UNIVERSIDAD HISPANOAMERICANA

CONTADURÍA PÚBLICA

Proyecto de tesis para optar por el Grado Académico de Licenciatura en Contaduría Pública

Título:

SEGURIDAD FÍSICA Y LÓGICA DE LA TECNOLOGÍA DE INFORMACIÓN, SEGÚN EL MARCO NORMATIVO COSO 2013 Y COBIT 5 EN LA COOPERATIVA DE AHORRO Y CRÉDITO, EN EL AÑO 2016, PARA MEJORAR LA EFICIENCIA Y EFICACIA DE LAS OPERACIONES

Autora: Karina de los Ángeles Mora Acuña

Tutora: Victoria Rojas Meneses

Año: 2017

Declaración Jurada

DECLARACIÓN JURADA

Yo Karina Mora Acuña, mayor de edad, portador de la cédula de identidad número 1-1588-0965 egresado de la carrera de Contaduría Pública de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura, juro solemnemente que mi trabajo de investigación titulado: Seguridad física y lógica de la tecnología de Información, según el marco normativo COSO 2013 y COBITS en la cooperativa de ahorro y crédito, en el año 2016, para mejorar la eficiencia y eficacia de las operaciones, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. en fe de lo anterior, firmo en la ciudad de San José, a los 16 días del mes de octubre del año dos mil 2017.

Firma del estudiante
Cédula 1-1588-0965

Carta del Tutor

CARTA DEL TUTOR

San José, 23 de setiembre de 2017.

Lic. Joaquín Hernández Aguilar
Director Contaduría
Universidad Hispanoamericana

Estimado señor:

La estudiante Karina de los Ángeles Mora Acuña**,** cédula de identidad número 1-1588-0965, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado **SEGURIDAD FÍSICA Y LÓGICA DE LA TECNOLOGÍA DE INFORMACIÓN, SEGÚN EL MARCO NORMATIVO COSO 2013 Y COBIT 5, EN LA COOPERATIVA DE AHORRO Y CRÉDITO, EN EL AÑO 2016, PARA MEJORAR LA EFICIENCIA Y EFICACIA DE LAS OPERACIONES** , el cual ha elaborado para optar por el grado académico de Licenciatura en Contaduría.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	29
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	19
	TOTAL		98

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Victoria Eug Rojas M

Licda. Victoria Rojas Meneses
Cédula identidad N. 3-0240-0045
Carné Colegio Profesional N. 1180

Carta del Lector

CARTA DEL LECTOR

Heredia, 12 de octubre de 2017.

Señores
Departamento de Registro
Universidad Hispanoamericana

Saludo cordial.

He leído el proyecto de tesis de la estudiante Karina de los Ángeles Mora Acuña, con cédula número 1-1588-0965 misma que presenta para optar por el grado académico de Licenciatura en Contaduría Pública, titulada:

"Seguridad física y lógica de la tecnología de información, según el marco normativo COSO 2013 y COBIT 5 en la Cooperativa de Ahorro y Crédito, en el año 2016, para mejorar la eficiencia y eficacia de las operaciones"

Además, hago constar que he revisado el contenido, estructura e interpretación de la misma que son necesarios para el cumplimiento de los requisitos solicitados por la Universidad Hispanoamericana.

De acuerdo con lo anterior considero que el proyecto de tesis presenta el nivel requerido y es apto para la presentación y defensa pública, ante el tribunal examinador correspondiente y en la fecha que se establezca.

Atentamente,

Lic. Alejandro Quirós Quirós
Lector de Tesis

Carta del Filólogo

San José 16 de octubre del 2017

Señores:
Comisión de Tesis
UNIVERSIDAD HISPANOAMERICANA
Sede Heredia

Estimados señores:

He revisado y corregido los aspectos referentes a la estructura gramatical, ortografía, puntuación, redacción y vicios del lenguaje de la Tesis Final para optar por el Grado de Licenciatura de Contaduría Pública, denominada "**SEGURIDAD FÍSICA Y LÓGICA DE LA TECNOLOGÍA DE INFORMACIÓN, SEGÚN EL MARCO NORMATIVO COSO 2013 Y COBIT 5 EN LA COOPERATIVA DE AHORRO Y CRÉDITO, EN EL AÑO 2016, PARA MEJORAR LA EFICIENCIA Y EFICACIA DE LAS OPERACIONES**", elaborada, por el estudiante Karina de los Ángeles Mora Acuña, cédula 1-1588-0965, por lo tanto, puedo afirmar que está escrita correctamente, según las normas de nuestra Lengua Materna.

Respeté, a lo largo del trabajo, el estilo de los autores.

Atentamente,
Profesor
Carlos Manuel Barrantes Ramírez
Filólogo
Cédula 1-0312-0358
Carné afiliado 16308
Teléfono: 6008-5668 / 83571348

Agradecimiento

En primer lugar le agradezco a Dios, por haberme dado las fuerzas para culminar esta investigación y a lo largo de mi carrera.

A familia, por siempre estar para mí apoyándome en todo momento y por formarme día a día.

A mi tutora Victoria, por ayudarme siempre y ser un pilar importante para la culminación de esta investigación.

Tabla de contenido

Índice de figuras

Índice de cuadros

Índice de Gráficos

Índice de Tablas

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema:

1.1.1 Antecedentes del problema

En el mundo, las entidades están sistematizando los procesos de las operaciones normales de los negocios; esto les contribuye, entre otros, en el ahorro de recursos, evitar errores humanos, implementar mejoras oportunas, mantener comunicaciones directas a pesar de las distancias, expandir el mercado. Lo anterior, tiene implicaciones económicas, es decir, se espera mejorar ganancias o utilidades al realizar una inversión tecnológica. Sin embargo, los negocios, muchas veces, también son perjudicados por el inadecuado uso de la tecnología o los fraudes cibernéticos a los que se exponen, cuando las empresas no cuentan con las medidas de seguridad para mitigar dichos impactos y tampoco existen regulaciones en leyes, o reglamentos para que estos reciban, protección de la información que manejan las entidades y colaboradores.

También, al existir mayor manipulación de la información por la expansión de los mercados y la tecnología, se presentan casos como lavado de dinero en las Cooperativas y fraudes en créditos. Por ejemplo: en Perú para el año 2016, se presenta la acusación de una Cooperativa, no sólo por el lavado de dinero, sino por perder el dinero de muchos asociados y la entidad no fue supervisada a tiempo por el ente regulador de dicho país. Por lo tanto, se producen pérdidas económicas para muchos clientes y la información confidencial queda al descubierto de la sociedad. Además, en el 2013 se publica por parte de la presidencia de la Confederación de Cooperativas de Colombia (Confecoop) la

existencia de falsas Cooperativas de crédito, donde utilizando métodos como repartir tarjetas en lugares concurridos, ofreciendo préstamos, estafan a miles de personas. Por lo anterior, ante la carencia de medidas de seguridad, tanto para las personas internas como externas usuarias de la información, la figura de Cooperativa en la actividad crediticia se está utilizando mal y eso engaña a muchas personas, ocasionando una baja en la credibilidad del sistema cooperativo.

Asimismo, el aumento de la tecnología y la apertura del mercado de las telecomunicaciones, hacen que las organizaciones utilicen nuevas herramientas, las cuales presentan debilidades y fortalezas, que otros utilizan para hacer daño. Por ejemplo: el “phishing” (suplantación de identidad), se ha vuelto uno de los timos usados por los ciberdelincuentes. En el año 2014 en Costa Rica, se presentan casos de fraudes electrónicos y según la noticia publicada en el periódico La Nación, por Alejandro Fernández se incrementó en un 600% las denuncias; sin embargo, la mayoría no llegan a juicio por falta del seguimiento de pruebas. Además, en ese mismo año el Banco Popular anuncia un fraude de tarjetas de un grupo de personas, que utiliza métodos engañosos para extraer información bancaria y así tener acceso digital a las cuentas de las víctimas, lo que deja entrever la falta de protección de las entidades por los cambios tecnológicos no sólo a nivel personal, sino organizacional.

1.1.2 Descripción del problema

La tecnología es un factor importante para generar valor a los negocios, por ende, el saber utilizarla de forma efectiva marca la diferencia en las empresas, para lograr posicionarse en el mercado. La tecnología trae consigo resultados positivos y negativos, por ejemplo: ahorro de recursos, mejorar la calidad del servicio, orden en los procesos, control de políticas; pero a la vez, puede generar fuga de información, pérdida de archivos, respaldos inadecuados, fraudes; entre otros. Por lo tanto, el estar capacitado al respecto, permite poder gestionar los riesgos inherentes a la tecnología, y el conocimiento de leyes, así como nuevas herramientas o metodologías fortalecen la protección de la seguridad física y lógica y son aplicables en cada país, y por ende, los activos. Además, las empresas buscan conocer las posibles acciones que representan consecuencias por el mal uso de la tecnología, tanto personas de internas como externas a cada una.

Muchas veces, las políticas de control interno y planes estratégicos de las empresas no se actualizan de manera efectiva y oportuna. Además, las funciones de cada colaborador y miembros directivos no están siendo definidas en las organizaciones de forma clara y concisa. Esto genera dificultad en la evaluación de la eficiencia y eficacia en las operaciones de la organización y se puede ver reflejado en desórdenes financieros-contables o un inadecuado uso de la información. En el caso de la Cooperativa de ahorro y crédito, no tiene una preocupación por establecer políticas en relación con la seguridad física y lógica

de los datos, incluso generar medidas de monitoreo de la información confidencial que se procesa.

La tecnología de la información y de la comunicación permiten que las personas logren acceder a condiciones para interactuar en varios escenarios, y por ende, incursionar en medios o plataformas tecnológicas que pueden contener información personal y, en consecuencia, se ha transformado la forma como la humanidad crea y distribuye conocimientos, lo que genera un riesgo a la intimidad o actividad privada. Por lo tanto, surge el Decreto Ejecutivo Nº 37554-JP de protección de la persona frente al tratamiento de los datos personales (2013), que busca proteger la información confidencial y personal procesada en la empresa. Al respecto, en la Cooperativa de ahorro y crédito son ejemplo de datos que guardan esta característica, los que corresponden a un asociado, colaborador o proveedor, y respecto de información confidencial que no se divulgue ni revele, la relacionada con el estatus de pagos de créditos, ahorros, convenios, entre otros.

Por la importancia que tiene un buen control interno es que éste delimita los lineamientos por seguir de forma estricta; por ejemplo, que los colaboradores utilicen las herramientas de trabajo únicamente para temas laborales y no personales. Esto, por una parte, para el resguardo de los derechos de las personas que trabajan para la empresa en cuanto a la libertad privada, y por otro lado, para la seguridad de la entidad por el flujo de información que se procesa y que no conviene mezclarla con información personal del trabajador.

Además, en Costa Rica existen entidades que se preocupan por proporcionar guías de aplicación en la mejora de controles para entidades supervisadas, como lo es la SUGEF (Superintendencia General de Entidades Financieras) que emite la norma 14-09 (2009 y sus reformas), que corresponde a un reglamento sobre la gestión de TI (Tecnologías de Información), donde se integran aspectos de controles y políticas por seguir, por ejemplo; si es correcto revisar el correo de los colaboradores, o facilitar códigos de usuarios a compañeros, entre otros, en razón del posible impacto en la privacidad de la información personal del colaborador, además de los lineamientos por seguir para utilizar los recursos de la organización en temas laborales, por lo tanto, sirve de ayuda para el constante monitoreo del desempeño de la entidad.

El plan estratégico de la Cooperativa de ahorro y crédito, que data del año 2013, carece de actualización, y las revisiones posteriores han sido de forma rápida y sin profundidad. A inicios del 2016, se inicia la revisión y evaluación, para la actualización del plan estratégico. Debido a la importancia de esta herramienta para la buena marcha de la organización, un punto discutido es en el área de "Sistemas de Información" y surge la preocupación de contar con un sistema integrado de información robusto y confiable de control interno que permita el procesamiento de información se lleve a cabo de manera confiable desde medidas de seguridad física y lógica.

1.1.3. Problematización del problema

Las empresas tienen la responsabilidad de conservar la integridad, confiabilidad y disponibilidad de la información que manejan en las operaciones normales del negocio, entre ellas se encuentra información de terceros como clientes o proveedores, o inclusive de los mismos colaboradores. Además, que forma parte de la legislación del país protegerla. Por lo tanto, cabe resaltar la siguiente pregunta: ¿Qué medidas de seguridad se presentan en la empresa para el resguardo de la integridad y confiabilidad de los datos, existe un plan de evaluación y monitoreo de éstas?

Al existir cambios tecnológicos constantes las empresas están llamadas a procurar mantener un adecuado aprovechamiento de los recursos informáticos y las tecnologías afines que son propiedad o se encuentran a disposición de la entidad. Debido a lo expuesto se puede realizar la siguiente pregunta: ¿Cuáles políticas se tiene en la empresa en cuanto a TI (Tecnologías de Información), y qué métodos utilizan para validar la correcta aplicación?

Además, las compañías ejecutan acciones de control interno, las cuales son la base para poder mantener monitoreado el ambiente de la organización y acceso físico y lógico de las herramientas tecnológicas de los sistemas de operación. Con esto se minimiza la probabilidad de ocurrencia de algún siniestro, manteniendo mayor seguridad, descartar falsas hipótesis sobre posibles incidentes y poder tener los medios para luchar contra cualquier tipo de acontecimiento. Las empresas pueden consultar el marco normativo COSO 2013 (Committee of

Sponsoring Organizations of the Treadway Commission) para conocer los criterios mínimos para tener un sistema de control interno apropiado. Con base en lo señalado, se puede realizar la siguiente pregunta: ¿Qué criterios utiliza la Cooperativa de ahorro y crédito para definir el control interno en cuanto a seguridad física y lógica de la información?

Al mismo tiempo, las empresas están llamadas por considerar los riesgos de seguridad física y lógica del sistema de información. La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y operaciones de control frente a posibles amenazas físicas al hardware, ocasionadas, tanto por el hombre como por la naturaleza, mientras, la seguridad lógica de un sistema informático consiste en la aplicación de barreras y operaciones que protejan al acceso a los datos y a la información contenida en él. Considerando lo anterior, se puede realizar la siguiente pregunta: ¿Con base en qué medidas de mitigación de riesgos aplica la empresa la seguridad física y lógica de la información?

También, el conjunto de colaboradores que trabaja en una empresa necesita adquirir habilidades que le permitan, tanto realizar el trabajo cotidiano como para obtener la preparación necesaria y enfrentar nuevos cambios y desafíos en el ámbito tecnológico, permitiendo así permanecer en el mercado. Con respecto de lo anterior, se realiza la siguiente pregunta: ¿Por qué razones se debe medir la periodicidad de las capacitaciones del personal en relación con los avances tecnológicos y el impacto en la eficiencia y eficacia de las operaciones?

En la actualidad, existen marcos normativos para que las organizaciones puedan gobernar y gestionar efectivamente la información y tecnología, independientemente del tamaño, ubicación o industria. Este es el caso de COBIT 5, el cual está orientado a todos los sectores de la organización, permite enfatizar el control de los negocios y la seguridad de TI (tecnología de información). Por ende, la correcta utilización de un marco de ese tipo permite conseguir una adecuada utilización de los recursos beneficiando a toda la institución. Para la Cooperativa surge el siguiente cuestionamiento ¿Cómo la aplicación del COBIT 5 mejora la eficiencia y eficacia de las operaciones en relación con la seguridad física y lógica de la tecnología de información?

1.1.4. Justificación del problema

Debido a constantes cambios en las normas de contabilidad que se han dado en los últimos años, la actualización de los programas de estudio en las universidades es importante para transmitir la enseñanza con la correcta aplicación que el mercado exige. Entre las actualizaciones que se han dado, se encuentra la NIA 315, que proporciona la guía para analizar los riesgos, tanto para la toma de decisiones de la directiva como para las funciones de revisión y monitoreo de la auditoría, siendo ésta interna como externa. Además, otra norma es la NIA 200 Objetivos y principios generales que gobiernan una auditoría de estados financieros. En ella, se mencionan atributos para que la información de la empresa específicamente de los Estados Financieros sea útil para los usuarios, estos internos como externos. Entre ellos mencionan los siguientes: las integridades de las operaciones de la empresa se den de manera razonable, la

relevancia de la información de la naturaleza de la entidad y los objetivos que se desean alcanzar, por lo que no tener controlado la seguridad física y lógica de la información pone en peligro el cumplimiento de dichos atributos de la norma y las reformas de ésta.

Según el plan estratégico proporcionado por la Cooperativa, elaborado por el presidente del consejo de administración y el gerente general (2008), destacan entre los puntos de mejora el tema de seguridad de la información, por la relevancia que representa en la compañía la actualización de los procesos sistematizados y los que están en proceso de serlo, esto por la expansión de mercado que se está dando en la empresa, hacia un área nueva de producción artesanal de productos lácteos de la región en un proceso industrializado, los cuales requieren automatizar y monitorear los sistemas actuales. Lo anterior, con el fin de medir la capacidad para manejar el mayor flujo de información, con calidad en los resultados, siendo íntegra y confiable los datos procesados, para seguridad de los socios y directivos de la compañía.

Las personas están siendo influenciadas por la tecnología desde el nacimiento. Esto genera que estén al contacto con las herramientas tecnológicas más del 80% del tiempo, incluso la comunicación con las personas del vínculo familiar y laboral no es de forma directa, sino utilizan aplicaciones o sistemas para hacerlo; por tanto, las empresas buscan optimizar los recursos para generar más utilidad y valor en las operaciones, aplicando los avances tecnológicos para incrementar las utilidades. Efectuar un análisis de la eficiencia y eficacia de la seguridad física y lógica en la Cooperativa cuya investigación no se ha realizado antes, va a

evidenciar si realmente se están cumpliendo los controles necesarios para evitar poner en riesgo la integridad de la información y funcionabilidad del negocio.

El documento de esta investigación va a permitir una consulta para mejorar el programa de estudio de la carrera de Contaduría de la Universidad Hispanoamericana. Con este trabajo se pretende mostrar la importancia de realizar aplicaciones de marcos normativos de casos reales, para analizar el comportamiento actualizado del mercado. Es decir, los profesores y directivos de las universidades deben preocuparse por transmitir el conocimiento con casos reales y actuales, capacitar a los estudiantes con las herramientas estándares de aplicación al mercado laboral, logrando así ser competitivos y desarrollar habilidades multidisciplinarias en los profesionales. Es aquí, donde aplicar conocimientos de contabilidad unidos a la seguridad física y lógica de la información, permite un aprovechamiento de oportunidades en la toma de decisiones y análisis de resultados financieros.

Muchas veces, se observa que los dueños de las entidades contratan un oficial de seguridad, pensando, tanto en la seguridad de las personas como de los datos de la empresa o activos, porque es una necesidad proteger el núcleo donde se procesa la información de las empresas, es decir, los sistemas. Aunado a lo anterior, es necesario analizar si los sistemas que se utilizan son los convenientes y soportan la cantidad de información que procesan, por lo cual, es importante crear adecuados controles de seguridad física y lógica de acuerdo con cada institución, para generar un control interno eficiente que considere un monitoreo constante que permite aplicar la toma de decisiones en el momento, logrando ser

proactivos y oportunos para actuar y generar mayor valor a la empresa para el crecimiento en el mercado, así como medir el impacto de la manipulación de información confidencial para contar con sistemas seguros y evitar perder el principio de negocio en marcha, y la integridad de los resultados financieros.

1.2. Formulación del problema

Por lo expuesto surge la siguiente pregunta central de la investigación: Según el marco normativo COBIT 5, ¿cuál es la eficiencia y eficacia de las operaciones de la seguridad física y lógica de la tecnología de la información en la Cooperativa de ahorro y crédito?

1.3. Objetivo de la investigación

1.3.1. Objetivo general

1. Analizar la eficiencia y eficacia de las operaciones de seguridad física y lógica en la Cooperativa de ahorro y crédito, durante el período 2016.

2. Proponer un conjunto de sanas prácticas sobre eficiencia y eficacia de las operaciones de seguridad física y lógica en la Cooperativa de ahorro y crédito, con base en COBIT 5 y COSO 2013.

1.3.2. Objetivos específicos

1. Identificar el control interno seguido respecto de los recursos de infraestructura y aplicaciones del procesamiento de la información en la Cooperativa de ahorro y crédito.

2. Medir el funcionamiento de las operaciones de los principios del COBIT 5 en relación con seguridad física y lógica.
3. Evaluar la respuesta al riesgo que respecto de la de seguridad física y lógica de la información, se genera en la Cooperativa de ahorro y crédito.
4. Elaborar una propuesta de mejoramiento de seguridad física y lógica en tecnología de información en la Cooperativa de ahorro y crédito.

1.4. Alcances y limitaciones

1.4.1. Alcances

La investigación contribuye para sensibilizar a los dirigentes de la Cooperativa de ahorro y crédito, acerca de la importancia de invertir en un sistema robusto para la seguridad física y lógica de la entidad, y para una mayor integridad en la información y exactitud en los datos para generar una mejora en el control en las políticas y normas de la empresa, logrando así un impacto es los resultados contables.

1.4.2. Limitaciones

Durante la investigación, se determina que la parte de la administración de la tecnología de la información es contratada externamente, con esto la tercerización de servicios puede influir en los resultados información. Además, no se permitió usar el nombre de la Cooperativa ni el de los funcionarios entrevistados, para el resguardo de la confidencialidad de la entidad y de los colaboradores.

CAPÍTULO II

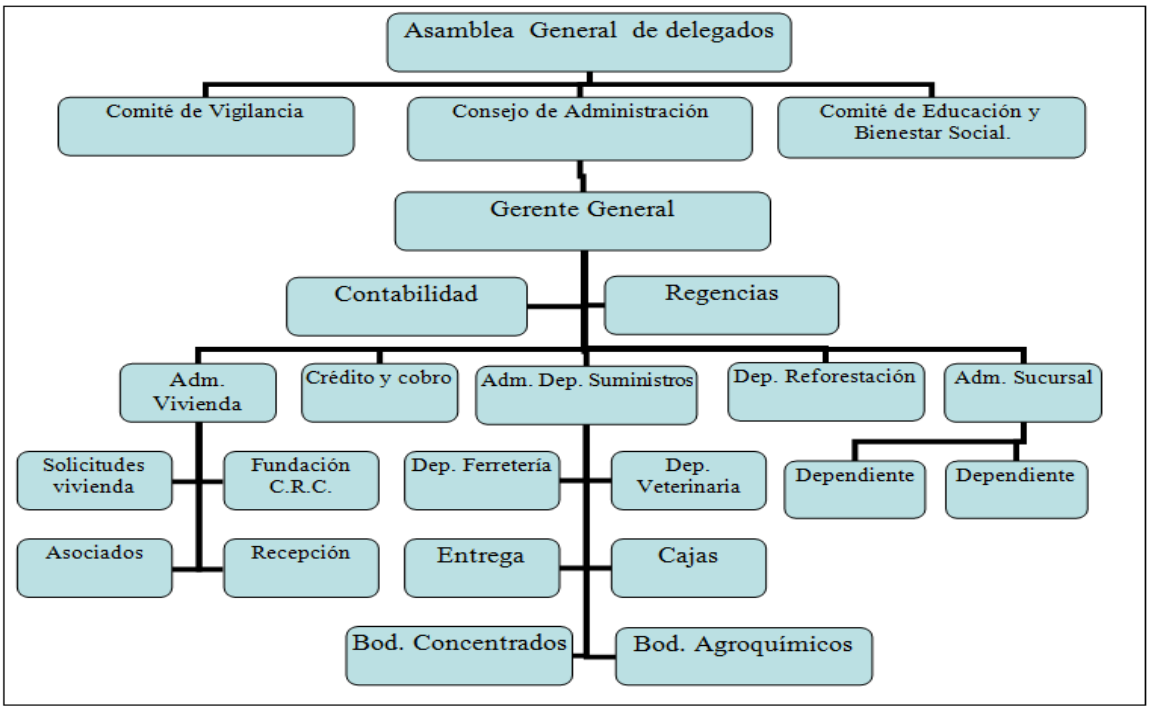
MARCO TEÓRICO

2.1. El contexto histórico

La Cooperativa de ahorro y crédito en estudio se encuentra ubicada a 40 kilómetros al suroeste de la ciudad de San José. En los tiempos de la colonización en la zona, los cultivos de tabaco se convierten en la actividad económica principal durante muchos años. Este producto se coloca a las empresas productoras, las cuales manipulan las condiciones que quisieran. Por esa razón y el auge del cooperativismo, las personas de la zona integran Coopetabaco RL, la cual se inscribe legalmente en el Departamento de Organizaciones Sociales del Ministerio de Trabajo y Seguridad Social en los libros de registro mediante la resolución número: C-0018 del día 18-10-1957. Con el transcurso de los varios años, la Cooperativa juega un papel muy importante para el desarrollo de la economía de la zona, por lo que los integrantes de la citada organización realizan un nuevo planteamiento para cumplir con las nuevas exigencias y el 8 de mayo de 1982, se celebra una Asamblea General, donde se decide dar nuevos servicios y también cambia el nombre de la Cooperativa. (Sánchez G, 2008)

Con el desarrollo de los nuevos servicios, en cumplimiento de los objetivos de la organización, se ha conformado la actual estructura organizativa, siendo: Asamblea General de delegados, Consejo de Administración, Comité de Vigilancia, Comité de Educación y Bienestar Social, Comisión de crédito, Gerencia y departamentos para los diferentes servicios que brinda la Cooperativa, entre ellos Almacén de Suministros, Vivienda, Ambiental, Crédito y servicios a los asociados. A continuación, se muestra el organigrama:

Figura 1. Organigrama de la Cooperativa



Fuente: Información de la Cooperativa

En el plan estratégico de la empresa, se consigna su misión y visión. Siendo la visión de la Cooperativa; "…ser la organización social más consolidada de la región, con una amplia membrecía, líder en servicios para sus asociados y con un fuerte compromiso social, manteniendo una excelente imagen a nivel general sustentada en ser; éticos, sensitivos, rentables". Por lo cual, buscan metas y objetivos estratégicos para lograrlos que se vean reflejados en sus acciones. También, se basan en la misión para expandir su mercado y lograr diferenciarse de los demás; siendo ésta el "…facilitar el desarrollo integral del asociado, a través de los servicios y producción en áreas estratégicas con carácter social, luchando por ofrecer oportunidades para los asociados y la sociedad". (Plan estratégico, 2008).

