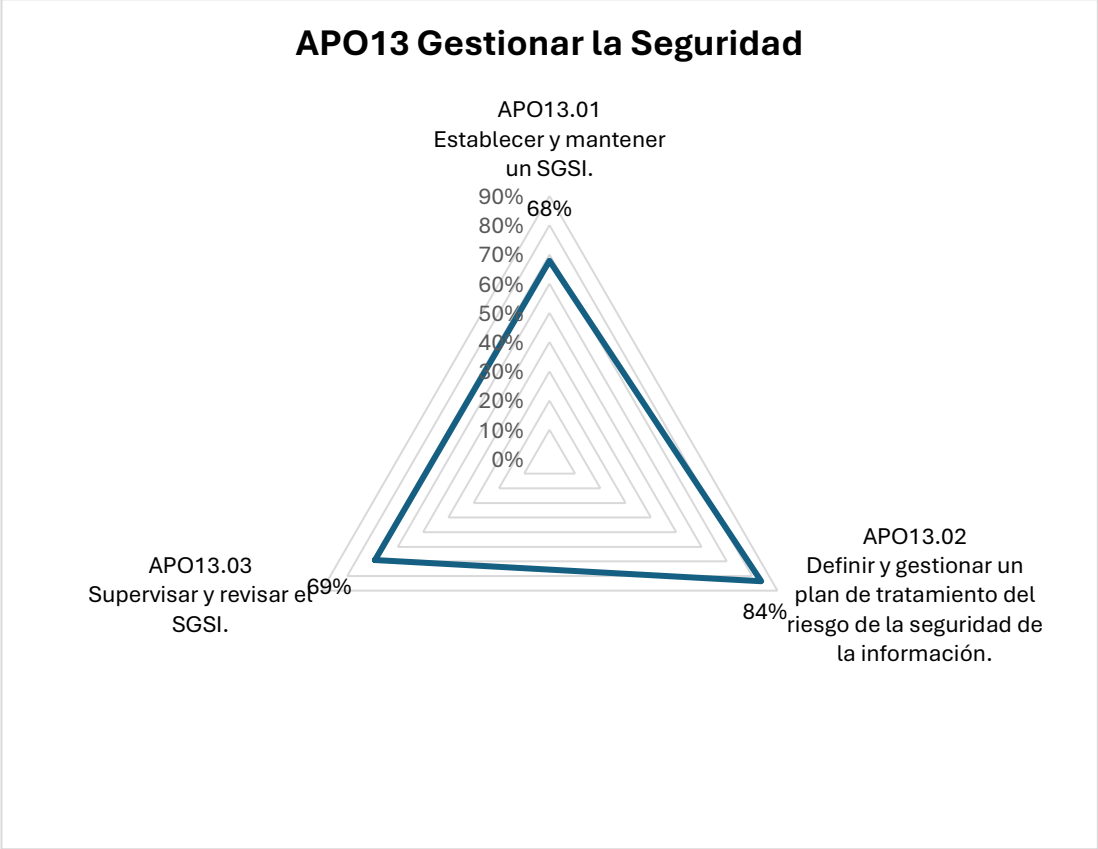
Elaborado por: Henriquez (2024)

3.1.2.2.10 APO13 "Gestionar la Seguridad"

Mediante el análisis del dominio Alinear, Planificar y Organizar, el objetivo de control APO13 "Gestionar la Seguridad"; dio como resultado que, APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información con el 84% cumple con mayor nivel de capacidad en eficacia. Las otras 2 prácticas clave se encuentran en un nivel establecido. El proceso está establecido, está documentado para garantizar su capacidad para cumplir sus objetivos, encontrándose en un nivel 3.

Ilustración 38

APO13 "Gestionar la Seguridad"



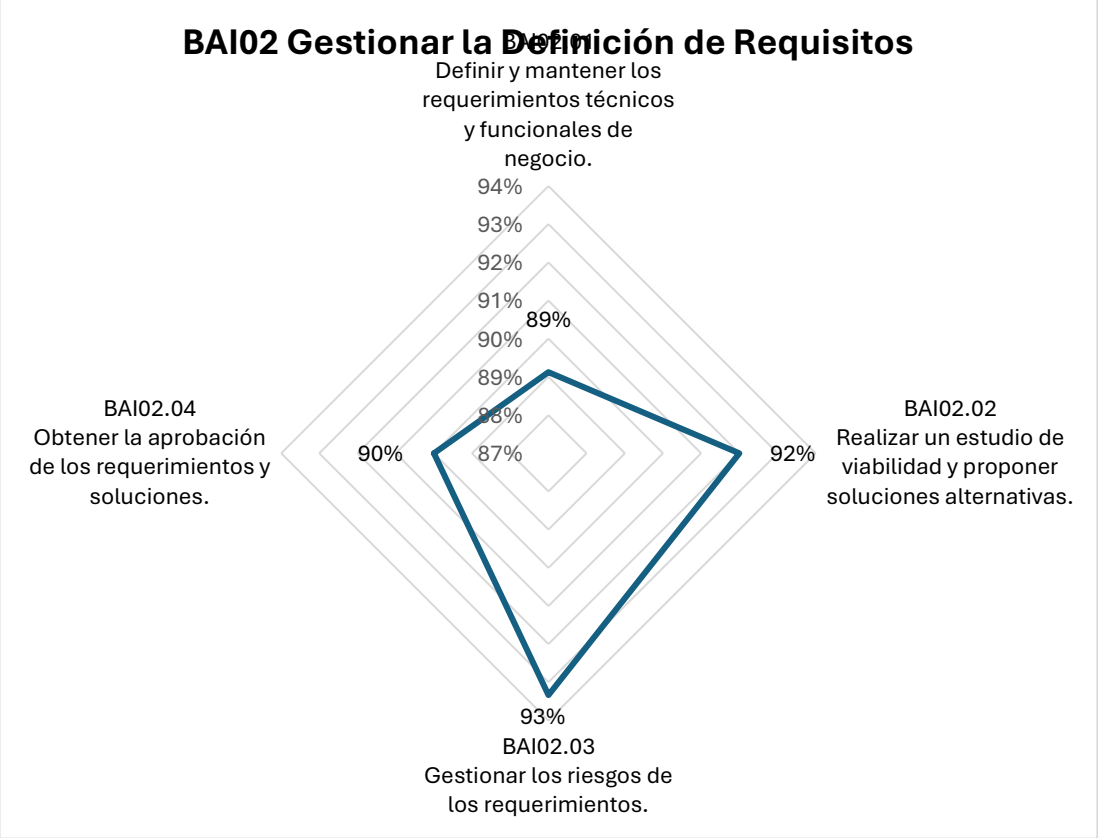
Elaborado por: Henriquez (2024)

3.1.2.2.11 BAI02 "Gestionar la Definición de Requisitos"

Mediante el análisis del dominio Construir, Adquirir e Implementar, el objetivo de control BAI02 "Gestionar la Definición de Requisitos"; dio como resultado que, BAI02.03 Gestionar los riesgos de los requerimientos con el 93% cumple con mayor nivel de capacidad en eficacia. Las demás prácticas clave se encuentran en un nivel optimizado. El proceso se encuentra en optimización, mejora continuamente para ayudar a alcanzar los objetivos actuales y futuro, encontrándose en un nivel 5.

Ilustración 39

BAI02 "Gestionar la Definición de Requisitos"



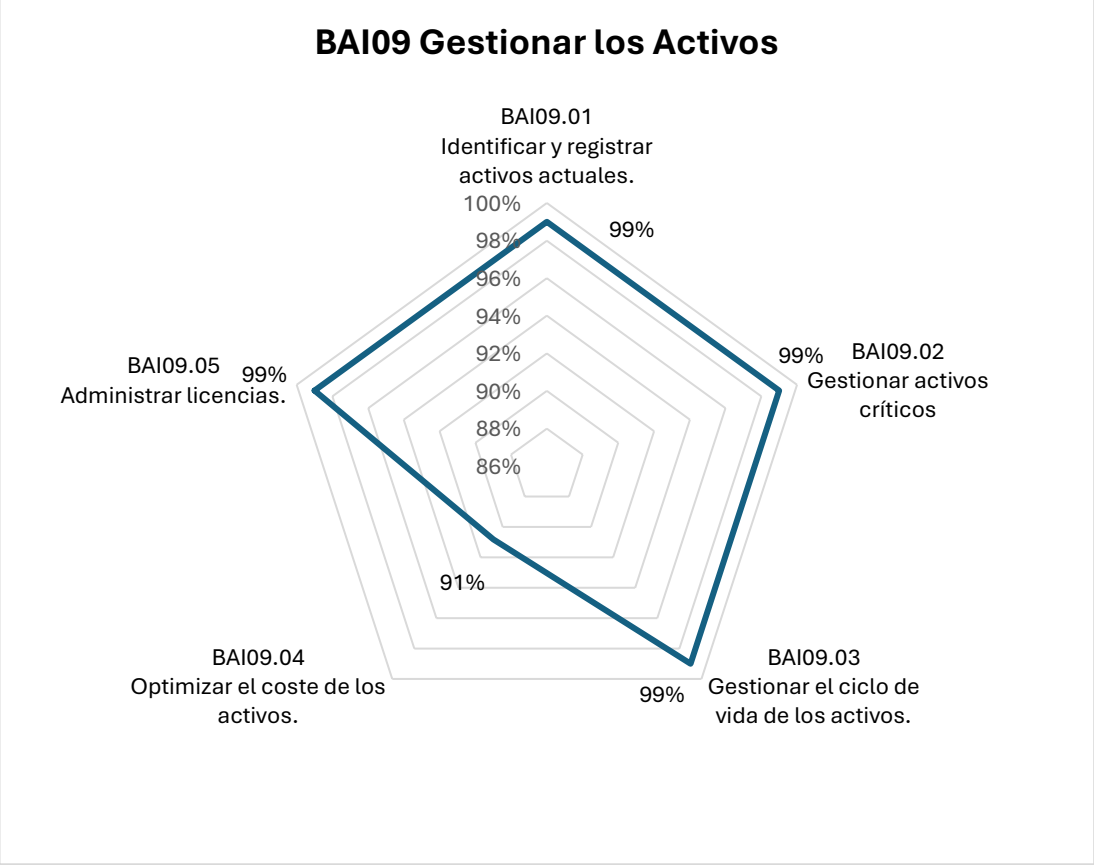
Elaborado por: Henriquez (2024)

3.1.2.2.12 BAI09 "Gestionar los Activos"

Mediante el análisis del dominio Construir, Adquirir e Implementar, el objetivo de control BAI09 "Gestionar los Activos"; se menciona que todas las practicas clave contribuyen al cumplimiento de la meta objetivo debido a que sus evaluaciones se identifican entre el 91% y 99% lo que significa que están en un nivel 5, es decir su proceso se encuentra optimizado.

Ilustración 40

BAI09 "Gestionar los Activos"



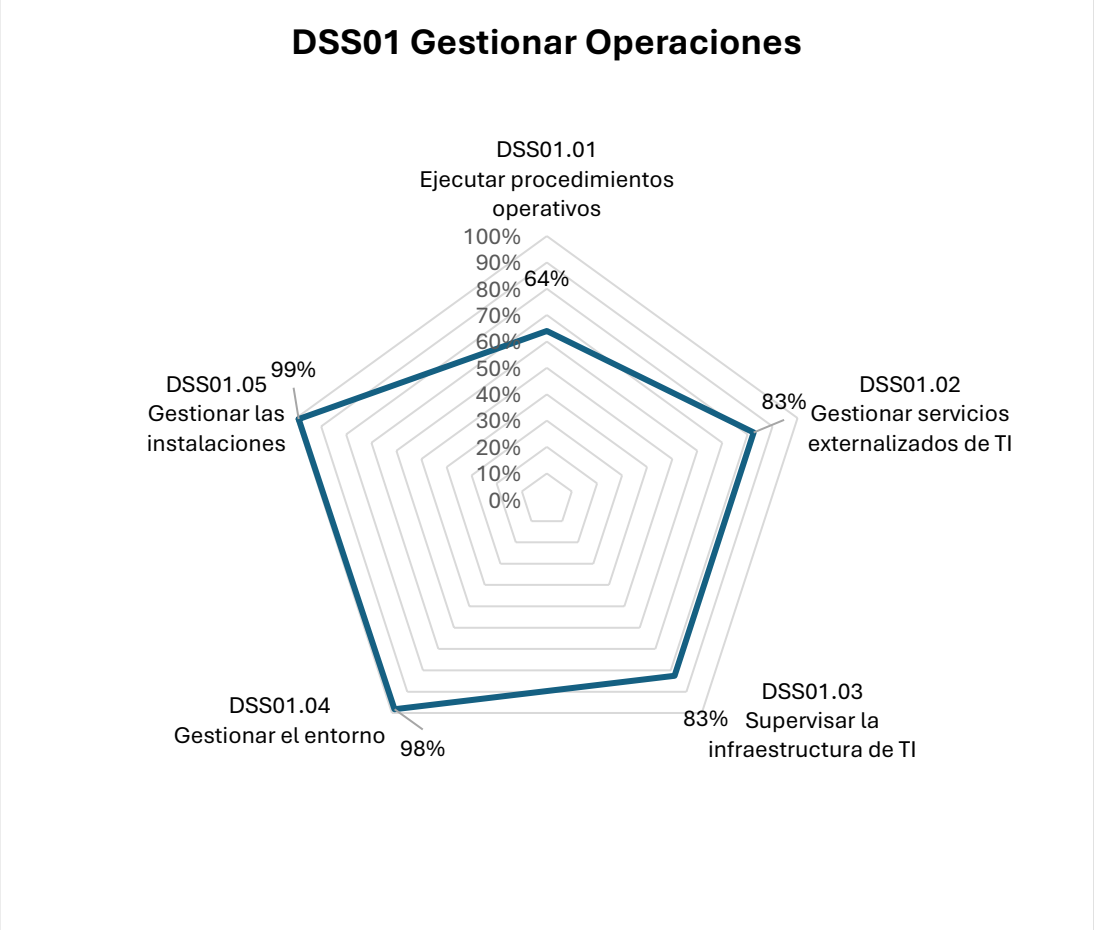
Elaborado por: Henriquez (2024)

3.1.2.2.13 DSS01 "Gestionar Operaciones"

Mediante el análisis del dominio Entrega, Servicio y Soporte, en el objetivo de control DSS01 "Gestionar Operaciones"; dio como resultado que, DSS01.05 Gestionar las instalaciones con el 99% cumple con mayor nivel de capacidad en eficacia, seguido de la práctica DSS01.04 Gestionar el entorno con el 98%. Las demás prácticas clave se encuentran en un nivel predecible. El proceso es predecible, opera de acuerdo con los objetivos de rendimiento definidos, encontrándose en un nivel 4.

Ilustración 41

DSS01 "Gestionar Operaciones"



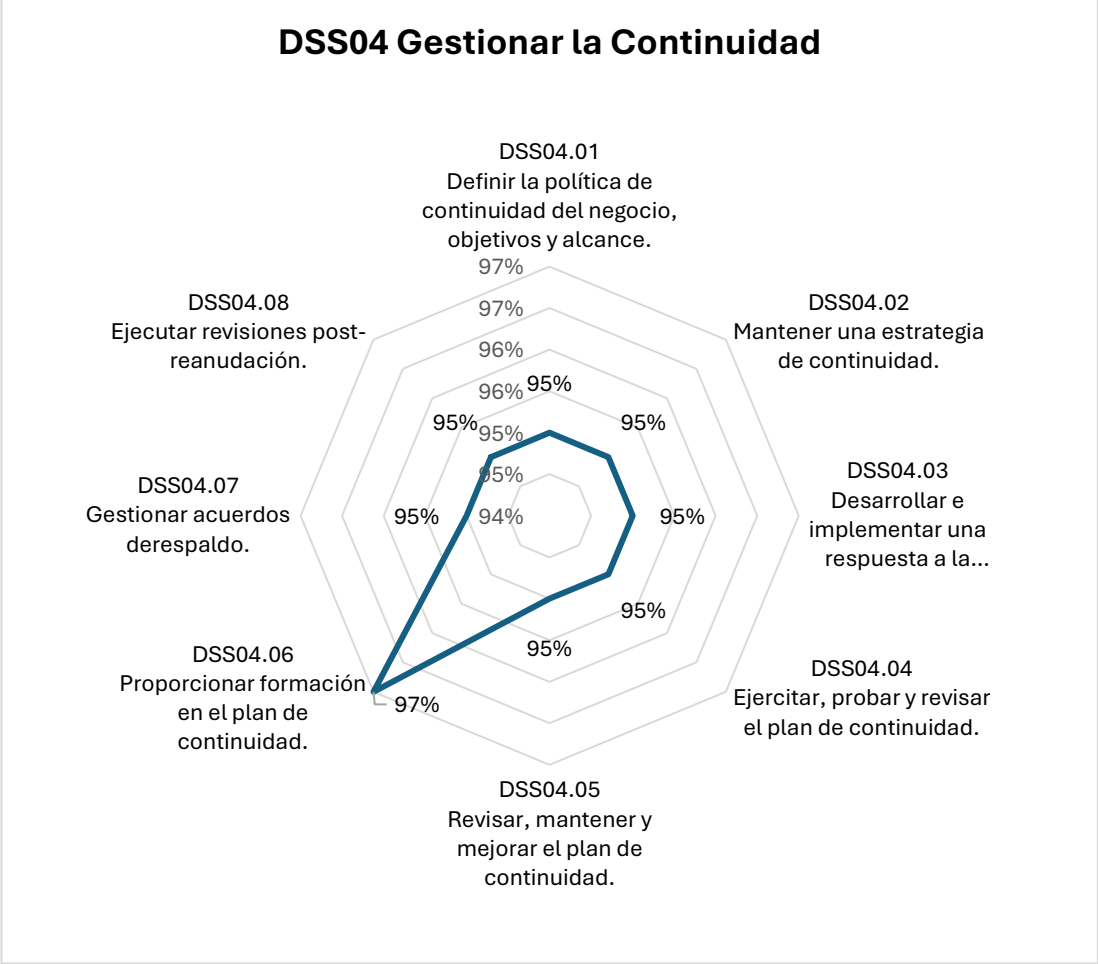
Elaborado por: Henriquez (2024)

3.1.2.2.14 DSS04 "Gestionar la Continuidad"

Mediante el análisis del dominio Entrega, Servicio y Soporte en el objetivo de control DSS04 "Gestionar la Continuidad"; se menciona que todas las practicas clave contribuyen al cumplimiento de la meta objetivo debido a que sus evaluaciones se identifican entre el 95% y 97% lo que significa que están en un nivel 5, es decir su proceso se encuentra optimizado.

