UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

ÁREA: Administrativas informáticas

LÍNEA DE INVESTIGACIÓN: Normas y estándares

AUTOR: Mayra Gabriela Cordero Núñez

TUTOR: Ing. Oscar Fernando Ibarra Torres

Ambato – Ecuador

marzo – 2022

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA., desarrollado bajo la modalidad Proyecto de Investigación por la señorita Mayra Gabriela Cordero Núñez, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2022

Ing. Oscar Fernando Ibarra Torres

TUTOR

AUTORÍA DEL TRABAJO DE TITULACIÓN

El presente Proyecto de Investigación titulado: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA., es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2022


Firmado electrónicamente por:
MAYRA GABRIELA CORDERO NUNEZ

Mayra Gabriela Cordero Núñez

C.C. 1804394656

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señorita Mayra Gabriela Cordero Núñez estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA., nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta de Tribunal.

Ambato, marzo 2022

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia Mg.
PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

PhD. Felix Fernández
PROFESOR CALIFICADOR

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Guevara Mg.
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2022

Firmado electrónicamente por:
MAYRA GABRIELA
CORDERO NUNEZ

Mayra Gabriela Cordero Núñez

C.C. 1804394656

AUTOR

DEDICATORIA

El presente proyecto de investigación está dedicado principalmente a Dios, quien ha sido mi fuerza y guía para continuar mis estudios.

A mi padre, Eduardo, que siempre me ha cuidado desde el cielo y ha sido mi ejemplo.

A mi abuelita Graciela, mi ángel del cielo, para ti serán siempre dedicados mis triunfos, sé que este momento hubiera sido tan especial para ti como lo es para mí.

A mi esposo Andrés, por sus palabras de aliento diario, por su paciencia y por la fortaleza que me ha dado para salir adelante en los momentos más difíciles.

A mis amigas, por su amistad, apoyo y ayuda en todo momento.

AGRADECIMIENTO

Agradezco a Dios por guiarme y permitirme terminar mi carrera, a mi esposo por su apoyo incondicional y presencia en mi vida.

A mi tutor, el Ingeniero Fernando Ibarra por su apoyo guía para culminar el presente trabajo.

A la COAC San Francisco Ltda., de manera especial al oficial de seguridad de la información y al departamento de tecnología por su apoyo en la realización de este proyecto de investigación.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo de investigación se enfoca en realizar un estudio de las políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda., para la cual se aplicó una metodología cuali-cuantitaiva para ello se diseñó una encuesta para obtener información del personal del departamento de Tecnología de la Cooperativa y también se aplicó una entrevista al oficial de seguridad de la información, para determinar en nivel de seguridad de la información implementado dentro la organización. De los resultados obtenidos de la encuesta y la entrevista se pudo determinar que la implementación de una política de seguridad basada en normas internacionales beneficiaría al Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Posteriormente se realizó un cuadro comparativo con las ventajas y desventajas de las normas internaciones referentes a la seguridad de la información, de la cual se pudo determinar que la norma ISO 27002 es la más indicada para políticas de seguridad de información y activos de una organización. Finalmente se realizó la propuesta basada en metodología Magerit, la cual consta de tres procesos fundamentales la planificación, el análisis de riesgos y la gestión de riesgos. Para la gestión de riesgos se empleó 5 dominios y 14 controles principales de la normativa ISO 27002 con los cuales se elaboró una política de seguridad de la información para la institución financiera.

Palabras Clave: Seguridad, información, política de seguridad, normativa, Magerit.

ABSTRACT

This research works focuses on conducting a study of information security policies based on international standards to ensure controls against threats and vulnerabilities in the Department of Technology of the Cooperativa de Ahorro y Crédito San Francisco Ltda., for which A qualitative-quantitative methodology was applied for this, a survey was designed to obtain information from the staff of the Technology Department of the Cooperative and an interview was also applied to the security officer of the Cooperative to determine the level of information security implemented within the organization. From the results obtained from the survey and the interview, it was possible to determine that the implementation of a security policy based on international standards would benefit the Technology Department of the Cooperativa de Ahorro y Crédito San Francisco Ltda. Subsequently, a comparative table was made with the advantages and disadvantages of international standards regarding information security, from which it was possible to determine that the ISO 27002 standard is the most suitable for information and asset security policies of an organization. Finally, the proposal was made based on the Magerit methodology, which consists of three fundamental processes: planning, risk analysis and risk management. For risk management, 5 domains and 14 main controls of the ISO 27002 standard were used, with which an information security policy was developed for the financial institution.

Keywords: Security, information, security policy, regulations, Magerit.

CAPITULO I.- MARCO TEÓRICO

1.1. Tema de Investigación

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.

1.2. Antecedentes investigativos

En el Ecuador existen algunas investigaciones relacionadas de las cuales se hará referencia a las que se considera aportarán al presente trabajo:

Para Pilla [1] en su proyecto de investigación "Diseño de una política de seguridad de la información para el área de tecnología de la información de la Cooperativa de Ahorro y Crédito Chibuleo LTDA., basado en la norma ISO/IEC 27002:2013" proyecto realizado para la maestría en tecnologías de la información de la Universidad Internacional SEK, en el año 2019, pudo determinar lo siguiente:

- A través del diagnóstico y de una revisión profunda de la norma internacional ISO/IEC 27002:2013 se diseñó una política de seguridad de la información para el área de TI de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. En la propuesta se tomó en cuenta tres aspectos fundamentales: la confidencialidad, integridad y disponibilidad de los datos que posee la institución. En base estos elementos se realizó un análisis actual de las medidas de seguridad que el área de tecnología ha implementado, además de plasmar en una matriz los incidentes de seguridad.
- En base a los incidentes de seguridad, se desarrolló una matriz de riesgo, basada en Deloitte (2015) y el Banco de España (2012), en la que se identificó las principales amenazas, eventos de riesgo y vulnerabilidades que tienen los activos de información dentro del área de Tecnología.

- Con la matriz de riesgo completa, se realizó una valoración de los activos de información, además de una reunión con el jefe de tecnología, el analista de riesgos y el oficial de seguridad de la información, quienes con criterios ponderaron los eventos y calificaron la vulnerabilidad y ocurrencia, los informantes identificaron los eventos críticos de seguridad de información que tiene el área de Tecnología.
- Para mitigar los eventos críticos de seguridad de información del área de tecnología, es necesario realizar un análisis a la norma ISO/IEC 27002:2013, identificando los controles adecuados para reducir dichas incidencias relacionadas a la seguridad de la información.
- En esta investigación el área de Tecnología de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., obtuvo una política de seguridad de información basado en los controles de la norma ISO 27002:2013, la cual contiene lineamientos y controles de seguridad de información que deben cumplir todas las áreas de la cooperativa.

Según Chipantiza [2] en su trabajo de grado "Análisis de Riesgo Tecnológico del Centro de Datos Basado en Normas Internacionales: Caso GADMCE", trabajo realizado en la Pontificia Universidad Católica del Ecuador Sede Esmeraldas, en el año 2018, pudo determinar lo siguiente:

- La situación en la que se encuentra el Centro de Datos del GADMCE muestra que no alcanza los requerimientos básicos en seguridad que una infraestructura tecnológica debe lograr.
- Por no tener plan de tratamiento de riesgos formal, el Centro de Datos es susceptible a incidentes que afectaría notablemente al personal que labora en las dependencias. Las aplicaciones de los controles sugeridos garantizarían la integridad y disponibilidad de la información.
- El análisis de riesgo tecnológico es el proceso de evaluación de los activos del centro de datos para poder determinar el nivel de seguridad y proponer mejoras, de ser necesarias.
- La investigación determina que el personal de la Unidad de Sistemas no se rige a procesos de seguridad con respecto al Centro de Datos.

Desde el punto de vista de Elizabeth Torres [3] en su proyecto de investigación "Políticas de Seguridad de la Información basado en la Norma ISO/IEC 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato, trabajo realizado como proyecto de investigación de la Universidad Técnica de Ambato, en el año 2015, pudo determinar lo siguiente:

- Al realizar la presente investigación se pudo determinar que el activo más importante de cada organización es la información, por lo tanto, es importante protegerla para lo cual una adecuada norma de protección es fundamental para evitar modificaciones o accesos no autorizados.
- El personal administrativo, docentes y estudiantes realizan sus funciones acorde a la información que brindan los sistemas de la universidad, por lo tanto, es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002, que ayuda a protegerla, puesto que las políticas de seguridad minimizan el riesgo de pérdida de información garantizando el correcto funcionamiento de los procesos.
- La tecnología cada día cambia, por esta razón la universidad debe estar constantemente actualizada en los ámbitos de tecnología, telecomunicaciones y políticas de seguridad, aplicando procedimientos, documentación y manuales para la estandarización de los procesos.

Como lo mencionan en la revista Publicayo [4] la información es el activo más valioso de las empresas en el mundo actual de tecnologías de la información (TI), las empresas guardan información sensible en sus servidores y en caso de llegar ésta a manos equivocadas, se verían afectadas tanto las empresas públicas como privadas .

El acceso a información de alta calidad, completa, precisa y actualizada es vital para respaldar el proceso de toma de decisiones gerenciales que conduce a decisiones acertadas [5]. Por lo tanto, asegurar los recursos del sistema de información es extremadamente importante para garantizar que los recursos estén bien protegidos. Dando como conclusión que la seguridad de la información no es solo una cuestión de tener nombres de usuario y contraseñas.

Dado que la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización, necesitamos un estándar o punto de referencia que regule la gobernanza sobre la seguridad de la información. Varias organizaciones privadas y gubernamentales desarrollan organismos de estándares cuya función es establecer puntos de referencia, estándares y, en algunos casos, regulaciones legales sobre seguridad de la información para garantizar que se mantenga un nivel adecuado de seguridad, para garantizar que los recursos se usen de la manera correcta y para garantizar las mejores prácticas de seguridad adoptadas en una organización [6].

1.2.1. Contextualización del problema

Constantemente toda organización, está captando una serie de datos; de los cuales en ocasiones no tienen significación alguna, pero en cambio existen otros datos que le sirven para conocer mejor el entorno que le rodea y conocerse a sí misma. Estos datos, que constituyen la llamada información, le van a permitir tomar decisiones más acertadas. Por ello, la información a tiempo y en la cantidad precisa es un factor clave para toda organización [7].

En la actualidad, las grandes y pequeñas empresas, negocios locales, etc, administran distintos tipos de información y recursos tecnológicos y se ven en la necesidad de buscar alternativas para que sus sistemas de información sean robustos y estables en materia de seguridad [8], por lo que asegurar los recursos del sistema de información es realmente importante; al hablar de seguridad de la información no solo nos referimos a tener usuarios y contraseñas sino a la manera eficaz de gestionar dicha información a través de políticas, estándares y regulaciones legales sobre seguridad de la información, garantizando el uso correcto de los recursos y la adopción de las mejores prácticas para el manejo de la información [9].

Hoy en día, las organizaciones están cada vez más expuestas a virus, gusanos, hackers e ingenieros sociales, es así que un 77.6% de todos los ataques que se producen en el mundo, están dirigidos a empresas, mientras que a particulares un 22.4%. Para el caso

específico de España, se menciona que las empresas que tienen alguna medida de seguridad informática son del 56.96% en empresas con menos de 10 empleados, 91.86% en empresas de 10 a 49 empleados, 96.78% en empresas de 50 a 249 empleados y del 98.2% en empresas de 250 a más empleados [10]. Esto nos permite evidenciar la importancia de la implementación de un sistema de gestión de la seguridad de información aún en empresas pequeñas.

En el Ecuador, son pocas las organizaciones que han invertido en recursos humanos y tecnológicos para mejorar sus seguridades, contener los ciberataques, proteger los recursos o activos y la información confidencial corporativa y la de sus clientes [11].

Para Nelson Dávalos del Diario Primicia [12], la ciberseguridad en el país ha mejorado, pero aún no lo suficiente ya que actualmente Ecuador se encuentra en la séptima posición de América Latina según el índice Global de Ciberseguridad. En base al informe Estado de Ciberseguridad en Ecuador, elaborado por la firma Deloitte, en la cual encuestaron alrededor de 100 empresas ecuatorianas, se puede evidenciar que el 51% de las empresas poseen un responsable a cargo de la seguridad física y digital, mientras que un 13% de las empresas no cuenta con un experto en seguridad.

La seguridad de los datos en territorio ecuatoriano aún es frágil, pese a que en el 2013 la extinta Secretaría Nacional de la Administración Pública emitió el Esquema Gubernamental de Seguridad de la Información (EGSI), en la que se dispuso el uso obligatorio de las normas ISO-27000 para la Seguridad de la Información. El 74% de las entidades públicas aún almacenan información sin seguridades estando expuestos a hackeos, robos y ciberataques [13].

Para el año 2016, dentro de las cifras emitidas por el Directorio de Empresas y Establecimientos del Instituto Nacional de Estadísticas y Censos (INEC), se determinó que Tungurahua está dentro de las cinco provincias que concentran al 62% de las empresas en el país. Otra de las cifras que muestra la importancia de la empresa privada

en la provincia es el número de empresas que existen por cada 10 mil habitantes, donde Tungurahua se ubica en segundo lugar, demostrando que muchos de los empleos están relacionados con la industria y comercio [14]. El incremento de empresas ha obligado a implementar mecanismos y controles para asegurar la confidencialidad e integridad de los sistemas de información y que ayuden a disminuir las amenazas a las que están expuestos.

La Cooperativa de Ahorro y Crédito San Francisco Ltda. es una institución que ha ido creciendo con el paso del tiempo y se ha visto en la necesidad de proteger y reforzar el activo más valioso: "la información", a pesar de que años atrás se realizó un SGSI (Sistema de Gestión de Seguridad de la Información), no se ha realizado su correcta implementación y por ende una actualización del SGSI y las políticas necesarias para precautelar los activos de información, esto ha ocasionado vulnerabilidades y riesgos en la información, mismos que podrían generar afectaciones administrativas y financieras en la institución

Con estos antecedentes se ha visto necesario el estudio de normas internacionales que conduzcan a la seguridad de la información y su correcta implementación, identificando la normativa que mejor se adapte a la institución.

1.2.2. Fundamentación teórica

Normas de Seguridad de la Información

Dado que la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización, necesitamos un estándar o punto de referencia que regule la gobernanza sobre la seguridad de la información. Varias organizaciones privadas y gubernamentales desarrollaron organismos de estándares cuya función es establecer puntos de referencia, estándares y, en algunos casos, regulaciones legales sobre seguridad de la información para avalar que se mantenga un nivel adecuado de seguridad, para garantizar que los recursos se usen de la manera correcta y se ejecuten

las mejores prácticas de seguridad adoptadas en una organización. Existen varios estándares para el gobierno de TI que conducen a la seguridad de la información, como PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL y COBIT [13].

Familia ISO 27000

Proporciona una visión general de las normas que componen la serie 27000, en el que cada una indica su alcance de actuación y propósito. Aporta bases de la importancia de la implantación de un SGSI y una introducción a los Sistemas de Gestión de Seguridad de la Información y los pasos para implantar, monitorear, mantener y mejorar un SGSI [15].

- **ISO/IEC 27001:** Es un estándar publicado por la Organización Internacional de Normalización (ISO). Pertenece a la familia de normas ISO 27000. Por ejemplo, ISO 27002, una directriz y un código de prácticas sobre la implementación de un SGSI, es un estándar complementario a ISO 27001. ISO 27002 se llamaba anteriormente ISO 17799, que fue desarrollado a partir de BS 7799 Parte 1. ISO 27005 se concentra en la gestión de riesgos de seguridad de la información, detallando el enfoque de gestión de riesgos adoptado por ISO 27001. El estándar ISO 27001 proporciona una especificación para SGSI. Oficialmente, ISO 27001 define SGSI como "un sistema de gestión que lleva a cabo el establecimiento, operación, mantenimiento, monitoreo y mejora de la seguridad de la información" [16].

  Áreas o Dominios de Seguridad de la ISO/IEC 27001 [17]

  - Políticas de seguridad.
  - Organización de seguridad.
  - Administración de activos.
  - Seguridad de los recursos humanos.
  - Seguridad física y ambiental.
  - Gestión de comunicaciones y operaciones.
  - Sistema de control de accesos.

- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Administración de incidentes de seguridad de la información.
- Plan de continuidad del negocio.
- Cumplimiento.
- Gestión de incidentes en la seguridad de la información.
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.
- Cumplimiento.

- **ISO/IEC 27002:** Es una guía de buenas prácticas donde describe objetivos de control y controles sugeridos en la seguridad de la información. La normativa contiene 14 dominios, 35 objetivos de control y 114 controles [16].
- **ISO/IEC 27003:** Es una guía que se centra en aspectos críticos necesarios para el diseño y exitosa implantación del SGSI en base a la ISO/IEC 27001 [16].
- **ISO/IEC 27004:** Es una guía enfocada al desarrollo y utilización de las métricas y técnicas de medida aplicables que permitan determinar la eficacia de un SGSI y los controles implementados según la ISO/IEC 27001 [16].
- **ISO/IEC 27005:** Proporciona directrices para la gestión de riesgos en la seguridad de la información [16].
- **ISO/IEC 27006:** Detalla los requisitos para las entidades que realizan auditorias y otorgan certificaciones [16].
- **ISO/IEC 27007:** Es una guía para Auditorías de SGSI [16].
- **ISO/IEC 27008:** Es una guía de auditoría para controles en el marco de implementación de un SGSI [16].
- **ISO/IEC 27009:** Requisitos para uso de la norma ISO/IEC 27001 en cualquier sector [16].
- **ISO/IEC 27010:** Guía para gestionar la Seguridad de la Información entre organizaciones [16].

ITIL

ITIL es un conjunto de conceptos y prácticas para la Gestión de Servicios de Tecnología de la Información (ITSM), el desarrollo de Tecnología de la Información (TI) y las operaciones de TI, que tiene partes centradas en la seguridad [18].

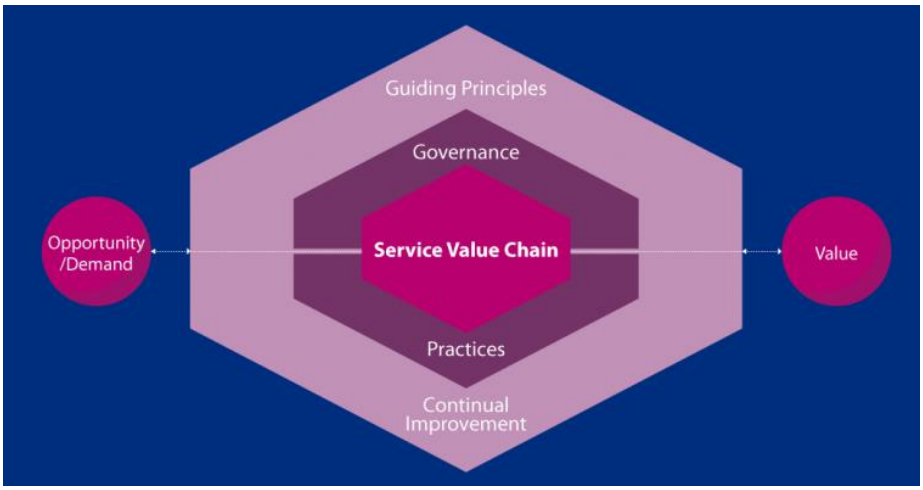

Figura 1. Sistema de valor del Servicio (SVS)

Elaborado por: [19]

COBIT

COBIT (Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como marco de trabajo, dirigida al control y supervisión de los objetivos de las TI. Es mantenido por ISACA y el IT GI (IT Governance Institute), contiene recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión [20].

En el contexto de COBIT 5, la creación de valor es un objetivo del Gobierno de las TI y se identifica con la realización de beneficios, la optimización del riesgo, así como la optimización de recursos [20].

Principios de COBIT

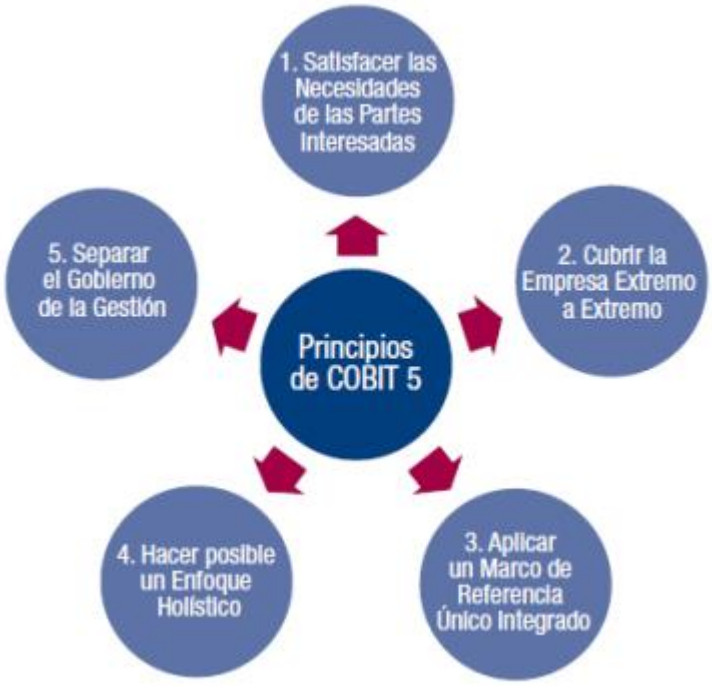

Figura 2. Principios COBIT 5

Elaborado por: [20]

- **Satisfacer las necesidades de las partes interesadas**: Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos [20].
- **Cubrir la empresa de extremo a extremo:** COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, cubriendo todas las funciones y procesos dentro de la empresa [20].
- **Aplicar un marco de referencia único e integrado**: Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI [20].
- **Hacer posible un enfoque holístico:** Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en

cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (cualquier cosa que puede ayudar a conseguir las metas de la empresa), para apoyar la implementación de un sistema de gobierno y gestión global [20].