Entre los valores que la Cooperativa fomenta para lograr ser eficaces y eficientes en las operaciones y, a la vez, crear un ambiente de trabajo agradable para los colaboradores, clientes y asociados se encuentran: la ética, según define Torres, Z (2014), es “Un cuerpo de conocimientos que aborda la naturaleza de las acciones humanas en la vida social, desde la óptica de los conceptos morales (bondad, verdad)”, por lo tanto, se debe fomentar en la Cooperativa la trasparencia en las acciones de los colaboradores. La honradez, según la Real Academia Española (2016) es la “Rectitud de ánimo, integridad en el obrar”. Es decir, aquella persona que en su actuar y pensar es justa, recta e íntegra.

La disciplina, según Oxford (2016) es el “conjunto de reglas de comportamiento para mantener el orden y la subordinación entre los miembros de un cuerpo”, buscando ser la guía para cumplir políticas y normas establecidas. Eficiencia que la define la Real Academia Española (2016), como la “capacidad de disponer de alguien o de algo para conseguir un efecto determinado”, es decir, lograr los objetivos fijados, sin embargo, tomando en cuenta la eficacia para ser oportunos. Además, la transparencia, según Oxford (2016) es la “cualidad de transparente que presenta una cosa, una persona, un objeto”. Esto para la prevención de actos corruptos y posibles fraudes que pongan en riesgo la seguridad de la información. Por último, el compromiso, según Oxford (2016) es la “obligación contraída por una persona mediante una promesa, un contrato u otro acuerdo”, para la Cooperativa es buscar dar el mejor servicio con los asociados y satisfacer las necesidades de la población.

Por la diversificación de los servicios que brinda la Cooperativa, se ha convertido en promotora del desarrollo de la zona, atendiendo distintas áreas para fines diferentes, siendo las siguientes: Ambiental: con el fin de lograr la conservación de los bosques existentes, fomentando en el asociado la importancia de sembrar árboles e impulsar la producción de la madera. El área Comercial: buscando ser la opción comercial más ágil y diversificada de la región, para así incrementar las utilidades. Área de vivienda e infraestructura: buscar la mejor condición de vivienda de los asociados en poblaciones y áreas de influencia.

Además, el Área de asociados para fomentar una educación y formación Cooperativa, basada en valores. Área de crédito: satisfacer todas las necesidades de los asociados de la Cooperativa. Área de producción: buscando producir en áreas estratégicas con carácter social. Área sistemas de información: ser la opción comercial más ágil y diversificada de la región, incrementando las utilidades. Por tanto, la participación en las actividades, en el corto y mediano plazo es necesario para la buena marcha de la organización y lograr un reemplazo generacional una necesidad para la organización y para la población.

2.2. El contexto teórico-conceptual

Debido a los constantes cambios en el mundo, la necesidad de adaptación de las empresas a los avances de la tecnología, genera que se incremente el nivel de riesgo ante un fraude cibernético, incurriendo así en pérdidas inclusive millonarias, las cuales ponen en peligro empleos, situación económica de la región o el país, entre otros. Por lo tanto, la actualización las normas, leyes y guías prácticas

adaptables a cada institución minimiza dichos riesgos o incrementa los resultados económicos para las entidades.

2.2.1. Importancia de la aplicación de la Ley N° 4179

Los inicios del cooperativismo en Costa Rica obedecen a las desigualdades que se presentaron en el pasado; tanto de explotación laboral, distinción de clases sociales, entre otros. Para el año 1968, se pública en la Gaceta la Ley de asociaciones cooperativas siendo la ley Nº4179, y las respectivas actualizaciones. Dicha ley en el Título I capítulo 1, artículo 2, define como Cooperativa:

> Las cooperativas son asociaciones voluntarias de personas y no de capitales, con plena personalidad jurídica, duración indefinida y responsabilidad limitada, en las que los individuos se organizan democráticamente a fin de satisfacer sus necesidades y promover su mejoramiento económico y social, como un medio de superar su condición humana y su formación individual, y en las cuales el motivo del trabajo y de la producción, de la distribución y del consumo, es el servicio y no el lucro.

Por lo cual, las entidades están en el deber de estar inscritas ante la ley, y seguir las disposiciones, así como someterse a las evaluaciones necesarias para comprobar la razonabilidad de los registros de la información que procesan.

También la Ley de Asociaciones Cooperativas N°4179, Título III en el capítulo 1, artículo 154 señala:

> Créase una institución denominada Instituto Nacional de Fomento Cooperativo, cuyo nombre podrá abreviarse como INFOCOOP. Esta institución tendrá personalidad jurídica propia y autonomía adminis-trativa y funcional. El domicilio legal del Instituto es la ciudad de San José y podrá establecer agencias en otros lugares del país.

El INFOCOOP, es la entidad responsable por ejercer la supervisión y corregir de ser necesario las acciones equivocas de las cooperativas para que sean íntegras y confiables. A la vez, es importante realizar las mejoras que se requieran a la ley, conforme se fiscalizan y se obtienen resultados, por lo tanto, la comunicación de hallazgos debe ser precisa y oportuna de estos organismos de supervisión.

La importancia de determinar cuáles son los parámetros que definen una cooperativa, marca la manera de establecer las políticas y normas para crear el máximo valor y mejores resultados. Las cooperativas se deben inscribir en el Ministerio de Trabajo y Seguridad Social, lo cual obliga a cumplir los mandatos de ley. También, a adoptar los mecanismos de protección de los activos y la información de los clientes y asociados. Las condiciones las cuales están sujetas las cooperativas para poder ser inscritas se describen en la ley N°4179 en el Título I Capítulo 3, el artículo 31:

- Se constituirán con responsabilidad limitada, y de sus compromisos responderán el haber social y los asociados hasta por el monto de los aportes suscritos.

- Se constituirán mediante asamblea que celebren los interesados, de la cual se levantará un acta.
- No podrán constituirse mientras no esté suscrito íntegramente el patrimonio social inicial y no se haya pagado, por lo menos, el 25% de la inversión obtenida.
- No podrá constituirse con un número menor de 20 asociados.
- Tendrán su domicilio legal en el lugar donde realicen el mayor volumen de sus operaciones.

Para la evaluación de los controles y el establecimiento de leyes, se deben crear responsables en las cooperativas. Según la ley N°4179 Título I, Capítulo IV, artículo 36 señala:

> La dirección, la administración, la vigilancia y la auditoría interna de las asociaciones cooperativas estarán a cargo de:
>
> a) La Asamblea General de asociados o de delegados.
> b) El Consejo de Administración.
> c) Al Gerente, los subgerentes y los gerentes de división.
> d) El Comité de Educación y Bienestar Social.
> e) El Comité de Vigilancia.
> f) Los comités y las comisiones que puedan establecerse con base en esta ley y las que designe la Asamblea General.

Sin embargo, no está limitado a crear otro organismo de control que colabore al ordenamiento interno de la Cooperativa, y que, a la vez, no contradiga otros artículos de ley del país. Esto en la necesidad de fomentar impactos positivos en la sociedad costarricense. Permitiendo así adaptarse a las necesidades del negocio.

2.2.2. Aplicación de COSO 2013

Para lograr tener eficiencia y eficacia de las operaciones de seguridad de la información, es importante tener un control interno de la empresa óptimo y para ello, se encuentra el marco normativo COSO 2013, el cual presenta los componentes básicos para realizar las políticas y normas de la institución, además, de realizar los objetivos y metas del plan estratégico de la compañía. COSO 2013 (Committee of Sponsoring Organizations of the Treadway Commission), define que: “Control interno es un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la Organización, diseñado para proporcionar una garantía razonable sobre el logro de objetivos relacionados con operaciones, reporte y cumplimiento”. (p.4)

Con lo anterior, las empresas buscan minimizar los riesgos por descontroles y desórdenes de la información. A la vez, diseñar las responsabilidades de cada colaborador, manteniendo así el rumbo correcto al logro de los objetivos de la entidad. Para ello, COSO 2013 busca identificar eventos potenciales que puedan afectar a la organización, gestionar el riesgo; y proporcionar una seguridad razonable que ayude a alcanzar los objetivos de la Organización. Por lo tanto, la misión de COSO es: "...Proporcionar liderazgo intelectual a través del desarrollo

de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude…". Para poder cumplir dicha misión, se desarrollan cinco componentes básicos del COSO 2013, y diecisiete principios que representan los conceptos fundamentales relacionados con los componentes. Por lo tanto, es importante analizar cada uno de ellos en las organizaciones.

Figura 2. Componentes del control interno

Fuente: Elaboración COSO 2013.

La imagen anterior muestra la manera como se complementan los objetivos con los componentes, a un nivel estructural adaptable a cada institución, según COSO 2013. Esto para lograr establecer un efectivo Sistema de Control Interno. A continuación, se describen cada uno de los componentes:

Ambiente de Control: “el cual es crear los criterios básicos de cumplimiento en la organización, donde se muestren principios y valores firmes hacia los objetivos que persigue la organización” (p.14).

Con esto existe independencia entre las supervisiones de cada área con el fin de no generar conflicto de interés y ser objetivos en las acciones necesarias por ejecutar. Además, saber desarrollar las habilidades de los colaboradores y realizar las capacitaciones correspondientes para mejorar la eficiencia, eficacia y competencias; logrando aprovechar dicha inversión en mejores rendimientos.

En este componente se desarrollan cinco principios, que buscan dar una guía para desarrollar de manera oportuna un ambiente de control de la organización. Los identifica COSO 2013, siendo los siguientes:

Principio 1: Demostrar compromiso con la integridad y valores éticos.

Principio 2: El consejo de administración ejerce su responsabilidad de supervisión del control interno.

Principio 3: Establecimiento de estructuras, asignación de autoridades y responsabilidades.

Principio 4: Demuestra su compromiso de reclutar, capacitar y retener personas competentes.

Principio 5: Retiene a personal de confianza y comprometido con las responsabilidades de control interno. (p.16)

Evaluación de Riesgos: el marco lo define como “la identificación y análisis de los riesgos relevantes para el logro de los objetivos, como base para determinar la forma de administrarlos” (p.29). Este componente busca promover el análisis de la entidad de la mano con los objetivos, para lo cual es relevante definirlos con claridad. Asimismo, evaluar la necesidad de realizar cambios oportunos donde el impacto en la organización sea menor. Por ejemplo, ante un fraude tener un control que permita mitigar al máximo los impactos, con políticas bien definidas y aplicadas de forma global por la entidad.

En este caso, los principios que están relacionados para el cumplimiento del componente de evaluación de riesgos, los cuales son pautas de ayuda para ser efectivos en la aplicación, son los cuatro siguientes:

> Principio 6: Se especifican objetivos claros para identificar y evaluar riesgos para el logro de los objetivos.
>
> Principio 7: Identificación y análisis de riesgos para determinar cómo se deben mitigar.
>
> Principio 8: Considerar la posibilidad del fraude en la evaluación de riesgos.
>
> Principio 9: Identificar y evaluar cambios que podrían afectar significativamente el sistema de control interno. (p.32)

Actividades de Control: se define como “las acciones establecidas por políticas y procedimientos para ayudar asegurar que las directivas de la administración para mitigar riesgos al logro de objetivos son llevadas a cabo” (p.46). Estas actividades lo que buscan es desarrollar acciones que permita de forma oportuna encontrar

deficiencias de control que deban ser corregidas sin necesidad de ver resultados negativos a la conclusión de un proyecto. O incluso medir si lo planeado es lo que se requiere en el desarrollo del proceso, o determinar la necesidad de cambiar los lineamientos y realizar nuevos análisis, para lograr las propuestas de la entidad establecidas.

Para poder cumplir el componente anterior; actividades de control, se desarrollan tres principios que contribuyen por orientar las actividades necesarias por realizar, según el tipo de organización, siendo los siguientes:

> Principio 10: Selección y desarrollo de actividades de control que contribuyan a mitigar los riesgos a niveles aceptables.
> Principio 11: La organización selecciona y desarrolla actividades de controles generales de tecnología para apoyar el logro de los objetivos.
> Principio 12: La organización implementa las actividades de control a través de políticas y procedimientos. (p.49)

Información y Comunicación: este pilar se basa en que “la organización comunica internamente información, incluido objetivos y responsabilidades sobre el Control Interno, necesaria para soportar el funcionamiento del Control Interno.” (p.57). Esto es fundamental para la corrección de los puntos de análisis encontrados. Por lo cual, deben ser comunicados de manera oportuna para no tener impactos negativos e irremediables, los que podrían repercutir en pérdidas económicas.

Inclusive hasta el cierre de operaciones y negocios, en los casos del inadecuado manejo de procesos y controles.

También, existen principios que se mencionan para la correcta aplicación del componente información y monitoreo, los cuales son pasos para lograr un efectivo control interno, los que se describen a continuación:

> Principio 13: Se genera y utiliza información de calidad para apoyar el funcionamiento del control interno.
>
> Principio 14: Se comunica internamente los objetivos y las responsabilidades de control interno.
>
> Principio 15: Se comunica externamente los asuntos que afectan el funcionamiento de los controles internos. (p.60)

Monitoreo: se definen como “evaluaciones concurrentes o separadas, o una combinación de ambas es utilizada para determinar si cada uno de los componentes del Control Interno, incluidos los controles para efectivizar los principios dentro de cada componente, está presente y funcionando.” (p.69). Este punto es importante, porque la organización constantemente debe estar al tanto de lo que ocurre en el día a día. Se pueden seleccionar formas para realizarlo que optimicen los recursos de la entidad, para mantener un control adecuado y confiable, pudiendo así realizar proyectos más seguros.

Son los siguientes principios, los que guían a las empresas para realizar un adecuado monitoreo de los procesos que se llevan a cabo en la institución, para

identificar de manera oportuna las correcciones o cambios de estrategias necesarios para cumplir las metas y planes estratégicos establecidos:

> Principio 16: Se llevan a cabo evaluaciones sobre la marcha y por separado para determinar si los componentes del control interno están presentes y funcionando.
>
> Principio 17: Se evalúa y comunica oportunamente las deficiencias del control interno a los responsables de tomar acciones correctivas, incluyendo la alta administración y el consejo de administración. (p.71)

2.2.3. El concepto de políticas y normas de seguridad física y lógica

Cuando las personas unen los esfuerzos de crear una empresa, comparten las opiniones y llegan a formar criterios que definen el inicio del negocio. Conforme avanza la tecnología y el entorno de los negocios, se crean patrones, los cuales son guías para realizar acciones con un impacto menor por la experiencia del mercado. Por tanto, el estar actualizado acerca del segmento del negocio donde el mercado tiene influencia en las posibles decisiones por ejecutar, permite planear las medidas para enfrentarlo o asumirlas y crear medidas de mitigación de riesgos. Entonces, en la necesidad de consultar y legalizar marcos normativos y mejores prácticas, los cuales son establecidos por instituciones acreditadas que pueden aplicar internacional o regionalmente.

2.2.3.1. Política contable

En la importancia de crear un marco global para que las empresas lo adaptaran, según los planes estratégicos, y generar igualdad de oportunidades en un mercado competitivo. Se mencionan aspectos claves, como definición de una política contable.

Esta son una serie de procedimientos, reglas y principios, de los cuales las entidades crean los estados financieros, realizando sus registros y tratamientos contables con base en lineamientos estándares. También, según la Norma Internacional de Contabilidad 8 (NIC 8), párrafo 5, define como política contable a:

> …son los principios específicos, bases, acuerdos reglas y procedimientos adoptados por la entidad en la elaboración y presentación de sus estados financieros…las convenciones, reglas y acuerdos necesarios para que la empresa pueda determinar cómo va a reconocer, medir, presentar y revelar sus transacciones… (p.3)

Las cuales se adaptan, según la naturaleza o función de las empresas. En ellas se indican los rubros necesarios para que la información sea íntegra y confiable, cumpliendo con los atributos de ley para los usuarios internos y externos de dicha información. Según las normas internacionales de información financiera (NIIF o IFRS), emitidas por el IASB, establecen la importancia de la aplicación de políticas contables. Donde el orden de responsabilidad de cumplimento empieza en las normas, luego conceptos o definiciones y principios generales; permitiendo cumplir la relevancia y fiabilidad de la información. También, el aplicar la uniformidad de

las políticas, facilita el análisis de la veracidad de la información de las distintas clases de organizaciones. Si existiese la necesidad de cambiar el tratamiento contable de las políticas fijadas al comienzo por la organización, se debe dejar reflejado y justificado dicho proceso con causales fiables. Al ser las políticas contables un modelo de normas las emitidas por las NIIF (Normas Internacionales de Información Financiera), cada entidad tendrá el deber de personalizarlo, según los lineamientos que persigue y los instrumentos que posean. Teniendo en consideración el estar cumpliendo con lo requerido por las NIIF, NIAS, y demás reglamentos de cada país. (IFRS, 2015)

Al existir un mundo con cambios constantes y la necesidad de estar evaluando el nivel de riesgo del mercado y un posible efecto neto en las organizaciones, se debe realizar un entendimiento del entorno de la entidad, del cual se puedan definir controles, políticas y medidas de mitigación. En la Norma Internacional de Auditoría 315 (NIA 315), Entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa, párrafo 7, menciona: “Procedimientos de evaluación del riesgo…a) Investigaciones con la administración y otros dentro de la entidad;(b) Procedimientos analíticos; y(c) Observación e inspección” (p.4,5). Donde se explica algunos pasos para entender cómo está funcionando la entidad y si realmente se están ejecutando los procesos necesarios para mitigar los posibles riesgos. También, es importante realizar la búsqueda de la información desde varias fuentes, como directivos, colaboradores, entidades externas influyentes, obteniendo una perspectiva diferente para ejecutar el análisis con juicio más razonable.

2.2.4. NIA 200 Objetivos globales del auditor independiente y realización de la auditoría de conformidad con las normas internacionales de auditoría

En la búsqueda de realizar un análisis de la situación de las entidades, la NIA 200, muestra los objetivos globales que un auditor o usuarios de la información de las entidades deberían de aplicar. Por tanto, en la realización de la auditoría de los estados financieros cita los siguientes:

> La obtención de una seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material, debida a fraude o error, que permita al auditor expresar una opinión sobre si los estados financieros están preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable.
>
> La emisión de un informe sobre los estados financieros, y el cumplimiento de los requerimientos de comunicación contenidos en las NIA, a la luz de los hallazgos del auditor. (p.3)

Lo anterior, es relevante para las compañías también, por ser necesario elaborar y mantener la información íntegra para cumplir con las normas de auditoría, generando así mayor control y evaluación interna, para lograr tomar decisiones oportunas y asumir riesgos cuando la empresa tiene como responder ante una eventualidad.

Además, en la NIA 200 se establecen requerimientos que deben cumplirse para que las auditorías externas tengan la validez para los usuarios de dicha información. Entre ellos se mencionan los siguientes: “Requerimientos de ética

relativos a la auditoría de estados financieros, escepticismo profesional, evidencia de auditoría suficiente y adecuada y riesgo de auditoría", donde los puntos relevantes son crear una evaluación con las normas actualizadas, y las que se adapten a la naturaleza de la empresa. Para que el análisis sea lo más razonable posible. Logrando así ser útiles para identificar las mejoras a corregir, incrementado la rentabilidad de la entidad, y evidenciando las falencias que requieren de atención, para la seguridad de los colaboradores de las entidades, que los usuarios de los servicios no se vean afectados.

Igualmente, la NIA 200 menciona atributos para que la información de la empresa, específicamente, de los Estados Financieros sea útil para los usuarios, estos internos como externos. Entre ellos mencionan los siguientes: las integridades de las operaciones de la empresa se den de manera razonable, la relevancia de la información de la naturaleza de la entidad y los objetivos que se desean alcanzar. En cuanto a la neutralidad, confiabilidad y comprensibilidad de la información indica la exactitud y libre de sesgo que debe existir. Entonces, el no tener control de la seguridad física y lógica de la información, se pone en peligro el cumplimiento de dichos atributos de la norma.

2.2.5. NIA 402 Consideraciones de auditoría relativa a una entidad que usa una organización de servicios.

En la actualidad, es cada vez más común que las organizaciones contraten servicios externos. Estos para la realización de tareas específicas de las

operaciones del negocio de la entidad. En la Norma Internacional de Auditoría 402 presenta la responsabilidad del auditor del usuario de obtener la suficiente y apropiada evidencia de auditoría cuando la entidad usuaria emplea los servicios de una o más organizaciones de servicios. La NIA 402 busca en sus objetivos:

> (a) obtener conocimiento suficiente de la naturaleza y significatividad de los servicios prestados por la organización de servicios y de su efecto en los controles internos de la entidad usuaria relevantes para la auditoría, para identificar y valorar los riesgos de incorrección material; y
> (b) diseñar y aplicar procedimientos de auditoría para responder a dichos riesgos. (p.3)

En la determinación de cuáles servicios externos son relevantes para la auditoría, son aquellos cuando los servicios y controles sobre ellos son parte del sistema de información de la entidad usuaria. Es decir, se involucran los procesos del negocio e influyen de manera relevante para la información financiera. En la NIA 402 indican los siguientes:

> "(a) los tipos de transacciones dentro de las operaciones de la entidad usuaria que son significativos para los estados financieros de dicha entidad;
> (b) los procedimientos, tanto los relativos a los sistemas de tecnologías de la información (TI) como los sistemas manuales, mediante los que las transacciones de la entidad usuaria se inician, registran, procesan, corrigen en caso necesario, se trasladan al libro mayor e incluyen en los estados financieros.
> (c) los correspondientes registros contables, ya estén en formato electrónico o manual, de soporte de la información y cuentas específicas de los estados financieros de la entidad usuaria que son utilizados para iniciar, registrar y procesar las transacciones de dicha entidad e informar sobre ellas. Esto incluye

> la corrección de información incorrecta y el modo en que la información se traslada al libro mayor.
>
> (d) el modo en que el sistema de información de la entidad usuaria capta los hechos y condiciones, distintos de las transacciones, significativos para los estados financieros.
>
> (e) el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad usuaria, incluidas las estimaciones contables y la información a revelar significativas; y
>
> (f) los controles sobre los asientos en el libro diario, incluidos aquellos asientos que no son estándar y que se utilizan para registrar transacciones o ajustes no recurrentes o inusuales. (p.2, 3)"

Por lo tanto, es importante tener un entendimiento de la naturaleza de la entidad en los servicios prestados por organizaciones y el efecto en el control interno. Para así poder identificar y evaluar riesgos de importancia relativa, para diseñar e implementar los procedimientos que respondan a dichos riesgos. Por ejemplo, los servicios de mantenimiento de los registros contables, administración de activos y manejo de transacciones como agente de la entidad usuaria, son relevantes para la entidad. Además, las personas interesadas en conocer la entidad, puede recurrir a manuales, contratos o acuerdos entre las entidades que brindan servicios, reportes emitidos previamente y la experiencia de expertos del entorno de la entidad.

En la búsqueda por obtener un entendimiento de los servicios prestados por la organización de servicios, incluido el control interno, las personas pueden recurrir a los contratos, para realizar el análisis de los términos y políticas que estos presentan, y así, determinar la integridad del servicio contratado y las

responsabilidades de las partes. De la misma manera al conocer la naturaleza de los servicios, la importancia y el efecto que estos representan para la entidad, se logra medir el impacto en el control interno de la entidad, por la interacción y relación entre ésta y la organización de servicios, teniendo en cuenta las actividades y procedimientos relevantes.

Obteniendo un entendimiento del control interno suficiente de la entidad, se pueden identificar los riesgos y así evaluar los que representan impactos significativos. Para ello, la auditoría recurre a los reportes I y II, donde para llegar a identificarlos se deben aplicar los procedimientos sustantivos necesarios. Estos reportes pueden ser usados como evidencia del entendimiento de los servicios prestados por la organización de servicios a la entidad usuaria, durante la auditoría. Según la NIA 402 un informe de tipo I es:

> "(i) una descripción, preparada por la dirección de la organización de servicios, del sistema de la organización de servicios, de los objetivos de control y de otros controles relacionados que se han diseñado e implementado en una fecha determinada; y
>
> (ii) un informe elaborado por el auditor de la entidad prestadora del servicio, con el objetivo de alcanzar una seguridad razonable, que incluya su opinión sobre la descripción del sistema de la organización de servicios, de los objetivos de control y otros controles relacionados, así como de la idoneidad del diseño de los controles para alcanzar los objetivos de control especificados."

Mientras que un informe tipo II es:

> "(i) una descripción, preparada por la dirección de la organización de servicios, del sistema de la organización de servicios, de los objetivos de control y otros

> controles relacionados que se han diseñado e implementado en una fecha determinada o a lo largo de un período específico y, en algunos casos, su eficacia operativa a lo largo de un período específico; y
> (ii) un informe elaborado por el auditor de la entidad prestadora del servicio con el objetivo de alcanzar una seguridad razonable, que incluya:
> a. Su opinión sobre la descripción del sistema de la organización de servicios, de los objetivos de control y otros controles relacionados, así como la idoneidad del diseño de los controles para alcanzar los objetivos de control especificados y la eficacia operativa de dichos controles; y b. una descripción de las pruebas de controles realizadas por el auditor y de los resultados obtenidos."

