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

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

Tema:

"Aplicación del método COBIT y el control de seguridad de la información en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda."

Autor: Freire Cerna, Jonatan Samuel

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de ciudadanía No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: **"APLICACIÓN DEL MÉTODO COBIT Y EL CONTROL DE SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO UNIBLOCK Y SERVICIOS LTDA."**, desarrollado por Jonatan Samuel Freire Cerna, 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, Febrero 2024.

TUTORA

.....

Dra. Patricia Paola Jiménez Estrella

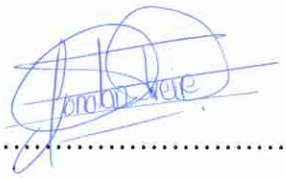
C.C. 180293423-0

AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jonatan Samuel Freire Cerna con cédula de ciudadanía No. 050443975-3, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"APLICACIÓN DEL MÉTODO COBIT Y EL CONTROL DE SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO UNIBLOCK Y SERVICIOS LTDA."**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autor de este Proyecto Integrador.

Ambato, Febrero 2024.

AUTOR



.....

Jonatan Samuel Freire Cerna

C.C. 050443975-3

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 integrador, 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 autor.

Ambato, Febrero 2024.

AUTOR

.....

Jonatan Samuel Freire Cerna

C.C. 050443975-3

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"APLICACIÓN DEL MÉTODO COBIT Y EL CONTROL DE SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO UNIBLOCK Y SERVICIOS LTDA."**, elaborado por Jonatan Samuel Freire Cerna, 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, Febrero 2024.

Dra. Tatiana Valle Ph. D.
PRESIDENTE

Lic. Claudio Hidalgo
MIEMBRO CALIFICADOR

Dra. Karina Benítez
MIEMBRO CALIFICADOR

DEDICATORA

El presente proyecto de titulación se lo dedico a mi familia quien han sido un gran apoyo en mi vida y en el transcurso de mi carrera universitaria. Muchos de mis logros se los debo a ellos incluido este.

A mi madre Wilma Cerna, quien a pesar de todo estuvo para mí en todo momento, ella es una parte muy importante en mi vida, que siempre me apoyado en las decisiones que he tomado, por su soporte y amor incondicional que me ayudaron en muchas situaciones difíciles.

A mis abuelitos Carmen Estrella y José Cerna que estuvieron desde mi niñez y me inculcaron buenos hábitos para ser la persona que soy hoy por hoy. Por confiar en mis capacidades y ser el soporte en mi vida.

Jonatan Samuel Freire Cerna

AGRADECIMIENTO

Agradezco principalmente a Dios por brindarme la vida, salud para terminar una etapa más en mi vida, por ser la guía en cada paso que he dado para lograr cumplir con una meta tan anhelada.

A mi familia que me ha apoyado en el transcurso de mi carrera universitaria sobre todo en los momentos difíciles.

A mi tutora Dra. Patricia Jiménez por brindarme sus conocimientos incluso su paciencia para culminar este proceso.

A la COOPERATIVA DE AHORRO Y CREDITO UNIBLOCK Y SERVICIOS LTDA. y a su personal por su amble colaboración con la información necesaria para el presente proyecto.

Agradezco sinceramente a mis amigos que estuvieron a mi lado en los momentos difíciles durante mi carrera universitaria. En particular, quiero expresar mi profundo agradecimiento a Raquel, cuyo apoyo incondicional y constante permitieron que no me rindiera. Su disposición para escucharme en todo momento ha sido invaluable, gracias por ser parte esencial de este importante capítulo de mi vida.

Jonatan Samuel Freire Cerna

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PÁGINA**

A. PÁGINAS PRELIMINARES

B. CONTENIDOS

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

ÍNDICE DE ILUSTRACIONES

CONTENIDO **PÁGINA**

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

TEMA: "APLICACIÓN DEL MÉTODO COBIT Y EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO UNIBLOCK Y SERVICIOS LTDA."

AUTOR: Jonatan Samuel Freire Cerna
TUTORA: Dra. Patricia Paola Jiménez Estrella
FECHA: Febrero, 2024

RESUMEN EJECUTIVO

El presente trabajo de titulación se realizó en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., ubicada en la ciudad de Latacunga, el cual tuvo como objetivo evaluar el control de seguridad de la información, la metodología aplicada fue el marco de referencia COBIT. Además, para la evaluación de activos de información fue necesario aplicar las directrices según normas ISO/IEC 27000, lo que permitió abordar los aspectos clave de gobierno y gestión de las TI. Por otro lado, para poder identificar los niveles de riesgo, confianza y madurez se tomó en cuenta los componentes de COSO ERM. Se obtuvo como resultado que los departamentos de la cooperativa han establecidos controles de eficacia en la gestión de sus riesgos de seguridad. Sin embargo, los activos de información presentaron la necesidad de abordar de mejor manera los riesgos ya que son más susceptibles a vulnerabilidades y amenazas por su naturaleza digital. Asimismo, se muestra las deficiencias en algunas prácticas claves de la metodología COBIT. Mediante esta observación se recomienda la aplicación de un sistema de monitoreo, así como la actualización de procesos y políticas para el mejoramiento continuo de los procesos y servicios de la cooperativa.

PALABRAS DESCRIPTORAS: COBIT, SEGURIDAD, INFORMACIÓN, COOPERATIVA, NORMA ISO

TECHNICAL UNIVERSITY OF AMBATO
FACULTY OF ACCOUNTING AND AUDITING
ACCOUNTING AND AUDITING CAREER

TOPIC: "APPLICATION OF THE COBIT METHOD AND THE CONTROL OF INFORMATION SECURITY IN THE SAVINGS AND CREDIT COOPERATIVE UNIBLOCK Y SERVICIOS LTDA."

AUTHOR: Jonatan Samuel Freire Cerna
TUTOR: Dra. Patricia Paola Jimenes Estrella
DATE: February, 2024

ABSTRACT

This degree work was carried out at the Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., it is located in Latacunga city. The main aim was to evaluate the information security. Moreover, to assess the security control the COBIT methodology was applied. For the evaluation of information assets, it was necessary to apply the ISO/IEC 27000 standards, which allowed us to address the key aspects of governance and management of IT. On the other hand, to identify the levels of risk, confidence, and maturity, the COSO ERM components were taken into account. The results showed that the cooperative's departments have established effective controls. However, the information assets presented a need to better address the risks since they are more susceptible to vulnerabilities and threats due to their digital nature. It also shows deficiencies in some key practices of the COBIT methodology. Through this observation, the implementation of a monitoring system is recommended, as is the updating of processes and policies for the continuous improvement of the cooperative.

KEYWORDS: COBIT, SECURITY, INFORMATION, COOPERATIVE, ISO STANDARD

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes

1.1.1.1 Historia de la empresa

La Coac Uniblock y Servicios Ltda fue fundada el 27 de junio del 2007 en el Barrio Tilipulo con el apoyo de 23 inversores, cada uno de los cuales aportó su visión y sus recursos respaldando la inversión de 46.000 dólares, su objetivo inicial fue satisfacer las necesidades comunes del gremio de artesanos de la pequeña industria dedicada a la fabricación de bloques, que hasta entonces habían pasado desapercibidos por la banca tradicional.

Con el paso del tiempo, la entidad demuestra la confianza de los socios. Los microcréditos fueron su primer producto, dirigido a personas que habían tenido dificultades para acceder a un financiamiento, y marcaron el inicio de su enfoque empresarial hacia la inclusión y el desarrollo sostenible.

En la actualidad la Cooperativa de Ahorro y Crédito UNIBLOCK y Servicios Ltda. tiene su sede en la Parroquia Eloy Alfaro, cantón Latacunga, Provincia de Cotopaxi, y es una organización sin fines de lucro cuyo objetivo principal es promover la cooperación financiera y el crédito para sus miembros. Así lo confirma el acuerdo ministerial de Bienestar Social, que figura en el Registro General de cooperativas.

1.1.1.2 Detalles estratégicos

Dentro de los detalles estratégicos que corresponden a la empresa se obtuvo la siguiente información de la página oficial de la empresa (Coac Uniblock y Servicios Ltda, 2023):

- **Misión**

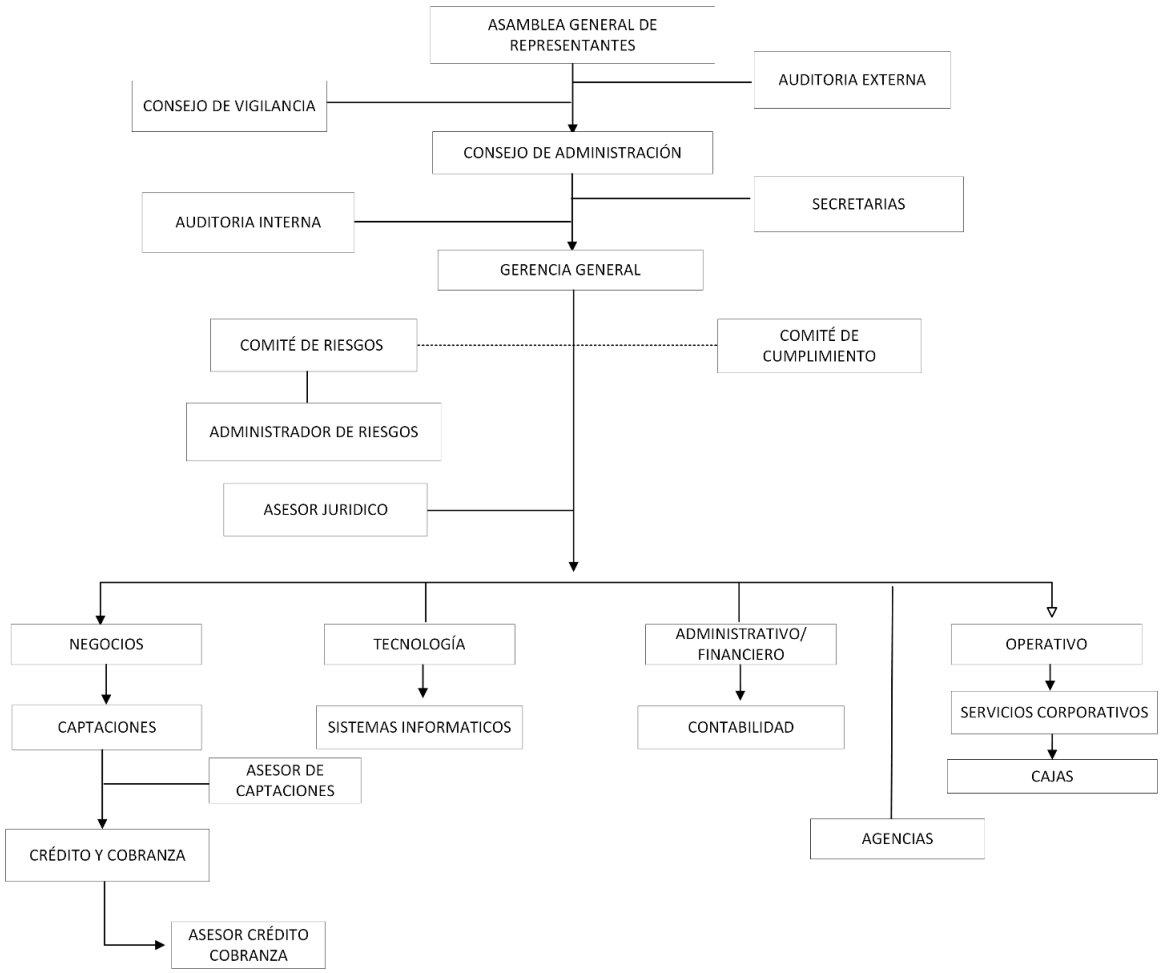
Somos una entidad solvente, solidaria, productiva, ágil e innovadora con servicios financieros oportunos a nivel nacional.

- **Visión**

En el 2022 la Cooperativa de Ahorro y Crédito UNIBLOCK y Servicios Ltda. Contará con nuevas agencias y sucursales a nivel nacional, seguir siendo una institución financiera con servicios de calidad y calidez para nuestros socios.

1.1.1.3 Estructura organizacional

Ilustración 1 Estructura organizacional



Fuente: Coac Uniblock y Servicios Ltda (2023)

Elaborado por: Freire (2023)

1.1.1.3.1 Descripción de funciones

Área Directiva: El comité de representación y gestión de la cooperativa está compuesto por los siguientes órganos:

Asamblea General: El máximo nivel de representación de la cooperativa lo constituyen todos sus socios, cada uno de los cuales dispone de un voto sin tener en cuenta la cuantía de sus aportaciones.

Consejo de Administración: Se compone de representantes designados por la asamblea para representarla durante un tiempo determinado.

Consejo de Vigilancia: Está compuesto por miembros elegidos por la asamblea para ejercer el control interno y la supervisión de las acciones ejecutivas y administrativas.

Área Ejecutiva: Se trata de una estructura organizativa cuya principal responsabilidad es aplicar las políticas establecidas por la administración y garantizar la adecuada toma de decisiones sobre las funciones operativas de la COAC.

Área de Apoyo: Son las áreas que contribuyen a la ejecución de las tareas ligadas a la empresa e incluyen las siguientes:

- Contabilidad
- Abogado Interno
- Secretaria de Consejos

Área Operativa: Está formada por todas las unidades que dirigen directamente la actividad de la institución y se compone de:

- Cajas
- Crédito y Cobranzas
- Servicios Cooperativos
- Sistemas
- Asesor de Negocios

1.1.1.4 Detalles de operaciones

Dentro de los productos que brindan están:

- **Ahorro a la vista:** Es una cuenta de ahorro que ofrece flexibilidad y disponibilidad inmediata del dinero. Es una opción popular para los clientes de la cooperativa que necesitan tener acceso a sus fondos en todo momento para satisfacer sus necesidades financieras diarias o imprevistas.
- **Ahorro programado:** Es una buena opción para quienes desean crear un sistema de ahorro disciplinado a largo plazo de forma disciplinada, conforme con las condiciones del contrato y con un tipo de interés preferente.
- **Chiqui ahorro:** Esta cuenta está diseñada específicamente para que los niños y adolescentes puedan ahorrar dinero de manera segura y fomentar hábitos de ahorro desde temprana edad para sus sueños futuros.
- **Créditos microempresariales:** Este es un crédito diseñado específicamente para microempresas o pequeños emprendimientos. Estos créditos están dirigidos a cubrir las necesidades de pequeños negocios, proporcionándoles acceso a capital para invertir en sus operaciones, expandir su negocio, adquirir activos o cubrir gastos operativos.
- **Crédito de consumo:** Nos ayudara a adquirir bienes de consumo o pagos de servicio, cuando la fuente de ingresos proceda de sueldos, salarios, honorarios, remesas y/o rentas promedias.
- **Depósitos a plazo fijo:** Se trata de un producto en el que los clientes depositan una determinada cantidad de dinero durante un tiempo establecido con el fin de recibir intereses sobre ese dinero. Estos depósitos se distinguen por un tipo de interés fijo. y plazos predeterminados

1.1.1.5 Detalles legales

La Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., está basada en la siguiente base legal:

- Código Orgánico Monetario y Financiero, Articulo 446
- Ley Orgánica de Economía Popular y Solidaria, literal b del articulo 147

- Reglamento General de la Ley Orgánica de Economía Popular y Solidaria, numeral 2 del artículo 154
- Resolución No. SEPS-ROEPS-2013-000667 de fecha 05 de abril de 2013
- Resolución No. JR-ST-2013-011, de 01 de agosto de 2013
- Resolución No. SEPS-IEN-IGPJ-2014-009, de 10 de febrero del 2014
- Conforme lo determinado en el artículo 1 de la Resolución No. SEPS-IGT-ISF-IGJ-2016-089 de 27 de abril del 2016
- Mediante tramite No. SEPS-IZ3-2018-001-26999 de fecha 15 de marzo de 2018
- Mediante memorando SEPS-SGD-IZ3-DZ3SF-2018-0465 de fecha 04 de abril de 2018
- Ley de seguridad social
- Código de trabajo
- Ley de propiedad intelectual
- Ley de protección de datos personales

1.1.1.6 Marca y logo

La Cooperativa de Ahorro y Crédito Uniblock y Servicios está representada

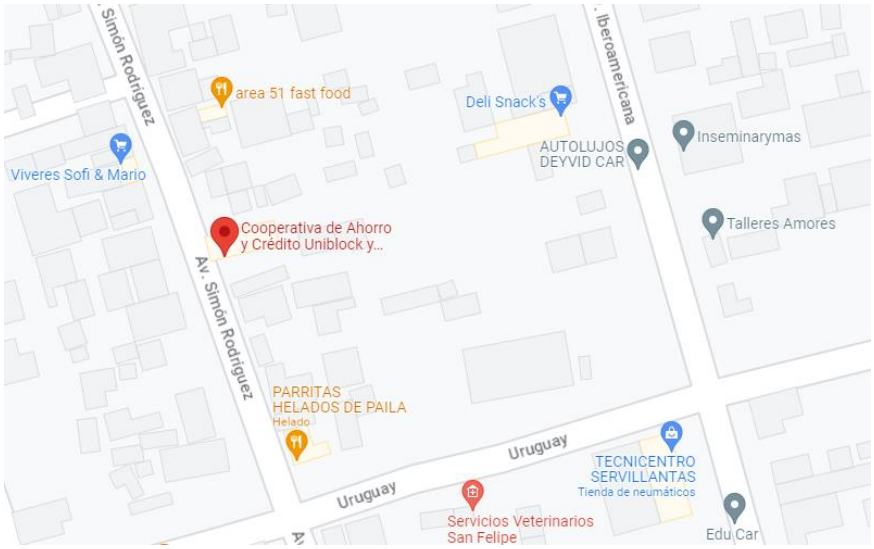
Ilustración 2 Logo COAC Uniblock y Servicios Ltda.

Fuente: Coac Uniblock y Servicios Ltda (2023)

1.1.1.7 Ubicación

La Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., está situada en la provincia de Cotopaxi en la ciudad de Latacunga en la avenida Simón Rodríguez y Uruguay, San Felipe donde se desarrollará el actual proyecto integrador.

Ilustración 3 Ubicación de la COAC Uniblock y Servicios Ltda.



Fuente: Google Maps (2023)

1.1.2 Descripción del entorno

1.1.2.1 La importancia de la seguridad de la información en la actualidad

Actualmente, las TIC en el mundo nos han permitido gozar de comodidad y rapidez en los diversos procesos que se realiza a diario, no obstante, existe una mayor necesidad de proteger los diferentes sistemas de la información a nivel de hardware, software y bases de datos frente a diversas amenazas y vulnerabilidades que impiden su correcto funcionamiento (Mora et al., 2020). Además, un sistema de seguridad de la información permitirá prevenir las amenazas y los riesgos para los sistemas mediante el análisis y la evaluación de sus actividades de seguridad, ya que las empresas se enfrentan a amenazas externas e internas que afectan a la integridad, disponibilidad y confidencialidad sobre la información para las operaciones diarias (Machuca, 2021).

Actualmente existen nuevos métodos que pueden repercutir en la seguridad de la información de las entidades por ello es necesario una estrategia de seguridad con el fin de prevenir fugas y fallas en los sistemas. Adicionalmente se suman vulnerabilidades internas que pueden llegar hacer un factor de riesgo, por ello es que existe un alto riesgo en la perdida de dinero además de perder la confianza por parte de los clientes y socios de la entidad (Alberto, 2022).

Según Pérez y Robayo (2019) mencionan que las instituciones financieras que crecen tecnológicamente y almacenan la información de los usuarios en una matriz de datos sin tener en cuenta la correcta configuración de la seguridad de la información, ni capacitando a sus empleados en temas de seguridad, se convierte en una entidad vulnerable ante posibles ataques, es por esto que las entidades financieras deben buscar opciones para disminuir las vulnerabilidades con el propósito de otorgar a sus clientes la tranquilidad de que su información esta llevada por normas de seguridad.

Los sistemas de seguridad que poseen cada empresa suelen ser un objetivo directo de los ladrones de información financiera, que emplean diversas técnicas para acceder a los servicios de la empresa con el fin de hacerse con el control y obtener la información necesaria. Por ello, es fundamental que los empleados dispongan en todo momento de medidas de seguridad básicas para proteger y contribuir a la conservación de los datos financieros de la organización. (Muñoz et al., 2019).

1.1.2.2 Impacto de la seguridad de la información en las cooperativas de ahorro y crédito del segmento 2

De acuerdo con Zhao et al. (2020) afirma que independientemente de la clasificación de las organizaciones cuentan con varios tipos de activos, como infraestructuras, vehículos, equipo de computación, efectivo, entre otros. Sin embargo, uno de los activos más importantes y que algunas veces se pasa por alto es la recopilación de información. De igual manera, algunos de los problemas que debe afrontar una organización está relacionado con el espionaje y el robo de información (Haghighat & Li, 2021).

Ramos (2021) menciona que las cooperativas de ahorro y crédito presentan un alto riesgo en el tema relacionado a la seguridad de la información por lo tanto no se debe olvidar que su manejo se basa en la tecnología que mejora de una forma rápida y que se necesita tomar ciertas medidas de seguridad para evitar pérdidas para la cooperativa. Por otro lado Muñoz Pinto (2020) señala que los riesgos inherentes a las tecnologías de la información afectan a la gestión y administración de las redes, siendo uno de los medios a través de los cuales pueden producirse graves daños a la información almacenada. Además, la asignación errónea de roles debido a una

gestión insuficiente de las claves de acceso representa otro riesgo, creando un punto de entrada vulnerable para diversos ataques.

Es innegable que una de las inversiones más significativas que realizan las empresas es en estrategias que garanticen la seguridad, integridad y disponibilidad de la información. Dado que es una actividad crítica en las empresas, ya que está expuesta a ataques dirigidos a obtener acceso a la información que se ha construido para garantizar el correcto funcionamiento y desarrollo de cada proceso (Suáres et al., 2019).

La seguridad de la información es fundamental porque, si no se aborda, puede producirse una pérdida de información sensible, lo que podría acarrear consecuencias como la pérdida de prestigio de la institución (Lema y Donoso, 2019). Por ello, es fundamental que el sistema utilizado por las cooperativas sea eficiente y funcione bajo estándares estrictos de seguridad, lo que permitirá gestionar su información de forma eficaz y al 0mismo tiempo saber que sus datos están totalmente protegidos contra cualquier tipo de ataque que se pueda tener un impacto significativo (Liu et al., 2021).

1.1.2.3 Los controles de seguridad como herramienta para el gobierno y gestión de las TI en la COAC Uniblock y Servicios Ltda.

De acuerdo con Barrera (2019) las partes administrativas de las Cooperativas de Ahorro y Crédito tienen poco interés en ampliar sus capacidades tecnológicas, debido sobre todo a los costes asociados a la implantación de recursos tecnológicos fiables y seguros. Como resultado, la información sensible de la empresa puede verse comprometida, lo que pone en peligro la integridad y seguridad de la información. Esto perjudica no sólo a la entidad, sino también a los individuos que poseen esta información.

Una entidad financiera que no considere como prioridad a resguardar la información personal de sus clientes corre el riesgo de perder su confianza. En consecuencia, la seguridad de los datos debe ser un pilar vital en el funcionamiento de cualquier entidad financiera.

Es fundamental que la institución financiera cuente con procesos de mitigación de riesgos en sus políticas para proteger la información que gestiona. La falta de aplicación de un marco de referencia integral como COBIT, para detectar los riesgos tecnológicos que vayan a influir en la organización limita a la institución que opere de forma organizada, aumentando el riesgo de que su información se vea comprometida.

Cuando las instituciones financieras incorporan a sus políticas el uso de procesos que identifican y mitigan los riesgos tecnológicos, pueden brindar mayor seguridad a sus socios y a su propia información personal, sabiendo que será manejada de manera confiable y segura, valorándola como uno de los activos más valiosos de la institución.

Es fundamental que la organización emplee controles de seguridad para salvaguardar sus sistemas y datos. En el caso de la COAC Uniblock y Servicios Ltda., se debe implementar herramientas para la gestión y gobernanza de TI. Estas herramientas pueden ayudar a supervisar y gestionar sus sistemas de manera más eficiente obteniendo resultados eficaces, lo que puede mejorar la seguridad en general. Algunas herramientas útiles incluyen software de monitoreo de red, software antivirus, firewalls y sistemas de detección de intrusos. Además, es fundamental que la entidad disponga de directrices y procesos precisos para garantizar que los controles de seguridad se aplican y mantienen adecuadamente sus procesos de gestión, así como la orientación al desarrollo de planes de contingencia ante posibles desastres.

1.1.3 Justificación

Uno de los puntos para tener en cuenta en las empresas es la presencia de vulnerabilidades de seguridad de la información en la ejecución de las operaciones diarias. Estas vulnerabilidades, si no se abordan, pueden causar daños en el rendimiento operativo de la empresa a lo largo del tiempo. Dichas vulnerabilidades pueden abordarse mediante la aplicación de políticas de seguridad de la información acordes con la normas ISO 27001 (Llano et al., 2021).

Las entidades financieras que están reguladas por la SEPS se ha observado la necesidad de aplicar y mejorar sus sistemas de información desarrollando productos

y servicios financiero formales a través de canales digitales (Espinoza Farfán & Vázquez Loaiza, 2020).

Sabillón y Cano (2019) mencionan que, las empresas intentan proteger los activos de información y adoptan medidas y programas de ciberseguridad, pero a pesar de este esfuerzo continuo, las violaciones y ataques de ciberseguridad son inevitables.

Se tomó como referencia para la recolección de información fuentes primarias como documentación interna de la empresa, así mismo se complementó con fuentes secundarias tomadas de revistas, artículos de interés y documentos de repositorios. Esta variedad de fuentes garantizó un análisis exhaustivo y equilibrado para la investigación que nos ocupa.

Para lo cual se utilizó diferentes técnicas como la observación, con el fin de conocer de primera mano las vulnerabilidades que pueden llegar a afectar a las operaciones de la cooperativa. Además, se realizó un cuestionario a los funcionarios de la entidad para obtener una perspectiva detallada de las posibles áreas de mejora y los riesgos potenciales a los que la cooperativa puede enfrentarse.

El método COBIT le permite gestionar y gobernar toda la información y la tecnología de su organización al tiempo que comprende el negocio y las áreas funcionales de principio a fin y tiene en cuenta a las partes internas y externas (Quillupangui, 2019). En otras palabras, COBIT se creó para ayudar a la dirección de una empresa a cumplir sus objetivos mediante una gestión adecuada de la tecnología y la información. Es fundamental destacar que la implantación de COBIT debe producirse en todos los niveles de la organización.

Este estudio se centra en lo crucial que es mantener controles de seguridad de la información en las operaciones y procesos de las cooperativas, identificando el estado actual, lo que hace necesario el análisis y la valoración de riesgo, identificación de amenazas con respecto a la seguridad de la información.

La COAC Uniblock y Servicios Ltda., fue la mayor beneficiaria de esta contribución, ya que la implementación de controles de seguridad constituyó a salvaguardar la disponibilidad, confidencialidad e integridad de la información financiera así mismo se estableció controles en el proceso contable para la emisión

de estados financieros requeridos por la SEPS, de igual manera la protección de datos personales mejorando así la eficacia del gobierno y gestión de la información mediante el uso de las TI, así como la seguridad de los activos digitales de la organización que promueven su sostenibilidad incorporando planes de contingencia y prevención de catástrofes.

1.1.4 Objetivos

1.1.4.1 Objetivo general

- Aplicar el método COBIT para el control de seguridad en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda. para la evaluación de la seguridad de la información.

1.1.4.2 Objetivos específicos

- Elaborar el diagnóstico para la determinación de los niveles de riesgo, confianza y madurez con base a los componentes COSO ERM
- Realizar la Evaluación de los activos de información, procesos y niveles de tasación y madurez en la gestión y gobiernos de las TI con base a las normas ISO 27000 y marco de referencia COBIT.
- Comunicar los resultados de la aplicación del modelo COBIT enfocados en los controles de la seguridad de la información a través del informe para la toma de decisiones de la alta gerencia.

1.2 Revisión de la literatura

1.2.1 Teoría de sistemas y su aplicación en la auditoria de la información

Según Bertalanffy (1989) el estudio de los sistemas como grupos interconectados de elementos que interactúan para lograr un objetivo común. La TGS ha intentado restar importancia a la comprensión de las relaciones e interdependencias entre los componentes del sistema, lo cual es importante en la auditoría de la información.

La auditoría informática desempeña un rol crucial en asegurar el correcto manejo de los sistemas de información por medio de la aplicación de los fundamentos generales de la teoría de sistemas (Párraga & Lara, 2013).

Esta teoría ayudara a estimular una revisión objetiva de los procesos, prácticas y sistemas más significativas en el desarrollo de la entidad. Así mismo, esta teoría es fundamental para logar entender de mejor manera los recursos de TI permitiendo examinar los sistemas de información, identificar posibles vulnerabilidades y evaluar la eficacia de los controles internos que afectan al proceso contable informatizado, con el fin de proporcionar recomendaciones pertinentes para optimizar la seguridad y el rendimiento informático empresarial.

1.2.2 Auditoría

El proceso de auditoría interna tiene lugar en el ámbito contable y se lleva a cabo de forma periódica en respuesta a los inconvenientes que se producen en las empresas. Su experiencia se centra por completo en la evaluación, supervisión de procesos, la eficiencia y el uso adecuada sobre los recursos (Serrano et al., 2022).

1.2.2.1 Importancia

El papel primordial de la auditoría puede encontrarse en varios contextos, como la segunda opinión imparcial. También se reconoce su importante función en la representación y defensa de los intereses de la sociedad. Este valor se basa en las cualidades que debe poseer el contable público, así como en la forma en que debe realizarse el trabajo, es decir, en las características de la labor del fiscalizador (Ramirez et al., 2022).

1.2.2.2 Fases de auditoria

Las fases generales de una auditoría son planificación, ejecución y comunicación. A continuación, se detallan cada una de ellas:

Tabla 1 Fases de auditoría

Fases	Definición	Normas
Planificación	Se obtendrá información y datos de la entidad. Además, determina los métodos a seguir durante el procedimiento de revisión.	NIA 200: Objetivos generales del auditor independiente y realización de la auditoria de conformidad con las NIA. NIA 210: Acuerdo de los términos de encarga de auditoría. NIA 300: Planificación de la auditoria de estados financieros. NIA 315: Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad.
Ejecución	Es la recopilación, evaluación y desarrollo de pruebas, cuyos resultados darán lugar a la opinión del auditor.	NIA 230: Documentación de auditoría. NIA 330: Respuestas del auditor a los riesgos valorados. NIA 500: Evidencia de auditoría NIA 520: Procedimientos analíticos NIA 580: Manifestaciones escritas
Comunicación	Es el documento que recoge los resultados y conclusiones obtenidos mediante el uso de controles respaldados por la documentación de la entidad.	NIA 700: Formación de la opinión y emisión del informe de auditoría sobre los estados financieros NIA 701: Asuntos claves de auditoría. NIA 705: Opinión modificada en el informe emitido por un auditor independiente.

Fuente: Bedor et al., (2020)

Elaborado por: Freire (2023)

1.2.2.3 Tipos de auditoria

Manrique Plácido (2019) señala que los tipos de auditoria son los siguientes:

Tabla 2. Tipos de Auditoria

Tipos	Concepto
Auditorias tributarias	La auditoría fiscal, ya sea preventiva y voluntaria por parte de auditores cualificados por parte de la Administración Tributaria, evalúa el cumplimiento por parte de una empresa de sus obligaciones fiscales. Su objetivo es confirmar la exactitud del estado financiero y los resultados presentados en el informe anual.
Auditoria financiera	La auditoría financiera implica que auditores independientes revisen los datos económicos y financieros de las instituciones financieras siguiendo las normas contables vigentes, a menudo las NIIF. Esto se hace para proporcionar un informe que evalúe la exactitud y coherencia de los datos presentados.
Auditoria administrativa	Es responsable de valorar la correcta realización de sus actividades, operaciones y funciones de la organización, especialmente dentro del área administrativa. Corresponde a la aplicación continuada de las políticas y procedimientos ya establecidos.