Ilustración 42

DSS04 "Gestionar la Continuidad"



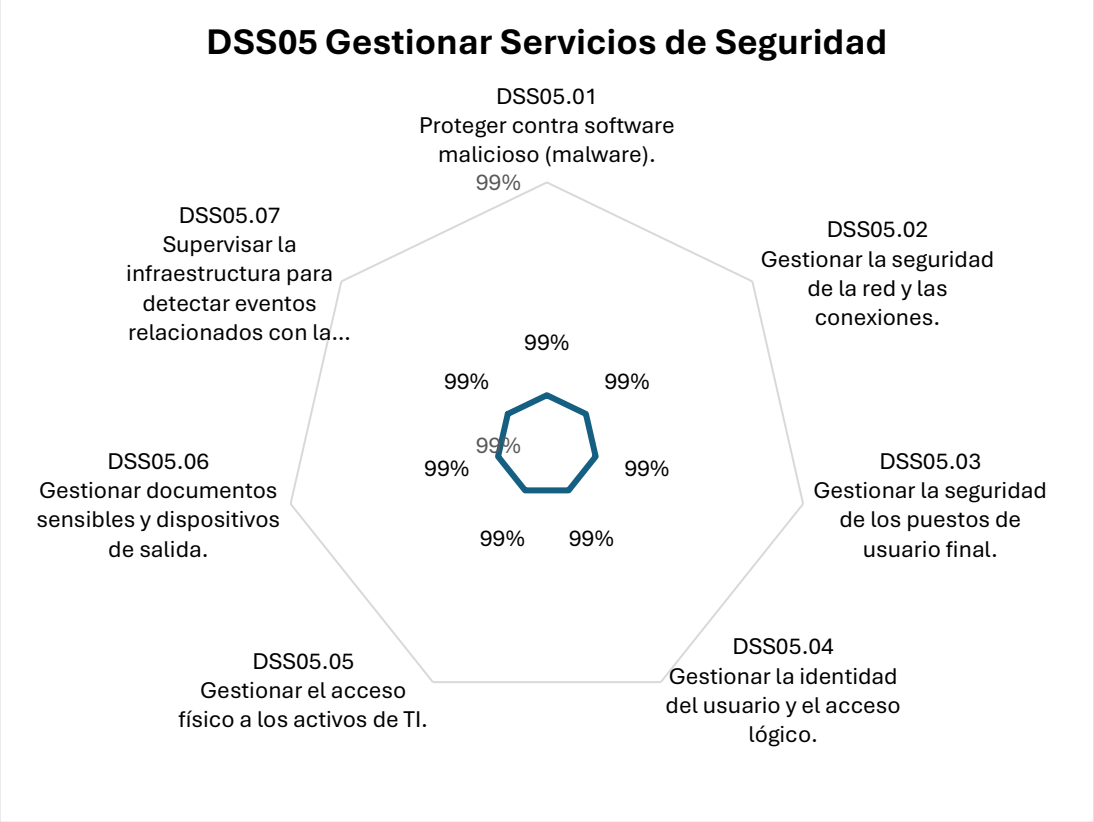
Elaborado por: Henriquez (2024)

3.1.2.2.15 DSS05 "Gestionar Servicios de Seguridad"

Mediante el análisis del dominio Entrega, Servicio y Soporte, en el objetivo de control DSS05 "Gestionar Servicios de Seguridad"; se menciona que todas las practicas clave contribuyen al cumplimiento de la meta objetivo debido a que sus evaluaciones se identifican con 99% lo que significa que están en un nivel 5, es decir su proceso se encuentra optimizado.

Ilustración 43

DSS05 "Gestionar Servicios de Seguridad"



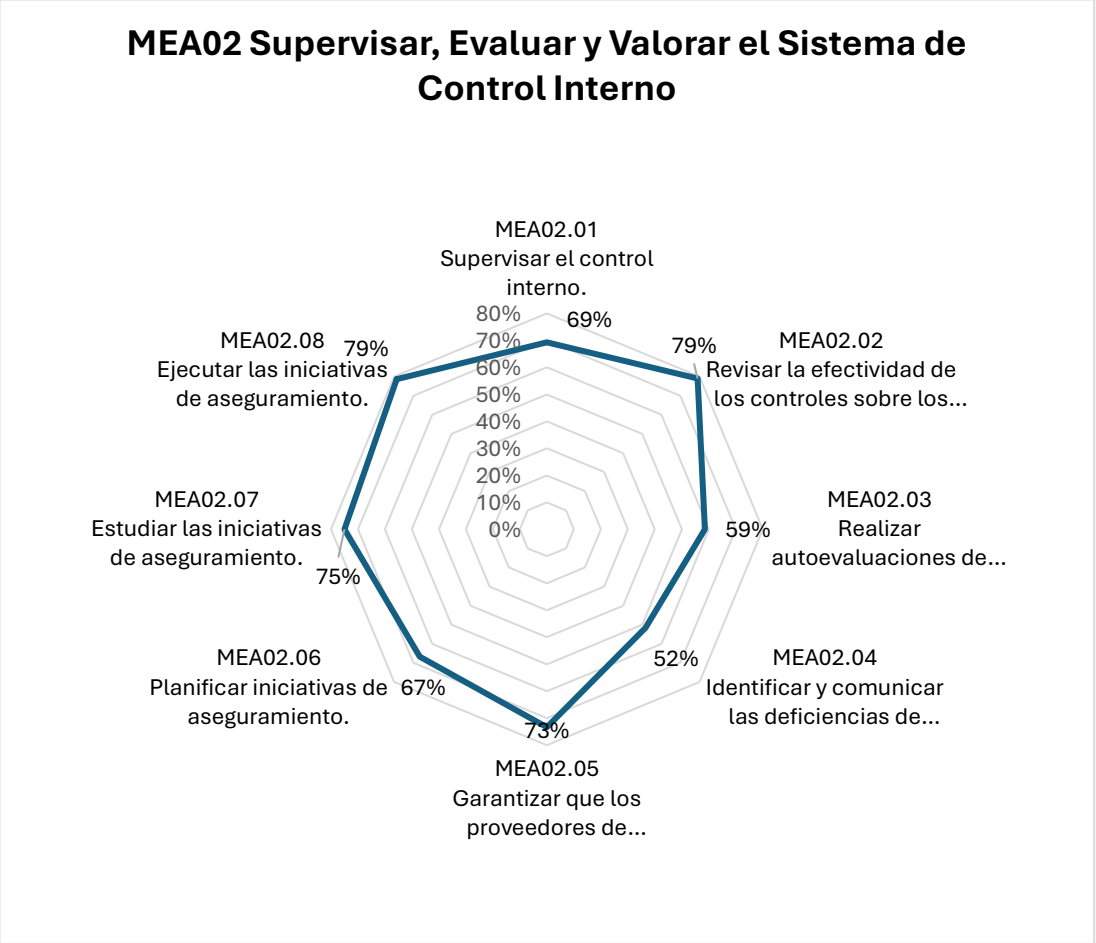
Elaborado por: Henriquez (2024)

3.1.2.2.16 MEA02 "Supervisar, Evaluar y Valorar el Sistema de Control Interno"

Mediante el análisis del dominio Supervisar, Evaluar y Valorar en el objetivo de control MEA02 "Supervisar, Evaluar y Valorar el Sistema de Control Interno" dio como resultado que, MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio y MEA02.08 Ejecutar las iniciativas de aseguramiento con el 79% cumplen con mayor nivel de capacidad en eficacia, seguido de la práctica clave MEA02.07 Estudiar las iniciativas de aseguramiento con el 75%. Mientras que la práctica clave con mayor deficiencia es MEA02.04 Identificar y comunicar las deficiencias de control con el 52%. Las demás prácticas clave se encuentran en un nivel establecido. El proceso está establecido, está documentado para garantizar su capacidad para cumplir sus objetivos, encontrándose en un nivel 3.

Ilustración 44 MEA02

MEA02 "Supervisar, Evaluar y Valorar el Sistema de Control Interno"



Elaborado por: Henriquez (2024)

3.1.3 Comunicación de resultados

3.1.3.1 Reporte preliminar de auditoría

El reporte preliminar de auditoría permite identificar de manera resumida los hallazgos encontrados en las áreas donde se evaluó así como el tipo de hallazgo si es de observación o no conformidad, tomando en cuenta que aquellos hallazgos que se marquen como observación serán sencillos de solucionar sin poner en riesgos los procesos, mientras que aquellos que sean marcados de no conformidad deberán ser considerados de manera prioritaria debido a que puede afectar a la operatividad de la institución, tanto los procesos como las políticas de seguridad.

Ilustración 45

Informe preliminar de auditoría

REPORTE PRELIMINAR DE AUDITORÍA				
Fecha:	Ambato, junio 2024			
Empresa:	Cooperativa de Ahorro y Crédito Kullki Wasi Ltda.			
Objetivo de la auditoría	Realizar una Auditoría del sistema de información en la Cooperativa Kullki Wasi Ltda., para la evaluación de su nivel de confianza en la seguridad y confiabilidad.			
Metodología	La audiotoría está basada en entrevistas, guías de observación, listas de chequeo, cuestionarios y matrices			
Descripción de los hallazgos				
N. Hallazgo	**Descripción del hallazgo encontrado**	**Área donde se encontró el hallazgo**	**Tipo de hallazgo**	
			Observación	**No conformidad**
1	No se realiza un análisis del foda institucional (fortalezas y oportunidades, debilidades,amenazas)	Área informática		x
2	El control de seguridad actualmente evidencia un nivel de confianza y riesgo moderado debido a que las revisiones que aplican registran medianamente los parámetros de control cuando son rebasados o fallan.	Área informática		x
3	Existe condiciones al seleccionar, y documentar los datos, parámetros y premisas.	Área informática	x	
4	No se identifica continuamente oportunidades para mejorar la calidad de datos relacionados con el sistema de información de la cooperativa.	Área informática		x
5	Se reporta información seleccionada sobre riesgos, cultura y desempeño de la cooperativa.	Área informática		x
6	Ha existido en cierto tiempo el mal uso de la información con fines de soborno o fraude.	Área informática		x
7	Se ha detectado ciertas inconsistencias en la información reportada por las herramientas informáticas que utiliza la cooperativa.	Área informática	x	
8	En el nivel de madurez y eficiencia del sistema de control interno, el componente Estrategias y objetivos tiene una calificación media lo que indica que se encuentra en un nivel en proceso.	Área informática y seguridad de la información	x	
9	Existe riesgo operativo, debido a vulnerabilidades detectadas en el software, personas, procesos y tecnologías de información.	Área de seguridad de la información	x	
10	Ha existido envío de la información a personas que no pertenecen a la cooperativa	Área de seguridad de la información		x
11	En la práctica clave de gobierno EDM03.01 no se determina el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.	Área de riesgos		x
12	En la práctica clave de gobierno EDM03.02 no se promueve una cultura consciente de los riesgos TI e impulsar a la cooperativa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.	Área de riesgos		x
13	En la práctica clave de gobierno EDM03.02 existe limitación en orientar a la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.	Área de riesgos		x
14	En la práctica clave de gestión APO02.03 la definición del objetivo de las capacidades de TI requiere alineación y acuerdo con los cambios en la arquitectura empresarial con el gobierno corporativo.	Área informática	x	

15	En la práctica clave de gestión APO13.01 no se define el alcance y los límites del SGSI en términos de las características de la cooperativa, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.	Área de seguridad de la información		x
16	En la práctica clave de gestión APO13.01 existe limitaciones en la definición del SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.	Área de seguridad de la información		x
17	En la práctica clave de gestión APO13.01 no se prepara ni se mantiene una declaración de aplicabilidad que describa el alcance del SGSI.	Área de seguridad de la información		x
18	En la práctica clave de gestión APO13.02 no se proporciona información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.	Área de seguridad de la información		x
19	En la práctica clave de gestión APO13.03 no se realizan auditorías internas al SGSI a intervalos planificados.	Área de seguridad de la información	x	
20	En la práctica clave de gestión APO13.03 no se realizan revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	Área de seguridad de la información		x
21	En la práctica clave de gestión BAI09.04 no se obtiene estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.	Área de seguridad de la información		x
22	En la práctica clave de gestión MEA02.03 no se determina la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.	Área de procesos de calidad		x

Elaborado por: Henriquez (2024)

3.1.3.2 Informe de auditoría

A continuación, se realizó el informe de auditoría, el cual proporciona una visión detallada de las áreas evaluadas, incluyendo el cumplimiento de las normativas establecidas, la identificación de posibles vulnerabilidades, y las recomendaciones específicas para mejorar la seguridad en nuestra cooperativa.

Ilustración 46

Informe general

"NATEF"AUDITORES INDEPENDIENTES

COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA.

INFORME GENERAL

AUDITORIA AL SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO KULLKI WASI LTDA.

MARZO- AGOSTO 2024

SIGLAS/ ABREVIATURAS	SIGNIFICADO
COSO	Committe of Sponsoring Organizations of the Tradeway Commission Comité de Organizaciones Patrocinadoras de Treadway
ERM	Enterprise Risk Management Gestión de riesgos empresariales
ISO	International Organization for Standardization Organización internacional de normalización
SI	Sistema informático
SGSI	Sistema de gestión de seguridad de la información
TI	Tecnologias de la información
AI	Activos de información
COBIT	Technology (Objetivos de control para la información y tecnología relacionada)
EDM	Evaluar, Orientar y Supervisar
APO	Alinear, Planificar y Organiza
BAI	Construir, Adquirir e Implementar
DSS	Entrega, Servicio y Soporte
MEA	Supervisar, Evaluar y Valorar

Elaborado por: Henriquez (2024)

"NATEF"AUDITORES INDEPENDIENTES

Ambato, junio de 2024

Mg. Juan Andagana
Gerente de la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda.

De mi consideración:
Se ha realizado la evaluación al sistema de información en el área de informática a la Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. ubicada en Ambato en el período comprendido del año 2024.

El examen se realizó de manera satisfactoria de acuerdo con las Normas de Auditoría Generalmente Aceptadas, con la utilización del marco de referencia COSO ERM 2017, aplicación de las normas ISO/IEC 27000 y 31000 y el marco de referencia COBIT. Se han detectado una serie de elementos informáticos que podrían estar interfiriendo en el desarrollo adecuado de las operaciones empresariales. Por ende, se propondrán sugerencias y posibles medidas correctivas con el fin de asegurar una gestión interna efectiva y mitigar los riesgos asociados a los activos de información.

El propósito de la auditoría del sistema de información es garantizar el adecuado desempeño del departamento de tecnologías de la información, abarcando aspectos como la confianza y la solidez en términos de control interno, la evaluación de los activos de información, la identificación de los controles implementados en dichos activos, así como la respuesta oportuna y adecuada a los riesgos que podrían afectar a la organización y evaluar el nivel de madurez del gobierno y gestión de las TI.

Los resultados de esta auditoría se presentan en este informe a través de condición, criterio, conclusión y recomendaciones.

Atentamente,

Nathaly Estefania Henriquez Cisneros

3.1.3.3 Resultados del examen

Hallazgo 1: Evaluación del control interno COSO ERM 2017 – Estrategias y Objetivos ~~9~~

Comentario

No se realiza un análisis del FODA institucional (fortalezas y oportunidades, debilidades, amenazas), por ello se incumple la **Norma ISO/IEC 27001 y la Norma ISO 31000.**

(Cláusula 4 de ISO/IEC 27001):

4.5 Comprensión de la organización y su contexto: Colabora en la identificación de los puntos fuertes y débiles internos, así como las posibles amenazas y oportunidades externas que podrían impactar la seguridad de la información.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas: Encuentra las oportunidades para cumplir de manera más eficiente con las expectativas de los involucrados y fortalece la relación con ellos.

Evaluación de Riesgos de Seguridad de la Información (Cláusula 6.1 de ISO/IEC 27001):

6.1.2 Evaluación de riesgos de seguridad de la información: Implica la detección de amenazas externas y debilidades internas que puedan tener un impacto en la seguridad de los datos.

Principios de Gestión del Riesgo (Cláusula 4 de ISO 31000):

4.3 Personalización: Es importante que la gestión del riesgo se ajuste a las particularidades de la organización, tomando en cuenta sus puntos fuertes y débiles, así como las amenazas y oportunidades específicas.

Marco de Gestión del Riesgo Cláusula 5 de ISO 31000):

5.3 Liderazgo y Compromiso: Es necesario que los líderes de la organización identifiquen y comprendan los riesgos, lo cual involucra reconocer tanto las fortalezas como las debilidades internas.

5.4 Integración: Es necesario que la gestión del riesgo se incorpore en todos los aspectos de la organización, lo cual permite adoptar un enfoque completo que puede involucrar el análisis DAFO.

Conclusiones

Los líderes o empleados de la cooperativa desconocen la importancia de llevar a cabo esta metodología, por lo cual existen limitaciones sobre su posición en el mercado y los factores internos y externos que impactan su desempeño.

Recomendaciones

Dirigido al gerente: Realizar un análisis FODA de manera inmediata lo que permitirá que sea considerado un elemento importante y clave en la gestión de la cooperativa para la toma de decisiones.