Entonces, la diferencia se enfatiza en determinar en el periodo de fechas, ya que el informe de tipo II incluye al primero por la evaluación de la eficacia operativa de un largo periodo específico, con descripciones más profundas de las pruebas de controles realizadas. Además, la importancia de mantener un control interno de la entidad para el resguardo de la información confidencial. Inclusive el riesgo que implica la pérdida del control ante posibles fraudes que pongan en peligro la funcionabilidad del negocio. Por lo anterior, es necesario controlar la entidad y las entidades que prestan los servicios y resguardar la información, incluso de los avances de la tecnología y los cambios que se deban implementar para la seguridad de la información.

2.2.6. Mejores prácticas con la aplicación de la norma 14-09

En Costa Rica la SUGEF (Superintendencia General de Entidades Financieras) es el ente encargado de regular las entidades financieras; sin embargo, las normas que emite pueden ser utilizadas como buenas prácticas por parte de otras

empresas o entidades y llegar a ser guía para mejorar en las organizaciones. Ese es el caso de la norma 14-09 publicada en la Gaceta en jueves 06 de julio del 2009 y sus reformas, en la que incorpora un reglamento sobre la gestión de TI (Tecnologías de Información). El objetivo de dicha normativa es la "definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI)". Por tanto, en ella se integran aspectos de controles y políticas a seguir, por ejemplo, si es correcto revisar el correo de los colaboradores, o facilitar códigos de usuarios a compañeros, entre otros, en razón del posible impacto en la privacidad de la información personal del colaborador, además de los lineamientos por seguir para utilizar los recursos de la organización.

Debido al aumento de la dependencia tecnológica que caracteriza el desarrollo de las actividades financieras y los costos de las inversiones actuales y futuras en sistemas de información, pueden surgir o propagarse amenazas y eventos no deseados; sin entrar a considerar en detalle el potencial que poseen las tecnologías para cambiar drásticamente los procesos de negocio de las organizaciones. Por lo tanto, es necesario en las empresas que la gestión del riesgo tecnológico utilice las mejores prácticas en la materia. La administración del riesgo tecnológico requiere que las entidades implementen un marco robusto de gestión y control, de tal manera que se apliquen los marcos normativos de amplia aceptación mundial, con la experiencia de los expertos de las buenas prácticas para la gestión y el control de la Tecnología de Información, a través de

un lenguaje común comprensible para todos los interesados, se deja así un margen para la adaptación, según las necesidades de cada organización.

En la norma mencionada se aconseja crear un comité de gestión de TI, de tal manera que los objetivos que lo guíen tengan relación con los planes estratégicos de la entidad; se gestione la administración de riesgos, que entreguen valor a la administración, donde se gestionen los recursos y que se dé la medición del desempeño de TI. La norma indica las siguientes funciones para la autoridad del comité:

> Asesorar en la formulación del plan estratégico de TI. b) Proponer las políticas generales sobre TI. c) Revisar periódicamente el marco para la gestión de TI. d) Proponer los niveles de tolerancia al riesgo de TI en congruencia con el perfil tecnológico de la entidad. e) Presentar al menos semestralmente o cuando las circunstancias así lo ameriten, un reporte sobre el impacto de los riesgos asociados a TI. f) Monitorear que la alta gerencia tome medidas para gestionar el riesgo de TI en forma consistente con las estrategias y políticas y que cuenta con los recursos necesarios para esos efectos. g) Recomendar las prioridades para las inversiones en TI. h) Proponer el Plan Correctivo-Preventivo derivado de la auditoría y supervisión externa de la gestión de TI. i) Dar seguimiento a las acciones contenidas en el Plan Correctivo-Preventivo. (p.6)

Por lo cual, es importante para la organización aplicar estas sugerencias, y que existan áreas responsables del monitoreo de las aplicaciones de los controles. Además, en el artículo 15, de la norma, se indica una calificación promedio:

Cuadro 1. Calificación promedio, según art. 15

Calificación	Nivel
Mayor o igual que 85%	Normal
Mayor o igual que 70% y menor que 85%	Irregularidad 1
Mayor o igual que 55% y menor que 70%	Irregularidad 2
Menor que 55%	Irregularidad 3

Fuente: Elaboración de SUGEF 14 09

La calificación depende de factores como el cumplimiento de los objetivos de control detallados para cada proceso evaluado, el nivel de madurez alcanzado en cada proceso evaluado, el peso relativo de cada proceso evaluado. Además, se considera la importancia relativa del proceso, en virtud del dominio al que pertenece y del eventual impacto en los procesos de negocio.

En el artículo 21, la norma menciona, asimismo, el caso de que las entidades contratan los servicios de manera externa en cuanto a la gestión de área de la tecnología de la información, haciendo referencia a lo siguiente:

> La entidad que contrate parte o la totalidad de uno o varios procesos o servicios de TI, relacionados con el procesamiento y almacenamiento de datos, independientemente del lugar en donde se lleven a cabo esas actividades, debe mantener las bases de datos actualizadas y las aplicaciones vigentes físicamente en el territorio nacional… es responsable de suministrar la información y proveer las facilidades para la ejecución de actividades de supervisión, indistintamente de que los procesos o servicios sean provistos por ella misma, otra empresa del grupo o conglomerado financiero o por un

> proveedor externo, o que sean llevados a cabo dentro o fuera del territorio costarricense.

Por consiguiente, es importante para las entidades, incluso cuando no sean supervisadas, velar por el constante análisis de los sistemas de información, para protegerse oportunamente ante una eventualidad y lograr crecer en el mercado. La aplicación de guías contribuye a efectuar una mejor evaluación de riesgos.

2.2.7. Importancia de la aplicación del decreto N°.37554

Debido a la cantidad del flujo de información que se ha ido incrementando en la sociedad, en el país se creó el decreto ejecutivo N°.37554-JP de protección de la persona frente al tratamiento de sus datos personales, publicado en La Gaceta (2013). Siendo uno de los principios de la creación:

> Que en actualidad las tecnologías de la información y de la comunicación han hecho posible que las personas puedan acceder a condiciones para interactuar en una gran cantidad de escenarios, y por ende, incursionar en medios o plataformas tecnológicas que pueden contener información personal y en consecuencia se ha transformado la forma en que la humanidad crea y distribuye sus conocimientos, lo que genera un riesgo a su intimidad o actividad privada. (p.1)

Lo anterior, refleja la importancia de que las organizaciones conozcan y apliquen los lineamientos del citado decreto que presenta reformas de la ley N°8968 publicada en el 2011. Por ejemplo, en el artículo cuatro; refiere que para la

existencia de consentimiento debe ser: “libre, específico, informado, expreso e individualizado” (p.7). Esto para que ambas partes guarden responsabilidades y compromisos para que exista igualdad sobre el uso de la información.

En el caso de limitar los derechos de la información, se creó el Artículo 21, donde el acceso a la información se determina que “el titular tiene derecho a obtener del responsable, la información relacionada con sus datos personales, entre ellos lo relativo a las condiciones, finalidad y generalidades de su tratamiento”. Lo anterior, cuando se presenta una relación laboral y lo requiere para cumplir con las funciones. Por ello, la importancia de crear y definir los procesos y las responsabilidades de las partes involucradas en relación con el tema.

En el Capítulo IV Del Tratamiento de los Datos Personales y las Medidas de Seguridad, en el Artículo 27 se define los procedimientos para el tratamiento, que son:

> El responsable establecerá y documentará procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de los datos personales, en el sitio o en la nube, con base en los protocolos mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales. Además, deberá el responsable de la base de datos velar por la aplicación del principio de calidad de la información.

Lo descrito crea pautas para velar por la integridad y seguridad de la información, tanto para los usuarios de dicha información, como para los que la producen.

También, se crean obligaciones por parte del encargado de la utilización de la base de datos personales, en el artículo 31 se indican las siguientes:

> Tratar únicamente los datos personales conforme a las instrucciones del responsable.
>
> Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
>
> Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, el presente Reglamento y las demás disposiciones aplicables.
>
> Guardar confidencialidad respecto de los datos personales tratados.
>
> Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable.
>
> Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. (p.14).

Esto es fundamental para el desarrollo de la confianza de la información que se procesa en las entidades, por lo que se pueden implementar medidas de seguridad para la protección de la base de datos personales. En el artículo 36 se mencionan los siguientes:

> Elaborar una descripción detallada del tipo de datos personales tratados o almacenados… Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias… Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales... Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes. (p.17)

En consecuente, es de vital importancia para las organizaciones, estar al pendiente de la información que se contempla en los procesos de base de datos, para así determinar cuáles medidas son necesarias para la protección y con esto poder brindar información íntegra y sin algún tipo de manipulación, que puede perjudicar a la compañía y a los usuarios.

2.2.8. Importancia de la Seguridad física y lógica.

Un pilar importante de las empresas es mantener el respaldo de la información, con un manejo íntegro y exacto de los datos, el cual evidencia que los registros están realizados razonablemente de acuerdo con las leyes del país y permite comprobar que los procesos están alineados con los planes estratégicos de los directivos y evaluar si estos son los adecuados para cada entidad. Según el marco normativo COBIT 5 la información se define como:

> Un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más

> y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios. (p.13)

Por tanto, los dirigentes de las empresas deberían considerar el riesgo respecto de seguridad física y lógica de la información, a la vez considerar la disponibilidad en invertir recursos de análisis de los cambios constantes del entorno que podrían representar un impacto para la institución. Por ejemplo, la fuga de datos confidenciales tanto de los colaboradores, asociados, clientes; entre otros, que estén bajo responsabilidad de los sistemas de las entidades.

2.2.8.1. Seguridad física

La seguridad física debería estar presente en todas las entidades, al no existir pone en riesgo la fuga de información clave y ser una amenaza incluso al principio de negocio en marcha de las operaciones del negocio. Según Cervantes (2012), la seguridad física:

> Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control, se empieza a proteger físicamente el sistema informático las amenazas físicas, pueden ser provocadas por el hombre de forma accidental o voluntaria o bien de factores naturales. (p. 4)

Esto quiere decir que todos los activos de la empresa deben ser protegidos y respaldados en forma oportuna y segura. El hecho de contar con equipo tecnológico actualizado no garantiza el uso correcto, debido a la forma que puede ser manipulado por los colaboradores, por lo que un aspecto clave es crear

políticas de seguridad en la información y controles internos que permitan cumplirlos y que sean reales y aplicables en el entorno en donde se desarrollan la organización.

2.2.8.2. Seguridad lógica

Además de la seguridad física, la empresa debe considerar el pilar donde se procesa la información, el cual es el activo más importante. Por lo tanto, deben existir técnicas y controles, las cuales las brinda la seguridad lógica. Según Cervantes (2012) la seguridad lógica se puede entender por " la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático". Para lograrlo se expresan técnicas para contar con integridad y resguardo de la información, por ejemplo: identificación y autentificación, palabras claves "passwords", encriptación, lista de control de acceso, límites sobre la interface de usuario y etiquetas de seguridad; entre otros. Todo lo anterior permite implementar las normas, políticas y controles para una seguridad de la información, realizando de manera eficiente y eficaz las labores de los colaboradores. Esto se representa inclusive en resultados económicos; analizando también la utilidad del negocio y la necesidad de ejecutar nuevas directrices de mejora oportuna.

Para realizar la protección de la información, existen dos tipos de seguridad: la activa y la pasiva. Según Cervantes (2012):

> La Seguridad pasiva sirve para minimizar los efectos causados por un accidente. Son tales como el uso de un hardware adecuado y la realización de

> copias de seguridad. La seguridad activa sirve para evitar daños a los sistemas informáticos. Son tales como el empleo de contraseñas adecuadas, la encriptación de datos y el uso de software de seguridad informática. (p.10)

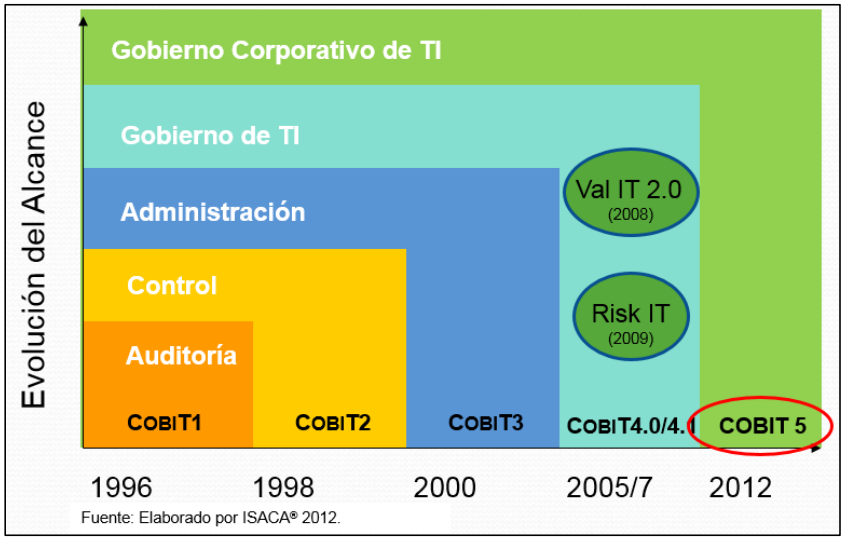
La importancia de esto radica en prevenir los daños que se puedan causar en los sistemas informáticos. Además, forman parte de los elementos que minimizan el impacto de ataque y accidente. En el caso de la seguridad pasiva es la gestión de los dispositivos de almacenamiento como pueden ser realizar copias de seguridad de la información. Por otro lado, la seguridad activa es la protección ante posibles intentos a componentes específicos de los sistemas. Es decir, busca filtrar el acceso a ciertos servicios en determinadas conexiones para bloquear el intento de ataque desde alguno de ellos. Por ejemplo, en el caso de pérdida de datos el poder recuperar la misma, es un elemento primordial dentro de cualquier organización ya que la información puede llegar a tener un valor incalculable.

Además, al ser los sistemas informáticos actuales una red de ordenadores; un ataque al equipo puede causar afectación a todo el sistema. Por tan razón, la principal prioridad de la seguridad informática debe ser minimizar las posibilidades que ocurra un daño al sistema y la información del mismo; o en caso inevitable que ocurra minimizar el impacto.

2.2.9. Análisis de los principios de COBIT 5 en cuanto a seguridad física y lógica de la información.

Con los constantes cambios en la tecnología, se presenta la iniciativa del Consejo de Dirección de ISACA frente a la necesidad de alinearse a las actuales tendencias sobre técnicas de gobierno y administración relacionadas con tecnologías de información de unificar y reforzar la base de conocimiento construida con más de 15 años de aplicación práctica en distintas empresas. Para ello, crean COBIT 5, siendo éste un marco de referencia para brindar apoyo comprensivo a las empresas, para lograr un gobierno y administración efectivo en cuanto a TI. Con esto las entidades aseguran crear valor del negocio y obtienen confianza de la información y los sistemas que la producen, además de contrarrestar los retos a los que se enfrentan actualmente las organizaciones con los cambios tecnológicos. También, COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de manera integral a nivel de toda la organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de los grupos de interés internos y externos. La siguiente imagen muestra la evolución de marcos normativos creados por ISACA, la cual indica la importancia de la investigación en los mercados y actualización de las empresas.

Figura 3. Evolución de marcos normativos



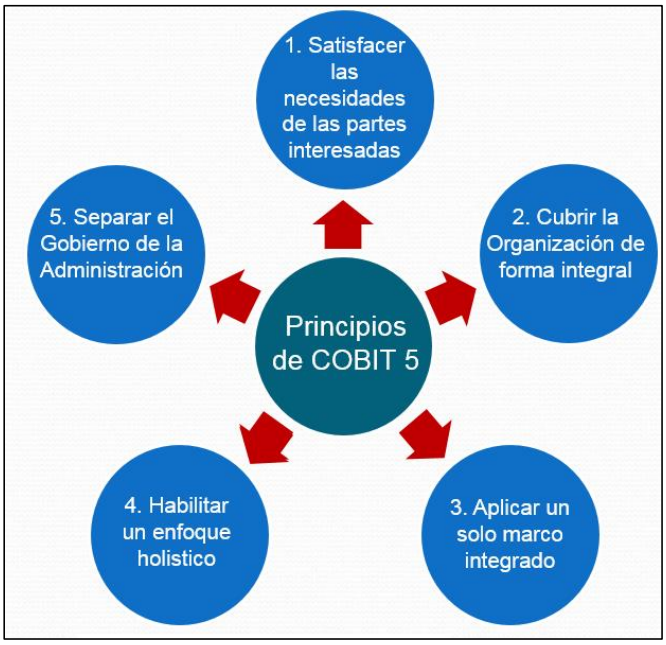
Fuente: Elaborado por ISACA ® 2012

Uno de los objetivos para el desarrollo de este marco normativo es ayudar a los profesionales de TI y líderes empresariales por cumplir con las responsabilidades de gobierno de TI, logrando dar valor al negocio. Además, buscar que el Gobierno asegure el logro de los objetivos de la organización, por medio de la evaluación de las necesidades de las partes interesadas. También, fijar directivas en el establecimiento de prioridades y toma de decisiones, para el conocimiento de mejores condiciones y opiniones. Por último, el monitorear el desempeño, cumplimiento y progreso, realizando un análisis de lo ejecutado con los objetivos acordados, permitiendo realizar mejoras oportunas.

La estructuración de COBIT 5 es la unión de cinco principios que permiten a la empresa construir una gobernabilidad efectiva y un marco de gestión basado en un conjunto holístico de siete facilitadores que optimiza la información y la

inversión en tecnología y el uso para el beneficio de las partes interesadas. Siendo los siguientes: Satisfacer las necesidades de las Partes Interesadas, cubrir la Compañía de Forma Integral, aplicar un solo Marco Integrado, Habilitar un Enfoque Holístico y Separar el Gobierno de la Administración. Detallándose a continuación la imagen integral:

Figura 4. Principios del COBIT 5



Fuente: Elaborado por ISACA ® 2012

El primer principio es Satisfacer las Necesidades de las Partes Interesadas, refiere a que las compañías en la creación están para dar valor a las partes relacionadas e interesadas. Para ello, el Gobierno debe diseñar objetivos donde optimicen los riesgos, los recursos y así satisfacer las necesidades de las partes interesadas recibiendo beneficios. Por lo tanto, los directivos se deben cuestionar a la hora de tomar decisiones lo siguiente: ¿Quién recibe los beneficios?, ¿Quién asume el

riesgo? ¿Qué recursos se necesitan?, con el fin de ser más acertadas. Luego se seleccionar las necesidades en posibles decisiones, se propone una estrategia ejecutable para la organización. COBIT 5 propone realizar el ejercicio de metas en cascada, lo cual es traducir las necesidades en metas específicas, según cada entidad. A la vez, que sean ejecutables y personalizadas dentro del contexto de la organización, donde se relacionen de manera integral con la tecnología de la información. En el marco de referencia COBIT 5 se mencionan los siguientes beneficios: Los beneficios de las Metas en Cascada de COBIT 5:

> Define objetivos y metas relevantes y tangibles a varios niveles de responsabilidad.
>
> Filtra la base de conocimiento de COBIT 5, sobre la base de las metas corporativas, para extraer las guías relevantes a incluir en proyectos específicos de implementación, mejora o aseguramiento.
>
> Identifica claramente y comunica cómo (algunas veces de forma muy operativa) los catalizadores son importantes para alcanzar metas de la empresa. (p.20)

Por lo anterior, es importante que las entidades hagan una estructura organizada de lo que necesitan, quieren hacer y lo que está dentro del alcance realizar, para así determinar las mejores decisiones.

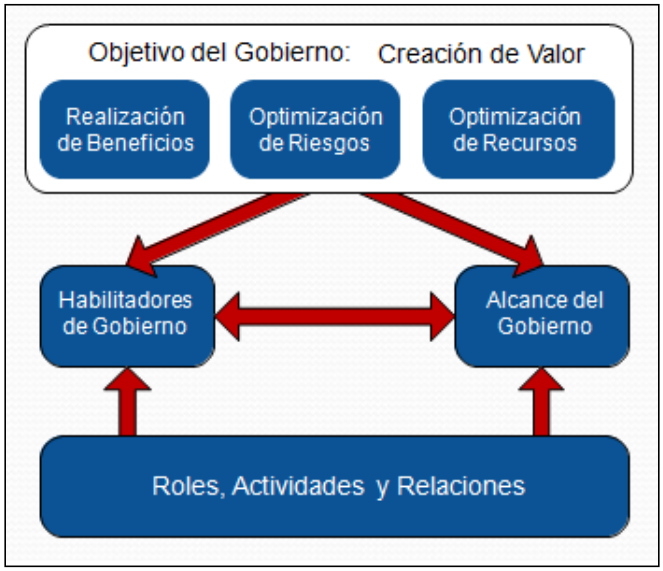
En cuanto al segundo principio se refiere a la importancia de cubrir de extremo a extremo la entidad. En donde la gestión de la información y la tecnología se une al

Gobierno de manera relacionada para toda la empresa, cubriéndola así de manera integral. Entonces los siguientes puntos representan temas centrales de COBIT 5:

> Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno.
>
> Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. (p.23)

Por lo cual, destaca la importancia de globalizar todos los procesos enfocados en un sistema único integrado de la empresa, donde las distintas áreas se interrelacionen para realizar los procesos en busca de las metas de la empresa. La siguiente imagen muestra la relación que existe en la organización utilizando como referencia el marco COBIT 5:

Figura 5. Relación organizacional, según el marco COBIT 5



Fuente: Elaborado por ISACA ® 2012.

En la figura anterior, se unifica el primer principio con los roles, actividades y relaciones de las empresas. En ese punto, se define quién está involucrado en el gobierno, cómo se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno, con el fin de diferenciar las actividades que son del gobierno y la gestión, para determinar la interconexión entre ellos y las partes involucradas. En COBIT 5 se define como catalizadores de gobierno a:

> …los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados. Los catalizadores también incluyen los recursos corporativos – por ejemplo, capacidades de servicios (infraestructura TI, aplicaciones, etc.), personas e información. (p.22)

Esto debido a que la falta de recursos en una organización afecta a la hora de crear valor. También, que contribuye a definir el alcance del sistema del gobierno dependiendo del tamaño y necesidades de la industria.

También, es importante rescatar que la gestión de la información se debe dar, tanto a lo interno como a servicios externos (outsourcing) de la institución. Y aun representando más cuidados en la definición del alcance y responsabilidades en el contrato, donde de ser necesarias definir cláusulas por indemnización de daños ante la pérdida de información. Por tanto, el realizar actividades de control interno y definir responsabilidades, tanto funciones de tecnología de información como del negocio, permitiría mejorar la eficacia y eficiencia de las operaciones, reduciendo así la probabilidad de presentar errores de controles, saltos en las políticas, pérdida de información, entre otros. COBIT 5 busca facilitar la gestión del cambio y la implementación de mejora continua en las entidades.

El principio 3 busca aplicar un Marco de Referencia Único Integrado, el cual permite realizar un mapeo de las prácticas y actividades contra los marcos y normas de terceros. Esto porque COBIT 5 se alinea con otros estándares de referencia, logrando así una cobertura completa de la empresa. Por tanto, proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente. Como lo indica COBIT 5:

> Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas claves del gobierno corporativo durante muchos años y ha desarrollado marcos, tales como COBIT, Val IT, Risk IT,

BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento.

Por tanto, la trayectoria descrita permite ser adaptada a cada organización, con distintas condiciones que se puedan presentar. Pudiendo así desarrollar las mejores prácticas dentro de la organización con experiencias de calidad, lo que genera un menor riesgo en el impacto de los resultados a la hora de ejecutarlos.

Además de las recomendaciones de los principios anteriores, según ISACA 2017 (Asociación de Auditoría y Control en Sistemas de Información) en el marco normativo COBIT 5, se describe el principio de habilitar un enfoque holístico, por la necesidad de administrar la organización de forma global. El cual lo establece COBIT 2013 principio 4, de la manera siguiente:

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las estructuras organizativas son las entidades de toma de decisiones claves en una organización.

- La Cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas. (p.27)

Los catalizadores o facilitadores anteriores son aspectos que se deben tener en control, ya que individualmente o juntos representan papeles de gran impacto en la toma de decisiones, y por consiguiente, en las acertadas que sean. Manteniendo la unión del gobierno corporativo y la gestión de tecnología de información, siendo estos relacionados con los objetivos de las entidades. La importancia de la evaluación constantes de ellos permite mejorar la eficiencia y eficacia de la seguridad de la información, con esto ser más competentes en el mercado.

