OFICINA POSTGRADOS

Tema:

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES FINANCIERAS COOPERATIVAS

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la información

Autor:

Luis Alberto Mungabusi Sisa

Director:

Mg. Edgar Fernando Solís Acosta

Ambato – Ecuador

Junio 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

MODELO DE GESTION DE SEGURIDAD DE LA INFORMACION EN ENTIDADES FINANCIERAS COOPERATIVAS

Línea de investigación:

Seguridad de la Información.

Autor:

Luis Alberto Mungabusi Sisa

Firmado electrónicamente por: EDGAR FERNANDO SOLIS ACOSTA

Edgar Fernando Solís Acosta, Mg. f. _____

CALIFICADOR

José Marcelo Balseca Manzano, Mg. f. _____

CALIFICADOR

Paul Hernan Zurita Llerena, Mg. f. _____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f. _____

DIRECTOR OFICINA DE POSTGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f. _____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
OFICINA DE POSGRADOS

Pontificia Universidad Católica del Ecuador
SECRETARIA GENERAL
PROCURADURÍA

Ambato - Ecuador

Junio 2022

DECLARACIÓN Y AUTORIZACIÓN

Yo: LUIS ALBERTO MUNGABUSI SISA, con CC. 180478341-1, autor del trabajo de graduación intitulado: "MODELO DE GESTION DE SEGURIDAD DE LA INFORMACION EN ENTIDADES FINANCIERAS COOPERATIVAS", previa a la obtención del título profesional de MAGISTER EN CIBERSEGURIDAD, en la oficina de POSTGRADOS.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, junio 2022

LUIS ALBERTO MUNGABUSI SISA

CC. 1804783411

AGRADECIMIENTO

A Dios porque siempre guía nuestro camino para que hagamos el bien y contribuyamos en la sociedad, de manera muy especial a mi esposa, mis padres y hermano por el apoyo incondicional que me brindaron para la culminación de mi educación superior, ellos me enseñaron el valor de luchar por mis sueños y que nada es imposible si se lo desea con el corazón.

Agradezco a los profesores que con su experiencia han sabido guiar para lograr desarrollar un trabajo que aportará de alguna manera la investigación en el ámbito de las entidades financieras que inician con temas de buenas prácticas de seguridad.

DEDICATORIA

Este trabajo de investigación está dedicado para mi esposa, quien han sido una parte fundamental e inspiradora para superar los obstáculos y dificultades que se han presentado durante la elaboración del presente proyecto.

Dedico sobre todas las cosas a Dios todo poderoso, porque siempre nos guía nuestro camino para que hagamos el bien y contribuyamos en la sociedad.

RESUMEN

El presente modelo de Gestión de Seguridad de la Información en una entidad financiera del sector cooperativo se constituye en un proceso metodológico, el mismo que le permite seguir una secuencia de pasos con las consideraciones necesarias para la implementación del presente modelo de gestión. Se inicia con la identificación de un proceso crítico, se encuentra el mapa de procesos de la entidad, en el cual, se detalla la cadena de valor con sus entradas y salidas, de igual manera entender el contexto de la entidad con sus objetivos estratégicos, así como resultado la identificación de un proceso crítico considerado para la definición del alcance, entonces, una vez definido el proceso crítico, se levanta un modelo de implementación de un Sistema de Gestión de Seguridad de la Información, considera el ciclo de mejora continua alineado a entidades financieras del sector cooperativo. Por otro lado, se realiza una revisión específica del estándar ISO/IEC 27005 para una adecuada valoración de riesgos. Se efectúa una evaluación inicial del estándar 27001 y controles del estándar 27002, obtener el estado actual de la entidad, así mismo, se identifican los activos de información del proceso crítico identificado para ser valorados los riesgos. Posteriormente, se prioriza e implementa los controles aplicables para la entidad que sean solventados con pocos recursos. Consecutivamente, se evalúa de nuevo los estándares mencionados con la finalidad de validar el cumplimiento resultante posterior a la implementación de controles. A continuación, de acuerdo con lo descrito se logra el objetivo principal que es, implementar un modelo de gestión de seguridad de la información en entidades financieras del sector cooperativo.

Palabras claves: Riesgos, modelo de gestión, seguridad.

ABSTRACT

This Information Security Management model in a financial entity of the cooperative sector is constituted in a methodological process, the same one that allows you to follow a sequence of steps with the necessary considerations for the implementation of this management model. It begins with the identification of a critical process considering the process map of the entity in which the value chain is detailed with its inputs and outputs, in the same way understanding the context of the entity with its strategic objectives, thus giving as a result the identification of a critical process considered for the definition of the scope, then, once the critical process is defined, an implementation model of an Information Security Management System is raised, considering the cycle of continuous improvement aligned to financial entities of the cooperative industry. On the other hand, a specific review of the ISO/IEC 27005 standard is carried out for an adequate risk assessment. An initial evaluation of the 27001 standard and controls of the 27002 standard are carried out, obtaining the current state of the entity, likewise, the information assets of the critical process identified to be assessed the risks are identified. Subsequently, the applicable controls for the entity that can be solved with few resources are prioritized and implemented. Consecutively, the aforementioned standards are evaluated again in order to validate the resulting compliance after the implementation of controls. Next, according to what has been described, the main objective is achieved, which is to implement an information security management model in financial entities of the cooperative sector.

Keywords: Risks, management model, security.

ÍNDICE

INTRODUCCIÓN

A medida que va evoluciona se va implementa las nuevas tecnologías, las mismas que serían aprovechadas por las organizaciones para brindar servicios digitales más eficientes para sus clientes, convirtiéndose poco a poco en vitales para todas las actividades de la sociedad, es por ello por lo que una interrupción de estos sistemas tecnológicos genera repercusiones instantáneas en la sociedad, por lo tanto, garantizar la información que transita por estos medios digitales es prioridad fundamental para las organizaciones.

Actualmente las instituciones a nivel nacional del sector cooperativo no cuentan con un marco regulatorio proveniente de la Superintendencia de Economía Popular y Solidaria (SEPS) referente a la seguridad de la información, por consiguiente, la entidad que no aplique las mejores prácticas mantiene una inadecuada gestión de los activos de información, por lo que como una opción de mejores prácticas es el marco regulatorio de la Superintendencia de Bancos (SBS), de ahí la importancia de la información que se maneja es fundamental y la implementación de un modelo de gestión de seguridad informática que proteja el activo más importante de una entidad es primordial, con el fin de no generar pérdidas económicas considerables.

La disponibilidad de los servicios electrónicos prestados por una entidad financiera es de vital importancia, debido a que garantizan al cliente que la información que se está maneja estará disponible la mayor parte del tiempo (Hurtado Pérez & Robayo Gonzales, 2019), por lo tanto, los servicios in Cloud aportan significativamente debido a que la gestión es transparente. El robo de la información y actos tecnológicos que atentan a la institución, suelen darse de manera interna, por lo tanto, se considera al colaborador interno como el eslabón más débil de cualquier entidad financiera.

La Cooperativa de Ahorro y Crédito (COAC) Ambato Ltda, es una institución de intermediación financiera controlado por la SEPS, la cual, actualmente dispone de un sistema financiero que automatiza procesos como créditos, ahorro, inversiones, contabilidad y talento humano; además,

dispone de otros servicios complementarios pertenecientes a terceros. Con todo lo mencionado la entidad ha logrado crecer rápidamente en el mercado crediticio y ha llegado a mantener un volumen considerable de información tanto de los asociados como de los procesos internos, esto conlleva a que la información que maneja internamente no se encuentre protegido adecuadamente con las recomendaciones de los estándares internacionales como son la ISO 27001, 27002 y como consecuencia la gestión inadecuada de los activos de información interna de la entidad.

Por lo indicado en el párrafo que antecede, se plantea que la entidad requiere de un modelo de gestión de seguridad de la información, basado en su proceso crítico según el contexto de la organización, la cual de alguna forma permita preservar adecuadamente los activos de información y permita de una forma metodológica alcanzar los objetivos propuestos por la entidad, de tal manera que la entidad cuente con un modelo a seguir en cumplimiento de normas internacionales y de buenas prácticas.

Entidades financieras que están en constante crecimiento a nivel tecnológico y mantienen sus servicios principales alojados in Cloud y Data Center físico, sin la mínima consideración en las configuraciones de seguridad a nivel infraestructura ni concientización a sus colaboradores en temas de seguridad, se convierte en una entidad vulnerable ante posibles ataques cibernéticos, es por ello que las entidades financieras buscarían mejores opciones para mitigar sus vulnerabilidades con el fin de ser una entidad que le otorgue a sus clientes la tranquilidad de que su información, está es manejada bajo una norma internacional de seguridad (Hurtado Pérez & Robayo Gonzales, 2019). Esta tranquilidad se evidencia en el incremento del número de socios en el uso de los servicios prestados por la entidad financiera.

Hacer uso adecuado de la información mediante un estándar internacional como lo es la ISO 27001 proporciona varias garantías a una entidad financiera del sector cooperativo, la cual, permite ser más competitiva en el mercado crediticio tanto del país como a nivel internacional, se demuestra así que la implementación de un modelo de Sistema de Gestión de Seguridad de la Información permite gestionar adecuadamente los recursos informáticos de una entidad.
Para el desarrollo del modelo de SGSI, se cumplirán con los siguientes objetivos específicos:

1. Diagnosticar e identificar el proceso más crítico a nivel de seguridad de la información en la organización.
2. Analizar las diferentes vulnerabilidades de la organización.
3. Seguir el modelo de Sistema de Gestión de Seguridad de la Información.
4. Implementar y evaluar el modelo de gestión de seguridad de la información en el área de crédito.

En cuanto a la implementación del Sistema de Gestión de Seguridad de la información con base en la ISO 27001:2013 en la entidad financiera, se pretende utilizar la metodología del ciclo de mejora continua (PHVA) tal como lo sugiere el estándar ISO.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Seguridad de la información – generalidades

Según la resolución de la Superintendencia de Economía Popular y Solidaria la cual, regula a las entidades financieras del sector cooperativo define a la seguridad de la información como "mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella" (Mejía Caguasango, 2017, pág. 4). El alcance de esta norma nacional hace referencia al control de las seguridades en el uso de transferencias electrónicas.

Todo tipo de información independiente del estado en el que se encuentre se considera como el activo más importante de una entidad, por lo que es una obligación protegerlo adecuadamente aplica controles de buenas prácticas con normas nacionales o internacionales.

> La información representa uno de los activos más importantes de una organización, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar a comprometer su confidencialidad, integridad y disponibilidad. La información se encuentra en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que la organización garantice y asegure la debida protección de la información durante su recolección, almacenamiento, tratamiento y uso (Guzman Silva, 2015, pág. 30).

A continuación, en la siguiente figura se muestra los tres pilares de la razón de ser de seguridad de la información:

Figura 1. Características de Seguridad de la Información.

Fuente: Tomado a partir de (Intekel, 2019)

Integridad

Consiste en que la información se mantenga completa y exactamente tal como fueron generados en un inicio, sin ninguna alteración ni manipulación por terceros (Hurtado Pérez & Robayo Gonzales, 2019). Esta propiedad consiste en que la información permanece integro durante todo el ciclo de vida.

La confidencialidad

Consiste en que la información no se divulga o revela a personas, entidades o procesos sin autorización (Hurtado Pérez & Robayo Gonzales, 2019). Esta propiedad garantiza que la información este accesible solamente al personal autorizado.

La disponibilidad

Consiste en que la información se mantiene siempre a disposición de quienes accederían a ella, ya sean personas, entidades, procesos o sistemas en cualquier momento (Hurtado Pérez & Robayo Gonzales, 2019). Esta propiedad garantiza que los servicios prestados y los datos de una entidad van a estar sin interrupciones para los usuarios finales.

1.1. Sistema de gestión de seguridad de la información (SGSI)

El SGSI es una perspectiva sistemática para establecer, implementar, analizar, mejorar actuaciones organizacionales a través de políticas, procedimientos, actividades y recursos con la intensión de conservar la confidencialidad, integridad y disponibilidad de la información almacenada y procesada por una organización (Hurtado Pérez & Robayo Gonzales, 2019). Es un proceso sistemático y documentado para garantizar que los riesgos de Seguridad de la Información sean aceptados, transferidos, evitados y mitigados.

La información de cualquier entidad está expuesta ante amenazas de irrupción en los cuatro factores de riesgo que son: proceso (por interés comercial, chantajes), persona (negligencia o intencionado), tecnología (fallos en el almacenamiento de datos informáticos o redes telemáticos) y eventos externos (inundaciones o incendio), por lo que cada organización establecerían sus propias políticas y objetivos de seguridad de la información en el marco global de una entidad (López, 2022). Al aplicar buenas prácticas de seguridad de la información se reduce el impacto ante la materialización de los riesgos de cada uno de los factores.

Por lo tanto, según el estándar ISO 27001, define al Sistema de Gestión de Seguridad de la información como el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales (López, 2022). Considera que el activo de información de cualquier organización hoy en día es muy importante y si llegase a ser filtrada estos estarían comercializa en el mercado negro por un costo importante, por lo que es

muy importante adoptar y tropicalizar las recomendaciones internacionales en temas de aseguramiento de información.

Aspectos claves para el SGSI

Según el estándar se contempla los aspectos claves para la implementación de SGSI, las mismas que se detalla a continuación:

Definición clara de un alcance apropiado. - Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases. Indicar las inclusiones con mapas de procesos de alto nivel, diagramas que representen instalaciones o infraestructuras de servicios de TI, conexiones de telecomunicaciones, entre otros, ayuda a entender mejor que funciones, servicios, departamentos, delegaciones, están dentro o fuera del alcance en atención a los intereses de las partes interesadas, requisitos legales y reglamentarios analizados en el momento inicial de implantación del SGSI (López, 2022). Para la definición del alcance se considera los procesos principales de la cadena de valor que aporta significativamente a la organización en otras palabras la razón de ser, debido a que estos manejan información crítica y en caso de perderlos conlleva a una pérdida económica considerable.

Concienciación y formación del personal. - Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI y satisfacer dichas necesidades por medio de formación o de otras acciones (p.ej. contratación de personal ya formado). Evaluar la eficacia de las acciones realizadas mantiene los registros de los estudios, formación, habilidades, experiencia y cual,ificación. (López, 2022). En la presente característica, se considera que todo el personal de una organización está siempre en constante formación o capacitación en temas de seguridad de la confirmación, con el fin de reducir los riesgos de persona que es considerado como el eslabón más débil de cualquier organización.

Proceso de evaluación de riesgos adecuada. - Es habitual comprobar que las organizaciones aplican metodologías inadecuadas por pensar erróneamente que el estándar ISO/IEC 27001

"obliga" a aplicar ciertas metodologías determinadas y/o herramientas software que se autodenominan "compliance" con la norma o con "ISO 31000". Tampoco es siempre acertado pensar que si otras organizaciones se han certificado utiliza una metodología concreta esa misma va a funcionar y ser comprensible en la organización. Cada organización valorarían varios tipos de metodologías hasta confirmar la más adecuada según la cultura y esfuerzo de análisis asociado (López, 2022). El estándar no menciona la metodología de riesgo a utilizar, considera que toda organización selecciona la metodología que más se adapte a sus procesos internos, la gestión de riesgo conlleva una parte fundamental en la implementación del SGSI, debido a que ayuda a tomar decisiones y gestionar adecuadamente los riesgos que mantiene la organización.