Hallazgo 2: Evaluación del control interno COSO ERM 2017 – Desempeño ~~9~~

Comentario

El control de seguridad actualmente evidencia un nivel de confianza y riesgo moderado, debido a que las revisiones que aplican registran medianamente los parámetros de control cuando son rebasados o fallan, por ello se incumple la **Norma ISO/IEC 27001, 27002 y la Norma ISO 31000.**

ISO/IEC 27001:2013 – Cláusula 9.1: Seguimiento, Medición, Análisis y Evaluación

Esta cláusula establece que la organización debe evaluar el desempeño y la eficacia del sistema de gestión de seguridad de la información (SGSI). Incluye:

Determinación de lo que se debe monitorear y medir: Esto implica identificar los controles clave y establecer parámetros para su rendimiento.

Métodos de seguimiento, medición, análisis y evaluación: Establecer los métodos y frecuencia para llevar a cabo la supervisión y evaluación, determinando las técnicas que serán empleadas.

Evaluación de la eficacia de los controles: Esto se refiere a determinar cuando los controles no están operando correctamente.

ISO/IEC 27001:2013 – Cláusula 8.2: Evaluación de riesgos de seguridad de la información

En esta cláusula se establece la necesidad de que las organizaciones realicen evaluaciones periódicas de riesgo, así como cuando se presenten cambios importantes. Esto permitirá detectar posibles fallas en los controles vigentes y situaciones donde los parámetros de control hayan sido sobrepasados.

ISO/IEC 27002:2013 – Control 16.1.2: Reporte de Eventos de Seguridad de la Información

Este control garantiza la obligatoriedad de tener protocolos formales para informar los incidentes relacionados con la seguridad de la información y las vulnerabilidades asociadas, lo que permite recopilar pruebas cuando los mecanismos de protección no cumplen su función.

ISO 31000:2018 – Cláusula 6.6: Seguimiento y Revisión

Esta cláusula establece la necesidad de vigilar y evaluar los riesgos. Además de evaluar la eficacia de las estrategias y planes de gestión de riesgos, es importante tener en cuenta la importancia de registrar e informar los eventos en los cuales se superen los parámetros establecidos o cuando estos fallen.

Conclusiones

Falta de planificación adecuada para la gestión de la calidad y los controles asociados, debido a que existe retraso en el registro, almacenamiento y análisis de datos, y por ello existe pérdida de datos, registros incompletos o inaccesibles y planes de calidad incompletos lo que puede contemplar riesgos y controles innecesarios.

Recomendaciones

Dirigido al ingeniero en sistemas: Establecer un sistema robusto de gestión de datos que asegure el registro, almacenamiento y análisis adecuados de los datos de control.

Definir los parámetros aceptables para el acceso a datos sensibles, como el número de intentos fallidos de inicio de sesión.

Desarrollar y mantener actualizado un plan de calidad detallado que incluya todas las actividades de control necesarias para asegurar la conformidad con los parámetros establecidos.

Hallazgo 3: Evaluación del control interno COSO ERM 2017 – Desempeño 9

Comentario

Existe condiciones al seleccionar, y documentar los datos, parámetros y premisas por ello se incumple la **Norma ISO/IEC 27001 y la Norma ISO 31000.**

ISO/IEC 27001:2013 – Cláusula 6: Planificación

6.1.2 Evaluación de riesgos de seguridad de la información:

Es responsabilidad de la organización establecer e implementar criterios para evaluar las amenazas a la seguridad de la información, así como también establecer criterios para determinar cuándo es aceptable asumir dichos riesgos. Además, es importante que se asegure de mantener estos criterios actualizados. Para realizar la evaluación de riesgos, es necesario elegir y registrar los datos y parámetros pertinentes.

6.1.3 Tratamiento del riesgo de seguridad de la información:

Elegir las opciones adecuadas para abordar el riesgo en función de los resultados obtenidos en la evaluación de riesgos. Se requiere la documentación de esta selección, incluyendo los datos, parámetros y supuestos utilizados para tomar las decisiones sobre el manejo del riesgo.

ISO/IEC 27001:2013 – Cláusula 7: Soporte

7.5 Información documentada:

La organización tiene la responsabilidad de generar y mantener actualizada toda la documentación necesaria para respaldar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando así un adecuado control sobre dicha información documentada. Esto abarca la documentación de los datos, parámetros y premisas empleados en el Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 31000:2018 – Cláusula 6: Proceso de gestión del riesgo

6.4.1 Identificación del riesgo:

Identificar fuentes de riesgo, áreas de impacto, eventos (incluyendo cambios en las circunstancias) y sus causas y posibles consecuencias. Este paso implica la selección y documentación detallada de datos, parámetros y premisas que son fundamentales para la identificación de riesgos.

6.4.2 Análisis del riesgo:

Evaluar los posibles riesgos teniendo en cuenta tanto sus implicaciones como la probabilidad de que lleguen a ocurrir.

Es importante documentar los datos y parámetros utilizados en el análisis para garantizar un proceso transparente y rastreable.

6.4.3 Evaluación del riesgo:

Evaluar si el riesgo y/o su magnitud es aceptable o tolerable al cotejar los resultados del análisis de riesgo con los criterios predefinidos. Es fundamental registrar también esta comparación, junto con las premisas y los parámetros que se hayan utilizado.

6.5.2 Selección de opciones de tratamiento del riesgo:

Elegir la opción de manejo del riesgo que sea más adecuada. Es esencial registrar esta selección, abarcando los datos, criterios y suposiciones empleados, con el fin de garantizar la justificación y responsabilidad de las decisiones adoptadas.

6.6 Seguimiento y revisión:

Mantener la documentación actualizada y revisada regularmente es imprescindible para garantizar su pertinencia a medida que cambien las circunstancias y evolucionen los riesgos.

Conclusiones

Existen procedimientos que no se encuentran establecidos de manera clara y estandarizados para la selección y documentación de datos y parámetros, y por ello se toman ciertas decisiones no acertadas, lo que puede llevar a acciones incorrectas o ineficientes.

Recomendaciones

Dirigido al gerente: Creación de manuales, guías o políticas documentadas que describan los procesos de selección y documentación.

Establecer un proceso continuo de monitoreo y revisión, donde se asegure que todos los documentos relevantes se mantengan actualizados y reflejen cualquier cambio en los parámetros o premisas.

Asignar responsabilidades claras a los empleados para garantizar que los procesos se lleven a cabo de manera consistente y efectiva.

Hallazgo 4: Evaluación del control interno COSO ERM 2017 – Información, Comunicación y Reporte 9

Comentario

No se identifica continuamente oportunidades para mejorar la calidad de datos relacionados con el sistema de información de la cooperativa, por ello se incumple la **Norma ISO/IEC 27001, 27002 y la Norma ISO 31000.**

ISO/IEC 27001:2013 – Cláusula 10: Mejora

10.1 Mejora continua:

La organización debe trabajar constantemente para mejorar la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información (SGSI). Esto implica la búsqueda de posibilidades para mejorar todos los aspectos del SGSI, incluyendo tanto la calidad de los datos como su relación con los sistemas de información.

10.2 No conformidad y acción correctiva:

En caso de que se presente una no conformidad, la organización tiene la responsabilidad de actuar y tomar acciones para gestionarla y solucionarla, además de hacer frente a las repercusiones correspondientes. Una parte de esto consiste en detectar y solucionar inconvenientes vinculados a la calidad de los datos.

ISO/IEC 27002:2013 – Directrices para controles específicos

Control 12.2: Gestión de cambios:

Se debe tener en cuenta la evaluación y control de los cambios en los sistemas de información con el fin de garantizar que no se afecte la calidad de los datos durante las actualizaciones o modificaciones.

Control 16.1: Gestión de incidentes de seguridad de la información:

Dentro de la identificación y gestión de incidentes se encuentra el análisis de la precisión de los datos, así como la búsqueda activa para encontrar áreas donde sea posible optimizar los procesos vinculados a la administración de información.

ISO 31000 (Gestión del Riesgo)

ISO 31000:2018 – Cláusula 6: Proceso de gestión del riesgo

6.6 Seguimiento y revisión:

Es necesario mantener un monitoreo y revisión constante del proceso de gestión del riesgo para garantizar su eficacia y adecuación. Esto implica la constante evaluación de la calidad de los datos empleados en la identificación y análisis del riesgo.

6.5.3 Implementación del tratamiento del riesgo:

Una parte esencial del manejo de riesgos consiste en la mejora continua de los procesos y controles, con el objetivo de garantizar que toda la información relacionada al riesgo, incluyendo los datos asociados, sea precisa y posea una calidad óptima.

Conclusiones

Existe una privación de procesos formales para monitorear y evaluar la calidad de los datos de manera regular, y por ello hay datos de baja calidad que pueden resultar en procesos operativos ineficientes y costosos, lo que afectaría la integridad de los mismos.

Recomendaciones

Dirigido a la directora de procesos de calidad: Implementar procesos formales para monitorear y evaluar regularmente la calidad de los datos, incluidas revisiones periódicas y análisis de datos.

Dirigido al gerente: Realizar auditorías de calidad de datos trimestrales y revisiones continuas de los datos para identificar y corregir problemas.
Asignar recursos adecuados, como tiempo, personal y presupuesto, para actividades de mejora de la calidad de datos.

Dirigido al jefe de seguridad de la información: Medir la precisión de los datos, asegurándose de que reflejan correctamente la realidad. Realizar revisiones periódicas de los permisos de acceso y ajustar según sea necesario.

Hallazgo 5: Evaluación del control interno COSO ERM 2017 – Información, Comunicación y Reporte 9

Comentario

Se reporta información seleccionada sobre riesgos, cultura y desempeño de la cooperativa, por ello se incumple la **Norma ISO/IEC 27001 y la Norma ISO 31000.**

ISO/IEC 27001:2013 – Cláusula 7: Soporte

7.4 Comunicación:

Para el sistema de gestión de la seguridad de la información (SGSI), es responsabilidad de la organización identificar y evaluar las necesidades tanto en comunicación interna como externa. Esto implica establecer qué información se va a compartir, cuándo se hará, quiénes serán los destinatarios y cómo se realizará dicha comunicación.
Esto incluye la comunicación sobre riesgos, desempeño del SGSI y aspectos de la cultura de seguridad de la información.

ISO/IEC 27001:2013 – Cláusula 9: Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación:

Es responsabilidad de la organización evaluar el rendimiento y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), lo cual involucra tanto medir como analizar los riesgos y controles. Es necesario informar a la alta dirección y otras partes interesadas relevantes sobre los resultados de esta evaluación.

9.2 Auditoría interna:

Es necesario que las auditorías internas brinden datos sobre el cumplimiento de los requisitos del SGSI, tanto de la organización como de la norma ISO/IEC 27001. Es necesario informar sobre los descubrimientos de estas auditorías y utilizarlos para mejorar el sistema.

9.3 Revisión por la dirección:

Es necesario que la alta dirección realice revisiones programadas del SGSI para garantizar su constante idoneidad, relevancia y efectividad. En esta revisión, se debe tener en cuenta la cultura de seguridad de la información, así como también los resultados obtenidos del monitoreo y evaluación del rendimiento.

ISO 31000:2018 – Cláusula 6: Proceso de gestión del riesgo

6.2 Comunicación y consulta:

La comunicación y consulta con las partes interesadas son cruciales en todos los momentos del proceso de gestión de riesgos. Esto engloba la comunicación acerca de los riesgos, la cultura y el rendimiento en la gestión de riesgos.

6.6 Seguimiento y revisión:

Es responsabilidad de la organización seguir de cerca y evaluar el rendimiento del proceso de gestión de riesgos, informando los resultados a las partes involucradas. Además de evaluar la cultura organizacional, también se debe considerar su relación con la gestión de riesgos.

ISO 31000:2018 – Cláusula 5: Marco de gestión del riesgo

5.4 Integración:

Es esencial que la gestión del riesgo se incorpore de manera integral en la estructura organizativa, abarcando tanto la cultura empresarial como los procesos y políticas corporativas. Es importante que los informes reflejen la forma en que la gestión de riesgos está integrada y respaldada por la cultura organizativa.

5.6 Evaluación del marco de gestión del riesgo:

Es necesario que la organización realice una evaluación del rendimiento de su marco de gestión del riesgo y presente un informe con los resultados, abordando tanto aspectos relacionados con la cultura organizacional como las áreas donde se requiere mejorar en términos de gestión del riesgo.

Conclusiones

Existen procesos que no se han especificado de manera clara y estructurada para recopilar, analizar y reportar información relevante sobre riesgos, cultura y desempeño, y por ello la dificultad en la identificación de áreas de mejora y oportunidades para el crecimiento y la innovación.

Recomendaciones

Dirigido a la directora de procesos de calidad: Desarrollar procesos claros y estructurados para recopilar, analizar y reportar información relevante sobre riesgos, cultura y desempeño de la empresa y realizar revisiones periódicas del proceso de reporte buscando constantemente formas de mejorarlo y perfeccionarlo.

Ingeniero en sistemas y directora de riesgos: Emitir informes trimestrales a la alta dirección sobre el estado del SGSI, incluyendo riesgos, incidentes y acciones correctivas.

Encuestas anuales de cultura de seguridad para evaluar la percepción y comportamiento de los empleados respecto a la gestión de riesgos.

Hallazgo 6: Evaluación del control interno COSO ERM 2017 – Sistemas de seguridad de la información ~~9~~

Comentario

Ha existido en cierto tiempo el mal uso de la información con fines de soborno o fraude, por ello se incumple la **Norma ISO/IEC 27001 y la Norma ISO 31000.**

ISO/IEC 27001:2013

Cláusula 6.1: Acciones para abordar riesgos y oportunidades

6.1.2 Evaluación de riesgos de seguridad de la información:

La organización debe realizar evaluaciones de riesgo para identificar y tratar los riesgos, incluyendo los riesgos de fraude y mal uso de la información por parte de colaboradores internos.

Cláusula 7.5: Información documentada.

7.5.2 Creación y actualización:

La documentación de incidentes de seguridad, incluyendo el mal uso de la información, debe ser precisa y estar actualizada

Cláusula 9: Evaluación del desempeño

9.1 Monitoreo, medición, análisis y evaluación:

Monitorear y evaluar los controles para asegurar que los riesgos de seguridad de la información, como el fraude interno, se están gestionando adecuadamente.

ISO 31000:2018 – Cláusula 6: Proceso de gestión del riesgo

6.4 Evaluación del riesgo

6.4.2 Análisis del riesgo:

Analizar los riesgos identificados, incluyendo el riesgo de fraude interno y soborno, para evaluar sus consecuencias y la probabilidad de ocurrencia.

6.5 Tratamiento del riesgo

6.5.2 Selección de opciones de tratamiento del riesgo:

Selección de opciones adecuadas de tratamiento de los riesgos de fraude y soborno, como implementar controles adicionales o reforzar políticas de seguridad.

6.6 Seguimiento y revisión

Realizar monitoreo y revisar los controles de riesgo para asegurar así su eficacia continua y realizar mejoras cuando sea necesario.

Conclusiones

Tiempo atrás existió falta de controles, ética y diligencia profesional, y por ello provocó pérdida directa de dinero y recursos debido a actividades fraudulentas, así como afectación a la reputación institucional.

Recomendaciones

Dirigido al gerente: Realizar auditorías trimestrales para revisar el cumplimiento de las políticas de seguridad, así como el fortalecimiento de controles preventivos, detectivos y correctivos en la seguridad de la información

Dirigido al ingeniero en sistemas: Evaluar la probabilidad de que un colaborador interno cometa fraude utilizando estos datos.

Hallazgo 7: Evaluación del control interno COSO ERM 2017 – Sistemas de seguridad de la información ~~9~~

Comentario

Se ha detectado ciertas inconsistencias en la información reportada por las herramientas informáticas que utiliza la cooperativa, por ello se incumple la **Norma ISO/IEC 27001, 27002 y la Norma ISO 31000.**

ISO/IEC 27001:2013 Gestión de la Seguridad de la Información

Cláusula 8: Operación

8.2 Evaluación de riesgos de seguridad de la información:

Realizar evaluaciones constantes de riesgos para poder identificar y evaluar riesgos de seguridad de la información, incluyendo los riesgos que están derivados de inconsistencias en la información reportada por herramientas informáticas.

8.3 Tratamiento del riesgo de seguridad de la información:

Implementar controles apropiados para tratar los riesgos identificados. Esto incluye medidas para detectar, corregir y prevenir inconsistencias en la información.

Cláusula 9: Evaluación del desempeño

9.1 Monitoreo, medición, análisis y evaluación:

La organización debe monitorear y medir regularmente la eficacia del SGSI (Sistema de Gestión de la Seguridad de la Información). Esto incluye la verificación de la precisión y consistencia de la información generada por las herramientas informáticas.

9.2 Auditoría interna:

Realizar auditorías internas periódicas para asegurar que el SGSI es conforme a los requisitos y es eficaz en gestión de riesgos, incluyendo la detección de inconsistencias en la información.

Cláusula 10: Mejora

10.1 No conformidad y acción correctiva:

La organización debe tomar acciones correctivas para abordar las no conformidades y prevenir su recurrencia cuando se detecten inconsistencias en la información.

ISO/IEC 27002:2013 – Directrices para controles específicos

Control 12.2: Gestión de cambios:

Tener la seguridad que todos los cambios en los sistemas de información están controlados y que no existen o reportan inconsistencias o errores en la información.

Control 12.4: Registros y monitoreo:

12.4.1 Eventos de registro:

Implementar el registro de eventos para monitorear actividades del sistema y detectar inconsistencias en la información.

Control 16.1: Gestión de incidentes de seguridad de la información:

16.1.2 Reporte de eventos de seguridad de la información:

Establecer un proceso para el reporte y gestión de incidentes.

ISO 31000:2018 Gestión del Riesgo

Cláusula 6: Proceso de gestión del riesgo

6.4 Evaluación del riesgo

6.4.2 Análisis del riesgo:

Evaluar los riesgos asociados con las inconsistencias en la información reportada por herramientas informáticas, el impacto potencial y la probabilidad de ocurrencia.