Auditoria operativa	Este estudio se centra en los procesos administrativos y las operaciones organizativas. Se analizan las diferentes áreas operativas y funcionales de una entidad con el fin de determinar si poseen los controles necesarios para funcionar eficazmente.
Auditoria gubernamental	Es un análisis exhaustivo, sistemático y detallado de las actividades presupuestarias y administrativas realizadas por los gobiernos del Estado.
Auditoria académica	Es una auditoria se centra en evaluar los planes de estudio, los perfiles de los estudiantes, los métodos de evaluación y el cumplimiento de las normas académicas en los sectores educativos público y privado.

Fuente: Manrique (2019)

Elaborado por: Freire (2023)

1.2.3 Auditoría de información

El auditor de sistemas de información se centra en evaluar los riesgos y las medidas de seguridad de cada etapa del proceso, que incluye datos, información, conocimientos, hardware y procedimientos. Se realizan pruebas de control interno para garantizar que se siguen las normas establecidas. Se utilizan técnicas como la validación cruzada y la verificación de saldo para demostrar la integridad de las pruebas. (Sánchez, 2021).

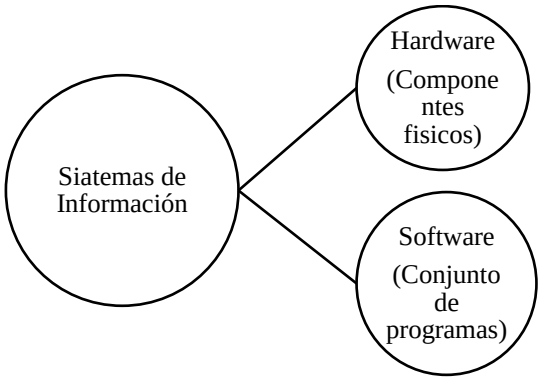
1.2.3.1 Importancia

Actualmente, un auditor informático es crucial para una empresa porque supervisa el correcto funcionamiento del SGSI y aporta claves necesarias que permitan garantizar un funcionamiento de los sistemas de la empresa con un alto grado de fiabilidad y seguridad (Albarracín et al., 2021).

1.2.4 Sistemas informáticos

El sistema de información se compone de dos partes: el hardware (un dispositivo físico) y el software (componentes no físicos que ayudan al funcionamiento de los dispositivos electrónicos). El uso de los sistemas de información consiste en servir de intermediarios para el intercambio de recursos entre los numerosos subsistemas internos de la empresa, así como entre éstos y el mundo exterior (Lapiedra et al., 2021).

Ilustración 4 Sistemas Informáticos



Fuente: Hernandez (2003)

Elaborado por: Freire (2023)

1.2.5 Seguridad informática

La puesta en práctica medidas de seguridad, como cortafuegos y detección de intrusos, junto con las políticas tecnológicas de la Administración, establece una línea de actuación para evitar errores en las actividades relacionadas con la información. La disciplina de Seguridad de la Información es responsable de evaluar los riesgos, identificar las amenazas y determinar las acciones para reducir los riesgos al tiempo que se adhiere a las mejores prácticas y normas (Cuasapaz Narvaez y Landázuri Narvaez, 2023).

Ilustración 5 Valores

Confidencialidad	• Se refiere al principio y la práctica de salvaguardar la información sensible y restringir el acceso únicamente a las personas o entidades autorizadas.
Integridad	• Es un conjunto de acciones, mecanismos y procedimientos utilizados para determinar si todas las operaciones y datos implican actos ilegales según la definición de la ley, y es la base de la profesionalidad.
Disponibilidad	• Esto implica un acceso continuo, incluso en situaciones adversas como cambios, catástrofes o ataques. Esto es fundamental para evitar cortes y mantener las operaciones empresariales en periodos críticos.

Fuente: Escrivá et al., (2013)

Elaborado por: Freire (2023)

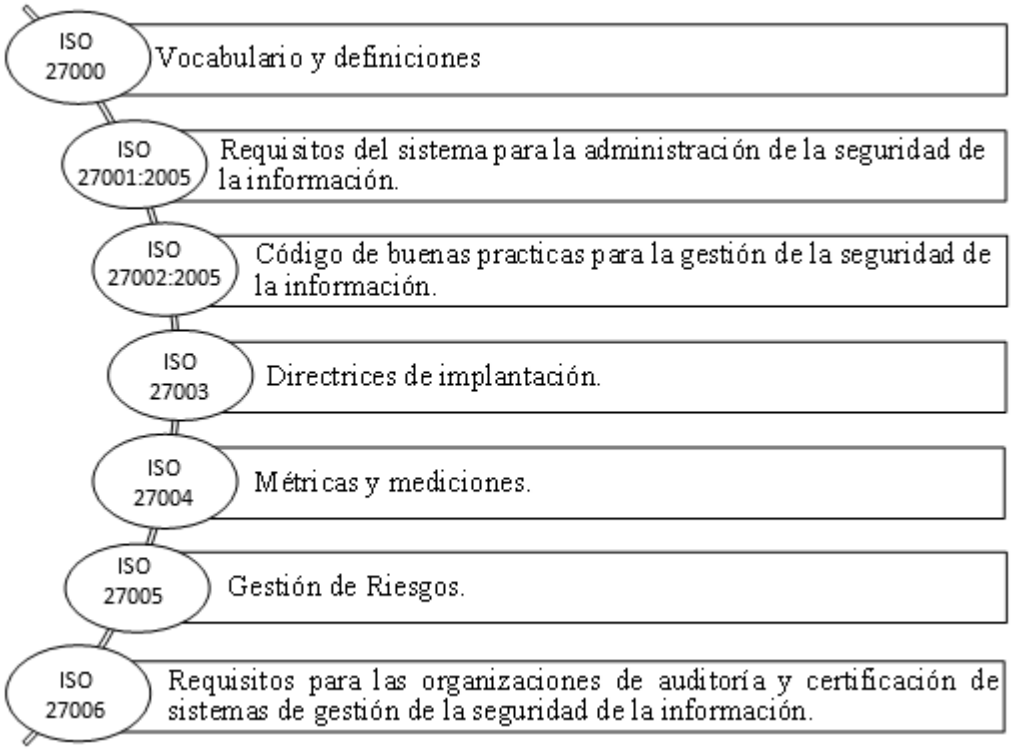
1.2.5.1 Importancia de la seguridad informática

Las empresas realizan actividades de recopilación de información extremadamente valiosa que debe salvaguardarse. Los sistemas pueden contener datos confidenciales, información sobre procesos y operaciones de la organización, planes estratégicos y empresariales, secretos comerciales y otra información crítica. Sin embargo, el valor de esta información disminuye drásticamente si es conocida por personas ajenas a la empresa. (Sisti, 2019).

1.2.6 Norma ISO

Es una organización internacional de normalización sin fines lucrativos, fundada el 2 de febrero de 1947, dedicada a fomentar el avance y la aplicación de normas en organizaciones de fabricación y servicios internacionales. La ISO también proporciona herramientas que ayudan a la consecución de objetivos como el avance de las actividades tecnológicas, científicas, económicas e intelectuales (Organización Internacional de Estandarización, 2017).

Ilustración 6 Norma ISO 27000



Fuente: Normas ISO 27000 (2016)
Elaborado por: Freire (2023)

1.2.7 Marcos de referencia

Existen un sin número de marcos de referencia para el control de la seguridad, cada uno con su propio conjunto de controles y características que se aplican en base a las necesidades y situaciones de la organización. A continuación, se menciona algunos marcos de referencia comúnmente utilizados en la administración de la seguridad de la información:

Tabla 3 Marcos de referencia

ITIL	ITIL ofrece directrices detalladas en todos los aspectos de la administración de servicios, cubriendo una amplia gama de temas desde el personal a los procesos, productos hasta el uso del proveedor (Alvarado, 2014).
MAGERIT	La metodología aborda la gestión de los riesgos de seguridad de la información de manera sistemática, estableciendo objetivos claros y mensurables para un seguimiento detallado (Rojas, 2019).
COSO ERM	Es un proceso de gestión de riesgos que permite a los ejecutivos de la empresa operar de manera más eficiente en un entorno de alto riesgo (Sánchez, 2016).
COSO	El modelo COSO es una herramienta eficaz que permite evaluar el control interno, porque abarca factores relevantes tales como el entorno de control, la gestión de riesgos, las prácticas de control, la información y comunicación, y el seguimiento (Santa Cruz, 2015).

Elaborado por: Freire (2023)

1.2.7.1 Marco de referencia COBIT

La información es una de las actividades críticas en cualquier entidad a la hora de adoptar políticas, por lo que su correcta gestión es fundamental. Asimismo, COBIT es un grupo de principios y recomendaciones cuyo objetivo es mejorar su administración y gestión de los diferentes soportes de información que utilizan ciertas empresas. La finalidad del método es proporcionar instrumentos para evaluar los riesgos y el reconocimiento de los beneficios asociados a la gestión del trabajo y de las tecnologías de la información (Hernández, 2019).

1.2.7.2 Principios de COBIT

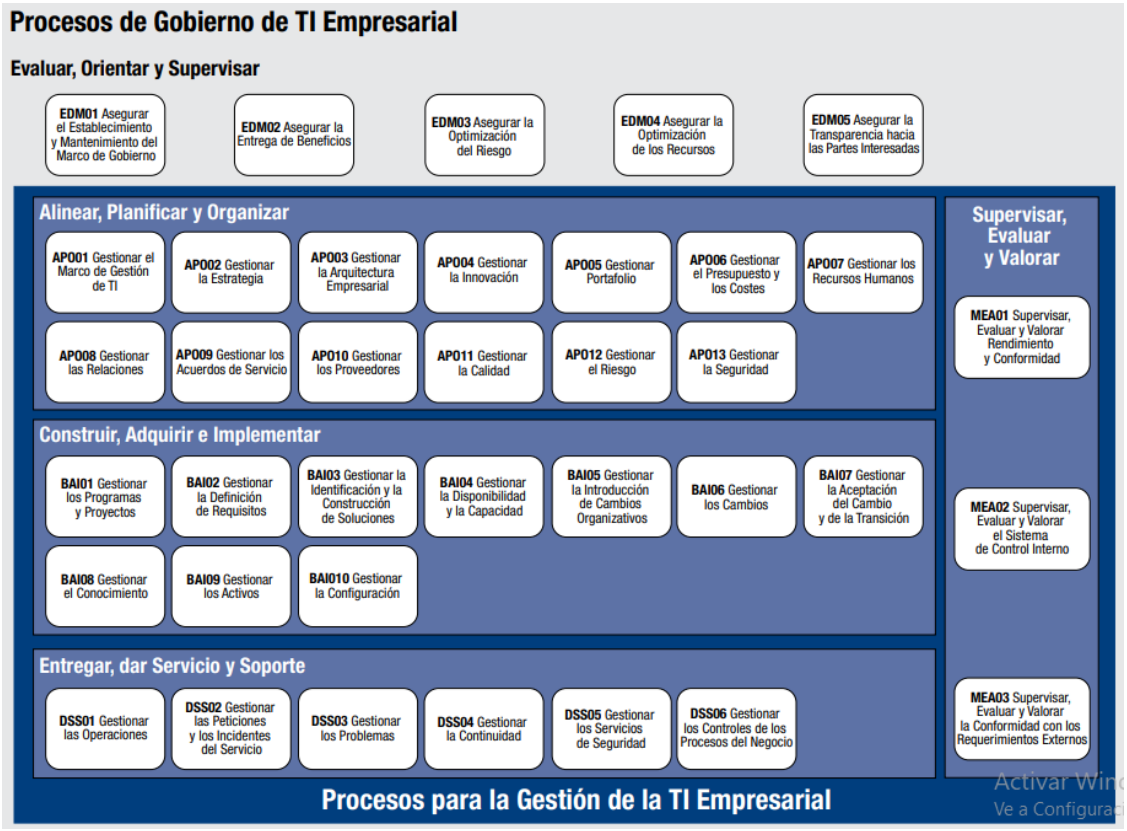
La metodología COBIT se sustenta en cinco principios clave para la gestión de riesgos gobierno y gestión de las TI. A continuación, representa estos cinco fundamentos.

Ilustración 7 Principios del método COBIT

Fuente: ISACA (2012)

1.2.7.3 Dominios y procesos catalizadores de COBIT

Ilustración 8 Procesos de gobierno COBIT

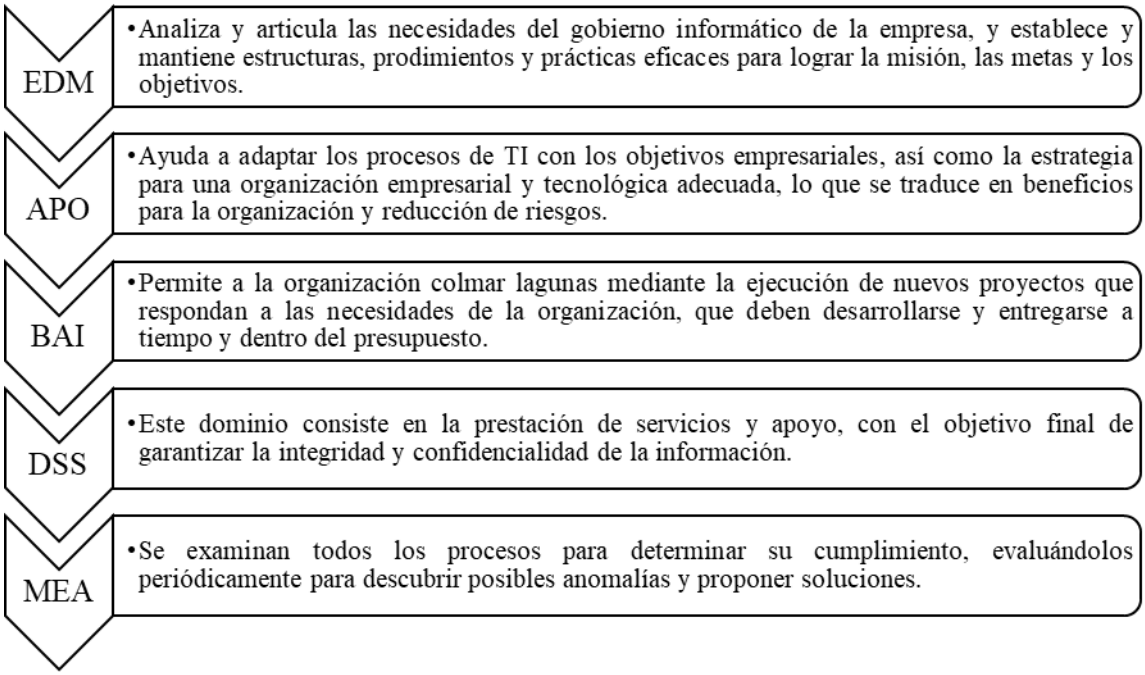


Fuente: ISACA (2012)

Dentro del marco de referencia COBIT, los procesos de gobierno y gestión de TI se dividen en dos ámbitos principales:

- **Gobierno:** Contiene cinco procesos de gobierno, cada uno de los cuales define las prácticas de evaluación, orientación y supervisión.
- **Gestión:** Consta de cuatro dominios que corresponden a las áreas de responsabilidad de planificar, construir, ejecutar y supervisar, y facilita una cobertura completa de la TI.

Ilustración 9 Dominios de modelo de referencia COBIT



Fuente: Adaptado de ISACA (2012b)

Elaborado por: Freire (2023)

Tabla 4 Procesos Catalizadores

Dominios	Procesos	Prácticas clave	N.º de actividades
EVALUAR, ORIENTAR Y SUPERVISAR	EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	3 prácticas	20 actividades
	EDM02 Asegurar la Entrega de Beneficios	3 prácticas	20 actividades
	EDM03 Asegurar la Optimización del Riesgo	3 prácticas	16 actividades
	EDM04 Asegurar la Optimización de Recursos	3 prácticas	13 actividades
	EDM05 Asegurar la Transparencia hacia las Partes Interesadas	3 prácticas	10 actividades

PLANEAR, PLANIFICAR Y ORGANIZAR	APO01 Gestionar el Marco de Gestión de TI	8 prácticas	48 actividades
	APO02 Gestionar la Estrategia	6 prácticas	31 actividades
	APO03 Gestionar la Arquitectura Empresarial	5 prácticas	39 actividades
	APO04 Gestionar la Innovación	6 prácticas	25 actividades
	APO05 Gestionar el Portafolio	6 prácticas	28 actividades
	APO06 Gestionar el Presupuesto y los Costes	5 prácticas	31 actividades
	APO07 Gestionar los Recursos Humanos	6 prácticas	33 actividades
	AP008 Gestionar las relaciones	5 prácticas	24 actividades
	AP009 Gestionar los acuerdos de servicio	5 prácticas	20 actividades
	APO10 Gestionar los Proveedores	5 prácticas	27 actividades
	APO11 Gestionar la Calidad	6 prácticas	34 actividades
	APO12 Gestionar el Riesgo	6 prácticas	33 actividades
	APO13 Gestionar la Seguridad	3 prácticas	19 actividades
CONSTRUIR, ADQUIRIR E IMPLEMENTAR	BAI01 Gestión de Programas y Proyectos	14 prácticas	78 actividades
	BAI02 Gestionar la Definición de Requisitos	4 prácticas	17 actividades
	BAI03 Gestionar la Identificación y Construcción de Soluciones	11 prácticas	57 actividades
	BAI04 Gestionar la Disponibilidad y la Capacidad	5 prácticas	25 actividades
	BAI05 Gestionar la Facilitación del Cambio Organizativo	7 prácticas	29 actividades
	BAI06 Gestionar los Cambios	4 prácticas	18 actividades
	BAI07 Gestionar la Aceptación del Cambio y la Transición	8 prácticas	51 actividades
	BAI08 Gestionar el Conocimiento	5 prácticas	18 actividades
	BAI09 Gestionar los Activos	5 prácticas	36 actividades
	BAI10 Gestionar la Configuración	5 prácticas	16 actividades
ENTREGA, SERVICIO Y SOPORTE	DSS01 Gestionar Operaciones	5 prácticas	34 actividades
	DSS02 Gestionar Peticiones e Incidentes de Servicio	7 prácticas	24 actividades
	DSS03 Gestionar Problemas	5 prácticas	23 actividades
	DSS04 Gestionar la Continuidad	8 prácticas	42 actividades
	DSS05 Gestionar Servicios de Seguridad	7 prácticas	49 actividades
	DSS06 Gestionar Controles de Proceso de Negocio	6 prácticas	32 actividades

SUPERVISAREVALUAR Y VALORAR	MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	5 prácticas	26 actividades
	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	8 prácticas	44 actividades
	MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	4 prácticas	18 actividades

Fuente: (ISACA (2012b)

Elaborado por: Freire (2023)

1.2.8. Cuadro comparativo entre COBIT y COSO

Es posible distinguir las diferencias entre los distintos tipos de sistemas que se detallan a continuación:

Tabla 5 Cuadro comparativo del sistema COBIT con otros sistemas

	COBIT	COSO	ITIL	MAGERIT	COSO ERM
Características	*Se basa en la filosofía de que los recursos de TI deben estar organizados. *Se considera una norma aceptable y lo suficientemente flexible como para dar paso a prácticas correctas de seguridad y control de las TIC. * Facilita la comprensión y la conexión de los riesgos administrativos a las TIC por parte de la dirección.	* Ambiente de control * Evaluación de riesgos * Actividades de control * Información y comunicación * Supervisión	* Mejora del servicio al cliente. * Propone el establecimiento de normas. * No es rígido en su aplicación.	* Proporciona a la empresa el conocimiento de la existencia de riesgos y de cómo manejarlos. * Proporciona un método sistemático para analizar los riesgos asociados al uso de la tecnología al uso de la tecnología y la comunicación. * Ayuda a identificar y gestionar los riesgos.	* Facilita una comprensión del valor de la gestión de riesgos corporativos a medida que la empresa establece y aplica sus estrategias. * Se centra en el futuro y analiza varias tendencias a las que probablemente se enfrentan las empresas y que afectan en la gestión de riesgos.
Ventajas	* Mejora la calidad y la medición de la TI. * Ayuda a implementar un sistema de control. * Presenta las actividades en una estructura manejable y lógica	* Tener una visión amplia de algunos riesgos, lo que ayudará a elaborar planes de gestión adecuados. * Ayuda en la toma de decisiones más adecuadas y seguras. * Fomenta la gestión de riesgos como un pilar esencial para toda la organización.	* TI crea una estructura más definida que está orientada a los objetivos de la organización. * La administración tiene más poder. * Los cambios son más fáciles de gestionar. * Mejor aprovechamiento de los recursos y reducción de costes.	* Proporciona un método sistemático para determinar los riesgos en los sistemas de información. * Ayuda a identificar y planificar las medidas necesarias para reducir las vulnerabilidades.	* Permite que la dirección de la empresa tenga una comprensión global de los riesgos potenciales. * Facilita la alineación de los objetivos del grupo con los de cada una de las unidades de negocio.

Desventajas	* Las buenas prácticas COBIT se centran en el control más que en la ejecución. * El modelo de referencia mejora las áreas de TI desde la perspectiva del gobierno corporativo.	* Está demostrado que el control interno no debe costar más que los beneficios que proporciona. * El control interno se centra sobre todo en cuestiones rutinarias y no en situaciones globales.	* La aplicación requiere tiempo y esfuerzo. * Su lenguaje y terminología siguen estando muy limitados a un área muy pequeña de TI. * La mayoría de las organizaciones complican en exceso la implantación de ITIL, lo que conduce al fracaso en muchos casos.	* Adoptar esta metodología es costoso porque las actividades dan lugar a valores económicos.	* La aplicación de este modelo puede requerir cambios significativos en la cultura de la organización y la toma de decisiones.
Objetivo	* Garantizar el éxito en el futuro, hay que encontrar un equilibrio óptimo entre las posibilidades que brindan las TI y las necesidades tecnológicas de la empresa.	* Orientar a la dirección ejecutiva y a todas las entidades gubernamentales hacia el establecimiento de operaciones empresariales más eficientes, eficaces y éticas a escala mundial.	* Ayuda a las organizaciones a optimizar su eficiencia y eficacia operativas, mejorando al mismo tiempo la calidad del servicio prestado a la empresa dentro de unos parámetros de costes que permitan la rentabilidad.	* Ayuda a identificar y planificar las medidas adecuadas para mantener los riesgos bajo control, proporcionado a las organizaciones la capacidad de mitigar efectivamente las amenazas potenciales.	* Proporciona un marco para la gestión del riesgo que permite a las empresas identificar, evaluar y responder a los riesgos que puedan poner en peligro el logro de sus objetivos estratégicos.

Fuente: Adaptado de Santacruz et al., (2017)

Elaborado por: Freire (2023)

CAPÍTULO II

METODOLOGÍA

2.1. Descripción de la metodología

2.1.1. Unidad de análisis

Al desarrollar el proyecto integrador, se consideró como unidad de análisis a la Cooperativa Uniblock y Servicios Ltda., que está ubicada en la ciudad de Latacunga en el Barrio San Felipe, la misma que cuenta con 23 trabajadores que desempeñan funciones en varios departamentos de la entidad. Para lo cual el proyecto se centró en toda la empresa con el fin de identificar problemas con respecto a la seguridad de la información.

Se recopiló información en el ámbito de la tecnología de la información con el objetivo de identificar posibles vulnerabilidades, amenazas y riesgos en el sistema de información de la cooperativa, donde se obtuvo una visión global de la seguridad de la información, destacando sus puntos fuertes en lo que respecta a los controles, de igual manera aquellos puntos débiles en las áreas que se requieren mejorar.

2.1.2. Fuentes y técnicas de recolección de información

2.1.2.1. Fuente primaria

Para el desarrollo del proyecto integrador se utilizó información directamente proporcionada por el personal de la entidad. En base a esto se aplicó la técnica de la encuesta dirigida al gerente y a los jefes de áreas de la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda. que utilizan tecnologías de la información, con la finalidad de identificar las vulnerabilidades y así enfocar la aplicación de controles que permitió una detección oportuna de dichas debilidades evitando que las amenazas se materializaran.

Tabla 6 Personas encuestadas

Nombre	Cargo	Departamento
Abg. Fabian Proaño	Gerente General	Gerencia
Ing. Ricardo Mendoza	Jefe de sistemas	Área de Sistemas
Ing. Ledy Coba	Jefe de captaciones	Área de Captaciones
Ing. Alexandra Banda	Jefe de crédito	Área de Créditos

Ing. Jessica Yanez	Contadora General	Área de Contabilidad
Ing. Anita Rocha	Atención al cliente	Área de Atención al Cliente
Ing. Jenny Masabanda	Jefe de operaciones	Área de Caja

Elaborado por: Freire (2023)

Encuesta

Se realizó una encuesta a los jefes de las áreas involucradas para el estudio que dispone la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., de manera presencial en consecuencia, la investigación se desarrolló de manera verídica y confiable.

Cuestionario

Se utilizó un cuestionario compuesto por 55 preguntas referente al marco de referencia COSO ERM 2017 con respuestas de SI y NO con lo cual se identificó posibles brechas y áreas de mejora en la gestión de riesgos y controles.

Tabla 7 Extracto del cuestiona COSO ERM 2017

Componentes	Preguntas	SI	NO
Gobierno y Cultura	¿Existe políticas en el área de sistemas que incluyen controles específicos de TI? ¿Se revisan periódicamente las responsabilidades y los controles relacionados con TI en el área de sistemas? ¿La conservación de evidencias, como pistas de auditoría o de gestión, se realiza de forma sistemática en el área de sistemas? ¿Describe claramente el departamento de sistemas los requisitos obligatorios relacionados con la estructura operativa de la empresa? ¿Crea oportunidades de colaboración a través de toda la empresa? ¿El área de sistemas considera las oportunidades de forma sistemática con el objetivo de incorporarlas a la empresa? ¿Existe un control periódico para garantizar que los gestores de riesgos cumplen con sus responsabilidades en el área de sistemas? ¿Demuestra el área de sistemas un compromiso coherente con los valores éticos?		

Estrategias y Objetivos	¿El área de sistemas emplea a especialistas, tanto internos como externos, con experiencia en auditoría de TI? ¿Examina el área de sistemas los riesgos relacionados con los factores internos y externos que pueden afectar a la empresa? ¿Analiza el área de sistemas las debilidades, amenazas, fortalezas y oportunidades de la empresa? ¿Se evalúa con frecuencia la materialidad de las amenazas para determinar su impacto en la empresa? ¿Se evalúa la utilización de determinados recursos disponibles en el área de sistemas de la empresa en relación con los riesgos identificados?		

Fuente: Adaptado de COSO ERM 2017 (2017)

Elaborado por: Freire (2023)

2.1.2.2 Fuentes secundarias

Se determinó que la revisión de la investigación bibliográfica y documental era necesario para el desarrollo del proyecto integrador, que incluyó la revisión de libros, revistas, artículos y otros documentos relevantes. Además, se recopiló información de estudios anteriores, lo que permitió acceder a información más precisa y actualizada sobre el tema de interés.

2.1.3 Fases de desarrollo

Tabla 8 Fases de desarrollo

Objetivos	Fases	Descripción
Elaborar el diagnóstico para la determinación de los niveles de riesgo, confianza y madurez con base a los componentes COSO ERM	Diagnóstico	Durante la fase de diagnóstico, Se ha realizado un análisis de las actividades para recopilación de información de la organización con el fin de recabar datos preliminares e identificar posibles áreas de mejora. Se realizó una encuesta con el propósito de realizar una matriz de diagnóstico preliminar y se evaluó el riesgo y nivel de madurez con el marco de referencia COSO ERM 2017.
Realizar la Evaluación de los activos de información, procesos y niveles de tasación	Ejecución	En esta fase, se ha utilizado la norma ISO 27000 para evaluar los activos de la cooperativa relacionadas con la información

y madurez en la gestión y gobiernos de las TI con base a las normas ISO 27000 y marco de referencia COBIT.		considerando la confidencialidad, integridad y disponibilidad. Además, con la ayuda de los catalizadores de procesos del marco de referencia COBIT, se identificó el nivel de cumplimiento en la gobernanza y gestión de TI para a continuación aplicar un manual de políticas de seguridad de la información permitiendo minimizar los riesgos y amenazas, al tiempo que se desarrolló un plan de contingencia para posibles desastres.
Comunicar los resultados de la aplicación del modelo COBIT enfocados en los controles de la seguridad de la información a través del informe para la toma de decisiones de la alta gerencia.	Comunicación	Una vez concluida la evaluación del control interno y el análisis de los datos, se emitió el informe del auditor con los resultados obtenidos, así como sus respectivas conclusiones y recomendaciones para adoptar medidas correctoras y mejorar la eficiencia y eficacia de las áreas objeto de estudio.

Elaborado por: Freire (2023)

CAPÍTULO III

DESARROLLO

3.1. Resultados

3.1.1. Fase de diagnóstico

En el presente capítulo, se dio el desarrollo del proyecto de titulación en el mismo que se evaluó el nivel de riesgo, confianza y madurez de las áreas de la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda., para ello, se utilizó la metodología COBIT, complementado con otros marcos de referencia para la seguridad de la información y activos identificado vulnerabilidades y riesgos siendo necesario salvaguardar la integridad, confidencialidad y disponibilidad de los datos.

De igual manera se tomaron en cuenta las fases de auditoría, las cuales se utilizaron para el desarrollo del proyecto integrador, con la finalidad de emitir un informe en el cual se especificó las recomendaciones necesarias para elevar los niveles de eficiencia, eficacia de la cooperativa.

Durante la fase de diagnóstico, se ha llevado a cabo una revisión de los activos de información de la organización con el fin de recabar datos preliminares e identificar posibles áreas de mejora. Se aplicó una encuesta con el objetivo, de realizar una matriz de diagnóstico preliminar y se evaluó el riesgo y nivel de madurez y el marco de referencia COSO ERM 2017.

3.1.1.1 Nivel de madurez

Durante el proceso de evaluación se utilizó la matriz de (AUDITOOLS), que proporciona un marco estructurado para analizar en detalle las actividades de cada componente del COSO ERM. Además, para llevar a cabo esta evaluación, se aplicó las herramientas de evaluación de la implantación del COSO ERM 2017.

Este proceso de calificación se realizó asignando puntos en una escala de 0 a 5. Correspondiendo 5 a que la actividad se realiza siempre, 4 indica que se realiza casi siempre, 3 a que se realiza algunas veces, 2 a que se realiza casi nunca, 1 que no se realiza nunca y 0 a que no aplica la actividad.

Esta evaluación se realizó por departamentos, con un análisis detallado de las actividades, para determinar el valor de cada componente, se utilizó un criterio preciso, en el que los puntos obtenidos se dividieron en función de las calificaciones asignadas sobre la sumatoria total. Posteriormente, estos valores se situaron en los márgenes previstos en los criterios de evaluación, proporcionando una representación clara del nivel de madurez alcanzado por departamento.