Organización y comunicación. - Especialmente en situaciones que requieren de una respuesta rápida y eficaz como es la gestión adecuada de la continuidad de negocio, de los incidentes de seguridad, del cumplimiento legal y de la externalización de cadenas de provisión (López, 2022). La gestión apropiada de la comunicación con medios internos y externos es fundamental para evitar situaciones de crisis que impacten la imagen de la empresa o, al menos, limitar el impacto al mínimo posible.

Integración del SGSI en la organización. - Como en otros aspectos relevantes (p.ej. seguridad y salud laboral, seguridad física o medioambiental) conseguir que las medidas en seguridad de la información formen parte de los hábitos y procedimientos aplicados por todas las personas en sus actividades laborales implica un cambio más o menos drástico en los comportamientos que requiere de tiempo y esfuerzo para corregir/reconducir situaciones de resistencia. Un SGSI que se "alimenta" puntualmente de registros de actividad sin una atención real en las actividades diarias suele verse por el personal como una carga al tener "algo más que atender" que será corregido lo antes posible y que demuestra un grado muy bajo de madurez y eficacia en la implantación y mantenimiento del SGSI (López, 2022). Para que un SGSI se integra adecuadamente en una organización, el responsable de la implementación concientiza la importancia de la seguridad de la información en cada una de las actividades diarias que realiza el personal.

ISO 27001

La ISO 27001 es una norma internacional certificable que permite el aseguramiento de la información en el ámbito de los tres pilares fundamentales de la seguridad de la información como es la confidencialidad, integridad y disponibilidad, se ha demostrado que no es suficiente la implantación de controles y procedimientos de seguridad sin una previa evaluación de riesgos (EditorR, 2016). El proceso de implementación consiste en implementar políticas, procedimientos, controles en la organización que ayuda a reducir los riesgos analizados.

Ítems ISO 27001

Para poder implantar la ISO/IEC 27001 es necesario tener el conocimiento de las secciones obligatorias y las que no; las secciones 0 a 3 son introductorias (no son obligatorias), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una entidad implementarían todas las secciones si requiere cumplir o certificarse con la norma.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión. Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización. Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones. Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también, define las partes interesadas, sus requisitos y el alcance del SGSI. Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de

seguridad de la información. Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como, también, los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información. Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección. Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua. Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18) (Dejan Kosutic, s.f.).

Beneficios ISO 27001

Entre los principales beneficios de implementar la ISO 27001 es "(…) reducir el impacto de los riesgos y amenazas, mejora la planificación y la gestión de la seguridad de la empresa" (Juan A. Figueroa-Suárez, 2017, pág. 149). Uno de los beneficios es garantizar la continuidad del negocio de una entidad y proporcionar garantías frente a la competencia en cumplimiento de normativas tanto nacional e internacional.

El beneficio de contar con una certificación ISO 27001 le beneficia a cualquier tipo de entidad sin importar la actividad económica que esta se dedique o su tamaño, el factor clave para decidir sobre la implantación de un SGSI radica en la importancia para la entidad de la información que almacena y procesa, considerados elementos imprescindibles para alcanzar sus objetivos estratégicos en el ámbito de crecimiento y permanencia en el mercado.

ISO 27002

Según su historia este estándar viene de años la misma que fue establecida por la organización internacional de estándares, a continuación, se menciona un fragmento de los antecedentes de esta norma. En 1995, las organizaciones internacionales The International for Standardization (ISO) e International Electrotechnical Commission (IEC) dieron origen a un grupo de normas que consolidan las directrices relacionadas al alcance de la Seguridad de la información, es representada por la serie 27000.

La ISO/IEC 27002 (anteriormente se denominaba 17799:2005), es la norma que establece mejores prácticas para apoyar a la implementación de Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones (L., 2020). Los ataques cibernéticos incrementan diariamente debido a que la mayor parte de organizaciones ahora prestan servicio en línea. Lo primero a lo que afectan es a la reputación y las finanzas de la organización, pues supone que los controles aplicados no son eficientes.

Es un estándar internacional no certificable que establece las buenas prácticas para iniciar, implementar, mantener un SGSI, además, la versión más actual es ISO27002:2013, este estándar está enfocado a cualquier tipo de organizaciones, independientemente del tamaño, tipo o naturaleza (López, 2022). Esta norma que describe cómo se establece los controles previos a ser seleccionados en base a una valoración de riesgos de los activos de información más importantes de una organización, de igual forma cabe mencionar que se aplica en organizaciones, públicas o privadas, de pequeño y grande tamaño, con o sin fines de lucro.

Principales ítems de la ISO 27002

A continuación, se detalla los 14 Dominios, 35 Objetivos de control y 114 Controles, las cual,es serán seleccionadas previo a una valoración con la metodología de riesgo.

Tabla 1. Controles de la norma ISO27002.

Núm.	Nombre	Se lec	Descripción / Justificación
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información		Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información		Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información		Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información		Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial		Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.6.2.1	Política para dispositivos móviles		Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección		Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo		Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección		Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario		Control: Se debería contar con un proceso disciplinario formal el cual, debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo		Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos		Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos		Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos		Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos		Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información		Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

A.8.2.1	Clasificación de la información		Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información		Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos		Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles		Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios		Control: Se debería disponer en forma segura de los medios si ya no se requieran, utiliza procedimientos formales.
A.8.3.3	Transferencia de medios físicos		Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso		Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red		Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar si se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información		Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

A.9.4.2	Procedimiento de ingreso seguro		Control: Si lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas		Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados		Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía		
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos		Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves		Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física		Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada		Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales		Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde deberán entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos		Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro		Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado		Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos		Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, tenie en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos		Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos		Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados		Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios		Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos		Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo		Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información		Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes		Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.

A.12.5.1	Instalación de software en sistemas operativos		Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas		Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software		Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas		Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes		Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red		Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información		Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información		Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información		Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica		Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye, también, los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas		Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro		Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas		Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		Control: Si se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros		Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro		Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente		Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas		Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba		Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba		Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	Relación con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores		Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, tenie en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos		Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información		Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información		Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información		Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia		Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información		Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información		Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias		Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual		Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros		Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales		Control: Si sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos		Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información		Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o si ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico		Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Tomado a partir de (MINTIC, 2016).

Beneficios de la ISO 27002

Entre los principales beneficios de la implementación de los controles ISO27002 son:

- Mejor concienciación sobre la seguridad de la información.
- Mayor control de activos de información crítica.
- Ofrece un enfoque para la implementación de políticas de control.
- Oportunidad de identificar y corregir puntos débiles.
- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos.
- Se convierte en un diferencial competitivo para la conquista de clientes que valoran la certificación.
- Mejor organización con procesos y mecanismos bien diseñados y gestionados;
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información.
- Conformidad con la legislación y otras reglamentaciones.

Cabe mencionar que estos beneficios son aplicados con respecto a la evaluación de riesgos que la organización mantenga y la información considerada critica (L., 2020).

Cuadro comparativo entre ISO 27001 vs 27002

Tabla 2. Cuadro comparativo de las normas ISO 27001 y 27002

CUADRO COMPARATIVO		
ITEM	ISO 27001	ISO 27002
1	Gestión de la Seguridad de la Información apoyada en la identificación de gestión de riesgos de forma continuada.	Guía de buenas prácticas que describe una serie de objetivos de control.
2	Se debe auditar y certificar el SGSI.	Se podría utilizar para evaluar la integridad del programa de seguridad de la información y no es certificable.
3	Incluye una lista de controles de gestión para las organizaciones.	Mantiene una lista de controles operativos para las organizaciones.
4	Exige la valoración de riesgos sobre cada control para identificar si es necesario disminuir el riesgo.	No distingue entre los controles que son aplicables para una organización y los que no lo son.

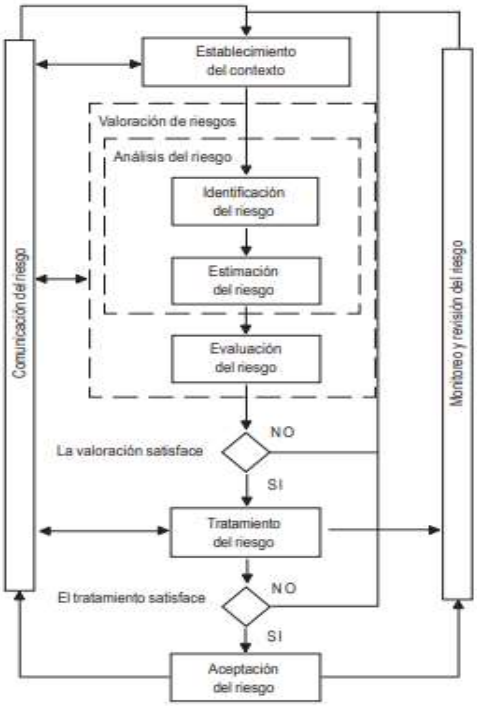
Fuente: Elaboración propia.

ISO 27005

En realidad esta norma es un apoyo a la ISO 27001 y ha sido diseñada para la puesta en práctica cómoda del análisis y la gestión del riesgo de acuerdo a los procesos de la organización, cabe mencionar que es, también, la fase principal de un buen diseño del sistema de gestión de la seguridad de la información (Velásquez, 2018, pág. 5). Para gestionar adecuadamente el riesgo de seguridad de la información, la organización conoce e identifica sus procesos críticos que aporta directamente al giro del negocio definie así el alcance.

Esta norma proporciona criterios de valoración para la gestión adecuada de los riesgos de Seguridad de la Información en una organización, sin embargo, no proporciona una metodología definida para el análisis de riesgo, sino que se detalla mediante sus requisitos el proceso recomendado (López, 2022). La norma cuenta con un listado de criterios de valoración de riesgos que es considerado al momento de la gestión de riesgos, sin embargo, no es obligatorio que se acoja, cada organización tiene su realidad y el giro de negocio. A continuación, en la Figura se muestra el flujo recomendado por esta norma

Figura 2. Proceso para la Gestión de Riesgo de Acuerdo con ISO 27005.



Fuente: Tomado a partir de (ISO, 2018)

Proceso de Gestión de Riesgos

Según la norma ISO 27005 Gestión de Riesgos de la Seguridad de la Información, el proceso recomendado contiene 6 actividades que se detalla a continuación:

Establecimiento del contexto (Cláusula 7)

Según la norma ISO 27005, indica que "Se debería establecer el contexto para la gestión del riesgo en seguridad de la información, la cual, implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de información, definir el alcance y los límites y establecer una organización adecuada que opere la gestión del riesgo en seguridad de la información" (ISO, 2018). Este apartado consiste en que antes de realizar algún tratamiento de riesgo, la organización conoce todos sus procesos, activos, registros, giro del negocio, etc. Posterior a esto el tratamiento depende del apetito de riesgo que la misma tenga definida.

En esta actividad se refiere a toda la documentación necesaria de la organización y se aconseja "seleccionar o desarrollar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos tales como: criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo" (ISO, 2018). Todo lo mencionado en el apartado anterior es considerado como el tratamiento de riesgo, debido a que se detallan los criterios para poder reducir el riesgo, no se eliminaría el riesgo en su totalidad.

Evaluación del riesgo (Cláusula8)

Este paso consta de dos partes, el primero es de un análisis de riesgo y el segundo la valoración del riesgo, esta última consiste en identificar los riesgos de los activos a proteger dentro del contexto de la entidad, la asignación del propietario del activo, Identificación de las amenazas, Identificación de los controles existentes, identificación de las vulnerabilidades y la identificación de las consecuencias. En la estimación del riesgo se basa a metodologías las cual,es podrían ser cual,itativas o cuantitativas o una combinación de ambas depende de las circunstancias, la estimación se basa en evaluación de las consecuencias, probabilidades de incidentes, nivel de estimación del riesgo (ISO, 2018). La evaluación del riesgo consiste en comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

Tratamiento del riesgo (Cláusula 9)

La organización adoptará con base a la evaluación realizada del riesgo el tratamiento correspondiente aplicado a los activos de información, en esta etapa se clasifica como reducir el riesgo, aceptar el riesgo y transferir el riesgo (ISO, 2018). Esta etapa consiste en mantener los riesgos bajo control con respecto al nivel o apetito de riesgo que se quiera definir.

Aceptación del riesgo (Cláusula 10)

En esta etapa se enfoca en la decisión de aceptar el riesgo después de realizar el tratamiento del riesgo, en el cual, se documentará y registrar por la alta dirección (ISO, 2018). Este criterio depende de las políticas, misión, visión y objetivos de la organización, debido a que si es necesario cumplir con algún objetivo específico de la organización y esto conlleva a generar un riesgo alto o medio, la decisión del cuerpo colegiado es aceptarlo con todas las posibles afectaciones que podría ocasionar.

Comunicación del riesgo (Cláusula 11)

Toda la información acerca del riesgo se intercambia y/o comparte entre la persona involucrada en la toma de decisiones (ISO, 2018). Esta actividad consiste en lograr un acuerdo entre las partes interesadas, respecto de la manera de tratar los riesgos identificados intercambia opiniones y comparte información, esto con el fin de entender el motivo de la toma de determinadas decisiones.

Monitorización y revisión del riesgo (Cláusula 12)

Los riesgos y sus factores serán periódicamente revisados y la información que dé como resultado de las revisiones sirve como insumo para las siguientes iteraciones del sistema. Esta norma no recomienda una metodología concreta, puesto que depende de una serie de factores relativos a cada empresa que se plantee implantarla como, por ejemplo: el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI) o el sector comercial de la propia industria. No obstante, como otras normas ISO y sistemas basados en procesos, un método considerado válido y, por lo tanto, recomendable es utilizar como base el modelo PHVA con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua (ISO, 2018).

Esta etapa consiste en realizar el seguimiento y revisión de los controles implementados en el transcurrir del tiempo, esta actividad genera nueva información valiosa para el ciclo de mejora

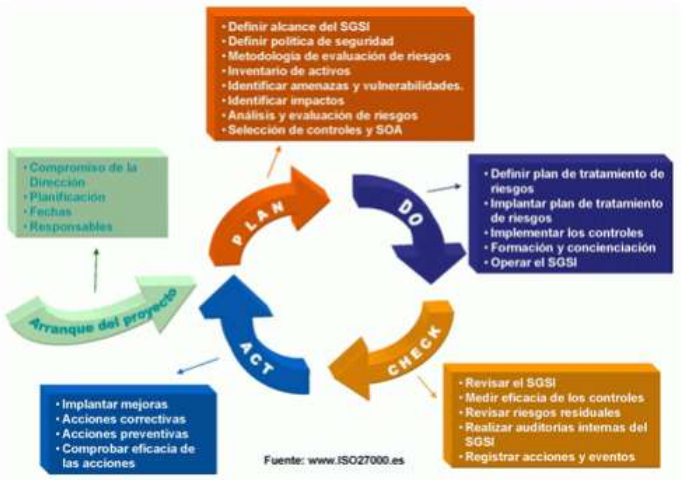
continua como encontrar carencias o problemas que podría tener el plan de tratamiento, así como nuevas vulnerabilidades o cambios en las probabilidades, etc.

1.1 . Ciclo de mejora continua

Dentro de todo tipo de entidades, la seguridad de la información depende del alcance que se le dé a los activos de información, por lo que, es fundamental aplicar medidas de seguridad como buenas prácticas, la mismas que serán valorados y monitoreados constantemente según el ciclo de Deming que consiste en Planificar, Hacer, Verificar y Actuar (PHVA) (Hurtado Pérez & Robayo Gonzales, 2019). El objetivo de esta metodología es definir una estrategia interactiva de resolución de problemas para mejorar continuamente los procesos de gestión.