Las cuatro dimensiones que presenta COBIT 5 son: “Grupos de interés: cada catalizador tiene grupos de interés”. Esto porque en las empresas se dan varios procesos, los cuales pueden ser internos o externos a la empresa. Lo que genera que presenten necesidades propias que se alineen entre sí o no. También, se generan necesidades de los grupos de interés se traducen en metas corporativas, que, a su vez, se traducen en objetivos de TI para la empresa. Donde la segunda dimensión es la “Meta”, las cuales se pueden definir con los resultados esperados y aplicando los recursos deseados. Además, COBIT 5 las divide en las siguientes categorías:

> Calidad intrínseca: Medida en que los catalizadores trabajan de manera precisa, objetiva y proporcionan resultados precisos, objetivos y de confianza. Calidad contextual: Medida en que los catalizadores y sus resultados son aptos para el propósito dado el contexto en el que operan. Accesibilidad y seguridad: Medida en que los catalizadores y sus resultados son accesibles y seguros. (p.28)

Esta clasificación para que los resultados sean más seguros a la hora de la toma de decisiones. También, para definir las autorizaciones de los accesos para quienes realmente pueden tomar decisiones y no existan otro tipo de influencias. Para que dichas metas a seleccionar sean relevantes, completas, actuales, apropiadas, consistentes, comprensibles y fáciles de usar. Logrando así el éxito de estás en la aplicación. La tercera dimensión es el ciclo de vida de cada catalizador, que según COBIT 5 consisten en: “Planificar (incluye el desarrollo y selección de conceptos), Diseñar, Construir/adquirir/crear/implementar, Utilizar/operar, Evaluar / monitorizar y Actualizar/eliminar”. Esto para la aplicación

de la información, procesos, estructuras y políticas; entre otros, en las organizaciones. La cuarta dimensión son las buenas prácticas, que son la proporción de las sugerencias, ejemplos o guías que se toman de marcos como COBIT 5, para implementar mejoras en los catalizadores o recursos, que son necesarias para fomentar los objetivos de la organización lograr crecer en el mercado.

El quinto principio es Separar el Gobierno de la Administración, donde COBIT busca hacer una distinción entre el Gobierno y la Administración. Donde define Gobierno como:

> …asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. (p.31)

Y a la gestión como “planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales”. Por tanto, partiendo de las definiciones entre gobierno y gestión, está claro que comprenden diferentes tipos de actividades, con diferentes responsabilidades; sin embargo, dado que el papel de gobierno es evaluar, orientar y vigilar, se requiere un conjunto de interacciones entre gobierno y gestión para obtener un sistema de gobierno eficiente y eficaz.

El Gobierno asegura que se evalúen las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos corporativos balanceados acordados a lograr; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso comparándolos contra las directivas y objetivos fijados. La Administración planifica, construye, ejecuta y monitorea las actividades conforme con las directivas fijadas por el ente de Gobierno para lograr los objetivos de la Compañía.

El marco de COBIT 5 describe siete categorías de habilitadores. Los cuales constituyen procesos que, a la vez, engloban una categoría. Una compañía puede organizar los procesos como estime conveniente, siempre y cuando se aseguren queden cubiertos todos los objetivos necesarios de gobierno y administración. Las compañías más pequeñas podrán tener menos o más procesos que las compañías más grandes, pero ambas deberán cubrir los objetivos. La siguiente imagen muestra la interacción Gobierno-Gestión, según las categorías:

Figura 6. Interacción gobierno- gestión

Catalizador	Interacción Gobierno-Gestión
Procesos	En el ilustrativo modelo de procesos de COBIT 5 (COBIT 5: Procesos Catalizadores), se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno. El modelo de procesos también incluye una matriz RACI que describe las responsabilidades de las diferentes estructuras organizativas y roles en la empresa.
Información	El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.
Estructuras organizativas	En cada empresa, se definen varias estructuras organizativas; en función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno - por ejemplo, decidir sobre la cartera de inversiones y establecer el umbral de riesgo - y las decisiones y operaciones que las implementan.
Principios, políticas y marcos	Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la empresa, y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones).
Cultura, ética y comportamientos	El comportamiento también es un catalizador clave del buen gobierno y la gestión empresarial. Se establece al más alto nivel (liderando mediante el ejemplo) y es, por tanto, una interacción importante entre el gobierno y la gestión.
Personas, habilidades y competencias	Las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas, pero una habilidad esencial para miembros tanto del órgano de gobierno como de gestión es entender tanto las propias actividades como cuáles son sus diferencias.
Servicios, infraestructura y aplicaciones	Se requieren servicios, soportados por las aplicaciones e infraestructura, para proporcionar la información adecuada al órgano de gobierno y soportar las actividades de gobierno a la hora de evaluar, establecer la orientación y supervisar.

Fuente: Elaborado por ISACA ® 2012

2.3. Hipótesis

La seguridad física y lógica de la información es la que brinda integridad y confiabilidad de los datos/registros en la Cooperativa frente a los cambios tecnológicos.

2.3.1 Operacionalización de la hipótesis

Hipótesis: La seguridad física y lógica de la información es la que brinda integridad y confiabilidad de los datos/registros en la Cooperativa de ahorro y crédito frente a los cambios tecnológicos.

Hipótesis	Conceptos	Variables	Indicadores
La seguridad física y lógica de la información es la que brinda integridad y confiabilidad de los datos/registros en la Cooperativa de ahorro y crédito frente a los cambios tecnológicos.	Seguridad física: son aquellos mecanismos que previenen y están destinados a proteger físicamente cualquier recurso del sistema. Seguridad lógica: aplicación de barreras y procedimientos que resguarden el acceso a los datos. Integridad y confiabilidad: manera de respaldar que la información que se procesa verdadera y realizada de acuerdo con la ley.	Cambios tecnológicos, Cambio de leyes y reglamentos. Seguridad de la información.	Fraudes, Pérdida de información, Control de procesos, Infraestructura adecuada.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación:

3.1.1 Finalidad

La siguiente investigación es aplicada, porque tiene como objetivo analizar del marco normativo COBIT 5 los principios de seguridad física y lógica para aplicar en la Cooperativa. Por tanto, es una guía para realizar los criterios de manuales y procedimientos de los controles de las operaciones de la entidad para la eficiencia y eficacia de la entidad.

3.1.2 Dimensión temporal

Esta investigación se realiza durante el período 2016; por tanto, se considera transversal; porque busca analizar el comportamiento de las operaciones en la Cooperativa sólo en ese periodo.

3.1.3 Marco

En el año 2016, existe un aumento en los servicios que ofrece la tecnología de la información, generando una ilimitación de los controles de redes de datos en el mundo; por lo cual existe la importancia de replantear la seguridad de la información. Al encontrar un nivel de accesos y consumo de datos mayor; se debe implementar infraestructura y recurso humano para tener la capacidad de adaptación a dichos cambios. Además, de protegerse del crecimiento de nuevas amenazas a través de Internet con métodos más sofisticados y riesgosos para el universo.

Para las organizaciones, la exposición del riesgo de la información aumenta y pone en peligro incluso el negocio en marcha. Esto porque existen fraudes informáticos donde sustraen bases de datos de clientes, productos o servicios que se ofrecen, exponiendo la integridad y confiabilidad de la información. Por lo cual, la gestión de la seguridad de la información permite proteger los activos de las entidades.

Sin embargo, sólo se va a investigar la eficiencia y eficacia de las operaciones para la seguridad física y lógica de la tecnología de información, según el marco normativo COBIT 5 en la Cooperativa., brindando con ello la visión de la importancia de la protección de los datos que se ve reflejado financieramente.

3.1.4 Condición

El presente trabajo se realiza con base en una investigación de campo. Los procedimientos necesarios para abordar el tema de la eficiencia y eficacia de las operaciones de seguridad física y lógica, se realizan en la Cooperativa.

3.1.5 Carácter

Esta investigación se considera exploratoria, al no haberse realizado ninguna investigación del tema propuesto en la Cooperativa. Por lo tanto, no existe información previa que pueda usarse como base de análisis y evaluación.

Con la siguiente investigación de tipo causal se quiere analizar las causas y efectos que generaría el inadecuado control de la seguridad física y lógica de la

empresa, que ocasionaría problemas en la integridad y confiabilidad de la información de la Cooperativa.

También, se considera una investigación descriptivo-analítica porque se realiza un análisis y reflexión sobre las características y atributos que se presenta en la Cooperativa, en busca de la eficiencia y eficacia de las operaciones en la seguridad física y lógica de la información.

A la vez, es retrospectiva porque toma en cuenta antecedentes del pasado como los cambios de la tecnología que se han venido dando, para un análisis de la importancia de la seguridad de la información en el presente y la influencia que tiene en la actualidad.

3.1.6 Naturaleza

Esta investigación busca realizar un análisis de la eficiencia y eficacia de las operaciones de la Cooperativa. Esto para medir por medio de variables cualitativas, como el cumplimiento de políticas, los criterios que utilizan para realizarlas, las conductas y actitudes del recurso humano de la entidad; entre otros. El impacto que genera en la seguridad física y lógica de la tecnología de la información. Por ende, percibir la integridad y confiabilidad de los datos de la entidad.

3.2. Sujetos y fuentes de investigación

3.2.1. Unidades de análisis o sujetos de estudio

Durante la investigación de campo se recurre al Gerente de la Cooperativa, los supervisores del Departamento de tecnología, los supervisores de las áreas principales de la Entidad, algunos colaboradores claves para el análisis de controles y políticas internas, y demás personas que se consideren necesarios para medir la eficiencia y eficacia de las operaciones de la Cooperativa, en cuanto a seguridad física y lógica.

3.2.2. Fuentes y documentos consultados

Las fuentes principales de consulta de esta investigación serán: el marco normativo COBIT 5 (Objetivos de control de los sistemas de información y tecnologías conexas), elaborado por Asociación de Auditoría y Control en Sistemas de Información (ISACA, 2017), con el fin de evaluar los principios de seguridad física y lógica de la tecnología de información. También, para el proceso investigativo y de análisis se utilizan guías del libro Sampieri R, Collado C & Baptista M. (2010). A la vez, para realizar el correcto análisis de las evaluaciones de la Entidad se recurrió a las Normas Internacionales de Contabilidad, Normas Internacionales de Información Financiera, principios de aplicación generales, ley N° 4179, entre otros, los cuales brindan conceptos claves para medir si la entidad es eficiente y eficaz en las operaciones de seguridad física y lógica que ejecuta.

3.2.3. Sujetos y fuentes de información:

Fuentes primarias

Los datos obtenidos de las aplicaciones propias de las técnicas e instrumentos de estudio en la empresa, con el fin de evaluar razonablemente los resultados. Además, de la información que se pueda obtener de manera específica del tema de seguridad física y lógica de la tecnología.

Secundarias

Fuentes internas de la empresa: en este caso Estados Financieros Auditados, contratos con empresas que le brinden servicios donde se deba analizar la seguridad física y lógica de los datos, políticas internas de procesos, plan estratégico, manuales de procedimientos, entre otros, solicitados con el Gerente de la Cooperativa. Además, publicaciones periódicas y libros: se seleccionarán de periódicos como la Gaceta, publicaciones que sean de relevancia en el tema de la seguridad de la información, como actualizaciones de leyes, guías actualizadas, entre otros.

3.3. Técnicas e instrumentos de recolección de datos.

3.3.1. Entrevista con el Gerente de la Cooperativa.

Se realiza una entrevista con Geovanny Sánchez, siendo ésta semi-estructurada llevando una guía temática para el conocimiento general del entorno de la Entidad, la cual se profundiza en temas que resalten la necesidad de mayor indagación.

3.3.2. Cuestionario con el encargado del Departamento de tecnologías de información en la Cooperativa

Se elabora un cuestionario con Fernando Jiménez, el fin de medir el grado de cumplimiento de las políticas y normas que debe aplicar la Cooperativa. Esto para el resguardo de la integridad de la información y su confiabilidad para los usuarios internos y externos.

3.3.3. Observación en las áreas de la Cooperativa

Realizar una observación de campo de las áreas básicas donde interviene la tecnología para analizar la seguridad física y lógica de la información, por medio de la descripción en bitácoras. Tomando en cuenta hacer varias observaciones para reducir el sesgo de operatividad; sentirse observado y actuar con más cautela de lo normal.

3.3.4. Análisis de Contenido- Fichas

Realizar un análisis de contenido por medio del instrumento de las fichas, permite efectuar un análisis cualitativo al describir los elementos de ciertas conductas, formas de registros, manera de clasificarlos o categorizarlos, para determinar la frecuencia cuantitativa y así medir los impactos en la seguridad de la información que se procesa. Lo anterior, basado en los principios de COSO 2013 y el marco normativo COBIT 5.

3.3.5. Análisis FODA

Realizar un análisis FODA del Área de tecnologías de información, abarcando los factores fortalezas, oportunidades, debilidades y amenazas. Con el fin de analizar si las metas del que impactan el área de seguridad física y lógica de la información están planeadas para alcanzar los objetivos de la organización y acorde con los principios del entorno de las Cooperativas.

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

En este apartado se recopila y analizan los distintos procesos y actividades identificadas en la Cooperativa. Esta base que se muestra, a continuación, es insumo necesario para la propuesta del mejoramiento de la seguridad física y lógica, según COBIT 5 y COSO 2013 en la Cooperativa de ahorro y crédito, en que se desarrolla esta investigación.

Para efectos de la evaluación del cumplimiento en la relación entre COSO 2013 y COBIT 5, respecto de seguridad física y lógica de la tecnología de la información, para verificar la integridad, transparencia y confiabilidad de los datos procesados, se estudia la aplicación de los componentes de los marcos normativos mencionados anteriormente.

4.1. Ambiente de control

En este componente se contemplan cinco principios, cuyo objetivo principal es mantener en las compañías un ambiente de control eficiente y eficaz que les permita tomar decisiones oportunamente. En relación con el primer principio, el cual es la demostración del compromiso con la integridad y valores éticos, en la búsqueda de medir el cumplimiento en la Cooperativa, según COSO 2013, se evalúa lo siguiente:

- **Código de ética:**

Este aspecto al ser de importancia en toda empresa se mide aplicando el conocimiento que trece de los funcionarios de la Cooperativa tienen al respecto y se obtiene el siguiente resultado:

Todos los colaboradores entrevistados manifiestan que en la Cooperativa existe un código de ética, que data del 2014, pero no se ha revisado su contenido. Además, coinciden en que no hay una directriz acerca de la obligación de leerlo y cumplirlo. También, los entrevistados presentan diferencias en relación con el conocimiento que cada uno tiene respecto del Código de Ética mencionado, según se observa en el cuadro a continuación:

Cuadro N° 1: Conocimiento del Código de Ética de la empresa

Conocimiento del Código de Ética	Total	%	A profundidad	%	Lo desconocen
Total empleados entrevistados	13				
Gerente		15%	1		
Contador			1		
Plataforma de servicios					3
Cajeros					2
Vendedores				85%	4
Supervisor del almacén					1
Encargada del control del inventario					1

Fuente: Elaboración propia

De los empleados entrevistados sólo un 15%, manifiesta conocer a profundidad el Código de Ética; siendo el Gerente y Contador. El restante 85%, afirma desconocer el contenido. Asimismo, del porcentaje de colaboradores que aduce desconocer el referido documento, presentan diferente grado en relación con ese conocimiento, de tal manera:

- un 31% indica que saben de la existencia del código de ética, pero no lo han leído.
- un 23% lo ha leído, pero no a profundidad.

- un 23 % no ve la necesidad de leerlo.
- un 8% no sabe de la existencia de un Código de Ética en la Cooperativa, siendo colaboradores del área del almacén como vendedores.

A continuación, se presentan algunas razones que aducen los colaboradores de la Cooperativa, como justificante de lo anterior:

- Siguen las buenas prácticas.
- Les da pereza leerlo, incluso sin saber si es extenso o pequeño.
- No lo consideran importante para la ejecución de los roles.
- La Cooperativa no los ha obligado u orientado a hacerlo.
- Saben que lo tienen guardado, pero desconocen el contenido.
- No les interesa leerlo, ya que no les genera algún plus en su desempeño, por ende, no sienten motivación.

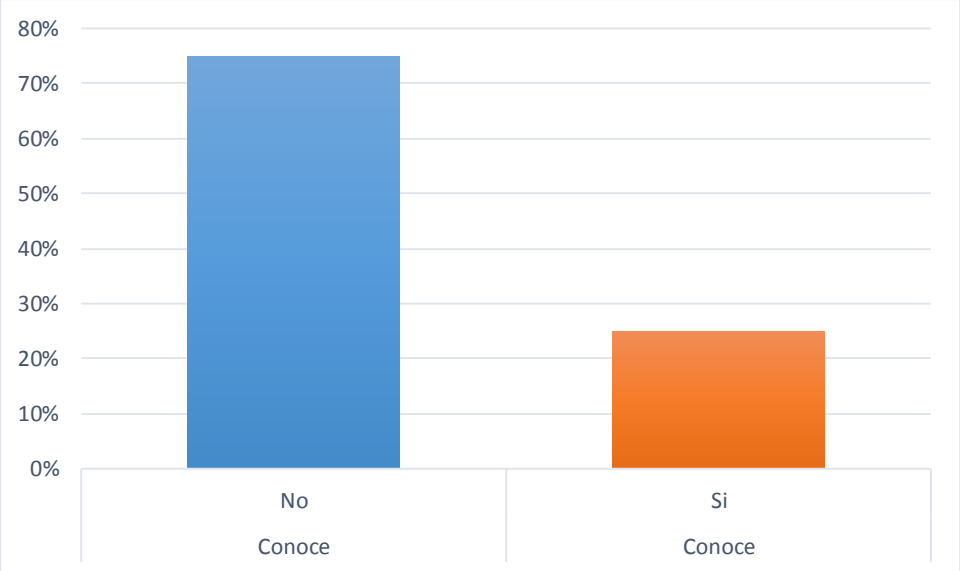
Debido a que ni la Gerencia ni el Consejo de Administración de la Cooperativa han mostrado interés para el cumplimiento del Código de Ética, ni han propiciado que los colaboradores lo conozcan y apliquen, la Cooperativa se ve expuesta a riesgos que pueden conllevar a fraudes por parte de los empleados, por ejemplo, en la manipulación de información, y que podrían no ser detectados oportunamente, por lo que los estados financieros, pueden verse afectados severamente.

- **Límites de responsabilidades de los colaboradores.**

En cuanto los lineamientos acerca de las responsabilidades de los colaboradores, según datos proporcionados por el Gerente, Subgerente y parte de los miembros del Consejo de Administración, se emiten con base en la experiencia de los directivos, conforme van surgiendo las necesidades de la Cooperativa, por ejemplo, se actualizan las funciones para cubrir las actividades o procesos en el desarrollo e implementación de nuevos proyectos, o incluso en mejoras de los actuales.

En relación con la aplicación del manual de puestos, por parte de los colaboradores, a continuación, el gráfico muestra los resultados:

Gráfico 3. Conocimiento de la existencia del manual de puestos



Fuente: Elaboración propia

Como se evidencia en el cuadro anterior, existe un 75% de colaboradores entrevistado desconoce el Manual de Puestos de la Cooperativa. Del cual existen diferentes razones por las cuales los colaboradores aducen no conocer el manual

de puestos, siendo las siguientes: doce empleados consultados, indican que no reconocen la existencia de un manual de puestos, a pesar de que éste se encuentra como documento físico y en medio virtual en la Cooperativa. Además, los empleados indican desconocer las funciones establecidas para cada puesto, ya que, según la opinión los supervisores en la Cooperativa son los que se encargan de indicarles qué hacer y, según las necesidades se van cambiando o agregando nuevas funciones. Esto incluso hace pensar a los trabajadores que pueden no ser sancionados en caso de falla en alguna labor que no ejecuten. Por otra parte, cuatro colaboradores indican que, sí conocen la existencia del Manual de Puestos, pero no se han preocupado por leerlo, esto porque han recibido indicaciones por parte de los compañeros, supervisores y no lo creen necesario. Entonces, únicamente el restante 25%, sí conoce y ha leído las funciones que deben desempeñar, por lo cual, realizan las labores con base en lo que la Cooperativa ha establecido. Entre ellos se encuentra el área de la Gerencia y de Contabilidad, cabe mencionar que los mismos llevan varios años trabajando para la Cooperativa.

Por parte de la Gerencia de la Cooperativa no se observa interés acerca de comunicar formalmente las funciones al personal que se encuentran en el Manual de Puestos, lo cual propicia un descontrol en éste, respecto de las funciones que deben ejecutar, según cada puesto y con ello se favorece la realización de funciones de manera inadecuadas e inapropiadas, exponiendo a la Cooperativa, entre otros a la pérdida de información clave, tanto del personal como de los asociados, aunado al riesgo de alteración de los datos por indicaciones erróneas.

Además, de ser el Manual de Puestos aprobado por el Consejo de Administración, lo cual representa un incumplimiento del acuerdo, incurriendo en una falta por la Cooperativa.

- **Aplicación de mecanismos para cumplir los valores en la Cooperativa**

En la importancia por conservar un ambiente de control en la aplicación correcta de los principios y valores en la Cooperativa, se realiza la consulta a los colaboradores acerca de la forma como son evaluados. A continuación, se muestran los resultados de las entrevistas:

Cuadro N°2: Existencia de mecanismos para evaluar el cumplimiento de los valores.

Mecanismos para el cumplimiento de valores	Total	%	Consideran que No	%	Consideran que Sí
Total entrevistados	15				
Área de Gerencia				13%	2
Área administrativa		13%	2	20%	3
Área de Plataforma de servicios		7%	1	13%	2
Área del almacén		33%	5		
Total		54%		46%	

Fuente: Elaboración propia

Se deduce que la Cooperativa a criterio del personal entrevistado no hay evaluaciones respecto de la ejecución de los valores, que por estrategia son definidos en la Cooperativa, representado por un 54% de los entrevistados. Sin embargo, el restante 46%, considera que, sí se evalúa, de tal manera que en un 33% (Gerencia y Área Administrativa) indican que se busca generar un ambiente de confianza entre los funcionarios, y con ello se cumple con el control de la

aplicación de los valores. Otro 13% de los entrevistados que considera existen mecanismos para evaluar el cumplimiento de valores (Plataforma de Servicios), estiman que cada supervisor de área es el responsable por buscar crear un ambiente de trabajo agradable, y así crear un compromiso por parte del colaborador con la empresa y así comportarse adecuadamente. Sin embargo, en una visita de observación realizada, se establece que los supervisores no están pendientes de esos aspectos, ya que se preocupan más por el cumplimiento de la parte operativa.

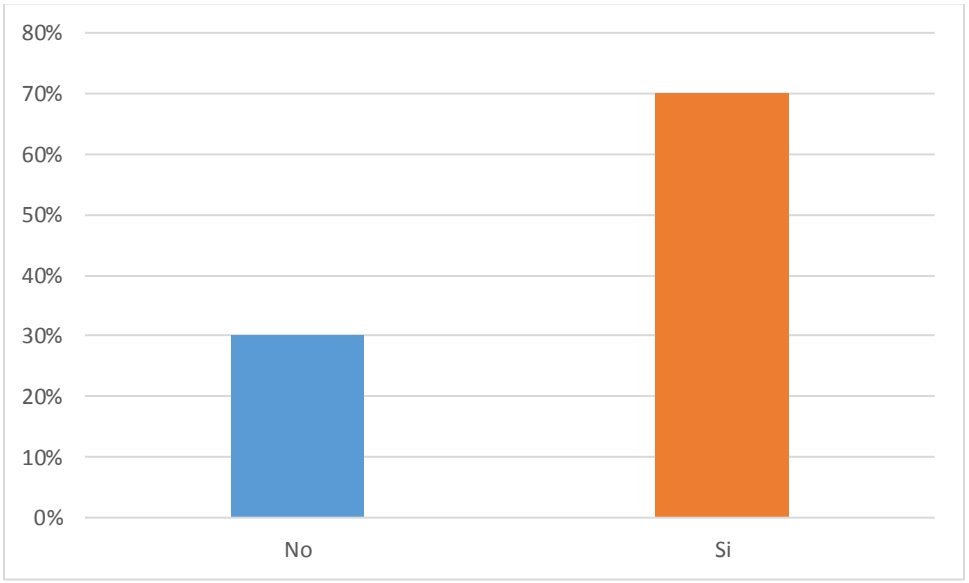
Debido a que no existen lineamientos para la medición de la aplicación de valores establecidos en la Cooperativa, los colaboradores tienen oportunidad para actuar de forma arbitraria o incorrecta, sin ser sancionados, ya que como no se aplica una evaluación al respecto, los empleados actúan, según su criterio. Ello puede generar posibles problemas de compañerismo, que afectan a los demás colaboradores e incluso a los clientes y asociados. Respecto de, por ejemplo, situaciones que se han dado en los últimos 5 años en la Cooperativa, se aportan comentarios por parte de dos de los colaboradores del área de servicio al cliente, los cuales indican que, en el año 2015, se da un fraude por parte de un funcionario considerado como colaborador de confianza, por los años de permanencia entre el personal de la Cooperativa. Posterior al fraude no conocen de medidas comunicadas al personal a raíz de la situación, únicamente se rescinde de la persona, pero no se toman algunas medidas de control internas para evitar de nuevo dicho altercado, y tampoco se da conocer lo sucedido a los asociados, a la espera que se obtenga un resultado favorable en el proceso que se está llevando

a cabo para recuperar al menos una parte de lo perdido. Lo expuesto, afecta en el periodo correspondiente los estados financieros de la Cooperativa, y por ende, los rendimientos de los asociados.

- **Organigrama de la Cooperativa**

En la búsqueda por el cumplimiento del tercer principio que es el establecimiento de estructuras, asignación de autoridades y responsabilidades, se analiza la existencia de un organigrama, ya que representa las directrices de control y supervisión dependiendo del área y puesto por desempeñar, es trascendente que los colaboradores lo conozcan y apliquen durante la ejecución de las funciones. Para ello, se les consulta a diez colaboradores, a continuación, se muestra un gráfico de las respuestas:

Gráfico 4 Conocimiento del organigrama



Fuente: Elaboración propia

Al respecto, indican en un 70% que conoce el organigrama, sin embargo, un 60% de estos colaboradores que admite conocerlo, no pueden asegurar si se encuentra actualizado, el restante 10%, conoce el organigrama y piensa que está actualizado.

