UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Análisis de Caso, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría C.P.A.

Tema:

"Evaluación al sistema de control interno del departamento de seguridad de la información de la Cooperativa de Ahorro y Crédito Credi Ya Ltda."

Autora: Tibán Analuisa, Jennifer María

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de identidad No. 180293423-0, en mi calidad de Tutora del Análisis de Caso sobre el tema: **"EVALUACIÓN AL SISTEMA DE CONTROL INTERNO DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA."**, desarrollado por Jennifer María Tibán Analuisa, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

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

Ambato, Marzo 2022.

TUTORA

……..……..

Dra. Patricia Paola Jiménez Estrella

C.I. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Jennifer María Tibán Analuisa con cédula de identidad No. 180434979-1, tengo a bien indicar que los criterios emitidos en el Análisis de Caso, bajo el tema: **"EVALUACIÓN AL SISTEMA DE CONTROL INTERNO DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA."**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Análisis de Caso.

Ambato, Marzo 2022.

AUTORA

……..

Jennifer María Tibán Analuisa

C.I. 180434979-1

CESIÓN DE DERECHOS

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

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

Ambato, Marzo 2022.

AUTORA

……..

Jennifer María Tibán Analuisa

C.I. 180434979-1

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el Análisis de Caso, sobre el tema**: "EVALUACIÓN AL SISTEMA DE CONTROL INTERNO DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA."**, elaborado por Jennifer María Tibán Analuisa, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, Marzo 2022.

Dra. Mg. Tatiana Valle
PRESIDENTE

Dra. Rocío Cando
MIEMBRO CALIFICADOR

Ing. Roberto Valencia
MIEMBRO CALIFICADOR

DEDICATORIA

En primer lugar quiero dedicar este trabajo a Dios por su fidelidad, por darme salud, fuerza y voluntad para seguir adelante y cumplir mis sueños.

A mis padres que son el pilar fundamentan en mi vida, por todo su amor y apoyo incondicional que me brindaron cada día para culminar mis estudios.

Jennifer María Tibán Analuisa

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Ambato por abrirme las puertas y permitirme prepararme a nivel profesional.

A la Facultad de Contabilidad y Auditoría y a sus docentes quienes me guiaron e inculcaron sus conocimientos.

A la Cooperativa de Ahorro y Crédito Credi Ya Ltda. por la apertura y su predisposición para desarrollar el presente estudio de caso.

A la Dra. Patricia Jiménez por dedicarme su tiempo y orientarme para ejecutar con éxito este estudio de caso.

Jennifer María Tibán Analuisa

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

TEMA: "EVALUACIÓN AL SISTEMA DE CONTROL INTERNO DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA."

AUTORA: Jennifer María Tibán Analuisa
TUTORA: Dra. Patricia Paola Jiménez Estrella
FECHA: Marzo 2022

RESUMEN EJECUTIVO

El presente análisis de caso efectuado en la COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA., tuvo como fin la realización de una evaluación al sistema de control interno de la seguridad de la información, en la cual se pudo identificar los riesgos expuestos a causa de factores internos, externos, ambientales o humanos. Este proceso se realizó mediante el uso de la metodología COSO 2017 orientado a la evaluación del control interno, donde se denota el buen desempeño en el manejo de las operaciones de acuerdo con los objetivos institucionales. De igual manera se utilizó la metodología MAGERIT que estandariza la seguridad de la información y los niveles de riesgos, lo cual permitió identificar que el sistema operativo, la base de datos y los recursos tecnológicos son los activos más vulnerables y están expuestos a amenazas que afecten el desarrollo de las operaciones. Así mismo, se utilizó la técnica de la observación para medir el nivel de cumplimiento en base la norma ISO/IEC 27002:2013 en el que se demuestra la buena gestión en la seguridad de las operaciones y en las comunicaciones para proteger la información que maneja la institución. En base a ello se definieron propuestas de mejora que permita a la institución administrar adecuadamente los riesgos para reducir el impacto en la consecución de los objetivos, lo que garantiza la confidencialidad, integridad y disponibilidad de la información.

PALABRAS DESCRIPTORAS: CONTROL INTERNO, SEGURIDAD DE LA INFORMACIÓN, COOPERATIVA, ADMINISTRACIÓN DE RIESGOS.

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

TOPIC: "EVALUATION OF THE INTERNAL CONTROL SYSTEM OF THE INFORMATION SECURITY DEPARTMENT OF THE SAVINGS AND CREDIT COOPERATIVE CREDI YA LTDA."

AUTHOR: Jennifer María Tibán Analuisa
TUTOR: Dra. Patricia Paola Jiménez Estrella
DATE: March 2022

ABSTRACT

The purpose of this case analysis carried out in the Savings and Credit Cooperative Credi Ya Ltda., was to carry out an evaluation of the internal control system for information security, in which it was possible to identify the risks exposed due to internal, external, environmental or human factors. This process was carried out through the use of the COSO 2017 methodology oriented to the evaluation of internal control, where good performance in the management of operations is denoted in accordance with institutional objectives. In the same way, the MAGERIT methodology was used, which standardizes information security and risk levels, which allowed us to identify that the operating system, the database and the technological resources are the most vulnerable assets and are exposed to threats that affect the development of operations. Likewise, the observation technique was used to measure the level of compliance based on the ISO/IEC 27002:2013 standard, which demonstrates good management in the security of operations and in communications to protect information. that runs the institution. Based on this, proposals for improvement were defined that allow the institution to adequately manage the risks to reduce the impact on the achievement of the objectives, which guarantees the confidentiality, integrity and availability of the information.

KEYWORDS: INTERNAL CONTROL, INFORMATION SECURITY, COOPERATIVE, RISK MANAGEMENT.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

ÍNDICE DE GRÁFICOS

CONTENIDO **PÁGINA**

CAPÍTULO I

FORMULACIÓN DEL ANÁLISIS DE CASO

1.1- Tema

Evaluación al Sistema de Control Interno del Departamento de Seguridad de la Información de la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

1.2- Antecedentes

La seguridad de la información es un requerimiento para mantener las medidas de protección que le permitan a la entidad desempeñar cada una de sus funciones, independientemente de los riesgos que amenazan el uso de la información (Cruz et al., 2015). Comúnmente en las empresas se determinan políticas y procedimientos de control para salvaguardar la autenticidad y fiabilidad de la información con el objetivo de reducir el impacto de los riesgos, relacionados con el tratamiento de la información (Altaminaro & Bayona, 2017). Estas políticas reflejan la confiabilidad de la empresa y su predisposición siempre en base a las leyes y normas aplicables.

Los sistemas de información son una parte fundamental dentro de las empresas que tienen la posibilidad de crear un entorno más automatizado en cada uno de sus procesos administrativos y operativos (Proaño et al., 2018). Por lo tanto, la información debe protegerse para garantizar que se mantenga su confidencialidad, integridad y disponibilidad para minimizar la posibilidad de daño o amenaza que pueda afectar la continuidad de una empresa (Da Veiga & Martins, 2015). De hecho, la seguridad en las organizaciones no se limita solo a la protección de los bienes y de las personas, sino también se trata de proteger un elemento primordial que es la información donde se almacenan datos confidenciales de los usuarios.

La filtración de datos se convierte en el principal obstáculo de la era digital, por lo que el riesgo de ataques cibernéticos es una prioridad para los altos ejecutivos empresariales. Pues según el Informe de Riesgos Globales 2021 del Foro Económico Mundial (2021), después de analizar los aspectos sociales y económicos a nivel

mundial, detectaron que entre los riesgos con más impacto en los próximos años va a ser la falta de ciberseguridad y los efectos adversos de la tecnología. Ahora, este tipo se situaciones es una gran preocupación, ya que por el covid-19 se ha creado mayor dependencia tecnológica y ha forzado la automatización de actividades sin el conocimiento suficiente lo cual es una amenaza.

De esta manera, el riesgo es la posibilidad de que no se obtengan los resultados esperados, en la cual las organizaciones tienen mayor probabilidad de sufrir un daño en su sistema informático y la amenaza más grave surge cuando los sistemas de información presentan puntos débiles (Baca, 2016). Por ello, la identificación y el análisis de los riesgos conllevan un proceso en el cual se establece un sistema de control interno eficaz. Los altos ejecutivos examinan los riesgos existentes en todos los niveles de la organización, tomar medidas oportunas y gestionarlos con el fin de reducir el impacto que puede afectar a los resultados esperados.

En definitiva, los riesgos van a estar presentes en las organizaciones, lo que afecta la continuidad de los servicios, la protección de la información y la eficiencia en los procesos. Por eso para mantener un nivel de seguridad aceptable es necesario medir los riesgos e identificar el impacto en la disponibilidad, confidencialidad e integridad de la información, lo que implica determinar qué se necesita proteger, de qué hay que protegerlos y cómo hacerlo (Mujica & Alvarez, 2010).

Por otra parte las instituciones financieras juegan un papel importante en el desarrollo económico y social del país, pues a través de ellas se maneja de forma eficiente los recursos financieros y se fomenta el ahorro y la inversión (Jácome, 2006). En este sentido, este tipo de organizaciones permiten la intermediación financiera, a través de la captación del excedente de dinero de las personas para la prestación del mismo a través de créditos (Banco Internacional, 2021). Es más, están sujeto bajo normas y leyes que han sido establecidas con el fin de proteger los intereses de los usuarios.

A la vez en el tercer trimestre del 2020, en base a los resultados del análisis del Banco Central del Ecuador (2021) concluyen que existe un incremento en el número de

personas que tienen acceso a los servicios que ofrece el sistema financiero, llegando a 8,5 millones, de los cuales 4,4 millones son del género masculino y 4,1 millones son del género femenino. De igual forma estas cifras duplican lo que se tenía en el 2016, que era cerca de 4,8 millones, es decir que entre el 2016 y 2020, 3,7 millones de personas han accedido a los servicios que ofrecen las instituciones financieras.

Respecto al caso de estudio la Cooperativa de Ahorro y Crédito Credi Ya Ltda. inició sus actividades bajo acuerdo ministerial N.-006-dpt-c-2011 del 24 de marzo del 2011. Nació gracias a la constancia y tenacidad de un grupo de 11 personas emprendedoras, quienes estaban convencidos de este proyecto, por lo que aportaron un capital inicial de aproximadamente 5 mil dólares, permitiéndose otorgar créditos de hasta un monto máximo de 1.000 dólares al sector de comercio minorista, el cual es el verdadero motor de la economía a pequeña escala con beneficio a las familias de bajos recursos.

Credi Ya abrió sus puertas al público el 06 de agosto del 2011 en sus oficinas en la calle Bolívar 07-22 y Joaquín Ayllón, donde hasta la actualidad brinda un servicio con calidez, siempre apoyando a los comerciantes, agricultores, ganaderos y microempresarios de la provincia de Tungurahua. Con el mismo fervor han ampliado su cobertura, en el año 2018 crearon una agencia en Quito y posteriormente en el 2019 se apertura su segunda agencia en Riobamba, además adquirieron un edificio propio, que será la oficina matriz en la ciudad de Ambato, el cual se inaugurará próximamente a mediados del año 2022, con una infraestructura sólida y funcional, donde se continuará cumpliendo con la misión institucional que permita a los socios mejorar su calidad de vida.

La Cooperativa de Ahorro y Crédito Credi Ya Ltda., fue calificada inicialmente por la CONAFIPS el 14 de octubre de 2013, con estados financieros con corte a 30 de septiembre de 2019, en el cual obtuvo una calificación CAFi A2 con 82 puntos. La institución requería un capital humano profesional y eficiente, que estén prestos a acompañar los proyectos y negocios de los socios. Pues en el 2011, contaron inicialmente con 3 colaboradores y actualmente cuentan con 42 empleados que se

capacitan para enfrentar las nuevas formas de interacción social y adentrarse al mundo digital.

Incluso la confianza es retribuida con la calidad en el servicio que ofrecer, por ello pusieron a disposición de los socios el asistente virtual llamado “Menthor Bot”, quien se conecta desde las diferentes plataformas digitales para que los socios puedan acceder en cualquier momento a sus cuentas, consultar sus saldos, los productos de créditos y más servicios con los que cuenta la institución. Por ello, el acceso lo pueden realizar desde el sitio web de la cooperativa, https://www.crediya.fin.ec/, o a través del número WhatsApp 0999933370.

También renovaron la página web, la cual fue desarrollado con un criterio de fácil navegabilidad para que los socios y clientes puedan desplazarse por todas las páginas que componen el sitio web e interactuar con los simuladores de créditos y de inversiones. Además, pueden realizar consultas de saldo sin salir de su casa o lugar de trabajo y próximamente implementaran la banca web desde su app móvil, para que los socios puedan realizar transacciones, transferencias internas y externas, pagos de servicios, entre otras facilidades con las que contaran los canales electrónicos.

Por otra parte, la situación financiera les permite ofrecer rentabilidad y seguridad, lo que les convierte en su principal aliado financiero, con una sobresaliente trayectoria. A julio del 2021 presenta las siguientes cifras:

- Activos: 13’010.544
- Pasivos: 11’628.956
- Patrimonio: 1’316.181

Igualmente manejan una cartera de crédito de más de 10.000 millones y cuentan con un indicador de morosidad del 1,65%, siendo una de las más bajas del sistema cooperativista del país. Esto denota la sanidad de la cartera y la correcta administración de los recursos de las personas que confían en la institución, lo que les ha permitido consolidarse como un referente del segmento 3.

1.3- Justificación

1.3.1- Justificación teórica

Las organizaciones constituyen un factor importante en el desarrollo económico del país, pero estas se enfrentan a riesgos y amenazas de forma interna o externa, que pueden afectar su estabilidad financiera (Correa et al., 2010). Por lo tanto es necesario implementar controles internos que les permita un buena gobierno para administrar los recursos de manera efectiva. De hecho, para Capote (2001) este sistema no surge por casualidad, sino que se planifica y gestiona en función de las necesidades de cada organización, para garantizar la confiabilidad de las operaciones y así no existan fraudes, errores o mal manejo de la información.

En el mismo sentido la SEPS (2018) señala que el personal administrativo y operativo es el responsable del diseño, mantenimiento, funcionamiento y evaluación de los controles internos. Por una parte, los directivos consideran los aspectos relevantes para determinar el riesgo y las consecuencias que se genera. En cambio, el personal sigue las normas y requerimientos que se exigen para diseñar y fortalecer este sistema. Pues para Da Veiga & Martins (2015) las empresas procesan información sensible sobre los empleados y socios, y el acceso no autorizado a la misma puede afectar la imagen de la organización. En definitiva, todos los sistemas de información están protegidos contra el acceso, uso, modificación o divulgación no autorizado para salvaguardar la integridad de los datos.

Ahora bien, los sistemas de seguridad son esenciales dentro de las empresas, pues pueden surgir situaciones indeseables en las que se involucra los activos de la empresa, poniéndolos en riesgo y pueden surgir graves consecuencias que afectan el giro del negocio (Abril et al., 2013). Por lo general, las empresas cuentan con políticas y procedimientos de seguridad para proteger la integridad de los datos, subsanando así las deficiencias que están vinculadas al uso de los sistemas de información, ya que estos reflejan el propósito de la empresa siempre en base a las normas y reglamentos aplicables (Altaminaro & Bayona, 2017).

En definitiva, estos sistemas son herramientas esenciales para todas las organizaciones, por lo que se deben implementar controles para proteger la información procesada, y así no sean alteradas o manipuladas por usuarios no autorizados. Por lo que la gerencia, evalúa periódicamente el funcionamiento de los controles implementados en la empresa para determinar su efectividad y así demostrar la buena gestión administrativa que desempeñan.

1.3.2- Justificación metodológica

La investigación proporcionó información relevante y significativa para la evaluación del control interno al sistema de seguridad de la información que mantiene la institución, para ello se basó en diferentes tipos de investigación, como es la investigación documental, en la cual se recopiló información, se analizó e interpretó los datos de fuente secundaria que se obtuvieron por otros investigadores relacionados con el tema de estudio para la ejecución del presente trabajo.

A través de la investigación de campo, se recolectó datos directamente de los funcionarios de la Cooperativa de Ahorro y Crédito Credi Ya Ltda., con el fin de recabar información útil sobre la situación de la seguridad de la información y los controles implementados objeto de estudio, para lo cual se aplicó un check list bajo la técnica de la observación enfocando cada componente de los procesos de gobierno y de gestión de los sistemas de información y sus seguridades a cargo del departamento de sistemas.

La metodología utilizada fue el COSO 2017 orientado a la evaluación del sistema de control interno juntamente con una comparación de otras metodologías y normas que estandarizan la seguridad de la información, sus niveles de capacidad en los procesos, los riesgos expuestos para la implementación de un plan de seguridad.

Cabe destacar que el estudio fue para examinar el cumplimiento de los controles y cómo se encuentra el sistema de control interno con respecto a la seguridad de la información, salvaguarda de sus datos y la eficiencia operativa dentro de la institución para la consecución de las metas y objetivos establecidos. La factibilidad de la

investigación también se apoyó en la normativa vigente que regula al sector cooperativista como es la Superintendencia de Economía Popular y Solidaria (SEPS).

1.3.3- Justificación práctica

Con la presente investigación se pretende realizar una evaluación a la aplicación de los controles que tiene la institución en temas de seguridad de la información en el centro de procesamiento de datos y se analizará si estos son ejecutados de manera oportuna, eficiente y efectiva por todo el personal, y en base a ello se verificará su cumplimiento, seguimiento y monitoreo para el tratamiento de la información.

Los resultados que se obtendrán, producto del estudio, permitirá orientar la política de control interno que rige dentro de la entidad en función de proteger los sistemas de información y las seguridades de la misma, implementar procedimientos de mejora, que aporte en la toma de decisiones gerenciales y así garantizar la fiabilidad, disponibilidad e integridad de la información.

Se procurará establecer alternativas o estrategias para el adecuado manejo del sistema de control a través de un plan de seguridad de la información, cuyos beneficios garantizará la confidencialidad, de forma que se pueda prevenir posibles riesgos, amenazas, vulnerabilidades o ataques a su sistema de información de acuerdo con las leyes, directrices establecidas tanto en las normas, estandarización y la metodología aplicada de COSO 2017.

1.4- Objetivos

1.4.1- Objetivo general

Evaluar el sistema de control interno de la seguridad de la información de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. para la prevención de riesgos, administración y salvaguarda de los datos.

1.4.2- Objetivos específicos

- Examinar el sistema de seguridad de la información de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. que permita la identificación de las vulnerabilidades de red, software, hardware que compromete la confidencialidad, integridad y disponibilidad de la información.
- Emplear la metodología COSO 2017 para la verificación del cumplimiento de cada componente relacionado a la seguridad de la información.
- Medir la gestión de los controles adoptados por la institución a través de los indicadores de eficiencia y eficacia en la salvaguarda de datos.
- Narrar los resultados obtenidos del caso de estudio haciendo énfasis en las recomendaciones de técnicas y acciones de buenas prácticas para el sistema de gestión de seguridad de la información.

1.5- Preguntas de reflexión

- ¿De qué manera actualmente la institución asegura la confidencialidad de la información?
- ¿El centro de procesamiento de datos detecta filtración de la información por personas no autorizadas?
- ¿Cuál es el grado de eficiencia y eficacia del control interno?
- ¿Qué medidas de seguridad ha implementado dentro de la institución?
- ¿Cuáles serían las acciones de buenas prácticas que se deban implementar en el centro de procesamiento de datos para mantener un eficiente sistema de control interno en la seguridad de la información?