6.5 Tratamiento del riesgo

6.5.2 Selección de opciones de tratamiento del riesgo:

Implementación de opciones de tratamiento del riesgo adecuadas para abordar las inconsistencias en la información. Esto puede incluir la mejora de las herramientas de software y los procesos de verificación de datos.

Cláusula 7: Revisión y mejora continua

7.1 Monitoreo y revisión

Monitorear y revisar continuamente el desempeño del proceso de gestión de riesgos para asegurar que las inconsistencias en la información sean detectadas y corregidas oportunamente.

Conclusiones

Errores humanos en la entrada de datos por falta de capacitación en el manejo de las herramientas informáticas institucionales, conlleva a que exista información inconsistente lo que puede orientar a decisiones empresariales erróneas que afecten negativamente a la cooperativa. Gastos adicionales relacionados con la identificación y corrección de errores en la información y retrasos en la actualización de los datos que resultan en la presentación de información obsoleta.

Recomendaciones

Dirigido al gerente: Realizar talleres de capacitación para el personal sobre cómo detectar y reportar inconsistencias en la información. Proveer guías y procedimientos claros para la gestión de estos incidentes.

Dirigido al ingeniero en sistemas: Establecer un equipo de respuesta a incidentes que gestione y corrija las inconsistencias reportadas. Documentar cada incidente y su resolución para análisis futuro.

Evaluación del nivel de madurez COSO ERM

Hallazgo 8: Evaluación del nivel de madurez COSO ERM 2017 – Estrategias y Objetivos λ

Comentario

En el nivel de madurez y eficiencia del sistema de control interno, el componente Estrategias y objetivos tiene una calificación media lo que indica que se encuentra en un nivel en proceso, por limitaciones en el cumplimiento del apartado de **Estrategias y objetivos:** se centra en establecer metas y objetivos alineados con la misión y visión de la organización, así como en garantizar que se identifiquen y gestionen los riesgos que podrían afectar la capacidad de la organización para alcanzar esos objetivos.

Conclusiones

Los procesos deben ser efectivos para monitorear y revisar continuamente el cumplimiento de los objetivos estratégicos y las estrategias de la cooperativa, es posible que los problemas no se identifiquen ni se aborden a tiempo, y por ello existe una falta de alineación entre la gestión de riesgos y los objetivos estratégicos que puede llevar a la cooperativa a no cumplir sus metas a largo plazo. Esto puede resultar en una variable dirección y enfoque, así como el no aprovechamiento de oportunidades importantes.

Recomendaciones

Dirigido al gerente: Fortalecer procesos efectivos para monitorización y revisar continuamente cumplimiento de objetivos estratégicos y estrategias.

Evaluación de la matriz de riesgos informáticos

Hallazgo 9: Matriz de riesgos – Gestión de riesgos informáticos Ψ

Comentario

Existe riesgo operativo, debido a vulnerabilidades detectadas en el software, personas, procesos y tecnologías de información, por ello se incumple **la NORMA ISO 27001 y la NORMA 410-09**

Control de Acceso (Anexo A.9):

A.9.1.1 Política de control de acceso: Define los requisitos de acceso a la información y los sistemas de información. El acceso controlado ayuda a prevenir cambios no autorizados que puedan causar desactualización.

A.9.4.1 Restricción del acceso a la información: Asegura que solo los usuarios autorizados puedan modificar los datos.

Gestión de Activos (Anexo A.8):

A.8.1.1 Inventario de activos: Mantener un inventario de activos de información para asegurar que todos los datos sean gestionados adecuadamente.

A.8.2.2 Clasificación de la información: Clasificación y tratamiento de la información según su importancia, lo cual puede incluir políticas para mantener la información actualizada.

Seguridad en los Procesos Operativos (Anexo A.12):

A.12.1.1 Procedimientos operativos y responsabilidades: Establecer procedimientos operativos claros, incluyendo aquellos relacionados con la actualización de datos.

A.12.4.1 Registro y monitoreo de eventos: Monitorear y registrar eventos para detectar y corregir rápidamente cualquier desactualización de la información.

Gestión de Incidentes de Seguridad de la Información (Anexo A.16):

A.16.1.2 Notificación de eventos de seguridad: Identificación y gestión de incidentes que puedan resultar de información desactualizada.

NORMA 410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

Conclusiones

Existe limitados procedimientos definidos para la revisión y actualización periódica de la información debido a que se ha realizado el registro incorrecto de datos en algunas ocasiones, y por ello existen procesos interrumpidos o incorrectos pueden resultar en pérdida de tiempo y recursos, afectando la productividad y la desactualización de la base de datos lo que puede impedir que la cooperativa identifique y aproveche oportunidades de negocio y mejora.

Recomendaciones

Gerente: Proveer capacitación continua a los empleados sobre la importancia de la calidad de los datos y los procedimientos para mantener la información actualizada, realizar auditorías regulares de la calidad de los datos para asegurar la precisión y actualidad de la información.

Dirigido al ingeniero en sistemas: Establecer mecanismos de monitoreo continuo para detectar y corregir errores en los datos de manera oportuna.

Hallazgo 10: Matriz de riesgos – Gestión de riesgos informáticos Ψ

Comentario: Ha existido envío de la información a personas que no pertenecen a la cooperativa, por ello se incumple **la NORMA ISO 27001, la ISO 31000 y la NORMA 410-15.**

ISO 27001

Control de Acceso (Anexo A.9):

A.9.1.1 Política de control de acceso: Establece la necesidad de definir políticas de acceso claras para asegurar que solo las personas autorizadas tengan acceso a la información sensible.

A.9.4.1 Restricción del acceso a la información: Implementa controles para restringir el acceso a la información solo a las personas autorizadas.

Gestión de Comunicaciones y Operaciones (Anexo A.13):

A.13.1.1 Política de seguridad de la red: Asegura la protección de la información en las redes y la gestión segura de la transmisión de datos.

A.13.2.1 Políticas y procedimientos para la transferencia de información: Desarrolla políticas y procedimientos para proteger la información durante su transferencia, incluyendo controles sobre el envío de información a destinatarios no autorizados.

Gestión de Incidentes de Seguridad de la Información (Anexo A.16):

A.16.1.2 Gestión de incidentes de seguridad: Identificación, respuesta y gestión de incidentes relacionados con el envío de información a personas no autorizadas.

Cumplimiento (Anexo A.18):

A.18.1.4 Privacidad y protección de datos personales: Asegura el cumplimiento con las leyes y regulaciones de protección de datos, previniendo la divulgación no autorizada de información personal.

ISO 31000

Proceso de Gestión del Riesgo (Cláusula 6):

6.4.2 Identificación del riesgo: Identificación de riesgos específicos relacionados con el envío de información a personas no autorizadas.

6.4.3 Análisis del riesgo: Evaluación de la probabilidad e impacto de estos riesgos.

6.4.4 Evaluación del riesgo: Determinación del nivel de riesgo aceptable y priorización de los riesgos identificados.

6.5 Tratamiento del riesgo: Implementación de controles y medidas para mitigar estos riesgos, tales como políticas de seguridad de la información, capacitación del personal y tecnologías de protección de datos.

NORMA 410-15 Capacitación informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

Conclusiones

En la cooperativa existió personal con malas prácticas para en el manejo de la información, y por ello la información sensible llegó a usuarios no autorizados, comprometiendo la privacidad de los socios y la seguridad.

Recomendaciones

Dirigido al gerente: Proveer capacitación continua al personal sobre las mejores prácticas para el manejo de la información y la importancia de la confidencialidad.

Los niveles de capacidad de los procesos según el marco de referencia COBIT 5 a los procesos más asociados con las necesidades de operatividad y evaluación de la cooperativa

Hallazgo 11: Evaluación del proceso EDM03 φ

Comentario

En la práctica clave de gobierno EDM03.01 no se determina el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 2 –Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **EDM03.01 Evaluar la gestión de riesgos.**

Práctica: Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.

Actividad: 3 Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.

Conclusiones

Existe una desconexión entre los equipos de TI y los responsables de la gestión de riesgos empresariales debido a una comunicación ineficaz y las prioridades y objetivos de la gestión de riesgos de TI no están alineados con las prioridades estratégicas y objetivos de la cooperativa, y por ello la gestión de riesgos de TI y la gestión de riesgos empresariales pueden tomar direcciones diferentes, resultando en inconsistencias y potenciales brechas de seguridad. La falta de alineación puede llevar a decisiones empresariales mal informadas que no consideran todos los riesgos pertinentes, afectando negativamente la resiliencia de la organización.

Recomendaciones

Dirigido a la directora de riesgos: Establecer procesos de monitoreo y revisión continua para asegurar que las estrategias de riesgos de TI y empresariales se mantengan alineadas y se adapten a los cambios en el entorno empresarial y tecnológico.

Hallazgo 12: Evaluación del proceso EDM03 φ

Comentario

En la práctica clave de gobierno EDM03.02 no se promueve una cultura consciente de los riesgos TI e impulsar a la cooperativa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 2 –Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **EDM03.02 Orientar la gestión de riesgos.**

Práctica: Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.

Actividad 1: Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.

Conclusiones

Los empleados y directivos no están suficientemente informados sobre los riesgos de TI y su impacto en el negocio debido a la falta de programas de capacitación y concienciación, y por ello la incapacidad para identificar proactivamente oportunidades de mejora de TI limita la capacidad de la cooperativa para innovar y mantenerse competitiva en su mercado.

Recomendaciones

Dirigido al gerente: Reconocer y recompensar a los empleados que identifican proactivamente riesgos de TI y sugieren soluciones para mitigarlos, fomentando así una cultura de prevención.

Dirigido al ingeniero en sistemas: Establecer canales claros y seguros para que los empleados reporten incidentes de seguridad y asegurarse de que se tomen las medidas adecuadas en respuesta.

Dirigido al jefe de seguridad de la información: Presentar informes periódicos a la alta dirección sobre el estado de la seguridad de la información y cómo está protegiendo los activos y el negocio de la cooperativa.

Hallazgo 13: Evaluación del proceso EDM03 φ

Comentario

En la práctica clave de gobierno EDM03.02 existe limitación en orientar a la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 2 – Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **EDM03.02 Orientar la gestión de riesgos.**

Práctica: Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.

Actividad 2: Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.

Conclusiones

Las políticas y procesos establecidos para integrar TI con la estrategia empresarial, deben ser alineados de manera más clara, además la falta de un marco de gobernanza que guíe la integración de TI y la estrategia empresarial puede provocar que exista dificultad para innovar y adaptarse a cambios del mercado. Además, que se tomen decisiones incorrectas debido a que no se integre operaciones y estrategias de riesgos con decisiones empresariales.

Recomendaciones

Dirigido al gerente: Establecer canales de comunicación claros y regulares entre TI y las unidades de negocio.

Realizar un mapeo de los objetivos de TI con los objetivos estratégicos de la cooperativa.

Dirigido al ingeniero en sistemas: Colaborar estrechamente con líderes empresariales para asegurarse de que las iniciativas de TI apoyen estos objetivos.

Alinear los proyectos y prioridades de TI con las prioridades estratégicas de la cooperativa.

Hallazgo 14: Evaluación del proceso APO02 φ

Comentario

En la práctica clave de gestión APO02.03 la definición del objetivo de las capacidades de TI requiere alineación y acuerdo con los cambios en la arquitectura empresarial con el gobierno corporativo; lo que incumple la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS,** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como

iniciales o intuitivas no muy organizadas, en **APO02.03 Definir el objetivo de las capacidades de TI.**

Práctica: Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.

Actividad 5: Alinear y acordar los cambios en la arquitectura de empresa con el arquitecto corporativo.

Conclusiones

Las áreas operativas y los equipos de proyecto no comunican de manera oportuna sus iniciativas de cambio al arquitecto corporativo, los equipos no están conscientes del papel y la importancia del arquitecto corporativo en los cambios de arquitectura. Falta de una visión integral de la arquitectura empresarial, lo que provoca decisiones aisladas y descoordinadas y hay una inexistencia de un marco de gobernanza sólido que integre las decisiones de arquitectura a nivel corporativo, y por ello hay una incapacidad para responder rápidamente a cambios del mercado y oportunidades estratégicas y retrasos en la implementación de proyectos debido a problemas no anticipados de integración y compatibilidad.

Recomendaciones

Dirigido al gerente: Crear canales de comunicación formales y regulares entre los equipos de proyecto y el arquitecto corporativo.

Elaborar una visión integral de la arquitectura empresarial que sea compartida y entendida por todas las áreas.

Formar un comité de arquitectura que incluya al arquitecto corporativo y representantes clave de diferentes áreas.

Hallazgo 15: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.01 no se define el alcance y los límites del SGSI en términos de las características de la cooperativa, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas, en **APO13.01 Establecer y mantener un SGSI.**

Práctica: Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.

Actividad 2: Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología

Conclusiones

Falta de una evaluación integral de riesgos que identifique todas las áreas críticas. Subestimación de las amenazas y vulnerabilidades a las que está expuesta la organización y la existencia de otras prioridades de negocio que desvían la atención y los recursos necesarios, y por ello hay aumento en la frecuencia y gravedad de incidentes de seguridad.

Recomendaciones

Dirigido al gerente: Programas de formación para todos los empleados sobre la importancia del SGSI y sus componentes.
Incentivar certificaciones como ISO 27001 para el personal clave.

Dirigido al jefe de seguridad de la información: Documentar y justificar cualquier exclusión del alcance, asegurando que no se comprometa la seguridad general.
Establecer mecanismos de retroalimentación y mejora continua para el SGSI.

Hallazgo 16: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.01 existe limitaciones en la definición del SGSI de acuerdo con la política y alineada con la empresa, la organización, su localización, activos y tecnología; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS,** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas, en **APO13.01 Establecer y mantener un SGSI.**

Práctica: Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.

Actividad 2: Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.

Conclusiones

No se reconocen todas las amenazas y vulnerabilidades a las que está expuesta la organización y existe una falta de familiaridad con normas y estándares como ISO 27001, y por ello existen fallos en sistemas críticos que afectan la continuidad del negocio.

Recomendaciones

Dirigido al gerente: Realizar auditorías periódicas y revisiones del SGSI para asegurar su efectividad y conformidad.

Dirigido al jefe de seguridad de la información: Revisar y actualizar el alcance del SGSI según sea necesario para reflejar cambios en la organización, tecnología o entorno de amenazas.

Hallazgo 17: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.01 no se prepara ni se mantiene una declaración de aplicabilidad que describa el alcance del SGSI; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS,** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas, en **APO13.01 Establecer y mantener un SGSI.**

Práctica: Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.

Actividad 5: Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.

Conclusiones

Políticas de seguridad de la información no actualizadas que no reflejan las prácticas actuales, por ello existen vulnerabilidades no mitigadas debido a la falta de controles apropiados.

Recomendaciones

Dirigido al jefe de seguridad de la información: Revisar y actualizar las políticas de seguridad de la información para reflejar las prácticas actuales y los requisitos normativos.

Hallazgo 18: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.02 no se proporciona información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información; por el incumplimiento de la

NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS encontrándose en un **nivel de capacidad 2 – Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.**

Práctica: Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.

Actividad 4: Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.

Conclusiones

Existe fallos en la comunicación entre los equipos de seguridad y otros departamentos, y ausencia de procesos estandarizados para el diseño y desarrollo de prácticas de gestión de riesgos, por ello existe una falta de planificación adecuada para la obtención de controles y desarrollo de prácticas de gestión.

Recomendaciones

Dirigido a la directora de riesgos: Diseñar y desarrollar prácticas de gestión basadas en la información proporcionada por el plan de tratamiento de riesgos.

Dirigido al jefe de seguridad de la información: Establecer mecanismos para recolectar y analizar la retroalimentación de los equipos sobre la implementación del plan de tratamiento de riesgos.

Hallazgo 19: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.03 no se realizan auditorías internas al SGSI a intervalos planificados; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas, en **APO13.03 Supervisar y revisar el SGSI.**

Práctica: Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

Actividad 2: Realizar auditorías internas al SGSI a intervalos planificados.

Conclusiones

Falta de un calendario de auditorías bien definido y planificado y una falta de conformidad con estándares y regulaciones como ISO 27001, y por ello hay fallos en sistemas críticos que afectan la continuidad del negocio.

Recomendaciones

Dirigido al gerente: Implementar programas de formación continua sobre la importancia y los procedimientos de auditoría interna.

Fomentar la obtención de certificaciones relevantes y la participación en talleres de auditoría interna.

Crear un calendario detallado para realizar auditorías internas en intervalos planificados.

Revisar y ajustar el calendario según sea necesario para asegurar que se cumplan los plazos.

Asegurar el compromiso de la alta dirección para apoyar y priorizar las auditorías internas.

Hallazgo 20: Evaluación del proceso APO13 φ

Comentario

En la práctica clave de gestión APO13.03 no se realizan revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI; por el incumplimiento de **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 1 – Ejecutado donde:** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas, en **APO13.03 Supervisar y revisar el SGSI.**

Práctica: Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

Actividad 3: Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.

Conclusiones

Hay ausencia de procedimientos establecidos para la revisión del SGSI. Falta de planificación y programación de las revisiones periódicas, y no se realiza un seguimiento adecuado de las revisiones anteriores y las acciones correctivas, y por ello existen controles de seguridad que pueden no ser efectivos ante nuevas amenazas. Hay recursos desperdiciados debido a la falta de revisiones adecuadas y actualizaciones necesarias.

Recomendaciones

Dirigido al gerente: Realizar sesiones de sensibilización y capacitación para la alta dirección sobre la importancia de las revisiones del SGSI.

Crear y documentar procedimientos claros para la revisión periódica del SGSI.

Integrar las revisiones del SGSI en el calendario de la alta dirección.

Desarrollar y seguir planes de acción correctiva para abordar los problemas identificados durante las revisiones.

Dirigido al jefe de seguridad de la información: Proponer reuniones trimestrales o semestrales para revisar el estado del SGSI y discutir posibles mejoras.