Para implementar un Sistema de Gestión de la Seguridad de la Información con base a la norma ISO 27001:2013, se maneja un ciclo de mejora continua, planear, hacer, verificar y actuar (PHVA) (Hurtado Pérez & Robayo Gonzales, 2019). Esta metodología es muy flexible y es implementado en muchas áreas según el giro del negocio, debido a que es un ciclo infinito para modificar y mejorar el proceso al que se le aplique.

Figura 3 Ciclo de mejora continua.



Fuente: Tomado a partir de (López, 2022).

Plan (planificar)

Determinar qué hacer y quien es el responsable de hacerlo, valerse de una sesión para definir el contexto de la organización.
El objetivo principal es: Definir políticas, objetivos, procesos y procedimientos relacionados con la gestión adecuada de los riesgos y la mejora continua en temas de la seguridad de la información, esto con el fin de proporcionar resultados que ayuden a cumplir los objetivos de la organización (Hurtado Pérez & Robayo Gonzales, 2019).

Al finalizar esta actividad se determina lo siguiente:

- Quiénes son los responsables de los procesos y su cumplimiento.
- Qué resultados se obtiene del proceso.
- Qué eventos originan las actividades del proceso.
- Dónde se establece el proceso.
- Cuáles son los riesgos y las oportunidades del proceso

Do (hacer)

Desarrollar e implementar las políticas, controles, procesos y procedimientos del sistema de gestión de seguridad de la información (Hurtado Pérez & Robayo Gonzales, 2019). En la presente etapa es necesario un conocimiento previo del paso de la actividad anterior, como es la planificación para poder iniciar la actividad una vez llegada la entrada que da como resultado el origen del proceso y su salida de esta.

Check (verificar)

Medir los trabajos del proceso frente a las políticas, objetivos y la práctica de informar los resultados obtenidos a la gerencia general para su consideración (Hurtado Pérez & Robayo Gonzales, 2019). En esta fase donde se determina si la ejecución de esta actividad se ha llevado a cabo según lo planificado en la primera fase y si los resultados son los deseados.

Act (actuar)

Se lleva a cabo las actividades correctivas y preventivas, en base de los resultados obtenidos de una auditoría interna planificada y revisada por la gerencia, u otra información importante para la mejora continua del sistema (Hurtado Pérez & Robayo Gonzales, 2019). En esta fase se aplican las correcciones necesarias en función de la validación realizada y se ejecuta nuevamente el ciclo PHVA, por tal motivo su definición de mejora continua.

1.2. Gestión de riesgo

Definiciones de riesgo

Riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas produzcan pérdidas para la organización. Según la (SEPS, 2017) define a riesgo como "la posibilidad de que se produzcan pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de información y eventos externos".

Se considera como el grado de exposición al riesgo de un activo de información, o que una amenaza se materialice sobre el mismo causa daños a una organización, por lo que muestra lo que podría pasar a un activo si no se les resguarda apropiadamente (INCIBE, 2016).

CAPÍTULO II. DISEÑO METODOLOGICO

2.1. Caracterización de la empresa o institución

Historia

La Cooperativa de Ahorro y Crédito Ambato, nace en la Comunidad de Chibuleo San Alfonso, parroquia Juan B. Vela, mediante un proceso organizativo, social, económico con el objetivo de remediar necesidades de crédito del Ecuador. Es así como el 10 de enero del 2003 mediante Acuerdo No.001-SDRCC el Ministerio de Bienestar Social reconoce como una sociedad con personería jurídica.

El 13 de enero del 2003 abre las puertas a la ciudadanía la Cooperativa, en la ciudad de Ambato en una oficina ubicada en la calle Juan Benigno Vela y Lalama. Cooperativa Ambato con miras al crecimiento y cobertura nacional: En el año 2008 se adquiere un edificio en la Ciudad de Ambato, se transforma en el edificio matriz. A fines del año 2003 se abre una agencia en Latacunga, provincia de Cotopaxi, en el año 2011 se adquiere el edificio propio en el centro de la ciudad. En el 2004 ampliamos el servicio al cantón Cevallos. Para el año 2006 extendemos el servicio con una oficina en el cantón Pujilí y otra en el cantón Saquisilí para brindar un mejor servicio a la provincia de Cotopaxi.

En el año 2009 para ampliar la cobertura se apertura la oficina Quito provincia de Pichincha y otra en la ciudad de Guaranda provincia de Bolívar. En el año 2015 Según Resolución de la SEPS se resuelve Autorizar el Proceso de Fusión por absorción a la COAC Mushuk Yuyay. La misma que permita ampliar la Cobertura a nivel Nacional como COAC AMBATO LTDA y de esa manera brindar servicios financieros en la Provincia de Napo, Cantón Tena. En el mismo año Según Resolución SEPS se resuelve Autorizar el Proceso de Fusión por Absorción a la COAC Alli Pushak, permite brindar servicios financieros con responsabilidad social en la provincia de Cañar cantón Azogues.

En el año 2018 según resolución de la SEPS resuelve autorizar el Proceso de Fusión por absorción a la COAC Cordillera de los Andes en la ciudad de Quito Centro, COAC Fenix en la ciudad de Quito Norte, amplia la cobertura en la mayor parte de la Provincia de Pichincha.

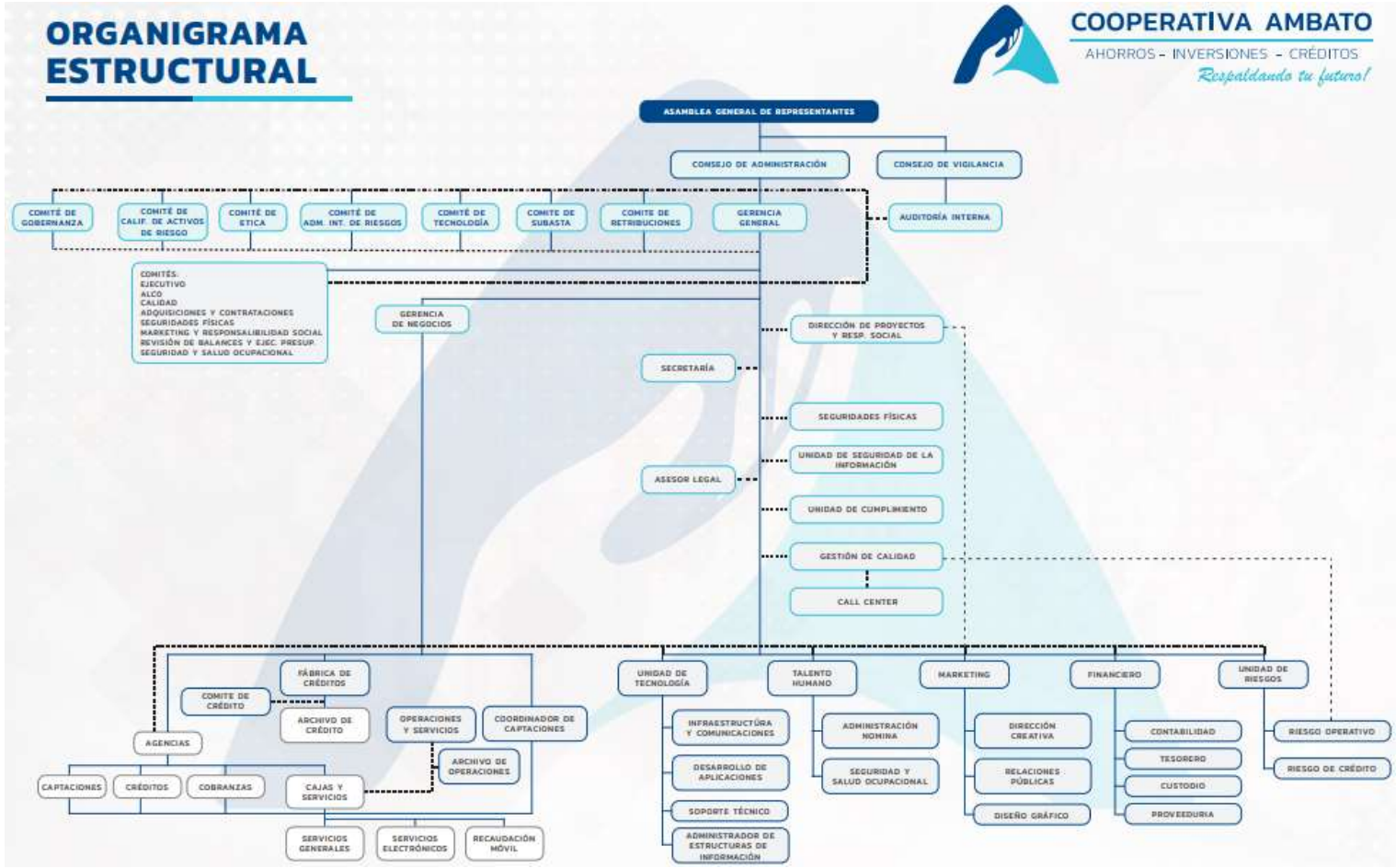
Misión

Promover el desarrollo socioeconómico de la comunidad brinda productos y servicios financieros de calidad.

Visión

Al 2024, alcanzar una calificación de riesgo A+ con mayor cobertura y servicios, basados en tecnología y talento humano competente.

Figura 4. Organigrama Estructural de la Entidad.

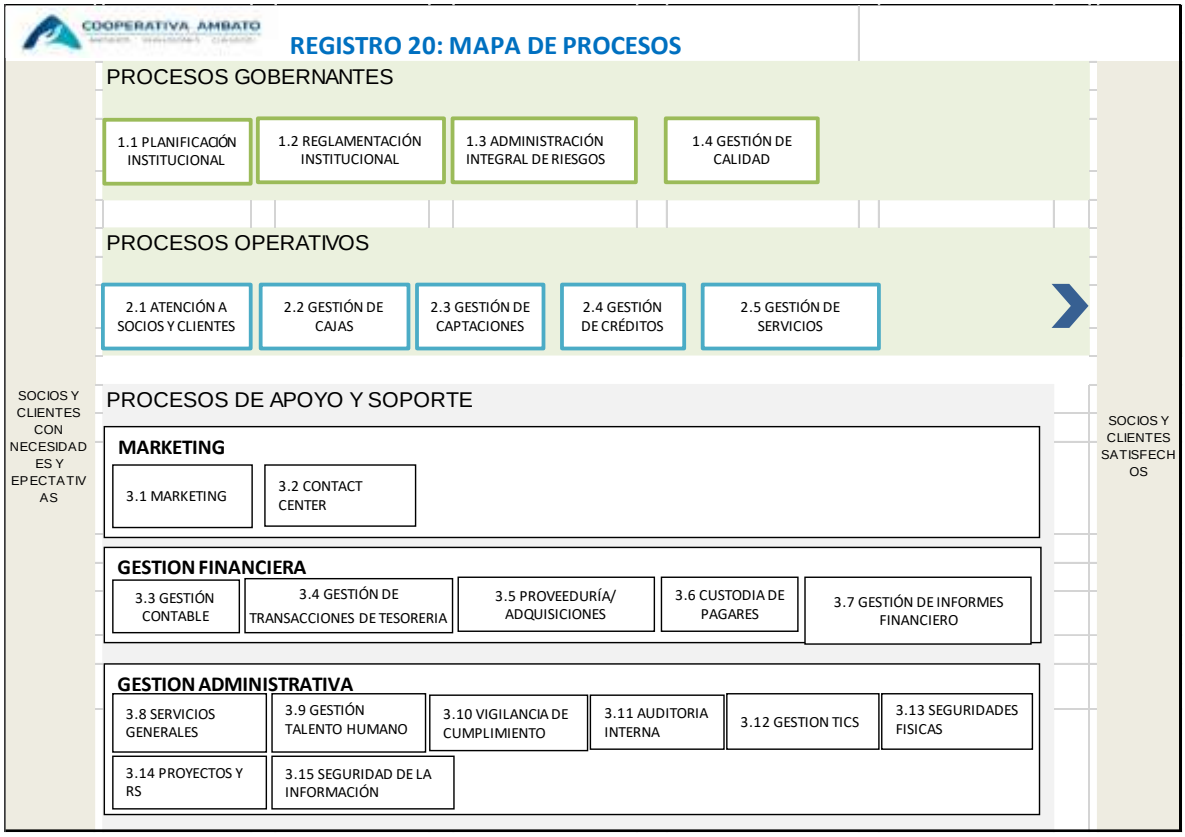


Fuente: Tomado de (COAC AMBATO, 2021)

Mapa de proceso institucional

Para el correcto desarrollo de las actividades de la institución y categorizar de forma correcta cada uno de los procesos identificados internamente, se ha definido por parte del área correspondiente el mapa de proceso institucional, la misma que se observa en la siguiente figura.

Figura 5. Mapa de Procesos de la entidad.



Fuente: Tomado de (COAC AMBATO, 2021)

La Cooperativa de Ahorro y Crédito Ambato Ltda., cuenta con el Mapa de Procesos que es la representación gráfica de los procesos que están presentes en la cooperativa, muestra la relación entre ellos y sus relaciones con las partes interesadas internas y externas. A su vez, los procesos se agrupen en Macro procesos en función de las macro actividades llevadas a cabo, es así como la Cooperativa cuenta con procesos divididos en 3 partes como indica la norma ISO 9001:2015, tales como los Procesos Gobernantes, Operativos y de apoyo y soporte, que son necesarios para la ejecución de los servicios financieros, no financieros y los productos que ofrece la institución.

Según la resolución de la SEPS define el mapa de procesos como un “diagrama que representa la visión global de la estructura de la entidad, donde se presenta todos los procesos que forman parte de la organización y sus principales relaciones” (SEPS, 2017).

Procesos gobernantes

En la resolución de la SEPS indica que “el proceso gobernante o estratégico se considerarán a aquellos que proporcionan directrices y políticas a los demás procesos cuya responsabilidad compete al consejo de administración o directorio y al representante legal, según corresponda, con el fin de cumplir con los objetivos y políticas institucionales. Se refiere a la planificación estratégica, los lineamientos de acción básicos, definición de estructura organizacional, la administración integral de riesgos, entre otros” (SEPS, 2017).

Procesos operativos

Se refieren a todos los procesos que tiene que ver con el giro del negocio. Estos procesos, para su eficiente ejecución, requieren de una normativa clara y precisa, de un soporte documental sólido. Aunque estos procesos son claves para el giro del negocio, por sí solos son insuficientes para conseguir resultados positivos de la gestión que les corresponde realizar. Sin políticas y normativas claras, que se asienten en un sólido soporte documental que señale en forma inequívoca su funcionamiento y alcances, sin sistemas claros y precisos de control y evaluación, y sin procesos de soporte eficientes y efectivos, es muy difícil el poder establecer su eficacia y eficiencia.

Hay que indicar, también, que en la resolución SEPS 0279 define a los procesos operativos como “procesos propios del giro del negocio, que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus socios, clientes o usuarios” (SEPS, 2017).

Procesos de control

Procesos importantes en el desarrollo de las operaciones de la institución, de su eficiencia y eficacia depende el funcionamiento de los procesos gobernantes y los procesos operativos. La normativa nacional lo define de la siguiente manera como “Los procesos administrativos, financieros, tecnología de información, contabilidad, control interno y talento Humano, que apoyan a los procesos gobernantes y productivos” (SEPS, 2017).