CAPÍTULO II

FUNDAMENTACIÓN CIENTÍFICA TÉCNICA

2.1- La seguridad de los sistemas de información

Los datos, la información y el conocimiento forman la base fundamental para los sistemas de información, pues los datos se almacenan en grandes cantidades como los registros de transacciones. La información es un mensaje que se transmite entre un emisor y un receptor con un propósito como la nómina de proveedores o el historial de ventas. Por otra parte, el conocimiento proporciona un marco para evaluar y comprender la nueva información (Cobarsi-Morales, 2011). En definitiva, el sistema de información es vista como una estructura compuesta por personas, equipos y procedimientos que hacen que la información esté disponible para planear, controlar e implementar funciones más eficientes (Baca Urbina, 2015).

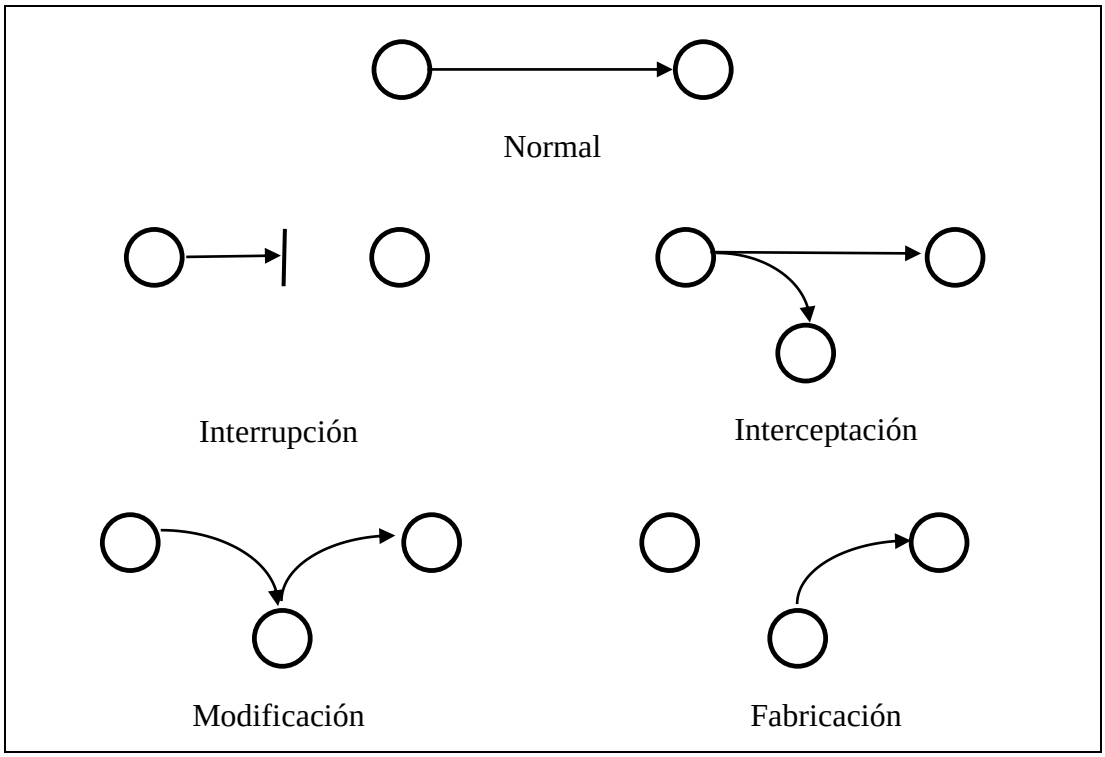

Gráfico 1. Flujo de información
Fuente: Costas (2014)

Después de todo, el éxito de las empresas no solo depende del manejo de los recursos, también tiene que ver con la gestión de la información, que les permite obtener datos relevantes para la toma de decisiones (Arévalo, 2007). De la misma manera, Aumatell (2013) asegura que esta se pueda ver como un activo valioso o como un problema, de acuerdo a la manera en que se la gestiona ya que afecta a la investigación, desarrollo e innovación (I+D+i), para ello se comprende el papel que desempeña la información en la organización para usarlo de manera eficiente.

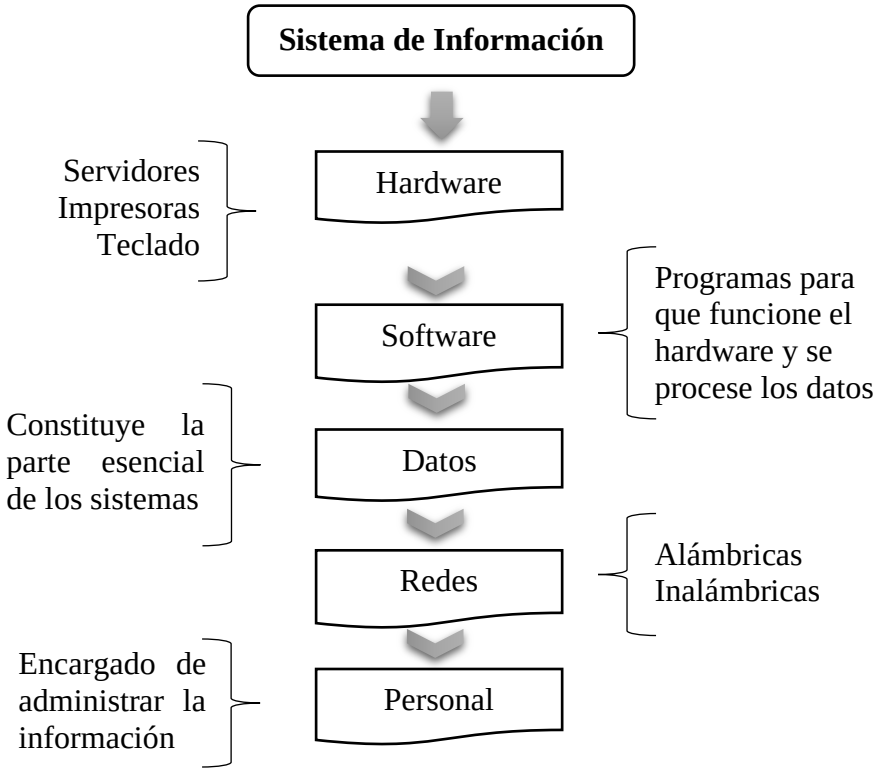

Gráfico 2. Elementos del sistema de información
Fuente: Baca (2015)
Elaborado por: Tibán (2022)

La seguridad para Costas (2014) está asociada con la contingencia, por lo que, dentro de cualquier sistema, los elementos principales a proteger son el hardware, que son elementos físicos de un sistema informático; el software que son sistemas operativos, aplicaciones o programas que hacen funcionar el hardware; y los datos que es la información que maneja el software y hardware. Pero para comprender el contexto de la seguridad de la información, Escrivá et al. (2013) menciona que es importante comprender unos conceptos básicos relacionados con la temática que son:

Tabla 1. Conceptos básicos relacionados con la seguridad de la información

Término	Descripción
Activo	Recurso necesario del sistema que tenga valor y sea protegido para que la organización alcance los objetivos propuestos, entre ellos se encuentra el activo de información, que son los elementos que contiene datos almacenados; los activos físicos, relacionada con la infraestructura tecnológica utilizada para gestionar la información; los programas o aplicaciones utilizados y el personal que maneja esta información.
Vulnerabilidad	Debilidad de un activo que pueda implicar en el funcionamiento del sistema informático, los cuales pueden estar relacionados con fallos en las aplicaciones, mal uso de los sistemas, ataques informáticos o virus, por ello es necesario detectar estas situaciones que ponen en peligro la seguridad del sistema.
Amenaza	Una amenaza es cualquier entidad que atente contra el buen funcionamiento de un sistema informático, estas pueden ser pasivas cuando se obtiene información relativa a una comunicación, y activas, en caso de que se realicen cambios no autorizados dentro de los sistemas, por lo que son más peligrosas.
Riesgo	Un riesgo es la probabilidad de que la amenaza se materialice causando daño en algún proceso o sistema, por lo que se debe tratar de manera inmediata a través del análisis de los riesgos para establecer prioridades e implementar procedimientos de seguridad adecuados de acuerdo con las necesidades de la organización.

Fuente: Escrivá Gascó et al. (2013)
Elaborado por: Tibán (2022)

La seguridad del sistema de información puede establecer un plan de seguridad para proteger la integridad de los datos dentro de diferentes áreas relacionadas con la gestión informática (Navarro & Díaz, 2014), entre las cuales se puede mencionar:

- *Entorno:* estudio de vulnerabilidades asociados con las instalaciones y equipos

- *Organización:* utilización de datos o programas, personal no autorizado y control de documentación.
- *Operación:* salidas de información o datos relevantes, alteración de configuraciones y fallos mal intencionados.
- *Soportes:* pérdida o robo de soportes magnéticos.
- *Software:* accesos ilícitos, alteración del sistema, destrucción de información
- *Mantenimiento:* acceso a datos durante los procesos de mantenimiento de los equipos

Cabe destacar que la seguridad absoluta no existe ya que no es posible que un sistema este completamente seguro, por lo que el riesgo siempre estará presente, aunque se tomen medidas para mitigarlos (Bustamante & Osorio, 2014). De hecho, se establecen principios de seguridad que son la base para proteger tanto la información confidencial como los activos de la organización.

Tabla 2. Principios de la seguridad de la información

Principio	Característica	Vulnerabilidad
Confidencialidad	Información accesible solo para personas o sistemas autorizados.	Divulgar claves de acceso y violar protocolos de comunicación.
Integridad	Información que no sea alterada y que permite comprobar que no se ha manipulado la información original.	Alterar información sin tener acceso y modificar el mensaje en la red de comunicaciones.
Disponibilidad	Capacidad de un servicio, dato o sistema que este accesible para los usuarios cuando lo requieran.	Presencia de virus y ataques que perjudican al sistema o a la red.

Fuente: Costas (2014)
Elaborado por: Tibán (2022)

La seguridad no solo se trata de proteger los activos o la infraestructura física de la organización, sino también se encarga de salvaguardar la información confidencial que

se maneja de los usuarios y clientes. Pues por una parte, la seguridad física consiste en la aplicación de barreras físicas y procedimientos de control ante las amenazas presentes a la información confidencial, con el fin de proteger el hardware y el almacenamiento de datos (Costas, 2014). Las principales amenazas detectadas que ponen en riesgo a un sistema informático son los desastres naturales, actos ocasionados por el hombre y acciones deliberadas como robo o fraude (Hernández & Flores, 2011).

En cambio, la seguridad lógica va más allá de la seguridad física ya que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los sistemas informáticos y espacios físicos dentro del centro de datos y solo se permite su uso a las personas autorizadas. Esto con el objetivo de restringir el acceso al sistema operativo, los programas y archivos para protegerlos contra amenazas también conocidas como ataques cibernéticos (Costas, 2014).

2.1.1- Análisis de riesgos en la seguridad de la información

Las organizaciones tienen éxito por tomar riesgos, pero algunas fallan cuando los riesgos no se gestionan de manera eficaz, por ello se destinan recursos no solo para la toma de riesgos, sino también para su gestión. Por lo general existen diversos factores que contribuyen con los desafíos empresariales, ente los cuales se destacan las fallas en el perfil de riesgos cuando se formulan las estrategias, insuficiente monitoreo y gestión de los riesgos asumidos y las fallas para reevaluar las estrategias frente a los cambios externos.

La gestión de los riesgos es fundamental para todas las empresas, pues ayuda a la protección de los activos, el manejo de las finanzas y operaciones de la empresa con el fin de mantener el buen desempeño corporativo. Ahora bien es conveniente implementar estrategias basadas en la política de riesgos considerando los recursos, normativa, las tecnologías de información, el entorno y los objetivos de la empresa, para identificar los riesgos potenciales y clasificarlos de acuerdo a su nivel de impacto, y en base a ello tomar medidas para contrarrestar dichos riesgos o monitorearlos de forma continua.

Tabla 3. Tipos de riesgos

Tipos	Relación	Riesgos
Riesgo Operativo	Ligados con la planeación que es de vital importancia para lograr la eficiencia operativa	La misión y visión no definidos
		Carencia de un organigrama formal
		Falta de procedimientos operativos para cada uno de los procesos
		Ausencia de canales de comunicación formales
Riesgo Administrativo	Ligado con el establecimiento del control en las operaciones para una adecuada administración.	Inadecuada separación de funciones
		Falta de controles en las áreas
		Inadecuada administración de los recursos humanos
		Información administrativa no confiable
Riesgo Financiero	Relacionado con los resultados económicos de las empresas	Inadecuada presentación de los estados financieros básicos
		Ausencia de asesores o consejeros
		Falta de supervisión en los cálculos
		Información financiera que no aporta seguridad razonable
Riesgo Estratégico	Relacionado con el cumplimiento de la visión empresarial	No cuenta con una planeación a mediano y largo plazo
		No cuenta con una seguridad eficiente de la base de datos
		Desconocimiento de los avances tecnológicos

Fuente: Pereira Palomo (2019)
Elaborado por: Tibán (2022)

En la actualidad con los avances tecnológicos, los procesos son más automatizados y fácilmente manejables, lo que provoca que algunas personas se dediquen a sustraer información o datos confidenciales de manera ilegal. Como lo indica la encuesta

realizada por PwC (2018) a 9.500 directivos y responsables de TI de 122 países sobre el estado de la seguridad de la información, donde muestran que las empresas tienen en promedio 3,4 incidentes de seguridad al año y en pérdidas económicas sobrepasa los 4 millones de dólares. En el caso de España, se vieron obligados a paralizar sus actividades laborales por lo menos 17 horas al año debido a los ataques informáticos que experimentaron.

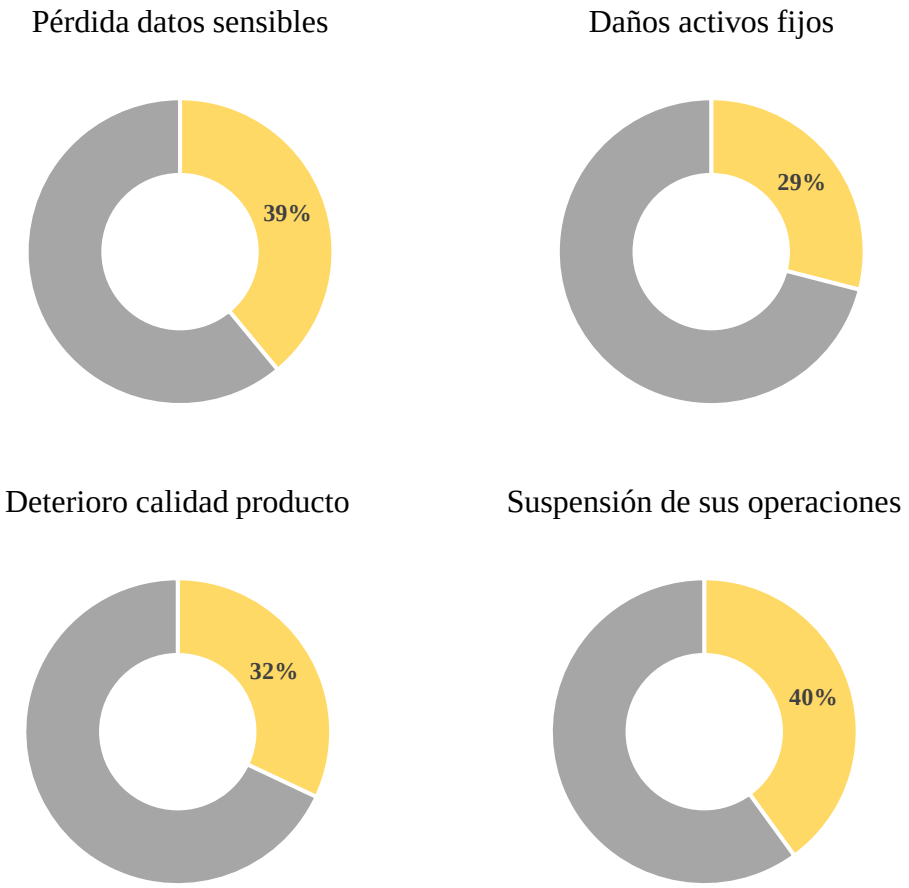

Gráfico 3. Consecuencias de los ciberataques en el mundo
Fuente: PwC (2018)

En cambio, en la investigación realizada por el Equipo de Detección y Respuesta Rápida de Microsoft, los ciberataques generan un gran impacto a nivel empresarial y los sectores más afectados son el comercio minorista (13%), los servicios financieros (12%), la industria manufacturera (12%), la administración pública (11%) y la sanidad (9%). Por consiguiente, Estados Unidos y China son los principales países que más ataques han recibido seguido de Japón y Alemania (Higuera, 2021). De hecho, esto

forzó a las empresas a tomar medidas y mejorar los protocolos de seguridad para minimizar los riesgos que perjudiquen la estabilidad de las empresas.

Por otra parte, el buen funcionamiento de las empresas está basado en la correcta administración de los riesgos y en la implementación de acciones preventivas en caso de que se presenten situaciones que pueda afectar la estabilidad económica de las empresas, aunque este no se elimine por completo, la intención es tolerar el impacto que este genere. En palabras de Coopers & Lybrand (2007), mencionan que la identificación y el análisis de los riesgos en todas las áreas de la empresa, es un proceso que se debe desarrollar para tener un sistema de control interno efectivo.

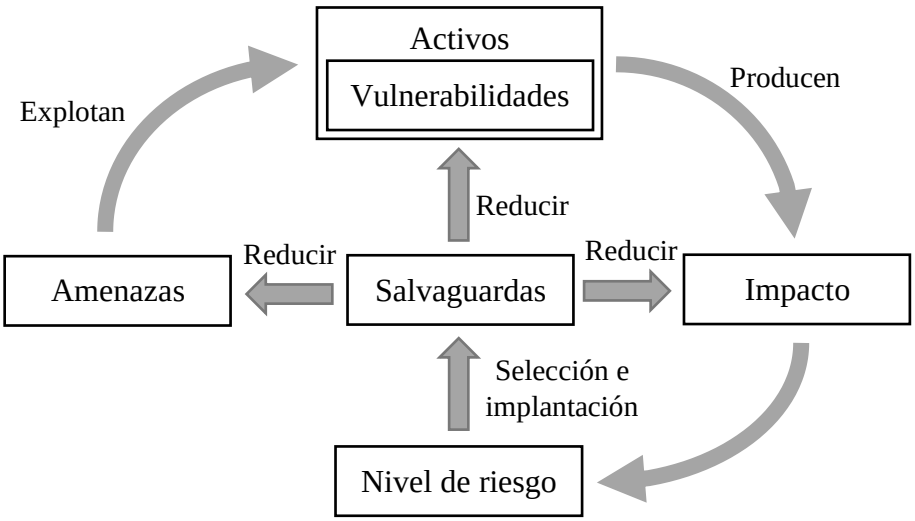

Gráfico 4. Proceso de evaluación y gestión de riesgos
Fuente: Gómez Vieites (2014)

Por ejemplo, un caso relacionado con los incidentes de seguridad de la información es Facebook, quien presentó una demanda en contra de una persona por sustraer la información de más de 170 millones de usuarios para venderla en foros ilegales empleando herramientas de hacking. Facebook logró detectar esta situación y tomó medidas para evitar que dicha información siga circulando en foros inusuales (Esage, 2021c). De forma similar le sucedió a una universidad de España que sufrió un ataque de ransomware a sus sistemas informáticos, lo cual interrumpió sus actividades y los estudiantes no han podido hacer uso de los recursos tecnológicos. La universidad, como medida de seguridad, desconecto todas sus redes para que nadie lo pueda acceder

al sistema hasta solucionar el problema y poder restablecer los sistemas (Esage, 2021b).