Tabla 9 Criterios de evaluación

Criterio de calificación del componente	
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: Auditools (2023)

Elaborado por: Freire (2023)

Tabla 10 Descripción de criterios de evaluación

	Descripción de los criterios
EFECTIVO	1. Es posible supervisar y medir el cumplimiento de los lineamientos y tomar medidas cuando los procedimientos del Gobierno Corporativo y Cultura no parezcan estar trabajando apropiadamente 2. Se toman acciones sobre las no conformidades detectadas sobre Gobierno Corporativo 3. Los procesos de Gobierno Corporativo se encuentran bajo un mejoramiento continuo y sirven como fuente de mejores prácticas 4. Formalización de las relaciones de convivencia con los Stakeholders (Accionistas, Distribuidores, Proveedores, Empleados y el Estado) 5. Se hace un seguimiento a las no conformidades del Gobierno Corporativo identificadas por los Auditores 6. La tecnología de información es utilizada de manera integrada para automatizar el flujo de trabajo, proporcionando herramientas para mejorar la calidad y la efectividad de las operaciones y del Gobierno Corporativo.
Cumplimiento Básico Táctico	1. Los procedimientos del Gobierno Corporativo no están documentados, pero se ejecutan en la operación diaria 2. El seguimiento de los procedimientos depende de la iniciativa de cada individuo y es poco probable que las posibles no conformidades sean detectadas 3. No hay un seguimiento permanente por los dueños de los procesos al cumplimiento de los procedimientos del Gobierno Corporativo 4. Inadecuado funcionamiento del Gobierno Corporativo 5. Se usa la automatización y herramienta de una manera limitada o fragmentada del Gobierno Corporativo
En Proceso	1. Los procedimientos de Gobierno Corporativo se encuentran en desarrollo 2. No existe entrenamiento formal en conceptos básicos del Gobierno Corporativo 3. No existe comunicación sobre los procedimientos del Gobierno Corporativo 4. No hay definición de responsabilidades sobre el Gobierno Corporativo a nivel operativo 5. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, las no conformidades son muy probables
Crítico y Reactivo	1. Ausencia total de cualquier procedimiento reconocible de Gobierno Corporativo. La organización ni siquiera ha reconocido la existencia de aspectos que requieren atención 2. No existe ningún tipo de documentación de procesos de Gobierno Corporativo 3. Existen enfoques ad hoc del Gobierno Corporativo que tienden a aplicarse en forma individual y "caso por caso" 4. El enfoque general de la administración es reactivo y no se hace ningún tipo de seguimiento a las no conformidades 5. La entidad no ha reconocido que existe un problema y/o riesgo latente

Fuente: Auditools (2023)

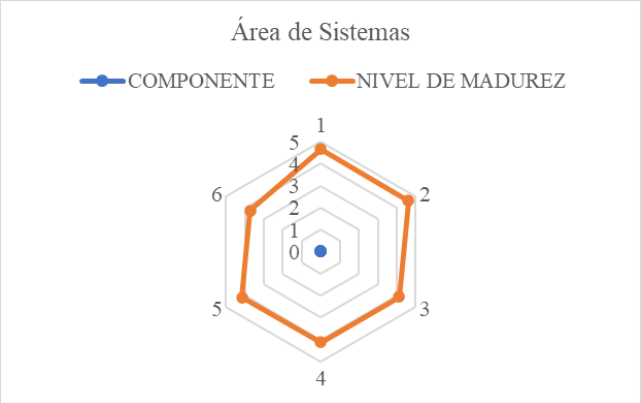
Elaborado por: Freire (2023)

A continuación, se muestra el desarrollo de la fase de diagnóstico, en la que se recopilo toda la información necesaria de la cooperativa para realizar los análisis correspondientes y así conocer la situación actual.

Los resultados obtenidos como diagnóstico del nivel de madurez de los componentes COSO ERM 2017 indica que en el departamento de sistemas el componente gobierno y cultura organizacional tiene un nivel de madurez mayor que corresponde a los 4,67 puntos lo que significa que es efectivo.

No obstante, existe un componente que se encuentra en un estado de cumplimiento básico táctico que es sistema de seguridad de la información con un nivel de madurez de 3,72 puntos lo que representa que existe un inadecuado funcionamiento del gobierno corporativo en cuanto a un correcto seguimiento. Sin embargo, los demás componentes se encuentran en un nivel de proceso adecuado.

Ilustración 10 Nivel de madurez del área de sistemas

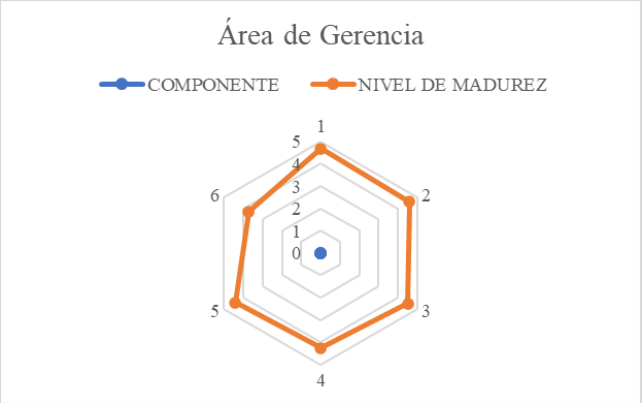


Elaborado por: Freire (2023)

De la misma forma en la ilustración 11 se muestra el nivel de madurez del área de gerencia en donde se observa que el componente gobierno y cultura organizacional tiene un nivel de madurez mayor con una ponderación de 4,67 lo que constituye que se hace un seguimiento a las no conformidades del gobierno corporativo.

Por otro lado, se menciona que también existe un componente que se encuentra en un estado cumplimiento básico táctico que es: sistema de seguridad de la información con un nivel de madurez del 3,72 respectivamente lo que nos indica que no se realiza un correcto seguimiento. Sin embargo, los demás componentes se encuentran en un nivel de proceso adecuado.

Ilustración 11 Nivel de madurez del área de gerencia

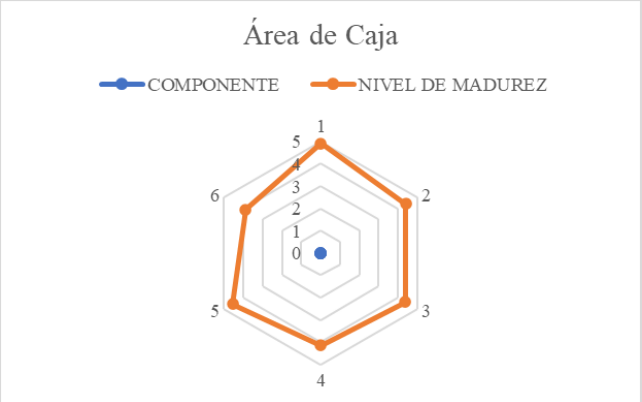


Elaborado por: Freire (2023)

La evaluación del nivel de madurez del área de caja concluyó que el componente gobierno y cultura organizacional presento un mayor índice de madurez con un valor de 4,89 lo que muestra que la empresa realiza un seguimiento indicado por los auditores.

A pesar de esto, se detecta la existencia de un componente en cumplimiento básico táctico, específicamente el sistema de seguridad de la información, con un nivel de madurez de 3,89 lo que indica el inadecuado funcionamiento del gobierno corporativo. Este indicador señala una falta de seguimiento adecuado. Sin embargo, el resto de los componentes muestran un nivel de proceso adecuado.

Ilustración 12 Nivel de madurez del área de caja

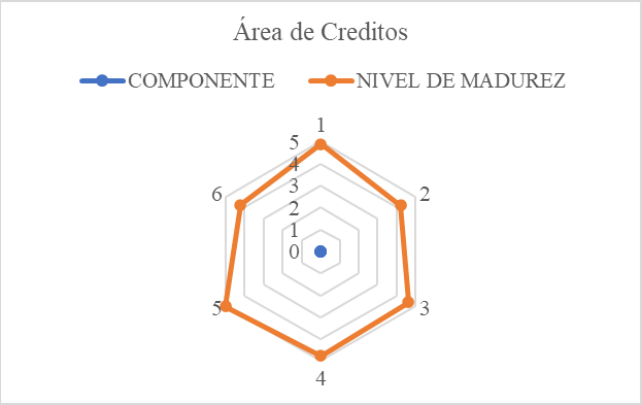


Elaborado por: Freire (2023)

Al evaluar el nivel de madurez en el área de créditos se determinó que el componente sistemas de seguridad de la información obtuvo 3,89 puntos, lo que significa que se encuentra en un nivel de cumplimiento básico táctico debido al

inadecuado funcionamiento del gobierno corporativo en cuanto a este componente, cabe destacar que los demás componentes se encuentran en un nivel efectivo.

Ilustración 13 Nivel de madurez del área de créditos



Elaborado por: Freire (2023)

Asimismo, cuando se examinó la madurez en el sector de atención al cliente, se evidenció que el componente gobierno y cultura organizacional presenta un mayor nivel de madurez con un estimado de 4,44 lo que demuestra que el uso de las tecnologías de información está integrado proporciona herramientas para mejorar la calidad y la eficacia.

Sin embargo, se hace referencia de un componente en fase de cumplimiento básico táctico, concretamente del elemento revisión con un nivel de madurez de 3,38. Este dato sugiere una falta de seguimiento adecuado del componente. Por el contrario, el resto de los elementos presentan un nivel adecuado.

Ilustración 14 Nivel de madurez del área de atención al cliente

Elaborado por: Freire (2023)

El análisis realizado al departamento de captaciones dio como resultado el nivel más alto de madurez en el componente de gobierno y cultura organizacional de 4,78

lo que conlleva que los procesos de gobierno corporativo se encuentran en mejoramiento continuo.

De todos modos, se destaca un componente que se encuentra en un estado de cumplimiento básico táctico el cual es: sistema de seguridad de la información con un valor de 3,83, lo que indica un limitado seguimiento. En cambio, los componentes restantes demuestran un nivel de proceso efectivo.

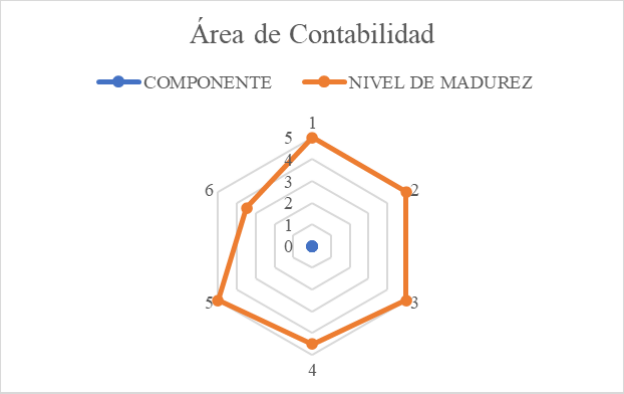
Ilustración 15 Nivel de madurez del área de captaciones

Elaborado por: Freire (2023)

Al evaluar el nivel de madurez en el departamento de contabilidad se observó que varios componentes como gobierno y cultura; estrategias y objetivos; desempeño e información, comunicación y reporte tiene un mayor nivel de madurez con un valor de 5, es decir la tecnología de la información se utiliza para automatizar el flujo de trabajo de forma integrada.

No obstante, se menciona que hay un componente que se encuentra en un nivel de cumplimiento básico táctico que es: sistema de seguridad de la información, que tiene un nivel de madurez de 3,50, lo que implica una falta de supervisión. A pesar de ello, el resto de los componentes se encuentran en un nivel de proceso adecuado.

Ilustración 16 Nivel de madurez del área de contabilidad

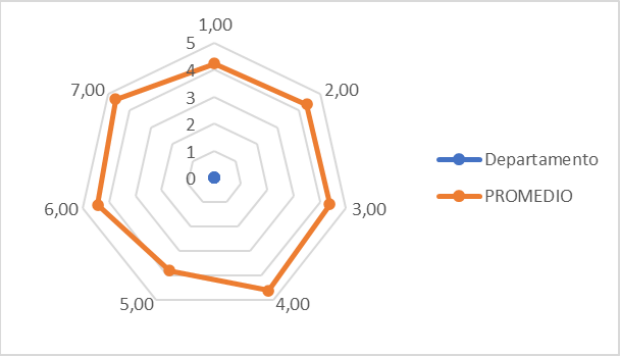


Elaborado por: Freire (2023)

Finalmente, la evaluación total de las siete áreas reveló un buen desempeño, destacando particularmente el departamento de contabilidad con un valor de 4,67 indicando un alto nivel de madurez y eficiencia en los procesos contables.

Por el contrario, el departamento de atención al cliente tiene un valor inferior de 3,81, por lo que fue fundamental enfocarse en reforzar esta área para garantizar una experiencia positiva. Del mismo modo el resto de las áreas evaluadas obtuvieron resultados notables superando el valor de 4,00 por lo que se llegó a concluir la empresa tiene un alto nivel de madurez en su conjunto, evidenciado la efectiva implementación de las prácticas y procesos.

Ilustración 17 Promedio del nivel de madurez



Elaborado por: Freire (2023)

El marco de referencia COSO desempeñó un papel importante al proporcionar un enfoque sistemático para determinar y evaluar de los riesgos de algunos departamentos de la entidad. Por otro lado, Canaza & Torres (2019) menciona que el COSO se presenta como una herramienta que no solo aborda la gestión del riesgo, sino también el sistema de control interno.

Este enfoque centrado en la alta dirección y el personal responsable promueve una cultura de prevención del fraude, protegiendo la integridad de la organización. En particular la revelación de un alto nivel de riesgo debido a la falta de conocimiento sobre medidas para contrarrestar posibles amenazas destaca la necesidad urgente de adoptar medidas preventivas y correctivas (Flores, 2022).

3.2. Fase de ejecución

3.2.1 Norma ISO 27000 evaluación de activos informáticos

En la fase de ejecución, se ha tomado en cuenta la norma ISO 27000 adaptando matrices (HACKMETRIX, s.f.) para la evaluación de activos de la cooperativa relacionadas con la información considerando el nivel de tasación de la confidencialidad, integridad y disponibilidad. Además, con la ayuda de los catalizadores de procesos del marco de referencia COBIT (ISACA, 2012)**,** se identificó el nivel de cumplimiento en la gobernanza y gestión de TI para a continuación aplicar un protocolo de actuación de seguridad de la información permitiendo minimizar los riesgos y amenazas, al tiempo que se desarrolló mejoras a las políticas de seguridad y plan de contingencia para posibles desastres.

El uso de esta norma no permite conocer mejor los activos de la empresa, identificar los más críticos y determinar las medidas de mitigación de riesgo. Los tipos de activos informáticos se evaluaron utilizando los criterios de confidencialidad, integridad y disponibilidad, y se obtuvo el valor promedio del nivel de tasación.

Al evaluar los actos de información de la cooperativa, se decidió concentrarse en las áreas que mantienen una presencia continua en el día a día. Aquellas áreas que se reúnen pero que no mantienen una presencia consistente en la organización fueron excluidas de este análisis. Por lo que fue posible conocer con mayor profundidad y detalle los riesgos asociados a las operaciones normales de la entidad, permitiendo una gestión más eficaz.

Tabla 11 Evaluación de activos de información

GRUPO DE ACTIVOS INFORMÁTICOS	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR	NIVEL DE TASACION	VULNERABILIDAD	AMENAZA	RIESGO
HARDWARE	Equipo de Cómputo	Son equipos electrónicos esenciales que ayudan a procesar, almacenar y gestionar la información. Estas herramientas son esenciales en entornos administrativos para tareas como la navegación web, la creación de documentos, análisis de datos y ejecución de programas.	3	4	4	3,67	ALTO	Contraseñas débiles o que no han sido cambiadas de forma periódica para el acceso al equipo informático.	Acceso no autorizado a los equipo de cómputo por parte de empleados. Instalación de programas maliciosos	Pueden dañar o comprometer la integridad de los datos y sistemas. Acceso a la información confidencial de los programas instalados.
	Impresoras	Son equipos esenciales que convierten la información digital en copias físicas de documentos y desempeñan un papel importante en la producción de informes, prestaciones y material impreso. Sus usos abarcan desde la generación.	3	4	4	3,67	ALTO	Configuraciones inadecuadas de acceso.	Instalación no autorizada del dispositivo en computadoras no requeridas.	Pérdida de funcionalidad de las impresoras afectando la eficiencia operativa.
	Equipo biométrico	Son dispositivos de seguridad que utilizan características únicas como huellas dactilares, estos dispositivos garantizan el acceso controlado a áreas sensibles, sistemas de información o datos confidenciales, eliminando la necesidad de contraseñas convencionales.	4	4	5	4,33	MUY ALTO	Técnicas de cifrado y medidas de bloqueo con limitada configuración.	Se puede comprometer la seguridad del equipo biométrico.	Acceso no autorizado comprometiendo los datos biométricos almacenados.
	Cámaras de vigilancia	Son dispositivos de seguridad que graban imágenes y videos para vigilar y proteger las instalaciones, contribuyen a la prevención de incidentes, la protección de activos y seguridad de los empleados. Además, proporcionan pruebas visuales en caso de sucesos inesperados.	4	5	4	4,33	MUY ALTO	Comunicaciones no cifradas entre cámaras y los sistemas de almacenamiento.	Intentos de acceso por personas no autorizadas a las imágenes capturadas por las cámaras.	La falta de funcionalidad de las cámaras puede tener un impacto negativo en la vigilancia y la seguridad en general.

REDES DE COMUNICACIÓN	Servidor Red compartida	Es un sistema de dispositivos electrónicos interconectados que permite la comunicación y el intercambio de datos entre los distintos departamentos de la entidad.	5	4	4	4,33	MUY ALTO	Configuración incorrecta en los dispositivos de red. No aplicar parches y actualizaciones de seguridad en sistemas operativos, aplicaciones y dispositivos de red.	Intentos de acceso no autorizado a la red compartida por parte de empleados.	Pérdida de datos confidenciales transmitidos a través de la red compartida.
	Router	Es un equipo de red que facilita la conexión y comunicación de varios dispositivos en un entorno específico. Gestiona el flujo de datos, proporciona seguridad mediante y facilita la conectividad para que los empleados puedan acceder eficientemente a recursos en línea.	3	4	4	3,67	ALTO	Contraseñas débiles de autenticación que podrían facilitar el acceso no autorizado.	Modificación no autorizada de la configuración del router.	La ausencia de funcionalidad del router puede perjudicar en la conectividad.
SOFTWARE	Software	Consiste en programas informáticos y aplicaciones diseñados para gestionar y optimizar diversas funciones y procesos internos. Este activo informático es fundamental para aumentar la eficiencia, gestionar datos y facilitar la toma de decisiones.	5	4	5	4,67	MUY ALTO	Falta de actualizaciones de seguridad en el software comprometiendo la integridad de los datos. Falta de capacitación al personal con respecto a las funciones del software.	Acceso no autorizado al software utilitario de la empresa. Modificaciones no autorizada en la base de datos.	Pérdida de datos sensibles almacenados en el sistema.
	Pagina web	Es un espacio digital accesible a través de internet que muestra información o contenidos multimedia. Sirve como plataforma para compartir información, promocionar productos o servicios y facilitar la interacción.	3	4	4	3,67	ALTO	Problemas de seguridad con el software utilizado para crear y mantener el sitio web.	Creación de replicas de la pagina web para engañar a los usuarios y obtener información confidencial.	Proporcionar información desactualizada a los clientes lo que puede afectar en la confianza de la empresa.

PERSONAL POR DEPARTAMENTO DE LA EMPRESA	Sistemas	**Jefe del área:** Ing. Ricardo Mendoza	5	4	4	4,33	MUY ALTO	Limitación en uso de bitácoras de las actividades que realiza el personal en el departamento de sistemas.	Facilidad de engaño de registro de actividades.	Pérdida o manipulación de datos críticos almacenados en el sistema.
	Gerencia	**Jefe del área:** Abg. Fabian Proaño	5	5	5	5,00	MUY ALTO	Ausencia de procedimientos de control y acceso a documentos estratégicos y sensibles.	Divulgación no intencionada de información estratégica.	Pérdida de confianza de los empleados y socios si se revela información crítica o se toma decisiones riesgosas.
	Créditos	**Jefe del área:** Ing. Alexandra Banda	5	4	5	4,67	MUY ALTO	Procesos deficientes en la evaluación de riesgos a clientes que soliciten un crédito	Presentación de documentos falsos o manipulados para obtener créditos.	Incumplimiento de las regulaciones y normativas planteadas por la entidad.
	Caja	**Jefe del área:** Ing. Jenny Masabanda	4	5	4	4,33	MUY ALTO	Procedimientos inadecuados en el manejo, contabilización del efectivo y cierres de caja.	Equivocaciones en el manejo de transacciones que podrían resultar en pérdidas financieras.	Pérdidas económicas debido a robos, fraudes o errores en la gestión del efectivo.
	Atención al cliente	**Jefe del área:** Ing. Anita Rocha	4	4	3	3,67	ALTO	Errores humanos al ingresar la información del cliente comprometiendo la integridad de los datos.	Uso indebido de la información confidencial por parte de los empleados.	La ausencia de ayuda hacia los clientes afectara en la satisfacción y fidelidad de los mismos. Quejas hacia el personal de la empresa provocando una calificación deficiente en su desempeño.

PERSONAL POR DEPARTAMENTO DE LA EMPRESA	Captaciones	**Jefe del área:** Ing. Lady Coba	4	5	5	4,67	MUY ALTO	No aplicar actualizaciones de seguridad en los sistemas utilizados para gestionar las captaciones.	Manipulación de transacciones o creación de cuentas falsas para obtener beneficios.	Pérdida económica debido a prácticas de captación inseguras o fraudes.
	Contabilidad	**Jefe del área:** Ing., Jessica Yanez	4	4	5	4,33	MUY ALTO	Débil seguridad en archivos contables físicos o digitales, que podrían estar expuestos a pérdidas.	Manipulación de registros contables para beneficio personal o de terceros.	Pérdida económica debido a prácticas contables inseguras afectando así la imagen y reputación de la entidad.
	Comité de riesgo	**Encargada del área:** Ing. Diana Muso	5	5	5	5,00	MUY ALTO	Limitaciones en recursos humanos, financieros o tecnológicos, que puede afectar a la capacidad del comité para llevar a cabo evaluaciones exhaustivas.	Falta de trasparencia de la información facilitada al comité, que podría distorcionar la percepción del riesgo real.	Toma de decisiones poco eficaces basadas en evaluaciones de riesgos incompletas por parte del comité.
	Comité de cumplimiento	**Encargada del área:** Ing. Amparito Travez	5	4	4	4,33	MUY ALTO	Falta de conocimiento detallado de los reglamentos y normas específicos que afectan a la empresa.	Falta de apoyo de otras áreas de la empresa para colaborar plenamente con el comité de cumplimiento.	Miebros del consejo que carecen de conocimientos especializados en las áreas relevantes de cumplimiento.
	Asesor jurídico	**Jefe del área:** Ing. Dani Almachi	3	3	3	3,00	MEDIO	Falta de seguimiento constante de cambios en la legislación.	Conflictos de intereses que pueden surgir entre los intereses de la empresa y los intereses de los abogados de la empresa.	Gestión ineficiente de documentos legales que podrían resultar en la pérdida de información crucial

Elaborado por: Freire (2023)

3.2.1.1 Evaluación de prioridad

Esta evaluación del riesgo se realizó minuciosamente utilizando criterios específicos, como se indica en cuadro siguiente. Durante este proceso se tuvieron en cuenta diversos factores, como la probabilidad de ocurrencia y el impacto del riesgo.

Tabla 12 Criterios de medición del riesgo

Medición del Riesgo	
Muy alto 5	Mayor o igual que 20
Alto 4	Mayor o igual que 10 y menor que 20
Medio 3	Mayor o igual que 5 y menor que 10
Moderado 2	Mayor o igual que 3 y menor que 5
Bajo 1	Menor que 3

Elaborado por: Freire (2023)

En la tabla 13, entre los activos de información algunos más vulnerables o propensos a sufrir ataques pertenecen a los niveles de riesgo medio y alto. Se trata de equipos de cómputo, cámaras de vigilancia, servidores, router y software. Estos elementos tecnológicos son importantes para el funcionamiento eficiente de la entidad, pero su naturaleza digital los hace susceptibles a amenazas o vulnerabilidades de seguridad.

Además, áreas específicas de la organización, como crédito, caja, servicio al cliente y contabilidad, son fundamentales para el flujo operativo y financiero. Estas áreas pueden ser objeto de amenazas como el fraude interno o externo, el robo de datos financieros o la interrupción de los procesos contables.

El comité de cumplimiento y el asesor jurídico, además de ser responsables de garantizar que la organización cumpla con las normas y reglamentos, pueden estar expuestos a amenazas legales y reglamentarias. El incumplimiento puede acarrear importantes sanciones o pérdidas financieras.

Tabla 13 Evaluación de la prioridad

Riesgo		Criterios para Evaluaar la Importancia del Riesgo						
Activos	**Riesgos**	**Medición del Riesgo**	**Impacto Económico**	**Tiempo de recuperación**	**Probabilidad de Ocurrencia**	**Probabilidad de interrumpir actividades**	**TOTAL**	**Priorizacion de Riesgo**
Equipo de Cómputo	Pueden dañar o comprometer la integridad de los datos y sistemas.	9	4	3	2	3	3	2
	Acceso a la información confidencial de los programas instalados.	4	3	2	2	1	2	1
Impresoras	Pérdida de funcionalidad de las impresoras afectando la eficiencia operativa.	2	3	2	2	3	3	2
Equipo biométrico	Acceso no autorizado comprometiendo los datos biométricos almacenados.	4	2	2	1	1	2	1
Cámaras de vigilancia	La falta de funcionalidad de las cámaras puede tener un impacto negativo en la vigilancia y la seguridad en general.	6	2	2	2	1	2	1
Servidor/Red compartida	Pérdida de datos confidenciales transmitidos a través de la red compartida.	6	3	3	2	2	3	2
Router	La ausencia de funcionalidad del router puede perjudicar en la conectividad.	6	3	3	3	4	3	2
Software	Pérdida de datos sensibles almacenados en el sistema.	9	4	3	2	3	3	2
Pagina web	Proporcionar información desactualizada a los clientes lo que puede afectar en la confianza de la empresa.	2	4	3	3	3	3	2

Sistemas	Pérdida o manipulación de datos críticos almacenados en el sistema.	4	4	4	3	4	4	2
Gerencia	Pérdida de confianza de los empleados y socios si se revela información crítica o se toma decisiones riesgosas.	3	4	3	3	4	4	2
Créditos	Incumplimiento de las regulaciones y normativas planteadas por la entidad.	6	4	3	3	4	4	2
Caja	Pérdidas económicas debido a robos, fraudes o errores en la gestión del efectivo.	5	4	3	3	3	3	2
Atención al cliente	La ausencia de ayuda hacia los clientes afectará en la satisfacción y fidelidad de los mismos.	9	4	3	1	3	3	2
	Quejas hacia el personal de la empresa provocando una calificación deficiente en su desempeño.	12	4	3	3	3	3	2
Captaciones	Pérdida económica debido a practicas de captación inseguras o fraudes.	4	1	3	3	3	3	2
Contabilidad	Pérdida económica debido a practicas contables inseguras afectando así la imagen y reputación de la entidad.	10	3	2	2	2	2	1
Comité de riesgo	Toma de decisiones poco eficaces basadas en evaluaciones de riesgos incompletas por parte del comité.	4	3	3	2	2	3	2
Comité de cumplimiento	Miembros del consejo que carecen de conocimientos especializados en las áreas relevantes de cumplimiento.	6	4	3	2	3	3	2
Asesor jurídico	Gestión ineficiente de documentos legales que podrían resultar en la pérdida de información crucial.	9	3	2	3	2	3	2

Elaborado por: Freire (2023)

3.2.2 Aplicación del marco de referencia COBIT

Para medir el nivel de acuerdo existen varios tipos de formatos, sin embargo, el que mejor se adapta y alinea con el modelo COBIT es el de tipo Likert, como se indica a continuación:

Tabla 14 Criterios de evaluación del nivel de acuerdo

Nivel de acuerdo	Valor de cumplimiento
Completamente	5
Bastante	3-4
Un poco	2
De ningún modo	0-1

Fuente: Adaptación de Pederiva (2003)

Elaborado por: Freire (2023)

Al aplicar el marco de referencia COBIT, se llevó a cabo una evaluación en la que se utilizó la metodología recomendada por ISACA. Este marco de referencia se centra en la gobernanza y la gestión de las tecnologías de la información, y su aplicación es crucial para alinear los objetivos de TI estén alineados con los objetivos de la entidad. A continuación, se muestra en detalle la tabla de evaluación:

Tabla 15 Niveles de madurez para procesos COBIT

NIVEL	DESCRIPCIÓN	CARACTERÍSTICAS
0	Incompleto	Falta de cualquier capacidad básica, estrategia incompleta la intención de todas las practicas de proceso no están definidas o no existe.
1	Ejecutado	El proceso logra mas o menos un propósito atreves de la aplicación de un conjunto de actividades incompleto que pueden caracterizarse como inicial o intuitiva, no muy organizada.
2	Administrado	El proceso logra su propósito atreves de la aplicación de un conjunto de actividades básicas pero completas que pueden caracterizarse como realizadas.
3	Establecido	El proceso logra su propósito de forma mucho mas organizada usando activos para la organización los procesos están bien definidos.
4	Predecible	El proceso logra su propósito esta bien definido y su rendimiento se mide de forma cuantitativa.
5	Optimizado	El proceso logra su propósito esta bien definido su rendimiento mide para mejorar su desempeño y se persigue la mejora continua.

Fuente: ISACA (2012)

Elaborado por: Freire (2023)

Además, en dichos procesos se utilizó criterios de evaluación de cumplimiento que debe tener la entidad por cada actividad, esta valoración se llevó a cabo de acuerdo con las directrices y normas ISO 15504.

Tabla 16 Niveles de capacidad de procesos normas ISO 15504

SIGLA	DESCRIPCIÓN	VALORACIÓN %	NIVELES DE CAPACIDAD
F	Completamente	>85-100%	5
L	En gran medida	>50-85%	3-4
P	Parcialmente	>15-50%	2
N	No cumple	0-15%	0-1

Fuente: Alarcón et al. (2011)

Elaborado por: Freire (2023)

Se llevó a cabo un proceso de selección de los procesos COBIT más relevantes para la evaluación, en colaboración con el jefe del área de sistemas de la cooperativa. Este proceso se basó en un Check list detallado para identificar las áreas que debían abordarse. En lugar de incluir todos los catalizadores, sólo se eligieron cuidadosamente aquellos que tenían un impacto significativo en la mejora y optimización de las operaciones de la cooperativa.

Los resultados detallados de este proceso de selección se incluyen en el Anexo 5 de este documento. Este enfoque permitió una identificación precisa y fundamentada de los procesos que necesitaban una priorización, con el objetivo de mejorar tanto la eficiencia y eficacia en el gobierno y gestión de las TI utilizadas en las operaciones de la cooperativa.

Una vez evaluadas las actividades de los distintos dominios del marco de referencia COBIT, se procedió a una evaluación adicional centrada en la madurez. Esta etapa es fundamental para comprender la capacidad de la cooperativa para gestionar y regular eficazmente sus procesos.

3.2.2.1 Evaluar, Orientar y Supervisar (EDM)

Como se observa en la tabla 17, se puede determinar que la práctica clave EDM03.01 Evaluar la gestión del riesgo muestra que las actividades 1 y 5 poseen un porcentaje del 50% lo que se puede decir que los procesos alcanzan su propósito mediante la aplicación de actividades esenciales pero completas que se diferencia por la forma en que se llevan a cabo.

Así mismo, las actividades 2 y 4 se encuentran en un nivel L lo que nos quiere decir que estos procesos logran su propósito ya que se encuentran bien definidos y su funcionamiento se mide cuantitativamente. Por otro lado, las actividades 3 y 6 son las que muestran un valor elevado a lo esperado con un valor de 90% dando a entender que el proceso está claramente definido para obtener el resultado deseado.

Tabla 17 EDM03.01 Evaluar la gestión de riesgos

EDM03.01 EVALUAR LA GESTIÓN DE RIESGOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		71%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	2		50%			50%	L	No cumple
2	3			65%		65%	L	Si cumple
3	5				90%	90%	L	Si cumple
4	4			80%		80%	L	Si cumple
5	2		50%			50%	L	No cumple
6	5				90%	90%	L	Si cumple
					PROMEDIO	71%		

Elaborado por: Freire (2023)

Así mismo como se muestra en la tabla 18 al evaluar los niveles de madurez se pudo determinar que la segunda actividad se encuentra en un nivel predecible ya que la cooperativa tiene su propósito bien definido de dicho proceso, incluso su rendimiento se mide de manera cuantitativa.