Se le consulta al respecto a la Gerencia e indica que el organigrama data del 2008 y que es la versión más actualizada con la que se cuenta. En relación con las respuestas de los colaboradores mencionadas anteriormente, no se han percatado que, si bien, piensan que está actualizado, no han tomado en cuenta que se han creado nuevos departamentos y no se encuentran considerados en el organigrama.

A la vez, un 30% de los colaboradores desconoce que hay un organigrama en la compañía, por lo cual determinan que hay departamentos diferentes por cómo van conociendo los procesos, pero no tienen la visión completa de la integración global de la Cooperativa, en relación con las líneas de autoridad y responsabilidad.

Por lo expuesto, en la Cooperativa existe una mayor posibilidad que se malinterpreten las líneas de autoridad y responsabilidad por la falta de actualización, lo cual, afecta la eficiencia y eficacia del personal en la realización de las distintas funciones y repercute en la contabilización de las transacciones, afectando la rentabilidad del negocio.

- **Evaluaciones del personal**

Como parte del segundo principio se considera en relación con el ejercicio por parte del Consejo de Administración de la responsabilidad de supervisión del control interno, que cada colaborador requiere que la organización cuente con las evaluaciones de las labores que desempeñan. Lo anterior, con el fin de determinar el cumplimiento de los objetivos que busca la Entidad, acorde con las políticas establecidas y los controles de seguridad que se deben implementar. En la Cooperativa se consulta a once personas, las cuales son consistentes en la respuesta de que en la entidad se carece de evaluaciones de desempeño, en áreas de servicio al cliente, plataforma de servicios y cajeros. Indican que en ocasiones existen llamadas de atención, sin embargo, respecto de ellas no tienen documentación soporte que las evidencie.

Además, no existe un departamento de recursos humanos que pueda dedicarse a realizar la supervisión del desempeño. Por lo anterior, la responsabilidad de la evaluación queda en manos de los supervisores del área, lo cual, para algunos colaboradores no es equitativo, porque muchas veces existe afectación por asuntos personales y al tomar decisiones por ejemplo respecto de ascensos, se pueden ver afectados, aparte de la mayoría del personal no cuenta con la formación académica ideal para desempañar necesariamente una labor que amerite competencias o destrezas, incluso profesionales, específicas.

Para el caso de los directivos, son evaluados por el Consejo de Administración, pero, según indican miembros de dicho Consejo, no tienen definido un periodo para hacerlo, es decir, puede pasar un largo tiempo y no se les evalúa el

desempeño, lo cual, puede perjudicar a la hora de tomar una decisión errónea, y no ser oportuno en poderla corregir, con lo cual pueden afectar la integridad de la información que se les brinda a los usuarios y asociados, repercutiendo en los estados financieros.

Un área de importancia para la compañía es la administración de los sistemas, la cual se determina que los servicios de soporte y mantenimiento son contratados externamente, por lo que se consulta acerca de qué manera es evaluado el área de servicio externo para obtener seguridad de la información de la Cooperativa. Según datos de la Gerencia de la Cooperativa y los encargados de brindar el servicio outsourcing, estos realizan un reporte semestralmente y, también, efectúan reuniones en rangos de un mes y medio, con el fin de evaluar alguna eventualidad que se presente e implementar mejoras.

Durante la entrevista realizada a las personas encargadas de dar soporte y mantenimientos del sistema, se identifica que son hermanos, que tienen un grado de escolaridad acorde con las labores para las que son contratados y se están capacitando constantemente. Ellos concuerdan en los reportes semestrales que le brindan a la Cooperativa y en las reuniones que hacen, aunque indican que en ocasiones por falta de tiempo son pospuestas o canceladas. Al consultar cuál ha sido la experiencia en la empresa, indican que, sí han pasado situaciones donde se cae el sistema, y normalmente ellos no asisten a la Cooperativa, ya que la primera fase es tratar de arreglarlo vía Internet, es decir, se les permite accesar vía remota a la computadora donde se está generando el problema, lo cual puede

afectar a la Cooperativa, dada la visualización o exposición de datos confidenciales y la posible divulgación.

Sin embargo, mediante una revisión realizada a la estructura del cableado y conectores, estos no funcionaban adecuadamente, por lo que se decidió cambiarlos. A raíz de lo anterior, se establece efectuar una revisión de equipo, que anteriormente no se hacía, para prevenir este tipo de problemas y se lleva un control por cada activo. Asimismo, se determina un cronograma de control preventivo de esos aspectos. No obstante, al ser consultados al respecto, 6 de los colaboradores entrevistados indican que el hardware se revisa sólo si presenta fallas, de lo contrario no lo hacen, por lo que se deduce, que el control preventivo no se aplica.

Además, existe un riesgo en la Cooperativa respecto de la información que mantiene, en vista de que puede sufrir la pérdida, ya que, si bien es cierto, se cuenta con un respaldo de dicha información, esto no garantiza que sea íntegra y que no se estén realizando manipulaciones de los datos por parte del personal, incluso por parte de personas externas que brindan mantenimiento al sistema.

- **Incentivos por rendimientos**

En relación con la existencia de incentivos por rendimientos en la Cooperativa, se realiza la consulta a veinte de los funcionarios, resultando, que todos coinciden en la inexistencia del pago de incentivos en efectivo o especies, sea por rendimiento u otros aspectos, ya que ni la Gerencia ni el Consejo de Administración lo consideran necesario y no se ha medido si la ausencia de ese tipo de mecanismos

provoca alguna desmotivación en los empleados, que eventualmente los impulse a realizar acciones fraudulentas, afectando a la compañía.

- **Proceso de contrataciones**

Como parte del marco COSO 2013, el cuarto y quinto principio van de manera conjunta en la aplicación, siendo los siguientes: demuestra su compromiso de reclutar, capacitar y retener personas competentes; retiene a personal de confianza y comprometido con las responsabilidades de control interno.

Se establece que en el manual de funciones que tiene la entidad, se establece la existencia de un departamento encargado de realizar los procesos de reclutamiento del personal; sin embargo, según las observaciones aportadas por los empleados, los encargados de contratar y entrevistar son el Gerente y Subgerente. Ellos cuentan con un archivo de los currículos que las mismas personas van a entregar o que por recomendaciones de los mismos colaboradores reciben. Asimismo, los citados funcionarios comentan que, si sale a concurso alguna vacante seleccionan, según las competencias y habilidades que observan, y luego proceden a entrevistar y tomar la decisión de elegir a la persona considerada como la óptima para el puesto y que, en ocasiones, se realiza una entrevista con la persona que va a supervisar de forma directa el trabajo, para conocer otro criterio para la selección, pero ese proceso no es consistente, ya que depende de factores como disponibilidad de tiempo.

En el análisis con los colaboradores se determina que la mayoría de personas que laboran, lo hacen porque en el momento fueron a efectuar prácticas de colegios

técnicos y por recomendaciones de los colaboradores, siendo conocidos o parientes. Debido a esto, los directivos de la Cooperativa consideran que tienen mayor confianza en que el desempeño sea mejor, lo cual, genera que en la Cooperativa existan personas conocidas y de relaciones cercanas que incluso pongan en riesgo la manipulación de información para beneficios personales, que afecten los resultados íntegros y confiables de la Cooperativa, debido a que existen puestos de supervisión e inferiores que son realizados por parientes.

- **Evaluación de la escolaridad del personal**

Dada la importancia por mantener un ambiente de trabajo integrado por personas competentes y tengan la capacidad de desempeñar las labores de manera eficiente y eficaz, y acorde con los requerimientos del puesto, se evalúa el nivel en cuanto al grado de profesionalismo de diecisiete colaboradores. A continuación, se muestra el resultado:

Cuadro N°3 Escolaridad del personal

Escolaridad del personal	Total	%	Cantidad
Total empleados entrevistados	18		
Licenciatura		33%	6
Bachiller de secundaria		22%	4
Estudiantes del bachiller Universitario		22%	4
No tienen bachiller de secundaria		17%	3
Grado de Maestría		6%	1

Fuente: Elaboración propia

Al respecto, existe un 33% de colaboradores que cuenta con un grado de licenciatura, que va de acuerdo con el puesto, por ejemplo, el contador es licenciado en Contaduría Pública; en otros puestos hay licenciados en administración de empresas con diferentes énfasis como lo es recursos humanos,

finanzas y mercadeo. Además, un 17% de los empleados aún no concluye la secundaria, los cuales laboran en el área de cajas y sucursal. Incluso apenas un 6% cuenta con un grado de maestría siendo el gerente, la misma en Administración de empresas con énfasis en cooperativismo.

Lo anterior, resulta que la gran mayoría de trabajadores están en proceso de obtener un grado de profesionalismo mayor y otros no tienen interés de continuar los estudios. Por esto, la Cooperativa podría ser perjudicada, en aspectos como ejecución de labores equívocas, por falta de conocimientos básicos del puesto, y aplicación de políticas y procedimientos desactualizados, pudiendo afectar información clave para la Cooperativa.

- **Capacitaciones del personal**

Debido a los constantes cambios que se presentan en el entorno, las empresas procuran capacitar a los empleados, para que tengan las herramientas y habilidades para desempeñarse de la mejor manera. Esto, por ejemplo, en los ataques cibernéticos como phishing, fraudes bancarios, robo de datos, entre otros. Según las entrevistas realizadas a veinte colaboradores de la compañía, al respecto se obtienen los siguientes resultados:

Cuadro Nº4 Realización de capacitaciones al personal

Capacitación del personal	Total	%	Cantidad	Si	No
Total empleados entrevistados	20				
Área de Ventas		50%	10	x	
Área de Contabilidad		20%	4	x	
Plataforma de servicios		15%	3		x
Área de cajas		15%	3		x

Fuente: Elaboración propia

Según se muestra en el cuadro anterior, a un 50% de los entrevistados se le brinda capacitaciones, específicamente, al personal del área de ventas de la sucursal, por parte de los proveedores de los distintos productos que comercializa, con el fin de asegurarse que se genera la colocación de esta manera efectiva. Además, un 20% indica que se brinda capacitación permanente al personal de contabilidad y servicio al cliente, sobre conocimiento de productos, valores, atención al público, pero éste fue desmentido por el personal que, actualmente, labora en dichas áreas. Unido a lo anterior, un 30% de los entrevistados, indica que no han recibido ninguna capacitación, incluso personal con más de tres años de laborar para la Cooperativa.

Por consiguiente, las capacitaciones en la Cooperativa, sólo se dan si son brindadas con recursos externos, y en alguna ocasión, por voluntad de los compañeros. Se carece de un personal actualizado que no puede reconocer por ejemplo cambios del entorno, avances en la tecnología de la información o riesgos a los que se expone la Cooperativa, lo cual afecta las buenas prácticas para lograr la seguridad física y lógica de la información en la Cooperativa.

4.2. Evaluación de riesgos

Dentro de la composición de este componente se encuentran cuatro principios que buscan identificar y, posteriormente, evaluar las áreas más riesgosas en las compañías. El primer y segundo principio se interrelacionan y son los siguientes:

- se especifican objetivos claros para identificar y evaluar riesgos para el logro de los objetivos;
- se identifican y analizan riesgos para determinar cómo se deben mitigar.

Para determinar que estos principios se aplican en la Cooperativa de ahorro y crédito, se realizan varias entrevistas de las cuales se obtienen los siguientes resultados.

En las entrevistas realizadas al Gerente y miembros del Consejo de Administración, se determina que la responsabilidad de identificar los riesgos de la Cooperativa queda a cargo de ambas instancias; sin embargo, la mayor responsabilidad recae en el análisis del Gerente. En el caso de la actualización de los cambios, lo realizan ambos, pero en relación con el tema de la tecnología prefieren no actualizar de manera drástica los procesos, para no tomar riesgos grandes; por lo anterior, los procesos no están automatizados por completo, a pesar de los avances tecnológicos. Esto enfrenta de manera directa a la Cooperativa al riesgo de los controles que pudiera esperarse se encuentren programados en el sistema, no existan, y por otra parte, que al ser muchos de los procesos ejecutados de forma manual, existe más riesgo respecto de la manipulación de la información, y de la posibilidad de ser alterados los datos y registros de la información, afectando los resultados y la transparencia en la toma de decisiones.

Además, para evaluar qué tan acertada es la labor que realiza la administración en la Cooperativa, se consulta a 17 de los colaboradores, si cuentan con parámetros establecidos en cuanto a objetivos, metas y desempeño, coincidiendo todos que no, por tanto, existe un grado mayor de posibilidad de equivocarse en la

identificación de riesgos en los distintos enfoques de los puestos, porque para cada área hay diferentes características y medidas necesarias por aplicar, para obtener resultados óptimos, en consecuencia, la administración está dejando de lado factores importantes para reconocer los riesgos que se pudiesen enfrentar.

Para evaluar el área de sistemas de información de la Cooperativa, respecto de la capacidad de afrontar cambios y riesgos inherentes a los datos resguardados, se realiza la aplicación de un análisis FODA, el cual se muestra a continuación:

FORTALEZAS	**DEBILIDADES**
• Un sistema robusto para el procesamiento de información. • Sistemas Integrados. • Inventarios tecnológicos anuales. • Servidor certificado. • Switch certificados. • Sistemas de respaldo de electricidad. • Contrato de soporte en sistemas y técnico las 24 horas del día. • Sistema de respaldos diario sobre sistemas y uno semanal general. • Actualizaciones de sistemas operativos al día. • Antivirus y programas relacionados al día. • Conectividad vía fibra óptica hacia sucursal	• Falta de dominio propio para tener cuentas de email empresariales. • Cableado estructurado tipo 5 no cumple las normas actuales para flujo de información. • Inadecuada distribución de switch. • Hardware sin homologar a nivel de switch. • Cambios de posición de hardware sin un debido proceso de traslado y cambio. • Velocidad de Internet. • Falta licencias de una mayoría de sistemas y programas. • Sistema de impresión no centralizado. • Falta de un servidor robusto como plan de contingencia. • Navegación sin responsabilidad y conexiones de hardware de usuarios externos a la Cooperativa. (Dispositivos USB llaves maya).
OPORTUNIDADES	**AMENAZAS**
• Mejorar la comunicación de proveedores	• Robo de Información (Hackeo)

de software externo. • Implementación de tecnologías nuevas. • Innovación de servicios. • Homologar Switch de la central. • Fibra Óptica hacia los proveedores • Cambio proveedor de Internet y vía a fibra óptica. • Sistema de respaldo eléctrico al siguiente paso que sería planta eléctrica diésel. • Adquirir un servidor robusto para plan de contingencia.	• Virus informáticos. • Mal soporte de proveedores externos de plataformas de cobro. • Instalación de programas externos a la Cooperativa

En la evaluación de los procesos, se identifica que la gestión del área de tecnología de información, se tiene contratada por servicios externos a la Cooperativa, desde el año 1990, es decir, más de 27 años, pero por parte de la Cooperativa no se controla internamente ese proceso, y por ello la Entidad está retrasada en la identificación e implementación de mejoras tecnológicas, y sólo se requiere de manera esporádica algún cambio o asesoría, lo que pone en riesgo a la Cooperativa de presentar retrasos en función de la competencia, además carece de políticas y controles respecto del área de tecnología por lo que está expuesta a que se pueda manipular la información de los asociados de forma interna o externa, o bien, presentar un fraude que ocasione grandes consecuencias, sin que se pueda determinar oportunamente.

Por lo anterior, se analizan los contratos, uno para el soporte del sistema y otro para mantenimiento del sistema, ya que se manejan por separado, detallándose lo detectado, a continuación:

Contrato N°1 Soporte del sistema	
Objeto del contrato	Asesoría y mantenimiento en sistemas de aplicación
Personas involucradas	• Gerente General de la Cooperativa de ahorro y crédito. (Contratante) • Representante legal del Contratista.
Condiciones	1. El contratista dará servicio de asesoría y mantenimiento a el Contratante cubriendo 16 horas por mes en las oficinas de la Cooperativa, mediante dos visitas quincenales de 8 horas. 2. El servicio cubre mejoras permanentes, verificación y actualización de rutinas, depuración de directorios (carpetas), depuración de archivos, evacuación de consultas, elaboración de programas para cubrir nuevas necesidades, llamadas telefónicas y soporte de emergencia sin costo adicional. 3. El contratista registrará en una bitácora el trabajo realizado. Esta bitácora estará en custodia de la Cooperativa en las oficinas de Contabilidad. 4. El trabajo que se realice será en coordinación con el Contador de la empresa. 5. Horas adicionales aprobadas por la Gerencia General que se apliquen por complemento de requerimientos (no emergencias) tienen costo adicional. 6. El costo por asesoría y mantenimiento tiene un pago establecido mensual, pagadero quincenalmente, y el mismo tendrá un incremento anual del 10%.
Fecha de firma del contrato	01 de enero de 2011.
Plazo	Indefinido.

Contrato N°2 Mantenimiento del sistema	
Objeto del contrato	Servicios de mantenimiento preventivo y correctivo a equipos de cómputo tales como: Microcomputadores, impresoras, Accesorios y equipos relacionados.
Personas involucradas	Gerente General de la Cooperativa de ahorro y crédito. (Contratante) Representante legal del Contratista.
Condiciones	1. Inspección y comprobación de funcionalidad de los componentes básicos del equipo, limpieza, lubricación, ajuste del mismo si es necesario. 2. Además, el servicio incluye la observación de la operación Inspección del equipo, para detectar fallas de operación cuya repetición puede llegar a provocar averías. 3. El servicio de mantenimiento preventivo se brinda en base inventario físico y de acuerdo con un plan o cronograma. 4. El costo se tiene un pago establecido mensual, pagadero quincenalmente, y el mismo tendrá un incremento anual del 10%. Además, de un aumento adicional si ingresa nuevo equipo

	a la Cooperativa.
Fecha de firma del contrato	01 de marzo de 2012.
Plazo	Indefinido.

En el análisis de ambos contratos, se identifica la existencia de una relación familiar de primer grado entre las dos personas contratadas para los servicios externos. Por lo cual, la Cooperativa presenta exposición a riesgo, debido a la gran confianza en toda la organización, incluso cuando son servicios outsourcing.

Se establece que en los contratos se estipula la mensualidad por cancelar y las obligaciones de ambas partes en la prestación del servicio; sin embargo, en la entrevista con el encargado del área de soporte externo, se evidencia que sí existen deficiencias, ya que éste no se apersona a las instalaciones de la Cooperativa, sino que intenta solventar cualquier problema vía telefónica, o aún más riesgoso para la compañía por medio de un acceso remoto a la computadora que presenta el problema, lo soluciona, con lo cual un externo a la Cooperativa puede hasta sustraer o manipular información confidencial de los asociados o de las transacciones normales del negocio, sin que ésta lo perciba.

El contrato que se mantiene con el externo para los citados servicios, no incorpora reglas básicas necesarias para mantener la integridad y seguridad de la información de la Cooperativa, para evitar los riesgos asociados en la externalización de servicios, esto porque al ser el área de tecnología es una herramienta estratégica para las empresas, independientemente de su tamaño, y

que garantiza una mejora continua de los procesos de negocio por medio de la flexibilidad, la innovación y la optimización de los flujos de trabajo, al aportar dichos servicios, no sólo la propia tecnología, sino además, conocimientos y recursos especializados.

Además de todos estos aspectos puramente estratégicos, de negocio y financieros, debe prestarse especial atención a los aspectos meramente jurídicos, debiendo tomar especiales precauciones desde el momento mismo de la preparación del contrato de prestación de servicios. Así, deberán analizarse desde el inicio las implicaciones legales que el servicio puede conllevar en aspectos como:

- Cumplimiento normativo.
- Protección de datos de carácter personal.
- Normativas sectoriales como, por ejemplo, normativas de servicios financieros y de seguros.
- Confidencialidad / Secreto.
- Seguridad, Continuidad y Migración
- Responsabilidades y elementos de relación para gestionar el proceso
- Modelo de gestión que evite controversias y permita la revisión continua del contenido y alcance, además de su adaptación a las circunstancias del momento de forma fácil.
- Una descripción precisa de los productos que se esperan recibir y como se esperan recibir.

- Vínculos para proveedor con objetivos concretos y establecer cláusulas de penalización para el supuesto de que no sean alcanzados.
- Mecanismos necesarios para asegurar la continuidad del servicio en caso de rescisión.

Con lo anterior, se puede evidenciar que los contratos actuales que tiene la compañía no son los necesarios para poder establecer una seguridad hacia la Cooperativa en cuanto a la información. Esto porque no cumplen ni el 30% de los requerimientos mencionados. Por lo cual, pone en riesgo la continuidad del negocio. Cabe resaltar la falta de limitaciones y cláusulas que cubran la confidencialidad de la Cooperativa.

Este aspecto es de suma importancia en todas las empresas, para proteger la información de cada entidad, siendo ésta, tanto del funcionamiento normal de la entidad como de información personal de los usuarios y asociados. Por lo expuesto, existe un gran riesgo de que la Cooperativa se vea afectada por la divulgación de los datos de las personas que tienen de una u otra manera relación con la Entidad y a la cual han brindado la información personal.

Se realiza, además un análisis FODA del área de asociados para identificar los riesgos, y se determina los siguientes:

FORTALEZAS	**DEBILIDADES**
• Cantidad de asociados • Potencial de Crecimiento • Aporte de capital • Uso de servicios (médico, becas.	• Retiro de capital social • Ingresos por un fin • Diversidad de cultura • Falta de lealtad (intereses personales)

créditos) • Trayectoria • Imagen prestigiosa • Mejoramiento socioeconómico del asociado	• Deficiencia a nivel informativo • Falta de capacitación al asociado • Falta de líderes en las comunidades
OPORTUNIDADES • Líderes comprometidos en comunidades • Crecimiento económico • Crecer a partir de nuevas generaciones • Fomentar el cooperativismo como forma de vida.	**AMENAZAS** • Ingreso de asociados sin mantener permanencia • Constantes retiros de capital por parte del asociado • Globalización • Competencia

Existe una gran debilidad, porque la aplicación del sistema donde se ubica la información del asociado presenta opciones, que permite a varias personas manipular dicha información, causando que se alteren fechas y ocasionen molestias en los asociados, por tanto, para la Cooperativa, representa un riesgo que los asociados se retiren y pongan en peligro la operatividad de la compañía, aunado a que los resultados financieros, por ejemplo, en lo que se refiere a cartera crediticia pueden presentar diferencias debido a ello.

- **Análisis de las partes relacionadas del personal de la Cooperativa**

En la evaluación del personal de la Cooperativa, y dada la estrategia de la organización que apunta a crear un ambiente laboral de confianza, se investiga los grados de consanguinidad y de afinidad, para determinar la existencia de un riesgo en la ejecución de las funciones y se obtienen los siguientes resultados:

- El contador de la empresa es primo de dos colaboradores del almacén. A parte de uno de ellos establece una relación de noviazgo con una colaboradora del área de plataforma de servicios.
- Una cajera es pareja de un auxiliar de contabilidad, ambos tienen alrededor de 3 años en la Cooperativa, por lo cual ya conocen bastante del sistema y los procesos, lo cual podría ser riesgoso para la Cooperativa.
- El supervisor del almacén es hermano de una colaboradora de plataforma de servicios, la que tiene mayores responsabilidades también, en dicha área.
- El Subgerente y la Tesorera son cuñados.

Lo anterior, implica que en la Cooperativa existen relaciones de consanguinidad y afinidad muy cercanas, pero no se han establecido los mecanismos de control interno que minimicen el riesgo de posibles fraudes o manipulación de la información para conveniencia personal de algún colaborador.

4.3 Actividades de Control

Existe la necesidad que las organizaciones empleen actividades de control que contribuyen a la posible mitigación de los riesgos inherentes para el logro de los objetivos establecidos. Dichas actividades dan soporte a todos los componentes del control interno, pero en especial al de Evaluación de Riesgos.

Para esto se les consulta a los directivos de la Cooperativa, si conocen el marco normativo COBIT 5, a lo cual contestan negativamente; además, indican que piensan que es muy caro la aplicación de los controles y sugerencias que éste

consigna; con lo cual pareciera que por falta de conocimiento, en la Cooperativa no se busca la actualización de prácticas que fortalezcan el control interno, conforme cambian los entornos y surgen nuevos riesgos que pueden incluso amenazar la operación.

- **Plan de continuidad**

Cuadro N°5 Aplicación de un plan de continuidad

Aplicación de un plan de continuidad	Total	%	Si	No
Total empleados entrevistados	4			
Gerencia		25%	x	
Supervisor de Contabilidad		25%	x	
Supervisor de Plataforma de servicios		25%		X
Supervisor del Almacén		25%		X

Fuente: Elaboración propia

Como se muestra en el cuadro anterior, existe una disyuntiva entre la Gerencia y el Área de Contabilidad contra el área de plataforma de servicios y el almacén, y entre los empleados entrevistados se contradicen porque unos indican que sí cuentan con un plan de contingencia y otros, que no, lo cual demuestra que hay una falta de conocimiento entre las diferentes áreas de la compañía, respecto de las actividades de control con que cuenta, y que puede ser por la causa de desconocimiento de en qué consiste el referido plan. Según se indaga, la Cooperativa carece de un plan de continuidad de negocio, con lo cual no se han tomado medidas para no perder el objetivo principal de proteger los procesos críticos y operativos del negocio contra desastres naturales o fallas mayores por la interrupción de las operaciones en la Institución, con lo cual la Cooperativa se encuentra expuesta a mayores impactos financieros, pérdida de información

crítica, credibilidad y productividad. El no contar con un plan de continuidad de negocio impide a la Cooperativa continuar operando en caso de una interrupción, y propicia que los asociados opten por salirse de ella, además, de que un plan de este tipo es preventivo más que correctivo para continuar con las actividades críticas en la operatividad del negocio. Por otra parte, existen competencias directas e indirectas que por mejor servicio afectan la continuidad del negocio, las cuales no están identificadas ni son analizadas, para gestionar de forma oportuna los riesgos que les son asociados.