Hallazgo 21: Evaluación del proceso BAIA09 φ

Comentario

En la práctica clave de gestión BAI09.04 no se obtiene estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes; por el incumplimiento de la **NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 2 – Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **BAI09.04 Optimizar el coste de los activos.**

Práctica: Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.

Actividad 5: Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.

Conclusiones

No disponen de herramientas adecuadas para monitorear y analizar la capacidad y utilización de los activos y uso de sistemas antiguos que no proporcionan datos precisos o en tiempo real. Las políticas de gestión de activos que no incluyen la evaluación periódica de la utilización de recursos, y por ello hay un mantenimiento y operación de activos infrautilizados o redundantes aumentando los costos operativos. Existen fondos inmovilizados en activos que no aportan valor significativo, activos que se vuelven obsoletos sin una revisión regular de su utilización. Falta de datos precisos afecta la toma de decisiones estratégicas sobre la gestión de activos.

Recomendaciones

Dirigido al jefe de seguridad de la información: Implementar herramientas de monitoreo y análisis de capacidad y utilización de activos.

Actualizar sistemas y tecnologías obsoletas para mejorar la precisión y eficiencia del monitoreo.

Hallazgo 22: Evaluación del proceso MEA02 φ

Comentario

En la práctica clave de gestión MEA02.03 no se determina la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua; por el incumplimiento de **la NORMA ISO 15504 NIVELES DE CAPACIDAD DE LOS PROCESOS** encontrándose en un **nivel de capacidad 2 – Administrado donde:** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas, en **MEA02.03 Realizar autoevaluaciones de control.**

Práctica: Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.

Actividad 2: Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.

Conclusiones

Hay ausencia de un enfoque estructurado para determinar la frecuencia óptima de las autoevaluaciones y ausencia de un proceso formal para incorporar los hallazgos de las autoevaluaciones en la toma de decisiones y la mejora continua, y por ello hay pérdida de oportunidades para implementar mejoras proactivas y prevenir problemas futuros y riesgo de estancamiento y obsolescencia en un entorno empresarial en constante cambio.

Recomendaciones

Dirigido a la directora de procesos de calidad: Definir claramente los objetivos y propósitos de las autoevaluaciones periódicas en el contexto del sistema de gestión y los procesos organizacionales y establecer mecanismos formales para el seguimiento y la revisión de las acciones correctivas y preventivas derivadas de las autoevaluaciones.

Conclusión general

En conclusión, se puede decir que la gestión de los activos de información es adecuada, demostrado una sólida estructura de su gestión, asegurando la integridad, disponibilidad y confidencialidad de los datos. Existe un buen control interno, sin embargo, en la gestión de las TI existen actividades incompletas que dificultan en cierta manera el cumplimiento óptimo de las prácticas clave de gobierno evaluadas, no obstante existen prácticas que si se cumplen pero no en el plazo establecido, y existe una falta de comunicación de la gestión de los controles de seguridad existentes a los demás departamentos, por ello se propone un manual de políticas de seguridad direccionada a la utilización de las herramientas informáticas contables, por la importancia que representan, para el almacenamiento, procesamiento y salida de información.

3.1.4 Manual de políticas de seguridad

A continuación, se estableció un manual de políticas de seguridad que cubre una amplia gama de aspectos relacionados con la seguridad, incluyendo, pero no limitándose a, la gestión de accesos, la protección de datos, respuesta a incidentes y la concienciación sobre la seguridad de la información que maneja a través de sus plataformas y sistemas informáticos contables. Cada política ha sido diseñada para cumplir con las normativas y estándares de seguridad aplicables según la norma ISO/IEC 27001, así como para identificar amenazas y riesgos específicos a los que se expone la cooperativa.

4. **Protección y respaldo de información**

Objetivo: Garantizar la integridad, confidencialidad y disponibilidad de la información contable y financieros mediante la implementación de medidas de protección y respaldo de información.

Alcance: Esta política es aplicada a todos los sistemas, bases de datos y usuarios que manejan información dentro de Softbank que es el sistema informático contable en el cual se almacena la información histórica correspondiente a los movimientos financieros de la cooperativa.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones

Políticas:

- Realizar respaldos automáticos de toda la información diariamente de preferencia al inicio de la jornada laboral y al final de la misma.
- Almacenar los respaldos en ubicaciones seguras y diferentes de la ubicación principal, esto puede ser en la nube, en dispositivos externos que tengan capacidad de almacenamiento suficiente para su conservación.
- Probar regularmente la restauración de los respaldos para asegurar su efectividad, principalmente cuando exista una actualización del sistema contable informático permitiendo la obtención eficiente de los datos.

Roles y responsables

Jefe de seguridad de la información: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Ing. Sistemas de información: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el jefe de seguridad de la información.

2. Bitácora de accesos

Objetivo: Mantener un registro detallado de todos los accesos al sistema informático contable para poder monitorear y auditar actividades sospechosas.

Alcance: Se aplica a todos los usuarios que tienen acceso a Softbank sistema informático contable.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones

Políticas:

- Implementar registros automáticos de acceso que incluyan fecha, hora, usuario y el tipo de actividad realizada en el sistema contable.
- Guardar las bitácoras de acceso durante al menos 7 años.
- Revisar y auditar las bitácoras mensualmente para identificar y responder a actividades inusuales.

Roles y responsables

Jefe de seguridad de la información: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Ing. Sistemas de información: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el jefe de seguridad de la información.

3. Plan de educación y concientización del usuario en seguridad de la información

Objetivo: Asegurar que todos los usuarios se encuentren informados y capacitados sobre las mejores prácticas de seguridad de la información.

Alcance: Aplica a todos los empleados, especialmente a los departamentos de sistemas de la información y seguridad de la información.

Controles:

- Capacitaciones periódicas al personal de la cooperativa

Políticas:

- Desarrollar y distribuir material educativo sobre seguridad de la información.
- Realizar sesiones de capacitación semestrales para todos los usuarios.
- Evaluar regularmente el conocimiento de los usuarios sobre las políticas de seguridad.

Roles y responsables: informantes empleados

Gerente: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Jefe de seguridad de la información: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el gerente.

Jefes departamentales de la cooperativa: Su rol será de informantes de las políticas establecidas.

4. **Protección contra software malicioso**

Objetivo: Prevenir y detectar la presencia de software malicioso en el sistema Softbank.

Alcance: Todos los sistemas y dispositivos utilizados para acceder a Softbank.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones
- Antivirus
- EDR (Detección y respuesta de Endpoint)
- Controles implementados en los servidores de 104icrosoft

Políticas:

- Instalar y actualizar regularmente software antivirus y antimalware.
- Ejecutar análisis de seguridad completos en todos los sistemas semanalmente.
- Restringir la descarga e instalación de software no autorizado.
- Verificar trimestralmente la vigencia de las licencias de antivirus.
- Realizar pruebas de simulación de accesos a la red interna para la verificación de firewalls y restricciones de accesos.

Roles y responsables

Jefe de seguridad de la información: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Ing. Sistemas de información: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el jefe de seguridad de la información.

4. **Bloqueos de sesión**

Objetivo: Proteger los sistemas de acceso no autorizado mediante la implementación de bloqueos de sesión a las plataformas, correos, y aplicativos utilizables en los departamentos de la cooperativa.

Alcance: Todos los usuarios del sistema contable Softbank.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones
- Antivirus
- EDR (Detección y respuesta de Endpoint)
- Controles implementados en los servidores de 105icrosoft

Políticas:

- Configurar bloqueos automáticos de sesión luego de 15 minutos de inactividad.

- Requerir código de autenticación para reactivar una sesión bloqueada.
- Monitorear y registrar todos los bloqueos y reactivaciones de sesión.

Roles y responsables

Jefe de seguridad de la información: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Ing. Sistemas de información: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el jefe de seguridad de la información.

4. **Acceso y control a instalaciones físicas y sistemas de red**

Objetivo: Asegurar que solo personal autorizado tenga acceso a las instalaciones físicas del departamento informático y al sistema de red de Softbank.

Alcance: Aplica a las instalaciones físicas del departamento informático y de seguridad de la cooperativa y redes de Softbank.

Controles:

- Sistema CCTV sistema de circuito cerrado de televisión
- Bobedas o armarios de seguridad

Políticas:

- Establecer niveles de acceso basados en roles y responsabilidades.
- Monitorear y registrar el acceso a las instalaciones y a la red.
- Verificar la vigencia y autentificación de las tarjetas de acceso.

Roles y responsables

Gerente: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Jefes departamentales de la cooperativa: Su rol será de informantes de las políticas establecidas.

7. Gestión de archivos físicos

Objetivo: Asegurar una gestión adecuada y segura de los datos en todo su ciclo de vida.

Alcance: Todos los datos manejados por Softbank.

Controles:

- Archivero del personal de la cooperativa

Políticas:

- Clasificar los archivos según su nivel de sensibilidad.
- Implementar medidas de protección adecuadas para cada nivel de clasificación.
- Aplicar procedimientos para recolección, almacenamiento de archivos
- Mantener la información archivada durante 7 años.

Roles y responsables

Jefes departamentales de la cooperativa: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Gerente: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por cada jefe departamental.

8. Manejo y seguridad de la documentación interna

Objetivo: Proteger la documentación interna de accesos no autorizados y asegurar su integridad.

Alcance: Toda la documentación interna.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones
- Antivirus
- EDR (Detección y respuesta de Endpoint)

Políticas:

- Archivar la documentación en ubicaciones seguras y accesibles solo para personal autorizado.
- Usar cifrado para la documentación electrónica sensible.
- Realizar auditorías periódicas para asegurar la integridad y seguridad de la documentación.
- Mantener la información archivada de manera digital durante 10 años y de manera física durante 7 años.

Roles y responsables

Gerente: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Jefes departamentales de la cooperativa: Su rol será de informantes de las políticas establecidas.

9. Registro histórico de actividades

Objetivo: Mantener un registro detallado de todas las actividades importantes dentro de Softbank para auditorías y revisiones.

Controles:

- Firewall perimetral
- Software para prevención de fuga de información
- Firewall de aplicaciones
- Antivirus
- EDR (Detección y respuesta de Endpoint)

Alcance: Todas las actividades críticas dentro de Softbank.

Políticas:

- Registrar automáticamente todas las actividades relevantes, incluyendo transacciones, cambios en el sistema y accesos a datos sensibles.
- Conservar los registros históricos durante al menos siete años.

- Auditar los registros históricos trimestralmente para asegurar la precisión y detectar posibles incidentes de seguridad.

Roles y responsables

Ing. Sistemas de información: El rol que le compete será como responsable de llevar a cabo el cumplimento de las políticas incluidas.

Gerente: El rol será de administrador quien gestionará el cumplimiento de las políticas que son llevadas a cabo por el Ing. en sistemas.

3.1.5 Matriz de seguimiento y monitoreo

Se realizó una matriz de monitoreo y seguimiento de las políticas de seguridad con el fin de evaluar de manera sistemática y continua la implementación y efectividad de dichas políticas en la cooperativa. Esta matriz proporciona una visión integral de los diversos aspectos de la seguridad, identificando áreas de mejora y asegurando la conformidad con las normativas establecidas.

3.1.5.1 Instrucciones para utilización de la matriz de seguimiento y monitoreo

- El gerente o el jefe departamental según el encargado de la actividad deberá abrir el archivo al finalizar el mes, para el respectivo control.
- Los encargados deberán llenar los siguientes campos: fecha de seguimiento, control realizado, hora de inicio, hora de fin, porcentaje de cumplimiento y su respectiva firma. En cada actividad deberán detallar el control que realicen.
- Si el porcentaje de cumplimiento es igual o mayor a 50% se resaltará la celda SI con color verde, en caso de tener un porcentaje menor al 50% se enfatizará la celda NO con color rojo.
- Las actividades también se sombrearán según el porcentaje de cumplimiento en los siguientes rangos: rojo menor a 50%, amarillo de 50% hasta 79% verde de 80% a 100%. El color verde quiere decir que se completa la política, el color amarillo que la política se la cumple, pero hay falencias en el proceso de realizarla, el rojo es que la actividad está incompleta, o no se la realiza de forma correcta por ello el porcentaje de cumplimiento es bajo.

- Luego de llenada la matriz se imprimirá y se firmará de manera autógrafa o manuscrita, de igual manera se digitalizará en archivo pdf y deberá constar las firmas electrónicas como evidencia de verificación de la persona o las personas a cargo, la matriz impresa y digitalizada se archivará durante 7 años.

Ilustración 47

Ejemplo de utilización de la matriz de seguimiento

MATRIZ DE SUPERVISIÓN Y MONITOREO											
Política	**Fecha de seguimiento**	**Politicas**	**Descripción del control realizado**	**Hora de inicio**	**Hora de fin**	**Porcentaje de cumplimiento**	**Cumplimiento**		**Encargado de cumplimiento**	**Firma responsable**	**Firma de gerencia**
							SI	**NO**			
Protección y respaldo de información	**22/06/2024**	Realizar respaldos automáticos de toda la información diariamente de preferencia al inicio de la jornada laboral y al final de la misma.		8AM	7PM	**100%**			Jefe de seguridad de la información		
		Almacenar los respaldos en ubicaciones seguras y diferentes de la ubicación principal, esto puede ser en la nube, en dispositivos externos que tengan capacidad de almacenamiento suficiente para su conservación.		9AM	10AM	**50%**					
		Probar regularmente la restauración de los respaldos para asegurar su efectividad, principalmente cuando exista una actualización del sistema contable informático permitiendo la obtención eficiente de los datos.		10AM	11AM	40%					

Elaborado por: Henriquez (2024)

Mientras no se llene la matriz estará pintado el NO y todas las actividades de color rojo como incumplidas.

Ilustración 48

Matriz de supervisión y monitoreo

MATRIZ DE SUPERVISIÓN Y MONITOREO											
Política	**Fecha de seguimiento**	**Politicas**	**Descripción del control realizado**	**Hora de inicio**	**Hora de fin**	**Porcentaje de cumplimiento**	**Cumplimiento**		**Encargado de cumplimiento**	**Firma responsable**	**Firma de gerencia**
							SI	**NO**			
Protección y respaldo de información		Realizar respaldos automáticos de toda la información diariamente de preferencia al inicio de la jornada laboral y al final de la misma.							Jefe de seguridad de la información		
		Almacenar los respaldos en ubicaciones seguras y diferentes de la ubicación principal, esto puede ser en la nube, en dispositivos externos que tengan capacidad de almacenamiento suficiente para su conservación.									
		Probar regularmente la restauración de los respaldos para asegurar su efectividad, principalmente cuando exista una actualización del sistema contable informático permitiendo la obtención eficiente de los datos.									
Bitácora de Accesos		Implementar registros automáticos de acceso que incluyan fecha, hora, usuario y el tipo de actividad realizada en el sistema contable.							Jefe de seguridad de la información		
		Revisar y auditar las bitácoras mensualmente para identificar y responder a actividades inusuales.									
Plan de educación y concientización del usuario en seguridad de la información		Desarrollar y distribuir material educativo sobre seguridad de la información.							Gerente		
		Realizar sesiones de capacitación semestrales para todos los usuarios.									
		Evaluar regularmente el conocimiento de los usuarios sobre las políticas de seguridad.									

Protección contra software malicioso		Instalar y actualizar regularmente software antivirus y antimalware.							Jefe de seguridad de la información		
		Ejecutar análisis de seguridad completos en todos los sistemas semanalmente.									
		Restringir la descarga e instalación de software no autorizado.									
		Verificar trimestralmente la vigencia de las licencias de antivirus.									
		Realizar pruebas de simulación de accesos a la red interna para la verificación de firewalls y restricciones de accesos.									
Bloqueos de sesión		Configurar bloqueos automáticos de sesión luego de 15 minutos de inactividad							Jefe de seguridad de la información		
		Requerir código de autenticación para reactivar una sesión bloqueada.									
		Monitorear y registrar todos los bloqueos y reactivaciones de sesión.									
Acceso y control a instalaciones físicas y sistemas de red		Establecer niveles de acceso basados en roles y responsabilidades.							Gerente		
		Monitorear y registrar el acceso a las instalaciones y a la red.									
		Verificar la vigencia y autentificación de las tarjetas de acceso.									
Gestión de archivos físicos		Clasificar los archivos según su nivel de sensibilidad.							Jefes departamentales de la cooperativa		
		Implementar medidas de protección adecuadas para cada nivel de clasificación.									
		Aplicar procedimientos para recolección, almacenamiento de archivos.									
Manejo y seguridad de la documentación interna		Archivar la documentación en ubicaciones seguras y accesibles solo para personal autorizado.							Gerente		
		Usar cifrado para la documentación electrónica sensible.									
		Realizar auditorías periódicas para asegurar la integridad y seguridad de la documentación.									
Registro histórico de actividades		Registrar automáticamente todas las actividades relevantes, incluyendo transacciones, cambios en el sistema y accesos a datos sensibles.							Ing. Sistemas de información		
		Auditar los registros históricos trimestralmente para asegurar la precisión y detectar posibles incidentes de seguridad.									

Elaborado por: Henriquez (2024)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En la fase de planificación se logra determinar un nivel de confianza alto y un nivel de riesgo bajo y moderado, lo que indica que los controles internos aplicados en los departamentos de TI y seguridad de la información permiten alcanzar las metas establecidas de manera óptima. Sin embargo, existe el componente de estrategias y objetivos que alcanzan un nivel de confianza menor al de los otros componentes por lo tanto los riesgos expuestos pueden limitar que los objetivos se cumplan en los tiempos establecidos en lo que tiene que ver el sistema de información de la cooperativa.

La cooperativa posee activos de información de gran importancia como son: Software, hardware y documentación interna sensible según su nivel de criticidad calificados como muy altos, así mismo su sistema de información se encuentra expuesto a posibles amenazas como fraude, fuga de información, suplantación de identidad del cliente. El jefe de seguridad trata de minimizar el riesgo, y responder de manera efectiva ante cualquier eventualidad, aun así, existe el riesgo de afectación a la integridad al momento de ingresar datos sobre los clientes en el sistema contable debido a la falta de autentificación de los mismos, provocando en ciertas ocasiones errores en su sistema.