- **Separar el gobierno de la gestión:** COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos [20].

Seguridad de la Información

Para entender acerca de la seguridad de la información primero debemos conocer acerca de la seguridad informática.

El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. Para ello se utilizará estructuras organizacionales, técnicas administrativas, gerenciales o legales. Mientras que el objetivo secundario es garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total [21].

La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información [22].

Pilares de la Seguridad de la Información

Para *J. Fabián y otros autores* [23], la seguridad de la información es la disciplina que se encarga de garantizar la:

- Confidencialidad: Intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas. Para garantizar la confidencialidad necesitamos disponer de tres tipos de mecanismos:
- Autenticación. La autenticación intenta confirmar que una persona o máquina es quien dice ser, que no estamos hablando con un impostor.
- Autorización. Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella. Básicamente dos: solo lectura, o lectura y modificación.
- Cifrado. La información estará cifrada para que sea inútil para cualquiera que no supere la autenticación.
- Integridad: Significa que los datos queden almacenados tal y como espera el usuario, es decir que no sean alterados sin su consentimiento.
- Disponibilidad de la información: Intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido.

Políticas de la Seguridad de la Información

Las políticas de seguridad de la información contemplan la importancia de la protección de los activos de información al evitar el acceso no autorizado, divulgación, manipulación no autorizada de toda la información, comprometiéndose a implantar y mantener un Sistema de Gestión de Seguridad de la Información [24].

Mientras que Escudero [25] en su artículo menciona que, en las empresas, las políticas de seguridad de la información han surgido con la finalidad de concienciar a los usuarios acerca de la importancia y lo susceptible que es la información hoy en día. Las políticas de seguridad describen lo que se desea proteger y el porqué, a través de normativas, reglamentos y protocolos de actuación, definiendo responsabilidades, funciones de la organización y controlando su correcto funcionamiento.

También menciona aspectos importantes para establecer las políticas como son:

- Analizar riesgos informáticos en software y hardware.
- Comunicar el desarrollo de las políticas a todas las áreas involucradas.
- Designación de responsables en la toma de decisiones.
- Mejora continua de los procedimientos de la empresa.
- Especificar el alcance de las políticas establecidas en base a los activos que deben ser protegidos.

1.3. Objetivos

1.3.1. Objetivo General

Implantar Políticas de Seguridad de la Información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

1.3.2. Objetivos Específicos

- Analizar procesos aplicados en la Cooperativa de Ahorro y Crédito San Francisco Ltda, relacionados a la Seguridad Informática.
- Evaluar la situación actual de la Seguridad Informática en los activos de información de la Cooperativa de Ahorro y Crédito San Francisco Ltda. que servirá como punto de partida para crear las políticas de seguridad de la información.
- Investigar normas y estándares internacionales para la Seguridad Informática que se adapten a las necesidades y realidad de la Cooperativa de Ahorro y Crédito San Francisco Ltda.
- Desarrollar un conjunto de políticas que permitan obtener un adecuado nivel de seguridad en los activos de información de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

CAPITULO II.- METODOLOGÍA

2.1. Materiales

Para la investigación se utilizan una encuesta y una entrevista:

2.1.1. La encuesta

La encuesta va dirigida al personal del Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco con la finalidad de obtener información sobre la seguridad de la información actual que se encuentra implementado en la organización y las necesidades para implementar políticas de seguridad en caso de producirse algunas amenazas y riesgos que puedan producirse a los activos de la Cooperativa.

2.1.2. La entrevista

Se realiza al Oficial de Seguridad de la Información de la Cooperativa San Francisco con la finalidad de obtener la información respectiva para aplicar políticas de seguridad que contrarresten cualquier tipo de amenazas y riesgos que se puede producir dentro de la institución.

2.2. Métodos

2.2.1. Modalidad de la Investigación

La presente investigación tiene un enfoque Cuali-cuantitativo, es cuantitativo porque se realizarán encuestas al personal del Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda. y es cualitativo porque se recabará la información directamente al jefe del Departamento de Tecnología y de la Unidad de Riesgo uso de la técnica de la entrevista.

En el presente proceso investigativo se han aplicado la investigación de campo y la investigación bibliográfica.

Mediante la investigación de campo se puede obtener la información de las normas de seguridad dentro del departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda., mediante la investigación bibliográfica se realiza la recopilación y análisis de información sobre el tema que se encuentra escrito en fuentes como libros, textos y documentos auxiliares en Internet [26].

Investigación Bibliográfica

Porque se recurre a información de artículos científicos, libros, tesis e internet y de esta manera recopilar documentación necesaria para el desarrollo del proyecto.

Investigación de campo

Porque se realizó en la Cooperativa de Ahorro y Crédito San Francisco Ltda. para obtener elementos de juicio necesarios para la investigación. Las técnicas para que se utilizaron son entrevistas y encuestas.

2.2.2. Población y Muestra

La población se define como el conjunto de individuos que cumplen ciertas características y de quienes se quiere obtener datos para el desarrollo de la investigación. La muestra es un subconjunto seleccionado de una población, que sigue ciertos patrones establecidos en la teoría del muestreo [26].

Para la presente investigación, se realizará con la población total, debido a que es reducida se trabajará con el departamento de tecnología y dentro de la Unidad de

riesgos con el Oficial de Seguridad de la Información de la Cooperativa San Francisco Ltda.

Tipo de Población	Número
Departamento de Tecnología	12
Unidad de Riesgos – Oficial de Seguridad de la Información	1
TOTAL:	13

Tabla 1. Tipo de población

Elaborado por: El investigador

2.2.3. Recolección de información

Las técnicas a usarse en la presente investigación serán: la entrevista y la encuesta dirigida al personal del Departamento de Tecnología y en la Unidad de Riesgos, al Oficial de Seguridad de la Información, para esto, es necesario hacer uso de las herramientas Guía de entrevistas y Cuestionario de encuesta respectivamente.

Preguntas Básicas	Explicación
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Departamento de Tecnologías Unidad de Riesgos – Oficial de Seguridad de la Información
¿Sobre qué aspectos?	Seguridad informática
¿Quién, Quienes?	Investigador: Mayra Gabriela Cordero Núñez
¿Cuándo?	Período académico Abril - Septiembre 2021
¿Dónde?	Cooperativa de Ahorro y Crédito San Francisco Ltda.
¿Cuántas veces?	Una

Preguntas Básicas	Explicación
¿Qué técnicas de recolección?	Entrevista Encuesta
¿Con qué?	Guía de entrevistas Cuestionario de encuestas
¿En qué situación?	En la condición de investigador

Tabla 2. Recopilación de información

Elaborado por: El investigador

2.2.4. Formato del instrumento a utilizar

Encuesta

Está destinada a recopilar la información de los funcionarios responsables de laborar dentro del departamento de tecnología de la Cooperativa San Francisco Ltda., para lo cual se utilizó el siguiente cuestionario con preguntas cerradas:

1. ¿Conoce qué es una política de seguridad?
   SI ( ) NO ( )
2. ¿Existen políticas de seguridad para el Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?
   SI ( ) NO ( )
3. ¿El personal de la Cooperativa tiene conocimiento sobre las políticas de seguridad?
   SI ( ) NO ( )
4. ¿Han tenido amenazas dentro del Departamento?
   SI ( ) NO ( )
5. ¿Desearía que se elabore una política de seguridad basada en normas/estándares internacionales?
   SI ( ) NO ( )
6. ¿Conoce acerca de estándares y normativas internacionales para la seguridad de la información?
7. SI ( ) NO ( )

¿Conoce acerca de las normas ISO/IEC 27000?

SI ( ) NO ( )

8. ¿Cree que la aplicación de algún estándar o normativa representará una mejora en la seguridad en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?

   SI ( ) NO ( )

Entrevista

La entrevista aplicada al oficial de riesgos se realizó basado en identificar los verdaderos problemas de seguridad que atraviesa la Cooperativa de Ahorro y Crédito San Francisco Ltda.

1. ¿Conoce acerca de normas internacionales para la seguridad de la información?
2. ¿Han presentado dificultades en la aplicación de alguna norma internacional para la seguridad de la información?
3. ¿Se ha capacitado al personal del departamento de tecnología en alguna norma o estándar internacional para el manejo de la seguridad de la información?
4. ¿Qué considera usted que ayudaría a la Cooperativa a cumplir con una norma internacional para la seguridad de la información?
5. ¿El Departamento de tecnología de la Cooperativa cuenta con políticas para la seguridad de la información? Si…. No…. ¿Por qué?
6. ¿Considera que las políticas de seguridad de la información son relevantes para el progreso y seguridad de la Cooperativa?
7. ¿Con qué frecuencia se actualizan las políticas de seguridad?
8. ¿Se socializan las políticas de seguridad con todo el personal de la Cooperativa?
9. ¿Cuentan con un área exclusiva para Seguridad de la Información?
10. ¿Existe un inventario de los activos de información?
11. ¿Al presentarse un fallo en los diferentes activos de información críticos, cómo se actuaría?

2.3. Procesamiento y Análisis de Datos

Encuesta

1. **¿Conoce qué es una política de seguridad?**

¿Conoce qué es una política de seguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	10	90,9	90,9	90,9
	NO	1	9,1	9,1	100,0
	Total	11	100,0	100,0	

Tabla 3. Conoce qué es una política de seguridad

Fuente: Investigador

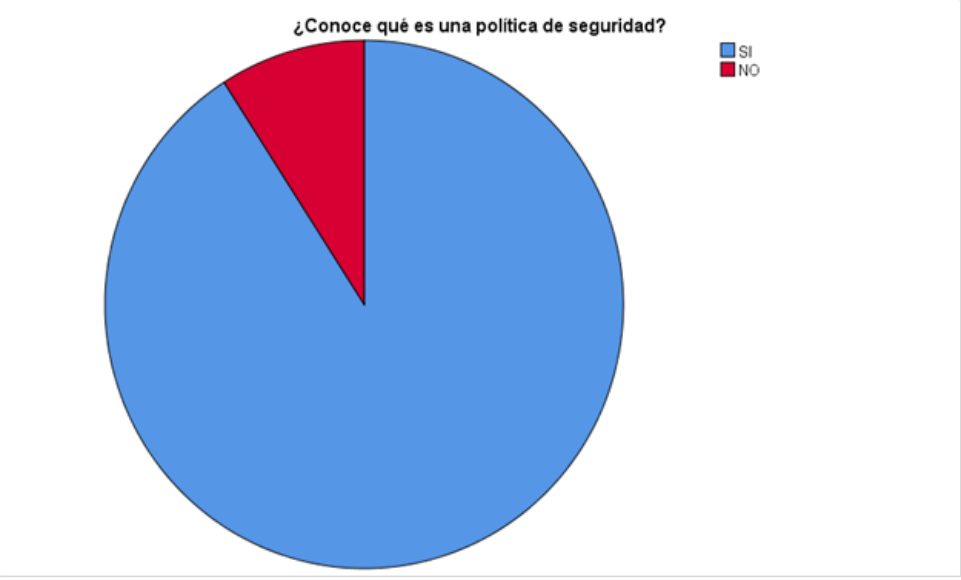

Figura 3. Conoce qué es una política de seguridad

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 10 correspondiente al 9% manifiesta que, si conoce lo que se refiere una política de seguridad, mientras tanto 1 encuestado correspondiente al 9% menciona que no conoce sobre el concepto de una política de seguridad.

2. **¿Existen políticas de seguridad para el Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?**

¿Existen políticas de seguridad para el Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	11	100,0	100,0	100,0

Tabla 4. Existen políticas dentro del Departamento TI

Fuente: Investigador

Figura 4. Existen políticas en el Departamento TIC

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 11 correspondiente al 100% manifiesta que si existen implementadas políticas de seguridad de la información dentro del Departamento de Tecnología de la Cooperativa de Ahorro y Cerdito San Francisco.

3. **¿El personal de la Cooperativa tiene conocimiento sobre las políticas de seguridad?**

¿El personal de la Cooperativa tiene conocimiento sobre las políticas de seguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	7	63,6	63,6	63,6
	NO	4	36,4	36,4	100,0
	Total	11	100,0	100,0	

Tabla 5. Personal conoce sobre las políticas de seguridad

Fuente: Investigador

Figura 5. Personal conoce sobre las políticas de seguridad
Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 7 correspondiente al 64% manifiesta que, si conocen sobre políticas de seguridad de la información dentro del Departamento de Tecnología de la Cooperativa de Ahorro y Cerdito San Francisco, mientras que 4 encuestados correspondiente al 36% manifiesta que no conocen estas políticas.

4. **¿Han tenido amenazas dentro del Departamento?**

¿Han tenido amenazas dentro del Departamento?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	8	72,7	72,7	72,7
	NO	3	27,3	27,3	100,0
	Total	11	100,0	100,0	

Tabla 6. El Departamento ha tenido amenazas

Fuente: Investigador

Figura 6. El Departamento ha tenido amenazas

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 8 correspondiente al 64% manifiesta que ha existido diferentes amenazas dentro Departamento de Tecnología de la Cooperativa de Ahorro y Cerdito San Francisco, mientras que 3 encuestados correspondiente al 36% manifiesta que no ha existido amenazas.

5. **¿Desearía que se elabore una política de seguridad basada en normas/estándares internacionales?**

¿Desearía que se elabore una política de seguridad basada en normas/estándares internacionales?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido SI	11	100,0	100,0	100,0

Tabla 7. Elaboración de una política de seguridad con estándares internacionales

Fuente: Investigador

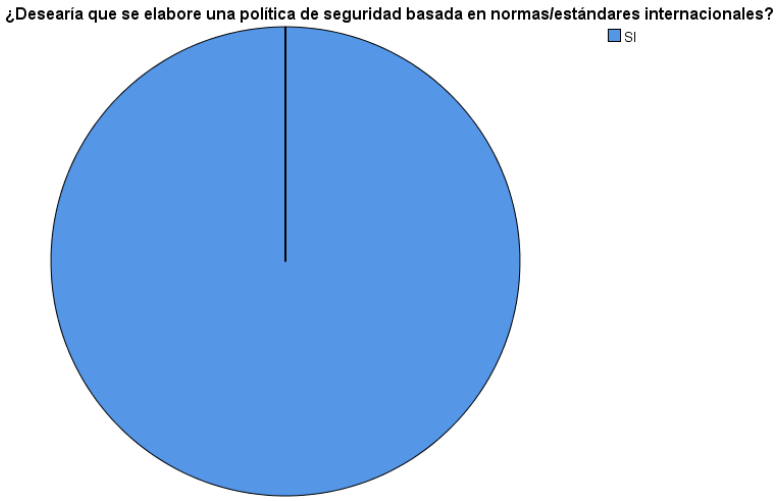

Figura 7. Elaboración de una política de seguridad con estándares internacionales

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 11 correspondiente al 100% está de acuerdo en que se elabore una política de seguridad para el Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco que se contemple en estándares internacionales.

6. **¿Conoce acerca de estándares y normativas internacionales para la seguridad de la información?**

¿Conoce acerca de estándares y normativas internacionales para la seguridad de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	7	63,6	63,6	63,6
	NO	4	36,4	36,4	100,0
	Total	11	100,0	100,0	

Tabla 8. Conoce las normas y estándares internaciones de seguridad

Fuente: Investigador

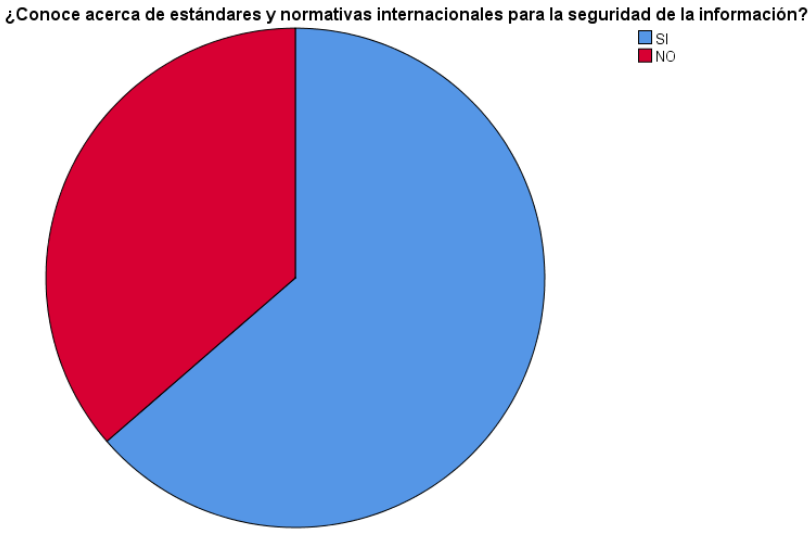

Figura 8. Conoce las normas y estándares internaciones de seguridad

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 7 correspondiente al 64% si conocen sobre las normas y estándares internaciones de seguridad, mientras tanto que 4 encuestados correspondientes al 36% manifiestan que no conocen de estos estándares.

7. ¿Conoce acerca de las normas ISO/IEC 27000?

¿Conoce acerca de las normas ISO/IEC 27000?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	4	36,4	36,4	36,4
	NO	7	63,6	63,6	100,0
	Total	11	100,0	100,0	

Tabla 9. Conoce las normas ISO/IEC 27000

Fuente: Investigador

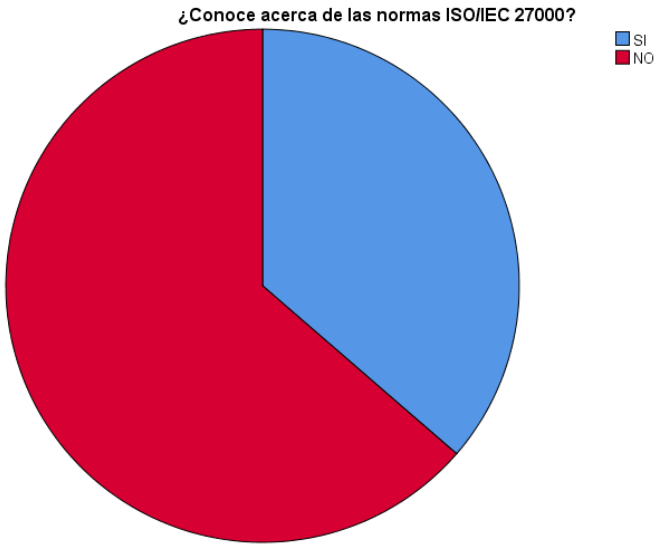

Figura 9. Conoce las normas ISO/IEC 27000

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 7 correspondiente al 64% no conoce sobre las normas de seguridad ISO/IEC 27000, mientras tanto que 4 encuestados correspondiente al 36% manifiestan que si conocen de estos estándares.

8. **¿Cree que la aplicación de algún estándar o normativa representará una mejora en la seguridad en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?**

¿Cree que la aplicación de algún estándar o normativa representará una mejora en la seguridad en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido SI	11	100,0	100,0	100,0

Tabla 10. La aplicación de un estándar intencional mejorará la seguridad

Fuente: Investigador

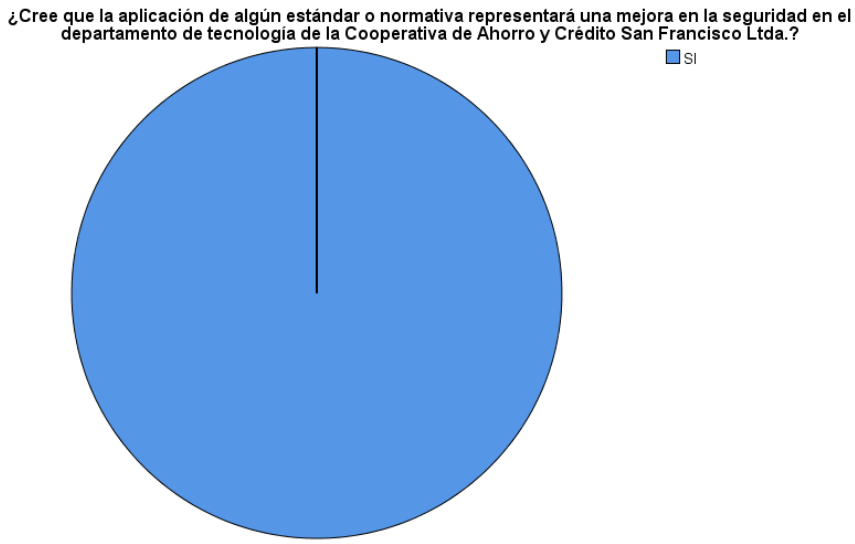

Figura 10. La aplicación de un estándar internacional mejorará la seguridad

Fuente: Investigador

Interpretación:

Se puede inferir que, de la población encuestada, 11 correspondiente al 100% creen que la aplicación de alguna norma o estándar internacional mejorará la seguridad en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

Análisis de resultados de las encuestas

Como se pude dar cuenta la encuestada manifiesta que la implementación de una política de seguridad basada en normas internacionales beneficiaría al Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.
La normativa ISO/IEC 27000 basada en los 14 dominios permitirá realizar políticas de seguridad para contrarrestar las amenazas y riesgos que puedan sufrir los activos de la cooperativa.