Cuadro N°6 Evaluación del cumplimiento del área contable

Evaluación del cumplimiento del área contable			
Acciones	Si	No	Comentarios
Supervisión de los procesos contables.	x		
Evaluaciones y supervisión de los accesos a la información y archivos, utilizados en los procesos contables.		x	Por parte de la gerencia
Presentación de informes de seguimiento.		x	No quedan registros
Validaciones de calidad de la información, revisando que las transacciones u operaciones sean veraces y están adecuadamente calculadas y valoradas aplicando principios de medición y reconocimiento.	x		De forma diaria por el Contador General
Comparaciones, inventarios y análisis de los activos de la entidad, realizadas a través de fuentes internas y externas.	x		No se hacen externas
Autorización apropiada de las transacciones por los órganos de dirección y administración.	x		
Autorización y control de documentos	x		

Fuente: Elaboración propia

En la evaluación de las actividades de control que aplica la Cooperativa al Área Contable, se establece que existe control por parte del supervisor hacia la información que se produce en la Cooperativa, ya que éste supervisa a los asistentes en la comparación de documentación física, versus sistema que se registra diariamente, es decir, se lleva un control exacto de forma diaria, sin contar los fines de semana, ya que esa área no labora en ese horario. Lo anterior, debido a que el personal encargado de supervisar los fines de semana no labora, por tanto, en ese sentido, se incrementa el riesgo de que exista robo de información o manipulación de dicha información, en ese lapso, pero no existen controles definidos en la Cooperativa al respecto.

Cuadro N°7 Evaluación del cumplimiento del área de Sistemas de Información

Evaluación del cumplimiento del área de sistemas de información			
Mantenimiento preventivo	**Aplican**	**No aplican**	**Observaciones**
Eliminación de virus y actualización del antivirus.	Si		
Instalación y actualización de programas anti-phishing.		No	
Depuración de Disco duro, depuración de registros y eliminación de programas dañinos.	Si		En ocasiones, no constantemente
Limpieza de polvo en las torres u otros dispositivos.		No	Delegan a la Cooperativa
Limpieza Interna del equipo	Si		Es necesario más frecuente
Verificación de conexiones.		No	Sólo si se presenta alguna falla
Actualizaciones de Firmware según programa o necesidad.	Si		
Revisión de Routers, Switches, tarjetas de red, cables.		No	Sólo si es solicitado
Desarrollo paulatino de Inventario Tecnológico y políticas de carpetas por departamento.	Si		
Bitácora por equipo	Si		

Fuente: Elaboración propia

En cuanto a la limpieza del equipo, no se ejerce de manera adecuada, esto porque la limpieza de memorias, fuente de poder, ventiladores, tarjeta madre, no se

hacen, según las mejores prácticas. Además, a los empleados nunca se les envía correos informativos, respecto de posibles amenazas, o ataques cibernéticos. Sólo se ha adoptado la medida de llevar un control del equipo, para revisarlo cada cierto tiempo como paliativo por los casos de problemas presentados años atrás. Por lo tanto, el control no está bien diseñado, de tal manera que permita identificar y llevar un histórico por equipo para mantener un historial de cambios de hardware y ubicación, así como incorporar más configuraciones a nivel empresarial para prevenir manipulación de información. Tampoco se ha designado una persona calificada en la Cooperativa como encargada de verificar que las funciones de soporte y mantenimiento externos se den adecuadamente, por tanto, pone en un gran riesgo la seguridad de la información del personal, asociados, y demás personas relacionadas con la Cooperativa.

Llama la atención, que según las Normas Internacionales de Auditoría (NIA), específicamente la NIA 402, considera que para emitir el informe de auditoría debe tomar en cuenta el informe tipo 1 ó 2,para describir los riesgos que se tienen al contratar personal externo de la compañía para la administración del área de Tecnología de Información, pero en el informe del auditor externo, no se puede inferir que se haya recurrido a ese tipo de informe (1 ó 2), ya que parece no se ha detectado lo acontecido en la Cooperativa respecto de la contratación del personal externo de la entidad en relación con el mantenimiento y soporte del sistema y que se describe en esta investigación.

- **Verificación de accesos al sistema**

A pesar de la gran importancia que tiene mantener controles en relación con las aplicaciones de sistema que utilizan los usuarios para efectos de restringir las funciones de cada usuario para lo que necesita exclusivamente en el desempeño de las labores, en la Cooperativa no se practican revisiones de ese tipo. Como parte de esta investigación se realiza una evaluación del sistema y los accesos de cada colaborador, para funciones específicas y en el siguiente cuadro se muestra las marcas utilizadas consignadas en ellos:

Marcas	
N	No
S	Si
N/A	No aplica

Para la evaluación de accesos se consideran los siguientes módulos:

- Módulo de bancos
- Módulo de créditos
- Módulo de inventario
- Módulo de cuentas por pagar
- Módulo de propiedad, planta y equipo (PPE)
- Módulo de tecnología de información (TI)

Sobre el módulo de bancos se evalúa el acceso del personal involucrado y se obtienen los siguientes resultados:

Tabla N°1 Accesos al módulo de bancos

Personal de la Cooperativa	Módulo de Bancos Información					
	Ingresa	Modifica	Autoriza	Ejecuta	Consulta	Anular
Encargado de Bancos	N	S	S	S	S	N
Cajeros	N	N	N	S	S*	N
Contador	N	N	N	N	S	N
Asistentes de bancos	N	N	N	N	S	N
Auxiliar Supernúmerico	N	N	N	S	S	N

Gerente	N	N	S	N	S	S
Subgerente	N	N	S	N	S	N

Fuente: Elaboración propia

Para el caso de los cajeros, se evidencia que S* significa que los mismos colaboradores sólo tienen acceso a la información del detalle del pago que los asociados ofrezcan cancelar. Además, autorizan gestiones que son parte de las labores, por ejemplo, salidas de dinero. En la Cooperativa una persona asiste está designada para cubrir cuando falta algún cajero o cubre el tiempo de almuerzo, o en casos especiales donde se concedan permisos personales, (supernumerario), al cual se le asigna un usuario diferente al que utiliza normalmente para ejecutar sus funciones en otra área de la Cooperativa, por lo que existe un riesgo ya que un mismo empleado puede ingresar a distintos módulos y lograr obtener información que podría manipular para beneficio personal.

Respecto del módulo de crédito se evalúa el acceso del personal involucrado y se obtienen los siguientes resultados:

Tabla N°2 Accesos al módulo de créditos

Personal de la Cooperativa	Módulo de Crédito Información					
	Ingresa	Modifica	Autoriza	Ejecuta	Consulta	Anular
Encargado de Bancos	N	N	N	N	S	N
Cajeros	N	N	N	N	S	N
Contador	N	N	N	N	S	N
Plataformista,	S	S	S	S	S	N
Asistente de plataforma	N	S	S	S	S	N
Auxiliar Supernúmerico	N	N	N	S	S	N
Gerente	N	S	S	N	S	S
Subgerente	N	S	S	N	S	S

Fuente: Elaboración propia

En el caso del módulo de crédito, debido a que en la Cooperativa no se ha previsto la importancia de establecer seguridad lógica a los sistemas, se presenta en relación con este módulo los siguientes riesgos:

- Varias personas pueden modificar datos de los créditos de los asociados o clientes.
- En el sistema se presenta la opción de realizar abonos a las cuotas de forma parcial, lo cual hace que se alteren la tasa de interés por el no pago oportuno.
- Debido que el auxiliar supernumerario es de otra área diferente a la de Crédito, se genera mayor posibilidad de manipulación y alteración de datos.
- Debido a que el empleado de plataforma simultáneamente efectúa cobro de dinero, se incrementa la posibilidad de manipulación de datos y fraude, lo cual repercute en los Estados Financieros de la Cooperativa.

En relación con el módulo de inventario se evalúa el acceso del personal involucrado y se obtienen los siguientes resultados:

Tabla N°3 Accesos al módulo de inventario

Personal de la Cooperativa	Módulo de Inventario Información					
	Ingresa	Modifica	Autoriza	Ejecuta	Consulta	Anular
Encargado de Bancos	N/A	N/A	N/A	N/A	N/A	N/A
Cajeros	N	N	N	N	N	N
Contador	N	N	N	N	S	N
Asistentes de inventario	S	S	N	S	S	N
Auxiliar Supernúmerico	N	N	N	S	S	N
Gerente	N	N	S	N	S	S
Subgerente	N	N	N	N	S	S

Fuente: Elaboración propia

En relación con el módulo de inventario, existe una sola empleada encargada de realizar todo el proceso y no es supervisada. Igualmente cuando dicha empleada falta, la cubre el encargado del almacén el cual realiza las funciones con otro usuario y tampoco es supervisado. A parte del registro en el sistema, se implementan unas boletas donde los bodegueros deben firmar dando fe que la mercadería ha ingresado con las medidas de calidad necesarias para ser vendida; si bien, esto se considera como un control, la persona encargada del inventario no verifica físicamente las cantidades, dimensiones y características de la mercadería que recibe, finalmente ese control no es concluyente y podrían darse casos de un eventual fraude de cantidades ingresadas de más a inventario, debido a ello y con el consecuente perjuicio en los Estados Financieros.

En cuanto al módulo de cuentas por pagar, se evalúa el acceso del personal involucrado y se obtienen los siguientes resultados:

Tabla N°4 Accesos al módulo de cuentas por pagar

Personal de la Cooperativa	Módulo de Cuentas por Pagar Información					
	Ingresa	Modifica	Autoriza	Ejecuta	Consulta	Anular
Encargado de Bancos	N	N	N	N	S	N
Cajeros	N	N	N	N	N	N
Contador	N	N	N	N	S	N
Asistentes de pagos	S	S	S	S	S	N
Auxiliar Supernúmerico	N	N	N	N	S	N
Gerente	N	N	N	N	S	S
Subgerente	N	N	N	N	S	S

Fuente: Elaboración propia

El encargado de cuentas por pagar es el asistente de área quien, únicamente, es el que realiza esta función en la Cooperativa, pero no puede modificar datos de información de los proveedores de la Cooperativa, pero sí cuenta con accesos

para efectuar otros cambios que podrían alterar los saldos por pagar a proveedores, sin que se encuentren necesariamente justificados esos cambios con la consecuencia que ello implica en los Estados Financieros. Según el gerente de la Cooperativa, él supervisa las funciones del asistente de pagos, y el supervisor de área de cuentas por pagar manifiesta que cree que es el Gerente el que supervisa al asistente de pagos y que, a su vez, a veces directamente le da supervisión. No hay evidencia de dichas supervisiones y debido a que hay una aparente dualidad de mando en determinadas circunstancias ya sea el jefe de área o el Gerente pueden creer que el otro está dando la supervisión, sin que esto sea correcto, lo que puede ocasionar que el asistente de pagos pueda manipular la información en provecho propio o en favor de algún proveedor o funcionario.

En lo relativo al módulo de propiedad, planta y equipo se evalúa el acceso del personal involucrado y se obtienen los siguientes resultados:

Tabla N°5 Accesos al módulo de Propiedad, Planta y Equipo.

Personal de la Cooperativa	Módulo de PPE Información					
	Ingresa	Modifica	Autoriza	Ejecuta	Consulta	Anular
Encargado de PPE	S	S	N	N	N	S
Cajeros	N	N	N	N	N	N
Contador	N	N	N	N	S	N
Asistente de PPE	N	N	S	S	S	N
Auxiliar Supernúmerico	N	N	N	N	S	N
Gerente	N	N	S	N	S	S
Subgerente	N	N	N	N	S	N

Fuente: Elaboración propia

En el módulo de propiedad, planta y equipo, una vez realizada la orden de compra y aprobada, cuando ingresa el activo se revisa que cumpla con lo solicitado y se registra por el encargado de propiedad, planta y equipo. Luego el encargado del

pago debe realizarlo contra factura, verificando que lo que está en el sistema sea lo mismo que se adquirió. Por lo tanto, se considera que la Cooperativa presenta un control adecuado sobre este módulo.

En relación con el módulo de TI, se determina lo siguiente:

- Tal como se ha comentado la función de TI se realiza por medio de personal externo a la Cooperativa, lo que conlleva a los riesgos mencionados en el punto 4.2 Evaluación de resultados de esta investigación.
- Según manifiesta el personal de la Cooperativa, en caso de que los sistemas sufran alguna afectación, los expertos contratados ingresan de manera remota a dicho sistema para detectar la falla y subsanarla, con lo cual tienen acceso a la información de la cooperativa siempre.
- Además, no se preparan bitácoras de las labores realizadas y el tiempo de permanencia en el sistema por parte de los profesionales contratados, con lo cual la Cooperativa no está teniendo control de la información que maneja y no asegura a terceros (asociados, por ejemplo), la confidencialidad de la información que acerca de ellos maneja y tampoco puede asegurar que los datos no hayan sufrido manipulación por incursiones no autorizadas de esas personas al sistema.
- La Cooperativa carece de limitaciones para esas personas contratadas, de tal forma que se está exponiendo completamente la información interna que maneja ya que tienen acceso para ingresar, modificar, autorizar, ejecutar y

consultar ésta, lo cual genera un riesgo de que, por ejemplo, se pueda vender la base de datos de los clientes, lo cual puede ocasionar, entre otros, que estos se disgusten con la Cooperativa y que ésta pierda asociados con la afectación que conlleva en los Estados Financieros.

4.4 Información y comunicación

La comunicación oportuna de los resultados propicia la posible toma de decisiones y por ello, se identifica por medio de entrevistas y observaciones en la Cooperativa, el proceso de información y comunicación de las operaciones normales del negocio Los resultados recopilados se presentan en los siguientes cuadros:

Cuadro N°8 Utilización de información relevante-calidad para el Control Interno.

Aplicación del Principio N°13 Utilización de información relevante y de calidad para el Control Interno	**Cumple**	
	SI	**NO**
Identifica los requerimientos de información		X
Captura fuentes internas y externas de datos	X	
Transforma datos relevantes en información		X
Mantiene la calidad en todo el procesamiento	X	X
Considera la relación costo beneficio	X	

Fuente: Elaboración propia

Como se muestra en el cuadro anterior, la Cooperativa no presenta un proceso globalizado donde se pueda identificar la información requerida para soportar la funcionabilidad de los demás componentes que integran el control interno y sean acorde con la estrategia definida en la Cooperativa. Además, en el caso de la

percepción de información proveniente de fuentes externas de datos, la Cooperativa no cuenta con fuentes confiables de información, esto porque no destinan fondos para adquirirlas de entidades especializadas y sin alguna relación con el mismo personal de la entidad. Asimismo, existe un obstáculo en la transformación de datos en información relevante, esto porque existen personas encargadas del área de plataforma de servicios que pueden manipular esos datos, como incluir fechas de cobro distintas, cancelar montos parciales de cuotas de los asociados, lo cual altera los cobros de los intereses de la Cooperativa y la información financiera está afectada, lo que genera confusión y molestias en los asociados y no hay un control en dicha área para que mitigue el riesgo que surge. En cuanto a la calidad del procesamiento de la información, se perciben ciertas situaciones como las siguientes: la información que se procesa se encuentra de manera accesible, está protegida y no está restringida para ciertas áreas y puestos; tampoco se encuentra actualizada, lo que genera que pueda ser manipulada, no se pueda verificar y e influye de manera negativa en la toma de decisiones oportunas. Este riesgo se incrementa los fines de semana cuando se procesa información, porque no se encuentran los supervisores de área laborando, lo cual permite que se incremente la posibilidad de cometer algún fraude o manipulación de la información por parte de los colaboradores y posible hacker y no ser detectados a tiempo. Al carecer la Cooperativa del establecimiento de objetivos específicos para cada área y colaborador, hay una falencia en la relación de costo beneficio que debe existir para lograr que la naturaleza, cantidad y precisión del procesamiento de la información éste de acuerdo con los objetivos.

Cuadro N°9 Utilización de información relevante-calidad para el Control Interno.

Aplicación del Principio N°14	**Cumple**	
Se comunica internamente los objetivos y las responsabilidades de control interno.	**SI**	**NO**
Comunica la información de Control Interno.	X	X
Comunica entre la administración y el directorio	X	
Provee líneas de comunicación separadas.		X
Selecciona los métodos de comunicación relevantes		X

Fuente: Elaboración propia

Sobre la utilización relevante (de calidad) para fortalecer el control interno, la administración no comunica la información respecto de medidas tomadas para fortalecer éste de forma adecuada, lo que se puede evidenciar que no se cuenta con un proceso para comunicar la información requerida que permita a todo el personal comprender y ejecutar las responsabilidades de conformidad con el control interno, y tampoco se está perfeccionando como un proceso continuo el control interno para dar a conocer a los empleados oportunamente políticas, procedimientos, objetivos específicos, roles y responsabilidades; entre otros, además de las debilidades.

La comunicación directa entre la Gerencia y el Consejo de Administración no permite a ambos contar con la información necesaria para cumplir los roles en relación con el logro de los objetivos de la entidad, respecto de las responsabilidades que le son inherentes al control interno, o sea, la definición y mantenimiento.

Según el análisis de la información obtenida de las entrevistas, la Cooperativa no cumple con las características mínimas que debe tener la comunicación, por ejemplo: accesible, correcta, actualizada, protegida. Por tanto, no están establecidos roles, actividades, responsabilidades, las cuales podrían mitigar los peligros de comunicar las situaciones a destiempo.

Asimismo, los resultados de las entrevistas demuestran que en la Cooperativa no se brinda la comunicación oportuna, como, por ejemplo:

- No se comunica al personal nuevos controles acordados por la Gerencia y el Consejo de Administración.
- No existen contrataciones de evaluaciones externas, que permitan conocer nuevas visiones y recomendaciones de mejoras.

Lo anterior, implica a la Cooperativa un riesgo de realizar acciones que no van de acuerdo con el logro de los objetivos de la entidad.

4.5. Actividades de monitoreo

Se evidencia que no se lleva una supervisión en cada área de la Cooperativa, por ejemplo, a los consultores de TI cuando mantienen acceso remoto a los sistemas de la Cooperativa ni cuando permanecen en las instalaciones de ésta y accede a dichos sistemas, por lo cual no se tiene control de las opciones a las que puede consultar o la información que puede extraer o manipular, y que es propiedad de la cooperativa, además de la falta de supervisores en las jornadas de los fines de semana, incrementa el riesgo de fraude. Lo anterior, es muy peligroso, y conlleva riesgo de que la Cooperativa pierda información, podrían ser borrados datos de

préstamos o incluso préstamos completos, por obtener beneficio personal, sin que lo perciba la Cooperativa, lo que puede traer pérdidas a ésta, que afectan los resultados financieros.

En general, no existe un adecuado monitoreo de la realización de funciones y de las actividades de control para los procesos, y en relación con contrataciones del departamento de Tecnología de Información, que se encuentra por medio de outsourcing, existe gran riesgo para que se cometan acciones que perjudiquen a la Cooperativa, esto porque no existe un seguimiento por parte de los miembros de la administración que protejan a la información que mantiene la Entidad.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Para el estudio de la metodología COBIT 5 se analiza los principios, habilitadores, gobierno, gestión, términos que se comprendieron y que fueron factibles para aplicar a las Tecnologías de la Cooperativa. Al aplicar la metodología COBIT 5, se obtienen resultados que ayudaron a identificar dificultades, problemas, vulnerabilidades y debilidades en la Administración de las Tecnologías:

1. En la Cooperativa se carece de un ambiente de control que propicie la adherencia de políticas y procedimientos, ya que ni la Gerencia ni el Consejo de Administración han percibido la necesidad de formalizar controles para las distintas operaciones. Lo anterior, en relación con la tecnología de información, representa potencialmente un problema para la empresa, pues a pesar de que se subcontratan los servicios de soporte y mantenimiento de los sistemas, se encuentra a expensas del proveedor para ingresar irrestrictamente de manera remota a los sistemas y no se controlan siquiera los motivos ni las aplicaciones a las cuales tienen acceso éste.
2. En la Entidad tampoco se miden los diferentes riesgos que afronta la Cooperativa en el área de Tecnología de Información respecto de la seguridad física y lógica, en cuanto al acceso de particulares, por lo que no se toman las medidas que pueden evitar, por ejemplo, la pérdida o manipulación de información. Asimismo, la organización no se ha preocupado siquiera por la formalización de un organigrama para delimitar las principales líneas de la Entidad, por lo que no se ha medido el riesgo de

que los colaboradores actúen más allá de las funciones asignadas, o bien, dado que los servicios de soporte y mantenimiento de tecnología se subcontratan, el personal no tiene claro la amplitud de la relación, por lo tanto, no se establecen controles en relación con la ejecución de esos servicios.

3. La Cooperativa no da importancia a la profesionalización del recurso humano, por lo que no existe interés para captar al mejor empleado desde el momento de la contratación y tampoco se programan capacitaciones para el personal, además de que éste ejecuta las labores sin tener conocimiento formal de las funciones de los puestos, ya que se carece de un manual en ese sentido. También, no se ha dado importancia a fomentar la ética y los valores en el recurso humano, por lo que ni siquiera se les da a conocer el Código de Ética de la empresa.
4. En la evaluación de la información y comunicación, se logra establecer que la Entidad no efectúa la gestión oportuna de ésta, inclusive en algunos casos no se comunica a los colaboradores de situaciones relevantes, como por ejemplo, medidas de control en consecuencia de un fraude presentado, por lo cual, se presenta la posibilidad que se vuelva a dar la situación si no se toman medidas.
5. En relación con el monitoreo de las distintas áreas que realiza la Entidad, se deja en manos de los supervisores, por lo cual muchas veces no se realiza por la carga laboral de estos, que priorizan la parte operativa y dejan de lado la verificación.

6. La Cooperativa carece de actividades de control en relación con las políticas y procedimientos en las distintas áreas, y tampoco se encuentran presentes en el área de Tecnología de Información, donde no existen formalización de las funciones de los servicios subcontratados, medidas de control de riesgos inherentes a la contratación de servicios outsourcing, tampoco hay informes de resultados de los servicios prestados a la Entidad, en cuanto a la cantidad de personas involucradas, tiempo en el desempeño de las labores y aplicaciones a las que tienen acceso.

5.2 Recomendaciones

En relación con la investigación realizada en la Cooperativa de ahorro y crédito, se generan las siguientes recomendaciones:

Recomendaciones Generales

Al Consejo de Administración

- Girar instrucciones a la Gerencia para que instruya al personal de la entidad respecto del Código de Ética vigente y su aplicación para todas las labores que se llevan a cabo en la Cooperativa.
- Solicitar a la Gerencia la presentación de un plan de mejoras en relación con el método de contratación, que considere la necesidad de contar con colaboradores calificados y capacitados para desempeñar de forma eficiente y eficaz las labores de la cooperativa.

A la Gerencia:

- Preparar una actualización y revisión del Manual de Puestos de la Cooperativa, para verificar la incorporación de los nuevos procesos y responsabilidades de los distintos puestos, para presentarlo al Consejo de Administración, de tal manera que su aplicación se constituya en una obligación de los colaboradores.
- Actualizar el organigrama de la Entidad, para presentarlo a ratificación del Consejo de Administración, para hacerlo de conocimiento de todos los miembros de la Cooperativa, logrando así limitar las líneas de autoridades y responsabilidades en todas las áreas de la Entidad.
- Definir de manera formal el medio de comunicación formal en la entidad, sea cuadros de control o mails, entrenamiento personal o en línea, memorandos, discusiones personales, evaluaciones de rendimiento, presentaciones en video, webcast o Sitios webs, entre otros, para dar a conocer información relevante en las distintas áreas de la Entidad.
- Preparar un cronograma de actividades para la implementación de la propuesta que se anexa a esta investigación, que consigne todas las actividades necesarias, así como el presupuesto de la empresa, el requerimiento de recursos materiales y humanos necesarios para dicha implementación y presentarlo al Consejo de Administración para la correspondiente ratificación.

Recomendaciones que fortalecen la propuesta

Al Consejo de Administración

- Requerir a la Gerencia la presentación para estudio y aprobación un plan estratégico de Tecnología de Información, que conlleve una dirección tecnológica congruente con la dirección estratégica de la Cooperativa, para lograr una administración de la inversión en TI, que se requiere para ser más eficientes y eficaces en las operaciones normales de la Entidad.
- Realizar una evaluación de la ejecución de los servicios contratados a terceros en el área de tecnología, para lo cual se pueden analizar las siguientes opciones:
    - Solicitar la preparación de una evaluación periódica, por lo menos cada tres meses, por medio de la contratación de una empresa externa, para que presente un informe técnico de los resultados de la supervisión del área de TI. Esta debe ser una bitácora detallada de toda la información que se procesa.
    - Contratar un empleado en la Cooperativa, con estudios y experiencia que lo faculten para que realice una labor de supervisión continua de las labores subcontratadas en TI.

A la Gerencia:

- Diseñar un plan de continuidad de todos los procesos de la Cooperativa, el cual permita garantizar que los servicios que brinda la Entidad seguirán funcionando en casos de emergencia, generando así confianza y seguridad en los asociados actuales y los futuros, además, de permitir tener una mejor reacción ante los problemas que se vayan presentando en el camino.