Sin embargo, la actividad 3 se encuentra con un nivel de capacidad de 3 puntos dando como resultado que este procesó se realice en gran medida. Por otro lado, las demás actividades presentaron un nivel de capacidad optimizado es decir que los procesos cumplen con su propósito y se persigue la mejora continua

Tabla 18 EDM03.02 Orientar la gestión de riesgos

EDM03.02 ORIENTAR LA GESTIÓN DE RIESGOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		85%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	4			80%		80%	F	Si cumple
3	3			70%		70%	F	Si cumple
4	5				90%	90%	F	Si cumple
5	5				90%	90%	F	Si cumple
6	5				90%	90%	F	Si cumple
					PROMEDIO	85%		

Elaborado por: Freire (2023)

Según indican estos datos se pudo evidenciar que las actividades del proceso que se muestra en la tabla 19 se cumplen adecuadamente con un valor del 90% ya que sus propósitos se encuentran muy bien definidos, su rendimiento ayuda a mejorar su desempeño y se persigue la mejora continua. Sin embargo, la actividad 2 posee un valor del 70% es decir que esta actividad se realiza en gran medida logrando su objetivo mediante la aplicación de una serie de actividades básicas pero completas.

Tabla 19 EDM03.03 Supervisar la gestión de riesgos

EDM03.03 SUPERVISAR LA GESTIÓN DE RIESGOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		85%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	3			70%		70%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	5				90%	90%	F	Si cumple
					PROMEDIO	85%		

Elaborado por: Freire (2023)

Así mismo al evaluar las actividades correspondientes al EDM05.01 se pudo observar que una de las actividades específicas no cumple con la meta establecida, ya que esta actividad tiene un rendimiento del 50%. A pesar de que el proceso en su conjunto alcanzara su objetivo mediante la ejecución de actividades básicas que se puede caracterizar como realizadas.

Tabla 20 EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas

EDM05.01 EVALUAR LOS REQUERIIENTOS DE ELABORACIÓN DE INFORMES DE LAS PARTES INTERESADAS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		63%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			80%		70%	L	Sicumple
2	2		50%			50%	L	No cumple
3	3			75%		70%	L	Sicumple
					PROMEDIO	63%		

Elaborado por: Freire (2023)

De igual manera en el proceso EDM05.02, concretamente en las actividades de orientación de la comunicación con las partes interesadas y elaboración de informes, se observa que dos de ellas no alcanzan la meta establecida, lo que se refleja un rendimiento del 50%. Esta situación puede atribuirse a diversos factores, como la falta de claridad en los protocolos de comunicación, la faltan de recursos suficientes o una planificación insuficiente.

Tabla 21 EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes

EDM05.02 ORIENTAR LA COMUNICACIÓN CON LAS PARTES INTERESADAS Y LA ELABORACIÓN DE INFORMES

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		65%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	2		50%			50%	L	No cumple
2	4			80%		80%	L	Si cumple
3	4			80%		80%	L	Si cumple
4	2		50%			50%	L	No cumple
					PROMEDIO	65%		

Elaborado por: Freire (2023)

El proceso EDM05.03 relacionado con la supervisión de la comunicación con las partes interesadas, está claro que ninguna de las actividades cumple con la meta, ya que todas tienen un porcentaje de cumplimiento del 50%. Dicha situación puede deberse a una serie de factores, como la falta de un sistema de supervisión eficaz, la ausencia de indicadores clave de rendimiento.

Tabla 22 Supervisar la comunicación con las partes interesadas

EDM05.03 SUPERVISAR LA COMUNICACIÓN CON LAS PARTES INTERESADAS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
	50%				

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	2		50%			50%	L	No cumple
2	2		50%			50%	L	No cumple
3	2		50%			50%	L	No cumple
					PROMEDIO	50%		

Elaborado por: Freire (2023)

Por otro lado, se han identificado dos actividades en el proceso APO02.01 referente a comprender la dirección de la empresa, no alcanzan los niveles de ejecución deseados. Una de estas actividades tiene un porcentaje del 75% mientras que la otra tiene un porcentaje del 80%. A pesar de que ambas actividades se llevan a cabo, la ineficiencia puede explicar la desproporción.

3.2.2.2 Alinear, Planificar y Organizar (APO)

Tabla 23 APO02.01 Comprender la dirección de la empresa

APO02.01 COMPRENDER LA DIRECCIÓN DE LA EMPRESA

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			86%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	5				90%	90%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	5				90%	90%	F	Si cumple
5	3			75%		75%	F	No cumple
6	4			80%		80%	F	No cumple
					PROMEDIO	86%		

Elaborado por: Freire (2023)

Así mismo al evaluar el proceso APO02.02 referente a evaluar el entorno, capacidades y rendimientos actuales, destaca una actividad que posee un valor del 90%b es decir que cumple con la meta establecida. Sin embargo, las otras actividades a pesar de que se realizan no llegan a tener un nivel óptimo. Esto se puede dar debido a la falta de recursos, herramientas de análisis o personal capacitado afectando en su eficiencia.

Tabla 24 APO02.02 Evaluar el entorno, capacidades y rendimientos actuales

APO02.02 EVALUAR EL ENTORNO, CAPACIDADES Y RENDIMINEOT ACTUALES

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		78%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			80%		80%	F	No cumple
2	3			70%		70%	F	No cumple
3	3			70%		70%	F	No cumple
4	5				90%	90%	F	Si cumple
					PROMEDIO	78%		

Elaborado por: Freire (2023)

En el proceso APO02.03, centrada en la definición de los objetivos de las capacidades de TI, cabe destacar que solo una actividad alcanza la meta fijada, con un notable porcentaje de éxito del 90%. En cambio, las demás actividades presentan una realización parcial y requieren acciones específicas para alcanzar la meta deseada. Es posible que sea necesario mejorar la organización de los equipos o utilizar prácticas más eficientes en la planificación y ejecución de estas actividades.

Tabla 25 APO02.03 Definir el objetivo de las capacidades de TI

APO02.03 DEFINIR EL OBJETIVO DE LAS CAPACIDADES DE TI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		70%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	3			70%		70%	F	No cumple
3	4			75%		75%	F	No cumple
4	4			75%		75%	F	No cumple
5	2		45%			45%	F	No cumple
6	3			65%		65%	F	No cumple
					PROMEDIO	70%		

Elaborado por: Freire (2023)

Al analizar el proceso APO02.04 centrado en la realización de análisis de diferencias, es evidente que ninguna de las actividades alcanza la meta fijada, con un porcentaje inferior al 80%. A pesar de realizar las actividades planificadas, no se alcanza la eficiencia deseada. Es fundamental establecer un sistema de seguimiento continuo que permita detectar y gestionar proactivamente cualquier desviación en el rendimiento.

Tabla 26 APO02.04 Realizar un análisis de diferencias

APO02.04 REALIZAR UN ANÁLISIS DE DIFERENCIAS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		66%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	2		50%			50%	F	No cumple
2	4			75%		75%	F	No cumple
3	3			70%		70%	F	No cumple
4	3			70%		70%	F	No cumple
					PROMEDIO	66%		

Elaborado por: Freire (2023)

Una vez evaluado las actividades del proceso APO02.05, dedicado a la formulación del plan estratégico y la hoja de ruta, cabe destacar que las actividades se están desarrollando correctamente, cumpliendo en gran medida los objetivos establecidos.

Sin embargo, para alcanzar plenamente con las metas fijadas, es necesario identificar áreas de mejora. Es por ello por lo que se debe centrar los esfuerzo en la actualización continua de la información estratégica, garantizando la alineación con los cambios en el entorno empresarial. Además, la participación de las principales partes interesadas en el desarrollo del plan estratégico y la hoja de ruta puede potenciar aún más su eficiencia.

Tabla 27 APO02.05 Definir el plan estratégico y la hoja de ruta

APO02.05 DEFINIR EL PLAN ESTRATÉGICO Y LA HOJA DE RUTA

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		75%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	4			75%		75%	F	No cumple
3	3			70%		70%	F	No cumple
4	4			80%		80%	F	No cumple
5	4			80%		80%	F	No cumple
6	4			75%		75%	F	No cumple
7	4			75%		75%	F	No cumple
					PROMEDIO	75%		

Elaborado por: Freire (2023)

Según los resultados obtenidos después de valor el proceso APO02.06, orientado a la comunicación de la estrategia y la dirección de TI, se observa que las actividades presentan un nivel óptimo. Para ello puede ser necesario reevaluar los métodos de comunicación, además de implementar un sistema de seguimiento. Sin embargo, se identifica que una actividad alcanza la meta establecida, es decir el propósito del proceso está bien establecido y se persigue la mejora continua.

Tabla 28 APO02.06 Comunicar la estrategia y la dirección de TI

APO02.06 COMUNICAR LA ESTRATEGIA Y LA DIRECCIÓN DE TI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		78%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	4			75%		75%	F	No cumple
3	3			70%		70%	F	No cumple
4	4			75%		75%	F	No cumple
					PROMEDIO	78%		

Elaborado por: Freire (2023)

Al evaluar el proceso APO13.01 centrado en establecer y mantener un sistema de gestión de la seguridad de la información, se observó que la mayoría de las actividades realizadas cumplen con las metas establecidas. Este análisis permitió constatar que dichos procesos se llevan a cabo con eficiencia y eficacia. Sin embargo, es fundamental destacar que dos actividades no cumplen con la meta, con un porcentaje del 50%. Este bajo rendimiento puede atribuirse a diversos factores, como la ausencia de procedimientos adecuados.

Tabla 29 APO13.01 Establecer y mantener un SGSI

APO13.01 ESTABLECER Y MANTENER UN SGSI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		63%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			65%		65%	L	Si cumple
2	3			65%		65%	L	Si cumple
3	3			70%		70%	L	Si cumple
4	3			70%		70%	L	Si cumple
5	2		50%			50%	L	No cumple
6	3			70%		70%	L	Si cumple
7	2		50%			50%	L	No cumple
					PROMEDIO	63%		

Elaborado por: Freire (2023)

Tras una evaluación exhaustiva del proceso APO13.02 se constató que las actividades cumplen las metas fijadas. Este análisis revela un nivel satisfactorio de eficiencia en la ejecución de los procesos relacionados con la definición y gestión de estrategias de seguridad de la información, demostrando un compromiso con las normas establecidas, garantizando una aplicación eficaz del plan de gestión de riesgos.

Tabla 30 APO13.02 Definir y gestionar un plan de tratamiento del riesgo y seguimiento de la información

APO13.02 DEFINIR Y GESTIONAR UN PLAN DE TRATAMIENTO DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		76%			

ACTIVIDADES	NIVELES DE CAPACIDAD/OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			80%		80%	L	Si cumple
2	3			70%		70%	L	Si cumple
3	4			75%		75%	L	Si cumple
4	4			85%		85%	L	Si cumple
5	3			70%		70%	L	Si cumple
6	3			70%		70%	L	Si cumple
7	4			80%		80%	L	Si cumple
					PROMEDIO	76%		

Elaborado por: Freire (2023)

Al realizar una breve evaluación del proceso APO113.03 se identificó que tres de las actividades evaluadas no alcanzan la meta establecida, es decir poseen un índice de cumplimiento del 50%. Por otro lado, es importante resaltar que dos de las actividades cumplen satisfactoriamente la meta fijada, demostrando que existen elementos positivos en la ejecución de algunos aspectos del proceso.

Tabla 31 APO13.03 Supervisar y revisar el SGSI

APO13.03 SUPERVISAR Y REVISAR EL SGSI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		60%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	2		50%			50%	L	No cumple
2	2		50%			50%	L	No cumple
3	2		50%			50%	L	No cumple
4	4			80%		80%	L	Si cumple
5	3			70%		70%	L	Si cumple
					PROMEDIO	60%		

Elaborado por: Freire (2023)

3.2.2.3 Construir, Adquirir e Implementar (BAI)

Tras una valoración del proceso BAI08.01, se ha determinado que, a pesar de llevar a cabo todas las actividades previstas, el grupo no alcanza la meta prevista. Sin embargo, es de interés señalar que una de estas actividades destaca por su óptima ejecución. La diferencia de resultados puede atribuirse a varios motivos, entre ellos una posible falta de alineación entre las actividades y los objetivos, así como la necesidad de revisar y ajustar los procedimientos.

Tabla 32 BAIO8.01 Cultivar y facilitar una cultura de intercambio de conocimientos

BAI08.01 CULTIVAR Y FACILITAR UNA CULTURA DE INTERCAMBIO DE CONOCIMIENTOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		82%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	4			75%		75%	F	No cumple
3	4			80%		80%	F	No cumple
4	4			80%		80%	F	No cumple
5	2		50%			50%	F	No cumple
					PROMEDIO	82%		

Elaborado por: Freire (2023)

Una vez evaluado los niveles de cumplimiento del proceso BAI08.02 se ha podido observar de forma positiva que todas las actividades llevadas a cabo cumplen con las metas fijadas. Este rendimiento eficiente puede deberse a una serie de factores interconectados que contribuyen al éxito del proceso.

Este resultado favorable no solo valida la eficacia del proceso, sino que también resalta la importancia de una gestión proactiva y unos objetivos bien estructurados para lograr resultados optimizados.

Tabla 33 BAI08.02 Identificar y clasificar las fuentes de información

BAI08.02 IDENTIFICAR Y CLASIFICAR LAS FUENTES DE INFORMACIÓN

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		75%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			75%		75%	L	Si cumple
2	4			80%		80%	L	Si cumple
3	3			70%		70%	L	Si cumple
4	4			85%		85%	L	Si cumple
					PROMEDIO	75%		

Elaborado por: Freire (2023)

Al realizar una evaluación detallada del proceso BAI08.03, dirigida a actividades específicas, se identificó que dos de las actividades no alcanzan los objetivos establecidos, con un valor del 70% a pesar de realizar dichas actividades lo que indica un rendimiento inferior al esperado.

Este bajo rendimiento puede deberse a la necesidad de revisar y optimizar los métodos utilizados. Por otro lado, es notable que dos de las actividades cumplan con las metas, lo que indica que hay aspectos positivos en la ejecución de determinados componentes del proceso.

Tabla 34 BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento

BAI08.03 ORGANIZAR Y CONTEXTUALIZAR LA INFORMACIÓN, TRANSFORMÁNDOLA EN CONOCIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		77%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	3			70%		70%	F	No cumple
3	3			70%		70%	F	No cumple
4	5				90%	90%	F	Si cumple
					PROMEDIO	77%		

Elaborado por: Freire (2023)

Después de una evaluación detallada del proceso BAI08.04 se pudo decir que todas las actividades planificadas cumplen eficazmente con las metas fijadas, lo que se refleja un rendimiento satisfactorio. Este resultado positivo apunta a una aplicación eficaz de los procedimientos, una asignación adecuada de los recursos y un enfoque estratégico que se ajusta a los objetivos previamente fijados.

Tabla 35 BAI08.04 Utilizar y compartir el conocimiento

BAI08.04 UTILIZAR Y COMPARTIR EL CONOCIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		77%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	L	Si cumple
2	4			80%		80%	L	Si cumple
3	4			80%		80%	L	Si cumple
					PROMEDIO	77%		

Elaborado por: Freire (2023)

La cooperativa lleva a cabo las actividades asociadas al proceso BAI08.05, sin embargo, existe un desajuste significativo entre su rendimiento actual y la meta fijada. Este desnivel, que puede atribuirse a la falta de recursos adecuados, tanto humanos como financieros, puede estar limitando la eficiencia de las operaciones.

Tabla 36 BAI08.05 Evaluar y retirar la información

BAI08.05 EVALUAR Y RETIRAR LA INFORMACIÓN

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		70%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
					PROMEDIO	70%		

Elaborado por: Freire (2023)

Al analizar detenidamente las actividades del proceso BAI09,01, centrado en la identificación y registro de las actividades en curso, se descubrió que estas presentan un nivel de capacidad óptimo. Este desempeño garantiza que las actividades cumplan las metas previstas de manera eficaz y eficiente. Este resultado es positivo, ya que garantiza una gestión sólida y fiable de las actividades, contribuyendo a la seguridad y eficacia de los procesos de la organización.

Tabla 37 BAI09.01 Identificar y registrar activos actuales

BAI09.01 IDENTIFICAR Y REGISTRAR ACTIVOS ACTUALES

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			93%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	5				95%	95%	F	Si cumple
3	5				95%	95%	F	Si cumple
4	5				95%	95%	F	Si cumple
5	5				95%	95%	F	Si cumple
6	5				95%	95%	F	Si cumple
					PROMEDIO	93%		

Elaborado por: Freire (2023)

A pesar de la ejecución de las actividades del proceso BAI09.02, encargado de gestionar los activos críticos, se enfrenta a importantes retos. Incluso cuando las acciones se lleven a cabo con la intención de alcanzar la meta establecida, en ocasiones los resultados pueden no estar a la altura de las expectativas. Esto podría atribuirse a una serie de factores, como la complejidad de los activos críticos, la variabilidad de las condiciones operativas.

Tabla 38 BAI09.02 Gestionar activos críticos

BAI09.02 GESTIONAR ACTIVOS CRITICOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		82%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	5				90%	90%	F	Si cumple
3	4			85%		85%	F	No cumple
4	3			70%		70%	F	No cumple
5	3			70%		70%	F	No cumple
6	3			65%		65%	F	No cumple
7	3			70%		70%	F	No cumple
8	5				90%	90%	F	Si cumple
9	3			70%		70%	F	No cumple
					PROMEDIO	82%		

Elaborado por: Freire (2023)

De igual manera al evaluar las actividades del proceso BAI09.03 se determinó que cada una de ellas tiene un valor adecuado, lo que garantiza que se cumplan con éxito las metas fijadas. Este resultado positivo demuestra la eficiencia y eficacia en la planificación y ejecución de las actividades.

La correcta alineación de los recursos, la atención a los detalles y la coordinación eficaz entre los equipos implicados son factores que contribuyeron a alcanzar el objetivo.

Tabla 39 BAI09.03 Gestionar el ciclo de vida de los activos

BAI09.03 GESTIONAR EL CICLO DE VIDA DE LOS ACTIVOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			92%		

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	L	Si cumple
2	5				90%	90%	L	Si cumple
3	5				90%	90%	L	Si cumple
4	4			85%		85%	L	Si cumple
5	5				90%	90%	L	Si cumple
6	3			70%		70%	L	Si cumple
7	5				90%	90%	L	Si cumple
8	5				90%	90%	L	Si cumple
9	3			70%		70%	L	Si cumple
					PROMEDIO	92%		

Elaborado por: Freire (2023)

Dentro del proceso BAI09.04 diseñado específicamente para la optimizar el coste de los activos, se ha detectado que tres de sus actividades funcionan actualmente con bajo nivel de capacidad. Esta situación es atribuible a múltiples factores, entre ellos la falta de alineación estratégica en la asignación de recursos financieros y tecnológicos. La falta de conocimiento detallado de las actividades por parte del personal involucrado.

Tabla 40 BAI09.04 optimizar coste de los activos

BAI09.04 OPTIMIZAR EL COSTE DE LOS ACTIVOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		67%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			80%		80%	L	Si cumple
2	3			70%		70%	L	Si cumple
3	2		50%			50%	L	No cumple
4	2		50%			50%	L	No cumple
5	2		50%			50%	L	No cumple
6	3			70%		70%	L	Si cumple
					PROMEDIO	67%		

Elaborado por: Freire (2023)

En el caso del proceso BAI09.05, se ha observado que, por lo general, las actividades alcanzan un nivel de capacidad medio, lo que indica que se lleva a cabo en gran medida, pero aún presentan oportunidades para mejorar su eficiencia.
Sin embargo, cabe destacar una actividad concreta que se realiza de forma adecuada alcanzando un nivel óptimo. Esta ejecución puede atribuirse a una combinación de factores, como el uso de las Prácticas más apropiadas y la dedicación del personal implicado.

Tabla 41 BAI09.05 Administrar licencias

BAI09.05 ADMINISTRAR LICENCIAS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		82%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	4			85%		85%	F	No cumple
3	5				90%	90%	F	Si cumple
4	3			70%		70%	F	No cumple
5	3			70%		70%	F	No cumple
6	2		50%			50%	F	No cumple
					PROMEDIO	82%		

Elaborado por: Freire (2023)

3.2.2.4 Entregar, Servicio y Soporte (DSS)

Cabe destacar que al analizar las actividades del proceso DSS01.01 se determinó que la mayoría alcanza con un nivel óptimo, cumpliendo así con el objetivo establecido. No obstante, a pesar de su atenta ejecución, dos de las actividades demuestran un nivel medio de capacidad. Este hecho puede atribuirse a diversos factores, entre ellos la necesidad de actualizar los recursos.

Tabla 42 DSS01.01 Ejecutar procedimientos operativos

DSS01.01 EJECUTAR PROCEDIMIENTOS OPERATIVOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		77%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
3	5				90%	90%	F	Si cumple
4	5				90%	90%	F	Si cumple
5	5				90%	90%	F	Si cumple
					PROMEDIO	77%		

Elaborado por: Freire (2023)

Al analizar el proceso DSS1.02 cabe destacar el alto nivel de eficacia que caracteriza a la mayoría de sus actividades, que alcanzan sistemáticamente el objetivo fijado, es decir el proceso logra su propósito ya que se encuentra bien definido y buscando la mejora continua. No obstante, es crucial destacar que, a pesar de esto una actividad especifica se enfrenta a diversos aspectos para alcanzar el objetivo establecido.

Tabla 43 DSS01.02 Gestionar servicios externalizados de TI

DSS01.02 GESTIONAR SERVICIOS EXTERNALIZADOS DE TI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		83%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	5				90%	90%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	5				90%	90%	F	Si cumple
					PROMEDIO	83%		

Elaborado por: Freire (2023)

Después de una evaluación más detallada de las actividades relacionadas con el proceso DSS01.03, se descubrió que la mayoría de ellas lograron superar la meta establecida, demostrando un rendimiento satisfactorio en general. Sin embargo, se observó que una determinada actividad presentó un nivel de capacidad significativamente bajo, lo que impidió la obtención de la meta prevista.

Tabla 44 DSS01.03 supervisar la infraestructura de TI

DSS01.03 SUPERVISAR LA INFRAESTRUCTURA DE TI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85 %	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		72%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	L	Si cumple
2	4			80%		80%	L	Si cumple
3	3			65%		65%	L	Si cumple
4	5				90%	90%	L	Si cumple
5	3			70%		70%	L	Si cumple
6	2		50%			50%	L	No cumple
					PROMEDIO	72 %		

Elaborado por: Freire (2023)

Tras una evaluación exhaustiva de las actividades incluidas en el proceso DSS01.04, se determinó que una de las actividades no cumplía con la meta prevista, mostrando un nivel de capacidad notablemente bajo. A pesar de este inconveniente, es positivo constatar que las demás actividades superaron el 80%, lo que indica un rendimiento superior.

Tabla 45 DSS01.04 Gestionar el entorno

DSS01.04 GESTIONAR EL ENTORNO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			95%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	L	Si cumple
2	5				95%	95%	L	Si cumple
3	5				95%	95%	L	Si cumple
4	5				90%	90%	L	Si cumple
5	4			85%		85%	L	Si cumple
6	2		50%			50%	L	No cumple
7	4			85%		85%	L	Si cumple
8	5				95%	95%	L	Si cumple
					PROMEDIO	95%		

Elaborado por: Freire (2023)

A partir de una breve evaluación de las actividades dentro del proceso DSS01.05, se constató que, si bien la mayoría de las actividades no alcanzaron a cumplir con la meta establecida, esto no implica que no se estén llevando a cabo. De hecho, estas actividades demuestran un alto nivel de proceso, lo que indica que sí, bien el objetivo aún no se ha cumplido en su totalidad, se está avanzando. Por otro lado, cabe señalar que las demás actividades alcanzaron la meta establecida, superando un rendimiento satisfactorio.

Tabla 46 DSS01.05 Gestionar las instalaciones

BAI09.05 GESTIONAR LAS INSTALACIONES

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			92%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	F	Si cumple
2	5				90%	90%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	5				95%	95%	F	Si cumple
5	5				90%	90%	F	Si cumple
6	4			85%		85%	F	No cumple
7	4			85%		85%	F	No cumple
8	3			70%		70%	F	No cumple
9	4			80%		80%	F	No cumple
10	4			80%		80%	F	No cumple
11	3			70%		70%	F	No cumple
					PROMEDIO	92%		

Elaborado por: Freire (2023)

Una vez evaluado el nivel de madurez del proceso EDM05.01 se pudo observar que a pesar de que dos actividades no alcanzaron la meta prevista, se encuentran en un nivel de proceso que se ejecutan en gran medida. Por otro lado, las demás actividades superaron las previsiones y cumplieron el objetivo establecido.

Tabla 47 DSS05.01 Proteger contra software malicioso

DSS05.01 PROTEGER CONTRA SOFTWARE MALICIOSO (MALWARE)

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			87%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	4			85%		85%	F	No cumple
3	5				95%	95%	F	Si cumple
4	5				90%	90%	F	Si cumple
5	5				90%	90%	F	Si cumple
6	3			70%		70%	F	No cumple
					PROMEDIO	87%		

Elaborado por: Freire (2023)

Tras una evaluación de las actividades asociadas al procedo DSS05.02 se identificó que solo un pequeño número de ellas cumplían con la meta establecida. Sin embargo, aunque no alcanzan el objetivo, las actividades no conformes presentan un nivel medio de capacidad en su ejecución, y solo una actividad presentó un nivel de capacidad bajo. Esto podría deberse a la influencia de sucesos externos inesperados.

Tabla 48 DSS05.02 Gestionar la seguridad de la red y las conexiones

DSS05.02 GESTIONAR LA SEGURIDAD DE LA RED Y LAS CONEXIONES

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		81%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	5				95%	95%	F	Si cumple
3	4			85%		85%	F	No cumple
4	4			80%		80%	F	No cumple
5	5				90%	90%	F	Si cumple
6	5				95%	95%	F	Si cumple
7	3			70%		70%	F	No cumple
8	2		50%			50%	F	No cumple
9	3			70%		70%	F	No cumple
					PROMEDIO	81%		

Elaborado por: Freire (2023)

Como resultado de una evaluación detallada de las actividades asociadas al proceso DSS05.03, se determinó que solo cuatro de ellas cumplían con las metas establecidas, demostrando un rendimiento optimo al alcanzar el nivel de capacidad deseado. No obstante, a pesar de no alcanzar el objetivo previsto, las actividades restantes muestran un nivel de ejecución establecido y predecible.

Éste último aspecto indica que, con una atención focalizada y estratégica, es posible elevar el rendimiento de estas actividades a niveles que se acerquen a las metas establecidas.

Tabla 49 DSS05.03 Gestionar la seguridad de los puestos de usuario final

DSS05.03 GESTIONAR LA SEGURIDAD DE LOS PUESTOS DE USUARIO FINAL

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		84%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	F	Si cumple
2	5				95%	95%	F	Si cumple
3	3			70%		70%	F	No cumple
4	3			70%		70%	F	No cumple
5	5				95%	95%	F	Si cumple
6	3			70%		70%	F	No cumple
7	5				95%	95%	F	Si cumple
8	4			85%		85%	F	No cumple
9	4			85%		85%	F	No cumple
					PROMEDIO	84%		

Elaborado por: Freire (2023)

Al realizar un examen detallado al proceso DSS05.04 se obtuvo como resultado que la mayor parte de las actividades no alcanzaban la meta establecida. Esta situación revela la importancia de llevar a cabo un seguimiento detallado. Este monitoreo será fundamental para identificar las áreas específicas que requieren ajustes y mejoras con el fin de llevar el desempeño de estas actividades a un nivel más adecuado.

Tabla 50 DSS05.04 Gestionar la identidad del usuario y el acceso lógico

DSS05.04 GESTIONAR LA IDENTIDAD DEL USUARIO Y EL ACCESO LÓGICO

NIELEZ DE MMADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		78%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
3	2		50%			50%	F	No cumple
4	4			85%		85%	F	No cumple
5	4			85%		85%	F	No cumple
6	4			85%		85%	F	No cumple
7	5				90%	90%	F	Si cumple
8	5				90%	90%	F	Si cumple
					PROMEDIO	78%		

Elaborado por: Freire (2023)

Luego de la evaluación del proceso DSS05.05, se descubrió que las actividades no cumplían con la meta establecida con excepción de una actividad que se encuentra en un nivel óptimo. Sin embargo, es fundamental destacar que el incumplimiento no implica una falta de ejecución de estas actividades, al contrario, implica un nivel medio de capacidad. Implementado un monitoreo se puede mejorar significativamente estas actividades.

Tabla 51 DSS05.05 Gestionar el acceso físico a los activos de TI

DSS05.05 GESTIONAR EL ACCESO FISICO A LOS ACTIVOS DE TI

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		72%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	5				90%	90%	F	Si cumple
3	3			70%		70%	F	No cumple
4	3			70%		70%	F	No cumple
5	2		50%			50%	F	No cumple
6	4			85%		85%	F	No cumple
7	3			70%		70%	F	No cumple
					PROMEDIO	72%		

Elaborado por: Freire (2023)

El análisis del proceso DSS05.06 indicó que dos actividades habían alcanzado un nivel de capacidad optimo, lo que demuestra la eficacia de la aplicación del proceso. Sin embargo, se identificaron tres actividades que no cumplían la meta establecida. Es crucial señalar que esta falta de cumplimiento no implica la falta de ejecución, sino que se necesita una atención adicional, la mejora en ciertos procedimientos, para lograr alcanzar la meta establecida en futuras evaluaciones.

Tabla 52 DSS05.06 Gestionar documentos y dispositivos de salida

DSS05.06 GESTIONAR DOCUMENTOS SENCIBLES Y DISPOSITIVOS DE SALIDA

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		78%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			80%		80%	F	No cumple
2	5				90%	90%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	4			80%		80%	F	No cumple
5	2		50%			50%	F	No cumple
					PROMEDIO	78%		

Elaborado por: Freire (2023)

Aunque es evidente que las actividades vinculadas al proceso DSS05.07 no alcanzaron la meta establecida, es fundamental destacar que estas actividades se están llevando a cabo. Sin embargo, el hecho de que no estén cumpliendo el nivel deseado señala la importancia de realizar un seguimiento más frecuente e implementar mejoras en los procesos pertinentes.

Tabla 53 DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

DSS05.07 SUPERVISAR LA INFRAESTRUCTURA PARA DETECTAR EVENTOS RELACIONADOS CON LA SEGURIDAD

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		68%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
3	3			70%		70%	F	No cumple
4	2		50%			50%	F	No cumple
5	4			80%		80%	F	No cumple
					PROMEDIO	68%		

Elaborado por: Freire (2023)

3.2.2.5 Supervisar, Evaluar y Valorar (MEA)

Tras evaluar las actividades del proceso MEA001.01, se determinó que estas presentan un nivel de capacidad medio, superando el umbral del 70%. Sin embargo, no alcanzaron el objetivo fijado de ser consideradas completamente optimas.

En cambio, las demás actividades tuvieron un rendimiento superior, lo que implica que sus procesos se encuentran bien definidos y funcionando a un nivel óptimo. Esta diferencia podría deberse a diversos factores, como posibles insuficiencias en la planificación o la ejecución.

Tabla 54 MEA01.01 Establecer un enfoque de la supervisión

MEA01.01 ESTABLECER UN ENFOQUE DE LA SUPERVISIÓN

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		77%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	3			70%		70%	F	No cumple
3	3			70%		70%	F	No cumple
4	4			85%		85%	F	No cumple
5	5				90%	90%	F	Si cumple
6	5				95%	95%	F	Si cumple
7	5				95%	95%	F	Si cumple
					PROMEDIO	77%		

Elaborado por: Freire (2023)

Una vez realizada una evaluación detallada del proceso mea01.02, se obtuvo como resultado que las actividades realizadas superaron la meta establecida con éxito. Este resultado indica un nivel de capacidad actual que supera las previsiones, demostrando una ejecución eficiente y eficaz de las actividades asignadas. Garantizando la mejora continua y rendimiento y la superación continua.