Por si fuera poco, los alcances de los fraudes son muy sorprendentes, que incluso logran burlar los sistemas de seguridad de las instituciones financieras, como es el caso de un banco que fue engañado por hackers, que clonaron la voz del dueño de una empresa para engañar al gerente del banco y realizar una transferencia bancaria por varios millones de dólares. Estos incidentes pueden ocurrir con más frecuencia ya que se pueden obtener registros de voz a través de notas de audio, publicaciones de redes sociales y demás plataformas de acceso público (Esage, 2021a). Para medir el impacto que puede causar los incidentes de seguridad a una organización, se puede emplear una escala cuantitativa o cualitativa.

Tabla 4. Escala propuesta para medir el impacto del daño en la organización

Escala	Descripción
Alto	• Perdida de recursos críticos • Interrupción de los procesos de negocio • Daños en la imagen y reputación de la organización • Robo o revelación de información estratégica
Moderado	• Perdida de recursos críticos pero que cuentan con elementos de respaldo • Caída notable en el rendimiento de los procesos de negocio en la actividad normal de la organización • Robo o revelación de información confidencial, pero no considerada estratégica
Bajo	• Perdida de recursos secundarios • Disminución del rendimiento de los procesos de negocio • Robo o revelación de información interna no publicada

Fuente: Gómez Vieites (2014)
Elaborado por: Tibán (2022)

Dentro de la seguridad de la información, se toma en cuenta los aspectos técnicos para dar respuesta inmediata a los problemas de seguridad a través de los cortafuegos o antivirus, sin embargo, también están involucradas el personal de una organización, ya que constituyen la principal línea de defensa. Los errores de configuración cometidos por el descuido de los empleados pueden hacer que la red sea vulnerable de ataques y que los sistemas estén desprotegidos, por lo tanto el comportamiento humano está relacionado con las fallas de seguridad (Ahmed et al., 2012). Los factores humanos y tecnológicos son elementos indispensables que deben trabajar en conjunto, pues las personas necesitan la ayuda de máquinas para desempeñar sus funciones, al igual que las maquinas no tienen inteligencia y requieren instrucciones para configurar sus operaciones.

Tabla 5. Porcentaje de pérdida económica en los sistemas de información

Porcentaje de pérdida económica	
Infracciones (22%)	**Errores (65%)**
Sabotaje • 3% forasteros maliciosos • 13% empleados deshonestos • 6% empleados descontentos	Resbalones y lapsos • Errores basados en habilidades • Errores basados en reglas • Errores basados en el conocimiento

Fuente: (Ahmed et al., 2012)
Elaborado por: Tibán (2022)

En la Encuesta de Seguridad de la Industria de Servicios Financieros Globales (GFSI), revela que la mayoría de los encuestados confirman que el error humano es la causa principal de fallas en los sistemas de información. El 65% de la pérdida económica atribuida a violaciones de seguridad de la información fue causada por errores humanos, mientras que solo el 3% se atribuyó a personas externas malintencionadas. Aunque las estadísticas se centran en los errores humanos en entornos organizacionales, no hay investigaciones significativas sobre técnicas de mejora o mitigación de errores humanos, estos errores pueden causar brechas en la seguridad de la información de diversas maneras y pueden ser causados por falta de conocimiento informático, errores técnicos o simplemente por descuido (Ahmed et al., 2012).

2.2- La gestión administrativa dentro del sector empresarial

La palabra control es vista de forma negativa como una limitación o restricción, pero hace referencia a la revisión, inspección y regulación de todas las actividades que desempeña cada departamento (Torres & Torres, 2014). De hecho Lozano & Tenorio (2015) señalan que el control interno presenta tres generaciones, la primera estaba relacionada con los controles contables y administrativos. En la segunda, se establecen evaluaciones para definir el alcance de los controles y la tercera generación está marcada por garantizar la efectividad del control interno.

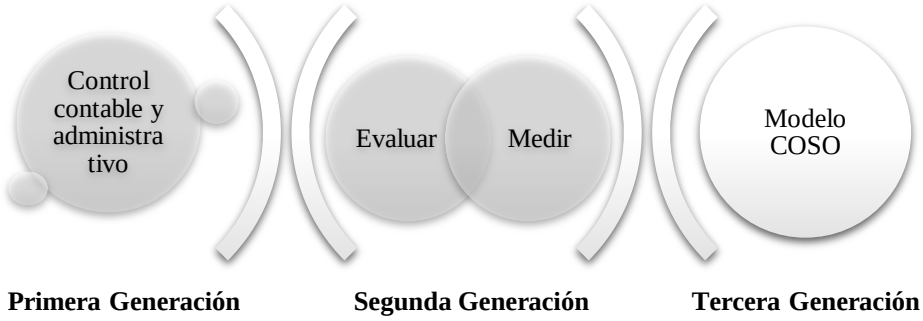

Gráfico 5. Evolución del control interno
Fuente: Lozano & Tenorio (2015)
Elaborado por: Tibán (2022)

El control interno es un proceso establecido por la administración y el personal de la organización para diseñar, modificar o mejorar las políticas y procedimientos institucionales, con el fin de proporcionar seguridad razonable en la información y así prevenir incidentes, siempre basados en las leyes y normativas aplicables para la gestión adecuada de los recursos (Estupiñán, 2006). En las empresas se practica continuamente y se implementan o modifican procesos de mejora que aporten al buen desempeño de acuerdo con las necesidades de la organización, además el control se ejerce mediante la evaluación personal, los resultados obtenidos y los informes técnicos (Sánchez Delgado, 2014), para ello existen los tipos de control que se detallan a continuación:

- *Control preliminar:* es un evento previo para preparar los recursos necesarios para la ejecución de las actividades.

- *Control coincidente:* observar y vigilar que todas las actividades se lleven a cabo de acuerdo con las políticas y procedimientos establecidos.
- *Control por retroalimentación:* centrarse en los resultados anteriores para controlar las actividades futuras.

El control interno es empleado sin tomar en cuenta la naturaleza de las operaciones, se definen políticas y procedimientos para detectar y prevenir los riesgos en busca de una mejora continua (Armenta & Aguirre, 2012). Inclusive, este sistema ayuda en la eficiencia de las operaciones, rentabilidad y confiabilidad de la información que proporciona un nivel de seguridad razonable para la consecución de objetivos (Chumpitaz & Gonzalez, 2015). De este modo, el control interno permite optimizar los recursos con el fin de llevar una gestión administrativa más eficiente y productiva.

2.2.1- Metodología COSO ERM 2017

Para la evaluación del sistema de control interno se utiliza el modelo COSO ERM 2017, como lo menciona PwC (2021) el Consejo del Committee of Sponsoring Organizations of the Treadway Commission (COSO) actualiza el marco integrado de la primera versión de 2004 y se implementó un nuevo enfoque en la administración de riesgos, la capacidad de las organizaciones para perfeccionar su estrategia en un entorno de cambios frecuentes. Este nuevo enfoque ayuda a manejar adecuadamente el riesgo, además de reducir los imprevistos negativos.

En las organizaciones, el capital humano es la primera línea de defensa en la administración de los riesgos, debido a que están involucrados en las actividades cotidianas, los procesos y controles internos que desarrolla la empresa, por lo que poseen mayor influencia y capacidad sobre el riesgo para identificarlo, analizarlo y prevenir cualquier afectación al giro del negocio (PwC, 2021). El marco COSO ERM 2017 esta estructurado a partir de cinco componentes y 20 principios, para que las personas puedan verlo desde la estrategia hasta la ejecución, esta nueva estructura le permite ver como se incorporan los riesgos en el gobierno corporativo, como pasan por los distintos procesos, como se identifican indicadores clave y como se hace un monitoreo.

Tabla 6. Componentes del control interno

Componentes del Control Interno	
Gobierno y Cultura	El gobierno establece el tono de la organización, estableciendo responsabilidades de supervisión, para la gestión de riesgos empresariales. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo en la entidad.
Estrategia y objetivos	Gestión de riesgos, estrategia y objetivos trabajan juntos en el proceso de planeación estratégica. El apetito de riesgo es definido y alineado con la estrategia; los objetivos de negocio ponen la estrategia en práctica mientras sirve para identificar, evaluar y responder a los riesgos.
Desempeño	Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados. Riesgos son priorizados por severidad y en el contexto del apetito del riesgo. La organización selecciona las respuestas al riesgo y toma el riesgo que ha asumido.
Revisión	Para revisar el desempeño de la entidad, una organización considera que tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y que revisiones se necesitan.
Información, comunicación y reporte	La gestión de riesgos empresariales requiere un proceso continuo para obtener y compartir información necesaria, de fuentes internas y externas, que fluya en todas las direcciones y a través de toda la organización.

Fuente: PwC (2021)
Elaborado por: Tibán (2022)

2.3- Funcionamiento del sistema financiero

A nivel nacional, las entidades financieras se clasifican en 2 grandes grupos, el primero es el sector bancario, cuyo organismo de control es la Superintendencia de Bancos, quien se encarga de supervisar y controlar a las entidades del sector público y privado

del sistema financiero para preservar su seguridad y transparencia. También dentro de este sector, se subdividen en bancos públicos y privados, de los cuales existen 31 instituciones activas que brindan sus servicios a la ciudadanía (Superintendencia de Bancos, 2021).

Tabla 7. Clasificación de las entidades del sector bancario

Sector Bancario			
Estado	**Privado**	**Público**	**Total**
Activa	23	8	**31**
Concluida existencia legal	23	1	**24**
Fusión por absorción	2	0	**2**
Inactiva	2	1	**3**
Inactiva por fusión	2	0	**2**
Liquidación	2	2	**4**
Total	**54**	**12**	**66**

Fuente: Superintendencia de Bancos (2021)
Elaborado por: Tibán (2022)

Por añadidura, de acuerdo con la Ley General de Instituciones del Sistema Financiero (2012), los bancos pueden efectuar las siguientes operaciones:

1) Recibir recursos del público en depósitos a la vista, de ahorro exigibles y cualquier otro exigible
2) Recibir depósitos a plazo
3) Asumir obligaciones por cuenta de terceros a través de aceptaciones, endosos o avales de títulos de crédito
4) Emitir obligaciones y cedulas garantizadas con sus activos y patrimonio
5) Recibir préstamos y aceptar créditos de instituciones financieras
6) Otorgar préstamos hipotecarios y prendarios, con o sin emisión de títulos, así como prestamos quirografarios
7) Conceder créditos en cuenta corriente, contratados o no
8) Negociar letras de cambio, pagares, facturas y otros documentos que representen obligación de pago
9) Negocias documentos resultantes de operaciones de comercio exterior

10) Negociar títulos valores y descontar letras documentarias sobre el exterior, o hacer adelantos sobre ellas
11) Constituir depósitos en instituciones financieras del país y del exterior
12) Adquirir, conservar o enajenar, por cuenta propia, valores de renta fija, de los previstos en la Ley de Mercado de Valores

Debido a que los bancos ven que sus clientes tienen que recorrer largas distancias para llegar a las instalaciones o tienen que hacer filas para realizar sus operaciones financieras, se proyectaron que sus servicios sean más accesibles y no solo puedan hacerlo en el banco, sino también en las tiendas de barrio, bazares y otros. Por consiguiente, en los estudios realizados por la Federación Latinoamericana de Bancos (FELABAN), el Ecuador es el cuarto país con más canales que prestan sus servicios a través de terceros, pues a marzo de 2021, se registró 200 canales por cada 100.000 habitantes, estos datos comparados con el 2020, presentan un crecimiento del 23,5% (Asobanca, 2021), lo que representa un gran avance para el sector.

En cambio, por otra parte, están las cooperativas de ahorro y crédito que han ayudado a la reactivación económica del país, pues en el 2021, hay más de 6 millones de socios distribuidos en las diferentes instituciones financieras. De hecho, en estos años, se han creado más cooperativas que bancos, en la cual se implementan mecanismos de intermediación financiera del sector popular y solidario de acuerdo con las necesidades de la población. Además, estas son controladas por la Superintendencia de Economía Popular y Solidaria (SEPS), quien es el organismo regulatorio que promueve la sostenibilidad y el adecuado funcionamiento para proteger a los socios. De la misma manera, se cuenta con más de 3.800 puntos de atención ubicados en sectores estratégicos para la colocación de créditos y microcréditos (SEPS, 2021a).

En este sentido, en el análisis realizado con los datos recogidos de la SEPS, en el Ecuador actualmente existen 488 cooperativas de ahorro y crédito activas, de los cuales en la Sierra se encuentra una mayor demanda de las cooperativas, a comparación de la Costa, Oriente y región Insular. Especialmente en la provincia de Pichincha se crearon alrededor de 98 instituciones financieras del sector popular y

solidario, de los cuales se concentran más dentro del segmento 4; seguido por la provincia de Tungurahua, Chimborazo y Cotopaxi. En definitiva, el sector financiero popular y solidario representa un tercio del sistema financiero nacional, lo que ha permitido un crecimiento sostenible.

Tabla 8. Cooperativas de ahorro y crédito en el Ecuador

Cooperativas de Ahorro y Crédito							
Región	**Provincia**	**Segmento**					**Total**
		1	**2**	**3**	**4**	**5**	
Costa	Esmeraldas	-	-	1	-	-	**1**
	Manabí	3	3	3	8	13	**30**
	Los Ríos	-	1	1	5	3	**10**
	Guayas	-	-	8	14	12	**34**
	Santa Elena	-	-	1	1	-	**2**
	Santo Domingo de los Tsáchilas	-	-	1	1	2	**4**
	El Oro	2	-	1	3	4	**10**
Sierra	Carchi	2	1	1	1	-	**5**
	Imbabura	2	5	6	3	6	**22**
	Pichincha	7	13	15	36	27	**98**
	Cotopaxi	1	3	12	14	12	**42**
	Tungurahua	8	3	16	26	24	**77**
	Bolívar	1	2	4	2	3	**12**
	Chimborazo	2	3	5	10	27	**47**
	Cañar	1	1	1	3	5	**11**
	Azuay	6	6	5	7	6	**30**
	Loja	2	2	5	14	8	**31**
Oriente	Sucumbíos	-	-	1	-	1	**2**
	Napo	-	1	-	1	-	**2**
	Orellana	-	-	1	2	2	**5**
	Pastaza	1	-	1	-	1	**3**
	Morona Santiago	-	1	-	-	-	**1**
	Zamora Chinchipe	-	2	1	2	1	**6**
Insular	Galápagos	-	-	1	1	1	**3**
Total		**38**	**47**	**91**	**154**	**158**	**488**

Fuente: SEPS (2021a)
Elaborado por: Tibán (2022)

Por añadidura, de acuerdo con la Ley Orgánica de la Economía Popular y Solidaria (2011), las cooperativas de ahorro y crédito podrán realizar las siguientes actividades:

1) Recibir depósitos a la vista y a plazo
2) Otorgar préstamos a sus socios
3) Conceder sobregiros ocasionales
4) Efectuar servicios de caja y tesorería
5) Efectuar cobranzas, pagos y transferencias de fondos, así como emitir giros contra sus propias oficinas
6) Recibir y conservar objetos muebles, valores y documentos en depósito para su custodia
7) Actuar como emisor de tarjetas de crédito y de debito
8) Asumir obligaciones por cuenta de terceros a través de aceptaciones, endosos o avales de títulos de crédito
9) Recibir prestamos de instituciones financieras y no financieras
10) Emitir obligaciones con respaldo en sus activos, patrimonio, cartera de crédito hipotecaria o prendaria
11) Negociar títulos cambiarios o facturas que representen obligación de pago
12) Invertir preferentemente en el Sector Financiero Popular y Solidario, sistema financiero nacional y en el mercado secundario de valores
13) Efectuar inversiones en el capital social de cajas centrales

En definitiva, según el análisis realizado por Lara (2021) todas las entidades del sistema financiero nacional alcanzan un crecimiento del 15% en sus activos, 51% en fondos disponibles, 17% en inversiones de los bancos privados y el 32% en inversiones de las cooperativas de ahorro y crédito del segmento 1. Por otra parte, los depósitos también reportaron un incremento del 17,9%, respecto al 2019, los cuales se destinan al ahorro y a la inversión. Pues con estos datos denota que las organizaciones se consolidan dentro del sector financiero, permanecen sólidos, se adaptan fácilmente a los cambios y generan rentabilidad a pesar de la grave crisis por la pandemia.

2.3.1- La importancia de la tecnología en el sistema financiero

La era digital es impulsada por las pequeñas y grandes organizaciones con el fin de cumplir con los requerimientos de los clientes del siglo XXI, lo que conlleva adentrase a la transformación digital. Así, en la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), revela que entre los años 2015 y 2020, se incrementó el número de personas que utilizan la banca digital que pasa del 7% al 15%, es decir, alrededor de 7,5 millones de personas (Forbes, 2021). De hecho, dentro de las instituciones financieras se realizan diferentes operaciones a través de dispositivos electrónicos y plataformas digitales que requieren de un alto nivel tecnológico para que la información fluya de manera confiable y oportuna (Zhañay et al., 2019).

Del mismo modo la SEPS (2021b) junto con la revista especializada en tecnología IT, desarrollaron la encuesta de "Servicios Financieros Digitales de las entidades del Sector Financiero Popular y Solidario", con el fin de conocer el nivel de capacidad para ofrecer productos y servicios financieros a través de canales digitales. Pues se presenta estrategias para obtener información sobre el avance que tiene las instituciones en cuanto a la digitalización de servicios, las medidas adoptadas con relación a la prevención y vigilancia de la seguridad de la información y ciberseguridad. Así mismo, esta encuesta permite tener una percepción de la evolución de los modelos de negocio a través de la tecnología.

Inclusive el equipo técnico de la SEPS desarrolló otra encuesta relacionada al "Estado actual de Seguridad de la Información y Ciberseguridad en el sector controlado por la SEPS", dando como resultado que 5 de cada 10 entidades se encuentran en desarrollo de servicios financieros digitales. En cambio, solo 1 de cada 10 entidades, destinan más del 20% de su presupuesto en la innovación y tecnología, lo que refleja la necesidad de enfocarse más en la educación financiera digital.

En otras palabras, la tecnología se está adentrando cada vez más al sector financiero para transformar sus operaciones y optimizar los recursos, entre los avances tecnológicos se destaca la automatización de los procesos para generar mayor

eficiencia en los servicios, también se puede resolver los problemas administrativos o de cualquier índole (Palomo et al., 2018). Además, algunas entidades han integrado a sus sistemas la identificación digital a través del reconocimiento facial, de voz, huellas dactilares y otros para evitar fraudes y poder realizar gestiones a través de internet (Aden, 2020).

A la vez la pandemia cambio drásticamente las costumbres de las personas, incluso en el manejo del sistema financiero, donde se ha adaptado la tecnología para realizas pagos y transferencias de manera segura y sin interrupciones (El Universo, 2020). Por ejemplo, Produbanco ha desarrollado nuevos productos y servicios a través de plataformas digitales para satisfacer las necesidades de sus clientes como la página web, app móvil y otros, lo que se ve reflejado en el registro de las incorporaciones de nuevos usuarios (Datta, 2021).