En el marco de referencia COBIT 5, todos los procesos llegan a un nivel predecible y optimizado; exceptuando un proceso que tiene un nivel establecido, lo cual es un logro significativo que indica una sólida gestión de la tecnología de la información y alineación con los objetivos del negocio. Aun así, hay actividades incompletas o básicas en algunos procesos permitiendo aplicar métricas en cuanto al desempeño, gobierno y gestión de las TI.

Se realiza la socialización de los resultados obtenidos a través del informe de auditoría definiendo que la gerencia y los jefes departamentales deben poner en práctica las políticas de seguridad y los controles tanto preventivos, como detectivos y correctivos para mejorar la eficiencia en la gestión de las TI, sistema de información, activos de información internos.

4.2 Recomendaciones

Se recomienda llevar a cabo una revisión exhaustiva de las estrategias y objetivos actuales, si es necesario fortalecer los controles internos específicos relacionados con la implementación de estrategias y objetivos identificando y evaluando riesgos específicos para desarrollar planes de mitigación y contingencia.

Establecer códigos de autenticación multifactor (MFA) para acceder a los sistemas críticos, realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades. Realizar una configuración de alertas automáticas para actividades inusuales que requieran investigación inmediata, además distribuir folletos periódicos con información actualizada sobre nuevas amenazas y consejos de seguridad a los usuarios de los activos de información.

Establecer un procedimiento de seguimiento y revisión periódica para supervisar el avance hacia el logro de las actividades asociadas a COBIT y una implementación de estrategias para el desarrollo óptimo de actividades según el grado de importancia para cumplimiento de los objetivos, ya que cumplen con las actividades, pero no establecen plazos claros.

Para garantizar la eficacia y la coherencia en la implementación de políticas de seguridad sugeridas, se recomienda utilizar la matriz de seguimiento y monitoreo de políticas de seguridad. Esta herramienta ofrece una estructura organizada para evaluar y supervisar cómo se aplican las políticas, identificando áreas que necesitan mejoras, mitigando riesgos y garantizando el cumplimiento de las regulaciones y normativas. Al emplear esta matriz, la cooperativa en especial los departamentos de tecnologías y seguridad de la información puede tener un control minucioso del estado de sus

políticas de seguridad, lo que les permite actuar proactivamente ante posibles amenazas y vulnerabilidades.

REFERENCIAS BIBLIOGRÁFICAS

Abrego Almazán, D., Sánchez Tovar, Y., & Medina Quintero, J. M. (2017). Influencia de los sistemas de información en los resultados organizacionales. *Contaduria y Administracion*, *62*(2), 321–338. https://doi.org/http://dx.doi.org/10.1016/j.cya.2016.07.005

Albarracín, L. O., Marín, C. M., Lozada, J. C., & Martínez, J. P. (2021). Auditoría informática dentro de la empresa "Promalec"de la ciudad de Quevedo, en tiempo de COVID-19. *Universidad y Sociedad*, *13*(5), 345–354.

Amezcua Luján, M. K., & Santoyo Telles, F. (2021). Modelo de fiscalización electrónica. *Retos de La Dirección*, *15*(2), 8–107. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2306-91552021000200081&lng=en&tlng=en

Arbeláez, M. (2014). Las tecnologías de la información y la comunicación (TIC) un instrumento para la investigación. *Investigaciones Andina*, *16*(29), 997–1000. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81462014000200001

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de Las Ciencias*, *3*(3), 157–173. https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Auditool. (2024). *Herramientas para la Implementación de COSO ERM*. https://www.auditool.org/herramientas/coso-erm/herramientas-para-la-implementacion-de-coso-erm

Baena, G., Mendoza, R., & Coronado, J. (2019). Importancia de la Norma ISO/IEC 27000 en la implementación de un sistema de gestión de la seguridad de la información. *Dialnet*, 2–12. https://dialnet.unirioja.es/descarga/articulo/8990740.pdf

Bailon Lourido, W. A. (2019). Auditoría informática al control y mantenimiento de una infraestructura tecnológica. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, *5*(1), 73–87. https://doi.org/10.35381/cm.v5i1.248

Beltrán, L. (2018). Reglamento General De Adaptación De La Normativa Española : El Proyecto De Lopd. *Ponencias*, *28*, 74–96.

Bertalanffy, L. Von. (1989). Teoría general de los sistemas. In *Teoría general de los sistemas: fundamentos, desarrollo, aplicaciones* (Issue 65). https://archivosociologico.files.wordpress.com/2010/08/teoria-general-de-los-sistemas-ludwig-von-bertalanffy.pdf

Biler, S. (2017). Auditoría. Elementos esenciales. *Revista de Dominio de Las Ciencias*, *3*, 138–151. https://dialnet.unirioja.es/servlet/articulo?codigo=5907383

Bombón, V. (2024). *Ing. en sistemas de la información*.

Castello, R. J. (2017). Auditoría en entornos informáticos. In *Journal of Science and Research: Revista Ciencia e Investigación* (Vol. 3, Issue 2). https://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=552&Itemid=19

Colina, A. M., & Túa, J. J. (2020). Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI. *INNOVA Research Journal*, *5*(3.2), 196–213. https://doi.org/https://doi.org/10.33890/innova.v5.n3.2.2020.1608

Contraloría General del Estado. (2023). *Acuerdo No. 004-CG- 2023*. 1–93. file:///C:/Users/-PC-/Desktop/Acuerdo_004-CG-2023__Normas_de_Control_Interno.pdf

Cooperativa de Ahorro y Crédito Kullki Wasi Ltda. (2024). *Página Web*. https://www.kullkiwasi.com.ec/#/home

Díaz Varela, G. A. (2020). La auditoría a los sistemas de información como aporte a la actividad gerencial. *Universidad Latinoamericana y Del Caribe (ULAC)*, *5*(3), 180–212. https://biblat.unam.mx/es/revista/gestion-id/articulo/la-auditoria-a-los-sistemas-de-informacion-como-aporte-a-la-actividad-gerencial

Google Maps. (2024). *Mapa Ambato*. https://www.google.com.ec/maps/place/Cooperativa+de+Ahorro+y+Crédito+Kullki+Wasi+Ltda./@-1.2424342,-78.6291895,17z/data=!3m1!4b1!4m6!3m5!1s0x91d381bc4d839b5f:0x9aab8195a91434fc!8m2!3d-1.2424342!4d-78.6266146!16s%2Fg%2F11btrrsvdc?hl=es

Herrera, M. (2017). *Normas Internacionales de Auditoria*. http://docs.bvsalud.org/biblioref/2019/10/47933/art-7.pdf

ISACA. (2012). COBIT 5. In *Un Marco de Negocio para el Gobierno y la Gestión*

de las TI de la Empresa (Vol. 147, Issue 17).

ISO/IEC 15504. (2024). *EL estándar internacional ISO/IEC 15504*. https://www.normas-iso.com/iso-iec-15504-spice/

ISO 27000. (2024). *SGSI*. https://www.iso27000.es/sgsi.html

Llumiguano Poma, M. E., Gavilánez Cárdenas, C. V., & Chávez Chimbo, G. W. (2021). Importancia de la auditoría de gestión como herramienta de mejora continua en las empresas. *Revista Dilemas Contemporáneos: Educación, Política y Valores*, *March*, 1–19. http://www.dilemascontemporaneoseducacionpoliticayvalores.com/

Manrique, J. M. (2019). *Introducción a la auditoría*. https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/14790/INTRODUCCION A LA AUDITORIA (1).pdf?sequence=3

Martínez, A. Y., Blanco, B., & Loy Marichal, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista De Arquitectura E Inginieria*, *6*(15), 1–14. http://www.redalyc.org/articulo.oa?id=193924743004

Montilla, O. de J., & Herrera, L. G. (2006). El deber ser de la auditoría. *Estudios Gerenciales*, *98*, 83–110. http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=22465961&lang=es&site=ehost-live

Muñoz, C. (2002). *Auditoría en sistemas computacionales* (G. Trujano Mnedoza (ed.); Practice H).

Organización Internacional de Normalización. (2008). ISO 27000. *ISO27000*.

Pérez, M. D. (2018). Procedimiento para el diseño de Sistemas de Gestión de Información en Cooperativas de Producción. *Cooperativismo y Desarrollo*, *6*(1), 26–40. http://coodes.upr.edu.cu/index.php/coodes/article/view/185

Reyes, A. C., Montilla, A., Castillo, P., & Zambrano, M. (2017). Amenaza, vulnerabilidad y riesgo ante eventos naturales. Factores socialmente construidos. *Revista Ciencia e Investigación*, *2*(6), 22–28. https://dialnet.unirioja.es/descarga/articulo/6118736.pdf

Rocha, C. (2011). La Seguridad Informática. *Ciencia Unemi*, *4*(5), 26–33. https://www.redalyc.org/articulo.oa?id=582663867004%0ACómo

Salgado, M. del C., Osuna, N. del C., Sevilla, M., & Morales, J. I. (2017). La Auditoría Informática en las organizaciones. *Revista Electrónica Sobre Cuerpos*

Académicos y Grupos de Investigación En Iberoamérica., *4*(8), 1–14. https://www.cagi.org.mx/index.php/CAGI/article/view/165/324

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado*, *17 (78)*, 343–351. http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Sánchez Duarte, E. (2008). Las tecnologías de la información y comunicación (TIC) desde una perspectiva social. *Educare*, 155–162. https://doi.org/10.5325/jmodeperistud.5.1.0001

Sánchez, L. R. (2016). COSO ERM y la gestión de riesgos. *Quipukamayoc*, *23*(44), 43–50. https://doi.org/https://doi.org/10.15381/quipu.v23i44.11625

Sepúlveda, J., Lago, C., Rasete, A., Sepúlveda, R., & Lorenzo, J. (2008). Sistema de Información para análisis y procesamiento de datos de los computadores a bordo de la serie AGM-200X. *Revista Cubana de Ciencias Informáticas*, *2*, 11–19. http://www.redalyc.org/articulo.oa?id=378343635002

Superintendencia de Economía Popular y Solidaria. (2024). *Segmentación de entidades del SFPS, año 2023*. https://www.seps.gob.ec/institucion/segmentacion-de-esfps/

Tejeda, M. E. (2020). Auditoría a los sistemas como herramienta para examinar los procesos en las empresas. *Frecosapiens*, *3*. http://portal.amelica.org/ameli/jatsRepo/221/2211077005/index.html

Téllez, O., Ramírez, M., & Díaz, A. (2016). Auditoría de Sistema de TI como medio de aseguramiento de control en las empresas del Siglo XXI. *RECI Revista Iberoamericana de Las Ciencias Computacionales e Informática*, *5*(10). https://doi.org/10.23913/reci.v5i10.54

Vecino P, H. (2017). Normas ISO y marcos de referencia para gobernanza de las TIC. Revision general. *Revista Colombiana de Computación*, *18*(1), 70–81. https://doi.org/10.29375/25392115.3199

Villardefrancos, M. del C., & Rivera, Z. (2006). La Auditoria como proceso de control: concepto y tipologia. *Ciencias de La Informacion*, *37*, 53–59.

Yánez, J., & Yánez, R. (2012). Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. *Ingeniería Industrial. Actualidad y Nuevas Tendencias*, *III*(9), 83–92. https://www.redalyc.org/pdf/816/81606112.pdf%0Ahttp://www.redalyc.org/arti

culo.oa?id=81606112%0Ahttps://www.redalyc.org/html/2150/215026158006/

Zambrano, G. M., Álvarez, D. E., & Yoza, N. R. (2021). La importancia de la auditoria de gestión y los procesos administrativos y técnicos, realidades y perspectivas. *UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166*, *5*(3), 127–140. https://doi.org/10.47230/unesum-ciencias.v5.n3.2021.568

Zhañay, O. A., Erazo, J. C., & Narváez, C. I. (2019). Modelo de auditoría de sistemas de información para las cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, *5*(1), 361–393. https://doi.org/10.35381/cm.v5i1.271

ANEXOS

Anexo 1. Entrevistas

Entrevista 1

Entrevistado: Mgs. Juan Andagana

Cargo: Gerente

1. **¿La cooperativa dispone de un código de ética?**

Si, para la elaboración del código se tomó en cuenta al parámetro de la resolución 2021-019 Buen gobierno.

2. **Si la respuesta fue afirmativa a la pregunta anterior comente si el código ha sido socializado entre sus empleados**

Si, y su última socialización fue en abril del 2022.

3. **¿La cooperativa cuenta con estrategias y metas institucionales a corto o largo plazo?**

A corto y largo plazo.

4. **¿La cooperativa tiene definido políticas internas por departamento?**

Si cada departamento tiene sus manuales con políticas internas.

5. **¿La cooperativa tiene un plan estratégico institucional o por departamentos?**

Plan estratégico institucional.

6. **¿La cooperativa evalúa el FODA institucional y con qué frecuencia lo realiza?**

Si, se lo realiza mensualmente.

7. **¿La cooperativa realiza evaluación de la eficiencia, eficacia, economía a través de indicadores?**

Si, se mide con relación a las metas institucionales.

8. **¿Para el registro de sus transacciones operativas, la cooperativa utiliza un Software Contable? Señale el nombre de este.**

Softbank.

9. **¿Se mantienen reuniones frecuentes con el departamento de TI para evaluar las posibles amenazas, vulnerabilidad y riesgos a los que está expuesto la información de la cooperativa?**

Si, cada semana se monitorea y se analiza.

10. **¿La gerencia tienen conocimiento completo sobre el plan de seguridad de la información que manejan los departamentos a cargo del gobierno y gestión de las TI?**

Si se tiene conocimiento.

11. **¿La gerencia se ha involucrado en aportar acciones para el plan de contingencia sobre riesgos informáticos?**

Si, la cooperativa tiene el comité gerencial y el comité revisor de documentos y todos los planes y estrategias son validados por la gerencia general la misma que aporta acciones para el plan de contingencia sobre los riesgos informáticos.

Entrevista 2

Entrevistado: Víctor Bombón

Cargo: Ing. en sistemas

1. **¿Se ha realizado anteriormente auditorías de sistemas en la cooperativa?**

No se han realizado este tipo de auditorías, la SEPS solo han realizado auditorías generales

2. **¿El departamento tiene definido planes de contingencia contra riesgos informáticos?**

Si, la cooperativa tiene definido planes de contingencia, pero están de actualizar.

3. **¿Tienen identificados los activos de información por departamentos?**

Si, cada activo de información está identificado.

4. **¿Realizan evaluaciones periódicas a los activos de información?**

No, solo empíricamente.

5. **¿Cada qué tiempo evalúan los activos de información?**

La cooperativa tiene un mantenimiento preventivo 2 veces al año.

6. **¿Cuáles son los activos de información más relevantes o críticos que se han identificado en el área tecnológica?**

Principalmente la base de datos, el repositorio synology y las PC.

7. **¿Cuáles son las vulnerabilidades, amenazas y riesgos del área de sistemas?**

Tienen definido en el manual las siguientes amenazas: fallas eléctricas, incendio de instalaciones, actos mal intencionados, terrorismo, sabotaje, cierre parcial de instalaciones, desastres naturales, oposición por políticas y procedimientos y pandemia.

8. **¿Evalúan las amenazas, vulnerabilidades y riesgos del sistema de información?**

Si son evaluadas.

9. **¿Tienen definidos controles ante las amenazas que están expuestos los activos de información más importantes?**

Si, por cada amenaza tienen controles establecidos, como actuar y las soluciones.

10. **¿Existen políticas específicas para la gestión de activos de información en la cooperativa? ¿Cuáles son?**

Procesos de monitoreo de activos de información.

11. **¿Cuáles son los medios de almacenamiento para los backups de las bases de datos de las herramientas informáticas que utiliza la cooperativa?**

Discos.

12. **¿Existe el cumplimiento de políticas y procedimientos establecidos para los sistemas de información?**

Si, pero a veces no cumplen con las fechas.

13. **¿Realizan un seguimiento continuo a las políticas y procedimientos establecidos?**

Si realizan un seguimiento tanto a políticas como procedimientos.

14. **¿Realizan un seguimiento a los controles implementados en seguridad de la información?**

Si se realiza un seguimiento a todos los controles implantados.

15. **¿Evalúan niveles de madurez tanto en los riesgos como en la gestión y gobierno de las TI? ¿Qué procesos han evaluado?**

La cooperativa no tiene implantado COBIT.

Anexo 2. Listas de verificación

Lista de verificación 1.

Preguntas	SI	NO	Observación
1. ¿La instalación de la red local es flexible y adaptable a las necesidades departamentales para la conexión de los equipos informáticos de la cooperativa?	X		
2. ¿Las direcciones IP's configuradas en la red permite dar seguimiento de las conexiones entrantes para su funcionamiento?	X		
3. ¿Existen niveles de acceso y seguridad en la red? ¿Cuáles son?	X		Son políticas de seguridad implementadas directamente en el firewall.
4. ¿Evalúan las medidas preventivas o correctivas en caso de siniestros en el sistema contable?	X		
5. ¿Realizan respaldos o backups de la base de datos? ¿Con qué frecuencia?	X		Diaria
6. ¿Se verifica la vigencia de antivirus? ¿Con qué frecuencia?	X		El administrador de antivirus se encargade verificar diariamente.
7. ¿Tienen controles en los procesos operativos? ¿Qué tipos de controles?	X		Firewall de seguridad perimetral.
8. ¿Manejan bitácoras de las revisiones que se hacen a los sistemas de información?	X		
9. ¿Tienen políticas de seguridad para el acceso a las instalaciones?	X		
10. ¿Cuentan con la señalética de emergencia y acceso a las instalaciones?	X		
11. ¿Tienen instaladas camaras de seguridad en las áreas operativas de la cooperativa?	X		
12. ¿Cumplen con los parámetros establecidos en la normativa ISO 27000?	X		Cumplen con la normativa, pero no están certificados en ISO 27000.