Tabla 55 MEA01.02 Establecer los objetivos de cumplimiento y rendimiento

MEA01.02 ESTABLECER LOS OBJETIVOS DE CUMPLIMIETO Y RENDIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		79%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	L	Si cumple
2	4			85%		85%	L	Si cumple
3	4			80%		80%	L	Si cumple
4	4			80%		80%	L	Si cumple
					PROMEDIO	79 %		

Elaborado por: Freire (2023)

Por otro lado, el proceso MEA01.03 una vez evaluado sus actividades se determinó que estas no cumplen con la meta establecida a pesar de que se lleva a cabo de manera coherente. Este resultado se debe que el proceso se encuentra en un nivel de capacidad predecible y establecido, lo que significa que la ejecución actual de las actividades se mantiene dentro de los parámetros conocidos y, en consecuencia, no supera los objetivos fijados.

Tabla 56 MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento

MEA01.03 RECOPILAR Y PROCESAR LOS DATOS DE CUMPLIMIENTO Y RENDIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		80%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
3	4			85%		85%	F	No cumple
4	3			70%		70%	F	No cumple
5	4			85%		85%	F	No cumple
					PROMEDIO	80 %		

Elaborado por: Freire (2023)

Cuando se examinó en detalle el proceso MEA01.04 se descubrió que dos de sus actividades tienen una capacidad baja, con un valor del 50%. Esta situación puede atribuirse a diversos factores, como la falta de claridad en los procedimientos o la necesidad de optimizar la capacidad del personal encargado de estas actividades. Por otro lado, dos actividades superaron la meta establecida, alcanzando un nivel óptimo de ejecución.

Tabla 57 MEA01.04 Analizar e informar sobre el rendimiento

MEA01.04 ANALIZAR E INFORMAR SOBRE EL RENDIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		78%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	L	Si cumple
2	5				90%	90%	L	Si cumple
3	2		50%			50%	L	No cumple
4	4			85%		85%	L	Si cumple
5	3			70%		70%	L	Si cumple
6	2		50%			50%	L	No cumple
					PROMEDIO	78%		

Elaborado por: Freire (2023)

Las actividades del proceso MEA01.05, que se centran en la garantizar la aplicación de medidas correctivas, han demostrado un rendimiento significativo al alcanzar un nivel de capacidad medio alto y así cumpliendo con la meta establecida.

Este éxito puede atribuirse a la aplicación eficaz de un sistema de seguimiento y medidas correctivas, así como la gestión preventiva de los problemas. La dedicación del personal implicado, así como el uso de las mejores prácticas en la planificación y ejecución de estas actividades, también han contribuido a su éxito.

Tabla 58 MEA01.05 Asegurar la implantación de medidas correctivas

MEA01.05 ASEGURAR LA IMPLANTACIÓN DE MEDIDAS CORRECTIVAS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		81%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			85%		85%	L	Si cumple
2	4			85%		85%	L	Si cumple
3	3			70%		70%	L	Si cumple
4	4			85%		85%	L	Si cumple
					PROMEDIO	81%		

Elaborado por: Freire (2023)

Se observa que determinadas actividades del proceso carecen de una supervisión adecuada, lo que provoca que no cumplan la meta establecida. Esta falta de control puede deberse a la ausencia de un proceso estructurado. Por el contrario, es de interés observar que tres actividades destacan por funcionar a un nivel óptimo. Este resultado sugiere que estos procesos están bien definidos y respaldados por prácticas eficaces.

Tabla 59 MEA02.01 Supervisar el control interno

MEA02.01 SUPERVISAR EL CONTROL INTERNO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		83%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	5				90%	90%	F	Si cumple
3	5				90%	90%	F	Si cumple
4	5				90%	90%	F	Si cumple
5	3			65%		65%	F	No cumple
6	3			65%		65%	F	No cumple
7	4			80%		80%	F	No cumple
					PROMEDIO	83%		

Elaborado por: Freire (2023)

La evaluación detallada revela que todas las actividades del proceso cumplen con la meta prevista, alcanzando un nivel óptimo. Este cumplimiento indica sin lugar a duda que los procesos están precisamente definidos y funcionan con gran eficacia. La coherencia en la realización del objetivo apunta a una ejecución precisa y una alineación adecuada con los objetivos estratégicos del proceso.

Tabla 60 MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio

MEA02.02 REVISAR LA EFECTIVIDAD DE LOS CONTROLES SOBRE LOS PROCESOS DE NEGOCIO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			90%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				95%	95%	L	Si cumple
2	5				95%	95%	L	Si cumple
3	4			85%		85%	L	Si cumple
4	4			85%		85%	L	Si cumple
5	5				90%	90%	L	Si cumple
					PROMEDIO	90%		

Elaborado por: Freire (2023)

En una evaluación detallada de las actividades del proceso, se determinó que algunas de ellas no cumplen los criterios establecidos, lo que se traduce a un nivel de capacidad medio. Esta constatación indica que hay potencial de mejora en cuanto al rendimiento y eficacia. Sin embargo, cabe señalar que, en contraste con estas observaciones, hay dos actividades que destacan a la hora de cumplir los objetivos fijados.

Tabla 61 MEA02.03 Realizar autoevaluaciones de control

MEA02.03 REALIZAR AUTOEVALUACIONES DE CONTROL

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		80%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	3			70%		70%	F	No cumple
3	4			85%		85%	F	No cumple
4	5				90%	90%	F	Si cumple
5	3			65%		65%	F	No cumple
6	5				90%	90%	F	Si cumple
7	3			70%		70%	F	No cumple
					PROMEDIO	80%		

Elaborado por: Freire (2023)

La valoración detallada de todas las actividades del proceso revelo un notable nivel de cumplimiento, ya que cada una de ellas alcanzo o supero los objetivos establecidos. Sin embargo, cabe destacar que tres de estas actividades sobresalen por haber superado significativamente dichos objetivos. Esta situación puede deberse a una combinación de factores, como una planificación estratégica más eficaz o la aplicación de prácticas adecuadas.

Tabla 62 MEA02.04 Identificar y comunicar las deficiencias de control

MEA02.04 IDENTIFICAR Y COMUNICAR LAS DEFICIENCIAS DE CONTROL

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		83%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	L	Si cumple
2	5				90%	90%	L	Si cumple
3	5				90%	90%	L	Si cumple
4	5				95%	95%	L	Si cumple
5	3			65%		65%	L	Si cumple
6	4			75%		75%	L	Si cumple
					PROMEDIO	83%		

Elaborado por: Freire (2023)

Las tres actividades del proceso MEA02.05 destacan por cumplir sistemáticamente el objetivo, lo que indica un rendimiento sólido y eficaz. Este rendimiento demuestra eficacia y un enfoque centrado en la realización de las actividades asignadas. A pesar de este notable resultado, es prudente completar una búsqueda continua de mejoras. Implementando medidas que permitan una mayor optimización del proceso, como la identificación y adopción de mejores prácticas.

Tabla 63 MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados

MEA02.05 GARANTIZAR QUE LOS PROVEEDORES DE ASEGURAMIENTO SON INDEPENDIENTES Y ESTÁN CUALIFICADOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50 %	>50-85 %	>85-100 %	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		75%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	L	Sicumple
2	3			70%		70%	L	Sicumple
3	3			65%		65%	L	Sicumple
					PROMEDIO	75%		

Elaborado por: Freire (2023)

Las actividades del proceso se llevan a cabo de manera adecuada, alcanzando la meta establecida de forma constante. Este resultado puede atribuirse a varios factores, como la planificación eficaz, la asignación apropiada de recursos, la claridad de los procedimientos y la competencia del personal implicado. La eficacia en la ejecución de las tareas refleja una comprensión clara de los objetivos del proceso y un esfuerzo constante por lograr la rentabilidad operativa

Tabla 64 MEA02.06 Planificar iniciativas de aseguramiento

MEA02.06 PLANIFICAR INICIATIVAS DE ASEGURAMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		83%			

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	4			80%		80%	L	Si cumple
2	5				90%	90%	L	Si cumple
3	4			80%		80%	L	Si cumple
					PROMEDIO	83%		

Elaborado por: Freire (2023)

Todas las actividades del proceso han demostrado un rendimiento excepcional al cumplir sistemáticamente el objetivo establecido, alcanzando un nivel en el que los procesos se llevan a cabo de manera eficiente. No obstante, cabe destacar que algunas actividades han superado este objetivo, demostrando un nivel de capacidad aún mayor. Esto se puede atribuirse a la aplicación de prácticas más eficientes.

Tabla 65 MEA02.07 Estudiar las iniciativas de aseguramiento

MEA02.07 ESTUDIAR LAS INICIATIVAS DE ASEGURAMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			87%		

ACTIVIDADES	NIVELES DE CAPACIDAD/ OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	L	Si cumple
2	5				90%	90%	L	Si cumple
3	4			80%		80%	L	Si cumple
4	4			80%		80%	L	Si cumple
5	5				90%	90%	L	Si cumple
					PROMEDIO	87%		

Elaborado por: Freire (2023)

Tras una breve evaluación de las actividades del proceso, se destaca la ausencia de ineficiencias, ya que cada una de ellas han alcanzado sistemáticamente las metas fijadas. Este solido rendimiento indica una ejecución eficaz y una alineación precisa con los objetivos del proceso. La búsqueda activa de mejoras sigue siendo fundamental porque, a pesar de la fiabilidad actual, se ha énfasis en la identificación de oportunidades para optimizar aún más los procesos.

Tabla 66 MEA02.08 Ejecutar las iniciativas de aseguramiento

MEA02.08 EJECUTAR LAS INICIATIVAS DE ASEGURAMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		73%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			65%		65%	L	Si cumple
2	3			65%		65%	L	Si cumple
3	5				90%	90%	L	Si cumple
4	5				90%	90%	L	Si cumple
5	3			70%		70%	L	Si cumple
6	4			85%		85%	L	Si cumple
7	5				90%	90%	L	Si cumple
8	5				90%	90%	L	Si cumple
					PROMEDIO	73%		

Elaborado por: Freire (2023)

En el transcurso de evaluar las actividades del proceso se determinó que se encuentran en un nivel de capacidad que, si bien no alcanzan las metas previstas, fue razonable. Es fundamental señalar que el desempeño se mantuvo dentro de los parámetros recomendables. Sin embargo, con el respaldo y los ajustes estratégicos adecuados, quedó claro que el proceso podría mejorarse para alcanzar y superar el objetivo.

Tabla 67 MEA03.01 Identificar requisitos externos de cumplimiento

MEA03.01 IDENTIFICAR REQUISITOS EXTERNOS DE CUMPLIMIENTO

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		80%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	4			80%		80%	F	No cumple
3	3			70%		70%	F	No cumple
4	3			70%		70%	F	No cumple
5	3			65%		65%	F	No cumple
6	4			85%		85%	F	No cumple
					PROMEDIO	80%		

Elaborado por: Freire (2023)

Las actividades del proceso MEA03.02 destacan por encontrarse en un nivel óptimo. Lo que indica que sus procesos están bien establecidos y se ajustan a las metas deseadas. Este nivel de eficiencia implica una gestión adecuada y un conocimiento profundo de los procedimientos implicados. La regularidad con la que se llevan a cabo estas actividades refleja un compromiso con la calidad operativa y la búsqueda de mejora continua.

Tabla 68 MEA03.02 Optimizar la respuesta a requerimientos externos

MEA03.02 OPTIMIZAR LA RESPUESTA A REQUERIMIENTOS EXTERNOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
			90%		

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	5				90%	90%	F	Si cumple
2	5				90%	90%	F	Si cumple
					PROMEDIO	90%		

Elaborado por: Freire (2023)

Aunque las actividades en cuestión no alcancen las metas establecidas, es fundamental observar que se desarrollan en un nivel de capacidad aceptable, presentando un valor de rendimiento superior o igual al 70%. Este indicador señala que, aunque no se hayan alcanzado las metas, las actividades se han llevado a cabo de forma significativa y eficiente.

Tabla 69 MEA03.03 Confirmar el cumplimiento de requerimientos externos

MEA03.03 CONFIRMAR EL CUMPLIMIENTO DE REQUISITOS EXTERNOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		70%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			70%		70%	F	No cumple
2	4			75%		75%	F	No cumple
3	3			70%		70%	F	No cumple
4	3			70%		70%	F	No cumple
					PROMEDIO	70%		

Elaborado por: Freire (2023)

Tras una evaluación detallada del proceso MEA03.04, se determinó que en general la meta establecida se alcanza satisfactoriamente. Sin embargo, es importante señalar que una actividad no cumple con la meta prevista ya que esta posee un valor de cumplimiento del 50%. Por otro lado, con la implementación de un monitoreo más detallado podría ayudar a identificar los puntos críticos y los posibles obstáculos a la finalización de la actividad.

Tabla 70 MEA03.04 Obtener garantía del cumplimiento de requisitos externos

MEA03.04 OBTENER GARANTIA DEL CUMPLIMIENTO DE REQUISITOS EXTERNOS

NIVELES DE MADUREZ (ISO 15504)

0-15%	>15-50%	>50-85%	>85-100%	NIVEL DE CUMPLIMIENTO	NIVEL DE CUMPLIMIENTO OBJETIVO DE LAS ACTIVIDADES
		70%			

ACTIVIDADES	NIVELES DE CAPACIDAD OBSERVADO	N	P	L	F	VALOR	META	OBSERVACIÓN
1	3			65%		65%	L	Si cumple
2	5				95%	95%	L	Si cumple
3	2		50%			50%	L	No cumple
4	3			65%		65%	L	Si cumple
5	4			75%		75%	L	Si cumple
6	4			75%		75%	L	Si cumple
					PROMEDIO	70%		

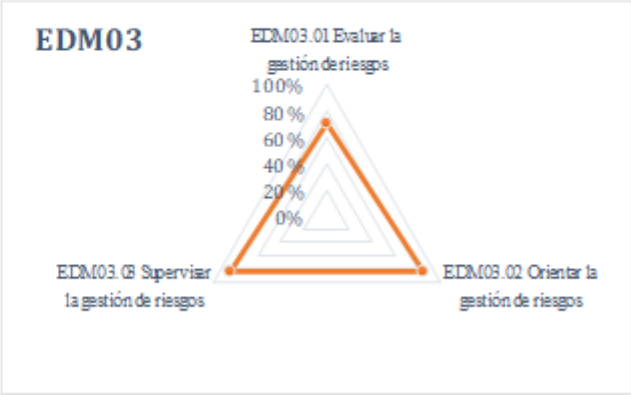
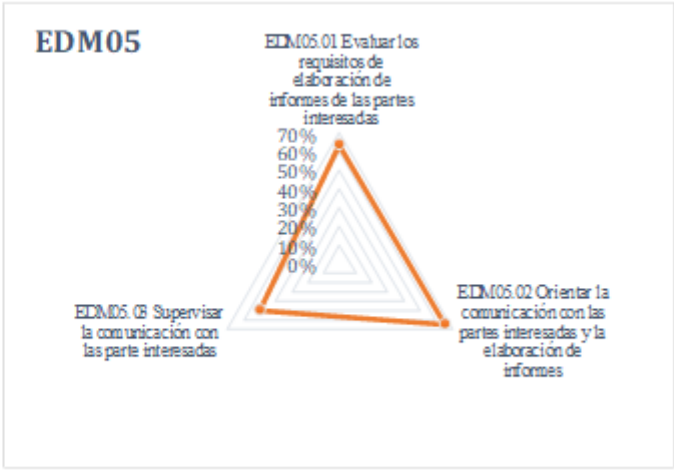
Elaborado por: Freire (2023)

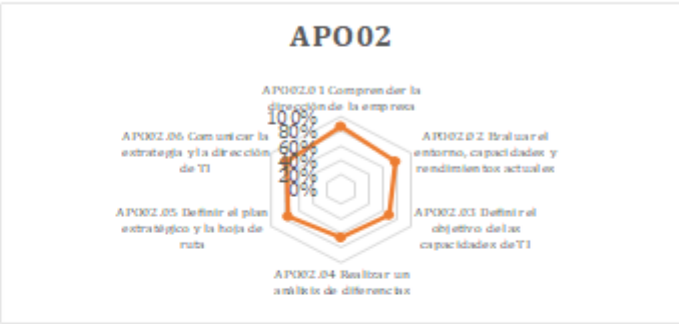
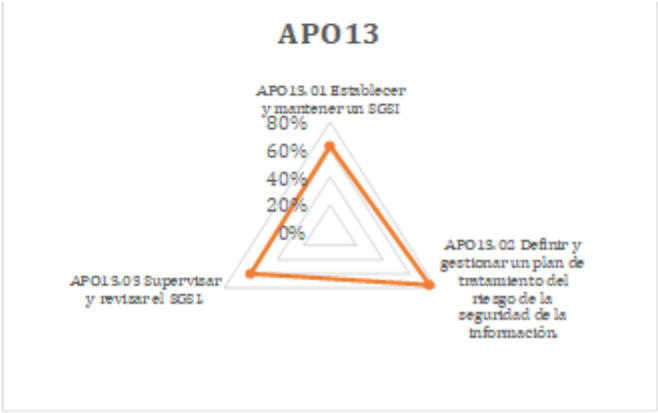
3.2.2.6 Cuadro resumen marco de referencia COBIT

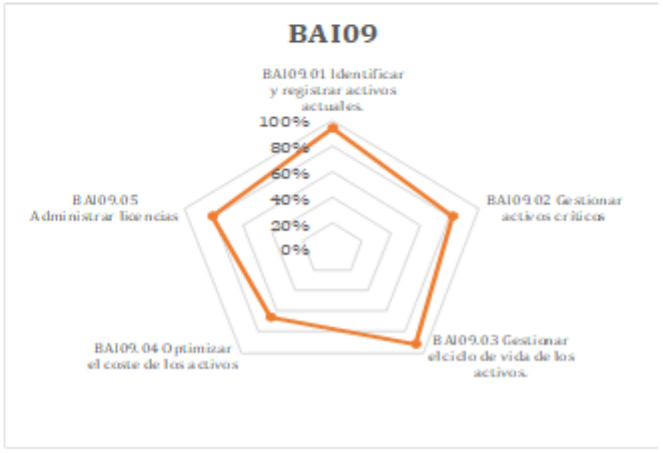
Se ha creado un cuadro resumen que permite ver los resultados obtenidos de las prácticas clave de los dominios evaluados. Esta sección permite agrupar y organizar los datos pertinentes, facilitando la comprensión y el análisis de los logros en cada área. Utilizando esta herramienta, puede ver exactamente como se ha desempeñado en cada dominio y que aspectos necesitan más atención o mejora.

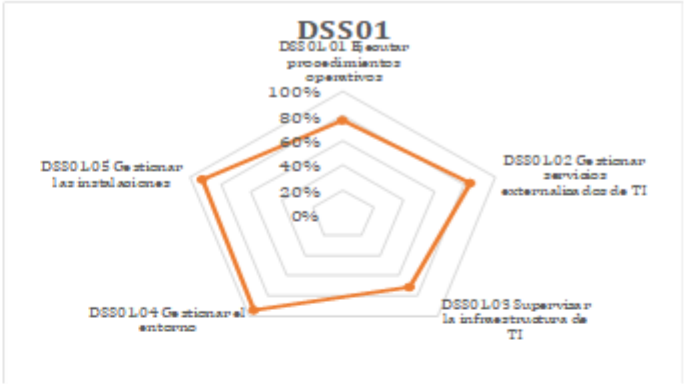
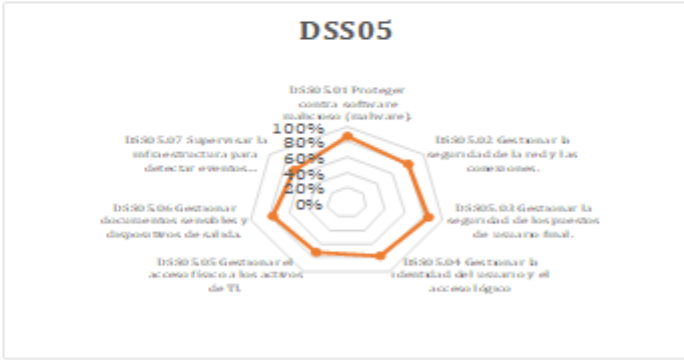
Además. Ofrece una visión detallada de los resultados facilitando la comunicación y el entendimiento entre los distintos equipos y partes interesadas. Esta estructura es de gran ayuda no solo para tomar decisiones, sino también como punto de partida para desarrollar futuras estrategias, centrándose en reforzar las áreas identificadas como oportunidades de mejora.

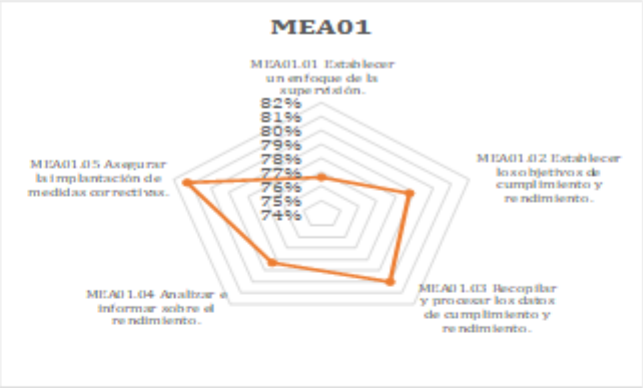
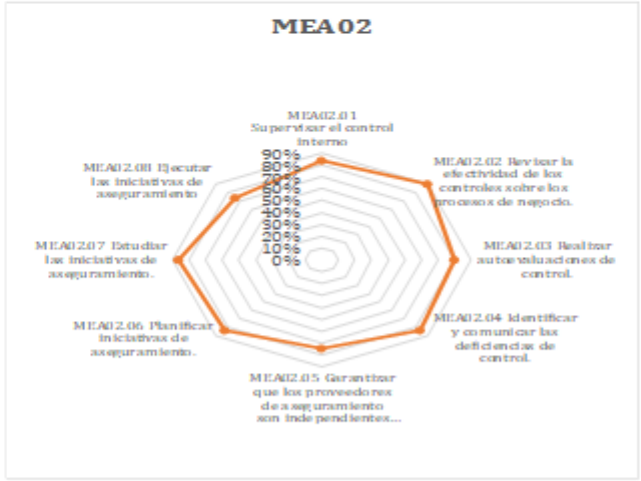
Tabla 71 Cuadro resumen por prácticas clave de gobierno

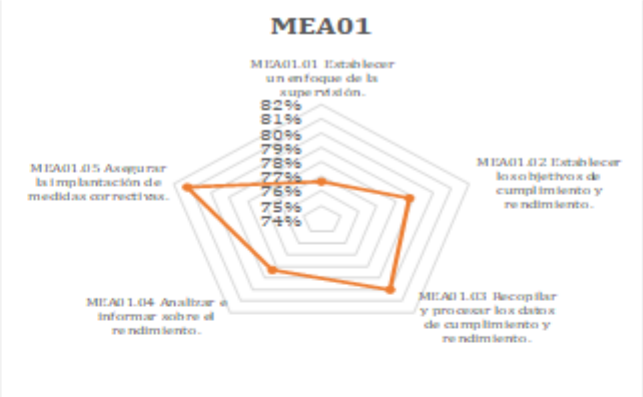
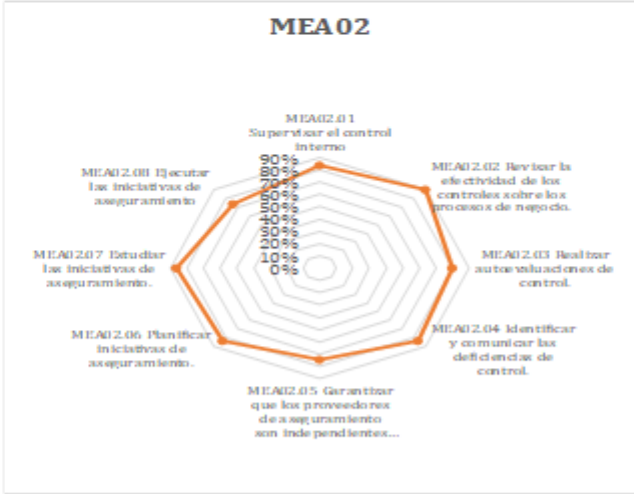
PRÁCTICAS CLAVES DE GOBIERNO	NIVELES DE CAPACIDAD	GRÁFICO	INTERPRETACIÓN
EDM03.01 Evaluar la gestión de riesgos	71%		Según los resultados obtenidos se pudo evidenciar que el componente EDM03.01 que se centra en la gestión de riesgos con un porcentaje del 71%. Este porcentaje inferior podría atribuirse a diversos factores, entre ellos la falta de herramientas adecuadas para identificar y evaluar los riesgos. Es fundamental investigar las causas para realizar los ajustes necesarios para mejorar la capacidad de evaluación de riesgos. En cambio, los componentes EDM03.02 Y EDM03.03, que se centran en la orientación y supervisión de las estrategias de gestión de riesgos, presentan un rendimiento del 85% lo que indica una solida eficacia en las estrategias de gestión de riesgos.
EDM03.02 Orientar la gestión de riesgos	85%		
EDM03.03 Supervisar la gestión de riesgos	85%		
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas	63%		En la evaluación de los indicadores de gestión relacionados con la comunicación y la preparación de informes para las partes interesadas, se observo que el componente EDM05.03 presenta el rendimiento mas bajo con un porcentaje del 50%. Es fundamental realizar un examen exhaustivo de los factores que contribuyen y así desarrollar estrategias para reforzar la supervisión de la comunicación con el fin de mejorar la eficacia en la gestión de las relaciones con las partes interesadas. Por el contrario los componentes EDM05.01 Y EDM05.02, centrados en evaluar las necesidades de información y dirigir la comunicación, obtienen un 63% y un 65% respectivamente. Esta diferencia pone de resalto la necesidad critica de mejorar la supervisan para lograr una gestión efectiva de la información con las partes interesadas.
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes	65%		
EDM05.03 Supervisar la comunicación con las parte interesadas	50%		

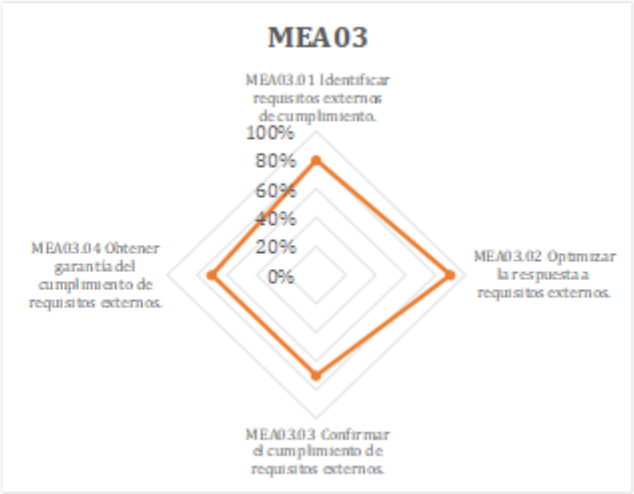
APO02.01 Comprender la dirección de la empresa	86%		Varios aspectos destacan en la evaluación de los indicadores clave de rendimiento relacionados con la gestión estratégica de las tecnologías de la información. Los porcentajes mas altos corresponden a los componentes APO02.01 "Comprender la dirección de la empresa con el 86%, APO02.02 "Evaluar el entorno, capacidades y rendimientos actuales con un valor del 78%, APO02,06 "Comunicar la estrategia y la dirección de TI con el 78% y APO02.05 " Definir el plan estratégico y la hoja de ruta con el 75%. Estos resultados implican un conocimiento profundo de la visión empresarial. Por el contrario, los porcentajes mas bajos se observa en los componentes APO02.04 con el 66% y APO02.03 con el 70%. Estos resultados pueden deberse a la falta de herramientas adecuadas para llevar a cabo un análisis eficaz, así como una posible falta de claridad en la definición de los objetivos específicos de las capacidades de TI. Es fundamental abordar estas deficiencias implementando herramientas y procesos que permitan una mayor eficiencia general en la gestión de TI.
APO02.02 Evaluar el entorno, capacidades y rendimientos actuales	78%		
APO02.03 Definir el objetivo de las capacidades de TI	70%		
APO02.04 Realizar un análisis de diferencias	66%		
APO02.05 Definir el plan estratégico y la hoja de ruta	75%		
APO02.06 Comunicar la estrategia y la dirección de TI	78%		
APO13.01 Establecer y mantener un SGSI	63%		Según los resultados obtenidos existen diversos niveles de eficacia como el componente APO13.02 que se refiere a la definición y gestión de un plan de gestión de los riesgos para la seguridad de la información alcanzando un nivel de realización mas elevado, llegando al 76%. Este resultado sugiere un mayor nivel de eficacia. En cambio el componente APO13.01 que se refiere al establecimiento y mantenimientos del SGSI, ha alcanzado un nivel del 63%, lo que indica un aplicación parcial de las medidas necesarias. Sin embargo, cabe señalar que el componente APO13.03, que se encarga de supervisar y revisa el SGSI, presenta el porcentaje mas bajo, con un 60%. Esto podría deberse a la falta de atención o a la insuficiencia de recursos dedicados, lo que afectaría a la capacidad del SGSI para adaptarse a los cambios en el entorno de la seguridad de la información.
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	76%		
APO13.03 Supervisar y revisar el SGSI.	60%		

BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos	82%		La importancia de cultivar y facilitar una cultura de intercambio de conocimientos, como demuestra el componente BAI08.01 con un porcentaje de 82% reflejando el firme compromiso de la cooperativa por fomentar la colaboración y el flujo constante de información entres sus miembros. Además, la identificación y clasificación de las fuentes de información, medida por el BAI08.02 con un75%, demuestra una capacidad satisfactoria para distinguir y organizar diversas fuentes, contribuyendo a la base de conocimientos de la organización . El componente BAI08.03 "organizar contextualizar la información, transformadora en conocimiento" con un porcentaje del 77% así como el uso eficaz y compartido del BAI08.04 igual con un 77%, demuestran la eficiencia de los proceso internos de la empresa. Por otro lado, la evaluación y recuperación de la información BAI08.05 con un porcentaje del 70% teniendo un indicador ligeramente bajo, lo que implica la necesidad de una revisión mas detallada de los criterios de evaluación. Estos datos en conjunto proporcionan una base solida en la gestión del conocimiento, con oportunidades identificadas para la mejora continua de la practica organizativa.
BAI08.02 Identificar y clasificar las fuentes de información	75%		
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento	77%		
BAI08.04 Utilizar y compartir el conocimiento	77%		
BAI08.05 Evaluar y retirar la información	70%		
BAI09.01 Identificar y registrar activos actuales.	93%		La evaluación de la gestión de las actividades revela una solida ejecución en diversas áreas, como resultado que varian entre 67% y un notable 93%. En primer lugar el componente BAI09.04, que muestra un indicador mas bajo del 67%. Este resultado puede apuntar a posibles ineficiencias en los procesos relacionados con la adquisición, mantenimiento o renovación de activos lo que implica la necesidad de una revisión en profundidad para identificar áreas de mejora. Por otro lado, el componente BAI09.01 obtuvo el valor mas alto, alcanzando un 93%. Esta cifra refleja una capacidad excepcional para reconocer y documentar las actividades existentes. La gestión del ciclo de vida de las actividades BAI09.03 demuestra una gran eficacia del 92%, lo que indica un fuerte compromiso con el mantenimiento y la maximización del valor de los recursos criticos. Los componentes BAI09.02 Y BAI09.05 muestran un solido rendimiento, pero podria beneficiarse de un análisis mas detallado para garantizar una gestión optima y el cumplimiento de la normativa.
BAI09.02 Gestionar activos críticos	82%		
BAI09.03 Gestionar el ciclo de vida de los activos.	92%		
BAI09.04 Optimizar el coste de los activos	67%		
BAI09.05 Administrar licencias	82%		