En consecuencia, como se incrementa la demanda de servicios financieros electrónicos, también aumenta los delitos informáticos para sustraer información confidencial y así suplantar identidades. Por tanto, el Intendente General Técnico de la SEPS (2021b) detecta un riesgo que puede afectar la estabilidad de las entidades financieras y presenta algunas recomendaciones a tomar en cuenta:

- Evitar el uso de correo electrónico, mensajes de texto, llamadas telefónicas o redes sociales para el envío de información personal o financiera.
- No abrir correos electrónicos ni enlaces de remitentes que no sean de contactos conocidos.
- Comprobar siempre que se acceda a sitios seguros verificando que el URL de la página inicie con “https”.
- Usar siempre antivirus y mantenerlo actualizado y con licencia en cualquier dispositivo que acceda a internet.
- No acceder a las páginas de internet a través de enlaces, en correos u otras páginas, sino escribiendo el URL en la barra de direcciones.

2.4- Teoría general de sistemas aplicable al sector empresarial

La teoría general de sistemas presenta un conjunto de enfoques que proporcionan técnicas para la investigación y además se aplican en casos específicos (Bertalanffy, 1968). Pues los sistemas dentro de las organizaciones se encargan del estudio de los procesos aislados y ayudan a resolver los problemas detectados, es decir, se encuentran ante sistemas generalizados. De hecho, esta teoría sirve para crear modelos acordes al área o proceso específico y así evitar que las malas decisiones perjudiquen el progreso de las mismas. Ahora bien, la teoría de los sistemas tiene una amplia extensión que se aplica a diferentes ciencias o modelos, pues dentro del modelo cibernético esta teoría se basa en la transferencia de información. Dentro de la tecnología, las computadoras se han adentrado al mundo de los sistemas automatizados, facilitando cálculos y procedimientos que de otra manera llevarían mucho tiempo desarrollarlas.

CAPÍTULO III

METODOLOGÍA

3.1.- Metodología e instrumentos de recolección de información

3.1.1- Unidad de análisis

La Cooperativa de Ahorro y Crédito Credi Ya Ltda. es una institución del sector popular y solidario, con 10 años de experiencia trabajando para apoyar a los productores, artesanos, empresarios y emprendedores, la cual es la unidad de análisis donde se efectúa el análisis de caso, esta institución ha venido desarrollando actividades de recepción de depósitos y la concesión de créditos o préstamos. La entidad se ha ido consolidando dentro del ámbito financiero, tanto que actualmente se encuentra dentro del segmento 3. Pues, las instituciones financieras tienen que cumplir con ciertos requisitos establecidos por la Superintendencia de Economía Popular y Solidaria para posicionarse dentro de cada segmentación.

La institución fue creciendo al igual que el número de socios, y por ello manejaban gran cantidad de datos e información confidencial, lo que causó que la planificación, organización, dirección y control de los recursos en lo que respecta la seguridad de la información se torne insuficiente, lo que le ha limitado en el cumplimiento de los objetivos organizacionales. Por ello se percibió la necesidad de implementar políticas, manuales y procedimientos aplicables a cada departamento para desempeñar sus actividades de manera eficiente y eficaz de acuerdo con los requerimientos del mercado financiero.

3.1.2- Fuentes y técnicas de recolección de información

3.1.2.1- Fuentes de información primaria

Las fuentes de información primaria para el desarrollo del presente estudio se basaron en datos recopilados del personal de los departamentos: centro de procesamiento de datos y auditoria que forma parte de la Cooperativa de Ahorro y Crédito Credi Ya Ltda., los cuales fueron la base fundamental dentro del estudio del caso, pues

proporcionaron información relevante respecto al sistema de control interno y la seguridad de la información que maneja la institución.

Cuestionario

Para este estudio se utilizó un cuestionario para evaluar los componentes del sistema de control interno relacionado con la seguridad de la información, el cual está conformada por 42 preguntas cerradas categorizadas según el modelo COSO 2017. Este cuestionario ayudó a medir el nivel de confianza y riesgo inherente
que existe dentro de la institución.

Tabla 9. Cuestionario de control interno

Componente	Preguntas
Gobierno y cultura	¿El comportamiento y las decisiones de la Gerencia y los niveles de supervisión reflejan su compromiso en el cumplimiento de la ética y los valores?
	¿Se evalúa periódicamente el comportamiento de los colaboradores de acuerdo con las normas establecidas?
	¿Se revisa periódicamente el cumplimiento de las normas de confidencialidad en el personal de la institución?
	¿Se establecen supervisiones sobre el funcionamiento del sistema de control interno?
	¿Los procedimientos de control interno contribuyen al desarrollo de las actividades operativas de la institución?
	¿Se verifica el cumplimiento de las políticas y procedimientos en la ejecución de las actividades operativas de la institución?
	¿Cuentan con un manual de funciones con el perfil de competencias para cada cargo?
	¿Se realiza actividades de inducción y capacitación al personal?
	¿Existe segregación de funciones en los niveles institucionales?
	¿El desempeño del personal tanto técnico como administrativo es evaluado periódicamente?
Estrategia y establecimiento de objetivos	¿Los jefes departamentales apoyan en la fijación de los objetivos institucionales?
	¿Los objetivos institucionales están alineados con las normas que las regulan?

	¿La dirección identifica los recursos necesarios para alcanzar los objetivos?
	¿El plan estratégico institucional apoya al cumplimiento de los objetivos institucionales?
	¿Los objetivos establecidos son comunicados a todos los colaboradores de la institución de forma oportuna para su cumplimiento?
	¿Los objetivos departamentales están contemplados dentro del POA institucional?
Desempeño	¿Se evalúa el impacto que puede tener en el control interno realizar cambios en las tecnologías?
	¿Se analiza los riesgos derivados de fuentes externas como en lo económico, ambiental o tecnológico?
	¿Detecta los riesgos de fuentes internas relacionados con los sistemas de información en el caso de fallos que afecten la continuidad de las operaciones?
	¿La institución ha definido la administración de los riesgos identificados, en los parámetros de: asumir, mitigar, transferir, evitar o eliminar?
	¿Existen problemas informáticos que impidan la correcta realización de las operaciones?
	¿Se evalúa si son adecuados los sistemas de información en el desarrollo de las actividades?
	¿Se aumenta la capacidad de los sistemas informatizados para poder tratar volúmenes crecientes de información?
	¿Realiza un estudio preliminar para la adquisición o actualización de nuevos sistemas para el flujo de información?
	¿Se efectúa un seguimiento de las nuevas tecnologías o aplicaciones desarrolladas?
Revisar y ajustar	¿Se tienen alineados los controles de TI con los procesos de la organización y los controles generales?
	¿Los controles implementados están alineados con la reducción y gestión de los riesgos?
	¿Se han ejecutado los controles orientados a la infraestructura de TI?
	¿Han establecido perfiles de acceso a los usuarios en las herramientas tecnológicas de acuerdo con el rol desempeñado?

	¿Se han implementado controles de seguridad que protejan a la organización de un ataque informático externo?
	¿Se han implementado controles sobre el desarrollo, compra y mantenimiento de TI?
	¿Se han establecido controles orientados a la restricción de usuarios no autorizados?
	¿Las actividades de control que aplica la empresa se relacionan a controles preventivos, correctivos y detectivos?
	¿La aplicación de los procedimientos y las políticas cuentan con un responsable para su cumplimiento?
	¿Las políticas y procedimientos de la institución son revisados y ajustados periódicamente?
Información, comunicación y reporte	¿La información está disponible y es oportuna para permitir el control efectivo de las actividades?
	¿La información cumple con los principios de las normas ISO 27000: confidencialidad, integridad y disponibilidad de la información?
	¿Para cada reporte se tienen un control de validación que asegure que la información está completa?
	¿La información generada está directamente asociada con los objetivos institucionales establecidos?
	¿Los informes departamentales son entregados a la dirección de forma oportuna?
	¿La institución utiliza como medios de comunicación correos electrónicos, memorandos, Messenger interno?
	¿La gerencia toma en cuenta las recomendaciones de mejora aportadas por los empleados?

Fuente: Coopers & Lybrand (2007)
Elaborado por: Tibán (2022)

3.1.2.2- Fuentes de información secundaria

Se aplicó la técnica de la observación, a través de un check list para examinar, de manera cualitativa, el sistema de seguridad de la información de la institución que permitió identificar las vulnerabilidades presentes en la red, software o hardware que comprometan la confidencialidad de los datos. El check list estaba conformado por 45 preguntas clasificadas de acuerdo a las normas ISO/IEC 27002:2013.

Tabla 10. Check list

PREGUNTAS	SI	NO	OBSERVACIÓN
POLITICAS DE SEGURIDAD DE LA INFORMACION			
Dirección de gestión para la seguridad de la información			
¿La institución ha implementado políticas de seguridad de la información?			
¿Las políticas de seguridad de la información son aprobadas por la administración?			
¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?			
¿Se revisa frecuentemente las políticas de seguridad de la información?			
¿Se establecen responsabilidades para la revisión y evaluación de las políticas?			
GESTIÓN DE ACTIVOS			
Responsabilidad por los activos			
¿Disponen de un inventario de activos de información?			
¿Se ha definido responsabilidades en cuanto a los activos de información?			
¿Existen políticas relacionadas con el uso adecuado de los activos de información?			
¿Se ha definido un proceso para que los empleados devuelvan los activos de la institución que tienen a su cargo al terminar su contrato laboral?			
Clasificación de la información			
¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?			
Manejo de medios de almacenamiento			
¿Los soportes de almacenamiento están en un entorno seguro y protegido?			
¿Los datos se almacena en múltiples copias para reducir el riesgo de daño o perdida?			
CONTROL DE ACCESO			
Requisitos comerciales de control de acceso			
¿Existen políticas de control de acceso en función a la seguridad de la información?			

¿Las políticas se basan en los requerimientos de la institución?			
¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?			
Gestión de acceso de usuarios			
¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?			
¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?			
Control de acceso al sistema y a las aplicaciones			
¿Se controla los datos a los que puede acceder un usuario en particular?			
¿El acceso es protegido contra varios intentos de inicio de sesión?			
¿Las contraseñas de los usuarios se cambian regularmente?			
¿La selección de contraseñas son complejas?			
¿Se restringe el acceso al código fuente del programa de la institución?			
SEGURIDAD FISICA Y DEL ENTORNO			
Áreas Seguras			
¿Los perímetros del edificio de la institución son físicamente solidos?			
¿Existe un área de recepción para controlar el acceso físico al edificio?			
¿Implementan controles de acceso a áreas donde se almacena información confidencial de la institución?			
¿Mantienen seguridad en puertas, escritorios y archivadores de la institución?			
¿La información confidencial es visible desde el exterior de las instalaciones?			
¿Cuentan con un plan de seguridad para evitar daños por desastres naturales o ataques maliciosos a la institución?			
¿Las áreas donde el personal desarrolla sus actividades es segura?			
Equipo			
¿Los equipos esta ubicados en sitios adecuados para reducir el acceso innecesario a las áreas de trabajo?			

¿Las instalaciones de almacenamiento están protegidas para evitar accesos no autorizados?			
¿Los equipos están protegidos contra interrupciones causadas por fallas en los servicios públicos (electricidad, telecomunicaciones, agua)?			
¿El cableado está protegido contra interceptaciones, interferencias o daños?			
¿Cuentan con una programación de mantenimiento de los equipos informáticos?			
¿Se identifica a los usuarios que se les permite la salida de los activos fuera de la institución?			
¿Se mantiene un control a los activos que están fuera de las instalaciones?			
SEGURIDAD DE LAS OPERACIONES			
Protección contra malware			
¿Se implementan controles para evitar el uso de sitios web maliciosos o sospechosos?			
Copia de seguridad			
¿Las copias de seguridad se almacenan en un lugar seguro?			
SEGURIDAD EN LAS COMUNICACIONES			
Gestión de la seguridad de la red			
¿Las redes son administradas y controladas para proteger la información de la institución?			
¿Se monitorea periódicamente la capacidad del proveedor de servicios de red?			
GESTION DE INCIDENTES			
Gestión de incidentes y mejoras de seguridad de la información			
¿Se establecen responsabilidades para desarrollar los procedimientos establecidos en la institución?			
¿Se reportan eventos o incidentes de seguridad de la información?			
¿Se notifica cualquier debilidad de seguridad observada en los sistemas o servicios?			
¿Se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente?			
¿Los incidentes de seguridad de la información se responden de acuerdo con los procedimientos establecidos?			

Fuente: ISO/IEC 27002:2013
Elaborado por: Tibán (2022)

3.2.- Método de análisis de información

La investigación al ser un estudio de caso se enfoca en una situación específica por lo tanto es considerado como un análisis particularista debido a que revela las circunstancias de la seguridad de la información y lo que podría representar para la institución, esto puede ser de apoyo para el lector que pase por una situación similar. También es considerado heurístico ya que con el análisis realizado surgen conocimientos sobre cómo las cosas llegan a ser en realidad a partir del estudio de caso, lo que ayuda a explicar las razones del problema, los antecedentes de la situación y lo que sucedió.

De igual manera se lo considera un análisis descriptivo, pues se realizó una descripción completa de lo que está sucediendo en la institución relacionado con la seguridad de la información, por lo general tiene un enfoque cualitativo, se basa en varias preguntas de investigación y se utilizan técnicas literarias para ilustrar los sucesos desde diferentes puntos de vista. En definitiva, el estudio de caso es más concreto, representa el conocimiento aprendido en base a la experiencia vivida con el propósito de establecer un tema de discusión y debate.

En el cuestionario de control interno efectuado se categorizaron las 42 preguntas realizadas con los criterios definidos. Para la clasificación, se ubicaron en las categorías establecidas de acuerdo con los componentes del COSO 2017:

- Gobierno y cultura
- Estrategia y establecimiento de objetivos
- Desempeño
- Revisar y ajustar
- Información, comunicación y reporte

Esta técnica permite evaluar la efectividad de la gerencia y los colaboradores de la institución, como se observa en la tabla 11, se contabilizó las respuestas de Si y No de tal manera que se logró identificar la gestión que lleva la institución para resguardar los sistemas de información.

Tabla 11. Formato cuestionario de control interno

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
PERIODO 2021

N°	PREGUNTAS	SÍ	NO	Fecha
1				
2				
3				
4				
5				
6				
7				
	TOTAL	**0**	**0**	

Grado de confianza del control interno:
ALTO ( ) MODERADO ( ) BAJO ( )

Comentarios adicionales:

Responsable de la evaluación:

_____	_____	_____
Iníciales	**Fecha**	**Firma**

Elaborado por: Tibán (2022)

Una vez categorizado las preguntas, se procedió a ponderar las respuestas de cada componente, como se muestra en la Tabla 12, en base a ello se calculó el nivel de confianza y el nivel de riesgo inherente, aplicando la siguiente fórmula:

$$\boldsymbol{Nivel\ de\ Confianza} = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$\boldsymbol{Nivel\ de\ Riesgo} = 100 - Nivel\ de\ confianza$$

Tabla 12. Formato matriz de calificación del nivel de confianza y riesgo

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
MATRIZ DE CALIFICACIÓN DEL NIVEL DE CONFIANZA Y RIESGO
PERIODO 2021

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN			
CALIFICACIÓN TOTAL = CT			0
PONDERACIÓN TOTAL = PT			0
NIVEL DE CONFIANZA: NC= CT/PT x 100			0%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			0%

Elaborado por: Tibán (2022)

Para determinar si los niveles calculados son altos o bajos, se utilizaron los siguientes parámetros:

NIVEL DE CONFIANZA		
BAJO	**MODERADO**	**ALTO**
15% - 50%	51% - 75%	76% - 95%
85% - 50%	49% - 25%	24% - 5%
ALTO	**MODERADO**	**BAJO**
NIVEL DE RIESGO		

De igual manera se aplicó indicadores de gestión relacionados con la seguridad de la información, clasificados en indicadores de eficiencia para evaluar el nivel de ejecución de los procesos establecidos y los indicadores de eficacia que mide el cumplimiento de los resultados propuestos por la administración de la institución en cuanto a la seguridad de la información.

Tabla 13. Indicadores de gestión

INDICADORES DE EFICIENCIA		
Organización de Seguridad de la Información		
Descripción de Variables		**Fórmula**
OI01: Número de personas que asisten a las capacitaciones		(OI01/OI02)*100
OI02: Número total del personal de la entidad		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Plan de Sensibilización		
Descripción de Variables		**Fórmula**
PS01: Número de fallas o no cumplimientos		(PS01/PS02)*100
PS02: Total de personal a capacitar		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Cubrimiento del SGSI en activos de información		
Descripción de Variables		**Fórmula**
AC01: Número de activos clasificados como críticos de información		(AC01/AC02)*100
AC02: Número total de activos identificados		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Perfil de usuarios		
Descripción de Variables		**Fórmula**
PU01: Número de usuarios con perfiles de acuerdo a su cargo		(PU01/PU02)*100
PU01: Total de usuarios		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Infraestructura tecnológica		
Descripción de Variables		**Fórmula**
IT01: Número de equipos tecnológicos activos		(IT01/IT02)*100
IT02: Total de equipos tecnológicos		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
INDICADORES DE EFICACIA		
Implementación de controles		
Descripción de Variables		**Formula**
IC01: Número de controles implementados		(IC01/IC02)*100
IC02: Número de controles que se planearon implementar		
Metas		

Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Protección de servidores		
Descripción de Variables		**Fórmula**
SI01: Número de servidores con antimalware		(SI01/SI02)*100
SI02: Total de servidores		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Sistema operativo		
Descripción de Variables		**Fórmula**
SO01: Número de servidores con versiones de sistema operativo actualizado		(SO01/SO02)*100
SO02: Total de servidores		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Controles de seguridad		
Descripción de Variables		**Fórmula**
CS01: Número de controles de seguridad efectivos		(CS01/CS02)*100
CS02: Total de controles de seguridad		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%
Configuración de seguridad		
Descripción de Variables		**Fórmula**
GC01: Número de equipos con estándares de configuración segura		(GC01/GC02)*100
GC02: Total de equipos		
Metas		
Mínima: 60-75%	Satisfactoria: 76-90%	Sobresaliente: 91-100%

Fuente: Ministerio de las tecnologías de la información y las comunicaciones (2015)
Elaborado por: Tibán (2022)

Por otra parte, para el check list se analizó los factores que afectan a la seguridad física, lógica y la seguridad de la información, en base a las normas ISO/IEC 27002:2013. Lo cual se reflejó los resultados en una gráfica de barras para medir el nivel de cumplimiento de la institución. Cabe destacar que el estudio se realizó sin alterar o manipular ninguna de las variables, donde se limitó solo a la medición y descripción de estas, pues la información proviene directamente del grupo de estudio.