Marco legal

La institución al estar legalmente constituida ante los entes de control definidos por el gobierno ecuatoriano, se acoge obligatoriamente a las normas nacionales legales definidas, decretos y leyes, por tal motivo a continuación se presenta un listado con las resoluciones más relevantes en temas de seguridad pertenecientes al marco legal.

> Resolución SEPS-IGT-IR-IGJ-2018-0279 Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la superintendencia de economía popular y solidaria
>
> Resolución No. 128-2015-F Normas para la Administración Integral de Riesgos en las Cooperativas de Ahorro y Crédito y Cajas Centrales y las diferentes normas reformatorias.
>
> Resolución SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 Norma de control de las seguridades en el uso de transferencias electrónicas RESOLUCIÓN JB-2012-2148 de la Junta Bancaria.

2.2. Tipo de investigación y enfoque de investigación

Para realizar el diagnostico actual de la entidad en sus procesos, definir el ámbito de aplicación del SGSI, alcance y limitaciones, se aplica la investigación de campo, debido a que se acude a las partes interesadas o stakeholders para obtener información necesaria, así, también, para la tasación o valoración de riesgo de activos de información se utiliza la investigación cual,itativa, se utiliza la metodología de riesgos basados en la ISO 27005 para seguridad de la información, de igual forma para la demostración de los resultados se utiliza la revisión mediante la investigación explicativa, se mostrara una comparativa del antes y después de la aplicación de la propuesta.

2.3. Tipo de recolección de la información

Para la recolección de la información necesaria se utiliza las siguientes técnicas:

Técnica Documental

Se considera esta técnica debido a que se recurre a diferentes fuentes bibliográficas como: libros, artículos técnicos, tesis desarrolladas en Universidades nacionales e internacionales para profundizar sobre el tema planteado.

Técnica de entrevista

La entrevista se lo realiza a cada dueño de proceso para poder identificar el flujo de la información que maneja cada una, la cual, permite obtener información útil para el desarrollo del presente proyecto.

Técnica de observación

Se considera esta técnica debido a que se realiza la observación directa de cada uno de los flujos de procesos de la entidad, comportamiento de la información en cada uno de sus estados y políticas de seguridad aplicados a la protección de información, esto con el fin de identificar las vulnerabilidades y valorar los riesgos adecuadamente.

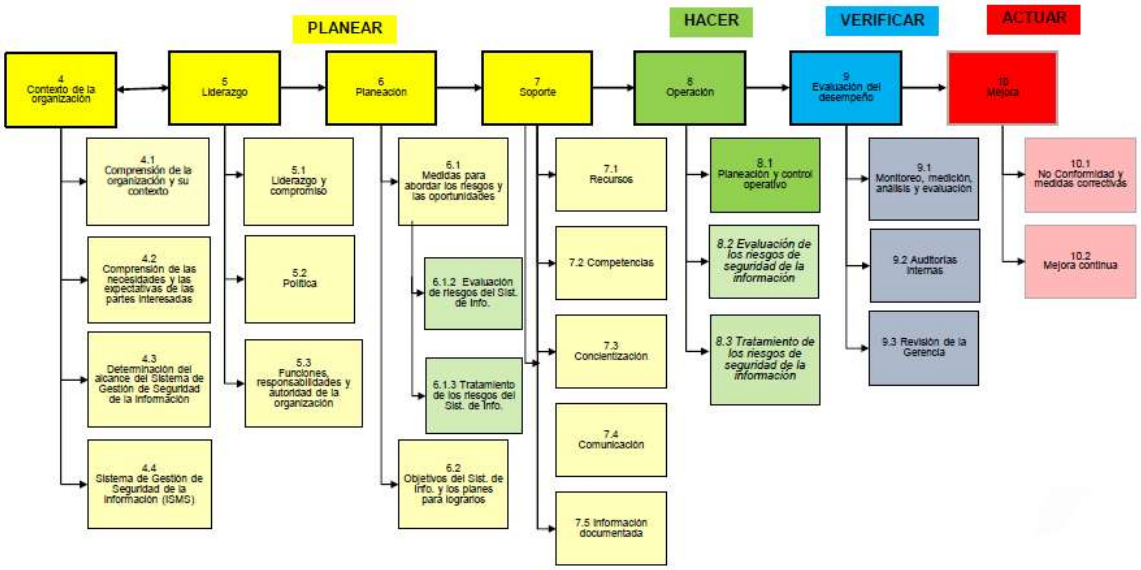
Instrumento de obtención de información

El instrumento para la obtención de la información de cada uno de los procesos involucrados es la matriz de preguntas basadas en la ISO 27001 y 27002.

2.4. Propuesta de Investigación

A continuación, se presenta de manera Grafica el CICLO PHVA asociado a la estructura general de la norma ISO 27001:2013.

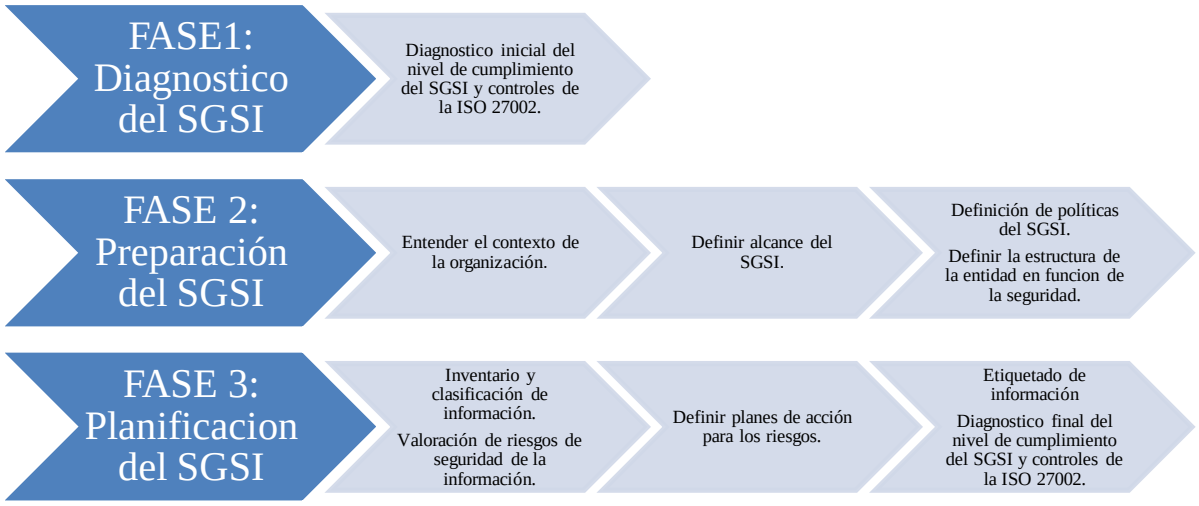
Figura 6. Ciclo PHVA Asociado a la Norma ISO 27001:2013. MINTEL (2020)



Fuente: Tomado de (MINTEL, 2020)

Toma en cuenta los requisitos de la norma ISO/IEC 27001:2013 para el diseño de un modelo de gestión de seguridad de la información, se establecieron las siguientes fases para el desarrollo del presente proyecto.

Figura 7. Modelo de Gestión de Seguridad de la Información.



Fuente: Elaboración propia.

FASE1: Corresponde a las actividades para diagnosticar el nivel de cumplimiento con respecto al SGSI y controles de la ISO 27002, para la recolección de la información, en esta fase se utiliza los mecanismos como:

- Aplicación de entrevistas al personal de la institución con el objetivo de determinar el nivel de cumplimiento del SGSI.
- Revisión de documentación existente del sistema de calidad implementada en la entidad financiera, información de partes interesadas, roles y funciones asociados a la seguridad de la información.
- Fuentes externas como normas de regulación para entidades financieras.

FASE2: Corresponde a las actividades para establecer el SGSI, las cual,es son:

- Analizar el contexto de la organización según el requisito 4 en la cual, se determina las partes interesadas internas y externas de la entidad financiera.
- Definir el alcance del SGSI, en la cual, se establece los límites organizacionales, geográficos y tecnológicos.
- Definir la política de Gestión de Seguridad de la Información.
- Definir la estructura organizacional que contenga los roles y responsabilidades concernientes a la seguridad de la información.

FASE3: En esta fase contempla las actividades relacionadas con:

- Identificación de los activos de información del proceso definido en el alcance y clasificación de acuerdo con la confidencialidad, disponibilidad e integridad.
- Valoración de riesgos de seguridad de la información de acuerdo con el alcance planteado.
- Definir el plan de tratamiento de riesgos identificados que incluya la aplicabilidad de los controles y objetivos, esto hace referencia a los controles establecidos en el Anexo A de la norma ISO 27001:2013.
- Levantar la política y matriz de etiquetado de la información.
- Elaborar el diagnostico final del nivel de cumplimiento con respecto al SGSI y controles de la ISO 27002.

2.4.1. Fase 1 Diagnostico del SGSI

Diagnóstico inicial del SGSI

En la presente fase se realiza un diagnóstico inicial del SGSI que permite diagnosticar los elementos esenciales para actuar según la norma.

El diagnostico permite establecer el nivel de cumplimiento de la norma ISO/IEC 27001:2013. Por lo tanto, se considera en la siguiente tabla los parámetros de evaluación:

Tabla 3. Parámetros de evaluación del SGSI

SIGLA	ESTADO	DESCRIPCIÓN
NC	NO CUMPLE	No existe y/o no se está hace ninguna actividad referente a la ISO7001
CP	CUMPLE PARCIALMENTE	Se está hace de manera parcial, se está hace diferente, no está documentado, se definió y aprobó, pero no se gestiona.
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado, se está cumple con lo que la norma ISO 27001 requiere, es conocido, está documentado, y aplicado por todos las partes interesadas del SGSI.

Fuente: Elaboración propia.

A continuación, se presenta la entrevista aplicada al Oficial de Seguridad de la Información de la Cooperativa de Ahorro y Crédito Ambato Ltda., esto hace referencia a las cláusulas principales del SGSI y el test de cumplimiento normativo ISO 27001.

Tabla 4. Diagnóstico de las cláusulas principales del SGSI

CLÁUSULA	PREGUNTAS APLICADAS	NC	CP	CS	Observación
4	**La Organización y su Contexto**	**8**	**0**	**0**	
4.1	**Entende la Organización y su contexto**	**3**	**0**	**0**	No se ha implementado el SGSI en la entidad.
1.-	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	X			
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	X			
3.-	¿Se han identificado como las partes internas y externas podrían suponer amenazas o riesgos para la seguridad de la Información?	X			
4.2	**Expectativas de las partes interesadas**	**3**	**0**	**0**	
1.-	¿Se han identificado las partes interesadas?	X			
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	X			
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a	X			

	reglamentos, requisitos legales y requisitos contractuales?				
4.3	**Alcance del SGSI**	**1**	**0**	**0**	
1.-	¿Se ha determinado el alcance del SGSI y se conserva información documentada?	X			
4.4	**SGSI Sistema de Gestión de la Seguridad de la información**	**1**	**0**	**0**	
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considera oportunidades de mejora?	X			
5	**Liderazgo**	**1**	**3**	**5**	
5.1	**Liderazgo y compromiso**	**1**	**2**	**0**	
1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		X		Se mantiene un Comité de Seguridad de la Información.
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		X		
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	X			
5.2	**Política de la Seguridad de la Información**	**0**	**1**	**3**	
1.-	¿Se ha definido una Política de la Seguridad de la Información?			X	Se mantiene un manual de políticas de seguridad de la información.
2.-	¿Se ha establecido un marco que permita el establecimiento de objetivos?			X	
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?			X	
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		X		
5.3	**Roles y Responsabilidades**	**0**	**0**	**2**	
1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?			X	Se mantiene definido los roles y responsabilidades de seguridad de la información en el manual de cargos y perfiles de talento humano.
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?			X	
6	**Planificación**	**2**	**5**	**1**	
6.1	**Tratamiento de Riesgos y Oportunidades**	**2**	**3**	**0**	

1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?		X		Se mantiene con un tratamiento de riesgos parcial para seguridad de la información.
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	X			
3.-	¿Se ha definido un proceso de tratamiento de riesgos?		X		
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?	X			
5.-	¿Se mantiene información documentada de los puntos anteriores?		X		
6.2	**Planificación para consecución de objetivos**	**0**	**2**	**1**	
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?		X		Se encuentra definido en el plan estratégico de la entidad.
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		X		
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización tene en cuenta las funciones principales dentro de la Organización?			X	
7	**Soporte**	**2**	**5**	**3**	
7.1	**Recursos**	**0**	**1**	**0**	
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?		X		Se contempla en el presupuesto anual.
7.2	**Competencia**	**1**	**0**	**1**	
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	X			Se emite mensualmente consejos de seguridad pero no se evalúa.
2.-	¿Se mantiene información actualizada sobre la competencia del personal?			X	
7.3	**Concienciación**	**0**	**0**	**2**	
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?			X	Anualmente se realiza la concientización de todo el personal de la entidad.
2.-	¿Existe conciencia de los daños que se podrían producir de no seguir las pautas de la Seguridad de la Información?			X	
7.4	**Comunicación**	**0**	**2**	**0**	

1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		X		Las políticas se dan a conocer mediante correo electrónico e intranet.
2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		X		
7.5	**Información Documentada**	**1**	**2**	**0**	
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluye? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluye registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)		X		Se mantiene documentado como buenas prácticas los manuales, procedimientos, registros y documentos externos alineados a la norma, sin embargo es necesario alinear estrictamente.
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección	X			
3.-	¿Se controlan los documentos de origen externo?		X		
8	**Operación**	**7**	**1**	**0**	
8.1	**Control Operacional**	**3**	**1**	**0**	
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?		X		No se cuenta con un análisis de riesgo en temas de seguridad de la información.
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?	X			
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?	X			
4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?	X			
8.2	**Análisis de riesgos de la Seguridad de la Información**	**1**	**0**	**0**	
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique?	X			No se cuenta con un análisis de riesgo en temas de

	-El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia				seguridad de la información.
8.3	**Tratamiento de riesgos de la Seguridad de la Información**	**3**	**0**	**0**	
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados	X			No se cuenta con un tratamiento de riesgos
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justifica su aplicación?	X			
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?	X			
9	**Evaluación del desempeño**	**7**	**0**	**0**	
9.1	**Seguimiento y medición**	**2**	**0**	**0**	Como aún no se cuenta con el SGSI no se podría realizar el seguimiento correspondiente.
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información tene en cuenta los controles para la seguridad de la información?	X			
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?	X			
9.2	**Auditorías Internas**	**3**	**0**	**0**	
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	X			
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	X			
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	X			
9.3	**Informe de Revisión por la Dirección**	**2**	**0**	**0**	
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	X			
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?	X			
10	**Mejora**	**3**	**0**	**0**	
10.1	**No Conformidades y acciones correctivas**	**2**	**0**	**0**	Como aún no se cuenta con

1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	X			el SGSI no se podría realizar el seguimiento correspondiente.
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	X			
10.2	**Mejora continua**	**1**	**0**	**0**	
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identifica las oportunidades de mejora?	X			

Fuente: Modificado a partir de la ISO 27001:2013.

De acuerdo con la entrevista realizada referente a cada uno de los clausulas mínimas y obligatorios del numeral 4 al 10 de la norma ISO 27001:2013, a continuación, en la siguiente tabla se presenta el resumen del nivel de cumplimiento:

Tabla 5. Diagnóstico inicial del SGSI.