DSS01.01 Ejecutar procedimientos operativos	77%		Al obtener los resultados se ha registrado una amplia gama de resultados en tareas clave. El porcentaje mas bajo se registra en la ejecución de procedimientos operativos DSS01.01 con un77%. Este resultado podria atribuirse a posibles deficiencias en la definición de los procedimientos. Es fundamental abordar estas áreas de bajo rendimiento para mejorar la eficiencia general de las operaciones de servicios de TI. Por otro lado, el componente DSS01.04 con un valor del 95% indica un control eficaz y una optimización del entorno tecnológico. este alto rendimiento puede atribuirse a una gestión adecuada de los recursos. Además los componentes DSS01.02 destaca con un porcentaje del 83% lo que indica una gestión eficiente de los recurso. DSS01.03 "supervisión de la infraestructura de Ti tiene un valor de 72% lo que indica que es necesario prestar atención a la optimización de este componente. Por ultimo el componente DSS01.05 con un valor del 92% lo que refleja una coordinación y un mantenimiento eficaces de los espacios fisicos.
DSS01.02 Gestionar servicios externalizados de TI	83%		
DSS01.03 Supervisar la infraestructura de TI	72%		
DSS01.04 Gestionar el entorno	95%		
DSS01.05 Gestionar las instalaciones	92%		
DSS05.01 Proteger contra software malicioso (malware).	87%		La evaluación de las medidas de seguridad en la infraestructura de las tecnologías de la información (TI) arroja una serie de resultados que proporcionan una imagen completa de la postura de seguridad de la organización. DSS05.07 con un porcentaje del 68% es el valor mas bajo. Este resultado puede indicar la necesidad de reforzar los mecanismos de supervisión y detección de la seguridad para mejorar la capacidad de respuesta ante posibles amenazas. Por le contrario, se alcanza un solido 87% en la protección contra software maliciosos DSS05.01, lo que indica una efectiva implementación de medidas para salvaguardar el sistema frente a amenazas de tipo virtual. El componente DSS05.03 "Gestionar la seguridad de los puestos de usuario final" y DSS05.02 gestionar la seguridad de las redes y conexión reciben un 84% y un 81%, respectivamente, lo que indica un enfoque equilibrado tanto en la protección de los dispositivos como la seguridad de las redes. Gestionar la identidad del usuario y el acceso lógico "DSS05.04" y gestionar documentos sensibles y dispositivos de salida "DSS05,06" obtiene un 78% lo que pone de relieve la importancia de la seguridad de los datos y del control de acceso. Así mismo el componente DSS05.05 recibió una calificación del 72% lo que sugiere áreas de mejora en el control y la supervisión del acceso físico a los recursos de TI. Estos resultados proporcionan una valiosa orientación para la mejora continua de las medidas de seguridad en la infraestructura de TI.
DSS05.02 Gestionar la seguridad de la red y las conexiones.	81%		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.	84%		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico	78%		
DSS05.05 Gestionar el acceso físico a los activos de TI.	72%		
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	78%		
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	68%		

MEA01.01 Establecer un enfoque de la supervisión	77%		Durante el proceso de evaluación se revelo un desempeño positivo en general, aunque con variaciones en ,los porcentajes obtenidos en cada fase. El componente con el porcentaje mas bajo es establecer un enfoque de supervisión MEA01.01 , que tiene 77%. Este resultado puede atribuirse a la necesidad de mayor claridad y alineación en la definición del enfoque. Por otro lado, el componente con el valor mas alto MEA01.05 asegurar la implementación de acciones correctivas con el 81% destacando la eficacia de las actividades de dicho componente. Además se observa un solido 80% en la recopilación y el procesamiento de datos MEA01.03, en el componente MEA01.02 realización de objetivos y la medición del rendimiento con un 79%. Por ultimo MEA01.04 con un valor del 78% en el análisis del rendimiento y la elaboración de informes. Estos datos reflejan un compromiso general con la mejora continua y señalan áreas especificas que podrían beneficiarse de ajustes para mejorar el rendimiento.
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.	79%		
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	80%		
MEA01.04 Analizar e informar sobre el rendimiento.	78%		
MEA01.05 Asegurar la implantación de medidas correctivas.	81%		
MEA02.01 Supervisar el control interno	83%		La evaluación de los distintos componentes del sistema de seguridad muestra resultados diversos. El porcentaje mas bajo es del componente MEA0.2.05 con un valor del 75%. Este valor puede indicar dificultades en la selección y verificación de la independencia y cualificaciones de los proveedores, lo que subraya la importancia de reforzar los criterios de selección y la supervisión continua de sus capacidades. en cambio, se alcanza un porcentaje del 90% en el componente MEA02.02 lo que demuestra la eficacia de los controles internos. Los componentes de estudio de iniciativas de seguridad MEA02.07 posee un valor del 87%, lo que indica una cuidadosa atención a la revisión de iniciativas. Además, la identificación y comunicación de deficiencias de control MEA02.04 y la supervisión del control interno MEA02.01 además del componente MEA02.06 comparten un solido 83% lo que muestra una minuciosa atención al control interno como. Así mismo el componente MEA02.08 tiene un valor del 73% lo que implica una planificación solida pero con oportunidades para mejorar la ejecución de las iniciativas de seguridad y el componente MEA02.03 recibe un 80% respectivamente lo que indica una capacidad equilibrada para reconocer y abordar áreas de mejora interna.
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	90%		
MEA02.03 Realizar autoevaluaciones de control.	80%		
MEA02.04 Identificar y comunicar las deficiencias de control.	83%		
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados	75%		
MEA02.06 Planificar iniciativas de aseguramiento.	83%		
MEA02.07 Estudiar las iniciativas de aseguramiento.	87%		
MEA02.08 Ejecutar las iniciativas de aseguramiento	73%		

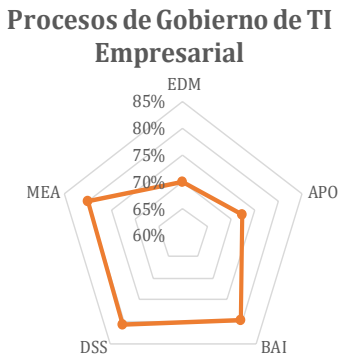
MEA01.01 Establecer un enfoque de la supervisión.	77%		Durante el proceso de evaluación se revelo un desempeño positivo en general, aunque con variaciones en ,los porcentajes obtenidos en cada fase. El componente con el porcentaje mas bajo es establecer un enfoque de supervisión MEA01.01 , que tiene 77%. Este resultado puede atribuirse a la necesidad de mayor claridad y alineación en la definición del enfoque. Por otro lado, el componente con el valor mas alto MEA01.05 asegurar la implementación de acciones correctivas con el 81% destacando la eficacia de las actividades de dicho componente. Además se observa un solido 80% en la recopilación y el procesamiento de datos MEA01.03, en el componente MEA01.02 realización de objetivos y la medición del rendimiento con un 79%. Por ultimo MEA01.04 con un valor del 78% en el análisis del rendimiento y la elaboración de informes. Estos datos reflejan un compromiso general con la mejora continua y señalan áreas especificas que podrían beneficiarse de ajustes para mejorar el rendimiento.
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.	79%		
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	80%		
MEA01.04 Analizar e informar sobre el rendimiento.	78%		
MEA01.05 Asegurar la implantación de medidas correctivas.	81%		
MEA02.01 Supervisar el control interno	83%		La evaluación de los distintos componentes del sistema de seguridad muestra resultados diversos. El porcentaje mas bajo es del componente MEA0.2.05 con un valor del 75%. Este valor puede indicar dificultades en la selección y verificación de la independencia y cualificaciones de los proveedores, lo que subraya la importancia de reforzar los criterios de selección y la supervisión continua de sus capacidades. en cambio, se alcanza un porcentaje del 90% en el componente MEA02.02 lo que demuestra la eficacia de los controles internos. Los componentes de estudio de iniciativas de seguridad MEA02.07 posee un valor del 87%, lo que indica una cuidadosa atención a la revisión de iniciativas. Además, la identificación y comunicación de deficiencias de control MEA02.04 y la supervisión del control interno MEA02.01 además del componente MEA02.06 comparten un solido 83% lo que muestra una minuciosa atención al control interno como. Así mismo el componente MEA02.08 tiene un valor del 73% lo que implica una planificación solida pero con oportunidades para mejorar la ejecución de las iniciativas de seguridad y el componente MEA02.03 recibe un 80% respectivamente lo que indica una capacidad equilibrada para reconocer y abordar áreas de mejora interna.
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	90%		
MEA02.03 Realizar autoevaluaciones de control.	80%		
MEA02.04 Identificar y comunicar las deficiencias de control.	83%		
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados	75%		
MEA02.06 Planificar iniciativas de aseguramiento.	83%		
MEA02.07 Estudiar las iniciativas de aseguramiento.	87%		
MEA02.08 Ejecutar las iniciativas de aseguramiento	73%		

MEA03.01 Identificar requisitos externos de cumplimiento.	80%		Según los resultados obtenidos se pudo obtener como resultado que el componente MEA.03.03 "confirmación de requisitos externos es el que tiene el valor mas bajo con un porcentaje del 70%. Este resultado sugiere la necesidad de una revisión mas detallada de lo procesos de confirmación, identificando posibles fallos. Además, se observa un porcentaje similar del 70% en el componente MEA03.04, lo que indica la importancia de abordar eficazmente la verificación y validación de los requerimientos para reforzar la confianza en el cumplimiento. Por otra parte, un porcentaje del 80% en la identificación de los requisitos de cumplimiento externos MEA03.01 . El componente MEA03.02 obtiene un valor del 90% siendo el mas alto, lo que demuestra adaptabilidad y mejora continua para cumplir las normas externa. Estos resultados proporcionan una visión global de la gestión del cumplimiento.
MEA03.02 Optimizar la respuesta a requisitos externos.	90%		
MEA03.03 Confirmar el cumplimiento de requisitos externos.	70%		
MEA03.04 Obtener garantía del cumplimiento de requisitos externos.	70%		

Elaborado por: Freire (2023)

De igual manera se realizó un resumen por dominios que ofrece una visión detallada de los resultados obtenidos anteriormente. Este enfoque permite un análisis más preciso y centrado, haciendo hincapié en las características únicas de cada dominio evaluado.

Tabla 72 Cuadro resumen por dominios

PROCESO/OBJETIVO DE CONTROL	NIVEL DE MADUREZ	GRÁFICA
EDM	70%	
APO	72%	
BAI	80%	
DSS	81%	
MEA	80%	

INTERPRETACIÓN

Después de una evaluación realizada a los procesos de las diferentes áreas claves de gobierno y gestión, se obtuvo varios resultados de los cuales existen algunos que demuestran ser eficientes, el dominio EDM correspondiente a "Evaluar, orientar y supervisar" cuenta con un 70%,señala un nivel moderado de cumplimiento en ese aspecto especifico, el dominio APO correspondiente a "Alinear, planificar y organizar" cuenta con un 72%,representa una mejora con respecto al anterior dominio, lo que indica un proceso positivo en la ejecución de las actividades. El componente BAI "Construir, adquirir e implementar" y MEA que se refiere a "Supervisar, evaluar y valorar" comparten un destacado 80%, lo que demuestra un rendimiento excepcional en estas áreas especificas y el dominio DSS correspondiente a "Entregar, dar servicios y soporte" cumple con un 81%, las mismas que se encuentran en un nivel eficiente sin embargo hay que recalcar que varios procesos y sus respectivas actividades deben cumplir el nivel objetivo meta, por lo que es importante que se creen estrategias de mejoramiento para poder obtener resultados positivos y que ayuden al crecimiento de la entidad.

Elaborado por: Freire (2023)

3.3 Fase de comunicación

Tras evaluar los controles internos y analizar los datos, se emitió un informe con resultados, conclusiones y recomendaciones para mejorar la eficacia y eficiencia de las áreas estudiadas.

RESULTADOS DEL EXAMEN

Tras una evaluación detallada de los activos de información de la cooperativa, se identificaron los riesgos potenciales que podrían ocurrir y poner en peligro la integridad, confidencialidad y disponibilidad de los recursos críticos. Por lo que se diseñó políticas de seguridad especificas con el objetivo de abordar estos riesgos.

Estas políticas se desarrollaron con el objetivo principal de mitigar las vulnerabilidades y garantizar que las actividades estén adecuadamente protegidas, estableciendo directrices claras y medidas preventivas para salvaguardar la información que maneja la cooperativa.

Política para garantizar la integridad de los datos y de los sistemas

Principios y terminología de la norma ISO/IEC 27000

Confidencialidad: Garantiza que sólo el personal con autorización tenga acceso a la información específica.

Integridad: Consiste en garantizar el cumplimiento y a exactitud de la información, así como de los métodos de proceso.

Disponibilidad: Garantiza que solo las personas autorizadas accedan a la información siempre que lo necesiten a través de los canales adecuados que satisfagan sus necesidades.

1. **Políticas para equipo de cómputo**

Riesgo: Puede dañar o comprometer la integridad de los datos y sistemas

Propósito:

Esta política tiene como objetivo fijar medidas y procedimientos para prevenir y mitigar posibles daños o riesgos a la integridad de los datos y sistemas en los equipos informáticos. La confidencialidad, integridad y disponibilidad de las actividades digitales de la organización dependen de la seguridad de la información

Políticas: Control de acceso

- Se implantará un sistema de control de acceso basado en funciones, que garantizara que los usuarios solo tengan accesos a los recursos que necesitan para realizar sus tareas.

Parches y actualizaciones

- Para garantizar la protección frente a vulnerabilidades conocidas, se establecerá una revisión y aplicación periódica de las actualizaciones.

Respaldo de datos

- Se harán copias de seguridad regulares de los datos críticos que se almacenarán en la nube.

Control para el cumplimiento:

Se realizará revisiones periódicas para verificar el seguimiento de las políticas. Se implantarán herramientas de supervisión para detectar cualquier incumplimiento y se llevarán a cabo inspecciones frecuentes de los registros de acceso.

Responsable:

El jefe del departamento de sistemas se encargará de supervisar y hacer cumplir estas políticas. Cualquier incumplimiento será notificado y tratado de acuerdo con los procedimientos establecidos.

Periodicidad:

Esta política se revisará anualmente o cada vez que se produzcan cambios significativos en la infraestructura de TI. Se realizarán auditorias trimestrales para garantizar el cumplimiento continuo.

2. Políticas para cámaras de vigilancia

Riesgo: La falta de funcionalidad de las cámaras puede tener un impacto negativo en la vigilancia y la seguridad en general

Propósito:

El objetivo de esta política es garantizar el funcionamiento continuo y eficaz de las cámaras de vigilancia, ya que su inactividad puede repercutir de manera adversa en la seguridad de las instalaciones. Esta política establece directrices para prevenir fallos de funcionamientos, además de responder con rapidez y eficacia en caso de que se produzca un problema.

Políticas: Mantenimiento preventivo

- Se llevará a cabo un mantenimiento preventivo periódico de todas las cámaras de vigilancia, que incluirán la limpieza.

Alimentación de respaldo:

- Para garantizar el funcionamiento durante los cortes de luz, las cámaras estarán alimentadas por sistemas de alimentación interrumpida.

Respaldo de datos:

- Para evitar la pérdida de datos en caso de avería, se implantará un sistema de respaldo de datos para almacenar las grabaciones de las cámaras.

Control de cumplimiento:

El departamento de sistemas se encargará de realizar revisiones periódicas del estado operativo de las cámaras, así como de coordinar la respuesta a cualquier problema identificado. Se establecerá registros de mantenimiento y se realizaran auditorias para garantizar su cumplimiento.

Responsable:

El departamento de sistemas será el encargado de aplicar y supervisar estas políticas, cualquier incidente o problema que se descubra deberá comunicarse inmediatamente.

Periodicidad:

Esta política se revisará y actualizará anualmente o cada vez que se produzcan cambios sustanciales en la infraestructura de vigilancia. Las revisiones funcionales y de auditoria se llevarán a cabo trimestrales para garantizar el cumplimiento continuo y la eficacia de las medidas de seguridad.

3. Políticas para servidores y redes compartidas

Riesgo: Pérdida de datos confidenciales trasmitidos a través de la red compartida

Propósito:

Salvaguardar la confidencialidad y protección de los datos compartidos por los servidores o redes compartidas. La pérdida de datos confidenciales podría tener graves consecuencias para la entidad, por lo que estas políticas establecen medidas para prevenir y responder eficazmente a los incidentes de pérdidas de datos.

Políticas: Control de acceso

- Se aplicará controles de acceso eficaz para limitar el acceso a los datos confidenciales únicamente a los usuarios autorizados.

Supervisión continua:

- Se establecerá un seguimiento continuo para detectar actividades sospechosas o accesos no autorizados a los datos compartidos.

Respaldo periódico de datos:

- Se realizarán auditorias periódicas de los datos almacenados en los servidores compartidos para garantizar su disponibilidad y facilitar su recuperación en caso de perdida.

Capacidad del personal:

- Todos los miembros que tengan acceso a datos compartidos recibirán capacitación frecuente sobre prácticas seguras, e importancia de la seguridad de datos.

Control de cumplimiento:

Se implementar y mantener los controles de seguridad. Se realizarán auditorías a fin de comprobar el cumplimiento de la política y garantizar la eficacia de las medidas de seguridad.

Responsables:

El responsable del área de sistemas se encargará de supervisar y ejecutar estas políticas. Cualquier suceso o fallo de seguridad que se descubra deberá comunicarse inmediatamente.

Periodicidad:

Esta política se revisará y actualizara anualmente, o si se producen cambios significativos en la infraestructura de red. Se realizará auditorias de seguridad y evaluación de cumplimiento trimestrales para garantizar la eficacia continua de las medidas de seguridad

4. Políticas para el router

Riesgo: La ausencia de funcionalidad del router puede perjudicar en la conectividad

Propósito:

El objetivo de esta política es garantizar la continua y segura conectividad previniendo el mal funcionamiento de los routers, ya que el incorrecto rendimiento de este puede afectar en las operaciones y a la seguridad de la información.

Políticas: Configuración segura

- Todos los routers deben configurarse de acuerdo con las mejores prácticas de seguridad, incluyendo la modificación de contraseñas predeterminadas.

- Se implementará procedimientos de actualización periódica para mantener el firmware del router actualizado y protegido frente a vulnerabilidades.

Supervisión continua:

- Se establecerá un sistema de monitoreo para detectar posibles anomalías en el funcionamiento del router.

Respaldo de configuración:

- Se realizará comprobaciones periódicas de la configuración del router para facilitar una rápida recuperación en caso de fallo.

Control de cumplimiento:

Realizar y mantener los controles de seguridad de los routers. Se realizarán revisiones periódicas de la configuración y rendimiento, así como auditoria para evaluar el cumplimiento de la política.

Responsable:

El área de sistemas será el encargado de supervisar que se cumpla dichas políticas. Así mismo se deberá informar de cualquier incidente de manera inmediata para evitar problemas.

Periodicidad:

Las políticas planteadas se revisaras de forma anual o cada vez que se produzcan cambios relevantes en la estructura de la red. Las revisiones de la configuración y las auditorias de los sistemas de seguridad se llevarán a cabo trimestralmente para garantizar su eficacia permanente.

5. Políticas de seguridad para software

Riesgo: Perdida de datos sensibles almacenados en el sistema

Propósito:

El fin de estas políticas es establecer mecanismos de protección de prevención de pérdidas de datos sensibles, garantizando al mismo tiempo la confidencialidad e integridad de la información. En caso de pérdida de datos la política pretende definir procedimientos para una respuesta rápida y eficaz.

Políticas: Cifrado de datos sensibles

- Como protección contra el acceso no autorizado, todos los datos sensibles almacenados en el sistema deben ser cifrados durante su almacenamiento.

Control de acceso:

- Restringir el acceso a los datos sensibles del sistema únicamente a los usuarios no autorizados y así evitar riesgos potenciales.

Supervisión de las actividades:

- Se establecerá un sistema de monitoreo para detectar actividades inusuales o accesos no autorizados a datos sensibles.

Actualización de seguridad:

- Todos los programas y sistemas que manejan datos delicados deberán mantenerse actualizados con los parches de seguridad más recientes.

Control de cumplimiento:

Se llevará a cabo revisiones regulares de los protocolos de seguridad, así como auditorias para evaluar el cumplimiento de la política.

Responsable:

El jefe del área de sistemas controlará y garantizarán el cumplimiento de la política. Así mismo cualquier perdida de datos se tendrá que informar inmediatamente.

Periodicidad:

Esta política se revisará anualmente o si se realiza un cambio de software. Las auditorias y las revisiones de protocolos se llevarán a cabo de manera trimestral para garantizar que las medidas siguen siendo eficaces.

6. Área de crédito

Riesgo: incumplimiento de las regulaciones y normativas planteadas por la entidad

Propósito:

Vela por el pleno cumplimiento de las regulaciones y normativas fijadas en el departamento de créditos. Se procura proteger la confidencialidad, integridad y disponibilidad de la información relacionadas con las operaciones de crédito, así como prevenir y mitigar los riesgos asociados al incumplimiento de la normativa.

Políticas: Confidencialidad de la información

- Está prohibido el acceso a los datos sensibles relacionados a las operaciones de crédito, como la información personal y financiera del cliente.

Cumplimiento normativo:

- Todo el personal de crédito debe conocer y cumplir las normas y reglamentos establecidos por el gerente de la entidad.
- Establecer mecanismos de control continuo que se aseguren que todas las operaciones de crédito se ajusten a la ley.

Seguridad de la información

- Implementar controles de seguridad de la información para proteger los sistemas y bases de datos utilizados en el procesamiento de las operaciones de crédito.

Controles de cumplimiento:

- Se realizará auditorías internas periódicas para evaluar el cumplimiento de las políticas de seguridad.

- Revisiones de los procesos y sistemas para detectar posibles fallos de seguridad.
- Cada asesor de crédito recibirá capacitación periódica sobre las normas y regulaciones aplicables.
- Se realizará pruebas de conocimientos para garantizar las correcta interpretación y aplicación de las políticas de seguridad.

Responsable:

El jefe del departamento de créditos será designado como punto de contacto para supervisar a los asesores de crédito y así verificar el cumplimiento de las normas y reglamentos establecidos por la entidad.

Periodicidad:

Estas políticas se revisarán y recibirá actualizaciones anualmente, o si se produce cambios importantes en la normativa financiera. Se realizarán auditorías internas trimestrales para garantizar que las medidas de seguridad establecidas se aplican eficazmente, La formación se impartirá semestralmente para mantener al personal al día de las actualizaciones más recientes en materia de normativa y seguridad.

7. Área de caja

Riesgo: Perdida económica debido a robos, fraudes o errores en la gestión del efectivo

Propósito:

El objetivo de estas políticas es proporcionar medidas preventivas y correctivas que minimicen las pérdidas económicas causadas por robos, fraudes o la mala gestión del efectivo. La seguridad y la integridad de los recursos financieros son fundamentales para la solidez financiera y la reputación de la organización.

Políticas: Control de acceso

- El acceso a las zonas de cajas estará estrictamente controlado, y solo se permitirá la entrada al personal autorizado.

Supervisión continua:

- Se llevará a cabo una supervisión continua de las transacciones de efectivo mediante auditorias frecuentes de los registros y sistemas.
- Se instalará cámaras de seguridad para controlar la actividad de la zona de cajas

Procedimientos de conciliación

- Se establecerá procedimientos rigurosos para el recuento y la conciliación del dinero al principio y al final de cada turno.
- Se realizará auditorias sorpresas para garantizar la exactitud de los registros financieros.

Control de cumplimiento:

- Cada miembro encargado en la administración del efectivo recibirá formación periódica sobre los procedimientos de seguridad y las mejores prácticas para la gestión del efectivo.
- Se realizará auditorías internas periódicamente como sorpresas para evaluar y cumplimiento de las políticas de seguridad.
- Se revisará los procedimientos de gestión del efectivo y los registros contables.

Responsable:

El responsable de la gestión del efectivo será el jefe de operaciones quien supervisará a al personal que se encuentre en caja y así verificar el cumplimiento de estas políticas para lograr mitigar cualquier riesgo que se presente.

Periodicidad:

Las políticas serán examinadas y actualizadas anualmente, o si se produce cambios relevantes en los procedimientos internos. Además, se realizarán auditorías internas trimestrales para garantizar la eficacia de las medidas de seguridad. La formación del personal se impartirá semestralmente.

8. Departamento de atención al cliente

Riesgos:

- La ausencia de ayuda hacia los clientes afectara en la satisfacción y fidelidad de estos.
- Quejas hacia el personal de la entidad provocando una calificación deficiente en su desempeño.

Propósito:

El objetivo de estas políticas es ofrecer un servicio de atención al cliente eficaz y orientado al cliente para evitar la falta de asistencia a los mismo, lo que afectaría negativamente a la entidad. Además, pretende prevenir las quejas dirigidas al personal evitando así las evaluaciones inadecuadas del rendimiento.

Políticas: Atención obligatoria

- Todo el personal de atención al cliente debe estar disponible para ayudar a los clientes con sus consultas y problemas.

Capacitaciones del personal:

- El personal de atención al cliente recibirá formación continua sobre los servicios de la cooperativa, así como sobre habilidades de comunicación y resolución de problemas.
- El personal debe estar actualizado con respecto a la normativa y procesos

Confidencialidad y protección de datos:

- El personal debe salvaguardar la confidencialidad de la información del cliente ya que podría ser información sensible.

Control de cumplimiento:

Se realizarán evaluaciones de desempeño para verificar la calidad del servicio proporcionado. Además de llevar a cabo auditorias de forma periódica para determinar si se cumplen con los procedimientos.

Responsables:

Las políticas se revisarán y actualizarán anualmente o cuando sea necesario para reflejar los cambios en los productos, servicios o normativas. Las evaluaciones de desempeño se llevarán a cabo trimestralmente, y se realizarán auditorías internas al menos dos veces al año para garantizar el cumplimiento continuo de las políticas de seguridad y la mejora continua del servicio al cliente.

9. Departamento de contabilidad

Riesgo: Pérdida económica derivadas de prácticas contables inseguras

Propósito:

El objetivo es proporcionar directrices y medidas de seguridad en el ámbito contable con el fin de evitar pérdidas económicas causadas por la utilización de las normas. Así mismo cuidar la imagen de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información financiera.

Políticas: Selección y aplicación de normas contables

- Las políticas deben elegirse y aplicarse de acuerdo con las normas internacionales de contabilidad (NIC).
- Las normas utilizadas se deben documentar y comunicar a todo el personal contable.

Revisiones periódicas:

- Se llevará un registro detallado de todas las transacciones contables con el fin de evitar riesgos potenciales.
- Se realizarán auditorias periódicas para garantizar el cumplimiento de las normas establecidas.

Comunicación de errores:

- Los errores contables deben corregirse lo antes posibles y cualquier inexactitud sustancial informarse con tiempo.

Capacitación al personal:

- Se dará formación continua al personal responsable sobre las normas que se utilizan y el correcto funcionamiento del sistema contables.

Control de cumplimiento:

La aplicación de estas políticas se supervisará mediante revisiones periódicas realizadas por el equipo de auditoría interna. Se aplicarán controles con el fin de garantizar el cumplimiento de las medidas de seguridad establecidas.

Responsable:

El jefe del departamento de contabilidad será el encargado por el cumplimiento de las normas contables y supervisión del personal para evitar errores y no perjudicar la imagen de la entidad.

Periodicidad:

Se realizará una revisión anual de las políticas para garantizar su pertinencia y eficacia. Se realizarán auditoria internas de forma trimestral para evaluar el cumplimiento de las Prácticas establecidas. Cualquier actualización o modificación de la política se comunicará al personal pertinente lo antes posible.

10. Comité de cumplimiento

Riesgo: Miembros del consejo que carecen de conocimiento especializados en las áreas relevantes de cumplimiento.

Propósito:

El alcance de las políticas es establecer directrices para mitigar los riesgos asociados a la falta de conocimientos por parte de los miembros del consejo en ámbitos esencial para el cumplimiento. Además de asegurar que el comité de cumplimiento este debidamente informado y preparado para hacer frente a los retos y responsabilidades que conlleva el cumplimiento de las normas.

Políticas: Conocimiento de la normativa

- Los miembros del comité de cumplimiento deben tener conocimientos como la normativa legal, las normas del sector y políticas internas de la organización.

Programa de capacitación continua:

- Se impartirá capacitaciones para los miembros del comité, con actualizaciones periódicas sobre los cambios en las normativas y políticas pertinentes.

Evaluación de riesgo:

- El comité debe realizar evaluaciones periódicas de los riesgos relacionadas con el cumplimiento.
- Se identificarán las áreas en las que faltan mejorar y se aplicaran medidas correctivas.

Comunicación transparente:

- Los miembros del comité deben informar de cualquier carencia de conocimientos durante las reuniones.
- Las decisiones importantes relativas al cumplimiento serán revisadas antes de su aplicación.

Control de cumplimiento:

Se aplicarán controles de seguimiento a través de evaluaciones periódicas de competencias y participación en programas de capacitación.

Responsable:

La dirección de cumplimiento se encargará de controlar la aplicación de las políticas. El departamento de recursos humanos colaborara en la verificación de las cualificaciones y en la formación continua de los miembros del comité de cumplimiento.

Periodicidad:

La comprobación de la cualificación se realizará anualmente en la revisión del rendimiento. El programa de capacitación se ejecutará trimestrales, con revisiones semestrales para evaluar a eficacia. Cualquier cambio en la estructura del comité se comunicará inmediatamente.

11. Asesor jurídico

Riesgo: Gestión ineficiente de documentos legales que podrían resultar en la perdida de información crucial.

Propósito:

El objetivo es proporcionar una gestión eficaz de los documentos jurídicos, reduciendo al mínimo el riesgo de pérdida de información crucial. Por ello se trata de proteger la confidencialidad, integridad y disponibilidad de los documentos jurídicos importantes.

Políticas: Clasificación y organización de la documentación

- Todos los documentos deberán ser clasificados y organizados en función de su importancia y prioridad.
- Para facilitar la búsqueda y recuperación, se establecerá un sistema de etiquetado.

Accesos controlado y seguro:

- El acceso a documentos confidenciales estará restringidos al personal no autorizado.

Recuperación y respaldo:

- Se realizarán copias de periódicas de seguridad de los documentos digitales.
- Los documentos que hayan pasado a ser innecesarios o que ya no sean relevantes se eliminaran de forma segura.

Control de cumplimiento:

Se realizará revisiones y auditorías internas de forma periódica para evaluar el cumplimiento de las directrices sobre la gestión documental y así mitigar los posibles riesgos que se puedan suscitar.

Responsable:

El asesor jurídico será el principal encargado de supervisar, aplicar y garantizar el cumplimiento de las políticas de seguridad establecidas.

Periodicidad:

Se realizará auditorías internas semestralmente para evaluar la eficacia de las medidas de seguridad aplicadas. Los documentos legales se revisarán y actualizarán anualmente o cuando sea necesario en respuesta a cambios significativos en la legislación o las normas aplicables. Se investigará inmediatamente cualquier incidente de perdida de información.

RESULTADOS DEL EXAMEN

1. En la aplicación del marco de referencia COBIT la práctica clave EDM03.01 “Evaluar la gestión de riesgos”, presenta actualmente un bajo índice de cumplimiento, con un máximo de 71%. Este indicador refleja una situación que requiere atención a las actividades de dicha práctica por lo que no se encuentra dentro de los parámetros establecidos.

Comentario

El bajo rendimiento en la práctica EDM03.01 podría atribuirse a diversos factores, como la falta de información sobre la importancia de una gestión eficaz de los riesgos, la insuficiente asignación de recursos para aplicar estrategias de mitigación de riesgos.

Conclusión

Para garantizar que cualquier entidad tenga capacidad de recuperación, es esencial evaluar la gestión de riesgos. La baja calificación de la práctica pone en evidencia

la necesidad de revisar y reforzar los procesos asociados a la identificación, evaluación y gestión de riesgos. No atender a esta práctica puede exponer a la cooperativa a amenazas.