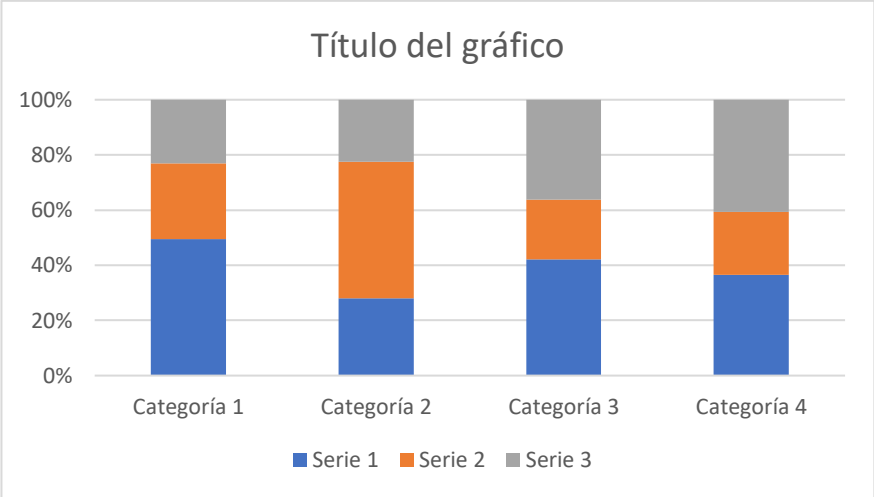

Gráfico 6. Formato nivel de cumplimiento
Elaborado por: Tibán (2022)

En el mismo sentido se definió los activos de información que posee la institución, esto se logró a través de entrevistas realizadas al personal del departamento de sistemas y mediante la técnica de la observación al realizar las visitas al departamento. Cada activo se clasificó por categorías y se valoró de acuerdo con los principios de confidencialidad, integridad y disponibilidad a través de una escala de valoración establecida, con el fin de identificar las amenazas y vulnerabilidades que pongan en peligro la estabilidad de la institución. Cada activo se clasificó por categorías y se valoró de acuerdo a los principios de confidencialidad, integridad y disponibilidad a través de una escala de valoración establecida, con el fin de identificar las amenazas y vulnerabilidades que pongan en peligro la estabilidad de la institución.

Tabla 14. Formato de los activos de información

TIPO	CATEGORÍA	ACTIVO	VALORACIÓN DE ACTIVOS		
			C	I	D

Elaborado por: Tibán (2022)

Además, se presentó en un mapa de calor los riesgos a los que está expuesto la institución, los que tienen mayor impacto en el tratamiento de la información, en el cual se refleja el impacto y la probabilidad de ocurrencia de los activos de información frente a las amenazas. Estos se miden en una escala que va del 1 al 9 y están representados por un color, donde 1-2 es bajo, 3-4 es apreciable, 5-6 es importante y 7-9 se define como crítico.

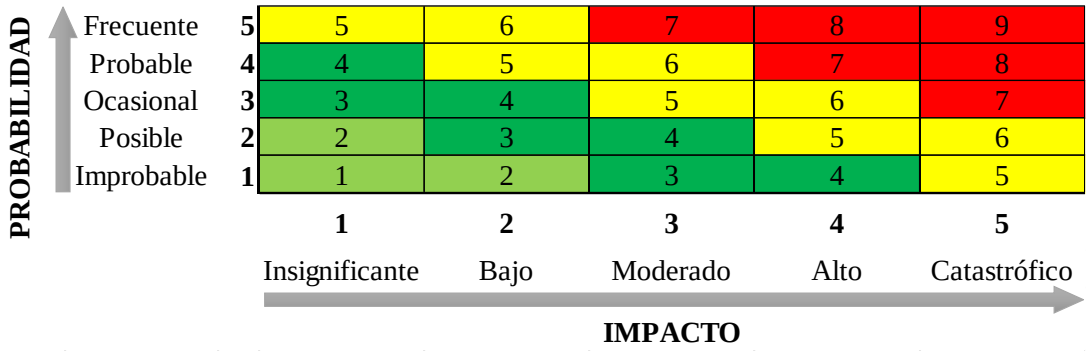

Gráfico 7. Estructura de la matriz de riesgo
Elaborado por: Tibán (2022)

De igual manera se definió un tratamiento del riesgo como se muestra en la Tabla 15, donde se identifica el activo, el nivel de riesgo y se proponen medidas de control a tomar en cuenta, el tipo de control ya sea preventivo, detectivo o correctivo según el caso, también la frecuencia y los responsables de la aplicación de los controles con el fin de minimizar el riesgo y su impacto negativo en la institución.

Tabla 15. Formato administración del riesgo

Activo	Nivel de riesgo	ADMINISTRACIÓN DEL RIESGO				
		Nivel de administración del riesgo	Medidas de control propuesta	Tipo de control	Frecuencia	Responsable

Elaborado por: Tibán (2022)

CAPÍTULO IV

DESARROLLO DEL ANÁLISIS DE CASO

4.1.- Análisis y categorización de la información

Al tratarse de una cooperativa que ofrece servicios financieros, se consideran indispensables a los clientes, los procesos operativos y los empleados que forman parte de la institución. En este sentido se definió que el equipo que participa en los grupos focales para el desarrollo del presente estudio de caso corresponde a las personas encargadas del departamento de sistemas que tienen experiencia y conocimiento del tema a tratar, quienes contribuyeron en la recolección de información a través de los instrumentos y técnicas de investigación utilizadas para el efecto. Adicionalmente se incluyó al auditor interno que forma parte de la institución el mismo que apoyó en la realización del análisis del caso.

A continuación, son presentados los datos recopilados y resultados obtenidos de la aplicación de la evaluación al Sistema de Control Interno del departamento de Seguridad de la Información, referente al estudio de caso de la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

4.1.1.- Sistema de seguridad de la información

Al examinar el sistema de seguridad de la información de la cooperativa a través de la utilización del instrumento planteado en la metodología que es el check list, el mismo fue elaborado de acuerdo con los estándares establecidos en la norma ISO/IEC 27002:2013, permitió verificar el nivel de su cumplimiento en lo que respecta a las normas aplicables a las actividades de la institución según se muestra en el Gráfico 10.

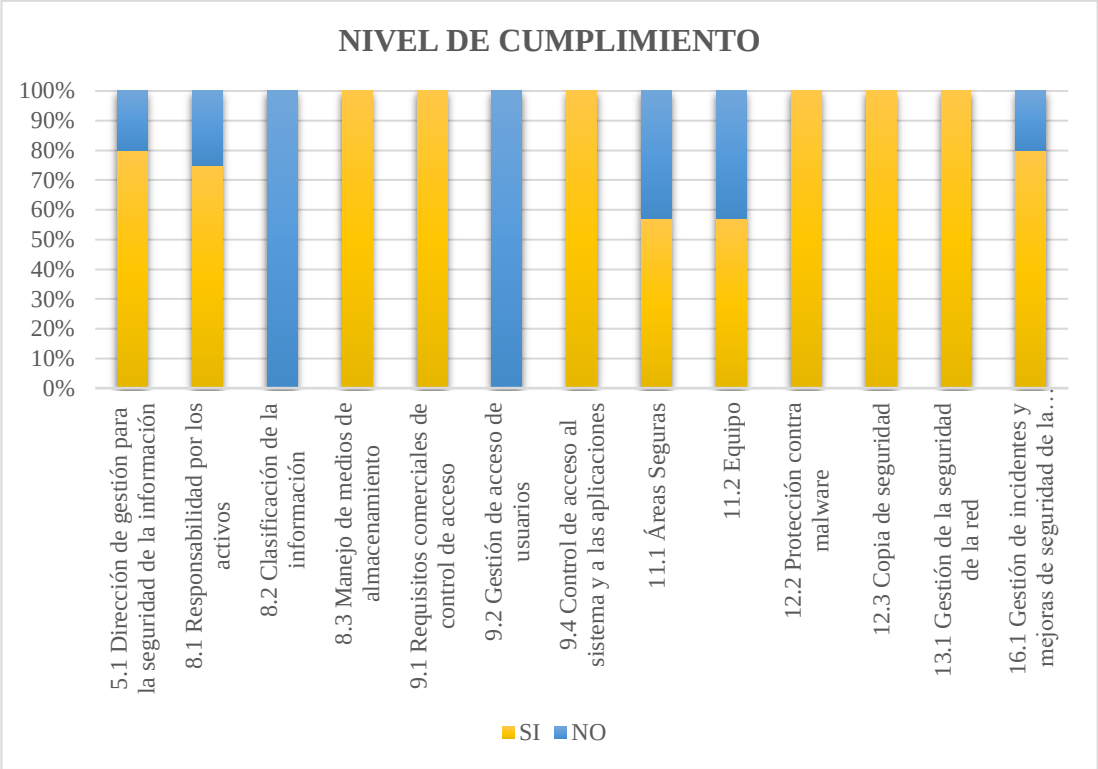

Gráfico 8. Nivel de cumplimiento
Fuente: COAC Credi Ya Ltda.
Elaborado por: Tibán (2022)

Como se puede notar en la gráfica, la mayoría de las normas tienen un alto nivel de cumplimiento por parte de la institución en los aspectos relacionados con la seguridad de la información. Sin embargo, existe falencias en cuatro puntos débiles identificados como: la clasificación de la información en términos de valor, criticidad y sensibilidad a la divulgación, la gestión de acceso de usuarios autorizados, áreas seguras y equipos en los cuales se evidencia que las dos primeras no se cumplen, mientras que en las dos siguientes se cumplen en un 50%. En definitiva, a nivel general la institución presentó en promedio, un nivel de cumplimiento del 73%, lo que representa un nivel favorable para gestión de la seguridad de la información, sin embargo, se necesita implementar acciones para prevenir los riesgos que pongan en peligro a la institución.

Otra particularidad relevante a la seguridad de la información fue la identificación de los activos de información de la institución, en el que se realizó un análisis de riesgos con base en la metodología MAGERIT. El cual permitió identificar los activos más importantes destinados al tratamiento de la información, las amenazas y

vulnerabilidades presentes. A partir de ello, se estableció una valoración a los mismos para medir el nivel de gravedad en los activos considerando los principios de confidencialidad (C), integridad (I) y disponibilidad (D), este va del 0 al 3, en el cual 0 no es aplicable y 3 representa un alto nivel de riesgo que afectaría al desarrollo de las operaciones, como se muestra en la Tabla 16.

Tabla 16. Activos de información

TIPO	CATEGORÍA	ACTIVO	VALORACIÓN		
			C	I	D
Sitio Web	Aplicaciones	https://www.crediya.fin.ec/	0	1	2
Datos y/o Información	Datos	Base de datos de los clientes	3	2	2
		Data de créditos			
		Balances			
Sistema operativo	Aplicaciones	Softbank	3	3	2
Equipamiento informático	Tecnología	Computadoras	0	1	2
		Switch			
		Router			
		Disco externo			
		Impresoras			
Red de comunicaciones	Tecnología	Internet	0	1	2
		Red de datos interna			
		Red local			
		Red telefónica			
Equipamiento auxiliar	Tecnología	UPS	0	1	2
		Cámaras de seguridad			
		Proyector			
		Radio sonido			
Servicios externos	Servicio subcontratado	Telconet	1	1	1
		APP Recaudaciones			
Instalaciones	Instalaciones	Centro de control	0	1	2
Personal	Personal	Jefe de sistemas	0	0	1
		Técnico de sistemas			

Fuente: COAC Credi Ya Ltda.
Elaborado por: Tibán (2022)

Como se observa, el sistema operativo softbank, las bases de datos de los socios y toda la información financiera que manejan, han sido considerados los activos más vulnerables en lo que concierne al principio de Confidencialidad, debido a que contiene información privada y sensible por lo que están expuestos a que pueda ser divulgada o en cierto momento se pierda su protección, lo cual de materializarse la amenaza presente podría causar problemas en el desarrollo de las operaciones institucionales afectando al prestigio de la institución y la confianza de sus socios. En cambio, los activos relacionados con la tecnología informática están propensos a recibir ataques que perjudiquen a su sistema o a la red, afectando al principio de Disponibilidad, debido a que personas no autorizadas podrían tener acceso.

Además, se elaboró una lista de las principales amenazas que pueden interferir en la seguridad de dichos activos a los que se enfrenta la institución, con el fin de valorar las vulnerabilidades y el impacto que tendrían los activos frente a las amenazas (ver Anexo 2) para implementar actividades de mejora que ayuden a minimizarlo. Estas se clasificaron de acuerdo a su nivel de ocurrencia como:

1. Improbable: fuego, inundación
2. Posible: contaminación, interrupción del suministro eléctrico, interrupción de las redes de comunicación, robo de dispositivos o soportes
3. Ocasional: errores de usuario
4. Probable: errores del software

Tabla 17. Valoración de amenazas de los activos de información

ACTIVOS	**AMENAZAS**			
	1	**2**	**3**	**4**
Datos	2	2	2	1
Aplicaciones	1	1	2	1
Tecnología	2	2	1	1
Servicio subcontratado	0	1	1	0
Instalaciones	2	1	0	0
Personal	0	0	2	0

Elaborado por: Tibán (2022)

Se valoró de acuerdo a una escala establecida para medir el nivel de vulnerabilidad, si es alta (3), media (2), baja (1) o nula (0) como se muestra en la Tabla 17. De esto se deduce que los datos y el equipamiento tecnológico como los equipos, la red de comunicaciones y el equipamiento auxiliar que posee la institución son más vulnerables a las amenazas de tipo ambiental como al fuego e inundación y a amenazas externas como la interrupción del suministro eléctrico o las redes de comunicación. Por lo que se necesita que la administración de la institución preste mayor atención a estos resultados y tome acciones que ayuden a reducir su impacto.

Una vez identificado y valorado los activos de información y las amenazas que pueden afectar a cada uno, se calcula su nivel de impacto en base a la valoración establecida de los activos de información reflejada en la Tabla 16, junto con la calificación de las vulnerabilidades establecida en la Tabla 17. A partir de ello se calculó el impacto basado en el siguiente índice:

1. Insignificante
2. Bajo
3. Moderado
4. Alto
5. Catastrófico

Tabla 18. Nivel de impacto

ACTIVOS	**AMENAZAS**			
	1	**2**	**3**	**4**
Datos	3	3	3	2
Aplicaciones	2	2	3	2
Tecnología	2	2	1	1
Servicio subcontratado	0	1	1	0
Instalaciones	2	1	0	0
Personal	0	0	2	0

Elaborado por: Tibán (2022)

Como se puede notar las bases de datos y las aplicaciones como el sitio web y el sistema operativo de la institución, son propensas a amenazas como los desastres naturales, interrupción del suministro eléctrico, de las redes de comunicación, entre otros. Lo que causaría que las operaciones sean detenidas por un lapso de tiempo, y provocaría que la prestación de los servicios efectuados tenga complicaciones y no funcionen de manera eficiente.

Con los valores obtenidos para cada activo se calculó el riesgo para cada amenaza, que será en función de la probabilidad de ocurrencia y el nivel de impacto que producirá sobre el activo identificado en la Tabla 16. El objetivo es cuantificar el nivel de riesgo para poder establecer una comparación entre distintos activos, para ello se identifica una escala de valoración del riesgo, el cual puede ser:

- 0-2: Bajo
- 3-4: Apreciable
- 5-6: Importante
- 7-9: Crítico

Tabla 19. Nivel de riesgo

ACTIVOS	**AMENAZAS**			
	1	**2**	**3**	**4**
Datos	3	4	5	5
Aplicaciones	2	3	5	5
Tecnología	2	3	3	4
Servicio subcontratado	0	2	3	0
Instalaciones	2	2	0	0
Personal	0	0	4	0

Elaborado por: Tibán (2022)

Se puede notar que, en la institución, el riesgo detectado en los activos de información no ha llegado a un nivel crítico, sin embargo, se identificó riesgos importantes en la base de datos y en las aplicaciones respecto a las amenazas relacionadas con los errores del software y del usuario en la manipulación de la información. En definitiva, se deberán atender de forma prioritaria estas amenazas y destinar los recursos necesarios

para minimizar el impacto y el efecto que puede traer a la institución. Por otra parte, se podría asumir como apetito de riesgo aquellos que representan un nivel bajo, ya que la institución está en la capacidad de afrontar estos riesgos para alcanzar sus objetivos.

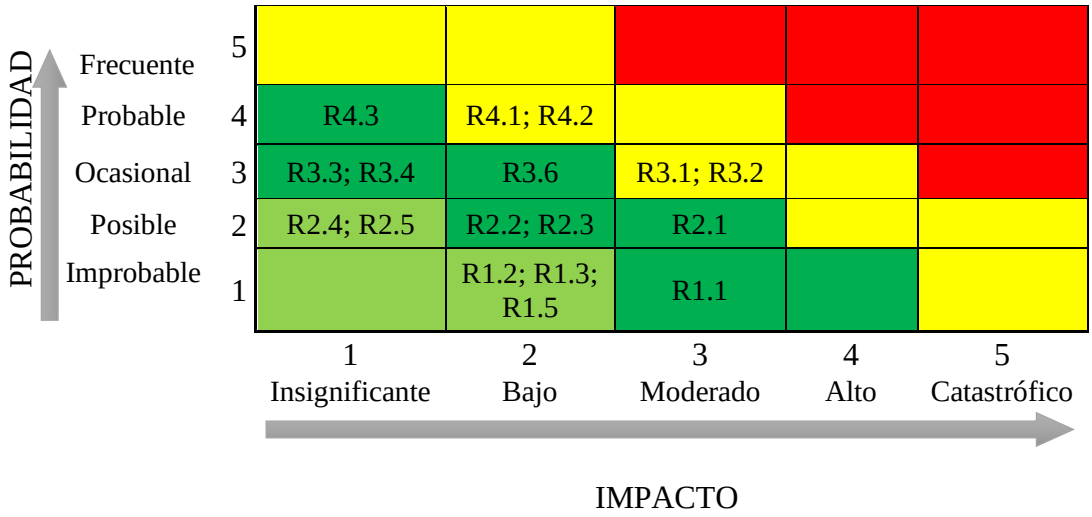

Gráfico 9. Matriz de riesgo
Elaborado por: Tibán (2022)

Aplicando este método se obtuvo un mapa de riesgo, donde se identificó a los activos de información con mayores riesgos y las amenazas que están ocasionando los mismos. En este caso, la institución no está expuesta a riesgos significativos, pues se midió un nivel de riesgo bajo, apreciable e importante, los cuales pueden ser tolerables. Además, se estableció un tratamiento del riesgo, en el que se decidió si se va a asumir, a mitigar, a transferir o a eliminar según la gravedad del riesgo y se propuso medidas de control que pueden tomar en cuenta para reducir su impacto.

Tabla 20. Administración del riesgo

ACTIVO	Nivel de riesgo	ADMINISTRACIÓN DEL RIESGO				
		Nivel de administración del riesgo	Medidas de control propuesta	Tipo de control	Frecuencia	Responsable
Sitio Web	Apreciable	Asumir	Realizar pruebas al sitio web para detectar falencias	Preventivo/Detectivo	Mensual	Departamento de sistemas
Datos y/o Información	Importante	Mitigar	Controlar los accesos al sistema de la base de datos	Detectivo/Correctivo	Diario	Departamento de sistemas
Sistema operativo	Importante	Mitigar	Monitoreo frecuente del software	Preventivo	Semanal	Departamento de sistemas
Equipamiento informático	Apreciable	Mitigar	Efectuar frecuentemente respaldos de información	Preventivo	Diario	Departamento de sistemas
Red de comunicación	Apreciable	Mitigar	Realizar rastreos de movimientos inusuales en el sistema	Preventivo/Detectivo	Diario	Departamento de sistemas
Equipamiento auxiliar	Apreciable	Asumir	Informar al departamento de sistemas cuando ocurre fallos en los equipos	Preventivo/Detectivo	Diario	Personal de la institución
Servicios externos	Apreciable	Asumir	Verificar el correcto funcionamiento de los servicios	Preventivo	Semanal	Personal de la institución
Instalaciones	Bajo	Asumir	Establecer un plan de contingencia frente a incidentes de seguridad	Preventivo/Detectivo	Semestral	Gerencia / Departamento de sistemas
Personal	Apreciable	Asumir	Realizar capacitaciones al personal sobre el adecuado manejo de la información	Preventivo	Semestral	Gerencia / Sistemas

Elaborado por: Tibán (2022)

4.1.2.- Administración del sistema de control interno

La implementación del sistema de control interno en las empresas promueve la optimización de los recursos y facilita el nivel de gestión en el desarrollo de las operaciones. En este caso, a través del modelo COSO 2017 se estudió el nivel de confianza (N.C) y riesgo inherente (R.I) de la institución, en el cual se evaluó los controles y la seguridad de la estructura organizacional.