Entrevista

	Preguntas	**Jefe de Tecnología**	**Oficial de Seguridad de la Información**
1.	**¿Conoce acerca de normas internacionales para la seguridad de la información?**	Si, en la Cooperativa como entidad financiera regulada debe cumplir reglamentos de seguridad de la información asociadas a normas internacionales y marcos de buenas prácticas como ITIL.	Si
2.	**¿Han presentado dificultades en la aplicación de alguna norma internacional para la seguridad de la información?**	La principal dificultad es que las normativas son muy extensas y tienen mucho contexto americano o europeo y al momento de aterrizarlo a	Si, si hemos presentado dificultades por tipo de conocimiento y

		la realidad de la cooperativa se vuelven complejos.	dificultades técnicas
3.	**¿Se ha capacitado al personal del departamento de tecnología en alguna norma o estándar internacional para el manejo de la seguridad de la información?**	En estándares internacionales no se ha capacitado salvo en marcos de trabajo como ITIL que más bien tiene relación a la gestión de TI y no en seguridad de la información.	Tienen nociones básicas de normas y buenas prácticas.
4.	**¿Qué considera usted que ayudaría a la Cooperativa a cumplir con una norma internacional para la seguridad de la información?**	Establecer un marco de trabajo o metodología que permita realizar una traducción operativa de lo que dice la norma contra lo que hay que implementar.	Ayudaría que haya un apoyo por parte de Administración, para que todo el personal se inmiscuya y se comprometa con las normas de seguridad
5.	**¿El Departamento de tecnología de la Cooperativa cuenta con políticas para la seguridad de la información?**	Si, anteriormente el Departamento de tecnología se encargaba de la definición de las políticas de seguridad de la información, pero hace un tiempo la Cooperativa separó la Seguridad de la información como un área independiente de TI, la misma que se encarga de coordinar las políticas con Gerencia General y Riesgos. Esto para no ser juez y parte.	Existe un manual de buenas prácticas que es confidencial de la cooperativa.

6.	**¿Considera que las políticas de seguridad de la información son relevantes para el progreso y seguridad de la Cooperativa?**	Definitivamente si, una adecuada definición de las políticas y el monitoreo y control es relevante.	Desde luego que sí.
7.	**¿Con qué frecuencia se actualizan las políticas de seguridad?**	Las políticas y procedimientos generalmente se deben actualizar al menos una vez al año y se encarga el Oficial de Seguridad de la Información. También se realizan actualizaciones cuando el marco normativo cambia.	Se revisan cada año
8.	**¿Se socializan las políticas de seguridad con todo el personal de la Cooperativa?**	Existe un proceso de socialización para el personal interno y se trata de hacer seguimiento mediante inducciones o difusión de información relevante pero en análisis internos sabemos que el eslabón más débil es el factor humano, es por eso que la seguridad de la información es responsabilidad de todos.	Inicialmente cuando el personal ingresa a la Cooperativa se realiza una inducción, donde se les indica las políticas más relevantes, pero el manual de seguridad de la información está disponible en la red corporativa.
9.	**¿Cuentan con un área exclusiva para Seguridad de la Información?**	Área como tal, estamos en proceso de desarrollo, actualmente tenemos al oficial de Seguridad de la	El Área de Seguridad de la Información está separada del área

		Información que se encuentra dentro de la Unidad de Riesgos, esperamos que con la madurez que vayamos adquiriendo se pueda generar un área de seguridad de la información que no solo se encargue de la definición de políticas y seguimiento sino también del aterrizaje de normativas, medición y monitoreo.	de TI, es un área independiente que inclusive controla Riesgos, pero no es un área aún ya que solo está integrado por el Oficial de Seguridad de la Información.
10.	**¿Existe un inventario de los activos de información?**	Sí, es una de las principales actividades que ha realizado el Oficial de Seguridad de la Información donde incluye la sensibilidad y criticidad de cada activo.	Sí, es confidencial
11.	**¿Al presentarse un fallo en los diferentes activos de información críticos, cómo se actuaría?**	Por buena práctica institucional tenemos establecido un Plan de Contingencias que es confidencial, el que nos permite darle continuidad al negocio en caso de fallos. Ejm Mecanismos de réplica, mecanismos de respaldo periódico que nos permita salvaguardar la información y protegerla de eventos e incidentes que involucren pérdida de información como desastres y ataques.	Se actúa dependiendo al activo que esté fallando.

Análisis de resultados de las entrevistas

El Jefe de Tecnología y el Oficial de Seguridad de la Información proporcionaron información mediante entrevistas individuales de las cuales podemos concluir lo siguiente:

- Tienen conocimientos de normativas internacionales, pero no se ha capacitado al personal del departamento de tecnología en normas para seguridad de la información sino en gestión de TI como es ITIL
- Han presentado dificultades en la aplicación de normativas internacionales para la seguridad de la información, en aspectos técnicos y por aplicación de las normativas ya enfocadas a la realidad de la Cooperativa
- Las políticas de seguridad de la información están a cargo del Oficial de Seguridad de la Información, área que es independiente y no forma parte del Departamento de Tecnología.
- Poseen un manual de buenas prácticas (confidencial).
- Consideran que establecer políticas de seguridad, su control y monitoreo son relevantes para el progreso de la Cooperativa.
- Se encuentran en desarrollo de un área de seguridad de la información, esperan alcanzar un nivel de madurez superior para obtener dicha área y que se encargue del aterrizaje y monitoreo de políticas con normativas.
- Cuentan con un inventario de activos de información (confidencial) incluyendo su sensibilidad y criticidad.
- Poseen un plan de contingencias ante eventos e incidentes.

2.4. Comparación de las normativas

Existen muchos estándares internacionales para implementar políticas de seguridad dentro de una organización, la selección de estos estándares va a depender de la finalidad que persigue la empresa y el nivel de seguridad que requiere implementar dentro de la misma.

En un artículo publicado[27] muestra un estudio de los estándares más importantes existentes en el mercado internacional entre los cuales tenemos la ISO, COBIT e ITIL, las cuales fueron mencionadas anteriormente.

Normativas	Positivo	Negativo
ISO 27000	• Funciona para PYMES. • Mejor para proceso de producción y distribución de productos. • Centrado en proceso organizativos y de procedimientos competitivo. • Consigue mejoras en corto plazo y visibles. • Reduce costos como resultado del consumo consiente de materias primas. • Incrementa la productividad y la calidad. • Mejora la adaptación de los procesos a lo avanece tecnológicos. • Elimina redundancias.	• Se corre el riego de eliminar la perspectiva de interdependencia entre departamentos. • Demanda de un proceso de cambio para la organización. • Ofrece más resistencia al cambio en empresas de tipo conservador.
COBIT	• Ideal para todo tipo de empresa. PYME o gran empresa. • Expande la base de conocimiento a todos los sectores productivos de la empresa. • Centrado en los documentos.	• Se limita a los temas particulares y hay que adoptarlos por separado. • Requiere un tiempo prudencial para adaptarlos. • Pronuncia el abismo entre gerencias y operaciones.

	• Mejora los criterios para la toma de decisiones. • Define los planes estratégicos de la TI basados en la arquitectura de la red, información y equipos asociados. • Asegura el servicio continuo. • Ayuda en los procesos de auditoria.	
ITIL	• Conecta las TI con el negocio de seguridad, precisión, velocidad y disponibilidad de la entrega de servicios. • Enfocado en los procesos de negocio. • Más sencilla de adaptar al ser flexibles. • Mejora la comunicación entre usuarios finales, clientes y empleados de tu comparación.	• Demanda de tiempo y esfuerzo para lograr su completa absorción a la cultura organizacional. • Puede fomentar la burocracia y entorpecer la adopción no se tiene bien claros los objetivos. • Tiene cierta oscuridad respecto a los resultados, indicadores y control de desempeño.

Tabla 11. Normas y Estándares internacionales

Elaborado por: [27]

En función a la investigación realizada se procede a realizar una comparación de los estándares más importantes y de relevancia para la Cooperativa.

CUADRO COMPARATIVO NORMAS Y ESTÁNDARES INTERNACIONALES				
NORMA/ESTÁNDAR	**ISO 27001**	**ISO 27002**	**COBIT**	**ITIL**
Desarrollador	Comité técnico ISO/IEC JTC 1 Tecnología de la Información de la Organización Internacional de Normalización (ISO)	Comité técnico ISO/IEC JTC 1 Tecnología de la Información de la Organización Internacional de Normalización (ISO)	ISACA	Central Computing and Telecommunications Agency (CCTA)
Campo de Aplicación	Seguridad de la Información	Seguridad de la Información	Gobierno empresarial de Tecnologías de la información	Administración de servicios y procesos de tecnologías de la información
Fases/Dominios/Controles	14 dominios, 35 objetivos de control y 114 controles	14 dominios, 35 objetivos de control y 114 controles	5 dominios del modelo de referencia, 37 procesos de gobierno y gestión	5 fases de gestión TI

Fortalezas	Mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos.	Establece un mayor control de accesos a aplicaciones y la información	Está enfocada al logro de objetivos de la organización.	Propone buenas prácticas para el mantenimiento y la mejora de la gestión en los servicios de las organizaciones.
Debilidades	Para que tenga éxito la normativa es necesario el compromiso de toda la organización empezando por la dirección.	Para que tenga éxito la normativa es necesario el compromiso de toda la organización empezando por la dirección.	Orientada a los objetivos de gobierno y delimita un poco la seguridad	Constantes prácticas de mantenimiento de los servicios de gestión.

Tabla 12. Cuadro Comparativo Normas y Estándares Internacionales

Elaborado por: Investigador

La normativa de seguridad ISO 27002 busca minimizar los riesgos de la gran variedad de amenazas internas como externas a las se somete la información de una determinada organización, esta normativa establece un mayor control de accesos a aplicaciones y a la información, además el mayor éxito se conseguirá con el compromiso y cumplimiento total de las políticas por parte de todas las autoridades, trabajadores y usuarios.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

Mediante la aplicación de la encuesta y la entrevista se pudo determinar que es importante la creación de políticas de seguridad de la información dentro de la Cooperativa de Ahorro y Crédito San Francisco basado en las normativas internacionales, las cuales nos permitirán tener un mejor control de los activos de información, así como su disponibilidad, integridad y confidencialidad.

Mediante la comparación de las normativas y estándares internacionales se pudo determinar que la norma ISO 27002 es la más indicada para la cooperativa ya que hoy en día en el país se ha observado que las instituciones financieras son un objetivo importante para los ataques cibernéticos y con la normativa ISO 27002, se busca minimizar los riesgos de la gran variedad de amenazas internas y externas a las que está expuesta la información; esta norma también nos permite identificar y enmendar puntos débiles en la seguridad de la información y está enfocada en la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

Adicionalmente, se ha elegido la Norma ISO 27002 para establecer las políticas de seguridad en la cooperativa por las siguientes razones:

- Detalla la definición de cada uno de los controles de la normativa.
- Permite conocer y mejorar el control de activos de la información
- Permite identificar y corregir puntos débiles e la seguridad de la información
- Permite el normal funcionamiento de la organización por ende mejora la reputación entre proveedores clientes.
- Una de las fortalezas es el control de acceso a la información.
- Debe existir una capacitación constante a los miembros de la organización para que aplique una normativa de seguridad y por ende el compromiso de todos para que se lleve las funciones con eficiencia.

3.2. Desarrollo de la propuesta

Existen varias metodologías para el análisis de riesgos como son OCTAVE, MEHARI y NIST SP, sin embargo, este proyecto se enmarca en la metodología Magerit ya que está enfocada al análisis y gestión de riesgos de TI, la cual permite dividir o seccionar los activos de información para de esta forma identificar riesgos y actuar para mitigar los mismos.

La metodología Magerit se divide en tres procesos principales, cada uno de estos compuestos por actividades y tareas hasta plantear políticas de seguridad en una organización.

1. Planificación
2. Análisis de riesgos
3. Gestión de riesgos

Figura 11. Procesos de la metodología Magerit para Análisis y gestión de Riesgos

Fuente: El investigador

3.2.1. Proceso 1: Planificación

Este proceso tiene como objetivo principal a establecer un marco general de referencia para el proyecto de seguridad que se lleva a cabo dentro de la organización.

Para lo cual debe cumplir con los siguientes objetivos:

- Motivar, concientizar e involucrar al personal del Departamento de Tecnología de Información de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

- Reflexionar sobre la oportunidad de construir un proyecto de Políticas de Seguridad dentro de la organización.

3.2.1.1. Actividad 1: Determinación del alcance del proyecto

En esta actividad se definen los objetivos finales del proyecto, además se realiza una identificación del entorno de la organización, así como también se analiza las restricciones generales dentro de la elaboración del mismo.

Objetivo:
Identificar las vulnerabilidades a las que se encuentra expuesto el flujo de información que se lleva a cabo en el área de gestión de la Cooperativa de Ahorro y Crédito San Francisco.

Restricciones:

- Personal no capacitado
- Conflictividad laboral
- Tiempos de respuesta a las solicitudes
- Tiempos de respuesta de las evaluaciones

Alcance:

Generar las recomendaciones necesarias para garantizar la seguridad del flujo de información dentro del Departamento de Tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

Identificación del Proceso:

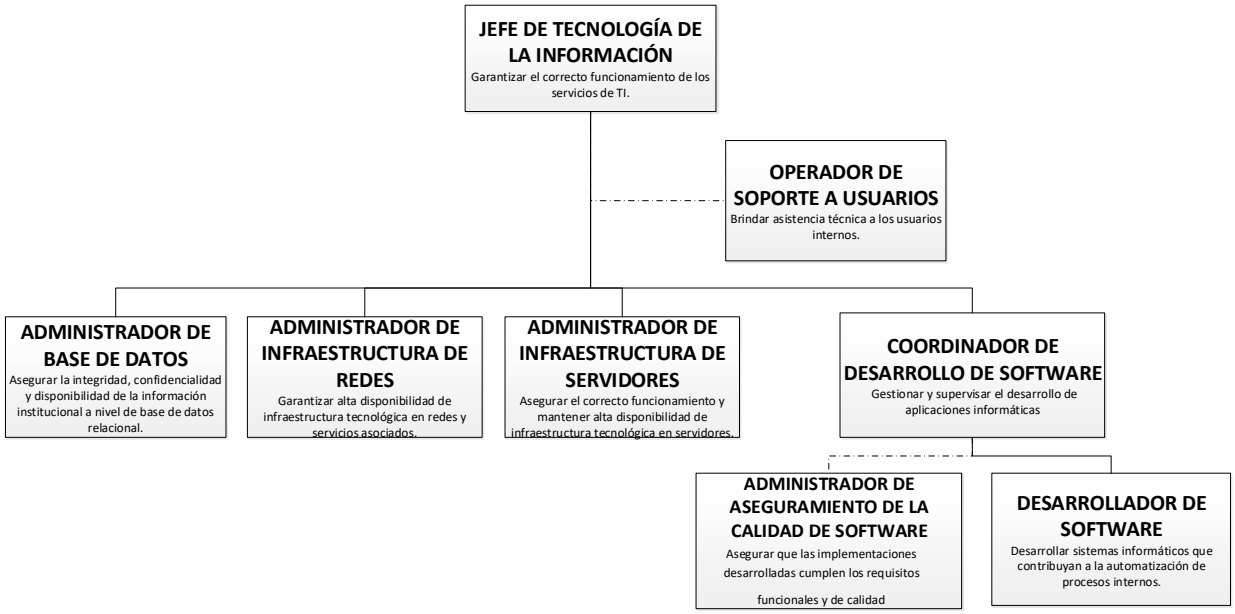

Figura 12. Organigrama del Departamento de Tecnología de la Cooperativa San Francisco Ltda.

Fuente: Cooperativa San Francisco Ltda.

Jefe de Tecnología de la Información

Tiene como finalidad garantizar el correcto funcionamiento de los servicios TI. Dentro del departamento de Tecnología de Información consta de 5 áreas que son:

Operador de soporte a usuarios:

Son responsables de brindar asistencia técnica a los usuarios internos.

Administrador de base de datos:

Tiene como finalidad garantizar la integridad, confidencialidad y disponibilidad de la información institucional a nivel de bases de datos relacionales.

Estas son las tareas más importantes que realiza el administrador de base de datos:

- Actualización de datos
- Ceración de usuarios
- Datos erróneos

- Modificación de datos.

Administrador de la infraestructura de redes:
Tiene como finalidad garantizar la alta disponibilidad de la infraestructura de redes y de los servicios asociados.

Administrador de la infraestructura de servidores:
Tiene como finalidad de asegurar el correcto funcionamiento y mantener la disponibilidad de la infraestructura tecnológica en servidores.

Coordinador de desarrollo de software:
Tiene como finalidad gestionar y supervisar el desarrollo de las aplicaciones informáticas. Dentro de este se tiene 2 subáreas:

- **Administrador de aseguramiento de la calidad de software**, tiene como finalidad asegurar que las aplicaciones desarrolladas cumplan con los requisitos de calidad.
- **Desarrollador de software,** tiene como finalidad desarrollar aplicaciones informáticas que contribuyan al funcionamiento de la organización.

3.2.1.2. Actividad 2: Planificación del proyecto

Dentro de esta actividad se define los participantes y se organiza el trabajo para llevar a cabo las siguientes tareas:

- Planificar las entrevistas
- Organizar e identificar a los participantes involucrados en la investigación
- Planificar el trabajo a realizar.

3.2.1.3. Actividad 3: Lanzamiento del proyecto

Se generan los instrumentos para la recolección de datos tanto encuestas y entrevistas para la recolección de datos y obtención de la información de las áreas más importantes.

De esta actividad se obtiene la información relevante de los activos, amenazas, impactos, controles existentes en la Cooperativa de Ahorro y Crédito San Francisco Ltda.

3.2.2. Proceso 2: Análisis de Riesgos

Este proceso es el núcleo central de la metodología Magerit [28] y tiene como finalidad verificar su validez y la utilidad del proyecto aplicando correctamente las directrices estipuladas. Aquí se identifican de los activos y sus posibles amenazas y se plantea posibles soluciones.

Este proceso tiene los siguientes objetivos:

- Desarrollar un modelo de sistema de seguridad para lo cual se identifican y se valoran los activos de la organización más relevantes.
- Evaluar el impacto y el riesgo de los activos.
- Mostrar al jefe del departamento las áreas con mayor impacto o riesgo.

3.2.2.1. Actividad 1: Caracterización de los activos

En esta actividad se identifica la información más importante del proceso, además se determina las dimensiones de seguridad más importantes:

- **Identificación de los activos**

A continuación, se describen los activos más importantes de la Cooperativa de Ahorro y Crédito San Francisco Ltda.:

Activo	**Especificación**	**Descripción**
[D] Datos e información	• Datos de gestión financiera • Datos de gestión administrativa • Datos de gestión interna • Copias de seguridad • Datos clasificados reservados • Datos clasificados confidenciales	La información general de la Cooperativa, socios, clientes, préstamos, información referente a los créditos, que se almacena en un dispositivo de almacenamiento o bases de datos.
[S] Servicios	• Página web (www) • Correo electrónico • Almacenamiento de datos • Gestión de permisos • Gestión de privilegios • Servicio de cajero automático • Servicios de terceros	Los diferentes servicios que presta la cooperativa para la ciudadanía.
[SW] Software - Aplicaciones informáticas	• Sistema de gestión financiera • Sistema Contable • Sistema de procesos internos de la cooperativa • Sitio Web de la Cooperativa • Microsoft Office • Antivirus • Drivers	Las diferentes aplicaciones y software de que utiliza la Cooperativa para que se ejecuten las diferentes actividades financieras así como también las actividades administrativas.

Activo	Especificación	Descripción
[HW] Hardware – Equipos informáticos	• Equipos de cómputo servidores • Equipos personales • Dispositivos de almacenamiento • Cajeros automáticos • Contador de billetes • Contador de monedas • Lector de huellas digitales • Impresoras • Escáner • Hubs • Routers • Cortafuegos • Puntos de acceso	Los diferentes equipos informáticos de la Cooperativa que son utilizados por el personal que labora en la cooperativa y el departamento de tecnologías.
[COM] Redes de comunicaciones	• Internet • Red local • Red con las sucursales • Red telefónica • Red inalámbrica	La infraestructura de la red del departamento de tecnología de la Cooperativa y de la Cooperativa.
[MEDIA] Soporte	• Discos duros externos • Dispositivos USB • CD ROM • DVD ROM • Material impreso	Son los dispositivos que nos permiten almacenar información en formato electrónico y que en general dentro de la Cooperativa San Francisco Ltda.
[L] Instalaciones	• Lugar para la ubicación de los equipos • Edificio	Lugar donde se ubican los diferentes equipos informáticos administrados por el departamento de tecnología.

Activo	Especificación	Descripción
[P] Personal	• Usuarios internos • Operadores • Administradores de sistemas • Desarrolladores	Controlan y supervisan el todo el trabajo que se desenvuelve dentro de la Cooperativa de Ahorro y Crédito San Francisco Ltda., mediante equipos de cómputo.