Lista de verificación 2

	NIVELES DE MADUREZ			
	Descripción de los procesos	**SI**	**NO**	**Observación (¿por qué no se evalúa?)**
1	**EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**			
	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.		X	Se tiene definido requerimientos para el gobierno de TI de la cooperativa
2	**EDM02 Asegurar la Entrega de Beneficios**			
	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.		X	Se realiza de manera continua procesos de negocio y mejora de los servicios de TI
3	**EDM03 Asegurar la Optimización del Riesgo**			
	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	X		
4	**EDM04 Asegurar la Optimización de Recursos**			
	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	X		
5	**EDM05 Asegurar la Transparencia hacia las Partes Interesadas**			
	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.		X	Se elabora informes en cuanto a conformidad y desempeño de TI transparentes
6	**APO01 Gestionar el Marco de Gestión de TI**			
	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores		X	Se tiene definido lo competente de misión y visión corporativa de TI.
7	**APO02 Gestionar la Estrategia**			
	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	X		
8	**APO03 Gestionar la Arquitectura Empresarial**			
	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes.		X	Se tiene definido y establecido procesos de negocio lo competente con la arquitectura y se realiza un seguimiento continuo

9	**APO04 Gestionar la Innovación**			
	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.	X		
10	**APO05 Gestionar el Portafolio**			
	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.		X	Se ejecuta frecuentemente estas direcciones estratégicas.
11	**APO06 Gestionar el Presupuesto y los Costes**			
	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.		X	Se gestiona frecuente y eficientemente las actividades financieras relacionadas con TI.
12	**APO07 Gestionar los Recursos Humanos**			
	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	X		
13	**AP008 Gestionar las relaciones**			
	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves		X	Se gestiona eficientemente relaciones de negocio y TI.

14	**AP009 Gestionar los acuerdos de servicio**			
	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento	X		
15	**APO10 Gestionar los Proveedores**			
	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.		X	Se administra de manera adecuada todo servicio prestado por proveedores.
16	**APO11 Gestionar la Calidad**			
	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia	X		
17	**APO12 Gestionar el Riesgo**			
	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	X		
18	**APO13 Gestionar la Seguridad**			
	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	X		
19	**BAI01 Gestión de Programas y Proyectos**			
	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.		X	Se gestiona frecuentemente programas y proyectos competentes al portafolio de inversiones
20	**BAI02 Gestionar la Definición de Requisitos**			
	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	X		
21	**BAI03 Gestionar la Identificación y Construcción de Soluciones**			
	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.		X	Se mantiene soluciones identificadas en línea con los requerimientos de la cooperativa

22	**BAI04 Gestionar la Disponibilidad y la Capacidad**			
	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.		X	Se tiene un equilibrio de necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes
23	**BAI05 Gestionar la Facilitación del Cambio Organizativo**			
	Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas del negocio y de TI.		X	Se gestiona eficientemente la facilitación del cambio organizativo
24	**BAI06 Gestionar los Cambios**			
	Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.		X	Se gestiona cambios de una forma controlada, en relación con los procesos de negocio
25	**BAI07 Gestionar la Aceptación del Cambio y la Transición**			
	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.		X	Se gestiona frecuentemente la aceptación del cambio y la transición de lo competente a TI
26	**BAI08 Gestionar el Conocimiento**			
	Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.		X	Se gestiona correctamente el conocimiento para el soporte a todas las actividades y procesos
27	**BAI09 Gestionar los Activos**			
	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia.	X		

28	**BAI10 Gestionar la Configuración**			
	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración		X	Se gestiona correctamente lo competente a la configuración
29	**DSS01 Gestionar Operaciones**			
	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	X		
30	**DSS02 Gestionar Peticiones e Incidentes de Servicio**			
	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.		X	Se gestiona eficientemente peticiones e incidentes de servicio
31	**DSS03 Gestionar Problemas**			
	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.		X	Se tiene una buena gestión de problemas
32	**DSS04 Gestionar la Continuidad**			
	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	X		
33	**DSS05 Gestionar Servicios de Seguridad**			
	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	X		
34	**DSS06 Gestionar Controles de Proceso de Negocio**			
	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.		X	Se gestiona correctamente los controles de procesos de negocio
35	**MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad**			
	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.		X	Se evalúa constantemente métricas y objetivos de negocio, de TI y de los procesos

36	**MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno**			
	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.	X		
37	**MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.**			
	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.		X	Se evalúa frecuentemente el cumplimiento de requisitos regulatorios y contractuales tanto en procesos de TI como en procesos de negocio

Anexo 3. Cuestionario COSO ERM

No.	DESCRIPCIÓN	RESPUESTA	
		SI	NO
A	**SUBCOMPONENTE: Gobierno y cultura**		
1	¿Existen políticas que incluyan controles de TI?	x	
2	¿Se han definido, asignado y aceptado las responsabilidades de TI y de controles de TI?	x	
3	¿Se conserva la evidencia (pistas de auditoría o de gestión)?	x	
4	¿Asigna o define los requisitos obligatorios relacionados con la estructura operativa de la empresa?	x	
5	¿Crea oportunidades de colaboración a través de toda la empresa?	x	
6	¿Contempla las oportunidades para incorporarlas a la empresa?	x	
7	¿Define los responsables para los riesgos relacionados con la empresa?	x	
8	¿Introduce capacidades, destrezas y conocimiento relacionados con los riesgos tecnológicos?	x	
9	¿Demuestra comprimiso con los valores èticos ?	x	
B	**SUBCOMPONENTE: Estrategias y Objetivos**		
1	¿Se dispone de especialistas con competencias en auditoría de TI (sea interna o externamente)?	x	
2	¿Tiene en cuenta los riesgos relacionados a los factores internos y externos a los que se encuentra expuesta la empresa?	x	
3	¿Analiza las debilidades, amenazas, fortalezas y oportunidades en la empresa?		x
4	¿Evalúa la materialidad de las amenazas y el riesgo al que se encuentra expuesta la empresa?		x
5	¿Analiza el uso de los recursos específicos con los que cuenta la empresa frente a los riesgos?	x	
C	**COMPONENTE: Desempeño**		
1	¿Se han asegurado lógica y físicamente los equipos y herramientas de la infraestructura de TI?	x	
2	¿Se ha implementado una tecnología de filtros de seguridad conforme a la política de la empresa (por ejemplo, en lo lugares de conexiones externas, como Internet, y en los lugares donde se necesita una separación entre redes internas)?	x	
3	¿Es efectivo el conjunto de controles preventivos, de detección y correctivos?		x
4	¿El control provee evidencia cuando los parámetros de control son rebasados o cuando fallan?		x
5	¿Examina los riesgos de la entidad para determinar la prioridad de los mismos?	x	
6	¿Entiende los criterios de la entidad para priorizar los riesgos?	x	
7	¿Selecciona los métodos apropiados de evaluación para medir la gravedad del riesgo?	x	
8	¿Selecciona, y documenta los datos, parámetros y premisas?		x

D	**COMPONENTE: Revisión**		
1	¿Se usan mecanismos de control para el acceso y la autenticación?	x	
2	¿Se ha implementado un software antivirus y se realiza su mantenimiento?	x	
3	¿Se han completado evaluaciones de vulnerabilidades, se han identificado los riesgos y todo se ha resuelto adecuadamente?	x	
4	¿Identifica y evalúa los cambios internos y externos que pueden afectar sustancialmente a la estrategia u objetivos del negocio?	x	
5	¿Revisa las actividades de la ERM para identificar la necesidad de las revisiones a los procesos y las capacidades?	x	
6	¿Realiza revisiones periódicas a las posibles amenazas y riesgos a los que se encuentra expuesta la empresa?	x	
7	¿Evalúa los cambios sustanciales en la empresa ante la materialización de una amenaza?	x	
8	¿La empresa ha implementado revisiones sorpresivas a los procesos internos operativos para prevenir algún tipo de riesgo?	x	
E	**COMPONENTE: Información, comunicación y reporte**		
1	¿Identifica información relevante y canales para la comunicación y divulgación interna y externa?	x	
2	¿Comunica internamente información relevante entorno a los riesgos relacionados con la empresa?	x	
3	¿Identifica continuamente oportunidades para mejorar la calidad de datos relacionados con el sistema de información de la empresa?		x
4	¿Comunica oportunamente la detección de nuevas amenazas para la empresa?	x	
5	¿Reporta sobre riesgos, cultura y desempeño de la empresa?		x
6	¿Comunica sobre los riesgos de la información?	x	
7	¿Aprovecha el uso de la tecnología para informar nuevos hallazgos en cuanto a riesgos empresariales?	x	
F	**COMPONENTE: Sistemas de seguridad de información**		
1	¿Permiten las copias de seguridad resolver en un plazo satisfactorio las pérdidas de información o fallos a causa de la materialización de las amenazas?	x	
2	¿Se llevan las copias de seguridad a dispositivos externos o en la nube?	x	
3	¿Está protegido el acceso físico a las instalaciones informáticas ?	x	
4	¿Están protegidas las instalaciones informáticas contra fallos en el fluido eléctrico, incendios, desastres naturales, etc.?	x	
5	¿Se controla regularmente la integridad de las bases y la coherencia de los datos?	x	
6	¿Existe un control permanente en los accesos a la red local?	x	
7	¿La empresa cuenta con las licencias de uso correspondientes a los productos de software vigentes en sus PC?	x	
8	¿Existe auditoría interna para los servicios informáticos?	x	
9	¿La empresa tiene a disponibilidad un plan de seguridad de la información?	x	
10	¿Utilizan herramientas establecidas e identificadas para evaluar la seguridad de la información?	x	
11	¿Utiliza la empresa alguna metodología de evaluación de riesgos en cuanto a la seguridad de la información?	x	
12	¿La empresa ha sido víctima de algún ataque cibernético?	x	
13	¿La empresa aplica la Norma ISO/ITEC de buenas prácticas en cuanto al SGSI?	x	
14	¿La empresa aplica controles preventivos en cuanto a antivirus, firewall, password de usuarios y otros que ayuden a salvaguardar la información?	x	
15	¿La empresa se encuentra preparada ante los avances tecnológicos, digitalización, interconectividad, e intercambio de información de manera segura?	x	
16	¿Mantiene un control interno en temas de infiltración de empleados para sacar provecho de la información confidencial de la empresa?	x	
17	¿Algún colaborador interno de la empresa ha hecho mal uso de la información con fines de soborno o fraude?	x	
18	¿Se ha detectado inconsistencia en la información reportada por las herramientas informáticas que utiliza la empresa?	x	

Anexo 4. Hoja de hallazgos

N. Hallazgo	REF. P/T	CONDICIÓN Lo que sucedió	CRITERIO (Disposición Legal - Norma contable - Norma de Control Interno)	CAUSA (por que sucedió la condición)	EFECTO (resultado de la condición) cuantificado	RECOMENDACIÓN (debe dar respuesta a a la causa)
EVALUACIÒN DEL CONTROL INTERNO ERM						
1	**EVALUACIÓN DEL CONTROL INTERNO COSO ERM 2017 - ESTRATEGIAS Y OBJETIVOS**	No se realiza un análisis del foda institucional (fortalezas y oportunidades, debilidades,amenazas)	**Contexto de la Organización (Cláusula 4 de ISO/IEC 27001):** **4.1 Comprensión de la organización y su contexto:** Colabora en la identificación de los puntos fuertes y débiles internos, así como las posibles amenazas y oportunidades externas que podrían impactar la seguridad de la información. **4.2 Comprensión de las necesidades y expectativas de las partes interesadas:** Encuentra las oportunidades para cumplir de manera más eficiente con las expectativas de los involucrados y fortalece la relación con ellos. Evaluación de Riesgos de Seguridad de la Información **(Cláusula 6.1 de ISO/IEC 27001):** **6.1.2 Evaluación de riesgos de seguridad de la información:** Implica la detección de amenazas externas y debilidades internas que puedan tener un impacto en la seguridad de los datos. Principios de Gestión del Riesgo	Los líderes o empleados de la cooperativa desconocen la importancia de llevar a cabo esta metodología	Limitaciones sobre su posición en el mercado y los factores internos y externos que impactan su desempeño.	**Dirigido al gerente:** Realizar un análisis FODA de manera inmediata lo que permitirá que sea considerado un elemento importante y clave en la gestión de la cooperativa para la toma de decisiones.
2	**EVALUACIÒN DEL CONTROL INTERNO COSO ERM 2017 - DESEMPEÑO**	El control de seguridad actualmente evidencia un nivel de confianza y riesgo moderado debido a que las revisiones que aplican registran medianamente los parámetros de control cuando son rebasados o fallan.	**ISO/IEC 27001:2013 - Cláusula 9.1: Seguimiento, Medición, Análisis y Evaluació**n Esta cláusula establece que la organización debe evaluar el desempeño y la eficacia del sistema de gestión de seguridad de la información (SGSI). **Incluye:** **Determinación de lo que se debe monitorear y medir:** Esto implica identificar los controles clave y establecer parámetros para su rendimiento. Métodos de seguimiento, medición, análisis y evaluación: Establecer los métodos y frecuencia para llevar a cabo la supervisión y evaluación, determinando las técnicas que serán empleadas. rotección no cumplen su función. **ISO 31000:2018 - Cláusula 6.6: Seguimiento y Revisión** Esta cláusula establece la necesidad de vigilar y evaluar los riesgos.	Falta de planificación adecuada para la gestión de la calidad y los controles asociados, debido a que existe retraso en el registro, almacenamiento y análisis de datos.	Pérdida de datos, registros incompletos o inaccesibles y planes de calidad incompletos lo que puede contemplar riesgos y controles innecesarios.	**Dirigido al ingeniero de sistemas:** Establecer un sistema robusto de gestión de datos que asegure el registro, almacenamiento y análisis adecuados de los datos de control. Definir los parámetros aceptables para el acceso a datos sensibles, como el número de intentos fallidos de inicio de sesión. Desarrollar y mantener actualizado un plan de calidad detallado que incluya todas las actividades de control necesarias para asegurar la conformidad con los parámetros establecidos.

3	**EVALUACIÒN DEL CONTROL INTERNO COSO ERM 2017 - DESEMPEÑO**	Existe condiciones al seleccionar, y documentar los datos, parámetros y premisas.	**ISO/IEC 27001:2013 - Cláusula 6: Planificación 6.1.2 Evaluación de riesgos de seguridad de la información:** Es responsabilidad de la organización establecer y implementar criterios para evaluar las amenazas a la seguridad de la información, así como también establecer criterios para determinar cuándo es aceptable asumir dichos riesgos. Además, es importante que se asegure de mantener estos criterios actualizados. Para realizar la evaluación de riesgos, es necesario elegir y registrar los datos y parámetros pertinentes.. **ISO 31000:2018 - Cláusula 6: Proceso de gestión del riesgo 6.6 Seguimiento y revisión:** Mantener la documentación actualizada y revisada regularmente es imprescindible para garantizar su pertinencia a medida que cambien las circunstancias y evolucionen los riesgos.	Existen procedimientos que no se encuentran establecidos de manera clara y estandarizados para la selección y documentación de datos y parámetros	Tomar ciertas decisiones no acertadas, lo que puede llevar a acciones incorrectas o ineficientes.	**Dirigido al gerente:** Creación de manuales, guías o políticas documentadas que describan los procesos de selección y documentación. Establecer un proceso continuo de monitoreo y revisión, donde se asegure que todos los documentos relevantes se mantengan actualizados y reflejen cualquier cambio en los parámetros o premisas. Asignar responsabilidades claras a los empleados para garantizar que los procesos se lleven a cabo de manera consistente y efectiva.
4	**EVALUACIÒN DEL CONTROL INTERNO COSO ERM 2017 - INFORMACIÓN, COMUNICACIÓN Y REPORTE**	No se identifica continuamente oportunidades para mejorar la calidad de datos relacionados con el sistema de información de la cooperativa.	**ISO/IEC 27001:2013 - Cláusula 10: Mejora 10.1 Mejora continua:** La organización debe trabajar constantemente para mejorar la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información (SGSI). Esto implica la búsqueda de posibilidades para mejorar todos los aspectos del SGSI, incluyendo tanto la calidad de los datos como su relación con los sistemas de información. **ISO 31000 (Gestión del Riesgo) ISO 31000:2018 - Cláusula 6: Proceso de gestión del riesgo 6.6 Seguimiento y revisión**: Es necesario mantener un monitoreo y revisión constante del proceso de gestión del riesgo para garantizar su eficacia y adecuación. Esto implica la constante evaluación de la calidad de los datos empleados en la identificación y análisis del riesgo.	Existe una privación de procesos formales para monitorear y evaluar la calidad de los datos de manera regular	Datos de baja calidad que pueden resultar en procesos operativos ineficientes y costosos, lo que afectaria la integridad de los mismos.	**Dirigido a la directora de procesos de calidad :**Implementar procesos formales para monitorear y evaluar regularmente la calidad de los datos, incluidas revisiones periódicas y análisis de datos. **Dirigido al gerente:** Realizar auditorías de calidad de datos trimestrales y revisiones continuas de los datos para identificar y corregir problemas. Asignar recursos adecuados, como tiempo, personal y presupuesto, para actividades de mejora de la calidad de datos. **Dirigido al jefe de seguridad de la información:** Medir la precisión de los datos, asegurándose de que reflejan correctamente la realidad. Realizar revisiones periódicas de los permisos de acceso y ajustar según sea necesario.