Tabla 21. Nivel de confianza y nivel de riesgo

Componentes del Control Interno	Nivel de confianza y riesgo		Riesgo	Argumento
Gobierno y cultura	N.C	80%	Alto	La institución no revisa periódicamente el cumplimiento de las normas de confidencialidad en el personal.
	R.I	20%	Bajo	
Estrategia y establecimiento de objetivos	N.C	83%	Alto	Los objetivos establecidos no son comunicados a todos los colaboradores de la institución de forma oportuna para su cumplimiento
	R.I	17%	Bajo	
Desempeño	N.C	67%	Moderado	No se realizan planes sobre la mitigación de los riesgos, ni se evalúa el impacto que tiene.
	R.I	33%	Moderado	
Revisar y ajustar	N.C	80%	Alto	Las políticas y procedimientos implementados en la institución no se revisan periódicamente.
	R.I	20%	Bajo	
Información, comunicación y soporte	N.C	86%	Alto	No se toma en cuenta las recomendaciones de mejora aportado por los empleados.
	R.I	14%	Bajo	

Elaborado por: Tibán (2022)

Como resultado, se denota el buen desempeño de la administración en el manejo de las operaciones de acuerdo con los objetivos establecidos. Esto se ve reflejado en el nivel de riesgo calificado como bajo; sin embargo, en el componente Desempeño se detectan vulnerabilidades en la administración de los riesgos y el impacto que esto tiene en el control interno, cuyo nivel de confianza representa el 67% y por diferencia el riesgo inherente es del 33%, calificándose como Moderado. Puesto que todavía es una institución que va en crecimiento y poco a poco es reconocida por la sociedad, no

se ha visto inmersa en circunstancias graves, razón por la cual no se da como prioridad en análisis de los riesgos.

Tabla 22. Indicadores de eficiencia

Indicador	Cálculo	Interpretación
Organización de Seguridad de la Información	Personas que se capacitan / Total del personal	Se ha capacitado a gran parte del personal en cuanto a la seguridad de la información
	71%	
Plan de sensibilización	Fallas o no cumplimientos / Personal a capacitar	Se ha mantenido un buen control de los incidentes de seguridad
	80%	
Cubrimiento del SGSI en activos de información	Activos de información críticos / Total de activos	Los nuevos activos de información se han incluido favorablemente con sus respectivos controles
	94%	
Perfil de usuarios	Perfiles de cargo adecuados / Total de usuarios	Los perfiles de cargo se establecieron de acuerdo a la función que desempeñan los usuarios
	94%	
Infraestructura tecnológica	Equipos tecnológicos activos / Total de equipos	La institución no cuenta con equipos tecnológicos obsoletos o que no estén en uso
	97%	

Elaborado por: Tibán (2022)

Para profundizar más el estudio se realizó una evaluación a la seguridad de la información a través de indicadores de eficiencia y eficacia para hacer un seguimiento de la asignación de los recursos y responsabilidades en la administración de la seguridad. En definitiva, no se ve enmarcado el compromiso de la institución en la seguridad de la información, dado que existe desconocimiento por parte del personal en temas relacionados con la confidencialidad de la información, lo que refleja un indicador del 71%, al igual que la falta de un plan de capacitación y sensibilización previamente definido con el fin de promover el control frente a incidentes de seguridad.

Tabla 23. Indicadores de eficacia

Indicador	Cálculo	Interpretación
Implementación de controles	Controles implementados / Controles planeados	Los controles programados se han ejecutado en el tiempo establecido
	97%	
Protección de servidores	Servidores con antimalware / Total de servidores	Todos los servidores de la institución tienen protección contra virus
	100%	
Sistema operativo	Sistema operativo actualizado / Total de servidores	Los servidores cuentan con versiones del sistema operativo actualizado
	100%	
Controles de seguridad	Controles efectivos / Total de controles	Los controles de seguridad implementados han sido efectivos
	93%	
Configuración de seguridad	Eq. con configuración segura / Total de equipos	Todos los equipos tienen los estándares de configuración segura
	100%	

Elaborado por: Tibán (2022)

Por otra parte, en lo referente a los indicadores de eficacia, se demuestra la capacidad de la institución de alcanzar lo que se propone, debido a que en lo que concierne a la protección de los servidores y actualizaciones del sistema operativo, todos los equipos cuentan con protección contra virus, estándares de configuración segura y versiones del sistema operativo actualizado, lo que les permite mantener un nivel de seguridad apropiado. De igual manera la implementación de controles se ha efectuado favorablemente, ya que todos los controles que se han planificado efectuar, han sido ejecutados en el tiempo establecido.

En definitiva, tras la evaluación realizada al sistema de seguridad de la información y a los controles interno de la institución, se han detectado ciertas vulnerabilidades, por lo que se detalla cada uno de ellos, como se demuestra en la Tabla 24, donde se establece la condición, causa y efecto encontrado, y se proponen recomendaciones que pueden tener en cuenta para la mejora de sus procesos.

Tabla 24. Hoja de hallazgos

ACTIV.	ATRIBUTOS	COMENTARIOS	RECOMENDACIÓN
Nivel de Cumplimiento	**CONDICIÓN**	Se identificaron falencias en los controles relacionados con la clasificación de la información, gestión de acceso de usuarios, áreas seguras y en los equipos.	Establecer un plan de seguridad para evitar las amenazas a las que la institución se encuentra expuesta
	CAUSA	Falta de un proceso formal para administrar la información en base a su valor y sensibilidad a la divulgación y establecer controles de protección asociados a los mismos	
	EFECTO	El nivel de riesgo podría ir en aumento afectando al tratamiento de la información	
Activos de Información	**CONDICIÓN**	Los equipos informáticos no se encuentran con la debida protección en lo que tiene que ver con la climatización y el cableado.	Implementar un sistema de climatización para controlar la temperatura de los equipos y verificar la adecuación del cableado para evitar daños
	CAUSA	No se lleva una clasificación de los activos considerando los principios de confidencialidad, integridad y disponibilidad	
	EFECTO	Deficiente manejo y control de los recursos de la institución	
Gobierno y Cultura	**CONDICIÓN**	Ausencia de procesos formales hacia el personal sobre el resguardo de la información que se maneja dentro de la institución	Implementar normas de confidencialidad en el personal para proteger la información que se maneja, además de asignar a una persona responsable de medir y evaluar periódicamente las capacidades del personal
	CAUSA	Falta de precaución y control por parte del personal en el manejo de la información y de datos importantes	
	EFECTO	Inconsistencias en la información presentada para la toma de decisiones	
Estrategia y Establecimiento de Objetivos	**CONDICIÓN**	Los objetivos establecidos no se comunican oportunamente a todos los colaboradores de la institución para su cumplimiento	Establecer un medio de comunicación específico para poner en conocimiento al personal acerca de la creación, actualización o modificación de los objetivos, normas o reglamentos.
	CAUSA	Falta de responsabilidad por parte del personal en la revisión, actualización y comunicación de los objetivos institucionales	
	EFECTO	Los objetivos establecidos no pueden ser alcanzables para brindar una mejora continua a los procesos.	

Desempeño	**CONDICIÓN**	Falta de administración de los riesgos identificados, en los parámetros de: asumir, mitigar, transferir, evitar o eliminar	Establecer controles para la gestión de los riesgos detectados e identificar su nivel de gravedad
	CAUSA	No se evalúa el impacto que tienen los riesgos en cada uno de los procesos de la institución	
	EFECTO	Los riesgos no se mitigaron como se esperaba y los procesos de la institución se pueden paralizar	
Revisar y Ajustar	**CONDICIÓN**	Las políticas y procedimientos de la institución no se revisan y ajustan periódicamente	Asignar a una persona responsable de supervisar el cumplimiento de las políticas y procedimientos de la institución y de ser el caso actualizarlas
	CAUSA	No se ha designado un encargado de evaluar y analizar el funcionamiento y cumplimiento de las políticas y procedimientos de la institución	
	EFECTO	Incumplimiento a las políticas y procedimientos de la institución por parte del personal.	
Información, Comunicación y Reporte	**CONDICIÓN**	No se toma en cuenta las recomendaciones de mejora aportado por los empleados	La administración de la empresa debería influir en los empleados para generar un buen ambiente de trabajo y que sean de apoyo para la toma de decisiones
	CAUSA	Falta de comunicación entre los departamentos y niveles institucionales	
	EFECTO	Las decisiones tomadas no complementan en su totalidad las necesidades de la institución	
Nivel de Eficiencia y Eficacia	**CONDICIÓN**	Falta de capacitación al personal en cuanto a la seguridad de la información	Implementar un plan de capacitación a todo el personal de la institución para poner en conocimiento la importancia de la información y las medidas de seguridad aplicables.
	CAUSA	Descuido del personal en el manejo de contraseñas y claves de acceso al sistema	
	EFECTO	Pérdida, eliminación o robo de la información de la institución	

Elaborado por: Tibán (2022)

4.2.- Narración del caso

¿De qué manera actualmente la institución asegura la confidencialidad de la información?

Para proporcionar protección a los datos sensibles, en la institución se cuenta con una identificación de cada usuario y se le proporciona una contraseña única para acceder al sistema, de acuerdo con las funciones que desempeña. Si por algún motivo se viola este método de control, el usuario afectado informará inmediatamente al departamento de sistemas, para tomar acciones correctivas. Como se deduce de las palabras del jefe de sistemas:

> La información está disponible para el usuario que lo desea dentro de los horarios establecidos. Hay controles para decir en qué momento pueden disponer de la información y obviamente dependiendo de los perfiles que tengan. Por ejemplo, el departamento financiero todo lo que es contabilidad, el departamento de negocios todo lo que tiene que ver con créditos e inversiones.

Por otra parte, para asegurar el flujo normal de la información y que no exista interferencias en la transmisión del mensaje, se establececiero medios de comunicación internos entre el personal de la institucion para facilitar la información requerida. Pues como menciona, "Damos prioridad o establecemos como métodos de comunicación el correo electrónico, y si le ponemos en escalas sería el 50%, seguido de WhatsApp con el 30%, Skype 15% y por último los memorándums en un 5%". Por otro lado, respecto al principio de integridad se asegura que la información proporcionada sea completa y se mantenga su contenido sin ninguna modificación, por lo que indica que:

> Normalmente cuando nos piden información o anexos, primero lo extraemos directamente de la base de datos y en el correo se les manifiesta la información en el formato solicitado, que efectúen las revisiones que correspondan e indiquen si existen alguna novedad, caso contrario se da por aceptada la información que cumple con los requerimientos.

¿El centro de procesamiento de datos detecta filtración de la información por personas no autorizadas?

Actualmente, en la institución no se ha detectado ataques a su sistema y ningún intento de acceso a la información sin previa autorización. Aunque no se han implementado actividades de control para esta situación, se han tomado en cuenta otras medidas para salvaguardar los datos, como lo indica:

> Tenemos dos herramientas: el antivirus, se realiza un monitoreo frecuente de su estado, como están los equipos, cual está más contaminado y los problemas que están teniendo. La otra también es con Telconet, quienes tienen la seguridad perimetral, tenemos acceso a los equipos y ocasionalmente hacemos revisiones para ver su estado, que equipos está consumiendo más el ancho del internet y todo eso. Pero no lo hemos hecho de tal forma que una persona se haga cargo de esto, lo revisa y al fin de mes se presenta un informe, que es lo ideal, y estamos apuntando a ello.

El alcance de los fraudes informáticos está llegando hasta el sector financiero, afectando a los bancos y cooperativas que son más reconocidas en el sector, sin embargo, en la institución hasta el momento no ha pasado por un acontecimiento desfavorable debido a que no ha existido problemas con el sistema, todos los servicios que ofrece se mantienen estables y no se han presentado reportes de algún incidente en el que se haya tenido que detener las operaciones.

> Existen novedades pequeñas a veces más por el desconocimiento del usuario interno dentro de las aplicaciones, de ahí no habido un incidente grave en el que hayamos tenido que paralizar las operaciones. Lo que más hemos parado es en los cortes de energía porque no hay un UPS, pero son solo 10 minutos. Acá también los cortes de energía no son permanentes y no habido un incidente relevante. Tal vez al inicio había cambios en la migración de datos, presentaban retardos en algunos servicios propios del sistema hasta que el personal se vaya adecuando.

¿Cuál es el grado de eficiencia y eficacia del control interno?

El sistema de control interno aporta un nivel de seguridad razonable para la consecución de los objetivos, y proporciona eficiencia en las operaciones. La institución, por ejemplo, posee manuales de procedimientos adecuados a cada departamento, pues cada manual es discutido y aprobado por el consejo de administración quienes certifican la validez de los documentos. De igual manera, implementaron varios formularios y fichas de control, respecto a la seguridad de la información como:

- Formulario de control de usuario
- Solicitud de restauración de respaldos de información
- Inventario de infraestructura tecnológica
- Ficha técnica de equipos de computo
- Hoja de vida del recurso informático
- Formulario de traslado o cambio de activo fijo
- Formulario para solicitud de servicios o requerimientos
- Bitácoras de respaldo de información de usuario

Se han establecido controles enfocados a cada nivel organizacional con el fin de establecer funciones orientadas a cada actividad de negocio. Por ejemplo, el departamento de sistemas tiene como función el diseño, implementación y administración de redes y comunicaciones, mantenimientos de la red interna y la administración de los sistemas y bases de datos. En cuanto al analista de operaciones, se encarga de receptar, archivar y custodiar los documentos de valor como pagares, escrituras, garantías y bienes prendarios que respaldan los créditos y otros documentos de propiedad de la institución.

Respecto al departamento de negocios, cada operación crediticia cuenta con un respaldo físico, además el asesor de negocios elabora la solicitud de créditos, el informe de inspección y los resultados de las consultas de páginas web gubernamentales. Esta carpeta crediticia está bajo el resguardo del asesor para preservar y mantener cautela en el manejo de la documentación. Por otra parte, el jefe

de negocios y el asesor son los únicos que tienen acceso a dicha documentación y esta no podrá salir de las instalaciones, salvo autorización de gerencia.

¿Qué medidas de seguridad ha implementado dentro de la institución?

A través de los constantes cambios en los avances tecnológicos, la institución ha visto la necesidad de desarrollar su propia banca web para agilizar sus procesos, esto permite al socio consultar saldos o realizar pagos o transacciones sin la necesidad de trasladarse a las oficinas. Para crear este tipo de servicios, primero se analizaron los riesgos y el impacto que puede generar en la institución, como lo menciona:

> De manera implícita, en los procesos que implementamos si consideramos los riesgos que afectan nuestros servicios, por ejemplo, en la banca en línea que lanzamos recientemente, vamos evaluando y a veces también con apoyo externo, se analiza los riesgos para sacar un nuevo servicio. Para este servicio, tenemos los certificados SSL y tuvimos que acelerar la compra del antivirus.

Para mantener las medidas de protección que permitan desempeñar las actividades normalmente, en lo referente a la seguridad física de la institución se han implementado varias medidas de seguridad a las zonas que contienen información confidencial o recursos de suma importancia. Por ejemplo, en lo que respecta al acceso a caja y bóveda de la institución, es destinado al cajero en cada agencia a través de un sistema biométrico, además podrán acceder el personal de auditoría interna, externa y miembros del consejo de vigilancia cuando lo requieran para las actividades de control interno.

En lo que respecta a la seguridad de las instalaciones, la institución cuenta con un sistema de videovigilancia, alarmas y botón de pánico. Cuando se culmina la jornada laboral, lo controlan a través de un sistema de movimiento que detecta cualquier acción inusual, también tienen un sistema de vibración cuando se fuerzan las ventanas al intentar acceder al edificio. En caso de que esto ocurra, el sistema le informa automáticamente al técnico de sistemas y a la policía para que actúen oportunamente.

¿Cuáles serían las acciones de buenas prácticas que se deban implementar en el centro de procesamiento de datos para mantener un eficiente sistema de control interno en la seguridad de la información?

La información es considerada el activo principal de la institución, por lo que su gestión es fundamental y recae sobre el departamento de sistemas, quienes se deberían encargar de mantener actualizado el inventario de los activos que maneja la institución. Sería aconsejable verificar que se encuentren correctamente clasificados según los criterios de seguridad más adecuados, que cuenten con las características básicas, y sobre todo que los equipos cuenten con una persona responsable.

Además de asegurar el correcto funcionamiento del equipamiento donde se efectúa el tratamiento de la información desde su instalación, actualización, realización de copias de seguridad frecuente para evitar la pérdida de datos importantes, hasta la monitorización y el registro de todos los acontecimientos. Esto permite tener mayor seguridad y protección contra virus, ataques cibernéticos y software malicioso para evitar cualquier daño o deterioro y así preservar el ciclo de vida de los equipos.

De igual manera se debe tener mayor responsabilidad en que todas las actividades técnicas que se realicen en la institución estén debidamente documentadas ya que permite establecer un procedimiento de cómo se debe actuar en cierta actividad. En este sentido ayuda a que otras personas del departamento puedan ejecutar la misma actividad garantizando su continuidad. Asimismo, es necesario informar al personal lo que se ha planeado y las mejoras establecidas para que conozcan y estén familiarizados con los procedimientos establecidos en la institución.

Por otra parte, se debe garantizar que la instalación de los sistemas o aplicaciones se realicen conforme a los requisitos de seguridad y verificar que los nuevos sistemas satisfagan los requisitos de rendimiento y capacidad para prevenir que los equipos se saturen o sufran un daño. Además de asegurarse de que cada usuario tenga un perfil de acuerdo a sus funciones y que no se utilice contraseñas débiles o básicas que sean fáciles de identificar por otras personas.

En definitiva, la institución debería tomar en consideración estos puntos de vista, identificar las necesidades de la institución, así como sus debilidades y amenazas para definir el objetivo a seguir. Esto le permite realizar ajustes a sus políticas y procedimientos relacionado con el procesamiento de la información, para que se ajusten a sus requerimientos.

4.3.- Limitaciones del estudio

El presente análisis de caso ha presentado algunas limitaciones en el acceso a cierta información, pues se considera que los datos son sensibles y si de alguna manera se divulgan a personas no autorizadas, podría ocasionar problemas a la institución. En este caso, se redacta un acuerdo de confidencialidad, donde se manifiesta que la información proporcionada por la institución es únicamente de uso académico.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1.- Conclusiones

Tras la evaluación al sistema de seguridad de la información, se evidenció que la institución tiene ciertas falencias en lo que respecta a los activos de información debido a la falta de buenas prácticas para el uso aceptable de los recursos asociados con el procesamiento de datos. Además, la falta de sistemas de detección de fuego que permita al personal actuar oportunamente, y la ausencia de climatización que mantengan estable la temperatura de los equipos para evitar que se deterioren. En cambio, la seguridad de red, seguridad física de las instalaciones y la gestión de las copias de seguridad mantienen un monitoreo periódico para controlar la seguridad.