Tabla 13. Definición de activos de la Cooperativa

Elaborado por: El investigador

Para cada tipo de activos se determinan las características que definen a cada activo tomando en cuenta las siguientes características de seguridad.

Disponibilidad (D): Asegurar de que los usuarios autorizados tengan acceso cuando se requiera información y sus activos.

Integridad (I): Garantizar que la información obtenida sea exacta y completa mediante métodos de procesamiento adecuados.

Confidencialidad (C): Asegurar que la accesibilidad de la información sólo sea para aquellos usuarios registrados con los permisos adecuados.

Autenticidad de los usuarios del servicio (A): Asegurar la identidad y origen de la información.

Trazabilidad (T): Asegurar de que los movimientos de la información sean realizados por las personas adecuadas.

[D] Datos / Información					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Datos de gestión financiera	X	X	X	X	X
Datos de gestión administrativa	X	X	X	X	X
Datos de gestión interna	X	X	X	X	X
Copias de seguridad	X	X	X	X	X
Datos clasificados reservados	X	X	X	X	X
Datos clasificados confidenciales	X	X	X	X	X

Tabla 14. Definición de activos – Datos / Información

Elaborado por: El investigador

Servicios					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Página web (www)	X		X		
Correo electrónico	X		X		
Almacenamiento de datos	X		X		
Gestión de permisos	X		X		
Gestión de privilegios	X		X		
Servicio de cajero automático	X		X		

Tabla 15. Definición de activos – Servicios

Elaborado por: El investigador

Software / Aplicaciones informáticas					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Sistema de gestión financiera contratado	X	X	X	X	X
Sistema de gestión administrativa	X	X	X	X	X
Sistema de gestión de base de datos	X	X	X	X	X

Software / Aplicaciones informáticas					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Navegador Web de la Cooperativa	X				
Microsoft office	X				
Antivirus	X				
Sistema operativo	X				
Sistema backup	X	X	X		
Drivers	X				

Tabla 16. Definición de activos – Software / Aplicaciones informáticas

Elaborado por: El investigador

Hardware – Equipos informáticos					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Equipos de cómputo servidores	X	X	X	X	X
Equipos personales	X				
Dispositivos de almacenamiento	X				
Cajeros automáticos	X				
Contador de billetes	X				
Contador de monedas	X				
Lector de huellas digitales	X				
Impresoras	X				
Escáner	X				
Hubs	X				
Routers	X				
Cortafuegos	X				
Puntos de acceso	X				
Cableado	X				

Tabla 17. Definición de activos – Hardware / Equipos informáticos

Elaborado por: El investigador

Redes de comunicaciones					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Internet	X		X		
Red local	X		X		
Red con las sucursales	X		X		
Red telefónica	X		X		
Red inalámbrica	X		X		

Tabla 18. Definición de activos – Redes de comunicaciones

Elaborado por: El investigador

Soporte de la información					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Discos duros externos			X		
Dispositivos USB			X		
CD ROM			X		
DVD ROM			X		
Material impreso			X		

Tabla 19. Definición de activos – Soporte de la información

Elaborado por: El investigador

Instalaciones					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Lugar para ubicar los equipos	X		X		
Edificio	X		X		

Tabla 20. Definición de activos – Instalaciones

Elaborado por: El investigador

Personal					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Usuarios internos	X		X		
Operadores	X		X		
Administradores de sistemas	X	X	X	X	X
Desarrolladores	X		X		

Tabla 21. Definición de activos – Personal

Elaborado por: El investigador

A continuación, se presenta la información en una tabla resumen:

Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[D] Datos / Información					
Datos de gestión financiera	X	X	X	X	X
Datos de gestión administrativa	X	X	X	X	X
Datos de gestión interna	X	X	X	X	X
Copias de seguridad	X	X	X	X	X
Datos clasificados reservados	X	X	X	X	X
Datos clasificados confidenciales	X	X	X	X	X
[S] Servicios					
Página web (www)	X		X		
Correo electrónico	X		X		
Almacenamiento de datos	X		X		
Gestión de permisos	X		X		
Gestión de privilegios	X		X		
Servicio de cajero automático	X		X		
[SW] Software / Aplicaciones informáticas					

Activos	Características de Seguridad				
	D	**I**	**C**	**A**	**T**
Sistema de gestión financiera contratado	X	X	X	X	X
Sistema de gestión administrativa	X	X	X	X	X
Sistema de gestión de base de datos	X	X	X	X	X
Navegador Web de la Cooperativa	X				
Microsoft office	X				
Antivirus	X				
Sistema operativo	X				
Sistema backup	X	X	X		
Drivers	X				
[HW] Hardware – Equipos informáticos					
Equipos de cómputo servidores	X	X	X	X	X
Equipos personales	X				
Dispositivos de almacenamiento	X				
Cajeros automáticos	X				
Contador de billetes	X				
Contador de monedas	X				
Lector de huellas digitales	X				
Impresoras	X				
Escáner	X				
Hubs	X				
Routers	X				
Cortafuegos	X				
Puuntos de acceso	X				
Cableado	X				
[COM] Redes de comunicaciones					
Internet	X		X		
Red local	X		X		

Activos	Características de Seguridad				
	D	**I**	**C**	**A**	**T**
Red con las sucursales	X		X		
Red telefónica	X		X		
Red inalámbrica	X		X		
[MEDIA] Soporte de la información					
Discos duros externos			X		
Dispositivos USB			X		
CD ROM			X		
DVD ROM			X		
Material impreso			X		
[L] Instalaciones					
Lugar para ubicar los equipos	X		X		
Edificio	X		X		
[P] Personal					
Usuarios internos	X		X		
Operadores	X		X		
Administradores de sistemas	X	X	X	X	X
Desarrolladores	X		X		

Tabla 22. Cuadro de descripción de los activos

Elaborado por: El investigador

- **Valoración de activos**

Para valorar los activos se utiliza la siguiente tabla de criterios:

Valoración de los activos			
Valor			**Criterio**
10	Muy Alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización

Valoración de los activos			
Valor			**Criterio**
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos prácticos

Tabla 23. Cuadro de criterios para la valoración de activos

Elaborado por: El investigador

Valoración de los activos					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[D] Datos / Información					
Datos de gestión financiera	10	10	10	10	10
Datos de gestión administrativa	10	10	10	10	10
Datos de gestión interna	10	10	10	10	10
Copias de seguridad	10	10	10	10	10
Datos clasificados reservados	10	10	10	10	10
Datos clasificados confidenciales	10	10	10	10	10
[S] Servicios					
Página web (www)	8				
Correo electrónico	9		9		
Almacenamiento de datos	10		10		
Gestión de permisos	10		10		
Gestión de privilegios	10		10		
Servicio de cajero automático	10		10		
[SW] Software / Aplicaciones informáticas					
Sistema de gestión financiera contratado	8	8	8	8	8
Sistema de gestión administrativa	8	8	8	8	8
Sistema de gestión de base de datos	8	8	8	8	8
Navegador Web de la Cooperativa	8				

Valoración de los activos					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Microsoft office	8				
Antivirus	8				
Sistema operativo	8				
Sistema backup	10	10	10	10	
Drivers	8				
[HW] Hardware – Equipos informáticos					
Equipos de cómputo servidores	9	9	9	9	9
Equipos personales	8				
Dispositivos de almacenamiento	8				
Cajeros automáticos	8				
Contador de billetes	8				
Contador de monedas	8				
Lector de huellas digitales	8				
Impresoras	8				
Escáner	8				
Hubs	8				
Routers	8				
Cortafuegos	8				
Puntos de acceso	8				
Cableado	8				
[COM] Redes de comunicaciones					
Internet	8		8		
Red local	10		10		
Red con las sucursales	10		10		
Red telefónica	10		10		
Red inalámbrica	8		8		
[MEDIA] Soporte de la información					

Valoración de los activos					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
Discos duros externos			8		
Dispositivos USB			9		
CD ROM			8		
DVD ROM			9		
Material impreso			9		
[L] Instalaciones					
Lugar para ubicar los equipos	10		10		
Edificio	10		10		
[P] Personal					
Usuarios internos	10		10		
Operadores	10		10		
Administradores de sistemas	10	10	10	10	10
Desarrolladores	10		10		

Tabla 24. Valoración de activos de la organización

Elaborado por: El investigador

3.2.2.2. Actividad 2: Caracterización de las amenazas

- **Identificación de las amenazas**

Esta actividad tiene como finalidad observar las amenazas que se pueden dar sobre los activos que han sido identificados, para la identificación de amenazas se basa en catálogo de elementos de metodología análisis y gestión de riesgos de los sistemas de información (Magerit).

Las amenazas son valoradas de acuerdo al siguiente nivel:

Nivel de Valoración	Relevancia
1	Muy Alta
2	Alta
3	Media
4	Baja
5	Despreciable

Tabla 25. Niveles de valoración de las amenazas

Elaborado por: El investigador

Existen algunos tipos de amenazas que son las siguientes:

- Desastres naturales
- Industriales
- Fallos no intencionales
- Ataques intencionados

Desastres naturales: Dentro de estas amenazas se encuentran todas las provocadas ocasionados por algún evento originado por la naturaleza.

[N] Desastres Naturales					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[N.1] Fuego					
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				
[MEDIA] Soportes de información	1				
[L] Instalaciones	1				
[N.2] Daños por agua					
[HW] Equipos informáticos (hardware)	1				

[N] Desastres Naturales					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[COM] Redes de comunicaciones	1				
[MEDIA] Soportes de información	1				
[L] Instalaciones	1				

Tabla 26. Amenazas de desastres naturales

Elaborado por: El investigador

Industriales: Son amenazas que pueden aparecer de forma accidental, mimas que son producto de la actividad humana de tipo industrial.

[I] Industrial					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[I.1] Fuego					
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				
[MEDIA] Soportes de información	1				
[L] Instalaciones	1				
[I.2] Daños por agua					
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				
[MEDIA] Soportes de información	1				
[L] Instalaciones	1				
[I.6] Corte de suministro eléctrico					
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				

[I] Industrial					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[MEDIA] Soportes de información	1				
[I.7] Condiciones inadecuadas de temperatura y/o humedad					
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				
[MEDIA] Soportes de información	1				
[I.8] Fallo de servicios de comunicaciones					
[COM] Redes de comunicaciones	1				
[I.10] Degradación de los soportes de almacenamiento de información					
[MEDIA] Soportes de información	1				
[I.11] Emanaciones electromagnéticas					
[HW] Equipos informáticos (hardware)			1		
[COM] Redes de comunicaciones			1		
[L] Instalaciones			1		

Tabla 27. Amenazas de tipo industrial

Elaborado por: El investigador

Errores o fallos no intencionales: Son aquellas amenazas producto de los errores o fallos no intencionales causados por las personas.

[E] Errores o fallos no intencionales					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[E.1] Errores de los usuarios					
[S] Servicios	3	1	2		
[D] Datos / información	3	1	2		
[SW] Aplicaciones (software)	3	1	2		

[E] Errores o fallos no intencionales					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[E.2] Errores del administrador					
[S] Servicios	1	2	3		
[D] Datos / información	1	2	3		
[SW] Aplicaciones (software)	1	2	3		
[HW] Equipos informáticos (hardware)	1	2	3		
[COM] Redes de comunicaciones	1	2	3		
[E.4] Errores de configuración					
[D] Datos / información		1			
[E.8] Difusión de software dañino					
[SW] Aplicaciones (software)	1	2	3	4	5
[E.14] Escapes de información					
[D] Datos / información			1		
[E.15] Alteración accidental de información					
[D] Datos / información		1			
[E.16] Introducción de información incorrecta					
[D] Datos / información		1			
[E.17] Degradación de la información					
[D] Datos / información		1			
[E.18] Destrucción de la información					
[D] Datos / información	1				
[E.19] Divulgación de la información					
[D] Datos / información			1		
[E.20] Vulnerabilidades de los programas (software)					
[SW] Aplicaciones (software)	2	1	3		
[E.21] Errores de mantenimiento / actualización de programas (software)					
[SW] Aplicaciones (software)	2	1			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)					
[HW] Equipos informáticos (hardware)	1				

[E] Errores o fallos no intencionales					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[E.24] Caída del sistema por agotamiento de recursos					
[S] Servicios	1				
[HW] Equipos informáticos (hardware)	1				
[COM] Redes de comunicaciones	1				
[E.28] Indisponibilidad del personal					
[P] Personal interno	1				

Tabla 28. Amenazas por errores o fallos no intencionales

Elaborado por: El investigador

Ataques intencionados: Son aquellas amenazas producto de los ataques intencionados provocados por las personas.

[A] Ataques intencionados					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[A.3] Manipulación de los registros de actividad					
[D] Datos / información		1			2
[A.4] Manipulación de la configuración					
[S] Servicios	3	1	2		
[D] Datos / información	3	1	2		
[SW] Aplicaciones (software)	3	1	2		
[HW] Equipos informáticos (hardware)	3	1	2		
[COM] Redes de comunicaciones	3	1	2		
[A.5] Suplantación de la identidad del usuario					
[S] Servicios		3	1	2	
[SW] Aplicaciones (software)		3	1	2	

[A] Ataques intencionados					
Activos	**Características de Seguridad**				
	D	**I**	**C**	**A**	**T**
[COM] Redes de comunicaciones		3	1	2	
[A.6] Abuso de privilegios de acceso					
[S] Servicios	3	2	1		
[SW] Aplicaciones (software)	3	2	1		
[HW] Equipos informáticos (hardware)	3	2	1		
[COM] Redes de comunicaciones	3	2	1		
[A.8] Difusión de software dañino					
[SW] Aplicaciones (software)	2	1	1		
[A.11] Acceso no autorizado					
[S] Servicios		2	1		
[D] Datos / información		2	1		
[SW] Aplicaciones (software)		2	1		
[HW] Equipos informáticos (hardware)		2	1		
[COM] Redes de comunicaciones		2	1		
[MEDIA] Soportes de información		2	1		
[L] Instalaciones		2	1		

Tabla 29. Amenazas por ataques intencionados

Elaborado por: El investigador

- **Valoración de las amenazas**

  Para la valorar las amenazas se toma en cuenta los siguientes aspectos:

  - Frecuencia de cada amenaza sobre cada activo
  - Degradación de los activos, se considera la degradación que causaría la amenaza en cada dimensión del activo si llegara a realizarse

Valor			Descripción
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	N	Una vez al año
0.1	Poco frecuente	PF	Cada varios años

Tabla 30. Frecuencia de amenazas

Elaborado por: El investigador

Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% - 99%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Tabla 31. Criterios para la degradación de activos

Elaborado por: El investigador

A continuación, se procede a valorar las amenazas en cada uno de los activos:

[D] Datos / información						
Amenazas	Frecuencia	Características de Seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	MF	3	1	2		
[E.2] Errores del administrador	PF	1	2	3		
[E.4] Errores de configuración	PF		1			
[E.14] Escapes de información	PF			1		
[E.15] Alteración accidental de información	PF		1			
[E.16] Introducción de información incorrecta	N		1			
[E.17] Degradación de la información	N		1			

[D] Datos / información						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[E.16] Destrucción de la información	PF	1				
[E.19] Divulgación de la información	PF					
[A.3] Manipulación de los registros de actividad	PF		1			2
[A.3] Manipulación de la configuración	N	3	1	2		
[A.11] Acceso no autorizado	PF		2	1		

Tabla 32. Valoración de amenazas – Datos / información

Elaborado por: El investigador

[S] Servicios						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[E.1] Errores de los usuarios	MF	3	1	2		
[E.2] Errores del administrador	PF	1	2	3		
[E.24] Caída del sistema por agotamiento de recursos	N	1				
[A.4] Manipulación de la configuración	PF	3	1	2		
[A.5] Suplantación de la identidad del usuario	PF		3	1	2	
[A.6] Abuso de privilegios de acceso	F	3	2	1		
[A.11] Acceso no autorizado	F		2	1		

Tabla 33. Valoración de amenazas – Servicios

Elaborado por: El investigador

[SW] Software – aplicaciones informáticas						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[E.1] Errores de los usuarios	MF	3	1	2		
[E.2] Errores del administrador	PF	1	2	3		
[E.8] Difusión de software dañino	N	1	2	3	4	5
[E.20] Vulnerabilidades de los programas (software)	PF	2	1	3		
[A.4] Manipulación de la configuración	PF	3	1	2		
[A.5] Suplantación de la identidad del usuario	PF		3	1	2	
[A.6] Abuso de privilegios de acceso	F	3	2	1		
[A.8] Difusión de software dañino	MF	2	1	1		
[A.11] Acceso no autorizado	F		2	1		

Tabla 34. Valoración de amenazas – Software – aplicaciones informáticas

Elaborado por: El investigador

[HW] Hardware – Equipos informáticos						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[N.1] Fuego	PF	1				
[N.2] Daños por agua	PF	1				
[I.1] Fuego	PF	1				
[I.2] Daños por agua	PF	1				
[I.6] Corte de suministro eléctrico	N	1				
[I.7] Condiciones inadecuadas de temperatura y/o humedad	N	1				

[HW] Hardware – Equipos informáticos						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[I.11] Emanaciones electromagnéticas	PF	1				
[E.2] Errores del administrador	PF	1	2	3		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PF	1				
[E.24] Caída del sistema por agotamiento de recursos	N	1				
[A.4] Manipulación de la configuración	PF	3	1	2		
[A.6] Abuso de privilegios de acceso	PF	3	2	1		
[A.11] Acceso no autorizado	N		2	1		
[A.25] Robo	PF	1		2		

Tabla 35. Valoración de amenazas – Hardware – equipos informáticos

Elaborado por: El investigador

[MEDIA] Soportes de información						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[N.1] Fuego	PF	1				
[N.2] Daños por agua	PF	1				
[I.1] Fuego	PF	1				
[I.2] Daños por agua	PF	1				
[I.6] Corte de suministro eléctrico	N	1				
[I.7] Condiciones inadecuadas de temperatura y/o humedad	N	1				

[MEDIA] Soportes de información						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[I.10] Degradación de los soportes de almacenamiento de información	N	1				
[A.11] Acceso no autorizado	PF		2	1		
[A.25] Robo	PF	1		2		

Tabla 36. Valoración de amenazas – Soportes de información

Elaborado por: El investigador

[COM] Redes de comunicaciones						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[I.8] Fallo de servicios de comunicaciones	N	1				
[E.2] Errores del administrador	PF	1	2	3		
[E.24] Caída del sistema por agotamiento de recursos	N	1				
[A.4] Manipulación de la configuración	PF	3	1	2		
[A.5] Suplantación de la identidad del usuario	PF		3	1	2	
[A.6] Abuso de privilegios de acceso	PF	3	2	1		
[A.11] Acceso no autorizado	PF		2	1		

Tabla 37. Valoración de amenazas – Redes de comunicaciones

Elaborado por: El investigador

[L] Instalaciones						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[N.1] Fuego	PF	1				
[N.2] Daños por agua	PF	1				
[I.1] Fuego	PF	1				
[I.2] Daños por agua	PF	1				
[I.11] Emanaciones electromagnéticas	N			1		
[A.11] Acceso no autorizado	PF		2	1		

Tabla 38. Valoración de amenazas – Instalaciones

Elaborado por: El investigador

[P] Personal						
Amenazas	**Frecuencia**	**Características de Seguridad**				
		D	**I**	**C**	**A**	**T**
[E.7] Deficiencias en la organización	N	1				
[E.28] Indisponibilidad del personal	N	1				

Tabla 39. Valoración de amenazas – Personal

Elaborado por: El investigador

3.2.2.3. Actividad 3: Caracterización de los controles existentes

- **Controles existentes**

Para cada activo se identifican los controles existentes, así como también el nivel de seguridad.

Controles existentes de los activos		
Activo	**Control existente**	**Eficacia**
[D] Datos / Información		
Datos de gestión financiera	Existente	80 %
Datos de gestión administrativa	Existente	80 %
Datos de gestión interna	Existente	80 %
Copias de seguridad	Existente	90 %
Datos clasificados reservados	Existente	90 %
Datos clasificados confidenciales	Existente	90 %
[S] Servicios		
Página web (www)	Existente	90 %
Correo electrónico	Existente	90 %
Almacenamiento de datos	Existente	90 %
Gestión de permisos	Existente	90 %
Gestión de privilegios	Existente	90 %
Servicio de cajero automático	Existente	90 %
Servicios de terceros	Existente	80 %
[SW] Software / Aplicaciones informáticas		
Sistema de gestión financiera contratado	Existente	90 %
Sistema de gestión administrativa	Existente	90 %
Sistema de gestión de base de datos	Existente	90 %
Navegador Web de la Cooperativa	Existente	90 %
Microsoft office	Existente	80 %
Antivirus	Existente	90 %
Sistema operativo	Existente	90 %
Sistema backup	Existente	80%
Drivers	Existente	90 %
[HW] Hardware – Equipos informáticos		
Equipos de cómputo servidores	Existente	90 %

Controles existentes de los activos		
Activo	**Control existente**	**Eficacia**
Equipos personales	Existente	90 %
Dispositivos de almacenamiento	Existente	90 %
Cajeros automáticos	Existente	90 %
Contador de billetes	Existente	90 %
Contador de monedas	Existente	90 %
Lector de huellas digitales	Existente	80 %
Impresoras	Existente	90 %
Escáner	Existente	50 %
Hubs	Existente	50 %
Routers	Existente	90 %
Cortafuegos	Existente	50 %
Puntos de acceso	Existente	50 %
Cableado	Existente	80 %
[COM] Redes de comunicaciones		
Internet	Existente	90 %
Red local	Existente	90 %
Red con las sucursales	Existente	90 %
Red telefónica	Existente	90 %
Red inalámbrica	Existente	90 %
[MEDIA] Soporte de la información		
Discos duros externos	Existente	90 %
Dispositivos USB	Existente	90 %
CD ROM	No Existente	
DVD ROM	Existente	40 %
Material impreso	Existente	90 %
[L] Instalaciones		
Lugar para ubicar los equipos	Existente	80 %
Edificio	Existente	80 %
[P] Personal		
Usuarios internos	Existente	90 %

Controles existentes de los activos		
Activo	**Control existente**	**Eficacia**
Operadores	Existente	90 %
Administradores de sistemas	Existente	90 %
Desarrolladores	Existente	90 %

Tabla 40. Controles existentes de los activos

Elaborado por: El investigador

- **Estimación del estado del riesgo**

Es una combinación de los resultados obtenidos en las actividades caracterización de los activos con la caracterización de las amenazas con la finalidad de estimar el estado de riesgo en el que se encuentra dicho proceso.