Recomendaciones

- Llevar a cabo una revisión detallada de los procesos actuales de gestión de riesgos para identificar posibles fallos o ineficiencias, asegurándose que existen protocolos claros para identificar, evaluación y mitigación de riesgos.
- Establecer un sistema de supervisión continua para evaluar el rendimiento de la gestión de riesgos y realizar los ajustes necesarios, esto garantiza que la organización pueda reaccionar ante los cambios en su entorno operativo.

2. La práctica clave EDM05.03, que se centra en Supervisar la comunicación con las partes interesadas, presenta actualmente un índice de realización especialmente bajo, ya que solo alcanza el 50%. Este indicador revela una situación crítica que requiere atención inmediata para comprender las razones de este bajo rendimiento.

Comentario

La baja valoración de la práctica EDM05.03 podría atribuirse a una variedad de causas, entre ellas la falta de procesos eficaces para gestionar la comunicación con las partes interesadas, la falta de claridad en la identificación de las necesidades de estas y la falta de mecanismos para recoger periódicamente la retroalimentación. Es fundamental realizar un análisis detallado para identificar las deficiencias y comprender por qué la práctica no cumple las expectativas.

Conclusión

La supervisión eficaz de la comunicación con todas las partes implicadas es fundamental para establecer relaciones sólidas y mantener la transparencia en todas las operaciones de la organización. La falta de cumplimiento en la práctica EDM05.03 hace en énfasis en la necesidad critica de aborda las deficiencias en la

gestión de la comunicación, ya que una comunicación ineficaz puede llevar a una mala comunicación, a una falta de apoyo y a una percepción negativa entre los implicados.

Recomendaciones

- Realizar un análisis detallado sobre las necesidades de las partes interesadas para desarrollar estrategias de comunicación adaptadas a sus intereses específicos.
- Definir procesos de comunicación claros y eficaces con las partes interesadas, garantizando una línea de comunicación abierta y una retroalimentación continua.
- Proporcionar capacitación adecuada a las personas encargadas de la comunicación con las partes interesadas, centrándose en las habilidades de comunicación eficaz, la resolución de conflictos y la empatía.

3. La práctica clave APO02.04, que se refiere a Realizar un análisis de diferencias, presenta un índice de cumplimiento relativamente bajo de 66%. Esta cifra indica que se trata de una falta de atención inmediata para comprender las razones de este rendimiento inferior al esperado.

Comentario

El bajo rendimiento en la práctica puede deberse a varios aspectos, como la posible falta de procesos normalizados para realizar análisis diferenciales, la falta de herramientas adecuadas para facilitar dichos análisis o la insuficiente. Es fundamental investigar a fondo estas posibles causas para abordar las deficiencias y mejorar el rendimiento en esta área. La falta de un enfoque preventivo para identificar y abordar las posibles deficiencias puede retribuir negativamente en la toma de decisiones y en la eficacia operativa.

Conclusión

Hacer un análisis de diferencias es fundamental para identificar desviaciones significativas y tomar medidas correctivas lo antes posibles. Los resultados deficientes en la práctica APO02.04 ponen en evidencia la necesidad de reforzar los procesos de análisis de diferencias para garantizar una toma de decisiones fundamentada y una respuesta eficaz a las diferencias detectadas.

Recomendaciones

- Establecer procesos transparentes y estandarizados para llevar a cabo un análisis de diferencias, garantiza que todos los miembros del personal son conscientes de las responsabilidades asignadas y de los pasos que deben seguir.
- Proporcionar al personal formación continua sobre las herramientas y metodologías necesarias para llevar a cabo un análisis de diferencias de forma eficaz.

4. La práctica clave APO13.03 que dedica a "Supervisar y revisar el sistema de gestión de la seguridad de la información (SGSI), tiene actualmente un índice de cumplimiento del 60%. Este índice revela que es necesario una mayor atención para comprender las razones de este rendimiento inferior a las expectativas.

Comentario

El bajo resultado en la práctica APO13.03 puede deberse a la posible falta de procesos rigurosos para la supervisión y revisión del SGSI, la ausencia de funciones y responsabilidades claramente definidas en este ámbito. Además, la ausencia de información sobre la importancia del sistema de gestión de la seguridad de la información puede contribuir al bajo nivel de cumplimiento. El entorno de la seguridad de la información requiere una atención continua, y la ausencia de una supervisión adecuada puede exponer a la organización a nuevas amenazas.

Conclusión

La supervisión y revisión periódica del SGSI son fundamentales para garantizar su eficacia y adaptabilidad a los cambios en el entorno de las amenazas. El incumplimiento de la práctica clave pone de manifiesto que es esencial mejorar los procesos de control y verificación para reforzar la seguridad de la información de la organización.

Recomendaciones

- Definir y documentar proceso detallados para la supervisión periódica del SGSI, garantizando que todas las áreas críticas se evalúen de forma sistemática.
- Identificar las funciones y responsabilidades relacionadas con la supervisión del sistema de gestión de la seguridad de la información, garantizando al mismo tiempo la existencia de personal designados para llevar a cabo estas actividades de forma periódica.
- Proporcionar al personal información sobre la importancia de realizar estas actividades de manera regular, haciendo énfasis en como ayuda a salvaguardar los datos sensibles.

5. El cumplimiento de la práctica clave BAI08.05, que se centra en "Evaluar y retirar la información, es actualmente el valor más bajo, ya que se sitúa en torno al 70%. Esta cifra indica que dicha práctica requiere una atención para comprender las razones que provocan este rendimiento inferior al esperado.

Cometario

El bajo índice de cumplimiento de la práctica clave BAI08.05 puede atribuirse a diversas razones, entre ellas la posible falta de procedimientos para evaluar la información, la ausencia de un proceso para identificar la información sensible o la falta de conocimiento sobre la importancia de realizar esta actividad con regularidad.

Además, la falta de conocimiento al personal sobre las políticas y procedimientos establecidos para llevar a cabo este proceso de evaluación y recuperación de la información.

Conclusión

Es fundamental evaluar y eliminar información obsoleta o innecesaria para asegurar así la integridad y seguridad respecto a los datos de la organización. El incumplimiento de la práctica BAI08.05 destaca la necesidad de mejorar los procesos de gestión de la información para reducir los riesgos asociados a la conservación innecesaria de datos.

Recomendaciones

- Establecer políticas claras y documentadas para la evaluación de dicha práctica, incluidos los criterios para determinar qué información debe retirarse y cuando.
- Realizar auditorías periódicas para garantizar el cumplimiento de las políticas establecidas y la eficacia de los procesos de evaluación y recuperación de la información.
- Evaluar e implementar herramientas tecnológicas que faciliten la identificación eficiente y la eliminación de información caduca, dando lugar a un proceso más rápido y preciso.

6. La práctica clave BAI09.04 enfocada en "Optimizar el coste de los activos", presenta actualmente un valor de cumplimiento bajo del 67%. Este porcentaje muestra una situación que requiere atención inmediata para comprender las razones de este rendimiento inferior a las perspectivas.

Comentario

Este porcentaje tan bajo de realización de la práctica BAI09.04 podría deberse a diversos aspectos. Entre ellos se encuentra la falta de procesos eficientes para gestionar los costes de los activos, la falta de herramientas adecuadas para realizar

un seguimiento y análisis eficaces de los costes y la ausencia de una cultura organizativa orientada a la mejora de los recursos.

Conclusión

La optimización de los costes de los activos es crucial para asegurar la eficiencia financiera y la rentabilidad de la organización. La falta de cumplimiento de dicha práctica pone manifiesto la necesidad critica de mejorar los procesos relacionados con la gestión de los costes de activos para garantizar un uso óptimo de los recursos financieros.

Recomendaciones

- Realización de un análisis de coste detallado de los activos implicados, identificando ineficiencias y oportunidades de mejor
- Evaluar e implementar herramientas de gestión financiera que permitan un seguimiento preciso de los costes de los activos y proporcionen un análisis detallado.
- Definir métricas claras y objetivos medibles para evaluar la eficiencia en la gestión de los costes de los activos, proporcionando una base para la mejora continua.
- Fomentar la optimización de los recursos de la organización incentivando la colaboración entre departamentos para compartir las mejores Prácticas y reducir los riesgos potenciales.

7. En el contexto de la práctica clave DSS01.01 que se dedica a “Ejecutar procedimientos operativos”, se observa una tasa de cumplimiento bajo que solo alcanza el 77%. Este resulta plantea dudas sobre la eficacia y eficiencia de la utilización de esta práctica en un contexto operativo.

Comentario

La baja ejecución de los procedimientos operativos, que muestra un índice del 77% puede atribuirse a varios aspectos. Puede haber problemas de comunicación, falta

de herramientas y recursos necesarios para llevar a cabo de las operaciones de manera eficiente.

Conclusión

La identificación del bajo porcentaje de ejecución en la práctica clave es crítica. DSS01.01 señala la importancia de revisar a fondo los procesos y la formación asociada, la eficacia de cualquier sistema depende en gran medida de la correcta aplicación de los procedimientos, y el fallo identificando revela posibles áreas de mejora.

Recomendaciones

- Llevar a cabo una revisión detallada de los procedimientos operativos existentes, asegurados que estén actualizados, sean claros y estén alineados con los objetivos de la organización.
- Proporcionar capacitación continua a los empleados para garantizar que se encuentren familiarizados con los procedimientos operativos y sean competentes en su ejecución.
- Evaluar y utilizar herramientas de gestión que faciliten la ejecución y el seguimiento de los procedimientos operativos, mejorando la eficacia y reduciendo los errores.
- ´Promover una cultura organizativa que valore la importancia de seguir los procedimientos operativos y fomente la colaboración para abordar cualquier desafió identificado.

8. Dentro del cumplimiento de la práctica clave DSS05.07, que se centra en la supervisión de la infraestructura para detectar incidentes de seguridad, se ha detectado una deficiencia, ya que el porcentaje de cumplimiento solo alcanza el 68%. Este hallazgo plantea inquietudes sobre la eficacia de la supervisión de la seguridad y la necesidad de abordar cualquier deficiencia en la aplicación.

Comentario

La baja valoración de cumplimiento del 68% en la práctica DSS05.07 podría atribuirse a varios factores, puede tratarse de limitaciones o deficiencias en los protocolos de respuesta ante incidentes de seguridad. Es fundamental examinar cada uno de estos aspectos para comprender las razones detrás y en consecuencia adoptar soluciones eficaces.

Conclusión

Este porcentaje sugiere que existe un fallo en la estrategia de supervisión, esto podría poner en riesgo la capacidad de la organización para detectar y abordar a tiempo las amenazas a la seguridad. Es fundamental reconocer la importancia de una supervisión eficaz para la protección de las actividades críticas y la integridad de la información.

Recomendaciones

- Formar continuamente al personal encargado de la supervisión para garantizar un conocimiento profundo de los procedimientos y protocolos de seguridad.
- Revisar y actualizar los protocolos de respuesta de seguridad para garantizar una actuación oportuna y eficaz. Esto podría implicar los análisis posteriores a los sucesos para aprender de las experiencias y mejorar continuamente los procesos.
- Realizar auditorías periódicas de la estructura de supervisión para identificar posibles vulnerabilidades y áreas de mejora. Esto ayudara a mantener la infraestructura de acuerdo con las mejores prácticas de seguridad.

9. En el domino supervisar, evaluar y valorar (MEA) la primera práctica clave que se centra en “Establecer un enfoque de supervisión” se identificó un importante desafío, ya que el nivel de cumplimiento es de solo 77%. Este resultado plantea dudas sobre la eficacia del enfoque de supervisión actual y la necesidad de investigar las razones de este bajo rendimiento.

Comentario

El bajo nivel de cumplimiento del 77% en la práctica MEA01.01 podría atribuirse a diversos factores, los cuales podrían ser una falta de alineación entre los objetivos de supervisión y las metas de la organización. Es fundamental examinar estos aspectos para comprender plenamente las razones de la baja valoración y adoptar las medidas correctivas adecuadas.

Conclusión ´

La práctica clave indica una posible insuficiencia en la eficacia del enfoque de supervisión actual. Esta actividad es esencial para conseguir los objetivos de la cooperativa, y una aplicación deficiente puede repercutir negativamente en la toma de decisiones y la eficacia operativa.

Recomendaciones

- Llevar a cabo una reevaluación detallada de los objetivos de supervisión para garantizar la conformidad con los objetivos de la organización. Es fundamental que la actividad este directamente vinculada a la obtención de los objetivos estratégicos.
- Actualizar las herramientas utilizadas para aumentar la eficacia y precisión de los procedimientos de inspección.
- Aplicar un sistema de evaluación continua para comprobar la eficacia del enfoque de la supervisión. Esto podría incluir revisiones periódicas y un análisis de los indicadores clave de rendimiento.

10. La práctica clave MEA02.08 se centra en la ejecución de las iniciativas de seguridad. Su objetivo es asegurar que las acciones planificadas con el fin de garantizar la calidad y la conformidad se lleve a cabo. Sin embargo, se ha detectado que esta práctica tiene un nivel de cumplimiento de 73% lo que indica una brecha significativa en la aplicación efectiva de las medidas se aseguramiento propuestas dentro de la organización.

Comentario

El bajo nivel que presenta esta práctica clave puede deberse a una variedad de factores, es posible que existan limitaciones en la comprensión y aplicación de las iniciativas por parte del personal. si no se comunica claramente la importancia y los beneficios de estas iniciativas el personal no podría realizarlo de manera eficiente.

Conclusión

La evaluación revela la necesidad de abordad las insuficiencias encontradas en la ejecución de las iniciativas de aseguramiento. Es fundamental reforzar la comprensión y compromiso del personal, asignar los recursos adecuados y mejorar la comunicación interna, además la identificación de áreas específicas de mejora para optimizar los procesos y garantizar un cumplimiento más sólido en el futuro.

Recomendaciones

- Se debe realizar actividades de formación para el personal, haciendo hincapié en la importancia y las ventajas de las iniciativas de aseguramiento.
- Es necesario asignar recursos adicionales en función de las necesidades identificadas para garantizar el éxito de la aplicación.
- Establecer canales de comunicación claros y abiertos para hacer más fácil el cambio de información relacionada con las prácticas de aseguramiento. Realizar revisiones periódicas de los avances y ajustar las estrategias según sea necesario.

11. En la práctica clave MEA03.03 que se centra en "Confirmar el cumplimiento de los requisitos externos, se ha observado un desafío notable, ya que el porcentaje de cumplimiento es bajo, alcanzado solo el 70%. Esta situación plantea duda sobre la eficacia del proceso de confirmación y la necesidad de investigar las razones asociadas para mejorar el rendimiento.

Comentario

El bajo porcentaje de cumplimiento del 70% en la práctica clave podría deberse a diversos aspectos. Podría ser por una falta de clarificación en los requisitos externos, una debilidad en los mecanismos de seguimiento o incluso una falta de recursos necesarios para garantizar el cumplimiento. Es fundamental realizar un estudio exhaustivo para identificar las causas y ejecutar acciones correctivas eficaces.

Conclusión

El nivel de cumplimiento de dicha práctica indica una posible deficiencia en la conformidad con los requisitos externos es importante para la fiabilidad de la organización y su capacidad de actuar de forma ética y legal. El incumplimiento puede tener consecuencias negativas tanto a nivel de reputación como operativo.

Recomendaciones

- Realizar un examen detallado de los requisitos externos para garantizar una comprensión completa. Esto puede incluir una revisión frecuente de las normas y reglamentos aplicables que puedan tener un impacto en la cooperativa.
- Mejorar la calidad de la transmisión tanto interna como externa sobre los requisitos, y asegurarse que todo el personal conoce los requisitos externos aplicables y sus responsabilidades asociadas.
- Aplicar una matriz de seguimiento para garantizarse que la organización está al tanto de cualquier cambo en los requisitos externos.
- Garantizar una asignación de recurso adecuada, tanto de personal como financiero, para cumplir los requisitos externos.

12. La práctica clave MEA03.04 que se basa en la obtención de garantías de cumplimiento de los requisitos externos, se ha identificado una situación delicada, ya que le porcentaje de cumplimiento es bajo, alcanzando solo el 70%. Este resultado lleva a cuestionarse la eficacia del proceso para cumplir los requerimientos externos, así como la necesidad de examinar las razones de este bajo rendimiento.

Comentario

En las Prácticas MEA03.04 con el bajo índice puede atribuirse a diversos factores, podría ser el resultado de la ineficiencia en la obtención de garantías, la falta de claridad en los procesos o incluso deficiencias en la comunicación externa. Es fundamental realizar un análisis exhaustivo para comprender las causas de este rendimiento y desarrollar estrategias para superar estos inconvenientes.

Conclusión

El nivel de cumplimiento del 70% de dicha práctica indica una posible debilidad en los procesos de garantía de conformidad. Esto puede influir negativamente en la reputación y la integridad de la organización, así como exponerla a riesgos legales y reglamentarias.

Recomendaciones

- Llevar a cabo revisiones exhaustivas de los procesos asociados a la obtención de garantías de conformidad. con el fin de identificar deficiencias para mejorar la eficacia del proceso.
- Mejorar el cumplimiento y las relaciones con las partes externa implicadas en el proceso.
- Realizar auditorías periódicas para obtener información y validar el cumplimiento de las Prácticas.
- Capacitar al personal en la interpretación y aplicación efectiva de los requisitos externos adecuados.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Al elaborar un diagnóstico basado en los componentes del modelo COSO ERM se determina que los niveles de riesgo y confianza son fundamentales para la dirección de la empresa en materia de información. Además, la evaluación del nivel de madurez por departamento añade un aspecto esencial a este proceso, demostrando que la cooperativa ha alcanzado un alto grado de madurez en la administración de riesgos. Este resultado indica que los departamentos han establecido controles eficaces y han desarrollado una cultura de responsabilidad con respecto al gobierno y cultura organizacional.

- El análisis a los activos de información según las normas ISO27000 proporciona una visión detallada de la cooperativa con respecto a los principales fundamentos de la información. La aplicación de estas normas permite establecer un esquema sólido que permita identificar, evaluar y gestionar los riesgos que eventualmente puedan surgir. Al desarrollar la matriz del nivel de tasación se destaca la necesidad crítica de abordar de forma preventiva los riesgos asociados a estos activos de información.

- Al aplicar el marco de referencia COBIT aporta una valiosa perspectiva sobre la gestión y el gobierno de las tecnologías de la información en la cooperativa. Durante la evaluación se detecta varios hallazgos que requieren la atención inmediata. Estos resultados indican una oportunidad para mejorar la eficiencia, la eficacia y la seguridad en áreas específicas del entorno de TI mediante la implementación de medidas correctivas y preventivas para fortalecer la madurez y el rendimiento de la organización.

4.2 Recomendaciones

- Es esencial que se tome medidas para salvaguardar la información crítica de la cooperativa, como la implementación de controles de seguridad adicionales, revisiones periódicas de las políticas y formación continua del personal sobre las mismas, así como el cumplimiento de las normas. Además, es fundamental alentar una cultura de seguridad en la que todos los miembros conozcan el valor de la seguridad de la información y se comprometan con la empresa.

- La evaluación de riesgos debe ser un proceso constante e integrado que incluya la detección de amenazas emergentes y la adaptación de los controles en consecuencia. La aplicación de sistemas de seguimiento continuo y la realización de auditorías periódicas ayudaran a verificar la eficacia de los controles y la alineación con las mejores prácticas. Es fundamental revisar y actualizar la documentación sobre procesos y políticas para que refleje con exactitud las operaciones actuales y cumplan las normas establecidas. Además, es importante garantizar que la documentación sea de fácil acceso para el personal esencial, ya que esto facilita la comprensión y el cumplimiento de los procedimientos fijados.

- Se sugiere dar cumplimiento a las políticas establecidas para la gestión y gobierno de las TI, siendo fundamental el cumplimiento, monitoreo y seguimiento continuo, ya que, de esta manera se protege los activos de información de la cooperativa, la información personal de sus clientes, así como la eficacia en la ejecución de sus operaciones.

REFERENCIAS BIBLIOGRÁFICAS

Albarracín, L. O., Marín, C. M., Lozada, J. C., & Martínez, J. P. (2021). Computer audit within the company “promaelec” of the city of quevedo, during covid-19. *Universidad y Sociedad*, *13*(5), 345-354.

Alberto, M. S. (2022). Modelo de gestión de seguridad de la información en entidades financieras cooperativas. *Braz Dent J.*, *33*(1), 1-12.

Alvarado, K. C. (2014). *Aplicación Del Marco De Referencia Itil Para Optimización De Procesos En Áreas De Tecnologías De La Información De Empresas De Telecomunicaciones*. http://repositorio.puce.edu.ec/bitstream/handle/22000/6383/9.21.000543.pdf?sequence=4

Barrera, C. (2019). *Telecomunicaciones E Industrial*. 1-2. https://repositorio.uta.edu.ec/bitstream/123456789/29843/1/Tesis_t1584msi.pdf

Bedor, D., Carrera, J., & Borja, E. I. (2020). *Auditoría financiera para el control interno en los procesos departamentales de una empresa*. *5*(03), 903-921. https://doi.org/10.23857/pc.v5i3.1520

Bertalanffy, L. Von. (1989). Teoría general de los sistemas: Fundamentos, Desarrollo, Aplicaciones; General System Theory: Foundations, Development, Applications. En *Teoría general de los sistemas: fundamentos, desarrollo, aplicaciones* (Número 65, p. 336). https://archivosociologico.files.wordpress.com/2010/08/teoria-general-de-los-sistemas-ludwig-von-bertalanffy.pdf

Canaza, A., & Torres, L. (2019). Gestión de riesgos empresariales COSO ERM 2017 y la prevención de fraude en las empresas del sector industrial que cotizan en la Bolsa de Valores de Lima (Lima Metropolitana - Callao 2018). En *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://repositorioacademico.upc.edu.pe/handle/10757/628051

Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda. (2023). *Acerca de*

nosostros. https://coacuniblock.fin.ec/Acerca/coac-uniblock

Cuasapaz Narvaez, K. A., & Landázuri Narvaez, K. D. (2023). *Universidad politécnica estatal del carchi*.

Escrivá, G., Romero, R., Ramada, D., & Onrubia, R. (2013). *Seguridad informática*.

Espinoza Farfán, V. N., & Vázquez Loaiza, J. P. (2020). Determinantes del control interno en la gestión del crédito de las cooperativas del Ecuador. *Apuntes Contables*, *27*, 95-111. https://doi.org/10.18601/16577175.n27.06

Flores, D. (2022). Facultad de Contabilidad y Auditoría. *Universidad Técnica de Ambato*, 96. https://repositorio.uta.edu.ec/jspui/handle/123456789/35167

Haghighat, M. H., & Li, J. (2021). Intrusion detection system using voting-based neural network. *Tsinghua Science and Technology*, *26*(4), 484-495. https://doi.org/10.26599/TST.2020.9010022

Hernandez, A. (2003). Los Sistemas de Información: Evolución y Desarrollo. *Dialnet*, 14. https://dialnet.unirioja.es/descarga/articulo/793097.pdf

Hernández, J. (2019). COBIT , una metodología que genera valor en las empresas. *Universidad Piloto de Colombia*, 1-8. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4677/00004999.pdf?sequence=1&isAllowed=y

ISACA. (2012). COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. En *Guía de inspiración para la implementación de PRME: Segunda Edición: Aprender para Avanzar* (Vol. 147, Número 17). https://doi.org/10.9774/gleaf.9781783537846_16

ISACA. (2012b). *Procesos Catalizadores*.

Lapiedra, R., Forés, B., Puig-Denia, A., & Martínez-Cháfer, L. (2021). Introducción a la gestión de sistemas de información en las empresas. En *Introducción a la gestión de sistemas de información en las empresas*. Universitat Jaume I. https://doi.org/10.6035/Sapientia178

Lema, R., & Donoso, D. (2018). Implementación de un sistema de gestion de seguridad de información basado en la norma ISO 27001:2013 para el control fisico y digital de documentos aplicando a la empresa LOCKERS S.A. *Trabajo De Titulación*, *4*(3), 121. http://repositorio.espe.edu.ec/handle/21000/14397

Liu, W., Huang, Q., Chen, X., & Li, H. (2021). Efficient functional encryption for inner product with simulation-based security. *Cybersecurity*, *4*(1), 2. https://doi.org/10.1186/s42400-020-00067-1

Llano, A., Gaibor, M., Cruz, C., & Cadena, J. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Revista Ciencia de la Ingeniería y aplicadas*, *5*(2).

Machuca, L. A. (2021). *Plan director de seguridad de la información para el departamento de tecnologías del Hospital Francisco Icaza Bustamante*. *669*.

Manrique, J. M. (2019). Introducción a la Auditoria. En *Universidad Católico los Ángeles Chimbote*. http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Mora, J., Díaz, R., Zhuma, E., & Díaz, E. (2020). *El sistema de gestión de seguridad de la informcación bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador)*. *16*, 546-559.

Muñoz, H., Zapata, L. G., Requena, D. M., & Villadiego, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia*, *24*(2). https://doi.org/10.37960/revista.v24i2.31508

Muñoz Pinto, O. G. (2020). Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el departamento de tecnologías de la información en la Cooperativa de ahorro y credito Indigena SAC. *Trabajo de titulación*. https://repositorio.uta.edu.ec/bitstream/123456789/31305/1/t1709si.pdf

Organización Internacional de Estandarización. (2017). Normas ISO y su cobertura. *Revista Panorama Contable Contaduria Pública*, 1-10.

http://www.eafit.edu.co/escuelas/administracion/publicaciones/panorama-contable/actualidad/Documents/Boletin-1-NORMAS-ISO-Y-SU-COBERTURA.pdf

Párraga, F. M., & Lara, A. S. (2013). Aplicación de la teoría de los procesos transformados y alterados a la auditoría. *Escuela Politécnica del Ejécito*, 150.

Pérez, A., & Robayo, O. (2019). Diseño del sistema de gestión de seguridad de la información SGSI. *Progress in Retinal and Eye Research*, *561*(3), S2-S3.

Quillupangui, D. A. (2019). Auditoría Informática Mediante Cobit 5 Para El Área Informática En La Empresa Rosas Del Corazón. *Universidad Técnica De Cotopaxi*, 153.

Ramirez, A. del P., Alarcón, G., Centeno, E., & Viscarra, C. (2022). *Análisis de los tipos de auditoría (post pandemia)*. https://www.researchgate.net/publication/367000090

Rojas, H. (2019). Aplicación de la metodología MAGERIT para el análisis de riesgos de los sistemas de control en la estación Tenay del oleoducto. *Universidad Nacional abierta y a distancia Ciencias básicas, tecnologías e ingeniería*, 97.

Sabillón, R., & Cano, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33-48. https://doi.org/10.17013/risti.32.33-48

Sánchez Ch, W. (2021). *Teoría de la auditoría*. Grupo Editorial Nueva Legislación SAS. https://elibro-net.uta.lookproxy.com/es/ereader/uta/188499

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

Santa Cruz, M. (2015). El control interno basado en el modelo COSO. *Revista de Investigación Valor Contable*, *1*(1), 36-40.

https://doi.org/10.17162/rivc.v1i1.832

Santacruz, J. J., Vega, C. R., Pinos, L. F., & Cárdenas, O. E. (2017). Sistema cobit en los procesos de auditorías de los de sistemas informáticos. *Journal of Science and Research: Revista Ciencia e Investigación*, *2*(8), 65. https://doi.org/10.26910/issn.2528-8083vol2iss8.2017pp65-68

Serrano, C. L., Cruz, R. I., Salcedo, J., & Malagón, A. C. (2022). La gestión del conocimiento en la auditoría interna: un modelo teórico-relacional para el crecimiento empresarial. *Información tecnológica*, *33*(1), 3-10. https://doi.org/10.4067/S0718-07642022000100003

Sisti, M. (2019). *Seguridad informática: La protección de la información en una empresa Vitivícola de Mendoza 2019*. 1-86. https://bdigital.uncu.edu.ar/15749

Suáres, A., Sotomayor, E., & Medina, M. (2019). *Perdida De Datos , Con Políticas De Seguridad , Mediante El Control De Dominio Por Medio De Una Herramienta De Terceros*. http://hdl.handle.net/20.500.12494/12736

Sugawara, E., & Nikaido, H. (2021). Auditoría informática, para la evaluación de riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito PRODVISIÓN, de la Provincia de Tungurahua, Canton Pelileo. *Trabajo de titulación*, 163. https://repositorio.uta.edu.ec/jspui/handle/123456789/32712

Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management*, *57*(6), 102355. https://doi.org/10.1016/j.ipm.2020.102355

ANEXOS

Anexo 1

CUESTIONARIO DE CONTROL INTERNO

No.	DESCRIPCIÓN	RESPUESTAS		
		SI	NO	N/A
A	**SUBCOMPONENTE: Gobierno y cultura**			
1	¿Existe políticas en el área de sistemas que incluyen controles especificos de TI?	X		
2	¿Se revisan periódicamente las responsabilidades y los controles relacionados con TI en el área de sistemas?	X		
3	¿La conservación de evidencias, como pistas de auditoría o de gestión, se realiza de forma sistemática en el área de sistemas?	X		
4	¿El área de sistemas asigna o define claramente 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	¿El área de sistemas considera las oportunidades de forma sistemática con el objetivo de incorporarlas a la empresa?	X		
7	¿Se realiza un control periódico para garantizar que los responsables de los riesgos cumplen con sus funciones en el área de sistema?	X		
8	¿Introduce capacidades, destrezas y conocimiento relacionados con los riesgos tecnológicos?	X		
9	¿El área de sistemas demuestra un compromiso permanente con los valores éticos ?	X		
B	**SUBCOMPONENTE: Estrategias y Objetivos**			
1	¿El área de sistemas emplea a especialistas, tanto internos como externos, con experiencia en auditoría de TI?		X	
2	¿El área de sistemas considera los riesgos relacionados con factores internos y externos que puede afectar a la empresa?	X		
3	¿El departamento de sistemas analiza las debilidades, amenazas, fortalezas y oportunidades en la empresa?	X		
4	¿Se evalúa con frecuencia la materialidad de las amenazas para determinar su impacto en la empresa?	X		
5	¿Se evalúa la utilización de determinados recursos disponibles en el área de sistemas de la empresa en relación con los riesgos identificados?	X		
C	**COMPONENTE: Desempeño**			
1	¿Se toman medidas específicas para garantizar logicamente y fisicamente la integridad de las herramientas utilizadas en la infraestructura de TI?	X		
2	¿Se ha implementado una tecnología de filtros de seguridad en los puntos de conexión externa, como Internet, de acuerdo con la política de seguridad de la empresa?	X		
3	¿Se han implantado controles preventivos, detectivos y correctivos que hayan demostrado su eficacia en la prevención y resolución de incidentes del sistema?		X	

4	¿Dispone de registros o notificaciones que muestren cuándo fallan los parámetros de control en el entorno del sistema?			X
5	¿Se lleva a cabo una evaluación de los riesgos en el area de sistema para establecer su prioridad?	X		
6	¿El área de sistemas comprende los criterios establecidos por la entidad para priorizar los riesgos?	X		
7	¿El área de sistemas selecciona los métodos de evaluación adecuados para valorar con precisión el riesgo?		X	
8	¿El área de sistemas selecciona los datos, parámetros y premisas adecuados y documenta claramente el proceso?	X		
D	**COMPONENTE: Revisión**			
1	¿En el área de sistemas se emplea mecanismos de control para gestionar eficazmente el acceso y la autenticación?	X		
2	¿El área de sistemas ha implementado un software antivirus y se realiza su mantenimiento?	X		
3	¿Existe una revisión periódica para garantizar que se han completado todas las evaluaciones de vulnerabilidad y se han abordado adecuadamente los riesgos en el área del sistema?		X	
4	¿El departamento de sistemas identifica y evalúa los cambios internos y externos que pueden tener un impactosignificativo a las estrategia u objetivos de la empresa?	X		
5	¿El departamento de sistemas revisa periodicamente las actividades de la ERM para identificar la necesidad de las revisar los procesos y las capacidades?		X	
6	¿Las revisiones de las amenazas y riesgos potenciales se documentan sistemáticamente en el área de sistemas?		X	
7	¿Existe un mecanismo para adoptar medidas preventivas y correctivas basadas en la evaluación de los cambios sustanciales en respuesta a la aparición de amenazas en la zona del sistema?	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	¿Las copias de seguridad en el área de sistemas permiten resolver satisfactoriamente las pérdidas de información o los errores causados por la materialización de amenazas.?	X		
2	¿Se llevan las copias de seguridad a dispositivos externos o en la nube en el departamento de sistemas?	X		
3	¿Está protegido eficazmente el acceso físico a los sistemas informáticos en la área de sistemas?	X		
4	¿En el dearatamento de sistemas 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 usuraios 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 2