En lo relacionado al sistema de control interno, la institución no tiene mayor control en la administración de los riesgos para medir su impacto y definir si estos deben mitigarse, transferirse o evitarse de tal forma que, los riesgos se mantengan controlados y estos no afecten al desarrollo de las operaciones ni a la seguridad de la información. Por otra parte, se detectaron algunas vulnerabilidades respecto a la documentación de los diferentes procedimientos efectuados en la institución, como la apertura de nuevos servicios financieros, la creación del sitio web y la banca en línea. Esta incidencia aumenta la probabilidad de cometer las mismas fallas al momento de implementar un proceso, lo que ocasiona la pérdida de tiempo y recursos.

Otro de los aspectos que podría afectar la estabilidad de la institución es el desconocimiento del personal sobre el resguardo de la información y el control de incidentes de seguridad, lo que afectaría a los principios de integridad, disponibilidad y confidencialidad de la información. Sin embargo, cabe destacar que una de las fortalezas de la institución es la eficacia en la protección de los servidores contra virus, ya que mantienen estándares de configuración segura, lo que demuestra su responsabilidad y compromiso.

5.2.- Recomendaciones

Implementar y ejecutar adecuadamente controles internos relacionados con la seguridad de la información en la institución para brindar mayor protección a los activos y realizar evaluaciones periódicas para detectar debilidades e implementar acciones de mejora para la gestión de riesgos. De igual manera, dar a conocer al personal sobre los requisitos básicos de seguridad y sobre todo que cada usuario sea responsable del uso adecuado de cualquier recurso de procesamiento de información.

Concientizar a todo el personal tanto administrativo como operativo, acerca de los riesgos a los que está expuesta la información, resaltar acerca de la importancia que ésta representa para la institución y enfatizar las consecuencias que traería a todos sus socios al divulgar la información confidencial. Igualmente realizar un seguimiento al personal para medir y evaluar sus competencias, así como crear un buen ambiente de trabajo entre los diferentes departamentos para que sean de apoyo en la toma de decisiones.

Por otra parte, es necesario contar con un asesoramiento profesional externo y especializado sobre cómo evitar posibles amenazas que afecten a la seguridad de la información. En este sentido es fundamental establecer controles para la gestión de los riesgos, medir el nivel de gravedad y así proponer un plan de seguridad que permita al personal actuar oportunamente frente a las amenazas que pueden ocurrir ya sea de manera interna o externa, intencional o no.

REFERENCIAS BIBLIOGRÁFICAS

Abril, A., Jarol, P., & John, B. (2013). Análisis de Riesgos en la Seguridad de la Información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, *1*, 39–53. https://revista.jdc.edu.co/index.php/rciyt/article/view/121/113

Aden. (2020, July 30). ¿Cómo las nuevas tecnologías están impactando en el sector financiero? *Business Magazine*. https://www.aden.org/business-magazine/las-nuevas-tecnologias-estan-impactando-sector-financiero/

Altaminaro, J. R., & Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI - Revista Ibérica de Sistemas y Tecnologias de Información*, *25*, 112–134. https://doi.org/10.17013/risti.25.112-134

Arévalo, J. A. (2007). Gestión de la Información, gestión de contenidos y conocimiento. *SIOU*, 1–15. http://eprints.rclis.org/11273/1/Jornadas_GRUPO_SIOU.pdf

Armenta, C. E., & Aguirre Choix, R. (2012). La importancia del control interno en las pequeñas y medianas empresas en México. *El Buzón de Pacioli*, 1–17. https://www.itson.mx/publicaciones/pacioli/Documents/no76/68d_-_la_importancia_del_contorl_interno_en_las_pequenas_y_medianas_empresas_en_mexicox.pdf

Asobanca. (2021). Ecuador está entre los cuatro países de la región con más Corresponsales No Bancarios. *Asociación de Bancos Del Ecuador*. https://asobanca.org.ec/innovacion-y-tecnologia/ecuador-esta-entre-los-cuatro-paises-de-la-region-con-mas-corresponsales-no-bancarios/

Aumatell, C. (2013). *Auditoría de la información: identificar y explotar la información en las organizaciones* (1st ed.). https://elibro.net/es/ereader/uta/56771

Baca, Gabriel. (2016). *Introducción a la seguridad informática*.

https://elibro.net/es/ereader/uta/40458

Baca, Gabriela. (2015). *Proyectos de sistemas de información* (1st ed.). https://elibro.net/es/ereader/uta/40423

Banco Internacional. (2021). *¿Qué es y cómo funciona el sistema financiero ecuatoriano?* Educación Financiera. https://www.bancointernacional.com.ec/que-es-y-como-funciona-el-sistema-financiero-ecuatoriano/

BCE. (2021, February 8). En cuatro años aumentó el acceso al sistema financiero en 3,7 millones de personas. *Boletines de Prensa*. https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1411-en-cuatro-anos-aumento-el-acceso-al-sistema-financiero-en-3-7-millones-de-personas

Bertalanffy, L. Von. (1968). *General System Theory; Foundations, Development, Applications*. https://fad.unsa.edu.pe/bancayseguros/wp-content/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Bustamante, G., & Osorio, J. A. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, *6*, 71–77. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Capote, G. (2001). El control interno y el control. *Economía y Desarrollo*, *129*(2), 11–19. http://www.econdesarrollo.uh.cu/index.php/RED/article/view/679/510

Chumpitaz, D. O., & Gonzalez, Y. G. (2015). Caracterización del control interno en la gestión de las empresas comerciales. *In Crescendo*, *6*, 64–73.

Cobarsi-Morales, J. (2011). *Sistemas de información en la empresa* (1st ed.). https://elibro.net/es/ereader/uta/33493

Coopers, & Lybrand. (2007). *Los nuevos conceptos del control interno (Informe COSO)* (3rd ed.). https://elibro.net/es/ereader/uta/52931

Correa, J. A., Ramírez, L. J., & Castaño, C. E. (2010). La importancia de la planeación financiera en la elaboracion de los planes de negocio y su impacto en el desarrollo empresarial. *Revista Facultad de Ciencias Económicas: Investigación y Reflexión*, *18*, 179–194. https://www.redalyc.org/pdf/909/90920479010.pdf

Costas, J. (2014). *Seguridad Informática*. https://elibro.net/es/ereader/uta/62452

Cruz, B., Fernández-Alemán, J. L., & Toval, A. (2015). Security in cloud computing: A mapping study. *Computer Science and Information Systems*, *12*(1), 161–184. https://doi.org/10.2298/CSIS140205086C

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

Datta. (2021, April 6). La Banca avanza en su transformación digital. *Negocios*. https://datta.com.ec/articulo/la-banca-avanza-en-su-transformacion-digital

El Universo. (2020, November 19). La pandemia de coronavirus ha impulsado la transformación digital financiera en Latinoamérica. *Economía*. https://www.eluniverso.com/noticias/2020/11/19/nota/8054308/pandemia-coronavirus-ha-impulsado-transformacion-financiera/

Esage, A. (2021a, October 18). Nueva estafa bancaria. Hackers clonan voz de director de una empresa para robar $35 millones de su cuenta. Así lo hicieron. *Noticias de Seguridad Informática*. https://noticiasseguridad.com/hacking-incidentes/nueva-estafa-bancaria-hackers-clonan-voz-de-director-de-una-empresa-para-robar-35-millones-de-su-cuenta-asi-lo-hicieron/

Esage, A. (2021b, October 21). Ataque de Ransomware interrumpe todos los sistemas de una prestigiosa universidad. *Noticias de Seguridad Informática*. https://noticiasseguridad.com/hacking-incidentes/ataque-de-ransomware-interrumpe-todos-los-sistemas-de-una-prestigiosa-universidad/

Esage, A. (2021c, October 25). Facebook demanda a hacker que robaba información de sus usuarios para venderla en foros ilegales. *Noticias de Seguridad Informática*. https://noticiasseguridad.com/hacking-incidentes/facebook-demanda-a-hacker-que-robaba-informacion-de-sus-usuarios-para-venderla-en-foros-ilegales/

Escrivá, G., Romero, R., Ramada, D. J., & Onrubia, R. (2013). *Seguridad informática*. https://elibro.net/es/ereader/uta/43260

Forbes. (2021, October 20). *La banca digital es lo de hoy. Confía en su seguridad*. https://www.forbes.com.mx/ad-la-banca-digital-es-lo-de-hoy-confia-en-su-seguridad/

Gómez, Á. (2014). *Seguridad en equipos avanzados*. https://elibro.net/es/ereader/uta/62466

Hernández, J., & Flores, J. (2011). Seguridad física y lógica en el manejo de la información policial. *Revista Logos, Ciencia & Tecnología*, *3*, 222–233. https://www.redalyc.org/pdf/5177/517751801016.pdf

Higuera, A. (2021, August 24). Los sistemas de control industrial en manos de los ciberdelincuentes: el 71% de las vulnerabilidades son de riesgo alto. *20 Bits*. https://www.20minutos.es/tecnologia/ciberseguridad/los-sistemas-de-control-industrial-en-manos-de-los-ciberdelincuentes-el-71-de-las-vulnerabilidades-son-de-riesgo-alto-4800375/?autoref=true

Jácome, H. (2006). El sistema financiero y su papel en el desarrollo económico y social. *La Tendencia, Revista de Análisis Político*, 98–103. https://repositorio.flacsoandes.edu.ec/bitstream/10469/4914/1/RFLACSO-LT04-18-Jacome.pdf

Lara, D. (2021, May 7). La realidad del sistema financiero ecuatoriano. *Crónica*. https://cronica.com.ec/2021/05/07/la-realidad-del-sistema-financiero-ecuatoriano/

LGISF. (2012). *Ley General de Instituciones del Sistema Financiero*. http://www.oas.org/juridico/pdfs/mesicic4_ecu_gral.pdf

LOEPS. (2011). *Ley Orgánica de Economía Popular y Solidaria*. https://cosede.gob.ec/wp-content/uploads/2013/09/leyorganicadelaeconomiapopularysolidariaydelsectorfinanciero.pdf

Lozano, G., & Tenorio, J. J. (2015). El sistema de control interno: Una herramienta para el perfeccionamiento de la gestión empresarial en el sector construcción. *Accounting Power for Business*, *1*, 49–59. https://revistas.upeu.edu.pe/index.php/ri_apfb/article/view/896

McLennan, M., SK Group, & Zurich Insurance Group. (2021). *Informe de Riesgos Globales*. https://www3.weforum.org/docs/WEF_GRR21_Executive_Summary_Spanish.pdf

Ministerio de las tecnologías de la información y las comunicaciones. (2015). *Guía de indicadores de gestión para la seguridad de la información*. https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Mujica, M., & Alvarez, Y. (2010). El Análisis de Riesgo en la seguridad de la información. *Ciencia y Tecnología*, *4*, 33–37.

Navarro, M., & Díaz, L. (2014). *Sistemas de información en la empresa*. https://elibro.net/es/ereader/uta/42929

Palomo, R., Fernández, Y., & Gutiérrez, M. (2018). Banca cooperativa y transformació digital: hacia un nuevo modelo de relacion con sus socios y clientes. *Revista de Estudios Cooperativos*, 161–182. https://dehesa.unex.es/flexpaper/template.html?path=https://dehesa.unex.es/bitstream/10662/10481/1/REVE_62490.pdf#page=1

Pereira, C. A. (2019). *Control interno en las empresas. Su aplicación y efectividad* (1st ed.). https://elibro.net/es/ereader/uta/124953

Proaño, M. F., Orellana, S. Y., & Martillo Pazmiño, I. O. (2018). Los sistemas de información y su importancia en la transformación digital de la empresa actual. *Revista Espacios*, *39*. https://www.revistaespacios.com/a18v39n45/a18v39n45p03.pdf

PwC. (2018). Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018. *PwC*. https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html

PwC. (2021). *Actualización COSO ERM 2017*. https://www.pwc.com/mx/es/coso-erm-framework.html

SEPS. (2018). *Manual De Control Interno Para Las Asociaciones Y Cooperativas No Financieras De La Economía Popular Y Solidaria*. 1–29. https://www.seps.gob.ec/documents/20181/494185/Manual+de+Control+Interno+para+Organizaciones+del+Sector+No+Financiero_cc.pdf/231c9229-e2e0-4539-969c-abb640bd3011

SEPS. (2021a). El Sector Cooperativo, un actor clave para la reactivación económica. *Superintendencia de Economía Popular y Solidaria*. https://www.seps.gob.ec/noticia?el-sector-cooperativo-un-actor-clave-para-la-reactivacion-economica

SEPS. (2021b). Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario. *Superintendencia de Economía Popular y Solidaria*. https://www.seps.gob.ec/documents/20181/25522/SEPS-SGD-IGT-2021-25968-OFC.pdf.pdf/2867d754-93cf-457b-8b81-abde61346c37

SEPS. (2021c). SEPS e IT ahora presentan encuesta de "Servicios Financieros Digitales de las Entidades del Sector Financiero Popular y Solidario." *Superintendencia de Economía Popular y Solidaria*.

https://www.seps.gob.ec/noticia?seps-e-it-ahora-presentan-encuesta-de-servicios-financieros-digitales-de-las-entidades-del-sector-financiero-popular-y-solidario-

Superintendencia de Bancos. (2021). *Superintendencia de Bancos*. https://www.superbancos.gob.ec/bancos/

Torres, Z., & Torres, H. (2014). *Planeación y control. Una visión integral de la administración* (1st ed.). https://elibro.net/es/ereader/uta/39408

Zhañay, O. A., Erazo, J. C., & Narvaéz, C. I. (2019). Modelo de Auditoria de Sistemas de Información para las Cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, *5*. https://www.cienciamatriarevista.org.ve/index.php/cm/article/view/271/311

ANEXOS

ANEXO 1. Check List

	CRITERIO	PREGUNTAS	SI	NO
5	**POLITICAS DE SEGURIDAD DE LA INFORMACION**			
5.1	**Dirección de gestión para la seguridad de la información**			
5.1.1	Políticas de seguridad de la información	¿La institución ha implementado políticas de seguridad de la información?	x	
		¿Las políticas de seguridad de la información son aprobadas por la administración?	x	
		¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	x	
5.1.2	Revisión de las políticas de seguridad de la información	¿Se revisa frecuentemente las políticas de seguridad de la información?		x
		¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	x	
8	**GESTIÓN DE ACTIVOS**			
8.1	**Responsabilidad por los activos**			
8.1.1	Inventario de activos	¿Disponen de un inventario de activos de información?	x	
8.1.2	Propiedad de los activos	¿Se ha definido responsabilidades en cuanto a los activos de información?	x	
8.1.3	Uso aceptable de activos	¿Existen políticas relacionadas con el uso adecuado de los activos de información?	x	
8.1.4	Retorno de activos	¿Se ha definido un proceso para que los empleados devuelvan los activos de la institución que tienen a su cargo al terminar su contrato laboral?		x
8.2	**Clasificación de la información**			
8.2.1	Clasificación de la información	¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?		x

8.3	**Manejo de medios de almacenamiento**			
8.3.1	Gestión de medios extraíbles	¿Los soportes de almacenamiento están en un entorno seguro y protegido?	x	
		¿Los datos se almacena en múltiples copias para reducir el riesgo de daño o perdida?	x	
9	**CONTROL DE ACCESO**			
9.1	**Requisitos comerciales de control de acceso**			
9.1.1	Política de control de acceso	¿Existen políticas de control de acceso en función a la seguridad de la información?	x	
		¿Las políticas se basan en los requerimientos de la institución?	x	
9.1.2	Acceso a redes y servicios de red	¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?	x	
9.2	**Gestión de acceso de usuarios**			
9.2.1	Registro y cancelación de registro de usuario	¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?		x
9.2.2	Aprovisionamiento de acceso de usuarios	¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?		x
9.4	**Control de acceso al sistema y a las aplicaciones**			
9.4.1	Restricción del acceso a la información	¿Se controla los datos a los que puede acceder un usuario en particular?	x	
9.4.2	Procedimientos de inicio de sesión seguro	¿El acceso es protegido contra varios intentos de inicio de sesión?	x	
9.4.3	Sistema de gestión de contraseñas	¿Las contraseñas de los usuarios se cambian regularmente?	x	
		¿La selección de contraseñas son complejas?	x	
9.4.5	Control de acceso al código fuente del programa	¿Se restringe el acceso al código fuente del programa de la institución?	x	
11	**SEGURIDAD FISICA Y DEL ENTORNO**			
11.1	**Áreas Seguras**			
11.1.1	Perímetro de seguridad física	¿Los perímetros del edificio de la institución son físicamente solidos?	x	

		¿Existe un área de recepción para controlar el acceso físico al edificio?		x
11.1.2	Controles de entrada física	¿Implementan controles de acceso a áreas donde se almacena información confidencial de la institución?	x	
11.1.3	Asegurar oficinas, salas e instalaciones	¿Mantienen seguridad en puertas, escritorios y archivadores de la institución?	x	
		¿La información confidencial es visible desde el exterior de las instalaciones?		x
11.1.4	Protección contra amenazas externas y ambientales	¿Cuentan con un plan de seguridad para evitar daños por desastres naturales o ataques maliciosos a la institución?		x
11.1.5	Trabajar en áreas seguras	¿Las áreas donde el personal desarrolla sus actividades es segura?	x	
11.2	**Equipo**			
11.2.1	Ubicación y protección del equipo	¿Los equipos esta ubicados en sitios adecuados para reducir el acceso innecesario a las áreas de trabajo?		x
		¿Las instalaciones de almacenamiento están protegidas para evitar accesos no autorizados?	x	
11.2.2	Utilidades de apoyo	¿Los equipos están protegidos contra interrupciones causadas por fallas en los servicios públicos (electricidad, telecomunicaciones, agua)?		x
11.2.3	Seguridad del cableado	¿El cableado está protegido contra interceptaciones, interferencias o daños?		x
11.2.4	Mantenimiento de equipos	¿Cuentan con una programación de mantenimiento de los equipos informáticos?	x	
11.2.5	Remoción de activos	¿Se identifica a los usuarios que se les permite la salida de los activos fuera de la institución?	x	
11.2.6	Seguridad del equipo y los activos fuera de las instalaciones	¿Se mantiene un control a los activos que están fuera de las instalaciones?	x	

12	**SEGURIDAD DE LAS OPERACIONES**			
12.2	**Protección contra malware**			
12.2.1	Controles contra malware	¿Se implementan controles para evitar el uso de sitios web maliciosos o sospechosos?	x	
12.3	**Copia de seguridad**			
12.3.1	Copia de seguridad de la información	¿Las copias de seguridad se almacenan en un lugar seguro?	x	
13	**SEGURIDAD EN LAS COMUNICACIONES**			
13.1	**Gestión de la seguridad de la red**			
13.1.1	Controles de red	¿Las redes son administradas y controladas para proteger la información de la institución?	x	
13.1.2	Seguridad de los servicios de red	¿Se monitorea periódicamente la capacidad del proveedor de servicios de red?	x	
16	**GESTION DE INCIDENTES**			
16.1	**Gestión de incidentes y mejoras de seguridad de la información**			
16.1.1	Responsabilidades y procedimientos	¿Se establecen responsabilidades para desarrollar los procedimientos establecidos en la institución?	x	
16.1.2	Notificación de eventos de seguridad de la información	¿Se reportan eventos o incidentes de seguridad de la información?	x	
16.1.3	Informar las debilidades de seguridad de la información	¿Se notifica cualquier debilidad de seguridad observada en los sistemas o servicios?	x	
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	¿Se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente?		x
16.1.5	Respuesta a incidentes de seguridad de la información	¿Los incidentes de seguridad de la información se responden de acuerdo a los procedimientos establecidos?	x	