Para la estimación del riesgo se utiliza la siguiente tabla:

RIESGO		**PROBABILIDAD**				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	

Tabla 41. Estimación del riesgo

Elaborado por: El investigador

3.2.3. Proceso 3: Gestión de Riesgos

Para mitigar el riesgo que puede producirse en la Cooperativa de Ahorro y Crédito San Francisco Ltda. La Metodología Magerit proporciona una serie de salvaguardas la cuales se deben poner en marcha para poder contrarrestar los riesgos.

3.2.3.1. Salvaguardas

La metodología Magerit presenta varias salvaguardas que permiten contrarrestar las amenazas, existen salvaguardas que están enfocadas principalmente en los avances tecnológicos.

Dentro de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Principalmente las salvaguardas se activan cuando aparecen nuevas tecnologías y van desapareciendo las antiguas tecnologías, además los activos correspondientes y la evolución de los posibles ataques.

Por ende, este catálogo de salvaguardas se limita a proporcionar métodos taxonómicos para ordenar y clasificar las diferentes acumulaciones materiales, tecnológicas, procedimentales y organizativas que pueden aplicarse en cada momento.

Para el desarrollo de los controles para la Cooperativa se ha establecido el uso de la Normativa ISO 27002.

3.2.3.2. Riesgos y aplicación de la normativa ISO 27002

Sin embargo, se aplica la normativa ISO 27002 la misma que presenta una serie de políticas de seguridad de la información para aplicar dentro de la Cooperativa San Francisco Ltda.

3.2.3.3. Declaración de aplicabilidad

Controles adecuados para la gestión de la seguridad dentro de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

Dominios	Objetivos	Justificación
9. Control de accesos		
9.2 Gestión de acceso a usuarios		
9.2.3 Gestión de los derechos a acceso con privilegios especiales	"La asignación y el uso de privilegios de acceso debería estar restringida y controlada" [29].	Es necesario establecer controles de acceso únicamente para el personal adecuado.
9.2.6 Retirada o adaptación de los derechos de acceso	"Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio" [29].	Se deben establecer políticas para la eliminación de cuentas de datos una vez que le empelado ya no labre en la organización.
9.4 Control de acceso a sistemas y aplicaciones		
9.4.3 Gestión de contraseñas de usuario	"Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas" [29].	Las contraseñas deben estar debidamente planificadas y cifradas para restringir el acceso a la información.
11. Seguridad física y ambiental		
11.1 Áreas seguras		
11.1.2 Controles físicos de entrada	"Se debe asegurar su entorno físico, y especialmente sus entradas para proteger la información digital" [29].	Mediante mecanismos de control de acceso se puede restringir la entrada de las personas no autorizadas.
11.1.4 Protección contra las amenazas	"Se debería diseñar y aplicar una protección física contra	Una normativa que detalle que hacer en caso

Dominios	Objetivos	Justificación
externas y ambientales	desastres naturales, ataques provocados por el hombre o accidentes" [29].	de desastres naturales minimizaría los riegos dentro de la organización.
11.2 Seguridad de los equipos		
11.2.4 Mantenimiento de los equipos	"Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas" [29].	El correcto estado de los equipos informáticos permitirá llevar las actividades con normalidad dentro de la organización.
11.2.5 Salida de activos fuera de las dependencias de la empresa	"Se debe aplicar medidas de seguridad a los equipos que se sitúan fuera las instalaciones de la COAC, teniendo en cuenta los diferentes riesgos que pueden producirse" [29].	Mediante los controles adecuados se puede restringir la salida de los equipos informáticos y aplicar normativas para la utilización de los equipos.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	"Mantener los puestos de trabajo correctamente aplicando las 5S y mantener la pantalla limpia y bloqueada cuando no se esté utilizando" [29].	Mediante la aplicación de las 5S se puede tener un muy buen ambiente del trabajo.
12. Seguridad en la operativa		
12.1 Responsabilidades y procedimientos de operación		
12.1.1 Documentación de procedimientos de operación	"Se debe documentar y mantener procedimientos de operación y poner a disposición de todos los	El tratamiento y manipulación de la información debidamente documentada permitirá

Dominios	Objetivos	Justificación
	usuarios que los necesiten" [29].	tener seguros los sistemas de información.
12.1.3 Gestión de capacidades	"Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten" [29].	Utilizar al máximo los recursos tecnológicos estableciendo tiempos de tal manera que no afecte a los distintos equipos informáticos ni a la parte de las redes de comunicaciones.
12.2 Protección contra código malicioso		
12.2.1 Controles contra el código malicioso	"Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario" [29].	La correcta configuración de las aplicaciones y servicios de red permitirá protegerse contra código malicioso.
13. Seguridad en las telecomunicaciones		
13.1 Gestión de la seguridad en las redes		
13.1.2 Mecanismos de seguridad asociados a servicios de red	"Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas" [29].	Todos los equipos informáticos deben estar enlazados a una red de datos principal.
15. Relaciones con suministradores		
15.1 Seguridad de la información en las relaciones con suministradores		
15.1.2 Tratamiento del riesgo dentro de	"Para asegurarse que los empleados y contratistas entiendan sus	Los acuerdos deben describirse adecuadamente y en caso

Dominios	Objetivos	Justificación
acuerdos de suministradores	responsabilidades y son adecuados para las funciones para las que se consideran" [29].	de existir fallos aplicar sanciones y multas.
15.2 Gestión de la prestación del servicio por suministradores		
15.2.1 Supervisión y revisión de los servicios prestados por terceros	"Se debe controlar, revisar y auditar regularmente la provisión de servicios del proveedor" [29].	Debe existir personal capacitado para supervisar los servicios de los proveedores de tal manera de garantizar el correcto funcionamiento de los servicios de terceros.

Tabla 42. Controles ISO 27002 identificados para la propuesta

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[D] Datos / Información	[E.1] Errores de los usuarios	Falta de manuales de usuario	MA	A	MA	12.1.1 Documentación de procedimientos de operación
	[E.2] Errores del administrador	Falta de manuales de usuario y manuales de procesos	A	A	MA	12.1.1 Documentación de procedimientos de operación
	[E.4] Errores de configuración	Falta de manuales de usuario y manuales de procesos	A	A	MA	12.1.1 Documentación de procedimientos de operación
	[E.14] Escapes de información	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.15] Alteración accidental de información	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.16] Introducción de información incorrecta	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
	[E.17] Degradación de la información	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.16] Destrucción de la información	Falta de controles en los procesos de eliminación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[E.19] Divulgación de la información	Falta de control en las cuentas dadas de baja	MA	A	MA	9.2.6 Retirada o adaptación de los derechos de acceso
	[A.3] Manipulación de los registros de actividad	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.4] Manipulación de la configuración	Falta de control en los procesos de modificación	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.11] Acceso no autorizado	Contraseñas inseguras	MA	M	MA	9.2.3 Gestión de contraseñas de usuarios

Tabla 43. Matriz de riesgos y Controles ISO/IEC 27002:2013 – Datos/Información

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[S] Servicios	[E.1] Errores de los usuarios	Falta de manuales de usuario	A	MA	MA	12.1.1 Documentación de procedimientos de operación
	[E.2] Errores del administrador	Falta de manuales de usuario y manuales de procesos	A	MA	MA	12.1.1 Documentación de procedimientos de operación
	[E.24] Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	M	MA	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores 15.2.1 Supervisión y revisión de los servicios prestados por terceros
	[A.4] Manipulación de la configuración	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.5] Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.6] Abuso de privilegios de acceso	Falta de control en los procesos de modificación	MA	B	MA	9.2.3 Gestión de los derechos a acceso con privilegios

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
						especiales
	[A.11] Acceso no autorizado	Falta de control en los procesos de modificación	MA	B	MA	9.4.3 Gestión de contraseñas de usuarios

Tabla 44. Matriz de riesgos y Controles ISO/IEC 27002:2013 - Servicios

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[SW] Software – aplicaciones informáticas	[E.1] Errores de los usuarios	Falta de manuales de usuario	A	MA	MA	12.1.1 Documentación de procedimientos de operación
	[E.2] Errores del administrador	Falta de manuales de usuario y manuales de procesos	A	A	MA	12.1.1 Documentación de procedimientos de operación
	[E.8] Difusión de software dañino	Virus y demás software malicioso	A	M	A	12.2.1 Controles contra el código malicioso
	[E.20] Vulnerabilidades de los programas (software)	Virus y demás software malicioso	A	A	MA	12.2.1 Controles contra el código malicioso
	[A.4] Manipulación de la configuración	Contraseñas débiles o predecibles	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.5] Suplantación de la identidad del usuario	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
	[A.6] Abuso de privilegios de acceso	Falta de control en los procesos de modificación	MA	M	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.8] Difusión de software dañino	Virus y demás software malicioso	B	MA	MA	12.2.1 Controles contra el código malicioso
	[A.11] Acceso no autorizado	Falta de control en los procesos de modificación	MA	B	MA	9.4.3 Gestión de contraseñas de usuarios

Tabla 45. Matriz de riesgos y Controles ISO/IEC 27002:2013 - Software – aplicaciones informáticas

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[HW] Hardware – Equipos informáticos	[N.1] Fuego	No se ha socializado el uso de extintores	M	A	A	11.1.4 Protección contra las amenazas externas y ambientales
	[N.2] Daños por agua	Filtros de agua	M	A	A	11.1.4 Protección contra las amenazas externas y ambientales
	[I.1] Fuego	No se ha socializado el uso de extintores	M	A	A	11.1.4 Protección contra las amenazas externas y ambientales
	[I.2] Daños por agua	Filtros de agua	M	A	A	11.1.4 Protección contra las amenazas externas y ambientales
	[I.6] Corte de suministro eléctrico	Fallo en los equipos informáticos	M	B	M	11.2.4 Mantenimiento de los equipos
	[I.7] Condiciones inadecuadas de temperatura y/o humedad	Fallo en los equipos informáticos	M	B	M	11.2.4 Mantenimiento de los equipos

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
	[I.11] Emanaciones electromagnéticas	Fallo en los equipos informáticos	M	A	A	11.2.4 Mantenimiento de los equipos
	[E.2] Errores del administrador	Falla en el uso de equipos	B	A	M	12.1.1 Documentación de procedimientos de operación
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de procesos de actualización y Mantenimiento	B	A	M	11.2.4 Mantenimiento de los equipos
	[E.24] Caída del sistema por agotamiento de recursos	Falla en el uso de equipos	B	M	B	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	[A.4] Manipulación de la configuración	Falla en el uso de equipos	B	A	M	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	[A.6] Abuso de privilegios de acceso	Falta de control en los Procesos	M	A	A	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
	[A.11] Acceso no autorizado	Equipos sin contraseñas	M	M	M	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	[A.25] Robo	Equipos extraídos fuera de las instalaciones.	M	M	M	11.2.5 Salida de activos fuera de las dependencias de la empresa.

Tabla 46. Matriz de riesgos y Controles ISO/IEC 27002:2013 - Hardware – Equipos informáticos

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[COM] Redes de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Falta de control en el uso de la red	A	M	MA	12.1.3 Gestión de capacidades
	[E.2] Errores del administrador	Falta de manuales de usuario y manuales procesos	A	A	MA	12.1.1 Documentación de procedimientos de operación
	[E.24] Caída del sistema por agotamiento de recursos	Falta de control en el uso de la red	A	M	MA	12.1.3 Gestión de capacidades
	[A.4] Manipulación de la configuración	Contraseñas débiles o Predecibles	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales
	[A.5] Suplantación de la identidad del usuario	Falta de control en los procesos de modificación	MA	A	MA	9.2.3 Gestión de los derechos a acceso con privilegios especiales

	[A.6] Abuso de privilegios de acceso	Controles no adecuados en el firewall de la red	M	A	M	13.1.2 Mecanismos de seguridad asociados a servicios de red
	[A.11] Acceso no autorizado	Controles no adecuados en el firewall de la red	M	A	M	13.1.2 Mecanismos de seguridad asociados a servicios de red

Tabla 47. Matriz de riesgos y Controles ISO/IEC 27002:2013 – Redes de comunicaciones

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[MEDIA] Soporte de información	[N.1] Fuego	No se socializa el uso de extintores	M	M	M	11.1.4 Protección contra las amenazas externas y ambientales
	[N.2] Daños por agua	Filtros de agua	M	M	M	11.1.4 Protección contra las amenazas externas y ambientales
	[I.1] Fuego	No se socializa el uso de extintores	M	M	M	11.1.4 Protección contra las amenazas externas y ambientales
	[I.2] Daños por agua	Filtros de agua	M	A	A	11.1.4 Protección contra las amenazas externas y ambientales
	[I.6] Corte de suministro eléctrico	Fallo en los dispositivos de almacenamiento	M	A	A	11.2.4 Mantenimiento de los equipos
	[I.7] Condiciones inadecuadas de temperatura y/o humedad	Fallo en los dispositivos de almacenamiento	M	A	A	11.2.4 Mantenimiento de los equipos

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
	[I.10] Degradación de los soportes de almacenamiento de información	Fallo en los equipos dispositivos de almacenamiento	M	A	A	11.2.4 Mantenimiento de los equipos
	[A.11] Acceso no autorizado	Equipos sin contraseñas	M	B	A	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	[A.25] Robo	Equipos se extraídos fuera de las instalaciones.	M	A	A	11.2.5 Salida de activos fuera de las dependencias de la empresa.

Tabla 48. Matriz de riesgos y Controles ISO/IEC 27002:2013 – Soporte de la información

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[L] Instalaciones	[N.1] Fuego	No se socializa el uso de extintores	A	A	MA	11.1.4 Protección contra las amenazas externas y ambientales
	[N.2] Daños por agua	Fugas de agua	B	A	M	11.1.4 Protección contra las amenazas externas y ambientales
	[I.1] Fuego	No se socializa el uso de extintores	A	B	A	11.1.4 Protección contra las amenazas externas y ambientales
	[I.2] Daños por agua	Fugas de agua	B	B	B	11.1.4 Protección contra las amenazas externas y ambientales
	[I.11] Emanaciones electromagnéticas	Fugas de agua	B	M	B	11.1.4 Protección contra las amenazas externas y ambientales
	[A.11] Acceso no autorizado	Falta de controles en el acceso físico	B	A	M	11.1.2 Controles físicos de entrada

Tabla 49. Matriz de riesgos y Controles ISO/IEC 27002:2013 – Instalaciones

Elaborado por: El investigador

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Dominio ISO 27002/IEC:2013
[P] Personal	[E.7] Deficiencias en la organización	[E.7] Deficiencias en la organización	MA	N	MA	11.1.4 Protección contra las amenazas externas y ambientales
	[E.28] Indisponibilidad del personal	[E.28] Indisponibilidad del personal	MA	N	MA	11.1.4 Protección contra las amenazas externas y ambientales

Tabla 50. Matriz de riesgos y Controles ISO/IEC 27002:2013 – Personal

Elaborado por: El investigador

3.2.3.4. Desarrollo de la política de seguridad

El desarrollo de esta política de seguridad se lo realiza con la finalidad de constituir las directrices y normativas para garantizar la confidencialidad, disponibilidad e integridad de la información dentro de la Cooperativa de Ahorro y Crédito San Francisco Ltda., sobre la base a una adecuada orientación y soporte de la gestión de la seguridad de la información de la misma.

Las políticas se han realizado en base al análisis de riesgos elaborado y a la vez, se han establecido controles necesarios con la finalidad de tener un manual completo de políticas para la seguridad de la información del departamento de tecnología de la Cooperativa.

3.2.3.4.1. Políticas de Seguridad

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**POLÍTICAS DE SEGURIDAD**	**REF.**
		5
OBJETIVO	Establecer los lineamientos iniciales para la creación de políticas de seguridad de la información, basadas en 3 características principales la integridad, confidencialidad y disponibilidad de la información.	
5.1 Directrices de la dirección en seguridad de la información		
5.1.1 Conjunto de políticas para la seguridad de la información		
a. El oficial de seguridad de la información debe elaborar un manual de roles y responsabilidades para cada uno de los funcionarios, mismo que debe estar aprobado, publicado y comunicado a todos los miembros de la Cooperativa. b. Para el cumplimiento, es necesario que el oficial de seguridad de la información asigne un comité conjuntamente con el departamento de tecnología para la elaboración creación del manual de roles, políticas y responsabilidades para cada uno de los funcionarios y debe estar aprobado		

por el gerente y autoridades de la Cooperativa.
5.1.2 Revisión de las políticas para la seguridad de la información.
a. Se debe realizar una revisión de políticas de seguridad de forma periódica (se recomienda establecer un cronograma de revisión). Es necesario que el departamento de tecnología designe un comité para controlar el cumplimiento de las políticas de seguridad y que las responsabilidades y roles de los funcionarios se cumplan de acuerdo al manual aprobado por la Cooperativa.

Tabla 51. Política de seguridad – Políticas de seguridad

Elaborado por: El investigador

3.2.3.4.2. Aspectos organizativos de la seguridad de la información

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**	**REF.** 6
OBJETIVO	Establecer los lineamientos para la aprobación, implementación y asignación de procedimientos y responsabilidades de políticas de seguridad dentro de la organización.	
6.1 Organización interna		
6.1.1 Asignación de responsabilidades para la seguridad de la información.		
a. El oficial de seguridad de la información debe definir y documentar las responsabilidades de los funcionarios del departamento de tecnología, se establecerán los diferentes roles y responsabilidades que serán analizadas y revisadas conjuntamente con el Jefe del Departamento de Tecnología para el cumplimiento de las mismas		
6.1.2 Segregación de tareas.		
a. La política trata en segregar tareas y áreas de responsabilidad para cada uno de los funcionarios del Departamento de Tecnología para evitar modificaciones no autorizadas o no intencionadas en la información.		

b. Para el cumplimiento, es necesario que el jefe de tecnología capacite al personal de su departamento sobre el manejo de los sistemas de información y bases de datos con la finalidad de evitar la modificación no autorizada o no intencionada, o el uso inadecuado de los activos de la organización.
c. En caso de ocurrir algún conflicto dentro de las áreas seguras, protección contra amenazas o control de accesos el encargado de seguridad de la información será el encargado de reportar al departamento de tecnología y solucionar inmediatamente.

6.1.3 Contacto con las autoridades

a. Esta política se refiere a establecer el contacto permanente con las autoridades de la Cooperativa para mantener actualizados sobre los cambios en los reglamentos, políticas o manuales.
b. Para el cumplimiento, es necesario que se mantenga contacto con autoridades de forma permanente con la finalidad de brindar un mejor un mejor asesoramiento en caso que exista una actualización en las políticas de uso de la información.

6.1.4 Contacto con grupos de interés especial

a. Esta política se refiere a establecer el contacto permanente con especialistas de seguridad de la información mediante foros de discusión.
b. Para el cumplimiento, es necesario que se conozca sobre los aspectos actualizados de la seguridad de la información, para ello es necesario que el oficial de seguridad de la informacióm se agregue a grupos de interés o foros con la finalidad de mantenerse actualizado en políticas de seguridad de la información.

6.1.5 Seguridad de la información en la gestión de proyectos

a. Esta política se refiere a implementar procedimientos de control de la información y la gestión proyectos dentro de la Cooperativa.
b. Para el cumplimiento, es necesario que para la gestión y desarrollo de nuevos proyectos dentro de la Cooperativa sin importar su tipo se debe aplicar políticas de seguridad de la información.

c. Para ello se debe asignar un comité que analice la información que se maneja dentro de la gestión de los proyectos.
6.2 Dispositivos para movilidad y teletrabajo
6.2.1 Política de uso de dispositivos para movilidad
a. Esta policía se refiere a acoger medidas de seguridad para manejo de datos mediante dispositivos de movilidad. b. Para el cumplimiento, es necesario que en las distintas redes móviles se restringa solo a páginas autorizadas, además debe existir un control de las aplicaciones o sistemas de información que se accedan desde los dispositivos móviles.
6.2.2 Teletrabajo
a. Esta política se refiere a proteger la información a la que acceden los funcionarios desde ubicaciones distintas, es decir cuando no se encuentren en su puesto de trabajo. b. Para el cumplimiento, es necesario que se realice una protección lógica de los equipos, el responsable de la seguridad de la información debe conceder permisos al personal para que puedan ingresar a realizar cambios o trabajo fuera de la oficina. c. En casos de ocurrir algún inconveniente en la red, el encargado de la seguridad debe configurar los puertos adecuados para restablecer la comunicación.