DIAGNOSTICO INICIAL DEL SGSI					
CLÁUSULA	DESCRIPCIÓN	NC	CP	CS	TOTAL PREGUNTAS
4	La Organización y su Contexto	8	0	0	8
5	Liderazgo	1	3	5	9
6	Planificación	2	5	1	8
7	Soporte	2	5	3	10
8	Operación	7	1	0	8
9	Evaluación del desempeño	7	0	0	7
10	Mejora	3	0	0	3
TOTAL		**30**	**14**	**9**	**53**
		NC	**CP**	**CS**	**TOTAL PREGUNTAS**

Fuente: Elaboración propia.

El nivel de cumplimiento y madurez general que se presenta actualmente en la entidad referente a los requisitos mínimos es:

Figura 8. Nivel de cumplimiento general SGSI.

Fuente: Elaboración propia.

Como se evidencia en la gráfica, el nivel de cumplimiento con respecto al estándar ISO 27001 tiene un 57% de incumplimiento con los requisitos, sin embargo, como la entidad se encuentra implementa buenas prácticas a nivel de seguridad cuenta con un 26% de cumplimiento parcial y 17% de cumplimiento.

Diagnóstico inicial de los objetivos de control y controles de la Norma NTC-ISO-IEC 27001:2013

Con el fin de realizar el diagnóstico completo de los requerimientos de la norma, se realiza una validación de los 114 objetivos de control y controles que se obtienen directamente del Anexo A de la norma ISO 27002:2013, en los numerales 5 al 18. Esta validación se lo realiza con los mismos criterios de evaluación de la Tabla 3.

Tabla 6. Diagnóstico inicial de la Matriz del Anexo A ISO 27002:2013

Cláusula	MATRIZ DEL ANEXO A ISO 27001	NC	CP	CS	Observación
A5	**Políticas de Seguridad de la Información**	**0**	**0**	**2**	
A5.1	**Dirección de gestión para la seguridad de la información**	**0**	**0**	**2**	
1.-	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordado con los requisitos del negocio?			X	Actualmente la entidad cuenta con un manual de seguridad de la información en la cual, se detallan las políticas internas.
2.-	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?			X	
A6	**Organización de la Seguridad de la Información**	**0**	**2**	**5**	
A6.1	Asignación de responsabilidades para la seguridad de la información.	**0**	**1**	**4**	
1.-	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?			X	Las responsabilidades se lo detallan en el manual de cargos y perfiles de talento humano, al igual que el oficial de seguridad de la información fue designado por el consejo de administración.
2.-	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?			X	
3.-	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		X		
4.-	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?			X	
5.-	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?			X	
A6.2	**Dispositivos Móviles y Teletrabajo**	**0**	**1**	**1**	

1.-	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?			X	La entidad cuenta con un procedimiento para el teletrabajo.
2.-	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?		X		
A7	**Seguridad en los Recursos Humanos**	**0**	**2**	**5**	
A7.1	**Antes de contratar a un empleado**	**0**	**0**	**2**	
1.-	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación -Referencias			X	Esta actividad se detalla en el manual de talento humano.
2.-	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?			X	
A7.2	**Durante el contrato**	**0**	**2**	**1**	
1.-	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?			X	
2.-	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		X		Se ejecuta la sensibilización pero no se cuenta con un proceso.
3.-	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		X		Se lo comunica mediante correo sin embargo no hay un plan.
A7.3	**Terminación del contrato**	**0**	**0**	**2**	
1.-	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?			X	Esta actividad se define en el manual de talento humano hace referencia al procedimiento de gestión de accesos de seguridad de la información.
2.-	¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como			X	

	por ejemplo cuestiones relativas a la confidencialidad de la Información?				
A8	**Gestión de Activos**	**6**	**4**	**0**	
A8.1	**Responsabilidad sobre los Activos**	**3**	**1**	**0**	
1.-	¿Se ha realizado inventarios de activos que dan soporte al negocio y de Información?	X			No cuenta con un inventario de activos de la entidad.
2.-	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	X			
3.-	¿Se han establecido normas para el uso de activos en relación a su seguridad?	X			
4.-	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?		X		Se realiza un acta entrega de equipos, sin embargo no hay un procedimiento.
A8.2	**Clasificación de la Información**	**1**	**2**	**0**	
1.-	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?		X		Se cuenta con un procedimiento inicial pero no se lo aplica.
2.-	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?	X			
3.-	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?		X		
A8.3	**Manipulación de Soportes**	**2**	**1**	**0**	
1.-	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado -Etc.	X			No se cuenta con ningún procedimiento de manipulación de soporte.
2.-	¿Existen procedimientos establecidos para la eliminación de soportes?	X			
3.-	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad?		X		Seguridad física realiza el control de salida de equipos.

	-Control de salidas -Cifrado etc.				
A9	**Control de Acceso**	**2**	**0**	**12**	
A9.1	**Requisitos generales para el control de acceso**	**0**	**0**	**2**	
1.-	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?			X	Se mantiene un procedimiento de control de accesos
2.-	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?			X	
A9.2	**Accesos de Usuario**	**1**	**0**	**5**	
1.-	¿Existen procesos formales de registros de usuarios?			X	Se mantiene un procedimiento de control de accesos
2.-	¿Existen procesos formales para asignación de perfiles de acceso?			X	
3.-	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?			X	
4.-	¿Se ha establecido una política específica para el manejo de información clasificada cono secreta ? en cuanto a: -Autenticación -Compromisos	X			Aun no se cuenta con la clasificación de la información.
5.-	¿Se establecen periodos concretos para renovación de permisos de acceso?			X	Renovación de claves
6.-	¿Existe un proceso definido para la revocación de permisos si se finalice una actividad, puesto de trabajo o cese de contratos?			X	Talento Humano lo mantiene
A9.3	**Responsabilidades de los usuarios**	**0**	**0**	**1**	
1.-	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?			X	Se detalla en el Manual de Seguridad de la Información
A9.4	**Control de acceso a sistemas y aplicaciones**	**1**	**0**	**4**	

1.-	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?			X	Se lo controla mediante el Directorio activo.
2.-	¿Se han implementado procesos de acceso seguro para el inicio de sesión considera limitaciones de intentos de acceso, controla la información en pantalla etc.?			X	
3.-	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?			X	
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?	X			No se controla a los usuarios privilegiados.
5.-	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?			X	Tecnología mantiene un control de cambios.
A10	**Criptografía**	**2**	**0**	**0**	
A10.1	**Control criptográfico**	**2**	**0**	**0**	
1.-	¿Existe una política para el establecimiento de controles criptográficos?	X			No se mantiene ningún procedimiento en tema criptográfico
2.-	¿Existe un control del ciclo de vida de las claves criptográficas?	X			
A11	**Seguridad Física y del entorno**	**1**	**1**	**12**	
A11.1	**Áreas de Seguridad**	**0**	**0**	**5**	
1.-	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?			X	Se detalla en el Manual de Seguridad Física
2.-	¿Existen controles de acceso a personas autorizadas en áreas restringidas?			X	
3.-	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas accesibles a personal externo?			X	
4.-	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?			X	

5.-	¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?			X	
A11.2	**Seguridad de los equipos**	**1**	**1**	**7**	
1.-	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?			X	Se detalla en el Manual de Seguridad Física
2.-	¿Se protegen los equipos contra fallos de suministro de energía?			X	
3.-	¿Existen protecciones para los cableados de energía y de datos?			X	
4.-	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			X	
5.-	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información?		X		
6.-	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?			X	Configuración de antivirus.
7.-	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?	X			No se cuenta con el procedimiento de destrucción de información
8.-	¿Se establecen normas para proteger la información de equipos si los usuarios abanan el puesto de trabajo?			X	cierre de sesión en 5 min de inactividad
9.-	¿Se establecen reglas de comportamiento para abanos momentáneos o temporales del puesto de trabajo?			X	
A12	**Seguridad en las Operaciones**	**3**	**3**	**10**	
A12.1	**Procedimientos y responsabilidades**	**2**	**0**	**3**	
1.-	¿Se documentan los procedimientos y se establecen responsabilidades?			X	Se detalla en el manual de talento humano
2.-	¿Se controla que la información sobre procedimientos se mantenga actualizada?			X	Mediante la intranet

3.-	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	X			
4.-	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?			X	Monitoreo con zabbix
5.-	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	X			No hay vlans
A12.2	**Protección contra software malicioso**	**0**	**0**	**1**	
	¿Existen sistemas de detección para Software malicioso o malware?			X	Antivirus
A12.3	**Copias de Seguridad**	**0**	**0**	**1**	
1.-	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?			X	Tecnología mantiene un procedimiento
A12.4	**Registros y supervisión**	**1**	**2**	**1**	
1.-	¿Se realiza un registro de eventos? -Intentos de acceso fallidos/exitosos -Desconexiones del sistema -Alertas de fallos Etc.		X		firewall, Waf
2.-	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?		X		Matriz de roles
3.-	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?	X			No hay sistema de control de acceso para administradores.
4.-	¿Existe un control de sincronización de los distintos sistemas?			X	Lo mantiene con el Directorio Activo
A12.5	**Control del Software**	**0**	**1**	**0**	
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?		X		No todos los sistemas mantiene un ambiente de pruebas
A12.6	**Vulnerabilidad Técnica**	**0**	**0**	**2**	
1.-	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?			X	Se maneja con un proveedor anualmente.

2.-	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evita las instalaciones por parte de usuarios finales?			X	Controla con el AD
A12.6	**Auditorias de Sistemas de Información**	**0**	**0**	**2**	
1.-	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?			X	1 vez al año
2.-	¿Se establecen protocolos específicos para desarrollo de auditorías Software considera su impacto en los sistemas?			X	
A13	**Seguridad en las Comunicaciones**	**1**	**3**	**3**	
A13.1	**Seguridad de Redes**	**1**	**2**	**0**	
1.-	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?		X		Se mantiene un Waf, firewall perimetral
2.-	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?		X		
3.-	¿Existe separación o segregación de redes toma en cuenta condiciones de seguridad y clasificación de activos?	X			
A13.2	**Intercambio de Información**	**0**	**1**	**3**	
1.-	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?		X		Manual de Seguridad de la Información
2.-	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?			X	Acuerdos de confidencialidad.
3.-	¿Se establecen normas o criterios de seguridad en mensajería electrónica?			X	Manual de Seguridad de la Información
4.-	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades			X	Acuerdos de confidencialidad.
A14	**Adquisición, desarrollo y mantenimiento de sistemas de información**	**1**	**3**	**10**	
A14.1	**Intercambio de Información**	**0**	**1**	**3**	

1.-	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?			X	En todo proyecto se considera la participación de seguridad de la información
2.-	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?			X	
3.-	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?			X	VPN
4.-	¿Se establecen medidas de protección para transacciones Online?		X		WAF, Firewall aún no se cuenta con una solución antifraude
A14.2	**Seguridad en los procesos de Soporte**	**1**	**2**	**6**	
1.-	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?	X			No existe procedimiento de desarrollo seguro
2.-	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?			X	Tecnología mantiene un procedimiento de control de cambios
3.-	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?			X	
4.-	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?			X	
5.-	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?			X	
6.-	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?		X		
7.-	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?		X		
8.-	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?			X	
9.-	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?			X	
A14.3	**Datos de prueba**	**0**	**0**	**1**	

1.-	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?			X	
A15	**Relación con Proveedores**	**0**	**1**	**4**	
A15.1	**Seguridad en la Relación con Proveedores**	**0**	**1**	**2**	
1.-	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?			X	Se detalla en el procedimiento de gestión de proveedores críticos.
2.-	¿Se han establecido requisitos de seguridad de la información en contratos con terceros¿			X	
3.-	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?		X		
A15.1	**Gestión de servicios externos**	**0**	**0**	**2**	
1.-	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?			X	
2.-	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?			X	
A16	**Gestión de incidentes de seguridad de la información**	**7**	**0**	**0**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	**7**	**0**	**0**	
1.-	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	X			Tecnología mantiene un procedimiento de incidentes de tecnología mas no de seguridad de la información
2.-	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?	X			
3.-	¿Se promueve que se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	X			
4.-	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	X			
5.-	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	X			

6.-	¿La información proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?	X			
7.-	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?	X			
A17	**Gestión de la Continuidad del Negocio**	**0**	**1**	**3**	
A17.1	**Continuidad de la seguridad de la información.**	**0**	**1**	**2**	
1.-	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?		X		plan de continuidad de negocio
2.-	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?			X	
3.-	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?			X	Al menos dos veces al año
A17.2	**Redundancias**	**0**	**0**	**1**	
1.-	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?			X	Se mantiene redundancia de los sistemas críticos.
A18	**Cumplimiento**	**4**	**2**	**2**	
A18.1	**Cumplimiento de los requisitos legales y contractuales.**	**4**	**0**	**1**	
1.-	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento? -LOPD -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad -Ley general de Telecomunicaciones			X	Entes de control aun no cuentan con normas para entidades financieras sin embargo se hace referencias a normas internacionales por buenas prácticas.
2.-	¿Existen procedimientos implementados sobre la propiedad intelectual?	X			

3.-	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	X			
4.-	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	X			
5.-	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	X			
A18.2	**Revisiones de la Seguridad de la Información**	**0**	**2**	**1**	
1.-	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?			X	Se lo ejecuta mediante auditorías internas y externas.
2.-	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?		X		
3.-	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?		X		

Fuente: Modificado a partir de la (MINTIC, 2016).

De acuerdo con la entrevista realizada referente al Anexo A de la ISO27001:2013 A5 hasta la A18, a continuación, en la siguiente tabla se presenta los resultados obtenidos:

Tabla 7 Resumen resultados Anexo A ISO 27001

Cláusula	ANEXO A ISO 27001	NC	CP	CS	TOTAL PREGUNTAS
A5	Políticas de Seguridad de la Información	0	0	2	2
A6	Organización de la Seguridad de la Información	0	2	5	7
A7	Seguridad en los Recursos Humanos	0	2	5	7
A8	Gestión de Activos	6	4	0	10
A9	Control de Acceso	2	0	12	14
A10	Criptografía	2	0	0	2
A11	Seguridad Física y del entorno	1	1	12	14
A12	Seguridad en las Operaciones	3	3	10	16
A13	Seguridad en las Comunicaciones	1	3	3	7
A14	Adquisición, desarrollo y mantenimiento de sistemas de información	1	3	10	14
A15	Relación con Proveedores	0	1	4	5
A16	Gestión de incidentes de seguridad de la información	7	0	0	7
A17	Gestión de la Continuidad del Negocio	0	1	3	4
A18	Cumplimiento	4	2	2	8
TOTAL		27	22	68	117
		NC	**CP**	**CS**	**TOTAL PREGUNTAS**

Fuente: Elaboración propia.

El nivel de cumplimiento y madurez general referente a la matriz del Anexo A de la ISO 27001:2013 es:

Figura 9. Nivel de Cumplimiento de la Matriz del Anexo A ISO 27001:2013.

Fuente: Elaboración propia.

Como se evidencia en las gráficas de cumplimiento de la matriz del Anexo A del estándar ISO 27001:2013, menciona que la institución tiene implementado ciertos controles de los 114 objetivos, la misma que aporta significativamente al cumplimiento del anexo mencionado, esto debido a que la entidad mantiene una buena práctica en temas de seguridad de la información, sin embargo, existen controles sin implementar como la gestión de incidentes y criptografía, debido a que conlleva a una inversión económica considerable.