- Integrar un comité de riesgos en la Cooperativa que realice, por ejemplo, las siguientes funciones:
    - Aprobar las políticas y la organización para la Gestión Integral de Riesgos, así como las modificaciones que se realicen a los mismos.
    - Definir el nivel de tolerancia y el grado de exposición al riesgo que la Cooperativa está dispuesta por asumir en el desarrollo de las actividades.
    - Decidir las acciones necesarias para la implementación de las acciones correctivas requeridas, en caso existan desviaciones con respecto de los niveles de tolerancia al riesgo y a los grados de exposición asumidos.
    - Evaluar la suficiencia de capital de la Cooperativa para enfrentar los riesgos y alertar de las posibles insuficiencias.
    - Proponer mejoras en la Gestión Integral de Riesgos
    - Revisar el contrato con la empresa externa e incorporar reglas básicas que permitan asegurar a la Cooperativa que se mantiene integridad y seguridad de la información confidencial y que el contrato sea revisado por un abogado.
    - Verificar que se incorpore en el contrato de mantenimiento del equipo (hardware), instrucciones para que la limpieza de dicho equipo, por ejemplo: memorias, fuentes de poder, ventiladores, entre otros, considere aspectos como: calidad de los materiales por utilizar,

capacitación para la correcta aplicación de esta; entre otros, y dar seguimiento al cumplimiento.

- Preparar un cronograma de actividades para implementar la propuesta sugerida en el capítulo 6 de esta investigación, que consigne todas las actividades necesarias e incorporar en el presupuesto de la empresa el requerimiento de recursos materiales y humanos necesarios para dicha implementación.

CAPÍTULO VI

PROPUESTA

6.1 Nombre de la propuesta

Manual de Políticas y Procedimientos de Seguridad Física y Lógica de la información, en la Cooperativa de ahorro y crédito.

6.2. Lugar de desarrollo, organización o población involucrada.

La propuesta se va a desarrollar en una Cooperativa de ahorro y crédito.

Factores críticos para el éxito de la propuesta

Se considera que para el éxito de la propuesta se requiere de los siguientes factores:

- Que en la Cooperativa de ahorro y crédito se ejecuten las recomendaciones que se orientan al fortalecimiento de esta propuesta.
- Que por parte del Consejo de Administración se efectúe una declaración explícita para aplicar un marco único integrado basado en COBIT 5.

6.3. Objetivo General y específicos

Objetivo de la Propuesta

- Implementar políticas y procedimientos para la seguridad física y lógica de los sistemas de información de la Cooperativa de ahorro y crédito, que le permita operar con eficacia y eficiencia.

Objetivos Específicos

- Establecer con base en el estudio efectuado en el capítulo IV de esta investigación, los fundamentos de la seguridad física y lógica que se requieren en la Cooperativa.
- Definir con base en las recomendaciones y la presente propuesta, la aplicación de nuevas políticas y procedimientos para la seguridad física y lógica.
- Incorporar los recursos requeridos para la implementación de la propuesta y calendarizar su implementación en un cronograma de actividades.

6.4. Cronograma de actividades y responsables.

Se incorpora una recomendación a la Gerencia.

6.5. Presupuesto necesario para su implementación.

Se incorpora una recomendación a la Gerencia.

6.6. Desarrollo de la propuesta.

Manual de Políticas y Procedimientos de Seguridad Física y Lógica de la información, en la Cooperativa de ahorro y crédito.

Aparte de Seguridad Física

AMBIENTE DE CONTROL

Premisa: Los asociados requieren que los empleados de la Cooperativa demuestren excelencia en la gestión en relación con la seguridad física de la información.

Objetivo:

Este aparte del Manual tiene como objetivo, estandarizar los requerimientos de políticas y procedimientos que deben respetarse para la seguridad física de TI, en la Cooperativa de ahorro y crédito.

Políticas:

1. Se designará un empleado encargado de la custodia de las llaves del cuarto de servidores.
2. El cuarto de servidores será protegido de accesos no autorizados y de otros factores, por ejemplo, los naturales, que podrían afectarlo y se respetarán las indicaciones del fabricante para el equipo y se usarán mecanismos de control.
3. Se realizará por lo menos una vez al año un conteo de inventario de equipo de cómputo y se revisará que dicho equipo no se encuentre deteriorado o no permita realizar las labores con eficiencia y eficacia.
4. Se implementará un sistema control de acceso por medio de huellas digitales para el ingreso de los colaboradores a las distintas dependencias de la Entidad.

5. Se prohíbe el consumo de alimentos y bebidas en el cuarto de servidores y en las áreas donde se ubican computadores y hardware en general en la empresa.
6. La Cooperativa mantendrá extintores de incendios que periódicamente serán probados y que cubran fuego generado por equipo eléctrico, papel o químicos especiales.
7. Se instalarán sensores de detección de humo e incendio en todos los centros de datos en la Cooperativa.
8. La Cooperativa protegerá los equipos de fallas de potencia u otras anomalías de tipo eléctrico, por medio de UPS (Sistemas de alimentación ininterrumpida).
9. Se revisará por lo menos una vez al año el estado del cableado de la red.

Procedimientos:

a. La Gerencia designará el responsable de la custodia de las llaves del cuarto de servidores considerando las siguientes categorías:

   i) Operadores y usuarios que trabajan regularmente en el área.

   ii) Personal de soporte que requiera acceso periódico.

   iii) Otros, que requieran acceder muy rara vez.

   Sólo la Gerencia mantendrá bajo llave otro juego de llaves de acceso al cuarto de servidores.

b. Cualquiera de los empleados con autorización para ingresar al cuarto de servidores que requieran ingresar a él deben reportarlo al funcionario que custodia las llaves.

c. En caso de pérdidas de llaves del cuarto de servidores, de inmediato se debe comunicar a la Gerencia y proceder a un protocolo de cambio de llavines.

d. El funcionario encargado del cuarto de servidores debe llevar una bitácora en un formulario detallando los motivos por los que ingresa, la fecha y la debida autorización de la Gerencia, firmar a la entrada y salida.

Logo	Formulario N°1 de ingreso a TI
	
Fecha:	Hora de entrada: Hora de salida:
Motivo por el que ingresa:	
Firma de autorización del gerente: _____	
Firma del colaborador:_____	

Fuente: Elaboración propia Serie: 001

e. El Departamento de Contabilidad con la colaboración del personal de TI, realizará periódicamente, por lo menos una vez al año, un inventario de equipos de la Cooperativa y se revisará si dicho equipo:

   1. No se encuentra deteriorado
   2. Requiere actualizaciones de hardware para mejorar su funcionamiento.

f. Mediante un comunicado formal, la Gerencia designará a los colaboradores que participarán de la realización de dicho inventario.

g. La Gerencia emitirá instrucciones formales por escrito a los colaboradores, respecto del inventario que se realizará, orden y documentos a llenar durante él, la fecha y su hora de la ejecución.

h. Se emitirá un listado de equipo de TI, con base en el registro de la contabilidad y según en ese listado se verificará la existencia y características del equipo que garantizan la continuidad de funcionamiento del hardware.

i. Se revisará el funcionamiento de las UPS de la Cooperativa.

j. Se detectará si existen diferencias en el inventario de equipo, se efectuarán las indagaciones acerca de esas diferencias y se solicitará explicaciones al encargado del inventario y la Gerencia debe autorizar que se realicen los ajustes correspondientes en la Contabilidad.

Logo **Formulario N°2 de Inventario de Equipos de la Cooperativa**

Fecha de inventario:

Ubicación	Código del activo	Nombre	Cantidad contada	Reconteo	Ajustes	Firma de Autorización de la gerencia

Firma del colaborador:_____
Firma del encargado del conteo: _____

Fuente: Elaboración propia Serie: 001

k. Todo personal que ingrese a alguna dependencia de la Cooperativa de acceso restringido requerirá poner su huella digital.

l. La Gerencia efectuará un estudio para identificar el personal que puede ingresar a determinadas áreas de la Cooperativa, por ejemplo, el cuarto de servidores y mantendrá una bitácora actualizada de las autorizaciones emitidas.

Logo **Formulario N°3 Estudio de accesos a la Cooperativa**

Fecha de estudio:

Nombre del Colaborador	Puesto del Colaborador	Razón por la que requiere ingresar al área restringuida	Acceso registrado por área	Área a la que ingresa	Observaciones	Puede ingresar	
						SI	NO

Firma de la subgerencia:_____
Firma de la gerencia: _____

Fuente: Elaboración propia Serie: 001

m. La Gerencia emitirá mensualmente con base en un reporte de los accesos a las diferentes áreas de la empresa, analizará la necesidad de que el personal requiera mantener de manera indefinida la autorización, y tomará las decisiones correspondientes, otorgando o cesando los accesos, según corresponda.

Logo	Formulario N°4 Reporte de accesos a las áreas restringidas		
Fecha de emisión:			
Nombre del Colaborador	Área a la que puede ingresar	Firma de Aprobación de la gerencia	Observaciones
Firma de la subgerencia:_____ Firma de la gerencia: _____			

Fuente: Elaboración propia Serie: 001

n. Cada tres meses la Subgerencia emitirá un comunicado vía correo electrónico a todo el personal, reiterando la prohibición de ingerir alimentos en el área de servidores y consignando que las jefaturas son responsables por velar el cumplimiento de esta disposición.
o. La Subgerencia solicitará la colaboración del Cuerpo de Bomberos de la localidad para organizar un simulacro, de forma periódica y se aprovechará la oportunidad para la revisión de los extintores y los sensores.
p. Se supervisará que la empresa contratada para el soporte y mantenimiento del sistema realice cada año la revisión completa del cableado, emitiendo un informe con los detalles de los resultados para la Gerencia.

EVALUACIÓN DE RIESGO

Premisa: Los asociados y la Cooperativa se encuentran interesados en que la gestión de riesgos en la entidad garantice la seguridad física de la información.

Objetivo: Identificar los principales riesgos a los que la Cooperativa se expone en cuanto a seguridad física.

Políticas:

1. Se realizará una actualización semestral de riesgos respecto de la seguridad física de la Cooperativa.

Procedimientos:

a. Se identificará por área las actividades que se realizan en la Entidad y de riesgos de seguridad física de la información.
b. Se definirá para cada una de las actividades determinadas, los principales riesgos que puede afrontar, calificándolos como bajo, medio, alto y crítico en relación con la seguridad física la información, para efecto de lo anterior, se aplica el siguiente instrumento de preguntas:

Logo 	Formulario N°4.1 Identificación de riesgos de seguridad física					
	Calificación		Ponderación			
Preguntas	SI	NO	CRÍTICO	ALTO	MEDIO	BAJO
¿Afronta esta actividad riesgos? Califique el riesgo afrontado.						
¿Existe una definición de riesgo de seguridad física?						
¿Está es comunicada y conocida?						
¿Hay una visión y lenguaje integrado de riesgos de seguridad física en todas las unidades de negocio de la organización? Califique.						
¿Se identifican, evalúan, comunican y monitorean los riesgos de seguridad física? Califique.						
¿Se asegura que el proceso de gestión de riesgo se efectúe correctamente? Califique.						
¿Los colaboradores entienden su rol como parte de la administración de riesgos? Califique.						

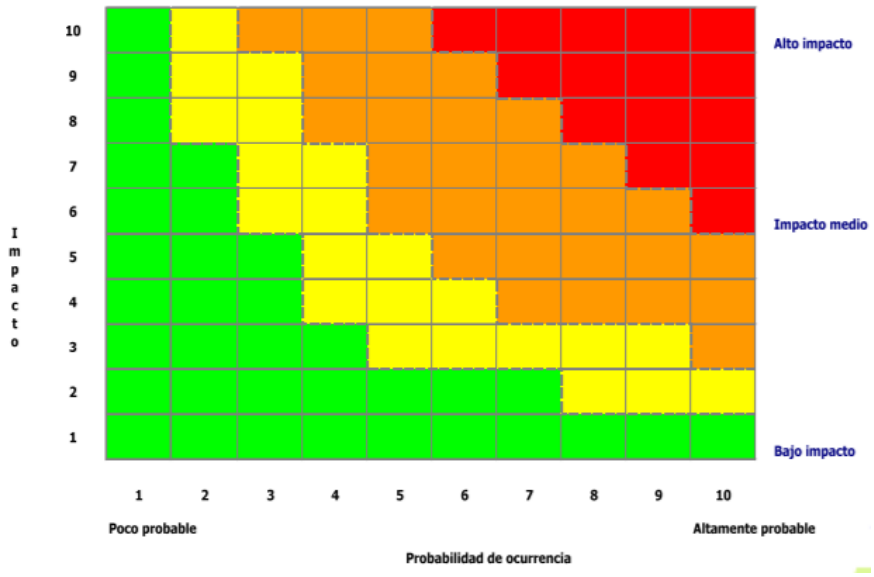
Fecha y Firma de la gerencia: _____ Serie: 001

Fuente: Elaboración propia

c. Mediante un mapa de riesgos, se identificará de manera integrada, una calificación de riesgo para las áreas las actividades con riesgos bajo, medio, alto y crítico, en relación con la seguridad física de la información. A continuación, se detalle un modelo de la matriz de riesgos:

Descripción de los cuadrantes de la matriz de riesgos:

Mapa de Riesgos



Calificación del riesgo:

Nivel de Riesgo	Calificación	Nivel de Riesgo	Calificación
Riesgo Bajo	1-15	RiesgoAlto	30-59
Riesgo Medio	16-29	Riesgo Crítico	> 60

d. Se preparará por parte de la Subgerencia un reporte de la matriz de riesgos de seguridad física y en él se detallarán las posibles medidas de prevención y corrección de los riesgos encontrados.

Logo	Formulario N°5 Reporte Matriz de Riesgos Seguridad Física						
Fecha:		**Calificación de Riesgo**				Descripción	
Área A	Hallazgos	Bajo	Medio	Alto	Crítico	Probabilidad	Impacto
a (*)		X					
b.			X				
Área B							
c.				X			
d (*)				X			
Área C							
e (*)					X		
f.		X					
Firma y fecha de aplicación: Firma del Gerente:							

Fuente: Elaboración propia Serie: 001

a* *Por ejemplo corresponde al área de plataforma de servicios, existe un riesgo Bajo, en el caso del área de tesorería al ser restringido el acceso sería* ***e**** *con un riesgo Crítico. En el caso del cuarto de servidores se ubicaría en el área* ***d**** *con un riesgo Alto y así sucesivamente se va calificando el riesgo para cada actividad.*

e. Luego de determinar los riesgos de seguridad física que presenta la Cooperativa, se determina cuál va a ser la respuesta; y a continuación, se muestran algunas posibles:

TABLA IDENTIFICACION RESPUESTAS	
EVADIR	**E**
COMPARTIR	**C**
REDUCIR	**R**
ACEPTAR	**A**

Logo	Formulario N°5.1 Respuesta al Riesgo		
Fecha:		**Evaluación Posible Respuesta**	
Área A	Calificación	Costo vs Beneficio	Respuesta al Riesgo
a (*)			
b.			
Área B			
c.			
d (*)			
Área C			
e (*)			
f.			
Firma y fecha de aplicación: Firma del Gerente:			

Fuente: Elaboración propia Serie: 001

f) Se debe presentar al consejo de administración los resultados de evaluación de riesgos efectuada, para la aprobación y la dotación de recursos requeridos.

ACTIVIDADES DE CONTROL

Premisa: Los asociados y la Cooperativa se encuentran interesados en que las actividades de control respecto de la seguridad física de las instalaciones de TI garanticen la seguridad de la información que se mantienen en el hardware.

Objetivo:

Establecer medidas de control de las actividades de la Cooperativa para la seguridad física de la información.

Políticas:

1. Se mantendrá actualizado el registro de los nuevos equipos para TI adquiridos.
2. Anualmente se revisarán las coberturas de los seguros de los equipos de la Cooperativa.
3. Se definirá la información que a juicio de la Cooperativa es altamente confidencial y será enviada a la impresora de la red, si no hay un empleado que, habiendo sido autorizado de previo, la vigile antes y después de efectuar la correspondiente impresión. Esta situación es aplicable también a los casos en que se requiera la reimpresión de documentos que pueden considerarse como confidenciales, por ejemplo: pagarés o letras de cambio, donde figure toda la información de un asociado.
4. Se prohíbe la adquisición de equipos con puertos de acceso a dispositivos electrónicos como llave maya o unidades de CD/DVD.
5. De conformidad con la normativa técnica, los cables de energía eléctrica y de comunicaciones deben estar separados.
6. Se hará uso por ejemplo de canaletas para proteger de daño o intercepción el cableado de la red.
7. Se realizarán mantenimientos preventivos sobre los equipos considerando su uso y las recomendaciones del fabricante, de conformidad con un cronograma de trabajo, únicamente por parte de personal autorizado, y en caso de que se requiera enviar el equipo fuera de las instalaciones, se considerará si dicho equipo tiene información confidencial previo a ello, tomando las disposiciones que amerite para la salvaguarda de esa información.

8. Los empleados en la relación con los asociados y proveedores sólo podrán usar el correo personal que se les asigne.
9. Se prohíbe el acceso a correos personales de los empleados desde las computadoras de la Cooperativa.
10. Se prohíbe a los empleados hacer uso de las computadoras de la Entidad para visitar las redes sociales.

Procedimientos:

1. La Gerencia designará a un encargado para que lleve el control del equipo de la Cooperativa en un formulario, donde se incluya, por ejemplo, un registro de: fecha de mantenimiento, fecha estimada de próxima revisión, si el equipo está en mantenimiento, un registro de las fallas que presenta y las soluciones que se le ha realizado. Con esto que permita anticiparse y realizar los cambios de manera oportuna para obtener seguridad de un negocio en marcha.

Logo **Formulario N°6 Control del Equipo de la Cooperativa**

Código	Ubicación	Nombre de activo	Fecha de última revisión	Deficiencias encontradas	Fecha estimada de próxima revisión	Recomendaciones	Firma del colaborador

Fuente: Elaboración propia Serie: 001

2. Se levantará un listado del equipo, se dividirá el equipo en un cronograma de trabajo de revisión del equipo, el cual la Gerencia designará a una persona que se encargue de realizar el proceso de revisión.

Logo	Formulario N°7 Cronograma de Trabajo de Revisión de Equipo			
Nombre del activo	I Trimestre	II Trimestre	III Trimestre	Firma y fecha de aplicación
a	X			
b	X			
c		X		
d			X	
e			X	
Firma y fecha de revisión:_____				

Fuente: Elaboración propia Serie: 001

3. Se mantendrá un control de las fallas presentadas en el sistema, en un formulario donde se resuma los principales fallos que presentan los equipos, y que se den a conocer al personal, proponiendo así implementar técnicas que propicien la disminución de dichas fallas.

Logo **Formulario N°8 Control de fallas presentadas**

Código del activo: _____
Descripcion de falla presentada: _____
_____
Fecha en que se dio la falla: _____
Persona que reporto la falla: _____
Duración en corrección de la falla: _____
Personal que participo en la corrección y cargo:_____
_____
Firma del responsable_____

Fuente: Elaboración propia Serie: 001

4. El encargado del mantenimiento preventivo mensualmente preparará y enviará a la Subgerencia un informe resumido de las sugerencias de cambio y adecuaciones que requieren los equipos de la Cooperativa.

Logo **Formulario N°9 Reporte a la Subgerencia de fallas**

Nombre del activo	Fallas presentada	Corrección aplicada	Firma de Aprobación
a			
b			
c			
d			
e			

Firma y fecha de reporte:_____

Fuente: Elaboración propia Serie: 001

5. Después de realizar el control de la revisión del equipo de la Cooperativa, la Subgerencia evaluará el realizar mantenimientos preventivos de los equipos, con los especialistas necesarios, esto para la prevención de fallas

futuras ejecutando un mantenimiento y manipulación adecuados, ahorrando así recursos de reparación más costosos para la Cooperativa.

6. Se adquirirá un seguro contra incendios y temblores, que permita la protección de los activos e información de la Cooperativa, para su seguridad y de los asociados.
7. Los colaboradores no podrán ingresar con los dispositivos móviles a la red de la Entidad, únicamente pueden utilizar el correo asignado por la Cooperativa. Ni utilizar llaves maya o CD para uso personal.
8. Se mantendrá una impresora en la oficina de la Gerencia, únicamente para impresiones confidenciales bajo vigilancia de la Gerencia.
9. Los empleados en sus relaciones con los asociados y proveedores sólo podrán usar el correo personal que se les asigne.
10. La proveeduría no comprará equipo con puertos de acceso a dispositivos CD/DVD y llaves maya.
11. Periódicamente, se dará mantenimiento a las instalaciones de las comunicaciones y tratando de proteger de cualquier daño cumpliendo la normativa aplicable.

INFORMACIÓN Y COMUNICACIÓN

Premisa: Los asociados y la Cooperativa se encuentran interesados en que se establezcan controles que garanticen el resguardo de la información de la seguridad de la seguridad física de las instalaciones y equipo de TI.

Objetivo:

Mantener una comunicación efectiva en toda la compañía, permitiendo ser oportunos en las decisiones a emplear.

Políticas:

1. Se diseñará un cronograma para efectuar evaluaciones de resultados de forma trimestral.

Procedimientos:

1. Se efectuará una planificación de fechas de las reuniones de resultados de la evaluación de la Cooperativa, y se definirá una estructura de forma estándar para presentar dichos resultados; así como los asistentes, los miembros del consejo administrativo, comité de vigilancia, entre otros. Se informará al personal de los cambios en políticas, procedimientos, implementación de nuevas actividades o procesos, cambios en estructuras del personal y responsabilidades, implementación de nuevos controles, entre otros.

Logo	Formulario N°10 Cronograma de revisión de resultados		
	I Trimestre	II Trimestre	III Trimestre
	Fecha	Fecha	Fecha
	Hora	Hora	Hora
Reunión de la Gerencia con el Consejo de Administración			
Temas a tratar			
Recomendaciones			
Observaciones			

Fuente: Elaboración propia Serie: 001

2. Se efectuará una reunión con el personal de manera posterior a cada una de las reuniones de revisión de resultados, para informar sobre los cambios política y procedimientos que deban implementarse.

Logo	Formulario N°11 Cronograma de revisión de resultados		
	I Trimestre	II Trimestre	III Trimestre
	Fecha	Fecha	Fecha
	Hora	Hora	Hora
Reunión de la Gerencia con el personal			
Temas comunicados			
Nuevos procedimientos			
Nuevas politicas			

Fuente: Elaboración propia Serie: 001

MONITOREO

Premisa: Los asociados y la Cooperativa se encuentran interesados en que exista un adecuado monitoreo en relación con la seguridad física de la Cooperativa.

Objetivo:

Gestionar un monitoreo eficiente y eficaz en relación con la seguridad física de la información de la Cooperativa.

Políticas:

1. Realizar una evaluación anual de Control Interno de seguridad física de la información.

Procedimientos:

a. La Gerencia programará una fecha para realizar la evaluación de CI respecto de la seguridad física y determinará los participantes en el evento.
b. Se evaluará en la reunión que se efectúe, todas las áreas de la Entidad en cuanto a seguridad física de la información que mantienen, y se analizarán los resultados para tomar medidas al respecto.

Logo	Formulario N°12 Evaluación Anual del CI de seguridad física		
Área a evaluar: _____	Atributos		
Políticas a cumplir (*)	A	B	C
a.			
b.			
c.			
d.			
e.			

Observaciones y Recomendaciones: _____
_____

Marcas
Atributos: Caracteristicas a evaluar por cada área.
A: Se completan correctamente todos los fórmularios de seguridad física
B: Las firmas tanto de preparado como revisado están acorde al periodo y puesto de trabajo
C: Las fechas de los formularios están dentro del periodo correspondiente
S: Cumple
N: No cumple

Firma y fecha de aplicación:_____

Fuente: Elaboración propia Serie: 001

Para efectos del ejemplo *(*)* ver políticas de ambiente de control 2, 3 y 4; en actividades de control ver políticas 1, 2, 4, 9 y 10.

Aparte de Seguridad Lógica

AMBIENTE DE CONTROL

Premisa: Los asociados requieren a los empleados de la Cooperativa que demuestren excelencia en su gestión en relación con la seguridad lógica de la información.

Objetivo: Crear en la Cooperativa un ambiente de seguridad del software en cuando a la información de los asociados.

Políticas:

1. Se prohíbe al personal de la Cooperativa el compartir contraseñas personales para ingreso a aplicaciones que les ha sido otorgados.
2. Realizar un adecuado seguimiento del uso del software especialmente del personal externo a la compañía.
3. Se implementará un sistema control de acceso por medio de huellas digitales para el ingreso de los colaboradores a las distintas áreas de la entidad.
4. En caso de necesitar sacar el equipo de la Cooperativa para realizar alguna actualización o reparación, se realizará bajo supervisión y resguardo de la información de la Cooperativa.
5. Realizar una limpieza del sistema, esto para evitar que el procesamiento se vuelva lento al realizar las operaciones normales del negocio.
6. Las contraseñas de acceso a las aplicaciones se cambiarán cada 30 días en la Cooperativa, y cada contraseña debe contener números y letras

alfanuméricos, con mayúsculas y minúsculas, con cierta cantidad de caracteres.

7. Se solicitará a la empresa que da el mantenimiento y soporte del software un informe mensual de los requerimientos del mantenimiento y soluciones realizadas, el cual debe entregarse a la Gerencia.
8. Se le informará a la Gerencia el informe de fallas y correcciones realizadas a los sistemas de la Cooperativa.