Tabla 52. Política de seguridad – Aspectos organizativos de la seguridad de la información

Elaborado por: El investigador

3.2.3.4.3. Seguridad ligada a los recursos humanos

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**	**REF.** 7
OBJETIVO	Capacitar a los funcionarios y colaboradores de la Cooperativa cuando ingresan la forma continua sobre	

	la importancia de preservar la confidencialidad de la información.

7.1 Antes de la contratación

7.1.1 Investigación de antecedentes.

a. Esta política trata sobre la necesidad de realizar una investigación para los aspirantes que están por ingresar a la Cooperativa para lo cual se realiza un análisis previo de antecedentes e historial laboral, con la finalidad de descartar todo tipo de amenaza a la seguridad de la información.
b. Para el cumplimiento, se debe realizar un proceso de selección que abarque pruebas de admisión de tipo psicológico, revisión de hojas de vida con referencias personales, laborares y record del aspirante que garantice no tener problemas de índole legal.
c. Luego de seleccionar al personal adecuado se debe hacer firmar "acuerdos de confidencialidad" con la finalidad de proteger la información en cualquier lugar y área que se desempeñen.

7.2 Durante la contratación.

7.2.1 Responsabilidades de gestión.

a. La política trata sobre la inclusión de todos los términos y condiciones de seguridad de la información cuando se realice los contratos de nuevos empleados, contratistas y terceros para gestionar adecuadamente la información dentro de la Cooperativa.
b. Para el cumplimiento, es necesario que las condiciones y términos de empleo estén incluidas en el contrato de trabajo, para lo cual se debe establecer responsabilidades concretas del empleado en la seguridad de la información. Cada empleado debe estar informado sobre los roles y responsabilidades de seguridad y sobre las sanciones que deberá someterse si incumple con lo establecido dentro de la Cooperativa.

7.2.1 Concienciación, educación y capacitación de seguridad de la información

a. Esta política trata sobre la inclusión de capacitaciones y requerimientos de seguridad, para lo cual se debe asignar responsabilidades a cada funcionario, al inicio y durante las labores.
b. Para el cumplimiento, es necesario que el Departamento de Talento

Humano en coordinación con el Departamento de Tecnología y el Oficial de Seguridad de la Información de la Cooperativa realicen las gestión adecuada para que todo el personal sea capacitado en seguridad, para lo cual el Departamento de Tecnología debe proporcionar los recursos adecuados para llevar cabo la capacitación.

7.2.3 Proceso disciplinario.

a. Esta política se refiere las omisiones e incumplimientos que realizan los funcionarios, los cuales deben ser sancionados según políticas administrativas internas de la Cooperativa.
b. Para el cumplimiento, el proceso disciplinario debe iniciarse cuando se haya detectado y verificado que se ha producido un atentado a la seguridad de la información, para llevar a cabo este proceso se debe garantizar el trato correcto y justo para los empleados y la Cooperativa.
c. El proceso debe ser bien ejecutado y se debe tomar en cuenta todas las consideraciones y el impacto que ha tenido la Cooperativa, si el funcionario fue capacitado correctamente, la sanción debe estar basada en el "acuerdo de confidencialidad" que fue firmado al iniciar el contrato. Todo va a depender de la gravedad del acto, si es altamente grave, el empleado debe ser removido de sus funciones inmediatamente.

7.3 Cese o cambio de puesto de trabajo

7.3.1 Cese o cambio de puesto de trabajo

a. Esta política se refiere a la inclusión de la comunicación de las responsabilidades a la terminación de las actividades, es decir las condiciones y términos incluidos en el contrato y el acuerdo de confidencialidad. El empleado debe presentar su renuncia por lo menos con 15 días de anticipación.
b. Para el cumplimiento, es necesario que el responsable supervise la entrega formal de los activos al nuevo empleado a ocupar la vacante, revisando las claves de acceso, la documentación, llaves, credenciales, herramientas de trabajo, equipos de cómputo, consignas y demás activos.
c. El área de seguridad es la encargada de suspender las claves de acceso del

empleado que cesa en sus funciones y asignarlas al nuevo empelado.

Tabla 53. Política de seguridad – Seguridad ligada a los recursos humanos

Elaborado por: El investigador

3.2.3.4.4. Gestión de activos

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**GESTIÓN DE ACTIVOS**	**REF.**
		8
OBJETIVO	Describir todos los activos que posee la Cooperativa, que son importantes para administrar los diversos procesos que se lleva a cabo, para lo cual debe incluir los activos informáticos, archivos, procedimientos, manuales, planes de contingencia y de continuidad, documentación de archivos, entre otros.	
8.1 Responsabilidad sobre los activos		
8.1.1 Inventario de Activos		
a. Esta política trata sobre la identificación de los activos de información, la Cooperativa debe tener identificado los más importantes y relacionarlos con los sistemas de información, además debe identificar los custodios adecuados y la ubicación física de los activos. b. Para el cumplimiento, es necesario que el encargado de activos fijos de la Cooperativa mantenga actualizado el inventario de activos de forma permanente, en caso de existir alguna modificación se deberá notificar al departamento de tecnología y este al oficial de seguridad de la información dependiendo del tipo de activo. c. Es de mucha importancia los equipos informáticos porque almacenan la información, los equipos de red que intercambian la información y las comunicaciones que se llevan dentro de la Cooperativa para lo cual se debe tener inventariados los activos. Ver Tabla 13. Definición de activos		
8.1.2 Propiedad de los activos		

a. La política trata sobre la información de los activos que pertenezca a la Cooperativa debe estar sujeta a revisiones periódicas por parte del departamento de tecnología.
b. Para el cumplimiento, es necesario que cada uno de los activos de la información tales como; software, hardware, equipos de cómputo, de comunicaciones y la información deben estar debidamente custodiadas por una persona que será la encargada de realizar las actividades relacionadas con dicho activo.
c. Para ello se crea perfiles, roles y responsabilidades a cada funcionario para el uso del activo, con esta relación se crea una responsabilidad sobre el uso del activo de la Cooperativa.

8.1.3 Uso aceptable de los activos

a. Esta política trata sobre los activos de información son de propiedad de la Cooperativa, por lo cual deben ser utilizados únicamente para las labores dentro de la institución.
b. Para el cumplimiento, es necesario establecer lineamientos para el uso adecuado de los activos:

- Los recursos tecnológicos como el internet, correo electrónico y sistemas de información, deben ser utilizados con fines laborales, o de ser el caso que se necesita para otra tarea específica debe tener la autorización del área de seguridad de la información.
- Las tareas y acceso a la información para cada empleado deben ser designadas por el jefe de cada departamento mediante roles.
- Está prohibido que se divulgue de la información que esta almacenada en los equipos informáticos o que ha sido creada o transmitida por los sistemas de Información de la Cooperativa.
- Las aplicaciones informáticas, software y antivirus deben contar con la licencia adecuada.
- Se deben crear cuentas de usuario con contraseñas seguras que permitan tener acceso autorizado a los sistemas de información.

- Está prohibido compartir las cuentas de usuario y contraseñas a terceros.
- El encargado del área de seguridad debe supervisar los equipos informáticos y aplicaciones de cada uno de los funcionarios.
- Se deben tener bloqueadas las páginas web de mala procedencia como páginas pornográficas, hacking, contenido inapropiado etc.
- Al enviar correos se debe tener en cuenta las normas de cordialidad Netiqueta.

8.1.4 Devolución de activos.

a. Esta política se refiere a garantizar que se cumpla con la entrega formal de los activos a cargo del empleado cuando cese en las funciones.
b. Para el cumplimiento, se debe tener en cuenta los siguientes aspectos:
   - Se debe devolver los equipos completos, con software, manuales y las herramientas de trabajo adecuadas.
   - Se debe devolver los activos organizacionales, los equipos móviles, y las claves de acceso y los medios de almacenamiento.
   - La información de la Cooperativa debe ser respaldada y entregada al área de seguridad de la información.

8.2 Clasificación de la información

8.2.1 Directrices de clasificación.

a. Esta política se refiere a clasificar la información tomando en cuenta las tres características principales de seguridad: confidencialidad, integridad y disponibilidad.
b. Para el cumplimiento, es necesario establecer criterios de seguridad para cada uno de los activos.

8.2.2 Etiquetado y manipulado de la información

a. Esta política se refiere a etiquetar los activos y la información, para que los empleados conozcan cómo manipularlos y de esta manera evitar la

pérdida, manipulación inadecuada o robo de información.

b. Para el cumplimiento, es necesario etiquetar la información mediante la utilización de colores, y de esta manera simular un semáforo de acuerdo al nivel de criticidad. Por ejemplo, criticidad baja color verde, criticidad media color amarillo y criticidad alta color rojo.

8.2.3 Manipulación de los activos

a. Esta política se refiere a que todos los empleados que utilizan activos de información, deben tener un amplio conocimiento de los diferentes niveles de criticidad y sobre las políticas de seguridad que deben dar cumplimiento que puedan manipular la información.

b. Para el cumplimiento, es necesario al ingresar un nuevo funcionario a la Cooperativa, este debe ser capacitado en los niveles de criticidad de la información a la que va a tener acceso, con la finalidad de evitar errores en la manipulación de activos de información.

8.3 Manejo de los soportes de almacenamiento.

8.3.1 Gestión de soporte extraíbles

a. Esta política se refiere a gestión de soporte extraíbles de la información de cada uno de los departamentos de la Cooperativa, dependiendo de la información, se debe controlar los medios informáticos removibles que ahí se utilicen.

b. Para el cumplimiento, es necesario que los medios removibles que se encuentran en cada departamento, deben estar asignados para cada procedimiento o para almacenar determinada información dentro de discos duros.

8.3.2 Eliminación de soportes

a. Esta política se refiere a la eliminación de soporte, es decir trata sobre la eliminación o expulsión de los medios informáticos removibles de forma segura, con el fin de evitar divulgación o plagio de información.

b. Para el cumplimiento, es necesario que el encargado del área de seguridad de la información de la Cooperativa realice una revisión del medio informático al que se va a eliminar y que se cuente con los respaldos

adecuados.
8.3.3 Soportes físicos en tránsito
a. Esta política se refiere a la protección de los medios de información contra acceso no autorizado cuando salgan del área o perímetro y seguridad. b. Para el cumplimiento, es necesario que la información que contengan los medios removibles que salen fuera de la Cooperativa, estén con adecuadas claves de acceso, o evitar que estos medios contengan información sensible o de gran criticidad con la finalidad de evitar acceso no autorizado o robo de la misma.

Tabla 54. Política de seguridad – Gestión de activos

Elaborado por: El investigador

3.2.3.4.5. Política para el control de acceso

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**POLÍTICA PARA EL CONTROL DE ACCESOS**	**REF.** 9
OBJETIVO	Restringir el acceso a la información y a las instalaciones de procesamiento de datos e información de los sistemas	
9.1 Requisitos de negocio para el control de accesos		
9.1.1 Política de control de accesos		
a. Esta política se refiere a proponer o definir los controles de forma adecuada de derechos de acceso individual y grupal a la información. b. Para el cumplimiento, es necesario se deben establecer los siguientes lineamientos: - Establecer mecanismos de seguridad para los diferentes sistemas, aplicaciones y sistemas de la Cooperativa. - Clasificar la información que se debe restringir. - Clasificar al personal para que tengan acceso a la información. - Establecer cronogramas para supervisar las claves de acceso del personal a las diferentes aplicaciones y sistemas de información.		

- Autorizar el acceso a los usuarios a ambientes simples y distribuidos siguiendo un procedimiento adecuado de seguridad.

9.1.2 Control de acceso a las redes y servidores asociados

a. Esta política se refiere a garantizar que los funcionarios que tengan acceso a la red y a los servidores, no compliquen o violen la seguridad de los mismos.
b. Para el cumplimiento, es necesario que el encargado de seguridad de la información de la Cooperativa brinde el acceso a los equipos servidores, redes y los diferentes recursos tecnológicos, los mismos que deben ser solicitados por el jefe del departamento de tecnología para cada empleado que está a su cargo.

9.2 Gestión de acceso de usuarios

9.2.1 Gestión de altas/bajas en el registro de usuarios

a. Esta política se refiere al registro y a la cancelación del usuario para lo cual se debe realizar de manera independiente cuando se quiera acceder a la información, esta tarea está a cargo del área de seguridad de la información de la Cooperativa.
b. Para el cumplimiento, se debe tomar en cuenta los siguientes lineamientos:
    - Chequear de forma permanente a los usuarios que acceden a los distintos sistemas de información y aplicaciones.
    - Colocar nombres únicos a los nuevos usuarios, así como también las contraseñas seguras.
    - Si un empelado deja de pertenecer a la Cooperativa inmediatamente debe ser notificado ala área de seguridad para restringir el acceso a los sistemas de información.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

a. Esta política se refiere a implementar una adecuada herramienta o procedimientos que permitan el control de usuarios, así como también gestiona los permisos y definir las actividades realizadas a cumplir por cada uno de ellos.
b. Para el cumplimiento, es importante utilizar aplicaciones open source, de manera que faciliten realizar auditorías e implementar procedimientos que

permitan controlar los permisos de los usuarios para que utilicen los sistemas de información.

9.2.3 Gestión de los derechos de acceso con privilegios especiales

a. Esta política se refiere a la gestión de derechos de los usuarios a los distintos sistemas de información de la Cooperativa.
b. Para el cumplimento, es necesario que el encargado del área de seguridad de la información establezca las cuentas de usuario para el acceso a los sistemas de escritorio y Web deberán ser analizados previo a su entrega; el análisis deberá basarse en la función que desempeña el usuario y privilegios necesarios.
c. Se deberá tomar en cuenta el tipo de usuarios y sus capacidades para la asignación de los perfiles de usuario.
d. Se recomienda el cambio de contraseñas en forma periódica para el acceso a la información confidencial, reservada y clasificada.
e. Para la manipulación, configuración y administración de la información se debe contar con manuales de usuario para evitar inconvenientes.

9.2.4 Gestión de información confidencial de autenticación de usuarios

a. Esta política se refiere a la asignación de contraseñas de acceso a los diferentes sistemas de información, previa autorización del jefe de seguridad.
b. Para el cumplimento, se debe tomar en cuenta los siguientes lineamientos:
    - El empelado debe firmar un formulario de creación de usuario con su contraseña respectiva.
    - Asignar una contraseña temporal de manera que pueda ser cambiada por el empleado.
    - Las calves de acceso a los servidores y bases de datos deben permanecer encriptados.
    - Cambiar periódicamente las claves de acceso.

9.2.5 Revisión de los derechos de acceso de los usuarios

a. Esta política se refiere a la revisión de forma periódica alas claves de acceso designados a los usuarios.

b. Para el cumplimento, se deben seguir los siguientes lineamientos:
    - Los claves de acceso por lo menos se deben cambiar de forma semestral.
    - Los accesos a los servidores por parte de los administradores se deben cambiar de forma trimestral.
    - Los usuarios con acceso a la información y equipos especiales deben ser auditadas de forma periódica.

9.2.6 Retirada o adaptación de los derechos de acceso

a. El Departamento de tecnología de la información deberá disponer de manera prioritaria si fuese necesario se niegue o se ajuste los permisos necesarios de acceso a los usuarios que han sido dados de baja o eliminados.
b. Además de debe restringir al acceso a los sistemas de información de la organización a personas no autorizadas.

9.3 Responsabilidad del usuario

9.3.1 Uso de información confidencial para la autenticación

a. Esta política se refiere a que se debe tener buenas prácticas de seguridad de la información con la finalidad de mantener la información con la seguridad adecuada dentro de la Cooperativa.
b. Para el cumplimento, se debe seguir los siguientes lineamientos:
    - Las claves de acceso a los diferentes sistemas de información deben ser confidenciales.
    - La contraseña debe ser compleja y segura, pero debe ser fácil de recordar al usuario.
    - Debe cambiar la contraseña temporal otorgada.
    - De perder las credenciales de acceso debe notificarse inmediatamente al departamento de tecnología.

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción del acceso a la información

a. Esta política se refiere restringir el acceso a los diferentes sistemas de la información a cada usuario, tanto a externos como a usuarios del Departamento de Tecnología de la Cooperativa.

b. Para el cumplimento, se deben seguir los siguientes lineamientos:
   - Cada sistema debe tener una página de login que permita a los usuarios colocar su usuario y contraseña.
   - Cada usuario debe saber las tareas a realizar.
   - Para manipulación de los sistemas se debe establecer permisos de lectura y escritura a los usuarios.
   - No permitir el acceso a la información de forma directa.

9.4.2 Procedimientos seguros de inicio de sesión

a. Esta política se refiere a la seguridad en los inicios de los sistemas desarrollados por la Cooperativa, así como a las aplicaciones de acceso de información.
b. Para el cumplimento, es necesario que cada empleado tenga asignado un usuario y contraseña para acceso a un determinado sistema de información o a las bases de datos financieras.

9.4.3 Gestión de contraseñas de usuarios

a. Utilizar claves seguras y encriptados que utilicen letras minúsculas, mayúsculas, números y signos especiales para el acceso a las aplicaciones de escritorio y sistemas Web, además deberán cumplir con un control de seguridad para ser activadas a los usuarios.
b. El Departamento de tecnología de información deberá cambiar las claves periódicamente de acuerdo a los perfiles de usuario en las diferentes aplicaciones y equipos de la Cooperativa.

9.4.4 Uso de herramientas de administración de sistemas

a. Esta política se refiere a la utilización de herramientas de administración, y los controles dentro de las aplicaciones de información deben estar restringidos.
b. Para el cumplimento, es necesario la creación de perfiles de usuario para cada uno de los empleados, todo va a depender del nivel de acceso que se asigne.

9.4.5 Control de acceso al código fuente de los programas

a. Esta política se refiere a restringir el acceso al código fuente de las

aplicaciones a los usuarios externos y no autorizados con la finalidad de evitar la robo o cambio de código fuente. b. Para el cumplimento, es necesario el programador o encargado de las aplicaciones debe dejar con contraseña el equipo cuando abandone el puesto de trabajo.

Tabla 55. Política de seguridad – Control de accesos

Elaborado por: El investigador

3.2.3.4.6. Cifrado

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**CIFRADO**	**REF.**
		10
OBJETIVO	Utilizar sistemas y técnicas criptográficas que permitan proteger la información, sobre la base de un análisis de riesgo realizado previamente, con la finalidad de conceder una adecuada protección.	
10.1 Controles criptográficos		
10.1.1 Política de uso de los controles criptográficos		
a. Esta política se refiere a proteger la confidencialidad de la información y que se utilice correctamente la misma dentro de la Cooperativa. **b.** Para el cumplimiento, es necesario seguir los siguientes lineamientos: - Los controles criptográficos serán utilizados para proteger los sistemas de información, bases de datos, servidores. - Se utilizará para la transmisión de información muy confidencial. - Se debe tener controles de encriptación y técnicas de des encriptación. - El área de seguridad de la información será encargada de implementar estas técnicas. - Se debe seleccionar los algoritmos adecuados.		
10.1.2 Gestión de claves		
a. Esta política se refiere a la gestión del ciclo de vida de las claves criptográficas, todo va a depender de los algoritmos seleccionados en el		

control anterior. b. Para el cumplimiento, es necesario que el jefe del área de seguridad establezca tiempos para cambiar las claves y se determinen cronogramas para la utilización de las mismas.

Tabla 56. Política de seguridad – Cifrado

Elaborado por: El investigador

3.2.3.4.7. Seguridad física y ambiental

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**SEGURIDAD FÍSICA Y AMBIENTAL**	**REF.** 11
OBJETIVO	Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.	
11.1 Áreas seguras		
11.1.1 Perímetro de seguridad física		
a. Esta política se refiere a establecer un perímetro para proteger la confidencialidad de la información, para lo cual se debe denegar el acceso no autorizado a los diferentes recursos tecnológicos que contengan información de la Cooperativa. b. Para el cumplimiento, es necesario que los empleados de la Cooperativa cuiden los componentes tecnológicos, que se realice la limpieza de los mismos, manteniéndolos en buen estado, así como también se lleve un registro de los cambios en la infraestructura la cual debe enfocarse en proteger la información.		
11.1.2 Controles físicos de entrada		
a. Establecer normas para el ingreso del personal a las instalaciones b. Cada área tendrá información de acceso de personal autorizado. c. El personal debe poseer claves de tarjetas magnéticas o huellas digitales para el acceso al departamento de tecnología.		
11.1.3 Seguridad de oficinas, despachos y recursos		

a. Esta política se refiere a la protección de las oficinas, agencias, despachos y lugares donde se hallen los recursos tecnológicos y que almacenen información, por lo general debe existir una protección adecuada en los departamentos de tecnología de seguridad de la información de la Cooperativa.
b. Para el cumplimiento, es necesario seguir los siguientes lineamientos:
   - Las oficinas no deben ser fáciles de identificarlas.
   - Se debe denegar el acceso a las oficinas que procesen información.
   - Mantener seguras las puertas y ventanas de las oficinas que procesen la información.
   - Almacenar los respaldos de la información financiera en lugares seguros,

11.1.4 Protección contra las amenazas externas y ambientales

a. El departamento de tecnología debe requerir, se imparta capacitaciones relacionadas a las maneras de evitar daños causados por riesgos naturales como inundaciones, terremotos, explosiones y otras amenazas ocasionadas por desastres naturales o por el hombre.
b. El jefe del departamento de tecnología deberá delegar al personal que forme parte de la Brigada de Gestión de Riesgos quienes deberán capacitarse en los protocolos y procedimientos para actuar ante las amenazas descritas anteriormente.
c. Se deber tener un plan de evacuación de los equipos, soporte de la información en caso que se produzca un desastre natural.