En términos generales, las siguientes fueron las situaciones identificadas:

1 No cuenta con un modelo de gestión de seguridad de la información.
2 Falta de un adecuado Gobierno de Seguridad de la Información.
3 Falta de formalizar un plan de concientización apropiada.
4 No se cuenta con un inventario de activos.
5 No existe una valoración de riesgos de seguridad de la información.
6 No cuenta con un procedimiento de gestión de incidentes de seguridad de la información.

2.4.2. Fase 2 Preparación del SGSI

Según la norma ISO 27001:2013 reitera la importancia de conocer y comprender los asuntos internos y externos que sean relevantes a su propósito y que son afectados de manera positiva o negativa por el establecimiento del SGSI.

Es por esta razón que la norma incluye en el capítulo 4 CONTEXTO DE LA ORGANIZACIÓN, en el cual, se determina el conocimiento de la organización, asuntos internos, externos e identificación de las partes interesadas las mismas que son pertinentes para poder establecer el alcance del SGSI.

Contexto de la Organización

Actualmente la institución cuenta con los procesos definidos según el sistema de gestión de calidad ISO 9001:2015, la cual, aporta significativamente para los procesos que se va a analizar en la implementación del caso de estudio.

De igual forma mantienen el manual de administración integral de riesgos, se cuenta con las evaluaciones e identificaciones de las áreas críticas con sus respectivas valoraciones de riesgos, cabe mencionar que estas valoraciones serán de mucha importancia, se parte con esta información para poder identificar la prioridad del producto crítico.
La Unidad de Tecnología cuenta con el manual, procedimientos y registros basados en la norma ITIL de buenas prácticas en la administración de tecnología, mantiene identificados los procesos y aplicativos críticos de la institución, la cual, de igual forma es muy útil para definir adecuadamente el alcance del caso de estudio.

Las entidades financieras del sector cooperativo actualmente buscan mejorar en los servicios tanto financieros y administrativos con la finalidad de desarrollarse y evolucionar en el mercado crediticio.

Actualmente el mejoramiento de la gestión administrativa de los procesos ha recobrado impulso, la misma que es validada por los entes de control como es la Super Intendencia de Economía Popular y Solidaria a través de normas nacionales.

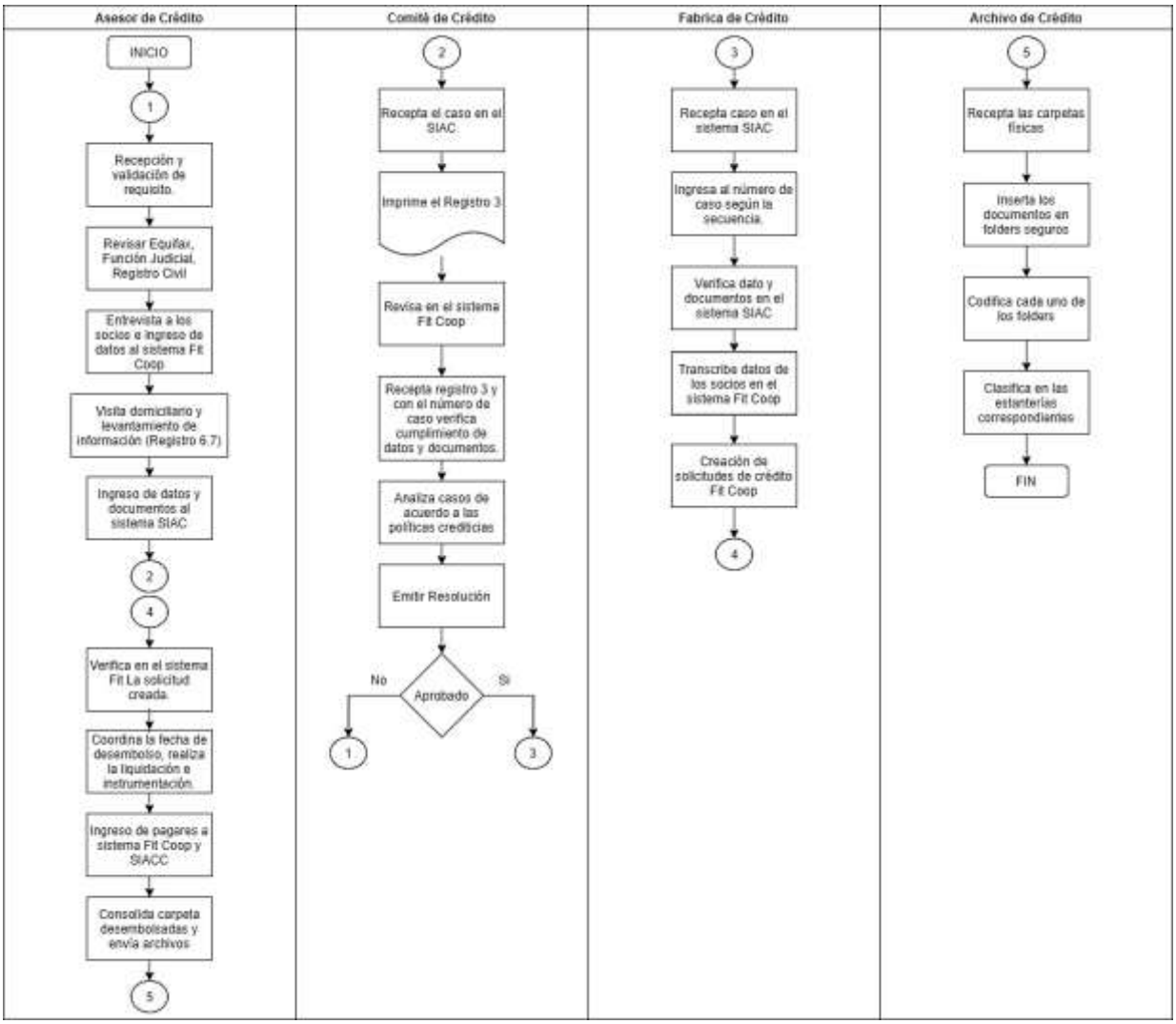
Según el boletín financiero publicado en la SEPS, hasta el mes de marzo del presente año, se obtienen la información necesaria para poder identificar el producto principal de la institución que es de utilidad para la definición del alcance del SGSI.

Figura 10. Identificación de producto principal según el boletín financiero.

Fuente: Modificado a partid de (SEPS, 2021)

A continuación, en la siguiente Figura se muestra el flujo del proceso de la gestión de crédito en la cual, se identifica la participación de varias partes interesadas en el proceso.

Figura 11. Flujo de proceso de otorgamiento de Crédito.



Fuente: Elaboración propia.

Proceso de Gestión de Crédito

Este proceso abarca cada una de las actividades que inciden desde la recepción de la solicitud de crédito, esto con las debidas asesorías e información acerca de tasas, plazos y requisitos hasta la aceptación o negación del crédito.

Actividades del procedimiento

Analista de crédito

- Receptar y validar los requisitos.
- Revisar Equifax.

- Revisar Función judicial.
- Revisar información del Registro civil.
- Entrevistar al socio e ingreso de datos al sistema Fit. Coop.
- Visita domiciliaria y levantamiento de información (Registro 6.7)
- Ingresar de datos y documentos al sistema SIAC.
- Enviar al comité de crédito la solicitud de crédito.
- Verificar en el sistema Fit la solicitud creada.
- Coordinar la fecha de desembolso, realizar liquidación e instrumentación.
- Ingresar el pagare al sistema Fit Coop y SIAC.
- Consolidar carpetas desembolsadas y enviar a archivos.

Comité de Créditos

- Receptar el caso en el sistema SIAC.
- Imprimir registro 3 y revisar en el sistema Fit. Coop.
- Receptar registro 3 y con el número de caso verificar los datos y documentos.
- Analizar el caso de acuerdo con las políticas crediticias.
- Emite la resolución a fábrica de crédito.

Fábrica de Créditos

- Receptar caso en el sistema SIAC.
- Ingresar el número de caso según la secuencia.
- Verificar datos y documentos en el sistema SIAC.
- Transcribir datos de los socios al sistema SIAC.
- Crear solicitudes de créditos Fit. Coop

Archivo de Créditos

- Receptar las carpetas físicas.
- Insertar los documentos en folders seguros.
- Codificar cada uno de los folders.
- Clasificar en las estanterías correspondientes.

Una vez revisado el tema el flujo anterior y las actividades del producto principal, a continuación, se identifica las partes interesadas o Stakeholders del proceso de gestión de crédito, la misma que se detalla en la siguiente Tabla.

Tabla 8. Stakeholders del proceso de otorgamiento de crédito

Partes Interesadas	Necesidades / Expectativas	Requerimiento Contractual	Requerimiento regulatorio o normativo
Asesor de crédito	Personal altamente capacitado para el análisis de crédito.	x	
Comité de crédito	Emitir resoluciones acertadas.		x
Fábrica de Crédito	Verificar información adecuadamente.	x	
Proveedores Tecnológicos	Innovar los sistemas informáticos.		x
Jefe de Tecnología	Garantizar la funcionalidad de los servicios tecnológicos.		x
Custodio de Pagares	Resguardar los documentos de valor.	x	
Archivo de Crédito	Almacenar los folders de crédito codificada adecuadamente.	x	

Fuente: Elaboración propia.

Relación entre el Objetivo y el Proceso

A continuación, en la siguiente figura se muestra la matriz comparativa de Objetivo y Proceso, en el cual, se detalla la valoración de acuerdo con los objetivos estratégicos de la institución:

Tabla 9. Objetivos estratégicos institucionales.

Objetivo	**Descripción**
1	Lograr un nivel de rentabilidad sobre activos (roa) no menor al 2,25%.
2	Alcanzar una cartera en riesgo (5d) no mayor al 4% y un nivel de cobertura mayor al 200%.
3	Lograr un crecimiento anual de captaciones no menor al 30%, con una relación de dpf no mayor al 75%.
4	Fomentar los servicios transaccionales alcanza al menos el 70% de los socios activos usa canales electrónicos.
5	Ampliar la cobertura en al menos 4 oficinas adicionales.
6	Lograr un nivel de satisfacción del cliente no menor al 90%.
7	Atender las novaciones de crédito en no más de 2 días y los créditos nuevos en no más de 4 días.
8	Alcanzar una calificación de riesgo “a+”
9	Alcanzar un nivel de satisfacción y competencia laboral superior al 90%.
10	Implementar el programa anual de desempeño social con enfoque a responsabilidad ambiental, capacitación para fomento de emprendimientos y educación financiera.

Fuente: Elaboración propia.

A continuación, en la siguiente tabla se realiza la matriz de relación entre los objetivos y procesos de la entidad.

Tabla 10. Matriz de relación entre objetivos y procesos.

	Objetivo	**ob.1**	**ob.2**	**ob.3**	**ob.4**	**ob.5**	**ob.6**	**ob.7**	**ob.8**	**ob.9**	**ob.10**	**Total**
Proceso	Gobernantes	1	0.5	0.5	1	1	1	0.5	1	0.5	1	8
	Operativos	1	1	1	1	1	1	1	1	0.5	0.5	9
	Apoyo y Soporte	0.5	0.5	1	1	0.5	0.5	0.5	1	1	1	7.5

Fuente: Elaboración propia.

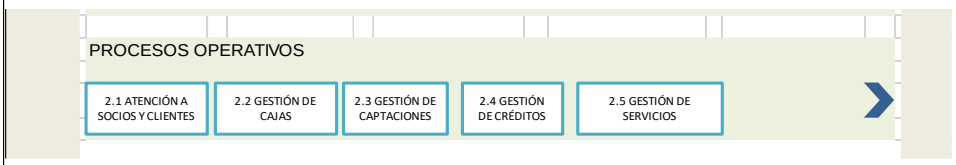
Escala de Valoración:

- **(1)** Aporte Mayoritario al cumplimiento de los objetivos de la institución
- **(0,5)** Aporte Mediadamente al cumplimiento de los objetivos de la institución
- **(0)** No Aporta al cumplimiento de los objetivos de la institución.

Definición ámbito de la aplicación

En la siguiente tabla se detalla el ámbito de aplicación del SGSI, esto enfocado a los objetivos estratégicos de la organización, con el fin de definir adecuadamente el proceso en el cual, se implementa el modelo de gestión de seguridad de la información.

Tabla 11. Identificación del ámbito de aplicación del SGSI.

Empresa:	**Cooperativa de Ahorro y Crédito Ambato Ltda.**	
Misión:	Promover el desarrollo socioeconómico de la comunidad brindando o productos y servicios financieros de calidad.	
Cadena de Valor:		
Objetivos generales del negocio :	Objetivo 1 Lograr un nivel de rentabilidad sobre activos (roa) no menor al 2,25%. Objetivo 2 Alcanzar una cartera en riesgo (5d) no mayor al 4% y un nivel de cobertura mayor al 200%. Objetivo 3 Lograr un crecimiento anual de captaciones no menor al 30%, con una relación de dpf no mayor al 75%. Objetivo 4 Fomentar los servicios transaccionales alcanzando al menos el 70% de los socios activos usando canales electrónicos. Objetivo 5 Ampliar la cobertura en al menos 4 oficinas adicionales. Objetivo 6 Lograr un nivel de satisfacción del cliente no menor al 90%. Objetivo 7 Atender las novaciones de crédito en no más de 2 días y los créditos nuevos en no más de 4 días. Objetivo 8 Alcanzar una calificación de riesgo "a+" Objetivo 9 Alcanzar un nivel de satisfacción y competencia laboral superior al 90%. Objetivo 10 Implementar el programa anual de desempeño social con enfoque a responsabilidad ambiental, capacitación para fomento de emprendimientos y educación financiera.	

ALCANCE SGSI		**JUSTIFICACION** (Explique porqué de su elección, únicamente en los recuadros de color amarillo
Límite Organizacional	**Productos / Servicio: Crédito**	Debido a que la actividad principal a la que se dedica una entidad financiera es a la intermediacion financiera, obteniendo mayores ingresos en el producto mencionado.
	Proceso / Subproceso: Operativo / Gestión de Crédito	Apalancan el cumplimiento de los objetivos institucionales.
Límite Tecnológico	Sistema Fit-Coop, Sistema SiaCC, Sistema Alfresco, Sistema Equifax, Sistema de Registro Civil.	En el proceso operativo intervienen estos activos tecnológicos.
Límite Geográfico	Oficina Matriz y agencia Huachi	Debido a que son las oficinas mas cercanas para evitar trasladarse a lugares lejanos, tomando mayor tiempo en la implementación.

Fuente: Elaboración propia.

Declaración del Alcance

El modelo de gestión de la seguridad de la información abarca solo el proceso crítico de la entidad, puesto que según los estados financieros obtenidos directamente desde la plataforma del organismo de control SEPS al cierre del mes de abril del año en curso cuenta con un activo total de $ 184,907,863.04 DÓLARES AMERICANOS, de los cual,es dentro de los pasivos cuentan con un valor de $ 130,764,442.91 que corresponden a la cartera de créditos otorgados a sus asociados, es esta el ingreso principal de la entidad por su giro de negocio, de igual manera, se hace referencia a los plazos fijos con un valor de $ 109,974,225.03 y los depósitos a la vista por $ 30.944.701,95.

Con estas referencias que antecede, el macro proceso operativo, su giro de negocio y su gran concentración en los resultados financieros, se ha definido el alcance del Sistema de Gestión de Seguridad de la Información al proceso crítico de Gestión de Crédito, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos es específicamente del proceso mencionado, considera que este proceso seleccionado es una fuente principal de crecimiento en sus activos.