ANEXO 2. Activos de información

Valoración de activos

Valoración	Descripción
0	No aplicable
1	La pérdida de seguridad no impedirá la actividad normal de la empresa
2	La pérdida de seguridad causaría trastornos leves en la actividad normal de la empresa
3	La pérdida de seguridad causaría trastornos graves en la actividad normal de la empresa

Valoración de vulnerabilidades

Valoración	Descripción
0	Vulnerabilidad nula
1	Vulnerabilidad baja
2	Vulnerabilidad media
3	Vulnerabilidad alta

Catálogo de amenazas

Amenaza	Descripción
Fuego	Fuego en el centro de procesamiento de datos o en las oficinas
Inundación	Inundaciones de agua en las instalaciones y oficinas
Contaminación	Contaminación de salas de equipos especialmente sensibles de polvo
Interrupción del suministro eléctrico	Cortes en la electricidad que afecten la red o sistemas de seguridad
Interrupción de las redes de comunicación	Afecta en la comunicación con los clientes o procesos de la empresa
Robo de dispositivos o soportes	Robo de soportes de almacenamiento de datos, sistemas de TI o información de clientes
Errores de usuario	Modificación de datos o documentos
Errores del software	Fallos en navegadores, aplicaciones web o errores de programación

Índice de probabilidad

Índice	Clasificación	Descripción
5	Frecuente	Una vez a la semana o menos
4	Probable	Una vez cada 30 días
3	Ocasional	Una vez en 1 a 12 meses
2	Posible	Una vez entre 1 y 10 años
1	Improbable	Una vez en 10 años o mas

Índice de impacto

Índice	Clasificación	Descripción
5	Catastrófico	Daños irreparables, los datos y activos se pierden sin posibilidad de reparación y restauración
4	Alto	Interrupción parcial de las operaciones, los activos están dañados y se podrá reparar en un lapso largo de tiempo
3	Moderado	Algunas operaciones se verán afectadas, existe daño limitado de los activos
2	Bajo	La interrupción es leve, existe un daño leve de los activos
1	Insignificante	La interrupción es menor, no hay perdida ni daño en los activos

Nivel de riesgo

Escala	Clasificación	Descripción	Riesgo
7-9	Crítico	Los riesgos necesitan acciones preventivas urgentes, como paralización inmediata de las actividades para su corrección	Mitigar, transferir o evitar
5-6	Importante	Los riesgos necesitan recomendaciones y acompañamiento para la realización de las tareas	Mitigar, transferir o evitar
3-4	Apreciable	Se analizan los riesgos y la magnitud de las consecuencias	Asumir o mitigar
0-2	Bajo	Los riesgos son de actualización y mejora	Asumir el riesgo

Nivel de administración del riesgo

Nivel	Descripción
Mitigar	Reducirlo a un nivel aceptable mediante la implantación de medidas de seguridad
Asumir	El propietario del riesgo acepta convivir con él, al estar debajo del umbral fijado o porque reducirlo sería más costoso que el beneficio que se obtendría.
Transferir	Transferir el riesgo a un tercero, pero la responsabilidad sobre el servicio o activo siempre será de la organización, que deberá valorar el impacto que pueda tener su deterioro.
Evitar o eliminar	Eliminar la fuente del riesgo o la actividad que lo produce. En casos extraordinarios, podrá suponer la suspensión de un producto o servicio.

Cálculo del impacto

Vulnerabilidad de la amenaza	Valor de la dimensión del activo			
	0	**1**	**2**	**3**
0. Vulnerabilidad nula	0	0	0	0
1. Vulnerabilidad baja	0	1	2	3
2. Vulnerabilidad media	0	2	3	4
3. Vulnerabilidad alta	0	3	4	5

Cálculo del riesgo

Probabilidad	Valor de impacto					
	0	**1**	**2**	**3**	**4**	**5**
1. Improbable	0	1	2	3	4	5
2. Posible	0	2	3	4	5	6
3. Ocasional	0	3	4	5	6	7
4. Probable	0	4	5	6	7	8
5. Frecuente	0	5	6	7	8	9

Valoración de amenazas

AMENAZAS	PROB	Sitio Web			Datos / Información			Sistema operativo			Equipo informático			Red de comunicación			Equipo auxiliar			Servicios externos			Instalación			Personal		
		C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D
Fuego	1	0	0	2	0	0	2	0	0	2	0	0	2	0	0	2	0	0	2	0	0	0	0	0	3	0	0	0
Inundación	1	0	0	2	0	0	2	0	0	2	0	0	2	0	0	2	0	0	2	0	0	0	0	0	3	0	0	0
Contaminación	2	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0
Interrupción del suministro eléctrico	2	0	0	1	0	1	1	0	0	1	0	0	2	0	0	2	0	0	2	0	0	0	0	0	1	0	0	0
Interrupción de las redes de comunicación	2	0	0	0	0	0	3	0	0	0	0	0	0	0	1	3	0	0	0	1	1	2	0	0	0	0	0	0
Robo de dispositivos o soportes	2	0	0	2	3	1	1	1	2	2	0	0	3	0	0	2	0	0	2	0	0	0	2	0	0	0	0	0
Errores de usuario	3	0	2	1	2	2	1	2	2	1	0	1	1	0	0	2	0	1	1	1	1	0	0	0	0	2	2	2
Errores del software	4	0	1	1	0	2	1	0	0	1	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0

Nivel de impacto

AMENAZAS	Sitio Web			Datos / Información			Sistema operativo			Equipo informático			Red de comunicación			Equipo auxiliar			Servicios externos			Instalación			Personal		
	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D
Fuego	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	0	0	0	4	0	0	0
Inundación	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	0	0	0	4	0	0	0
Contaminación	0	0	0	0	0	0	0	0	2	0	0	2	0	0	2	0	0	2	0	0	0	0	0	2	0	0	0
Interrupción del suministro eléctrico	0	0	2	0	2	2	0	0	2	0	0	3	0	0	3	0	0	3	0	0	0	0	0	2	0	0	0
Interrupción de las redes de comunicación	0	0	0	0	0	4	0	0	0	0	0	0	0	1	4	0	0	0	1	1	2	0	0	0	0	0	0
Robo de dispositivos o soportes	0	0	3	5	2	2	3	4	3	0	0	4	0	0	3	0	0	3	0	0	0	0	0	0	0	0	0
Errores de usuario	0	2	2	4	3	2	4	4	2	0	1	2	0	0	3	0	1	2	1	1	0	0	0	0	0	0	2
Errores del software	0	1	2	0	3	2	0	0	2	0	1	2	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0

Nivel de riesgo

AMENAZAS	Sitio Web			Datos / Información			Sistema operativo			Equipo informático			Red de comunicación			Equipo auxiliar			Servicios externos			Instalación			Personal		
	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D
Fuego	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	0	0	0	4	0	0	0
Inundación	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0	0	0	0	0	4	0	0	0
Contaminación	0	0	0	0	0	0	0	0	3	0	0	3	0	0	3	0	0	3	0	0	0	0	0	3	0	0	0
Interrupción del suministro eléctrico	0	0	3	0	3	3	0	0	3	0	0	4	0	0	4	0	0	4	0	0	0	0	0	3	0	0	0
Interrupción de las redes de comunicación	0	0	0	0	0	4	0	0	0	0	0	0	0	2	5	0	0	0	2	2	3	0	0	0	0	0	0
Robo de dispositivos o soportes	0	0	4	6	3	3	4	5	4	0	0	5	0	0	4	0	0	4	0	0	0	0	0	0	0	0	0
Errores de usuario	0	4	4	6	5	4	6	6	4	0	3	4	0	0	5	0	3	4	3	3	0	0	0	0	0	0	4
Errores del software	0	4	5	0	6	5	0	0	5	0	4	5	0	0	0	0	4	5	0	0	0	0	0	0	0	0	0

ANEXO 3. Descripción de equipos informáticos

Departamento	Clase	Cant.	Características	Sistema Operativo
Sistemas	Servidor	1	ProLiant ML350 Gen10 Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz (16 CPUs) 64 GB Ram	Windows Server 2019 Datacenter 64-bit
		1	ProLiant ML110 Gen10 Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz (8 CPUs) 16 GB Ram	Windows Server 2019 Datacenter 64-bit
		1	Biostars Group H61MGV3 Intel(R) Pentium(R) CPU G2030 @ 3.00GHz (2 CPUs) 12 GB Ram	Windows Server 2016 Datacenter 64-bit
		1	Gigabyte Technology Co., Ltd. Intel(R) Core (TM) i5-3330 CPU @ 3.00GHz (4 CPUs) 4 GB Ram	Windows Server 2008 Standard
	Portátil	2	Intel(R) Core (TM) i7-8550U CPU @ 1.80GHz (8 CPUs) 12 GB Ram	Windows 10 Home Single 64-bit
	Monitor	1	Monitor HP 19"	
	Teclado	1	Teclado HP	
	Mouse	4	Mouse Genius Negro DX-110	
	Router	1	Router Fortinet Telco	
		1	Router TP LINK Sistemas Dos Antenas	
	Switch	1	HP Telconet	
	DVR	1	DVR Cámaras de Seguridad	

	Radio Sonido	1	Radio Sonido Ambiental	
	UPS	1	UPS Data center	
	Proyector	1	Proyector Epson	
Negocios	Desktop	7	Intel(R) Pentium(R) Gold G5420 CPU @ 3.80GHz (4 CPUs) Spanish (Regional Setting: Spanish) 8 GB RAM	Windows 10 Pro 64-bit
		2	Intel(R) Core (TM) i3-7100 CPU @ 3.90GHz (4 CPUs)4GB RAM400GB Disco Duro	Windows 7 Ultimate 32-bit
	Portátil	2	Intel Core i5-1035G1 CPU @1.00 GHz 8GB Ram	Windows 10 Pro 64-bit
	Monitor	9	Monitor LG 19"	
	Teclado	9	Teclado Genius Negro	
	Mouse	11	Mouse Genius Negro	
	Regulador	9	Regulador CDP Blanco Negro	
	Parlantes	2	Parlantes Genius color negro	
	Impresora	1	Epson LX 395 Multifunción	
		1	Impresora Epson L395	
Marketing	Portátil	1	Dell Inc. Inspiron 3501 Intel(R) Core (TM) i7-1165G7 @ 2.80GHz (8 CPUs) 8GB RAM	Windows 10 Pro 64-bit
		1	ASUSTeK COMPUTER INC. Intel(R) Core (TM) i7-10870H CPU @ 2.20GHz (16 CPUs) 16 GB RAM	Windows 10 Home Single 64-bit

		1	ASUSTeK COMPUTER INC. Intel(R) Core (TM) i7-1065G7 CPU @ 1.30GHz (8 CPUs)	Windows 10 Pro 64-bit
	Mouse	3	Mouse Genius Red Black	
	Impresora	1	Impresora Epson L3160 Multifunción	
	Cooler	1	Cooler 5 Ventiladores	
Operaciones	Desktop	2	Intel(R) Pentium(R) Gold G5420 CPU @ 3.80GHz (4 CPUs) 8 GB RAM 256 GB SDD	Windows 10 Pro 64-bit
		2	Intel(R) Core(TM) i3-7100 CPU @ 3.90GHz (4 CPUs) 12 GB RAM	Windows 10 Pro for Workstations 64-bit
	Portátil	2	Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz (4 CPUs) 4GB RAM	Windows 10 Home Single Language 64-bit
	Monitor	2	Monitor LG 19"	
		2	Monitor LG - MODEL: 20MK400H	
	Teclado	4	Teclado genius SMART KB-100	
	Mouse	6	Mouse Dx - 110	
	Regulador	4	Regulador CDP Blanco Negro	
		1	Impresora Epson L395 Multifunción	
		1	Impresora Matricial LX 800II	
Financiero	Desktop	1	Intel(R) Pentium(R) Gold G5420 CPU @ 3.80GHz (4 CPUs) 8 GB RAM	Windows 10 Pro 64-bit
		1	INTEL CORE i5-5304 GIGA-BYTE TECHNOLOGY CO., LTD.	Windows 10 Pro 64-bit
		1	Intel(R) Core(TM) i3-7100 CPU @ 3.90GHz (4 CPUs) 4GB Ram.	Windows 10 Home Single Language 64-bit

	Monitor	3	Monitor LG 19"	
	Teclado	3	Teclado genius	
	Mouse	3	Mouse genius	
	Regulador	1	CDP Blanco Negro	
		1	Regulador Power West Negro	
	Impresora	1	Epson L355 Multifunción	
Asistente Gerencia	Desktop	1	Intel Corel i5-5422 CPU @2,8 GHz 8GB RAM - 500 TB HDD	Windows 10 Pro 32-bit
	Monitor	1	Monitor LG 19"	
	Teclado	1	Teclado DX-110	
	Mouse	1	Mouse Dx - 110	
	Parlantes	1	Parlantes Genius color rojo	
	Regulador	1	Regulador CDP Blanco Negro	
Gerencia	Desktop	1	Intel Core i3-9100F CPU @3.60 GHz 8 GB Ram	Windows 10 Pro 64-bit
	Monitor	1	Monitor LG 19"	
	Teclado	1	Teclado genius	
	Mouse	1	Mouse genius	
	UPS	1	UPS Blanco Negro	
	Impresora	1	Impresora Multifunción L4150	

ANEXO 4. Cuestionario de control interno

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
GOBIERNO Y CULTURA

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN	**10**		**8**
¿El comportamiento y las decisiones de Gerencia y las jefaturas reflejan su compromiso en el cumplimiento de la ética y los valores?		SI	1
¿Se evalúa periódicamente el comportamiento de los colaboradores de acuerdo con las normas establecidas?		SI	1
¿Se revisa periódicamente el cumplimiento de las normas de confidencialidad en el personal de la institución?		NO	0
¿Se establecen supervisiones sobre el funcionamiento del sistema de control interno?		SI	1
¿Los procedimientos de control interno contribuyen al desarrollo de las actividades operativas de la institución?		SI	1
¿Se verifica el cumplimiento de las políticas y procedimientos en la ejecución de las actividades operativas de la institución?		SI	1
¿Cuentan con un manual de funciones con el perfil de competencias para cada cargo?		SI	1
¿Se realiza actividades de inducción y capacitación al personal?		SI	1
¿Existe segregación de funciones en los niveles institucionales?		SI	1
¿El desempeño del personal tanto técnico como administrativo es evaluado periódicamente?		NO	0
CALIFICACIÓN TOTAL = CT			8
PONDERACIÓN TOTAL = PT			10
NIVEL DE CONFIANZA: NC= CT/PT x 100			80%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			20%

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN	**6**		**5**
¿Los jefes departamentales apoyan en la fijación de los objetivos institucionales?		SI	1
¿Los objetivos institucionales están alineados con las normas que las regulan?		SI	1
¿La dirección identifica los recursos necesarios para alcanzar los objetivos?		SI	1
¿El plan estratégico institucional apoya al cumplimiento de los objetivos institucionales?		SI	1
¿Los objetivos establecidos son comunicados a todos los colaboradores de la institución de forma oportuna para su cumplimiento?		NO	0
¿Los objetivos departamentales están contemplados dentro del POA institucional?		SI	1
CALIFICACIÓN TOTAL = CT			5
PONDERACIÓN TOTAL = PT			6
NIVEL DE CONFIANZA: NC= CT/PT x 100			83%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			17%

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
DESEMPEÑO

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN	**9**		**6**
¿Se evalúa el impacto que puede tener en el control interno realizar cambios en las tecnologías?		NO	0
¿Se analiza los riesgos derivados de fuentes externas como en lo económico, ambiental o tecnológico?		SI	1
¿Detecta los riesgos de fuentes internas relacionados con los sistemas de información en el caso de fallos que afecten la continuidad de las operaciones?		SI	1
¿La institución ha definido la administración de los riesgos identificados, en los parámetros de: asumir, mitigar, transferir, evitar o eliminar?		NO	0
¿Existen problemas informáticos que impidan la correcta realización de las operaciones?		NO	0
¿Se evalúa si son adecuados los sistemas de información en el desarrollo de las actividades?		SI	1
¿Se aumenta la capacidad de los sistemas informatizados para poder tratar volúmenes crecientes de información?		SI	1
¿Realiza un estudio preliminar para la adquisición o actualización de nuevos sistemas para el flujo de información?		SI	1
¿Se efectúa un seguimiento de las nuevas tecnologías o aplicaciones desarrolladas?		SI	1
CALIFICACIÓN TOTAL = CT			6
PONDERACIÓN TOTAL = PT			9
NIVEL DE CONFIANZA: NC= CT/PT x 100			67%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			33%

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
REVISAR Y AJUSTAR

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN	**10**		**8**
¿Se tienen alineados los controles de TI con los procesos de la organización y los controles generales?		SI	1
¿Los controles implementados están alineados con la reducción y gestión de los riesgos?		SI	1
¿Se han ejecutado los controles orientados a la infraestructura de TI?		SI	1
¿Han establecido perfiles de acceso a los usuarios en las herramientas tecnológicas de acuerdo con el rol desempeñado?		SI	1
¿Se han implementado controles de seguridad que protejan a la organización de un ataque informático externo?		NO	0
¿Se han implementado controles sobre el desarrollo, compra y mantenimiento de TI?		SI	1
¿Se han establecido controles orientados a la restricción de usuarios no autorizados?		SI	1
¿Las actividades de control que aplica la empresa se relacionan a controles preventivos, correctivos y detectivos?		SI	1
¿La aplicación de los procedimientos y las políticas cuentan con un responsable para su cumplimiento?		SI	1
¿Las políticas y procedimientos de la institución son revisados y ajustados periódicamente?		NO	0
CALIFICACIÓN TOTAL = CT			8
PONDERACIÓN TOTAL = PT			10
NIVEL DE CONFIANZA: NC= CT/PT x 100			80%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			20%

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.
CUESTIONARIO DE CONTROL INTERNO
INFORMACIÓN, COMUNICACIÓN Y SOPORTE

COMPONENTE ANALIZADO	PT	SI/NO	CT
SUMAN	**7**		**6**
¿La información está disponible y es oportuna para permitir el control efectivo de las actividades?		SI	1
¿La información cumple con los principios de las normas ISO 27000: confidencialidad, integridad y disponibilidad de la información?		SI	1
¿Para cada reporte se tienen un control de validación que asegure que la información está completa?		SI	1
¿La información generada está directamente asociada con los objetivos institucionales establecidos?		SI	1
¿Los informes departamentales son entregados a la dirección de forma oportuna?		SI	1
¿La institución utiliza como medios de comunicación correos electrónicos, memorandos, messenger interno?		SI	1
¿La gerencia toma en cuenta las recomendaciones de mejora aportadas por los empleados?		No	0
CALIFICACIÓN TOTAL = CT			6
PONDERACIÓN TOTAL = PT			7
NIVEL DE CONFIANZA: NC= CT/PT x 100			86%
NIVEL DE RIESGO INHERENTE: RI= 100% - NC%			14%