11.1.5 El trabajo en áreas seguras

a. Esta política se refiere al fortalecimiento de la seguridad en el desarrollo de las diferentes actividades y de trabajo en las áreas de la Cooperativa.
b. Para el cumplimiento, es necesario seguir los siguientes lineamientos:
   - Solamente debe conocer el personal que labora en esas áreas.
   - Los trabajos de remodelación de las instalaciones deben ser supervisados por el personal interno.
   - El acceso al personal externo debe ser muy limitado.
   - Denegar el acceso con equipos móviles o discos extraíbles.

- No ingresar con alimentos ni bebidas.

11.1.6 Áreas de acceso público, carga y descarga

a. Esta política se refiere a la creación de un área de carga y descarga que permita receptar materiales o recursos tecnológicos que sean adquiridos por la Cooperativa.
b. Para el cumplimiento, es necesario seguir los siguientes lineamientos:
    - Estas áreas deben estar alejadas de los equipos que procesan la información.
    - El personal administrativo no podrá acceder a estas áreas.
    - Se debe revisar los suministros recibidos.
    - Proteger las puertas de acceso a los lugares de carga y descarga.

11.2 Seguridad de los equipos

11.2.1 Emplazamiento y protección de equipos

a. Esta política se refiere a ubicar los equipos correctamente en un lugar seguro, los cuales no estén expuestos a amenazas físicas y ambientales con la finalidad de proteger la información.
b. Para el cumplimiento, es necesario que el responsable de la seguridad de la Cooperativa instale los equipos servidores en lugares seguros mismos que deben estar vigilados por el personal adecuado.

11.2.2 Instalaciones de suministro

a. Esta política se refiere a tener un control del lugar donde se encuentran los equipos tecnológicos ya que deben estar protegidos y deben soportar fallas eléctricas con la finalidad de evitar la pérdida de información, daños en los equipos tecnológicos y equipos de comunicación.
b. Para el cumplimiento, es necesario que el responsable de la seguridad revise conjuntamente con los técnicos el suministro de energía para que se adapte a los requerimientos de los equipos informáticos. Estos equipos deben estar conectados con UPS y con todas las seguridades posibles para mantener funcionado correctamente.

11.2.3 Seguridad del cableado.

a. Esta política se refiere a mantener el cableado de datos y eléctrico, debe estar protegido contra fallas provocadas para evitar desastres.
b. Para el cumplimiento, es necesario que el responsable de la seguridad de la Cooperativa proteja el cableado de datos y eléctrico con canaletas, tuberías o subterráneo con la finalidad de evitar interrupciones no autorizadas dentro de la Cooperativa y sus respectivas agencias, o a su vez impedir que el cableado salga a los exteriores de la misma.

11.2.4 Mantenimiento de los equipos

a. El Departamento de tecnología debe proporcionar mantenimiento de los equipos informáticos.
b. Elaborar un instructivo para dar mantenimiento periódico a los equipos informáticos por departamentos.
c. Dar soporte a los dispositivos que almacenan la información.
d. Adquirir los suministros necesarios para dar el mantenimiento.

11.2.5 Salida de activos fuera de las dependencias de la empresa

a. El Departamento de tecnología debe controlar los equipos que salen fuera de las dependencias, con autorización y estableciendo responsabilidades, así como para que un equipo sea llevado fuera de la dependencia cuando necesita mantenimiento.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones

a. Esta política se refiere a la protección que debe existir cuando los equipos se encuentren fuera de las instalaciones de la Cooperativa o de sus agencias.
b. Para el cumplimiento, es necesario que el responsable de la seguridad de la Cooperativa asegure el traslado de los equipos informáticos con las recomendaciones de fábrica, y proteger los datos que se manejen dentro de estos equipos deben estar correctamente encriptados.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento

a. Esta política se refiere a la revisión de los dispositivos que están conectados a los equipos, mismos que deben ser retirados sin que contengan información crítica o software con licencia.
b. Para el cumplimiento, es necesario que el encargado del departamento de

tecnología debe realizar las respectivas revisiones, el personal autorizado únicamente debe conectar los diferentes dispositivos de almacenamiento a los equipos que contengan información crítica.
11.2.8 Equipo informático de usuario desatendido
a. Esta política se refiere a las revisiones permanentes de los equipos que no están en constante utilización. b. Para el cumplimiento, es necesario que el responsable de administrar los activos, compruebe que los equipos estén con las contraseñas, además deben almacenarse en lugares seguros con las respectivas seguridades donde no haya humedad o filtraciones de agua, y con conexiones de datos y eléctricas estables.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
a. El Departamento de tecnología debe colocar las contraseñas periódicas en los equipos informáticos, así como también minimizar los tiempos de los bloqueos de las pantallas cuando no se esté utilizando. b. Los usuarios de los equipos dependiendo de su rol podrán acceder a sus privilegios para hacer cualquier modificación en la información siempre con los permisos adecuados. **c.** Establecer responsabilidades de los equipos y sus credenciales para el acceso a los mismos.

Tabla 57. Política de seguridad – Seguridad física y ambiental

Elaborado por: El investigador

3.2.3.4.8. Seguridad en la operativa

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**SEGURIDAD EN LA OPERATIVA**	**REF.**
		12
OBJETIVO	Asegurar la correcta operatividad y procesamiento de la información en los mecanismos de seguridad de la COAC SAN FRANCISCO LTDA.	
12.1 Responsabilidades y procedimientos de operación		

12.1.1 Documentación de procedimientos de operación

a. Realizar manuales de usuario para la instalación, configuración y manejo de las aplicaciones informáticas y del acceso a la información para mitigar que se comentan errores por partes de los usuarios.
b. En los manuales establecer todos los procedimientos a seguir en caso de producirse algún error en los sistemas.

12.1.2 Gestión de cambios

a. Esta política se refiere a revisar que antes de realizar un cambio en los equipos operativos, debe ser correctamente evaluado y documentado por el jefe del área de seguridad de la información conjuntamente con el personal del departamento de tecnología de la Cooperativa.
b. Para el cumplimiento, es necesario que el responsable de evaluar los posibles cambios requeridos por los usuarios que manipulan la información, además deben ser evaluados y aprobados por el jefe del departamento de tecnología de la Cooperativa.

12.1.3 Gestión de capacidades

a. Tramitar la adecuada capacidad de los servicios estableciendo tiempos para el funcionamiento de las diferentes aplicaciones y recursos informáticos:
    - Aprovechar el borrado de los discos.
    - La activación de los diferentes servicios se los realice mediante horarios.
b. Prestar atención especial aquellos recursos que tengan un periodo de adquisición o plazos de entrega largos o sean de coste elevados.

11.1.4 Separación de entornos de desarrollo, prueba y producción

a. Esta política se refiere a la creación de entornos para las fases principales del ciclo de vida de los diferentes proyectos, desarrollo, prueba y producción para trasladar un sistema de información.
b. Para el cumplimiento, es necesario que el oficial de seguridad de la Cooperativa separe las aplicaciones de desarrollo y servidores, fases y tipos de sistemas, con la finalidad de evitar que se mezcle el área de desarrollo y los códigos fuentes.

12.2 Protección contra código malicioso

12.2.1 Controles contra el código malicioso

a. El departamento de tecnología debe requerir antivirus actualizados y sofisticados con la finalidad de tener protegidos los sistemas operativos de los activos con los que cuenta la cooperativa.
b. Se debe restringir a los usuarios la instalación de cualquier aplicación informática, estas solamente podrán ser instaladas por el personal encargado del departamento de tecnología.
c. Gestionar las licencias para los antivirus y aplicaciones con sus respectivas licencias para mitigar cualquier tipo de amenazas.

12.3 Copias de seguridad

12.3.1 Copias de seguridad

a. Esta política se refiere a la comprobación de las copias de seguridad que se ejecuten correctamente y que sus respaldos se realicen de acuerdo a los cronogramas establecidos.
b. Para el cumplimiento, es necesario que el oficial de seguridad de la Cooperativa designe un responsable para que lleve a cabo las copias de seguridad, las diferentes pruebas y las restauraciones de los sistemas de información y bases de datos y aplicaciones que contenga la Cooperativa.
c. Las copias de seguridad deben permanecer en lugares seguros, con controles de acceso adecuados.

12.4 Registro de actividad y supervisión

12.4.1 Registro y gestión de eventos de actividad.

a. Esta política se refiere a la comprobación de los diferentes eventos que se realiza sobre los sistemas de información.
b. Para el cumplimiento, es necesario que el oficial de seguridad de la Cooperativa designe un responsable para que supervise el registro de los eventos que se realiza a los diferentes sistemas de información contenga la Cooperativa.

12.4.3 Registros de actividad del administrador y operador del sistema

a. Esta política se refiere a tener un control del registro de las actividades que realiza el administrador y los operadores del sistema dentro de los sistemas de información de la Cooperativa y de sus agencias.
b. Para el cumplimiento, es necesario que los empleados encargados de los departamentos de sistemas de cada una de las agencias de la Cooperativa conlleven un registro de sus actividades, para lo cual deben registrar la hora y las tareas realizadas.

12.4.4 Sincronización de relojes

a. Esta política se refiere a que los relojes deben estará sincronizados para los sistemas de información y bases de datos de la Cooperativa.
b. Para el cumplimiento, es necesario contar con un reloj fuente con la hora actualizada y hacer que todos los equipos informáticos se igualen a esa hora según Ecuador (GMT-5).

12.5 Control del software en explotación

12.5.1 Instalación del software en sistemas en producción

a. Esta política se refiere a tener un registro actualizado del inventario de los equipos informáticos, de la misma manera de las aplicaciones software registrando fecha de compra, actualizaciones, vida útil y aplicaciones instaladas, con la finalidad de evitar daños en los equipos.
b. Para el cumplimiento, es necesario que el responsable del área de seguridad asigne un responsable para monitorear y explorar las vulnerabilidades, también deberá establecer una planificación adecuada en línea de tiempo detallando todas las vulnerabilidades existentes.

12.6 Gestión de la vulnerabilidad técnica

12.6.1 Gestión de las vulnerabilidades técnicas.

a. Esta política se refiere a la planificación de los cambios en los diferentes sistemas de información con las pruebas necesarias con el fin de afirmar el funcionamiento correcto.
b. Para el cumplimiento, es necesario que los empleados de la Cooperativa que están involucrados hayan sido notificados con anterioridad acerca de algún cambio, además deberá asegurar que este no afecte a las actividades

funcionales de los sistemas de información de la Cooperativa.
12.6.2 Restricciones en la instalación de software
a. Esta política se refiere al control de las aplicaciones y del software que están instalado en los equipos informáticos de los funcionarios de la Cooperativa. b. Para el cumplimiento, es necesario que se realice una revisión periódica y un mantenimiento de los equipos informáticos de la Cooperativa, este proceso puede llevar a cabo el encargado de seguridad de cada una de las agencias.
12.7 Consideraciones de las auditorías de los sistemas de información
12.7.1 Controles de auditoría de los sistemas de información
a. Esta política se refiere a que se debe realizar auditorías internas y externas de forma periódica con la finalidad de verificar el correcto funcionamiento de los diferentes sistemas informáticos de la Cooperativa. b. Para el cumplimiento, es necesario que se sigan los siguientes lineamientos: - Id del usuario - Nombre el usuario - Fecha y hora de ingreso y salida. - Fecha y hora de actualización - Registro de IP - Registro de intentos no permitidos a los sistemas de información - Cambios en los perfiles de usuario - Control de activación y desactivación de antivirus

Tabla 58. Política de seguridad – Seguridad en la operativa

Elaborado por: El investigador

3.2.3.4.9. Seguridad en las telecomunicaciones

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**SEGURIDAD EN LAS**	**REF.**

	TELECOMUNICACIONES	13
OBJETIVO	Asegurar la integridad y veracidad de la información en las redes informáticas y en los procesos de intercambio de información.	

13.1 Gestión de la seguridad en las redes

13.1.1 Controles de red

a. Esta política se refiere a administrar y monitorear las redes de comunicaciones de forma permanente, para lo cual debe mantener la seguridad y de esta manera garantizar que la información que va ser transmitida sea segura.
b. Para el cumplimiento, es necesario que se sigan los siguientes lineamientos:
   - El administrador de red debe establecer responsables de administración y de monitoreo de redes de comunicaciones que incluya equipos de redes, routers, switchs y cableados.
   - Agregar controles para garantizar la confidencialidad de la información por redes inalámbricas, VPN y sistemas de encriptación.
   - Debe existir un control de acceso a las redes.
   - Cambiar la configuración de los equipos cada cierto tiempo.

13.1.2 Mecanismos de seguridad asociados a servicios de red

a. Todas las computadoras utilizadas en la matriz deben estar enlazadas a una red de datos principal.
b. Existirá una comunicación entre la matriz y las diferentes sucursales.
c. Todas las computadoras deben contar con políticas adecuadas de red que incluye lo siguiente:
   - Negación a páginas no autorizadas
   - Negación a contenidos inapropiados
   - Protección de las páginas web y aplicaciones informáticas
   - Protección del correo electrónico
   - Acceso seguro a los sitios web
   - Protección de servidores web
   - Sistema de detección de amenazas

- Sistema de protección de amenazas
- Supervisión de los puestos de comunicación

13.1.3 Segregación de redes

a. Esta política se refiere a dividir en segmentos la red de datos tomando en cuenta dominios lógicos y de esta manera mantener redes por separado.
b. Para el cumplimiento, es necesario que el administrador de redes documente los segmentos de red utilizados en cada agencia estableciendo perímetros de seguridad, también configurar *gateways* o *firewalls*, redes virtuales privadas con la correcta aplicación de políticas de seguridad para el acceso a las mismas.

13.2 Intercambio de información con partes externas

13.2.1 Políticas y procedimientos de intercambio de información

a. Esta política se refiere a autorizar y analizar todo clase de información que se va a transferir a entidades externas y por algún medio de comunicación.
b. Para el cumplimiento, es necesario utilizar los medios oficiales por el cual se realizará la transferencia de la información, si es manual, debe entregarse personalmente al destinatario y la entrega debe ser registrada.

13.2.2 Acuerdos de intercambio

a. Esta política se refiere a establecer la seguridad de la información a transferir a instituciones externas, del ser el caso es conveniente que la información para que sea transmitida sea encriptado.
b. Para el cumplimiento, es necesario que la información que se va a trasmitir sea revisada y aprobada. Para realizar una transferencia por vía electrónica necesita ser encriptado con los respectivos acuerdos de confidencialidad de la información entre las organizaciones y la Cooperativa.

13.2.3 Mensajería electrónica

a. Esta política se refiere a establecer la información que se envía por la mensajería electrónica.
b. Para el cumplimiento, es necesario que el jefe del departamento de tecnología realice el monitoreo de la información que se transmite en las cuentas de correo electrónico instantáneo. Los empleados deben transmitir la información utilizando el correo institucional que previamente ha sido

creado por el departamento de tecnología
13.2.4 Acuerdos de confidencialidad y secreto
a. Esta política se refiere a asegurar la información que se envía por la mensajería electrónica. b. Para el cumplimiento, es necesario que se identifique, revise y se documente de forma permanente los acuerdos de confidencialidad que se transmite dentro de la Cooperativa y sus agencias.

Tabla 59. Política de seguridad – Seguridad en las telecomunicaciones

Elaborado por: El investigador

3.2.3.4.10. Adquisición, desarrollo y mantenimientos de los sistemas de información

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE LOS SISTEMAS DE INFORMACIÓN**	**REF.**
		14
OBJETIVO	Realizar la adquisición, así como también desarrollar y dar mantenimiento a los diferentes sistemas de información que la Cooperativa maneja, incluyendo los controles para la validación de la información y el correcto funcionamiento dentro de la institución.	
14.1 Requisitos de seguridad de los sistemas de información		
14.1.1 Análisis y especificación de los requisitos de seguridad		
a. Esta política se refiere al análisis y las especificaciones de los requerimientos de seguridad de la información para determinar las mejoras y el requerimiento de nuevos sistemas de información. b. Para el cumplimiento, es necesario realizar la planificación, análisis y diseño de sistemas de información, los cuales deben incluir mecanismos de seguridad de la información, que no afecten al producto final y además debe cumplir con las necesidades actuales de la Cooperativa. Además es necesario que se detalle un análisis de riegos para los nuevos requerimientos de seguridad.		

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas

a. Esta política se refiere a la protección de la información que se transmite evitando la alteración, duplicación o divulgación que no esté autorizado.
b. Para el cumplimiento, es necesario realizar revisiones de forma periódica del almacenamiento y funcionamiento de la información que procesan sistemas, con la finalidad de verificar que esté instalado en los lugares correctos para evitar la alteración, duplicación o divulgación no autorizada.

14.2 Seguridad en los procesos de desarrollo y soporte

14.2.1 Política de desarrollo seguro de software

a. Esta política se refiere a establecer nuevas reglas para el desarrollo de aplicaciones informáticas que permitan proteger la información y controlar el código fuente de los diferentes sistemas.
b. Para el cumplimiento, es necesario establecer un ciclo de desarrollo de los sistemas, tomando como base las metodólogas ágiles que permitan aplicar normativas de seguridad y de calidad. Todos estos estándares legalizados por el Departamento de Tecnología.

14.2.2 Procedimientos de control de cambios en los sistemas

a. Esta política se refiere a establecer controles de cambios producidos en los sistemas.
b. Para el cumplimiento, es necesario establecer una solicitud por escrito al Departamento de Tecnología dando a conocer los cambios que se requieren en los diferentes sistemas de información como hardware, software o base de datos.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

a. Esta política se refiere a verificar el impacto de las aplicaciones informáticas una vez que se aplicados diferentes cambios.
b. Para el cumplimiento, es necesario analizar realizando pruebas con la finalidad de verificar el correcto funcionamiento de los sistemas de información los cuales han sido actualizados, una vez que hayan sido

modificados los sistemas deben tener el mismo rendimiento.

14.2.4 Restricciones a los cambios en los paquetes de software

a. Esta política se refiere a colocar seguridad en los paquetes software que se encuentran en los equipos informáticos de la Cooperativa.
b. Para el cumplimiento, es necesario que el Departamento de Tecnología evalué los cambios necesarios a realizar a los paquetes informáticos que no afecte la integridad, confidencialidad y disponibilidad de la información.

14.2.5 Uso de principios de ingeniería en protección de sistemas

a. Esta política se refiere a la aplicación de principios de seguridad en la ingeniería de sistemas de información las mismas que deben ser documentadas, y actualizadas de forma permanente.
b. Para el cumplimiento, es necesario que el Departamento de Tecnología asigne un responsable que se dedique a la investigación de los principios de ingeniería para proteger los distintos sistemas de la Cooperativa.

14.2.6 Seguridad en entornos de desarrollo

a. Esta política se refiere a la protección de los entornos de desarrollo que utiliza la el Departamento de Tecnología para desarrollar las aplicaciones.
b. Para el cumplimiento, es necesario que el Departamento de Tecnología elija un entorno adecuado para el desarrollo de sistemas aplicando las políticas de acceso y seguridades necesarias. Además, se debe seleccionar al personal adecuado para el desarrollo de sistemas.

14.2.7 Externalización del desarrollo de software

c. Esta política se refiere a supervisar y monitorear cada una de las actividades para el desarrollo de los sistemas que se realicen fuera de la Cooperativa.
d. Para el cumplimiento, es necesario que el Departamento de Tecnología elija un entorno adecuado para el desarrollo de sistemas aplicando las políticas de acceso y seguridades necesarias. Además, se debe seleccionar al personal adecuado para el desarrollo de sistemas. Todas las aplicaciones

desarrolladas fuera de la institución deben ser entregadas en los plazos establecidos.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas
a. Esta política se refiere a verificar que las pruebas que se realicen durante el desarrollo de sistemas no afecten al funcionamiento de los mismos. b. Para el cumplimiento, es necesario un cronograma de pruebas con los usuarios reales, con la finalidad de evaluar el nivel de seguridad de los sistemas y mejorarlos de ser el caso empleados para tener la información segura. c. Además, se debe documentar las pruebas realizadas, registrando fecha, hora y las observaciones encontradas en las mismas.
14.2.8 Pruebas de aceptación
a. Esta política se refiere a planificar una serie de pruebas para la aceptación de los nuevos sistemas de información que serán utilizados dentro de la Cooperativa. b. Para el cumplimiento, es necesario un crear un plan de pruebas de los sistemas mismo que debe estar aprobado por el Gerente de la Cooperativa ya que serán puesto en funcionamiento dentro de la institución, estas pruebas deben detectar incidencias, mejoras en los sistemas, código malicioso y observaciones con su respectiva documentación.
14.3 Datos de prueba
14.3.1 Protección de los datos utilizados en pruebas
a. Esta política se refiere a establecer los datos que se van a utilizar con la finalidad de evitar que se usen datos críticos. b. Para el cumplimiento, es necesario impedir la utilización de las bases de datos operacionales en un ambiente de pruebas, para lo cual se debe utilizarse las herramientas para generar datos personalizados.