El proyecto consiste solo en el análisis y diseño de un modelo de sistema de gestión de seguridad de la información, basado en la ISO27001:2013, pero no abarca las fases de implementación, revisión, mantenimiento y mejora del sistema de gestión de seguridad de la información, esto amerita inversión económica en soluciones de seguridad.

Política del SGSI

Una vez determinado el alcance del diseño del SGSI de la entidad, se establece la política para el apoyo del diseño se hace referencia al punto 5.2 Políticas de Seguridad de la Información, en la cual, indica que la alta dirección en este caso la Gerencia General establece una política de seguridad de la información apropiada para los fines de la entidad, que incluya los objetivos, requerimientos normativos vigentes relacionados con la seguridad de la información y el compromiso de mejora continua.

Ante el presente punto, se evidencia que la entidad cuenta con un Manual de Seguridad de la Información en la cual, se establece las políticas internas y externas, considera los requerimientos normativos legales vigentes y orientados a los objetivos estratégicos de la entidad.

La Gerencia General, representada en el Comité de Seguridad de la Información, considera que la seguridad de la información y el uso de datos personales es un aspecto vital para garantizar el alcance de los objetivos estratégicos planteados del giro de negocio.

Objetivo del SGSI

- Mantener la confidencialidad. Integridad y disponibilidad de la información gestionada por la institución.
- Cumplir con la normativa vigente de los entes de control en cuanto a la Seguridad de la Información.
- Incentivar la cultura de Seguridad de la Información a todos los colaboradores de la institución.

Roles y responsabilidades del SGSI

De acuerdo con el numeral 5.3 de la norma en la cual, indica que “la alta dirección debe asegurarse de que se asignen las responsabilidades y autoridades para las funciones relacionadas con la seguridad de la información” (Hurtado Pérez & Robayo Gonzales, 2019). Con base en este requerimiento de la norma, se identifican las áreas relacionadas con la seguridad de la información y sus responsabilidades la misma que esta detallado en el Manual de Cargos y Perfiles de Talento Humano:

Oficial de Seguridad de la Información.

- ✓ Elaborar, actualizar y proponer al Comité de Seguridad de la Información, la política General de Seguridad de la información para su aprobación.
- ✓ Elaborar y ejecutar el plan de comunicación de los beneficios de la Seguridad de la Información.
- ✓ Administrar el inventario general de activos de información.
- ✓ Elaborar, actualizar y difundir las normas, políticas, metodologías y demás documentos de seguridad de la información, alineados a las normas, reglamentos internos y leyes del Ecuador.
- ✓ Establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, considera un marco adecuado de gestión de riesgos, conforme el alcance.
- ✓ Supervisar que las decisiones tomadas por el comité de Seguridad de la Información sean ejecutadas por las partes involucradas.
- ✓ Diseñar y supervisar los niveles de implementación del Sistema de Gestión de Seguridad de la información, así como dar seguimiento a las acciones preventivas y correctivas.
- ✓ Promover proyectos orientados a reducir las brechas de seguridad de la información institucional.
- ✓ Gestionar el acceso de usuarios a los sistemas de información de la institución.
- ✓ Realizar el escaneo de vulnerabilidades de los equipos críticos.
- ✓ Coordinar con tecnología el parchado correspondiente de los equipos de la institución.
- ✓ El OSI atenderá y responderá inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- ✓ Es responsabilidad del OSI la elaboración de un Plan de Respuesta a Incidentes de Seguridad, con la finalidad de dar una respuesta rápida, que sirva para la investigación del evento y para la corrección del proceso mismo.
- ✓ El OSI creará una base de datos para el registro de incidentes en su red.

- ✓ Es responsabilidad del OSI coordinar la realización periódica de auditorías a las prácticas de seguridad informática, así como, dar seguimiento al corto plazo de las recomendaciones que hayan resultado de cada auditoria.
- ✓ Mantener actualizado de las posibles vulnerabilidades de seguridad de la información del entorno.
- ✓ Monitorear los accesos a canales electrónicos de la institución.

Comité de Seguridad de la Información.

- ✓ El comité de seguridad de la información se encargara de evaluar y supervisar el sistema de gestión de seguridad de la información.
- ✓ Determinar y aprobar el alcance del Sistema de Gestión de Seguridad de la Información en la institución.
- ✓ Conocer y aprobar la Metodología de Gestión de Riesgos de Seguridad de la Información; definir y delegar los equipos responsables del análisis y cálculo de matriz de riesgos de seguridad de la información.
- ✓ Determinar el rango de impuesto económico a causa del riesgo, que estaría dispuesto a correr la institución por temas de seguridad de la información.
- ✓ Analizar y aprobar la información obtenida de la evaluación del GAP Análisis de Seguridad de la información, así como de otras fuentes que permita determinar el estado de madurez y las decisiones a tomar en temas de seguridad de la información.
- ✓ Analizar y aprobar los proyectos orientados a la reducción de brechas de seguridad de la información, así como los costos y recursos necesarios para su implementación.
- ✓ Las reuniones de este comité se realizarán mensualmente deja evidencia de las decisiones adoptadas.
- ✓ El comité de Seguridad de la Información sesionará si Gerencia y/o el Oficial de Seguridad de la Información crean oportuno o por requerimiento de al menos tres de sus miembros.
- ✓ Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- ✓ Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información
- ✓ Definir y aprobar estructuras de la seguridad de la información los roles y responsabilidades del personal involucrado en seguridad de la información.
- ✓ Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- ✓ Formular, revisar y aprobar la política de Seguridad de la Información.
- ✓ El Comité de Seguridad de la Información aprueba normas y procedimientos de seguridad de la Información.
- ✓ Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la Institución.
- ✓ Conocer y aprobar las mallas curriculares de los eventos de capacitación y concientización dirigidos a los servidores de la institución en materia de seguridad de la información.
- ✓ Las responsabilidades determinadas en la conformación del comité, así como las demás inherentes a las atribuciones propias en temas de seguridad de la información.
- ✓ Delegar a un responsable del proceso de seguridad de la información, quien hará las funciones del Oficial de Seguridad de la información.

Dueño de Datos.

- ✓ Determinar los niveles de acceso a la información.
- ✓ Verificar periódicamente la integridad y coherencia de la información de su área.
- ✓ Clasificar la información de su área según la metodología de seguridad de la información.

2.4.3. Fase 3 Planificación del SGSI

Inventario y clasificación de información.

La identificación de los activos de información se lo realiza según el alcance del SGSI, el cual, contempla el proceso de gestión de crédito, por lo tanto, únicamente se identifican los activos de información que son gestionados por el proceso de gestión de crédito.

Tabla 12. Tipos de activos de Información.

Tipo de Activo	Descripción
Servicios	Contempla servicios prestados por el sistema o servicios de comunicación contratados a terceros.
Datos / Información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, manuales, procedimientos, registros, etc.
Software	Programas, aplicativos, desarrollos, software base, sistema de información que contribuye a la operación de un conjunto de procesamiento de datos.
Hardware	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Personal	Personas involucradas en el proceso de negocios y tratamiento de información con responsabilidad directa.
Sitio	Comprende los lugares abarcados por el alcance o parte del mismo, y los medios físicos requeridos para su operación.

Fuente: Modificado a partir de la recomendación de (ISO, 2018, pág. 51)

Tabla 13. Inventario de activos de información del proceso de otorgamiento de crédito.

Id	Área/Dependencia	Código	Nombre del activo de información.	Tipo
1	Tecnología	N/A	Sistema Core Financiero	Software
2	Tecnología	N/A	Sistema SiaCC	Software
3	Tecnología	N/A	Sistema Alfresco	Software
4	Créditos	NGCR-A-01	Anexo1 Requisitos según el tipo de crédito	Datos / Información
5	Créditos	NGCR-A-02	Anexo2 Tarifario de tasas de interés	Datos / Información
6	Créditos	NGCR-A-03	Anexo3 Ficha de productos de crédito	Datos / Información
7	Créditos	NGCR-A-04	Anexo4 Gestión de crédito	Datos / Información
8	Créditos	NGCR-A-05	Anexo5 Costo por asesoría en constitución y cancelación de garantías reales.	Datos / Información
9	Créditos	N/A	Consulta de Buro de crédito Equifax	Servicios
10	Créditos	N/A	Consulta de información de registro civil	Servicios
11	Créditos	N/A	Consulta de Función judicial	Servicios
12	Créditos	N/A	Copias de documentos personales del socio (matricula).	Datos / Información
13	Créditos	N/A	Rol mecanizado del IESS	Datos / Información
14	Créditos	NG-R-8	Registro 8 Solicitud de crédito	Datos / Información
15	Créditos	NG-R-6	FICHA DE SEGUIMIENTO	Datos / Información
16	Créditos	NG-R-7	UBICACION SATELITAL DE DOMICILIO	Datos / Información
17	Créditos	NG-R-3	ANALISIS Y DESICION DEL COMITE	Datos / Información
18	Créditos	NG-R-1	ACTA DE COMITE CREDITO SIACC	Datos /Información
19	Créditos	NG-R-2	CONTROL DE DOCUMENTOS PARA CREDITOS	Datos / Información
20	Créditos	NG-M01	MANUAL DE CRÉDITOS	Datos / Información
21	Tecnología	N/A	Equipos de computo	Hardware
22	Tecnología	N/A	Impresora	Hardware
23	Tecnología	N/A	Escáner	Hardware
24	Tecnología	N/A	Correo Electrónico	Servicios
25	Tecnología	N/A	Mesa de ayuda ITOP	Servicios
26	Tecnología	N/A	Enlaces de comunicación	Servicios
27	Tecnología	N/A	Equipos de Comunicación	Hardware
28	Tecnología	N/A	Proveedores de Core financiero	Servicios
29	Tecnología	N/A	Central Telefónica	Servicios
30	Tecnología	N/A	Personal de tecnología	Personas
31	Créditos	N/A	Personal del área de crédito	Personas
32	Tecnología	N/A	Servidor BDD Core Financiero	Hardware
33	Tecnología	N/A	Servidor APP Core Financiero	Hardware
34	Tecnología	N/A	Servidor Sistema Siacc	Hardware
35	Tecnología	N/A	Servidor Sistema Alfresco	Hardware

Fuente: Elaboración propia.

Valoración de riesgos de seguridad de la información.

Una vez identificado los activos de información del proceso de otorgamiento de crédito se procedieron a valorar su grado de importancia y criticidad para la institución, para lo cual, se valora la afectación o pérdida que se genera operativamente, económicamente, legales y de

imagen al materializarse una amenaza que afecte a los tres pilares principales de la seguridad de la información como es la disponibilidad, integridad o confidencialidad.

Para tal efecto, se utilizaron los siguientes criterios para realizar la valoración de los activos de información:

Tabla 14. Criterios de valoración de activos de información

NIVEL	*OPERATIVO (OP)*	*ECONÓMICO (EC)*	*IMAGEN (IM)*	*LEGAL (LE)*	*COLOR DEL VALOR ASOCIADO*
Muy Bajo (0)	No hay interrupción de las operaciones	Impacto que reduzca el patrimonio en un valor inferior o igual al 0,2%	No afecta las relaciones con los clientes.	Observaciones que no generan sanciones económicas y/o administrativas.	0
Bajo (1)	Interrupción de las operaciones por menos de 12 horas.	Impacto que reduzca el patrimonio en un rango superior a 0,2% y menor o igual al 0,4%	Existen reclamos por parte de los clientes pero no se afecta la continuidad de la relación.	Observaciones que posiblemente generen sanciones administrativas.	1
Medio (2)	Interrupción de las operaciones por mas de 12 horas hasta 24 horas.	Impacto que reduzca el patrimonio en un rango superior al 0,4% y menor o igual al 0,6%	Reclamos de clientes que requieren de un plan de acción a corto plazo y podrían afectar la continuidad de la relación.	Glosas establecidas que podrían generar sanciones económicas y ameritan un plan de acción.	2
	Retrasos en las labores de las áreas y/o en la respuesta a los entes reguladores por ausencia de información.				
Alto (3)	Interrupción de las operaciones por 2 a 4 días.	Impacto que reduzca el patrimonio en un rango superior al 0,6% y menor o igual al 0,8%	Impacto que afecte la imagen de la organización en el mercado.	Sanciones por parte de los entes reguladores.	3
	Pérdida de información crítica de la organización o de terceros que no se pueda recuperar fácilmente.				
Muy Alto (4)	Interrupción de las operaciones por más de 5 días.	Impacto que reduzca el patrimonio técnico en un rango superior al 0,8% y menor o igual al 1%	Impacto que genera una imagen negativa en el mercado.	Intervención por parte de lo entes reguladores por incumplimientos legales y/o contractuales.	4
	Pérdida de información crítica de la organización o de terceros que no se pueda recuperar.		Pérdida significativa de clientes.	Suspensión de actividades.	
			Incremento en el número de reclamos formulados por los clientes.	Condenas por procesos provenientes dela organización.	

Fuente: Modificado a partir de la recomendación de (ISO, 2018).

De igual forma a continuación se detalla los criterios de clasificación de información:

Tabla 15. Criterios de Clasificación de Información

Pilares de seguridad	Clasificación	Descripción
Confidencialidad	**PÚBLIC@**	Información que podría ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la institución sin que esto conlleve un impacto negativo de ninguna índole.
	USO INTERNO	Información dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma.
	RESTRINGIDA	Información que por su contenido sólo interesa a quienes va dirigida y cuya divulgación no autorizada podría ocasionar perjuicios a determinada agrupación o persona.
	CONFIDENCIAL	Información que por su contenido sólo interesa a quienes va dirigida y cuya divulgación no autorizada podría ocasionar perjuicios a determinada institución, agrupación o persona.
Integridad	**INTEGRIDAD ALTA**	Información cuya pérdida de exactitud y completitud podría llevar a cabo un impacto negativo de índole legal a cualquier nivel, de pérdida económica o de imagen de la organización o afectar la operación de varios de sus procesos.
	INTEGRIDAD BAJA	Información cuya pérdida de exactitud y completitud no conlleva a impactos significativos de ninguna índole para la organización.
Disponibilidad	**DISPONIBILIDAD ALTA**	La no disponibilidad de la información por más de 24 horas, podría conllevar un impacto negativo de índole legal, operativa, económica o de pérdida de imagen que afecta a todos los procesos de la organización.
	DISPONIBILIDAD BAJA	La no disponibilidad de la información por más de 24 horas, no conlleva a impactos significativos de ninguna índole para la organización.

Fuente: Modificado a partir de la recomendación de ISO27005.

Tabla 16. Valoración y Clasificación de información.