Procedimientos:

a) Mediante un comunicado oficial de la Gerencia indicará a los colaboradores la prohibición de compartir claves de usuarios o contraseñas, y las medidas sancionatorias de presentarse dicho caso.

b) Se deberá facilitar una programación que obligue al personal realizar el cambio de contraseñas cada 30 días, de tal manera que el sistema no pueda utilizarse si no se realiza la actualización.

c) Se solicitará al personal contratado la solución de problemas de sistema por medio de un requerimiento formal, que será firmado por el empleado correspondiente y autorizado por la Subgerencia**.**

Logo	Formulario N°13 Solicitud interna de solución de problemas del sistema		
Nombre de la aplicación	Fallas presentada	Fecha presentada	Firma del empleado
a			
b			
c			
d			
e			
Firma y fecha de la SubGerencia:_____			

Fuente: Elaboración propia Serie: 001

d) La Gerencia enviará un formulario físico o escaneado por medio de correo electrónico, de requerimiento externo a la empresa contratada con indicación expresa del problema que debe solucionarse. A continuación, se muestra el formulario de solicitud de atención de falla y el de la solución aplicada por la empresa externa.

Logo	Formulario N°14 Solicitud de atención de falla			
Nombre de la aplicación	Fallas presentada	Tiempo estimado	Módulo de aplicación y subaplicación	Observaciones
a				
b				
c				
d				
e				
Firma y fecha de reporte:_____				

Fuente: Elaboración propia Serie: 001

Logo	Formulario N°14.1 Solicitud externa de solución de problemas del sistema				
Nombre de la aplicación	Tiempo Invertido	Solución Aplicada y a qué Módulos	Fecha en que se solucionó	Fue presencial o virtual	Observaciones
a					
b					
c					
d					
e					
Firma y fecha de reporte:_____					

Fuente: Elaboración propia Serie: 001

e) La Subgerencia informará a la Gerencia trimestralmente, para que informe al Consejo de Administración, acerca de los problemas presentados en relación con el sistema. La Subgerencia debe establecer el costo invertido en las reparaciones incurridas en el sistema y recomendaciones de mejores prácticas en la utilización del sistema.

Logo	Formulario N°15 Reporte a la Gerencia del sistema			
Nombre de la aplicación	Falla presentada	Solución Aplicada	Costo Invertido	Recomendaciones
a				
b				
c				
d				
e				
Firma y fecha del reporte:_____				

Fuente: Elaboración propia Serie: 001

f) Se solicitará a la empresa subcontratada un informe mensual de fallas detectadas y solucionadas en el sistema, que se corroborará contra las solicitudes de atención de problemas, para efectos de determinar la cabalidad de lo cobrado.

Logo	Formulario N°15.1 Reporte Externo de fallas			
Nombre de la aplicación	Falla detectada	Solución Aplicada	Revisión de la Gerencia en concordancia	Firma y fecha de revisión
a				
b				
c				
d				
e				
Firma y fecha de la gerencia:_____				

Fuente: Elaboración propia Serie: 001

g) Se efectuará un seguimiento del equipo, para detectar el que requiera ser retirado de las instalaciones de la Cooperativa, (por ejemplo para mantenimiento o reparación externa) y tener así un control para que la información de la Cooperativa continúe siendo confidencial y se proteja también la base de datos de los asociados.

Logo	Formulario N°16 Salida externa del equipo			
Nombre de la aplicación	Fecha de salida	Fecha estimada de regreso	Razón por la que debe salir el activo de la institución	Encargado responsable de la supervisión
a				
b				
c				
d				
e				
Firma y fecha de la gerencia:_____				

Fuente: Elaboración propia Serie: 001

EVALUACIÓN DE RIESGO

Premisa: Los asociados y la Cooperativa se encuentran interesados en que la gestión de riesgos en la Entidad garantice la seguridad lógica de la información.

Objetivo: Identificar los principales riesgos en los que la Cooperativa se expone en cuanto a seguridad lógica.

Políticas:

1. Se realizará una actualización semestral de riesgos respecto de la seguridad lógica de la Cooperativa.

Procedimientos:

a. Se identificará por área las actividades que se realizan de riesgos de seguridad lógica de la Cooperativa.
b. Se definirá para cada una de las actividades los principales riesgos que puede afrontar, calificándolos como bajo, medio, alto y crítico, en relación con la seguridad lógica de la información, para efecto de lo anterior, se aplica el siguiente instrumento de preguntas:

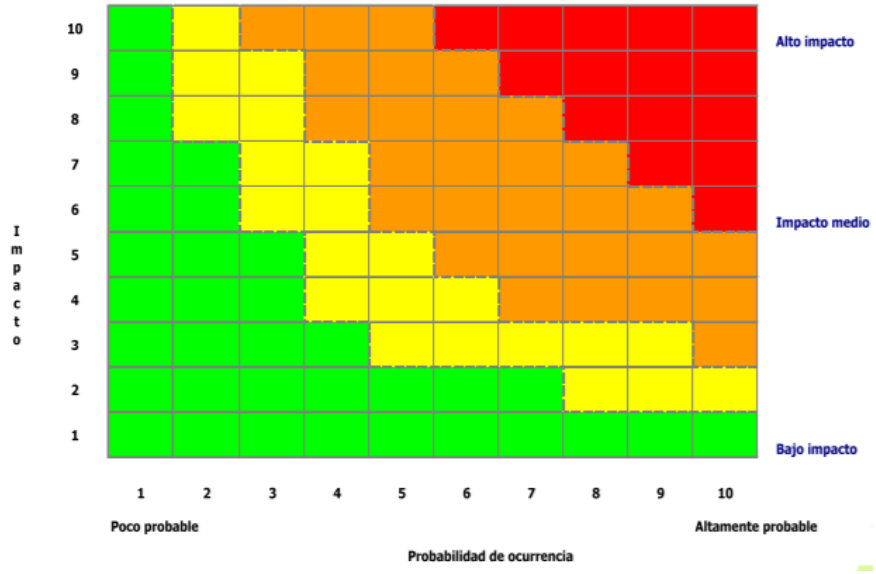
Logo	Formulario N°16.1 Identificación de riesgos de seguridad lógica					
	Calificación		Ponderación			
Preguntas	SI	NO	BAJO	MEDIO	ALTO	CRÍTICO
¿Afronta esta actividad riesgos? Califique el riesgo afrontado.						
¿Existe una definición de riesgo de seguridad lógica?						
¿Está es comunicada y conocida?						
¿Hay una visión y lenguaje integrado de riesgos de seguridad lógica en todas las unidades de negocio de la organización? Califique.						
¿Se identifican, evalúan, comunican y monitorean los riesgos de seguridad lógica? Califique.						
¿Se asegura que el proceso de gestión de riesgo se efectúe correctamente? Califique.						
¿Los colaboradores entienden su rol como parte de la administración de riesgos? Califique.						

Fecha y Firma de la gerencia: _____ Serie: 001
Fuente: Elaboración propia

c. Mediante el mapa de riesgos, identificar por áreas las actividades con riesgos bajo, medio, alto y críticas, en relación con la seguridad lógica. A continuación se detalle un modelo de la matriz de riesgos:

Descripción de los cuadrantes de la matriz de riesgos:

Mapa de Riesgos



Calificación del riesgo:

Nivel de Riesgo	Calificación	Nivel de Riesgo	Calificación
Riesgo Bajo	1-15	RiesgoAlto	30-59
Riesgo Medio	16-29	Riesgo Crítico	> 60

d. Se preparará por parte de la Subgerencia un reporte de la matriz de riesgos de seguridad lógica y en él se detallarán las posibles medidas de prevención y corrección de los riesgos encontrados.

Logo	Formulario N°17 Reporte Matriz de Riesgos Seguridad Lógica						
Fecha:		**Calificación de Riesgo**				Descripción	
Área A	Hallazgos	Bajo	Medio	Alto	Crítico	Probabilidad	Impacto
a (*)		X					
b.			X				
Área B							
c.				X			
d (*)				X			
Área C							
e (*)					X		
f.		X					
Firma y fecha de aplicación: Firma del Gerente:							

Fuente: Elaboración propia Serie: 001

a* corresponde al módulo de bancos, existe un riesgo Bajo, el módulo de cobro de asociados tiene un riesgo Crítico por lo que se ubicaría en ***e****. En el caso del módulo de pago a proveedores sería en el área ***d**** con un riesgo Alto. Y así sucesivamente se va calificando el riesgo para cada actividad.

e. Luego de determinar los riesgos de seguridad lógica que presenta la Cooperativa, se determina cuál va a ser la respuesta; a continuación, se muestran las posibles respuestas:

TABLA IDENTIFICACIÓN RESPUESTAS	
EVADIR	**E**
COMPARTIR	**C**
REDUCIR	**R**
ACEPTAR	**A**

Logo	Formulario N°17.1 Respuesta al Riesgo		
Fecha:		**Evaluación Posible Respuesta**	
Área A	Calificación	Costo vs Beneficio	Respuesta al Riesgo
a (*)			
b.			
Área B			
c.			
d (*)			
Área C			
e (*)			
f.			
Firma y fecha de aplicación: Firma del Gerente:			

Fuente: Elaboración propia Serie: 001

f. Se debe presentar al Consejo de Administración los resultados de evaluación de riesgos efectuada, para la aprobación y la dotación de recursos requeridos.

ACTIVIDADES DE CONTROL

Premisa: Los asociados se encuentran interesados en que la seguridad lógica de TI garantice la seguridad de la información, respecto de las actividades de control efectuadas.

Objetivo: Garantizar que se realicen las acciones necesarias para la seguridad lógica de la información que se procesa en la Cooperativa.

Política:

1. Se realizarán indagaciones de manera trimestrales acerca de las tendencias tecnológicas en el mercado, que permitan implementar mejoras en la seguridad lógica del sistema.
2. Se programará en el sistema un bloqueo de las páginas de Internet que no sean útiles para trabajar, dejando sólo la red de la empresa disponible.
3. Periódicamente se revisarán los accesos a las aplicaciones.
4. Realizar un back up con una frecuencia acorde con la operatividad del negocio, lo cual permita garantizar la seguridad de la información de los usuarios y de la Cooperativa.
5. Se deben revisar el funcionamiento del back up, para ver que esté bien.
6. Se garantizará que no se van a realizar las pruebas en el servidor, para no alterar datos financieros.

Procedimientos:

a) Implementar capacitaciones al personal de las tendencias, por ejemplo, de jaqueo en los sistemas, para que se efectúe la actualización conforme a cambios del entorno y en respuesta a los riesgos.

Logo	Formulario N°18 Bitácora de capacitaciones		
Miembros que participaron	Área en que labora	Temas tratados	Temas expuestos para la próxima sesión
a			
b			
c			
d			
e			
Firma y fecha de aplicación:_____			

Fuente: Elaboración propia Serie: 001

b) Diseñar un plan de actualización de programas como el antivirus, protección de datos, entre otros, para disminuir el riesgo de duplicación y/ pérdida de la base de datos o información.

Logo	Formulario N°19 Plan de actualización de programas			
Programas	Fecha de compra	Fecha de actualización	Versión adquirida	Firma de la gerencia
a.				
b.				
c.				
d.				
e.				
Observaciones y Recomendaciones: _____				
Firma y fecha de aplicación:_____				

Fuente: Elaboración propia Serie: 001

c) Cualquier prueba de cambios al sistema no podrá efectuarse de forma directa en el servidor de la empresa.

a) Se designará a un colaborador para que realice un back up del sistema con una frecuencia acorde con la operatividad del negocio, lo cual permita garantizar la seguridad de la información de los usuarios y de la Cooperativa. El respectivo respaldo quedará en la caja de seguridad de un banco. A continuación, se muestra el formulario de realización del Back Up y también la bitácora de respaldos del sistema, para controlar las fechas de ejecución.

Logo **Formulario N°20 Back up del sistema**

Programas	Quién lo realizará	Cada cuánto lo realizará	¿Cómo lo va a hacer?	Respaldo en CD	Encargado de revisión del respaldo	Cada cuánto lo revisará
a.						
b.						
c.						
d.						
e.						

Firma y fecha de la gerencia:_____

Fuente: Elaboración propia Serie: 001

Logo **Formulario N°20.1 Bitácora de respaldos del sistema**

Persona que realizó el respaldo	Fecha en que se realizó el respaldo	Programa al que se le aplicó el respaldo	Firma de revisión de la Gerencia

Firma y fecha de reporte:_____

Fuente: Elaboración propia Serie: 001

b) Implementar un formulario que detalle qué actividades están realizando las personas externas a la Cooperativa, en la solución de problemas del sistema, donde se indique el tiempo que se invirtió, en qué, cuál fue la solución que implementaron, quiénes fueron los involucrados incluyendo al personal de la Cooperativa, a qué módulos tuvieron acceso, y cualquier otro detalle que se considere necesario aclarar.

Logo	**Formulario N°21 Control de Ingreso al Sistema del personal Externo**

Razón por lo que se requiere que ingrese:

Firma de autorización del Gerente: _____

Fecha y duración en el sistema:
Actividades que realizó:

Informe detallado de los cambios ejecutados:

Firmas del personal y puesto de las personas involucradas:_____
_____

Firma del encargado de supervisar TI:_____

Fuente: Elaboración propia Serie: 001

c) Se le asignará a cada colaborador de la Cooperativa, una descripción de los accesos a las aplicaciones, donde se logre detallar para la Gerencia quién tiene acceso, por ejemplo: ejecutar, consultar, revisar.

Logo	Formulario N°22 Control de accesos al sistema del personal					
			Descripción del acceso			
Empleado	Aplicación	Ejecutar	Modificar	Revisar	Aprobar	Anular

Firma y fecha de la gerencia:_____

Fuente: Elaboración propia Serie: 001

INFORMACIÓN Y COMUNICACIÓN

Premisa: Los asociados y la Cooperativa se encuentran interesados en que se establezcan controles que garanticen información acerca del funcionamiento de la seguridad lógica del sistema.

Objetivo: Establecer medidas para la protección de la información mediante la seguridad lógica del sistema y la comunicación oportuna de resultados.

Políticas:

1. Se validará que se estén generando los reportes del sistema.
2. Se inspeccionará que se den accesos a reportes e impresión de reportes esté restringido.
3. Cualquier cambio en las tablas de la aplicación, debe ser pre autorizado por la Gerencia, indicando cuáles aplicaciones fueron afectadas.

Procedimientos:

a. Se preparará por parte del encargado de supervisión del área de TI internos, un reporte de los cambios en el sistema, y comunicarlo a los usuarios directos del proceso para que apliquen las medidas de seguridad pertinentes para el uso adecuado.

Logo **Formulario N°23 Reporte de Cambios en el Sistema**

Fecha de cambio:
Encargado de ejecutar el cambio:
Describir razón del cambio:

Aprobación de la gerencia para el cambio: SI: NO:

Firma de revisión que la corrección fue satisfactoria:_____

Firma del encargado de supervisar TI:_____

Fuente: Elaboración propia Serie: 001

b. Se implementará un informe por parte de los responsables de la administración de TI externos, especialmente el sistema, donde detalle las medidas de control nuevas a implementar, los cambios aplicados al sistema y la justificación del porqué se realizaron. Presentando un informe de cambios que se realicen en la programación del sistema, para la Gerencia, siendo éste trimestral.

Logo	Formulario N°24 Informe trimestral del Estado del Sistema
Fecha de Informe: Módulos nuevos implemetados: Módulos eliminados: Módulos actualizados y descripción de los cambios: Autorización de la Gerencia: Fecha de Autorización: Firma de revisión que la corrección fue satisfactoria:_____ Firma del encargado de supervisar TI:_____	

Fuente: Elaboración propia Serie: 001

MONITOREO

Premisa: Los asociados y la Cooperativa se encuentran interesados en que exista un adecuado monitoreo en relación con la seguridad lógica de la información de la Cooperativa.

Objetivo: Evidenciar el adecuado cumplimiento de un monitoreo eficiente y eficaz en relación con la seguridad lógica de la Cooperativa.

Políticas:

1. Se realizará una evaluación anual de Control Interno de seguridad lógica de la información.

Procedimientos:

a) Realizar una evaluación de la ejecución de las políticas y normas que tiene la Cooperativa definidas para la seguridad del sistema, permitiendo así tener información real y oportuna para la toma de decisiones con base en los resultados de los Estados Financieros.

b) La Gerencia en la programación anual de reuniones (ver formulario N° 10 y N°11 en el componente de información y comunicación de seguridad física; de este documento), considerará una fecha para realizar la evaluación de control interno respecto de la seguridad lógica.

c) La evaluación incorporará todas las áreas de la entidad en cuanto a seguridad lógica de la información que mantienen, y se analizará por la Gerencia y el Consejo de Administración los resultados para tomar medidas al respecto.

Logo	Formulario N°25 Evaluación Anual del CI de seguridad lógica		
Área a evaluar: _____	Atributos		
Políticas a cumplir (*)	A	B	C
a.			
b.			
c.			
d.			
e.			

Observaciones y Recomendaciones: _____

_____

Marcas

Atributos: Caracteristicas a evaluar por cada área.

A: Se completan correctamente todos los fórmularios de seguridad lógica

B: Las firmas tanto de preparado como revisado están acorde al periodo y puesto de trabajo

C: Las fechas de los formularios están dentro del periodo correspondiente

S: Cumple

N: No cumple

Firma y fecha de aplicación:_____

Fuente: Elaboración propia Serie: 001

Para efectos del ejemplo *(*)* ver políticas de ambiente de control 2, 3 y 4; en actividades de control ver políticas 1, 2, 4, 9 y 10.

6.7. Bibliografía utilizada.

COSO 2013 y COBIT 5.

Bibliografía

Diccionario de la Lengua Española. (2017, 17 de Febrero). *Eficiencia definición de eficiencia en español del Diccionarios d*e la Lengua Española Recuperado de http://dle.rae.es/?id=EPVwpUD=eficiencia (15/01/17, 13:00)

Diccionario de Oxford. (2017, 17 de Febrero). *Compromiso definición de compromiso en español del Diccionarios Oxford* Recuperado de https://es.oxforddictionaries.com/definicion/compromiso. (15/01/17, 14:00)

Diccionario de Oxford. (2017, 17 de Febrero). *Disciplina definición de disciplina en español del Diccionarios Oxford* Recuperado de https://es.oxforddictionaries.com/definicion/disciplina (15/01/17, 15:00)

Diccionario de Oxford. (2017, 17 de Febrero). *Transparencia definición de transparencia en español del Diccionarios Oxford* Recuperado de https://es.oxforddictionaries.com/definicion/transparencia. (15/01/17, 12:30)

DIGEIG, D. (2012, 01 de Octubre). *? MANUAL DE POLÍTICAS DE TECNOLOGÍA DE LA INFORMACIÓN DE LA DIGEIG* Recuperado de http://www.oas.org/juridico/pdfs/mesicic4_repdom_manTI.pdf (10/02/17 17:00)

DIPA 1009 - TÉCNICAS DE AUDITORÍA CON AYUDA DE COMPUTADORA (2016, 03 de Julio). Recuperado de https://onedrive.live.com/?authkey=!ANIT02MlYnLFPuU&cid=8AFA43B63A8797F4&id=8AFA43B63A8797F4!1242&parId=8AFA43B63A8797F4!1233&o=OneUp (11/02/17 10:00)

Graw hill, M. (Ed.). (2010). *Metodología de la Investigación* (Quinta ed.) McGraw-Hill.

Harold, K. (2004). Administración un Perspectiva Global (12ª ed.) McGraw-Hill.

ISACA. (2012). *COBIT 5 Español, para seguridad de información* Recuperado de https://drive.google.com/file/d/0B75-A280ptiWNUdtaHMzRnVUSFk/edit (4/2/2017 19:30)

ISACA. (2012). *COBIT 5 Ingles, para seguridad de información.* Recuperado de https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf (4/2/2017 19:00)

La asamblea legislativa de la República de Costa Rica, L. (1968, 22 de Agosto). *Ley de Asociaciones Cooperativas* Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=32655&strTipM=TC (14/02/17 13:00)

La Gaceta. (Ed.). (2005, 13 de Octubre). *LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS* Recuperado de http://www.firmadigital.go.cr/Documentos/ley%208454.pdf (06/02/17 20:51)

La Gaceta. (Ed.). (2013, 05 de Marzo). *REGLAMENTO A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES* Recuperado de http://www.redipd.org/legislacion/common/legislacion/costa_rica/Decreto_37554JP20102012ReglamentolCostaRica.pdf (06/02/17 21.00)

NIA 315. (2004, 15 de Diciembre). *ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO Y EVALUACIÓN DE LOS RIESGOS DE REPRESENTACIÓN ERRONEA DE IMPORTANCIA RELATIVA* Recuperado de http://www.leyes.com.py/documentaciones/infor_interes/contabilidad/NIA/NIA-315.pdf (27/02/2016 20:23)

NORMA INTERNACIONAL DE AUDITORÍA 200 OBJETIVOS GLOBALES DEL AUDITOR INDEPENDIENTE Y REALIZACIÓN DE LA AUDITORÍA DE CONFORMIDAD CON LAS NORMAS INTERNACIONALES DE AUDITORÍA (2013, 15 de Octubre). Recuperado de http://www.icac.meh.es/NIAS/NIA%20200%20p%20def.pdf (19/02/17, 9:00)

Norma Internacional de Contabilidad n º 8 (NIC 8) Políticas contables, cambios en las estimaciones contables y errores. (2005, 01 de Enero). Recuperado el 05 de Marzo del 2017, de http://www.normasinternacionalesdecontabilidad.es/nic/pdf/NIC08.pdf (16/02/17 15:00)

Pacter, P. (2015). *IFRS* Recuperado de http://www.ifrs.org/Use-around-the-world/Documents/IFRS-as-global-standards-Pocket-Guide-April-2015.PDF (19/2/17, 15:00)

SUGEF. (2009, 06 de Julio). *SUGEF 16-09 REGLAMENTO DE GOBIERNO CORPORATIVO* Recuperado de https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2016-09%20(v9%20marzo%202014).pdf (29/01/2017 13:00)

Torres Hernández, Z. (2014). *Teoría general de la Administración* (Segunda ed.) Patria.

USAID. (Ed.). (2012, 01 de Mayo). *ESTANDARES SOBRE SEGURIDAD INFORMATICA ISO -IEC 27002* Recuperado de http://pdf.usaid.gov/pdf_docs/PA00JRCT.pdf (07/02/17 18:00)

Glosario

Identificación y autentificación: Se denomina Identificación en el momento cuando el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Palabras claves: Un password es una combinación de letras y/o números que brinda, a quien lo conoce, la posibilidad de acceder a un recurso. El password sirve como protección y como mecanismo de seguridad:

Encriptación: (Cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Lista de control de acceso: Estas listas se refieren a un registro de Usuarios (incluye grupos de usuarios, computadoras, procesos), a quienes se les ha proporcionado autorización para usar un recurso del sistema.

Límites sobre la interfaz de usuario y etiquetas de seguridad: Los límites sobre la interfaz de usuario pueden proporcionar una forma de control de acceso muy parecida a la manera cómo la organización opera, es decir, el Administrador del Sistema restringe al usuario a ciertos comandos, generalmente a través de un menú.

Outsourcing: es un término del inglés que se puede traducir al español como ‘subcontratación’, ‘externalización’ o ‘tercerización’. En el mundo empresarial, designa el proceso en el cual una organización contrata a otras empresas externas para que se hagan cargo de parte de su actividad o producción.

Anexos

Bitacóra N°1	
Lugar: Coopepuriscal R.L	Fecha: 06/05/2017
Objetivo	Analizar el comportamiento del personal al realizar las funciones
Alcance	Evaluación del área administrativa
Observaciones	Durante los sábados el personal supervisor no labora, por lo que se incrementa el riesgo de fraude al existir mayor amplitud de la manupulación de la información y el ingreso a las oficinas de la subgerencia.
Limitaciones durante la sesión	
En ese momento no se encontraba la supervisora del área	
Puesto y área del colaborador analizado	
Plataforma de servicios	Colaborador 1

Fuente: Elaboración Propia

Bitacóra N°2	
Lugar: Coopepuriscal R.L	Fecha: 13/05/2017
Objetivo	Analizar el comportamiento del personal al realizar las funciones
Alcance	Evaluación del área administrativa
Observaciones	La revisión de la cuadratura de la contabilidad se revisa hasta el lunes, siendo ejecutados los procesos el sábado por lo cual, la corrección de un cobro mal ejecutado resulta más dificil de realizar. Por tanto, los estados financieros de la cooperativa se ven afectados.
Limitaciones durante la sesión	
En ese momento no se encontraba la supervisora del área	
Puesto y área del colaborador analizado	
Plataforma de servicios	Colaborador 2

Fuente: Elaboración Propia

Bitacóra N°3	
Lugar: Coopepuriscal R.L	Fecha: 20/05/2017
Objetivo	Visitar la empresa
Alcance	Evaluación de la infraestructura
Observaciones	La entidad le falta medidas de prevención contra incendios, es decir la ubicación de los extintores y salidas de seguridad no están señaladas. Los compañeros pueden prestarse los usuarios y contraseñas y no existe control de ello, por lo cual se puede realizar transacciones poniendose de acuerdo para beneficio personal.
Limitaciones durante la sesión	
Puesto y área del colaborador analizado	
Plataforma de servicios	Colaborador 3

Fuente: Elaboración Propia

Bitacóra N°4	
Lugar: Coopepuriscal R.L	Fecha: 03/06/2017
Objetivo	Visitar la empresa
Alcance	Evaluación de la seguridad de la infraestructura
Observaciones	Se encuentran cerradas las oficinas de los supervisores, sólo cuando estos se retiran, en horas de almuerzo quedan abiertas. Los sistemas quedan sin bloquear cuando las personas se levantan de sus puestos, quedan papeles encima del escritorio de reguardo de seguridad.
Limitaciones durante la sesión	
Puesto y área del colaborador analizado	
Plataforma de servicios	Colaborador 4

Fuente: Elaboración Propia