Tabla 60. Política de seguridad – Adquisición, desarrollo y mantenimiento de los sistemas de información

Elaborado por: El investigador

3.2.3.4.11. Relaciones con suministradores

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**RELACIONES CON SUMINISTARDORES**	**REF.** 15
OBJETIVO	Asegurar la confidencialidad, integridad y disponibilidad de la información en los procesos de compra, arrendamiento y contratación de servicios con terceros.	
15.1 Seguridad de la información en las relaciones con suministradores		
15.1.1 Política de seguridad de la información para suministradores		
a. Esta política se refiere a determinar los requerimientos de seguridad de la información para minimizar los riesgos que no están autorizados por parte del personal proveedor y de terceros. b. Para el cumplimiento, es necesario que se analice los riesgos de la información a los que está expuesta por accesos no autorizados o de terceros, una vez establecido el análisis se deben determinar las necesidades y requerimientos de seguridad en aprobación con el gerente y jefes de áreas del Departamento de Tecnología, todo esto debe estar debidamente documentado.		
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores		
a. La documentación como los contratos, términos de referencia, especificaciones técnicas, actas de entrega recepción y demás documentación que garantice la correcta administración, aseguramiento, obligaciones, costes, multas deberán estar ligados al Departamento de tecnología y la Superintendencia de Compañías para llevar los procedimientos de forma adecuada. b. Para el servicio que brinda el alojamiento de los datos y registros del sistema financiero, es necesario suscribir un acuerdo de confidencialidad de la información que debe garantizar la confidencialidad, integridad y disponibilidad de la información, así como establecer las posibles sanciones o multas a las personas que infrinjan cualquier clausula establecida en el acuerdo.		

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones
a. Esta política trata de determinar y documentar los requerimientos de seguridad de la información de los proveedores que accedan a los componentes tecnológicos. b. Para el cumplimiento, es fundamental cumplir con la política de seguridad para suministradores y establecer políticas para el mantenimiento y revisar configuraciones de fábrica de los equipos tecnológicos.
15.2 Gestión de la prestación del servicio por suministradores
15.2.1 Supervisión y revisión de los servicios prestados por terceros
a. Para todos los contratos que realiza la Cooperativa existirá un Administrador de Contrato quien será el responsable de supervisar los acuerdos y clausulas establecidas en los contratos y en todos los documentos suscritos con los proveedores tecnológicos, además será encargado de designar un técnico para supervisar todos los servicios tecnológicos de terceros. b. El personal designado debe supervisar los contratos mensualmente sobre los Acuerdos de Nivel de Servicio (SLA), suscritos con los proveedores. c. El personal designado debe supervisar periódicamente los informes mensuales de la disponibilidad técnica remitidos por los proveedores de servicio; de existir una inconformidad por parte de estos proveedores se debe informar al departamento de tecnología para establecer sanciones y multas aclaradas en los contratos.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
a. Esta política trata de determinar las especificaciones cuando haya cambios en la prestación de servicios. b. Para el cumplimiento, es importante tener la documentación de los cambios realizados que permitan mejorar los servicios. Además, es fundamental realizar nuevos controles a los cambios realizados con el fin de proponer mejoras a la seguridad de la información.

Tabla 61. Política de seguridad – Relaciones con suministradores

Elaborado por: El investigador

3.2.3.4.12. Gestión de incidentes en la seguridad de la información

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	**REF.** 16
OBJETIVO	Gestionar los diferentes incidentes que se pueden dar a la seguridad tomando en cuenta los activos de información de la Cooperativa ya que están expuestos a soportar incidentes de seguridad, además se debe garantizar la gestión adecuada de todos los incidentes comenzando desde comunicación, de tal manera que se corrijan oportunamente.	
16.1 Gestión de incidentes de seguridad de la información y mejoras		
16.1.1 Responsabilidades y procedimientos		
a. Esta política se refiere a establecer las responsabilidades y procedimientos, que deben tener cada uno de los empleados del departamento de tecnología de la Cooperativa y sus agencias para identificar incidentes de seguridad de información y poder minimizar los riesgos dentro de la institución. b. Para el cumplimiento, es necesario capacitar al personal involucrado del área de tecnología en los incidentes que se pueden ocurrir al manipular los sistemas de información. Para lo cual debe existir un responsable de gestionar los incidentes y poder mitigarlos a fin de proteger la información.		
6.1.2 Notificación de los eventos de seguridad de la información		
a. Esta política se refiere a notificar sobre los eventos de seguridad implementados o actualizados mediante el correo electrónico a los diferentes funcionarios de la institución. b. Para el cumplimiento, es necesario capacitar al personal involucrado sobre los eventos de seguridad implementados dentro de los sistemas de información de la Cooperativa con la finalidad de cometer errores.		
16.1.3 Notificación de puntos débiles de la seguridad		
a. Esta política se refiere a notificar sobre la notificación de puntos débiles		

de seguridad implementados los cuales afecten al correcto funcionamiento de los sistemas de información.

b. Para el cumplimiento, es importante crear cuentas de correo que permitan notificar cuando ocurre un evento o alguna vulnerabilidad en los sistemas. Esta configuración debe hacerlo el jefe del departamento de tecnología, el mismo que debe realizar el seguimiento adecuado al evento o incidente ocurrido.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

a. Esta política se refiere a evaluar y valorizar los eventos de seguridad del análisis realizado, se debe clasificarlos y luego tomar decisiones sobre el incidente.
b. Para el cumplimiento, es importante seguir los siguientes lineamientos:
    - Analizar los puntos débiles para determinar el tipo de incidente.
    - Si es una amenaza se debe notificar al usuario que reporto el evento y se cierra el registro.
    - Si corresponde a una debilidad se siguen los procedimientos necesarios para restablecer la funcionalidad de los sistemas de información.
    - Se activa inmediatamente un proceso de gestión de incidentes para dar solución a los problemas.

16.1.5 Respuesta a los incidentes de seguridad

a. Esta política se refiere a proporcionar una respuesta de forma inmediata a los incidentes ocurridos.
b. Para el cumplimiento, el encargado del área de seguridad debe contactase con el empleado que reporto el incidente en un plazo máximo de 48 horas, seguidamente debe poner en ejecución el proceso de gestión de incidentes con la finalidad de restablecer los sistemas.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

a. Esta política se refiere a utilizar los aspectos adquiridos en el análisis y las respuestas de incidentes de seguridad, con la finalidad de reducir el impacto en futuros incidentes.
b. Para el cumplimiento, el encargado debe realizar una revisión periódica de

incidentes y el impacto que obtenga sobre los activos de información de la Cooperativa. Esta revisión permitirá solucionar de mejor manera los incidentes mediante un plan adecuado.
16.1.7 Recopilación de evidencias
a. Esta política se refiere a mantener un registro de todos los incidentes ocurridos en los sistemas de información con la finalidad de reducir el impacto y que no vuelvan a suceder. b. Para el cumplimiento, el encargado de seguridad de la información debe tener un registro actualizado de las evidencias de todos los incidentes, verificar todas las consecuencias para la Cooperativa para dar solución oportuna y establecer los mecanismos adecuados para que no vuelvan a suceder.

Tabla 62. Política de seguridad – Gestión de incidentes en la seguridad de la información

Elaborado por: El investigador

3.2.3.4.13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**	**REF.** 17
OBJETIVO	Gestionar los diferentes incidentes que se pueden dar a la seguridad tomando en cuenta los activos de información de la Cooperativa ya que están expuestos a soportar incidentes de seguridad, además se debe garantizar la gestión adecuada de todos los incidentes comenzando desde comunicación, de tal manera que se corrijan oportunamente.	
17.1 Continuidad de la seguridad de la información		

17.1.1 Planificación de la continuidad de la seguridad de la información.
a. Esta política se refiere a determinar las necesidades y requerimientos para la gestión de la seguridad de la información en situaciones de crisis y desastres. b. Para el cumplimiento, es necesario que el responsable de la seguridad desarrolle un plan de continuidad. Se debe identificar y entender los riesgos que asechan a los activos de la información de la Cooperativa para analizarlos, priorizarlos y tomar las decisiones adecuadas.
17.1.2 Implantación de la continuidad de la seguridad de la información
a. Esta política se refiere a notificar sobre los eventos de seguridad implementados o actualizados mediante el correo electrónico a los diferentes funcionarios de la institución. b. Para el cumplimiento, es necesario capacitar al personal involucrado sobre los eventos de seguridad implementados dentro de los sistemas de información de la Cooperativa con la finalidad de cometer errores.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
a. Esta política se refiere a verificar, revisar y evaluar la continuidad de la seguridad de la información para garantizar la seguridad de la misma. b. Para el cumplimiento, es importante identificar los recursos humanos, tecnológicos y financieros para garantizar la seguridad de la información, posteriormente crear un plan de continuidad de seguridad, el mismo que debe ser difundido a todos los funcionarios.
17.2 Redundancias
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
a. Esta política se refiere a evaluar los lugares adecuados para las instalaciones con suficiente espacio para que la información este siempre disponible. b. Para el cumplimiento, es necesario verificar el lugar con planos ayudados de personal técnico donde contemple los avances tecnológicos, cantidad de equipos y que el espacio debe ser flexible para el crecimiento de la Cooperativa.

Tabla 63. Política de seguridad – Aspectos de la seguridad de la información en la gestión de la continuidad de negocio
Elaborado por: El investigador

3.2.3.4.14. Cumplimiento

INSTITUCIÓN	**COAC SAN FRANCISCO LTDA.**	
POLÍTICA	**CUMPLIMIENTO**	**REF.**
		18
OBJETIVO	Verificar el cumplimento de las políticas de seguridad por parte de los todos los funcionarios de la Cooperativa que procesen información directa o indirectamente, en especial los empleados que tengan contacto directo con los diferentes sistemas de información.	
18.1 Cumplimiento de los requisitos legales y contractuales		
18.1.1 Identificación de la legislación aplicable		
a. Esta política se refiere a identificar, documentar y mantener las normas y estatutos legales que se enmarcan en el cumplimiento de las políticas de seguridad de la Cooperativa. b. Para el cumplimiento, es necesario es necesario que se designe a una persona que mantenga actualizada con los estándares y normas legales que rigen en el país y para las instituciones financieras.		
18.1.2 Derechos de propiedad intelectual (DPI)		
a. Esta política se refiere a garantizar los derechos de la propiedad intelectual utilizando software con licencias. b. Para el cumplimiento, es necesario que el jefe del departamento de tecnología gestione las licencias correspondientes para las aplicaciones software, antivirus y páginas web. El software debe estar contemplado en las normativas y estándares vigentes del país.		
18.1.3 Protección de los registros de la organización		
a. Esta política se refiere a la protección de los registros de información de		

la Cooperativa.

b. Para el cumplimiento, el encargado del departamento de tecnología debe tener actualizado un registro de reglamentos y estatutos internos de la Cooperativa para lo cual la persona encargada debe estar lo suficiente capacitado para afrontar aspectos legales.

18.1.4 Protección de datos y privacidad de la información personal

a. Esta política se refiere a garantizar que la información financiera y datos de todos los funcionarios que laboran en la Cooperativa estén correctamente protegidos según los reglamentos y estatutos vigentes.
b. Para el cumplimiento, es necesario que toda la información financiera y datos que se procesan dentro de la Cooperativa estén protegidos con contraseñas seguras que impidan el acceso no autorizado.

18.1.5 Regulación de los controles criptográficos

a. Esta política se refiere a que se deben utilizar controles criptográficos para proteger la información según los reglamentos y estatutos vigentes.
b. Para el cumplimiento, es necesario utilizar políticas que abarquen controles criptográficos para proteger la información de forma eficiente y se contribuya a normal funcionamiento de la entidad financiera.

18.2 Revisiones de la seguridad de la información

18.2.1 Revisión independiente de la seguridad de la información

a. Esta política se refiere a que se deben identificar las políticas de seguridad establecidas en el presente documento para aplicarlas a la Cooperativa dependiendo de los requerimientos.
b. Para el cumplimiento, el Departamento de Tecnología debe analizar las políticas implementadas y utilizarlas con la finalidad de mejorarlas y utilizarlas para la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad

a. Esta política se refiere a que el encargado de seguridad de la información de la Cooperativa realice revisiones periódicas de las políticas de seguridad.
b. Para el cumplimiento, los encargados de la seguridad deben realizar periódicamente revisiones de las políticas de seguridad, verificar el cumplimiento y proponer mejoras en base a las normas y estatutos establecidos.

18.2.3 Comprobación del cumplimiento
a. Para el cumplimiento, el encargado de la seguridad de la información deben realizar pruebas en los sistemas de información y poner en ejecución todos los lineamientos para garantizar la integridad, confiabilidad y disponibilidad de la información dentro de la Cooperativa.

Tabla 64. Política de seguridad – Cumplimiento

Elaborado por: El investigador

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- En relación al cuadro comparativo de los estándares de seguridad de la información se obtuvo que la normativa ISO 27002:2013 presenta mejores ventajas, en vista de que permite preservar la información mediante la confidencialidad, integridad y disponibilidad de la información.

- Dentro de la COAC San Francisco Ltda. los activos de seguridad de la información están expuestos a diferentes amenazas y vulnerabilidades que fueron investigadas mediante la metodología Magerit que consistió en primera instancia en realizar una encuesta al personal del departamento de tecnología y mediante la elaboración de la matriz de riesgos la cual fue elaborada de acuerdo a la selección de amenazas y vulnerabilidades, el impacto y los riesgos sobre los activos.

- De acuerdo a los riesgos que recaen sobre los activos de la COAC San Francisco Ltda. se ha seleccionado un total 5 objetivos de control de la normativa ISO 27002:2013 y se ha establecido una política de seguridad completa con 14 objetivos de control, seleccionando 111 controles, los mismos que se han determinado que son los más adecuados y que se adaptan para minimizar las amenazas y el riesgo que provocaría dentro de la Cooperativa.

- Se diseñó una Política de Seguridad de la Información para el Departamento de Tecnología de la COAC San Francisco Ltda. mediante la Norma ISO/IEC 27002:2013, la misma que está enmarcada a supervisar los procesos de manejo de los servicios de las aplicaciones de gestión financiera y a las plataformas tecnológicas y administrativas, también contiene los aspectos y características sobre buenas prácticas necesarias para gestión de la seguridad y además está enfocada en orientar la correcta gestión de la información dentro de la Cooperativa.

4.2.Recomendaciones

- Con base a este trabajo realizado se puede recomendar que la metodología Magerit es adecuada para ser utilizada en proyectos, planes y procesos que requieren de una estructura debidamente organizada y fundamentada de la gestión de riesgos dentro de una organización.

- Para que la Política de Seguridad de la Información implementada dentro del Departamento de tecnología de la COAC San Francisco Ltda. garantice la seguridad de la información, es necesario realizar un control de forma periódica para verificar si el personal está cumpliendo con las normativas establecidas y si los controles realmente permiten satisfacer las necesidades de seguridad para los fines que fueron seleccionadas.

- Se debe organizar capacitaciones sobre la importancia de la seguridad de la información dentro de la COAC San Francisco, así como también se debe asesorar al cuerpo directivo del Cooperativa en el desarrollo planes, políticas o sistemas de seguridad de la información.

- Con base a la Política de seguridad diseñada y con la finalidad de complementar normativas generales basadas en la Norma ISO/IEC 27002:2013, se sugiere como trabajo futuro, diseñar un modelo de Política de Seguridad de la Información que pueda implementarse en los departamentos de Tecnologías de la Información en cualquier entidad del sector público, cuyo estatuto o nivel organizacional se encuentre a nivel de una Coordinación.

BIBLIOGRAFÍA

[1] C. J. Pilla Yanzapanta, "DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC 27002:2013," vol. 53, no. 9, p. 148, 2019, [Online]. Available: https://repositorio.uisek.edu.ec/handle/123456789/3601.

[2] G. R. Chipantiza Sifuente, "ANÁLISIS DE RIESGO TECNOLÓGICO DEL CENTRO DE DATOS BASADO EN NORMAS INTERNACIONALES: CASO GADMCE," p. 77, 2018, [Online]. Available: https://repositorio.pucese.edu.ec/handle/123456789/1476.

[3] E. Torres Núñez, *"Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato*, vol. 5, no. 54. 2015.

[4] Publicayo Revistas Especializadas, "La información, el activo más valioso de las empresas," Oct. 07, 2019. https://www.publicayo.com/la-informacion-el-activo-mas-valioso-de-las-empresas/ (accessed Mar. 22, 2021).

[5] Y. Alvarado, Richard; Acosta, Karla; Mata de Buonaffina, "Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones," 2018.

[6] H. Susanto, M. Almunawar, and Y. Tuan, "Information security management system standards: A comparative study of the big five," *Int. J. Electr. Comput. Sci. IJECS-IJENS*, vol. 11, no. 5, pp. 23–29, 2011.

[7] Escuela Neijing *et al.*, *Introduccion a la gestión de sistemas de información en la empresa*, vol. 2010. 2011.

[8] A. Suarez, Diana; Ávila, "Una forma de interpretar la seguridad informática," vol. 4, 2015.

[9] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, and J.

A. Saltos-Gómez, “La seguridad informática y la seguridad de la información,” *Polo del Conoc.*, vol. 2, no. 12, p. 145, 2018, doi: 10.23857/pc.v2i12.420.

[10] Ó. Granados, “Nube de Cifras Ciberseguridad: las cifras de los ataques informáticos,” Jul. 17, 2020. https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html. (accessed Nov. 01, 2020).

[11] J. Navarrete, “BDO Euador,” Sep. 14, 2020. https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques (accessed Nov. 01, 2020).

[12] N. Dávalos, “La ciberseguridad en el país ha mejorado, pero aún no es suficiente,” Jul. 06, 2020. https://www.primicias.ec/noticias/tecnologia/ciberseguridad-ecuador-mejorado-no-suficiente/ (accessed Mar. 18, 2021).

[13] M. V. Silva, “El Comercio,” Sep. 29, 2019. https://www.elcomercio.com/actualidad/ecuador-ciberseguridad-region-informe (accessed Nov. 15, 2020).

[14] E. Heraldo, “Tungurahua entre las provincias que más empresas concentran,” Feb. 22, 2016. https://lahora.com.ec/noticia/1101917714/tungurahua-entre-las-provincias-que-ms-empresas-concentran- (accessed Mar. 15, 2021).

[15] ISO, “Serie 27000.” https://www.iso27000.es/iso27000.html (accessed May 26, 2020).

[16] C. Hsu, T. Wang, and A. Lu, “The impact of ISO 27001 certification on firm performance,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2016-March, pp. 4842–4848, 2016, doi: 10.1109/HICSS.2016.600.

[17] R. A. Guevara, “Sistema de gestión de seguridad de información basado en la norma ISO 27001 para el departamento de tecnologías de la información y comunicación del distrito 18D01 de educación,” p. 104, 2017, [Online]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339si.pdf.

[18] M. J. Kenning, “Security management standard - ISO 17799/BS 7799,” *BT*

Technol. J., vol. 19, no. 3, pp. 132–136, 2001, doi: 10.1023/A:1011954702780.

[19] ITIL, "ITIL 4 Componentes Principales." https://www.itil.com.mx/componentes/ (accessed Mar. 19, 2021).

[20] R. Monfort Casañ, "Cobit 5 y el Cuadro de Mando Integral como herramientas de Gobierno de TI.," p. 55, 2016.

[21] S. Quiroz Zambrano and D. Macías Valencia, "Seguridad en informática: consideraciones," *Dominio las Ciencias*, vol. 3, no. 3, pp. 676–688, 2017.

[22] F. N. J. Solarte Solarte, E. R. Enriquez Rosero, and M. del C. Benavides Ruano, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.," *Rev. Tecnológica - ESPOL*, vol. 28, no. 5, pp. 497–498, 2015, [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

[23] J. Fabián, R. Buendía, and F. J. Sanz, *Seguridad informática*. 2013.

[24] E. I. Chilán-Santana and W. F. Pionce-Pico, "Apuntes teóricos introductorios sobre la seguridad de la información," *Dominio las Ciencias*, vol. 3, no. 4, p. 284, 2017, doi: 10.23857/dc.v3i4.686.

[25] J. M. Escudero, "IEDGE – Políticas de Seguridad Informática." https://www.iedge.eu/juan-manuel-escudero-politicas-de-seguridad-informatica (accessed May 28, 2021).

[26] P. B. R. Hernández, C. Fernández, *Metodología de la investigación*. 1375.

[27] Gb-advisors, "Normas y Estándares Internacionales," 2018, [Online]. Available: https://www.gb-advisors.com/es/normas-y-estandares-internacionales/.

[28] Ministerio de Hacienda y Administraciones Publicas, *Magerit Libro II - CATÁLOGO DE ELEMENTOS*. 2012.

[29] ISO/IEC, "NORMA ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).," pp. 1–34, 2017.