DEPARTAMENTO	COMPONENTE	NIVEL DE MADUREZ	CALIFICACION COMPONENTE	PROMEDIO
Sistemas	Gobierno y cultura	4,67	EFEFCTIVO	**4,23**
	Estrategias y Objetivos	4,60	EFEFCTIVO	
	Desempeño	4,13	EFEFCTIVO	
	Revisión	4,13	EFEFCTIVO	
	Información, comunicación y reporte	4,14	EFEFCTIVO	
	Sistemas de seguridad de información	3,72	CUMPLIMIENTO BASICO TACTICO	
Gerencia	Gobierno y cultura	4,67	EFEFCTIVO	**4,36**
	Estrategias y Objetivos	4,60	EFEFCTIVO	
	Desempeño	4,50	EFEFCTIVO	
	Revisión	4,25	EFEFCTIVO	
	Información, comunicación y reporte	4,43	EFEFCTIVO	
	Sistemas de seguridad de información	3,72	CUMPLIMIENTO BASICO TACTICO	
Caja	Gobierno y cultura	4,89	EFEFCTIVO	**4,37**
	Estrategias y Objetivos	4,40	EFEFCTIVO	
	Desempeño	4,38	EFEFCTIVO	
	Revisión	4,13	EFEFCTIVO	
	Información, comunicación y reporte	4,57	EFEFCTIVO	
	Sistemas de seguridad de información	3,89	CUMPLIMIENTO BASICO TACTICO	
Creditos	Gobierno y cultura	4,89	EFEFCTIVO	**4,61**
	Estrategias y Objetivos	4,20	EFEFCTIVO	
	Desempeño	4,63	EFEFCTIVO	
	Revisión	4,75	EFEFCTIVO	
	Información, comunicación y reporte	5,00	EFEFCTIVO	
	Sistemas de seguridad de información	4,22	EFEFCTIVO	
Servico al Cliente	Gobierno y cultura	4,44	EFEFCTIVO	**3,81**
	Estrategias y Objetivos	3,60	CUMPLIMIENTO BASICO TACTICO	
	Desempeño	3,75	CUMPLIMIENTO BASICO TACTICO	
	Revisión	3,38	CUMPLIMIENTO BASICO TACTICO	
	Información, comunicación y reporte	4,29	EFEFCTIVO	
	Sistemas de seguridad de información	3,39	CUMPLIMIENTO BASICO TACTICO	
Captaciones	Gobierno y cultura	4,78	EFEFCTIVO	**4,43**
	Estrategias y Objetivos	4,4	EFEFCTIVO	
	Desempeño	4,625	EFEFCTIVO	
	Revisión	4,375	EFEFCTIVO	
	Información, comunicación y reporte	4,57	EFEFCTIVO	
	Sistemas de seguridad de información	3,83	CUMPLIMIENTO BASICO TACTICO	
Contabilidad	Gobierno y cultura	5	EFEFCTIVO	**4,67**
	Estrategias y Objetivos	5	EFEFCTIVO	
	Desempeño	5	EFEFCTIVO	
	Revisión	4,5	EFEFCTIVO	
	Información, comunicación y reporte	5	EFEFCTIVO	
	Sistemas de seguridad de información	3,5	CUMPLIMIENTO BASICO TACTICO	

Anexo 3

Activos	Riesgos	Posibilidad de Ocurrencia	Impacto del Riesgo	Medición del Riesgo
Equipo de Cómputo	Pueden dañar o comprometer la integridad de los datos y sistemas.	3	3	9
	Acceso a la información confidencial de los programas instalados.	2	2	4
Impresoras	Pérdida de funcionalidad de las impresoras afectando la eficiencia operativa.	1	2	2
Equipo biométrico	Acceso no autorizado comprometiendo los datos biométricos almacenados.	1	4	4
Cámaras de vigilancia	La falta de funcionalidad de las cámaras puede tener un impacto negativo en la vigilancia y la seguridad en general.	2	3	6
Servidor/Red compartida	Pérdida de datos confidenciales transmitidos a través de la red compartida.	2	3	6
Router	La ausencia de funcionalidad del router puede perjudicar en la conectividad.	2	3	6
Software	Pérdida de datos sensibles almacenados en el sistema.	3	3	9
Pagina web	Proporcionar información desactualizada a los clientes lo que puede afectar en la confianza de la empresa.	1	2	2
Sistemas	Pérdida o manipulación de datos críticos almacenados en el sistema.	1	4	4

Gerencia	Pérdida de confianza de los empleados y socios si se revela información crítica o se toma decisiones riesgosas.	1	3	3
Créditos	Incumplimiento de las regulaciones y normativas planteadas por la entidad.	2	3	6
Caja	Pérdidas económicas debido a robos, fraudes o errores en la gestión del efectivo.	1	5	5
Atención al cliente	La ausencia de ayuda hacia los clientes afectará en la satisfacción y fidelidad de los mismos.	3	3	9
	Quejas hacia el personal de la empresa provocando una calificación deficiente en su desempeño.	3	4	12
Captaciones	Pérdida económica debido a practicas de captación inseguras o fraudes.	1	4	4
Contabilidad	Pérdida económica debido a practicas contables inseguras afectando así la imagen y reputación de la entidad.	2	5	10
Comité de riesgo	Toma de decisiones poco eficaces basadas en evaluaciones de riesgos incompletas por parte del comité.	2	2	4
Comité de cumplimiento	Miembros del consejo que carecen de conocimientos especializados en las áreas relevantes de cumplimiento.	2	3	6
Asesor jurídico	Gestión ineficiente de documentos legales que podrían resultar en la pérdida de información crucial.	3	3	9

Anexo 4

Procesos	Prácticas clave de gobierno	N.º de actividades
EVALUAR, ORIENTAR Y SUPERVISAR		
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	• EDM01.01 Evaluar el sistema de gobierno • EDM01.02 Orientar el sistema de gobierno. • EDM01.03 Supervisar el sistema de gobierno.	8 Actividades 6 Actividades 6 Actividades
EDM02 Asegurar la Entrega de Beneficios	• EDM02.01 Evaluar la optimización del valor. • EDM02.02 Orientar la optimización del valor. • EDM02.03 Supervisar la optimización del valor	8 Actividades 7 Actividades 5 Actividades
EDM03 Asegurar la Optimización del Riesgo	• EDM03.01 Evaluar la gestión de riesgos • EDM03.02 Orientar la gestión de riesgos • EDM03.03 Supervisar la gestión de riesgos	6 Actividades 6 Actividades 4 Actividades
EDM04 Asegurar la Optimización de Recursos	• EDM04.01 Evaluar la gestión de recursos • EDM04.02 Orientar la gestión de recursos. • EDM04.03 Supervisar la gestión de recursos.	5 Actividades 5 Actividades 3 Actividades
EDM05 Asegurar la Transparencia hacia las Partes Interesadas	• EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. • EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes • EDM05.03 Supervisar la comunicación con las partes interesadas	3 Actividades 4 Actividades 3 Actividades
PLANEAR, PLANIFICAR Y ORGANIZAR		
APO01 Gestionar el Marco de Gestión de TI	• APO01.01 Definir la estructura organizativa. • APO01.02 Establecer roles y responsabilidades • APO01.03 Mantener los elementos catalizadores del sistema de gestión. • APO01.04 Comunicar los objetivos y la dirección de gestión. • APO01.05 Optimizar la ubicación de la función de TI. • APO01.06 Definir la propiedad de la información (datos) y del sistema • APO01.07 Gestionar la mejora continua de los procesos • APO01.08 Mantener el cumplimiento con las políticas y procedimientos.	12 Actividades 7 Actividades 9 Actividades 3 Actividades 3 Actividades 4 Actividades 5 Actividades 5 Actividades

APO02 Gestionar la Estrategia	• APO02.01 Comprender la dirección de la empresa.	6 Actividades
	• APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.	4 Actividades
	• APO02.03 Definir el objetivo de las capacidades de TI.	6 Actividades
	• APO02.04 Realizar un análisis de diferencias.	4 Actividades
	• APO02.05 Definir el plan estratégico y la hoja de ruta	7 Actividades
	• APO02.06 Comunicar la estrategia y la dirección de TI.	4 Actividades
APO03 Gestionar la Arquitectura Empresarial	• APO03.01 Desarrollar la visión de la arquitectura de empresa	12 Actividades
	• APO03.02 Definir la arquitectura de referencia.	9 Actividades
	• APO03.03 Seleccionar las oportunidades y las soluciones.	10 Actividades
	• APO03.04 Definir la implantación de la arquitectura.	3 Actividades
	• APO03.05 Proveer los servicios de arquitectura empresarial.	5 Actividades
APO04 Gestionar la Innovación	• APO04.01 Crear un entorno favorable para la innovación.	5 Actividades
	• APO04.02 Mantener un entendimiento del entorno de la empresa	3 Actividades
	• APO04.03 Supervisar y explorar el entorno tecnológico.	4 Actividades
	• APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	5 Actividades
	• APO04.05 Recomendar iniciativas apropiadas adicionales.	4 Actividades
	• APO04.06 Supervisar la implementación y el uso de la innovación.	4 Actividades
APO05 Gestionar el Portafolio	• APO05.01 Establecer la mezcla del objetivo de inversión.	5 Actividades
	• APO05.02 Determinar la disponibilidad y las fuentes de fondos.	3 Actividades
	• APO05.03 Evaluar y seleccionar los programas a financiar.	6 Actividades
	• APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	8 Actividades
	• APO05.05 Mantener los portafolios	3 Actividades
	• APO05.06 Gestionar la consecución de beneficios	3 Actividades
APO06 Gestionar el Presupuesto y los Costes	• APO06.01 Gestionar las finanzas y la contabilidad.	5 Actividades
	• APO06.02 Priorizar la asignación de recursos	4 Actividades
	• APO06.03 Crear y mantener presupuestos.	7 Actividades
	• APO06.04 Modelar y asignar costes.	6 Actividades
	• APO06.05 Gestionar costes.	9 Actividades

APO07 Gestionar los Recursos Humanos	• APO07.01 Mantener la dotación de personal suficiente y adecuada	5 Actividades
	• APO07.02 Identificar personal clave de TI.	4 Actividades
	• APO07.03 Mantener las habilidades y competencias del personal.	7 Actividades
	• APO07.04 Evaluar el desempeño laboral de los empleados.	8 Actividades
	• APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	4 Actividades
	• APO07.06 Gestionar el personal contratado	8 Actividades
AP008 Gestionar las relaciones	• APO08.01 Entender las expectativas del negocio.	7 Actividades
	• APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	5 Actividades
	• APO08.03 Gestionar las relaciones con el negocio.	5 Actividades
	• APO08.04 Coordinar y comunicar.	4 Actividades
	• APO08.05 Proveer datos de entrada para la mejora continua de los servicios	3 Actividades
AP009 Gestionar los acuerdos de servicio	• APO09.01 Identificar servicios TI.	6 Actividades
	• APO09.02 Catalogar servicios basados en TI.	3 Actividades
	• APO09.03 Definir y preparar acuerdos de servicio.	5 Actividades
	• APO09.04 Supervisar e informar de los niveles de servicio	5 Actividades
	• APO09.05 Revisar acuerdos de servicio y contratos.	1 Actividades
APO10 Gestionar los Proveedores	• APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.	4 Actividades
	• APO10.02 Seleccionar proveedores	7 Actividades
	• APO10.03 Gestionar contratos y relaciones con proveedores.	8 Actividades
	• APO10.04 Gestionar el riesgo en el suministro.	2 Actividades
	• APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor.	6 Actividades
APO11 Gestionar la Calidad	• APO11.01 Establecer un sistema de gestión de la calidad (SGC).	8 Actividades
	• APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	2 Actividades
	• APO11.03 Enfocar la gestión de la calidad en los clientes.	6 Actividades
	• APO11.04 Supervisar y hacer controles y revisiones de calidad	7 Actividades
	• APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	3 Actividades
	• APO11.06 Mantener una mejora continua	8 Actividades

APO12 Gestionar el Riesgo	• APO12.01 Recopilar datos	7 Actividades
	• APO12.02 Analizar el riesgo.	7 Actividades
	• APO12.03 Mantener un perfil de riesgo.	7 Actividades
	• APO12.04 Expresar el riesgo.	5 Actividades
	• APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	3 Actividades
	• APO12.06 Responder al riesgo.	4 Actividades
APO13 Gestionar la Seguridad	• APO13.01 Establecer y mantener un SGSI.	7 Actividades
	• APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	7 Actividades
	• APO13.03 Supervisar y revisar el SGSI.	5 Actividades
CONSTRUIR, ADQUIRIR E IMPLEMENTAR		
BAI01 Gestión de Programas y Proyectos	• BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.	2 Actividades
	• BAI01.02 Iniciar un programa.	6 Actividades
	• BAI01.03 Gestionar el compromiso de las partes interesadas.	4 Actividades
	• BAI01.04 Desarrollar y mantener el plan de programa.	7 Actividades
	• BAI01.05 Lanzar y ejecutar el programa.	5 Actividades
	• BAI01.06 Supervisar, controlar e informar de los resultados del programa.	7 Actividades
	• BAI01.07 Lanzar e iniciar proyectos dentro de un programa.	6 Actividades
	• BAI01.08 Planificar proyectos	6 Actividades
	• BAI01.09 Gestionar la calidad de los programas y proyectos.	4 Actividades
	• BAI01.10 Gestionar el riesgo de los programas y proyectos.	6 Actividades
	• BAI01.11 Supervisar y controlar proyectos	10 Actividades
	• BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.	7 Actividades
	• BAI01.13 Cerrar un proyecto o iteración.	5 Actividades
	• BAI01.14 Cerrar un programa	3 Actividades
BAI02 Gestionar la Definición de Requisitos	• BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.	8 Actividades
	• BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.	4 Actividades
	• BAI02.03 Gestionar los riesgos de los requerimientos.	3 Actividades
	• BAI02.04 Obtener la aprobación de los requerimientos y soluciones	2 Actividades

BAI03 Gestionar la Identificación y Construcción de Soluciones	• BAI03.01 Diseñar soluciones de alto nivel.	4 Actividades
	• BAI03.02 Diseñar los componentes detallados de la solución	10 Actividades
	• BAI03.03 Desarrollar los componentes de la solución	6 Actividades
	• BAI03.04 Obtener los componentes de la solución	5 Actividades
	• BAI03.05 Construir soluciones.	8 Actividades
	• BAI03.06 Realizar controles de calidad.	4 Actividades
	• BAI03.07 Preparar pruebas de la solución	3 Actividades
	• BAI03.08 Ejecutar pruebas de la solución	5 Actividades
	• BAI03.09 Gestionar cambios a los requerimientos.	3 Actividades
	• BAI03.10 Mantener soluciones.	5 Actividades
	• BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.	4 Actividades
BAI04 Gestionar la Disponibilidad y la Capacidad	• BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	4 Actividades
	• BAI04.02 Evaluar el impacto en el negocio.	7 Actividades
	• BAI04.03 Planificar requisitos de servicio nuevos o modificados.	5 Actividades
	• BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.	4 Actividades
	• BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	5 Actividades
BAI05 Gestionar la Facilitación del Cambio Organizativo	• BAI05.01 Establecer el deseo de cambiar	4 Actividades
	• BAI05.02 Formar un equipo de implementación efectivo.	3 Actividades
	• BAI05.03 Comunicar la visión deseada.	5 Actividades
	• BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.	6 Actividades
	• BAI05.05 Facilitar la operación y el uso.	2 Actividades
	• BAI05.06 Integrar nuevos enfoques	5 Actividades
	• BAI05.07 Mantener los cambios.	4 Actividades
BAI06 Gestionar los Cambios	• BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.	7 Actividades
	• BAI06.02 Gestionar cambios de emergencia.	4 Actividades
	• BAI06.03 Hacer seguimiento e informar de cambios de estado.	4 Actividades
	• BAI06.04 Cerrar y documentar los cambios	3 Actividades

BAI07 Gestionar la Aceptación del Cambio y la Transición	• BAI07.01 Establecer un plan de implementación. • BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos • BAI07.03 Planificar pruebas de aceptación. • BAI07.04 Establecer un entorno de pruebas. • BAI07.05 Ejecutar pruebas de aceptación • BAI07.06 Pasar a producción y gestionar los lanzamientos. • BAI07.07 Proporcionar soporte en producción desde el primer momento • BAI07.08 Ejecutar una revisión postimplantación.	5 Actividades 9 Actividades 8 Actividades 5 Actividades 11 Actividades 6 Actividades 2 Actividades 5 Actividades
BAI08 Gestionar el Conocimiento	• BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. • BAI08.02 Identificar y clasificar las fuentes de información. • BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. • BAI08.04 Utilizar y compartir el conocimiento. • BAI08.05 Evaluar y retirar la información.	5 Actividades 4 Actividades 4 Actividades 3 Actividades 2 Actividades
BAI09 Gestionar los Activos	• BAI09.01 Identificar y registrar activos actuales. • BAI09.02 Gestionar activos críticos • BAI09.03 Gestionar el ciclo de vida de los activos • BAI09.04 Optimizar el coste de los activos. • BAI09.05 Administrar licencias.	6 Actividades 9 Actividades 9 Actividades 6 Actividades 6 Actividades
BAI10 Gestionar la Configuración	• BAI10.01 Establecer y mantener un modelo de configuración. • BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia. • BAI10.03 Mantener y controlar los elementos de configuración. • BAI10.04 Generar informes de estado y configuración. • BAI10.05 Verificar y revisar la integridad del repositorio de configuración.	2 Actividades 2 Actividades 4 Actividades 3 Actividades 5 Actividades

ENTREGA, SERVICIO Y SOPORTE		
DSS01 Gestionar Operaciones	• DSS01.01 Ejecutar procedimientos operativos	5 Actividades
	• DSS01.02 Gestionar servicios externalizados de TI	4 Actividades
	• DSS01.03 Supervisar la infraestructura de TI	6 Actividades
	• DSS01.04 Gestionar el entorno	8 Actividades
	• DSS01.05 Gestionar las instalaciones	11 Actividades
DSS02 Gestionar Peticiones e Incidentes de Servicio	• DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	5 Actividades
	• DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	3 Actividades
	• DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	3 Actividades
	• DSS02.04 Investigar, diagnosticar y localizar incidentes.	3 Actividades
	• DSS02.05 Resolver y recuperarse de incidentes.	4 Actividades
	• DSS02.06 Cerrar peticiones de servicio e incidentes	2 Actividades
	• DSS02.07 Seguir el estado y emitir informes.	4 Actividades
DSS03 Gestionar Problemas	• DSS03.01 Identificar y clasificar problemas	6 Actividades
	• DSS03.02 Investigar y diagnosticar problemas.	3 Actividades
	• DSS03.03 Levantar errores conocidos.	2 Actividades
	• DSS03.04 Resolver y cerrar problemas.	6 Actividades
	• DSS03.05 Realizar una gestión de problemas proactiva.	6 Actividades
DSS04 Gestionar la Continuidad	• DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.	4 Actividades
	• DSS04.02 Mantener una estrategia de continuidad.	8 Actividades
	• DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	8 Actividades
	• DSS04.04 Ejercitar, probar y revisar el plan de continuidad	6 Actividades
	• DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	4 Actividades
	• DSS04.06 Proporcionar formación en el plan de continuidad.	3 Actividades
	• DSS04.07 Gestionar acuerdos de respaldo.	5 Actividades
	• DSS04.08 Ejecutar revisiones postreanudación.	4 Actividades

DSS05 Gestionar Servicios de Seguridad	• DSS05.01 Proteger contra software malicioso (malware).	6 Actividades
	• DSS05.02 Gestionar la seguridad de la red y las conexiones.	9 Actividades
	• DSS05.03 Gestionar la seguridad de los puestos de usuario final.	9 Actividades
	• DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	8 Actividades
	• DSS05.05 Gestionar el acceso físico a los activos de TI.	7 Actividades
	• DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	5 Actividades
	• DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	5 Actividades
DSS06 Gestionar Controles de Proceso de Negocio	• DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	5 Actividades
	• DSS06.02 Controlar el procesamiento de la información.	8 Actividades
	• DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	6 Actividades
	• DSS06.04 Gestionar errores y excepciones.	5 Actividades
	• DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información	3 Actividades
	• DSS06.06 Asegurar los activos de información.	5 Actividades
SUPERVISAR, EVALUAR Y VALORAR		
MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	• MEA01.01 Establecer un enfoque de la supervisión.	7 Actividades
	• MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.	4 Actividades
	• MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento	5 Actividades
	• MEA01.04 Analizar e informar sobre el rendimiento.	6 Actividades
	• MEA01.05 Asegurar la implantación de medidas correctivas.	4 Actividades
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	• MEA02.01 Supervisar el control interno.	7 Actividades
	• MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	5 Actividades
	• MEA02.03 Realizar autoevaluaciones de control.	7 Actividades
	• MEA02.04 Identificar y comunicar las deficiencias de control.	6 Actividades
	• MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	3 Actividades
	• MEA02.06 Planificar iniciativas de aseguramiento.	3 Actividades
	• MEA02.07 Estudiar las iniciativas de aseguramiento	5 Actividades
	• MEA02.08 Ejecutar las iniciativas de aseguramiento.	8 Actividades

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	• MEA03.01 Identificar requisitos externos de cumplimiento. • MEA03.02 Optimizar la respuesta a requisitos externos. • MEA03.03 Confirmar el cumplimiento de requisitos externos. • MEA03.04 Obtener garantía de cumplimiento de requisitos externos	6 Actividades 2 Actividades 4 Actividades 6 Actividades

Anexo 5

PROCESO	PROPÓSITO	SE GESTIONA	SE GESTIONA (NECESITA MEJORA)
EVALUAR, ORIENTAR Y SUPERVISAR			
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Proporciona un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa.	X	
EDM02 Asegurar la Entrega de Beneficios	Asegura un valor óptimo de las iniciativas de TI, servicios y activos disponibles;	X	
EDM03 Asegurar la Optimización del Riesgo	Asegura que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo		X
EDM04 Asegurar la Optimización de Recursos	Asegura que las necesidades de recursos de la empresa son cubiertas de un modo óptimo	X	
EDM05 Asegurar la Transparencia hacia las Partes Interesadas	Asegura que la comunicación con las partes interesadas sea efectiva y oportuna con el fin de aumentar el desempeño		X
PLANEAR, PLANIFICAR Y ORGANIZAR			
APO01 Gestionar el Marco de Gestión de TI	Proporciona un enfoque de gestión que permite cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, roles y responsabilidades organizativos.	X	
APO02 Gestionar la Estrategia	Alinea los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas.		X
APO03 Gestionar la Arquitectura Empresarial	Representa a los diferentes módulos que componen la empresa y sus interrelaciones permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.	X	

APO04 Gestionar la Innovación	Logra ventaja competitiva, eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos.	X	
APO05 Gestionar el Portafolio	Optimiza el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios.	X	
APO06 Gestionar el Presupuesto y los Costes	Fomenta la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las T	X	
APO07 Gestionar los Recursos Humanos	Optimiza las capacidades de recursos humanos para cumplir los objetivos de la empresa.	X	
AP008 Gestionar las relaciones	Crea mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.	X	
AP009 Gestionar los acuerdos de servicio	Asegura que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa.	X	
APO10 Gestionar los Proveedores	Minimiza el riesgo de proveedores que no rindan y asegurar precios competitivos	X	
APO11 Gestionar la Calidad	Asegura la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas	X	
APO12 Gestionar el Riesgo	Integra la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM)	X	
APO13 Gestionar la Seguridad	Se mantiene el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.		X
CONSTRUIR, ADQUIRIR E IMPLEMENTAR			
BAI01 Gestión de Programas y Proyectos	Alcanza los beneficios de negocio y reducir el riesgo de retrasos mediante la mejora de las comunicaciones y la involucración de usuarios finales.	X	

BAI02 Gestionar la Definición de Requisitos	Crea soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.	X	
BAI03 Gestionar la Identificación y Construcción de Soluciones	Establece soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.	X	
BAI04 Gestionar la Disponibilidad y la Capacidad	Mantiene la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas.	X	
BAI05 Gestionar la Facilitación del Cambio Organizativo	Prepara y compromete a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.	X	
BAI06 Gestionar los Cambios	Posibilita una entrega de los cambios rápida y fiable, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno.	X	
BAI07 Gestionar la Aceptación del Cambio y la Transición	Implementa soluciones de forma segura y en línea con las expectativas y resultados acordados.	X	
BAI08 Gestionar el Conocimiento	Proporciona el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones y aumentar la productividad.		X
BAI09 Gestionar los Activos	Se contabiliza todos los activos de TI y optimización del valor proporcionado por estos activos.		X
BAI10 Gestionar la Configuración	Proporciona suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.	X	
ENTREGA, SERVICIO Y SOPORTE			
DSS01 Gestionar Operaciones	Entrega los resultados del servicio operativo de TI, según lo planificado.		X
DSS02 Gestionar Peticiones e Incidentes de Servicio	Logra una mayor productividad y minimiza las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	X	

DSS03 Gestionar Problemas	Incrementa la disponibilidad, mejora los niveles de servicio, y satisfacción del cliente reduciendo el número de problemas operativos.	X	
DSS04 Gestionar la Continuidad	Continua las operaciones críticas y mantiene la disponibilidad de la información a un nivel aceptable ante el evento de una interrupción significativa.	X	
DSS05 Gestionar Servicios de Seguridad	Minimiza el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.		X
DSS06 Gestionar Controles de Proceso de Negocio	Mantiene la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa.	X	
SUPERVISAR, EVALUAR Y VALORAR			
MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Proporciona transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.		X
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	Ofrece transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones.		X
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Asegura que la empresa cumple con todos los requisitos externos que le sean aplicables.		X

Anexo 6

CUADRO RESUMEN MARCO DE REFERENCIA COBIT 5					
DOMINIO	**PROCESO/ OBJETIVO DE CONTROL**	**PRÁCTICAS CLAVES DE GOBIERNO**	**DETALLE DE LA PRÁCTICA CLAVE DE GOBIERNO**	**NIVEL DE CAPACIDAD**	**NIVEL DE MADUREZ**
EVALUAR, ORIENTAR Y SUPERVISAR	**EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO**	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.	71%	L
		EDM03.02 Orientar la gestión de riesgos	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.	85%	F
		EDM03.03 Supervisar la gestión de riesgos	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	85%	F
	EDM05 ASEGURAR LA TRANSPARENCIA HACIA LAS PARTES INTERESADAS	EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas	Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación)de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación.	63%	L
		EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes	Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.	65%	L
		EDM05.03 Supervisar la comunicación con las parte interesadas	Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.	50%	P

PLANEAR, PLANIFICAR Y ORGANIZAR	**APO02 GESTIONAR LA ESTRATEGIA**	APO02.01 Comprender la dirección de la empresa	Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia)	86%	F
		APO02.02 Evaluar el entorno, capacidades y rendimientos actuales	Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.	78%	L
		APO02.03 Definir el objetivo de las capacidades de TI	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.	70%	L
		APO02.04 Realizar un análisis de diferencias	Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.	66%	L
		APO02.05 Definir el plan estratégico y la hoja de ruta	Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.	75%	L
		APO02.06 Comunicar la estrategia y la dirección de TI	Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa.	78%	L

PLANEAR, PLANIFICAR Y ORGANIZAR	**APO13 GESTIONAR LA SEGURIDAD**	APO13.01 Establecer y mantener un SGSI	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.	63%	L
		APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	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.	76%	L
		APO13.03 Supervisar y revisar el SGSI.	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.	60%	L
CONSTRUIR, ADQUIRIR E IMPLANTAR	**BAI08 GESTIONAR EL CONOCIMIENTO**	BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos	Concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos.	82%	F
		BAI08.02 Identificar y clasificar las fuentes de información	Identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivas de los procesos de negocio y los servicios de TI.	75%	L
		BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento	Organizar la información basándose en criterios de clasificación. Identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información. Identificar propietarios y definir e implementar niveles de acceso a los recursos de información.	77%	L
		BAI08.04 Utilizar y compartir el conocimiento	Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).	77%	L
		BAI08.05 Evaluar y retirar la información	Medir el uso y evaluar la actualización y relevancia de la información. Retirar la información obsoleta.	70%	L

CONSTRUIR, ADQUIRIR E IMPLANTAR	**BAI09 GESTIONAR LOS ACTIVOS**	BAI09.01 Identificar y registrar activos actuales.	Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.	93%	F
		BAI09.02 Gestionar activos críticos	Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.	82%	F
		BAI09.03 Gestionar el ciclo de vida de los activos.	Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.	92%	F
		BAI09.04 Optimizar el coste de los activos	Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.	67%	L
		BAI09.05 Administrar licencias	Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.	82%	F
ENTREGA, SERVICIO Y SOPORTE	**DSS1 GESTIONAR OPERACIONES**	DSS01.01 Ejecutar procedimientos operativos	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	77%	L
		DSS01.02 Gestionar servicios externalizados de TI	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio	83%	F
		DSS01.03 Supervisar la infraestructura de TI	Supervisar las infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.	72%	L
		DSS01.04 Gestionar el entorno	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno	95%	F
		DSS01.05 Gestionar las instalaciones	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	92%	F

ENTREGA, SERVICIO Y SOPORTE	**DSS05 GESTIONAR SERVICIOS DE SEGURIDAD**	DSS05.01 Proteger contra software malicioso (malware).	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).	87%	F
		DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	81%	F
		DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	84%	F
		DSS05.04 Gestionar la identidad del usuario y el acceso lógico	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio	78%	L
		DSS05.05 Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	72%	L
		DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad	78%	L
		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes	68%	L

SUPERVISAR, EVALUAR Y VALORAR	**MEA01 SUPERVISAR, EVALUAR Y VALORAR EL RENDIMIENTO Y LA CONFORMIDAD**	MEA01.01 Establecer un enfoque de la supervisión.	Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	77%	L
		MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.	Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento	79%	L
		MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	80%	L
		MEA01.04 Analizar e informar sobre el rendimiento.	Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.	78%	L
		MEA01.05 Asegurar la implantación de medidas correctivas.	Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	81%	F

SUPERVISAR, EVALUAR Y VALORAR	**MEA02 SUPERVISAR, EVALUAR Y VALORAR EL SISTEMA DE CONTROL INTERNO**	MEA02.01 Supervisar el control interno	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	83%	F
		MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.	90%	F
		MEA02.03 Realizar autoevaluaciones de control.	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.	80%	L
		MEA02.04 Identificar y comunicar las deficiencias de control.	Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.	83%	F
		MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados	Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.	75%	L
		MEA02.06 Planificar iniciativas de aseguramiento.	Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.	83%	F
		MEA02.07 Estudiar las iniciativas de aseguramiento.	Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	87%	F
		MEA02.08 Ejecutar las iniciativas de aseguramiento	Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	73%	L

SUPERVISAR, EVALUAR Y VALORAR	**MEA03 SUPERVISAR, EVALUAR Y VALORAR LA CONFORMIDAD CON LOS REQUERIMIENTOS EXTERNOS**	MEA03.01 Identificar requisitos externos de cumplimiento.	Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.	80%	L
		MEA03.02 Optimizar la respuesta a requisitos externos.	Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.	90%	F
		MEA03.03 Confirmar el cumplimiento de requisitos externos.	Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.	70%	L
		MEA03.04 Obtener garantía del cumplimiento de requisitos externos.	Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo	70%	L