5	**EVALUACIÒN DEL CONTROL INTERNO COSO ERM 2017 - INFORMACIÓN, COMUNICACIÓN Y REPORTE**	Se reporta información seleccionada sobre riesgos, cultura y desempeño de la cooperativa.	**ISO/IEC 27001:2013 - Cláusula 7: Soporte** **7.4 Comunicación:** Para el sistema de gestión de la seguridad de la información (SGSI), es responsabilidad de la organización identificar y evaluar las necesidades tanto en comunicación interna como externa. Esto implica establecer qué información se va a compartir, cuándo se hará, quiénes serán los destinatarios y cómo se realizará dicha comunicación. Esto incluye la comunicación sobre riesgos, desempeño del SGSI y aspectos de la cultura de seguridad de la información. **ISO 31000:2018 - Cláusula 5: Marco de gestión del riesgo** **5.4 Integración:** Es esencial que la gestión del riesgo se incorpore de manera integral en la estructura organizativa, abarcando tanto la cultura empresarial como los procesos y políticas corporativas. Es importante que los informes reflejen la forma en que la gestión de riesgos está integrada	Existen procesos que no se han especificado de manera clara y estructurada para recopilar, analizar y reportar información relevante sobre riesgos, cultura y desempeño	Difícultad en la identificación de áreas de mejora y oportunidades para el crecimiento y la innovación.	**Dirigido a la directora de procesos de calidad:** Desarrollar procesos claros y estructurados para recopilar, analizar y reportar información relevante sobre riesgos, cultura y desempeño de la empresa y realizar revisiones periódicas del proceso de reporte buscando constantemente formas de mejorarlo y perfeccionarlo. **Dirigido al ingeniero en sistemas y directora de riesgos:** Emitir informes trimestrales a la alta dirección sobre el estado del SGSI, incluyendo riesgos, incidentes y acciones correctivas. Encuestas anuales de cultura de seguridad para evaluar la percepción y comportamiento de los empleados respecto a la gestión de riesgos.
6	**EVALUACIÒN DEL CONTROL INTERNO COSO ERM 2017 - SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN**	Ha existido en cierto tiempo el mal uso de la información con fines de soborno o fraude	**ISO/IEC 27001:2013** **Cláusula 6.1: Acciones para abordar riesgos y oportunidades** **6.1.2 Evaluación de riesgos de seguridad de la información:** La organización debe realizar evaluaciones de riesgo para identificar y tratar los riesgos, incluyendo los riesgos de fraude y mal uso de la información por parte de colaboradores internos. **Cláusula 9: Evaluación del desempeño** **9.1 Monitoreo, medición, análisis y evaluación:** Monitorear y evaluar los controles para asegurar que los riesgos de seguridad de la información, como el fraude interno, se están gestionando adecuadamente. **ISO 31000:2018 - Cláusula 6: Proceso de gestión del riesgo** **6.6 Seguimiento y revisión** Realizar monitoreo y revisar los controles de riesgo para asegurar así su eficacia continua y realizar mejoras cuando sea necesario.	Tiempo atrás existió falta de controles, ética y diligencia profesional	Pérdida directa de dinero y recursos debido a actividades fraudulentas así como afectación a la reputación institucional	**Gerente**: Realizar auditorías trimestrales para revisar el cumplimiento de las políticas de seguridad, así como el fortalecimiento de controles preventivos, detectivos y correctivos en la seguridad de la información **Ingeniero de sistemas:** Evaluar la probabilidad de que un colaborador interno cometa fraude utilizando estos datos.

EVALUACIÒN DEL NIVEL DE MADUREZ DE CONTROL INTERNO						
8	**EVALUACIÒN DEL NIVEL DE MADUREZ COSO ERM 2017 - ESTRATEGIAS Y OBJETIVOS**	En el nivel de madurez y eficiencia del sistema de control interno, el componente Estrategias y objetivos tiene una calificación media lo que indica que se encuentra en un nivel en proceso.	**COSO ERM 2017** **Estrategias y objetivos:** Se centra en establecer metas y objetivos alineados con la misión y visión de la organización, así como en garantizar que se identifiquen y gestionen los riesgos que podrían afectar la capacidad de la organización para alcanzar esos objetivos.	Los procesos deben ser efectivos para monitorear y revisar continuamente el cumplimiento de los objetivos estratégicos y las estrategias de la cooperativa, es posible que los problemas no se identifiquen ni se aborden a tiempo	La falta de alineación entre la gestión de riesgos y los objetivos estratégicos puede llevar a la cooperativa a no cumplir sus metas a largo plazo. Esto puede resultar en una pérdida de dirección y enfoque, así como en la incapacidad de capitalizar oportunidades importantes.	**Dirigido al gerente:** Fortalecer procesos efectivos para monitorización y revisar continuamente cumplimiento de objetivos estrategicos y estrategias
MATRIZ DE RIESGOS - GESTIÓN DE RIESGOS INFORMÁTICOS						
9	**MATRIZ DE RIESGOS - GESTIÓN DE RIESGOS INFORMÁTICOS**	Existe riesgo operativo, debido a vulnerabilidades detectadas en el software, personas, procesos y tecnologías de información.	**ISO 27001** **Control de Acceso (Anexo A.9):** **A.9.1.1 Política de control de acceso:** Define los requisitos de acceso a la información y los sistemas de información. El acceso controlado ayuda a prevenir cambios no autorizados que puedan causar desactualización. **Gestión de Incidentes de Seguridad de la Información (Anexo A.16):** **A.16.1.2 Notificación de eventos de seguridad:** Identificación y gestión de incidentes que puedan resultar de información desactualizada. **NORMA 410-09** **Mantenimiento y control de la infraestructura tecnológica** La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.	Existe limitados procedimientos definidos para la revisión y actualización periódica de la información debido a que se ha realizado el registro incorrecto de datos en algunas ocasiones.	Procesos interrumpidos o incorrectos pueden resultar en pérdida de tiempo y recursos, afectando la productividad y la desactualización de la base de datos lo que puede impedir que la cooperativa identifique y aproveche oportunidades de negocio y mejora.	**Dirigido al gerente:** Proveer capacitación continua a los empleados sobre la importancia de la calidad de los datos y los procedimientos para mantener la información actualizada, realizar auditorías regulares de la calidad de los datos para asegurar la precisión y actualidad de la información. **Dirigido al ingeniero de sistemas:** Establecer mecanismos de monitoreo continuo para detectar y corregir errores en los datos de manera oportuna.
10	**MATRIZ DE RIESGOS - GESTIÓN DE RIESGOS INFORMÁTICOS**	Ha existido envío de la información a personas que no pertenecen a la cooperativa	**ISO 27001** **Control de Acceso (Anexo A.9):** **A.9.1.1 Política de control de acceso:** Establece la necesidad de definir políticas de acceso claras para asegurar que solo las personas autorizadas tengan acceso a la información sensible. **ISO 31000** **Proceso de Gestión del Riesgo (Cláusula 6):** **6.4.2 Identificación del riesgo:** Identificación de riesgos específicos relacionados con el envío de información a personas no autorizadas. **NORMA 410-15 Capacitación informática** Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.	En la cooperativa existió personal con malas prácticas para en el manejo de la información	La información sensible llegó a usuarios no autorizados, comprometiendo la privacidad de los socios y la seguridad.	**Dirigido al gerente:** Proveer capacitación continua al personal sobre las mejores prácticas para el manejo de la información y la importancia de la confidencialidad.

MARCO DE REFERENCIA COBIT						
11	**EDM03**	En la práctica clave de gobierno EDM03.01 no se determina el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado:*** El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas. **EDM03.01 Evaluar la gestión de riesgos.** **Practica:** Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	Existe una desconexión entre los equipos de TI y los responsables de la gestión de riesgos empresariales debido a una comunicación ineficaz y las prioridades y objetivos de la gestión de riesgos de TI no están alineados con las prioridades estratégicas y objetivos de la cooperativa.	La gestión de riesgos de TI y la gestión de riesgos empresariales pueden tomar direcciones diferentes, resultando en inconsistencias y potenciales brechas de seguridad. La falta de alineación puede llevar a decisiones empresariales mal informadas que no consideran todos los riesgos pertinentes, afectando negativamente la resiliencia de la organización.	**Directora de riesgos:** Establecer procesos de monitoreo y revisión continua para asegurar que las estrategias de riesgos de TI y empresariales se mantengan alineadas y se adapten a los cambios en el entorno empresarial y tecnológico.
12		En la práctica clave de gobierno EDM03.02 no se promueve una cultura consciente de los riesgos TI e impulsar a la cooperativa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado:*** ***El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.*** **EDM03.02 Orientar la gestión de riesgos.** **Práctica:** Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	Los empleados y directivos no están suficientemente informados sobre los riesgos de TI y su impacto en el negocio debido a la falta de programas de capacitación y concienciación.	La incapacidad para identificar proactivamente oportunidades de mejora de TI limita la capacidad de la cooperativa para innovar y mantenerse competitiva en su mercado.	**Dirigido al gerente:** Reconocer y recompensar a los empleados que identifican proactivamente riesgos de TI y sugieren soluciones para mitigarlos, fomentando así una cultura de prevención. **Dirigido al ingeniero en sistemas:** Establecer canales claros y seguros para que los empleados reporten incidentes de seguridad y asegurarse de que se tomen las medidas adecuadas en respuesta. **Dirigido al jefe de seguridad de la información:** Presentar informes periódicos a la alta dirección sobre el estado de la seguridad de la información y cómo está protegiendo los activos y el negocio de la cooperativa.
13		En la práctica clave de gobierno EDM03.02 existe limitación en orientar a la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado:*** ***El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.*** . **EDM03.02 Orientar la gestión de riesgos.** **Práctica:** Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	Las políticas y procesos establecidos para integrar TI con la estrategia empresarial, deben ser alineados de manera más clara, además la falta de un marco de gobernanza que guíe la integración de TI y la estrategia empresarial	Provocar dificultad para innovar y adaptarse a cambios del mercado. Tomar decisiones incorrectas debido a que no se integre operacionesy estrategias de riesgos con decisiones empresariales	**Dirigido al gerente:** Establecer canales de comunicación claros y regulares entre TI y las unidades de negocio. Realizar un mapeo de los objetivos de TI con los objetivos estratégicos de la cooperativa. **Dirigido al ingeniero en sistemas:** Colaborar estrechamente con líderes empresariales para asegurarse de que las iniciativas de TI apoyen estos objetivos. Alinear los proyectos y prioridades de TI con las prioridades estratégicas de la cooperativa.

14	**APO02**	En la práctica clave de gestión APO02.03 la definición del objetivo de las capacidades de TI requiere alineación y acuerdo con los cambios en la arquitectura empresarial con el gobierno corporativo.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 1 - Ejecutado:*** El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas. **APO02.03 Definir el objetivo de las capacidades de TI.** **Práctica:** Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.	Las áreas operativas y los equipos de proyecto no comunican de manera oportuna sus iniciativas de cambio al arquitecto corporativo, los equipos no están conscientes del papel y la importancia del arquitecto corporativo en los cambios de arquitectura. Falta de una visión integral de la arquitectura empresarial, lo que provoca decisiones aisladas y descoordinadas y hay una inexistencia de un marco de gobernanza sólido que integre las decisiones de arquitectura a nivel corporativo	Incapacidad para responder rápidamente a cambios del mercado y oportunidades estratégicas.y retrasos en la implementación de proyectos debido a problemas no anticipados de integración y compatibilidad.	**Dirigido al gerente:** Crear canales de comunicación formales y regulares entre los equipos de proyecto y el arquitecto corporativo. Elaborar una visión integral de la arquitectura empresarial que sea compartida y entendida por todas las áreas. Formar un comité de arquitectura que incluya al arquitecto corporativo y representantes clave de diferentes áreas.
15		En la práctica clave de gestión APO13.01 no se define el alcance y los límites del SGSI en términos de las características de la cooperativa, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 1 - Ejecutado: El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas.*** **APO13.01 Establecer y mantener un SGSI.** **Práctica:**Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	Falta de una evaluación integral de riesgos que identifique todas las áreas críticas. Subestimación de las amenazas y vulnerabilidades a las que está expuesta la organización. Otras prioridades de negocio que desvían la atención y los recursos necesarios.	Aumento en la frecuencia y gravedad de incidentes de seguridad.	**Dirigido al gerente:** Programas de formación para todos los empleados sobre la importancia del SGSI y sus componentes. Incentivar certificaciones como ISO 27001 para el personal clave. **Dirigido al jefe de seguridad de la información:** Documentar y justificar cualquier exclusión del alcance, asegurando que no se comprometa la seguridad general. Establecer mecanismos de retroalimentación y mejora continua para el SGSI.
16		En la práctica clave de gestión APO13.01 existe limitaciones en la definición del SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 1 - Ejecutado: El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas.*** **APO13.01 Establecer y mantener un SGSI.** **Práctica:**Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	No se reconocen todas las amenazas y vulnerabilidades a las que está expuesta la organización. Falta de familiaridad con normas y estándares como ISO 27001.	Fallos en sistemas críticos y activos de información que pueden afectar la continuidad del negocio.	**Dirigido al gerente:** Realizar auditorías periódicas y revisiones del SGSI para asegurar su efectividad y conformidad. **Dirigido al jefe de seguridad de información:** Revisar y actualizar el alcance del SGSI según sea necesario para reflejar cambios en la organización, tecnología o entorno de amenazas.

18	**APO13**	En la práctica clave de gestión APO13.02 no se proporciona información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado: El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.*** **APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.** **Práctica:** Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa.	Fallos en la comunicación entre los equipos de seguridad y otros departamentos. Ausencia de procesos estandarizados para el diseño y desarrollo de prácticas de gestión de riesgos.	Falta de planificación adecuada para la obtención de controles y desarrollo de prácticas de gestión.	**Dirigido a la directora de riesgos:** Diseñar y desarrollar prácticas de gestión basadas en la información proporcionada por el plan de tratamiento de riesgos. **Dirigido al jefe de seguridad de la información:** Establecer mecanismos para recolectar y analizar la retroalimentación de los equipos sobre la implementación del plan de tratamiento de riesgos.
19		En la práctica clave de gestión APO13.03 no se realizan auditorías internas al SGSI a intervalos planificados.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 1 - Ejecutado: El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas.*** **APO13.03 Supervisar y revisar el SGSI.** **Práctica:** Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua. **Actividad 2:** Realizar auditorías internas al SGSI a intervalos planificados.	Falta de un calendario de auditorías bien definido y planificado. Falta de conformidad con estándares y regulaciones como ISO 27001.	Fallos en sistemas críticos que afectan la continuidad del negocio.	**Dirigido al gerente:** Implementar programas de formación continua sobre la importancia y los procedimientos de auditoría interna. Fomentar la obtención de certificaciones relevantes y la participación en talleres de auditoría interna. Crear un calendario detallado para realizar auditorías internas en intervalos planificados. Revisar y ajustar el calendario según sea necesario para asegurar que se cumplan los plazos. Asegurar el compromiso de la alta dirección para apoyar y priorizar las auditorías internas.
20		En la práctica clave de gestión APO13.03 no se realizan revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 1 - Ejecutado: El proceso logra más o menos sus propósitos a través de la aplicación de un conjunto de actividades incompletas que puede caracterizarse como iniciales o intuitivas no muy organizadas.*** **APO13.03 Supervisar y revisar el SGSI.** **Práctica:** Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua. **Actividad 3:** Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	Ausencia de procedimientos establecidos para la revisión del SGSI. Falta de planificación y programación de las revisiones periódicas. No se realiza un seguimiento adecuado de las revisiones anteriores y las acciones correctivas.	Controles de seguridad que pueden no ser efectivos ante nuevas amenazas. Recursos desperdiciados debido a la falta de revisiones adecuadas y actualizaciones necesarias.	**Dirigido al gerente:** Realizar sesiones de sensibilización y capacitación para la alta dirección sobre la importancia de las revisiones del SGSI. Crear y documentar procedimientos claros para la revisión periódica del SGSI. Integrar las revisiones del SGSI en el calendario de la alta dirección. Desarrollar y seguir planes de acción correctiva para abordar los problemas identificados durante las revisiones. **Dirigido al jefe de seguridad de la información:** Proponer reuniones trimestrales o semestrales para revisar el estado del SGSI y discutir posibles mejoras.

21	**BAIA09**	En la práctica clave de gestión BAI09.04 no se obtiene estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado: El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.*** **BAI09.04 Optimizar el coste de los activos.** **Práctica:** Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio. **Actividad 5:** Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.	No disponen de herramientas adecuadas para monitorear y analizar la capacidad y utilización de los activos y uso de sistemas antiguos que no proporcionan datos precisos o en tiempo real. Políticas de gestión de activos que no incluyen la evaluación periódica de la utilización de recursos.	Mantenimiento y operación de activos infrautilizados o redundantes aumentando los costos operativos. Fondos inmovilizados en activos que no aportan valor significativo. Activos que se vuelven obsoletos sin una revisión regular de su utilización. Falta de datos precisos afecta la toma de decisiones estratégicas sobre la gestión de activos.	**Dirigido al jefe de seguridad de la información:** Implementar herramientas de monitoreo y análisis de capacidad y utilización de activos. Actualizar sistemas y tecnologías obsoletas para mejorar la precisión y eficiencia del monitoreo.
22	**MEA02**	En la práctica clave de gestión MEA02.03 no se determina la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.	**NORMA ISO 15504** **NIVELES DE CAPACIDAD DE LOS PROCESOS** ***Nivel 2 - Administrado: El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.*** **MEA02.03 Realizar autoevaluaciones de control.** **Práctica:** Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	Ausencia de un enfoque estructurado para determinar la frecuencia óptima de las autoevaluaciones y ausencia de un proceso formal para incorporar los hallazgos de las autoevaluaciones en la toma de decisiones y la mejora continua.	Pérdida de oportunidades para implementar mejoras proactivas y prevenir problemas futuros. Riesgo de estancamiento y obsolescencia en un entorno empresarial en constante cambio.	**Dirigido a la directora de procesos de calidad:** Definir claramente los objetivos y propósitos de las autoevaluaciones periódicas en el contexto del sistema de gestión y los procesos organizacionales y establecer mecanismos formales para el seguimiento y la revisión de las acciones correctivas y preventivas derivadas de las autoevaluaciones.