								Confidencialidad					Valoración	Clasificación		
Id	Área / Dependencia	Codigo	Nombre del activo de información.	Tipo	Origen	Propietario/Responsable	Custodio del Activo	Estado de la información	OP	EC	IM	LE	Total		Confidencialidad	Integridad	Disponibilidad
1	Tecnología	N/A	Sistema Core Financiero	Software	INTERNA	SoftwareHouse	Telconet	DIGITAL	Bajo	Bajo	Alto	Alto	Alto	ALTO	RESTRINGIDA	IA	DA
2	Tecnología	N/A	Sistema SiaCC	Software	INTERNA	Tecnología	Telconet	DIGITAL	Bajo	Muy ba	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
3	Tecnología	N/A	Sistema Alfresco	Software	INTERNA	Tecnología	Telconet	DIGITAL	Bajo	Muy ba	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
4	Créditos	NGCR-A-01	Anexo1 Requisitos según el tipo de crédito	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Bajo	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
5	Créditos	NGCR-A-02	Anexo2 Tarifario de tasas de interés	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Bajo	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
6	Créditos	NGCR-A-03	Anexo3 Ficha de productos de crédito	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Bajo	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
7	Créditos	NGCR-A-04	Anexo4 Gestión de crédito	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Bajo	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
8	Créditos	NGCR-A-05	Anexo5 Costo por asesoría en constitución y cancelación de garantías reales.	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Bajo	Medio	Bajo	Medio	MEDIO	USO INTERNO	IB	DB
9	Créditos	N/A	Consulta de Buro de crédito Equifax	Servicios	EXTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
10	Créditos	N/A	Consulta de información de registro civil	Servicios	EXTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
11	Créditos	N/A	Consulta de Función judicial	Servicios	EXTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
12	Créditos	N/A	Copias de documentos personales del socio (matricula).	Datos / Información	EXTERNA	Socio	Archivo de credito	FISICO Y DIGITAL	Alto	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
13	Créditos	N/A	Rol mecanizado del IESS	Datos / Información	EXTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Alto	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
14	Créditos	NG-R-8	Registro 8 Solicitud de crédito	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	ALTO	USO INTERNO	IB	DA
15	Créditos	NG-R-6	FICHA DE SEGUIMIENTO	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
16	Créditos	NG-R-7	UBICACION SATELITAL DE DOMICILIO	Datos / Información	INTERNA	Negocios	Archivo de credito	DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
17	Créditos	NG-R-3	ANALISIS Y DESICION DEL COMITE	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Alto	Medio	Alto	Medio	Alto	ALTO	RESTRINGIDA	IA	DB
18	Créditos	NG-R-1	ACTA DE COMITE CREDITO SIACC	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO Y DIGITAL	Alto	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
19	Créditos	NG-R-2	CONTROL DE DOCUMENTOS PARA CREDITOS	Datos / Información	INTERNA	Negocios	Archivo de credito	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
20	Créditos	NG-M-01	MANUAL DE CRÉDITOS	Datos / Información	INTERNA	Negocios	Secretaria de Gerencia	FISICO Y DIGITAL	Alto	Medio	Bajo	Alto	Alto	ALTO	RESTRINGIDA	IA	DA
21	Tecnología	N/A	Equipos de computo	Hardware	EXTERNA	Tecnología	Personal Autorizado	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
22	Tecnología	N/A	Impresora	Hardware	EXTERNA	Tecnología	Personal Autorizado	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
23	Tecnología	N/A	Escáner	Hardware	EXTERNA	Tecnología	Personal Autorizado	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
24	Tecnología	N/A	Correo Electrónico	Servicios	EXTERNA	Tecnología	Smarth Help	DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
25	Tecnología	N/A	Mesa de ayuda ITOP	Servicios	EXTERNA	Tecnología	Ddlinux	DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
26	Tecnología	N/A	Enlaces de comunicación	Servicios	EXTERNA	Tecnología	Telconet, CNT, Claro	DIGITAL	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
27	Tecnología	N/A	Equipos de Comunicación	Hardware	EXTERNA	Tecnología	Tecología	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
28	Tecnología	N/A	Proveedores de Core financiero	Servicios	EXTERNA	SoftwareHouse	SoftwareHouse	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
29	Tecnología	N/A	Central Telefónica	Servicios	EXTERNA	Tecnología	Agencias de institució	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
30	Tecnología	N/A	Personal de tecnología	Personas	EXTERNA	Tecnología	Gerencia General	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
31	Créditos	N/A	Personal del área de crédito	Personas	EXTERNA	Negocios	Agencias de institució	FISICO	Medio	Medio	Medio	Muy bajo	Medio	MEDIO	USO INTERNO	IB	DB
32	Tecnología	N/A	Servidor BDD Core Financiero	Hardware	EXTERNA	Tecnología	Telconet	DIGITAL	Bajo	Medio	Medio	Alto	Alto	ALTO	RESTRINGIDA	IA	DA
33	Tecnología	N/A	Servidor APP Core Financiero	Hardware	EXTERNA	Tecnología	Telconet	DIGITAL	Bajo	Medio	Medio	Alto	Alto	ALTO	RESTRINGIDA	IA	DA
34	Tecnología	N/A	Servidor Sistema Siacc	Hardware	EXTERNA	Tecnología	Telconet	DIGITAL	Bajo	Medio	Medio	Medio	Medio	ALTO	USO INTERNO	IB	DA
35	Tecnología	N/A	Servidor Sistema Alfresco	Hardware	EXTERNA	Tecnología	Telconet	DIGITAL	Bajo	Medio	Medio	Medio	Medio	ALTO	USO INTERNO	IB	DA

Fuente: Elaboración propia.

Matriz de Identificación de amenazas

Antes de identificar las amenazas de los activos de información se hace referencia a los Anexos C y D de la ISO 27005, donde se muestra los ejemplos de amenazas para poder identificar adecuadamente.

Tabla 17. Anexo C Ejemplo de amenazas típicas.

Tipo	Amenazas	Origen
Compromiso de información	Interceptación de señales de interferencias comprometidas	D
	Espionaje remoto	D
	Escucha secreta	D
	Robo de medios o documentos	D
	Robo de equipos	D
	Recuperación de medios reciclados o descartados	D
	Divulgación	A, D
	Datos de fuentes poco fiables	A, D
	Manipulación (tampering) con hardware	D
	Manipulación (tampering) con software	A, D
	Detección de posición	D
Fallas técnicas	Falla de equipo	A
	Mal funcionamiento de equipo	A
	Saturación de sistema de información	A, D
	Mal funcionamiento de software	A
	Brecha/fisura de mantenimiento de sistema de información	A, D
Acciones no autorizadas	Uso no autorizado de equipo	D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Corrupción de datos	D
	Procesamiento ilegal de datos	D
Compromiso de funciones	Error en uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Brecha de disponibilidad de personal	A, D, E

Fuente: Tomado a partir de la (ISO, 2018), donde A (accidental factor humano), D (acción deliberada) y E (ambiental).

Tabla 18. Fuente de Amenaza de Humana

Fuente de amenaza	Motivación	Acciones de amenaza
Hacker, cracker	Desafío Ego Rebelión Estatus Dinero	-Hacking -Ingeniería social - Intrusión de Sistema, irrupciones -Acceso no autorizado a sistema
Delito informático	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de datos	-Delito informático (por ejemplo, acoso cibernético) -Acto fraudulento (por ejemplo, repetición, personificación, interceptación) -Soborno de información -Engaño -Intrusión de sistemas
Terrorista	Chantaje Destrucción Explotación Venganza Ganancia política Cobertura mediática	-Bomba/Terrorismo -Guerra de información -Ataque de sistema (por ejemplo, negación distribuida de servicio) -Penetración de sistema -Manipulación (tampering) de sistema
Espionaje industrial (Inteligencia, compañías, gobiernos extranjeros, otros intereses del gobierno)	Ventaja competitiva Espionaje económico	-Ventaja de Defensa -Ventaja Política -Explotación económica -Robo de información -Intrusión en privacidad personal -Ingeniería social -Penetración de sistema -Acceso no autorizado al sistema (acceso a información clasificada, propietaria, y/o relacionada con tecnología)
Internos (empleados pobremente entrenados, descontentos, maliciosos, negligentes, deshonestos, o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (Por ejemplo, error de entrada de datos, error de programación)	-Asalto a un empleado -Chantaje -Mirada a información propietaria -Abuso de computadora -Fraude y robo -Soborno de información -Entrada de datos falsificados, corruptos -Interceptación -Código malicioso (Por ejemplo, virus, bomba lógica, caballo de Troya) -Venta de información personal -Errores de sistema -Intrusión de sistema -Sabotaje de sistema -Acceso no autorizado a sistema

Fuente: Tomado a partir de la (ISO, 2018)

Tabla 19. Ejemplo de principales Vulnerabilidades.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de esquemas periódicos de reemplazo	Destrucción de equipo o medios
	Susceptibilidad a humedad, Polvo, corrosión,	Polvo, suciedad, congelamiento
	Sensibilidad a radiación electromagnética	Radiación electromagnética
	Falta de control eficiente de cambio de configuración	Error en uso
	Susceptibilidad a variaciones de voltaje	Pérdida de suministro de voltaje
	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
	Almacenamiento no protegido	Robo de medios o documentos
	Falta de cuidado en eliminación	Robo de medios o documentos
	Copiado no controlado	Robo de medios o documentos
Software	Falta o insuficiente prueba de software	Abuso de derechos
	Fallas bien conocidas en el software	Abuso de derechos
	No se cierra la sesión si se abana la estación de trabajo	Abuso de derechos
	Eliminación o reutilización de medios de almacenamiento sin borrado apropiado	Abuso de derechos
	Falta de seguimiento de auditoría	Abuso de derechos
	Incorrecta asignación de derechos de acceso	Abuso de derechos
	Software ampliamente distribuido	Corrupción de datos
	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Corrupción de datos
	Complicada interface de usuario	Error en uso
	Falta de documentación	Error en uso
	Establecer parámetros incorrectos	Error en uso
	Fechas incorrectas	Error en uso
	Falta de mecanismos de identificación y autenticación como autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas no protegidas	Falsificación de derechos
	Manejo / pobre de contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento de Software
	Especificaciones poco claras o incompletas para desarrolladores	Mal funcionamiento de Software

	Falta de control de cambio efectivo	Mal funcionamiento de software
	Descarga y uso no controlado de software	Manipulación (tampering) con software
	Falta de copias de respaldo	Manipulación (tampering) con software
	Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos
	Falla en producir reportes de gestión	Uso no autorizado de equipos
Red	Falta de prueba de envío o recepción de un mensaje	Negación de acción
	Líneas de comunicación desprotegidas	Escucha (Eavesdropping)
	Tráfico sensible desprotegido	Escucha (Eavesdropping)
	Pobre conjunto de cableado	Falla en el equipo de telecomunicaciones
	Punto único de falla	Falla en el equipo de telecomunicaciones
	Falta de identificación y autenticación del remitente y el receptor	Falsificación de derechos
	Inseguridad en la arquitectura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Inadecuada gestión de red (Resiliencia de ruteo)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado de equipos
Personal	Ausencia de personal	Brecha de disponibilidad de personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipamiento o medios
	Entrenamiento insuficiente en seguridad	Error en uso
	Uso incorrecto de software y hardware	Error en uso
	Falta de conciencia de seguridad	Error en uso
	Falta de mecanismos de seguimiento	Procesamiento ilegal de datos
	Trabajo no supervisado por personal externo o de limpieza	Robo de medios o documentos
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	Uso no autorizado de equipamiento
Local	Uso inadecuado o descuidado de control de acceso físico a edificios y recintos	Destrucción de equipamiento o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red de energía inestable	Pérdida de suministro de energía

	Falta de protección física del edificio, puertas y ventanas	Robo de equipamiento
	Falta de procedimiento formal para registro de usuarios y su baja	Abuso de derechos
	Falta de proceso formal para revisión de derechos de acceso (supervisión)	Abuso de derechos
	Falta o insuficientes capítulos (concernientes a seguridad) en contratos con clientes y/o terceros	Abuso de derechos
	Falta de procedimiento de seguimiento de instalaciones de procesamiento de la información	Abuso de derechos
Organización	Falta de auditorías regulares (supervisión)	Abuso de derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de derechos
	Falta de reportes de fallas registrados en bitácoras del administrador y operador	Abuso de derechos
	Respuesta inadecuada de mantenimiento de servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta o insuficiente Acuerdo de Nivel de Servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento de control de cambio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento formal para control de la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para la supervisión de los registros del SGSI	Corrupción de datos
	Falta de proceso formal para autorización de información públicamente disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades por la seguridad de la información	Negación de acciones
	Falta de planes de continuidad	Falla de equipamiento
	Falta de política de uso de e-mail	Error en uso
	Falta de procedimientos para introducir software a sistemas operacionales	Error en uso
	Falta de registros en bitácoras del administrador y operador	Error en uso

	Falta de procedimientos para manejo de información clasificada	Error en uso
	Falta de responsabilidades de seguridad de la información en descripciones de puestos	Error en uso
	Falta o insuficientes estipulaciones (concernientes a seguridad de la información) en contratos con empleados	Procesamiento de datos ilegal
	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Robo de equipamiento
	Falta de política formal sobre uso de computadoras móviles	Robo de equipamiento
	Falta de control de activos fuera de las instalaciones	Robo de equipamiento
	Falta o insuficiente política de escritorio y pantalla limpia	Robo de medios o documentos
	Falta de autorización a las instalaciones de procesamiento de la información	Robo de medios o documentos
	Falta de mecanismos de seguimiento establecidos para brechas de seguridad	Robo de medios o documentos
	Falta de revisiones regulares de gestión	Uso no autorizado de equipamiento
	Falta de procedimientos para reportar debilidades de la seguridad	Uso no autorizado de equipamiento
	Falta de procedimientos de estipulación de cumplimiento con derechos de propiedad intelectual	Uso de software falso o copiado

Fuente: Tomado a partir de la (ISO, 2018).

En la siguiente Tabla se define la escala de riesgo para la clasificación general de riesgo:

Tabla 20. Clasificación general de riesgo.

	Probabilidad del escenario de incidencia	Muy bajo (Muy improbable)	Bajo (Improbable)	Medio (Posible)	Alto (Probable)	Muy alto (Frecuente)
Impacto en el negocio	Muy bajo	0	1	2	3	4
	Bajo	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy alto	4	5	6	7	8

Fuente: Tomado a partir de la (ISO, 2018).

Nivel de riesgo aceptable

- Riesgo Bajo: 0-2;
- Riesgo Medio: 3-5;
- Riesgo Alto: 6-8.

Tabla 21. Identificación de amenazas y vulnerabilidades.

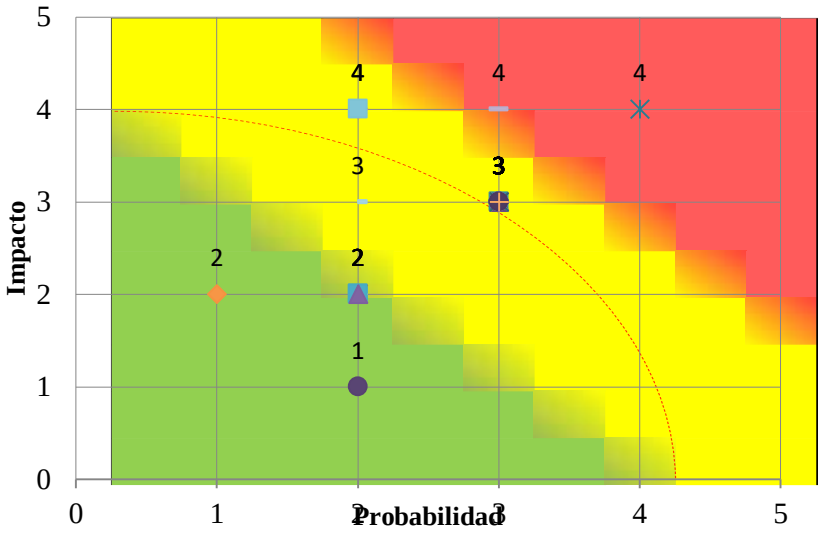
Nombre del activo de información.	Descripción de la amenaza	Vulnerabilidad	Probabilidad	Impacto	Calificación Riesgo (P+I)
Sistema core financiero	Saturación de sistema de información	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	2	4	Alto
Sistema siacc	Saturación de sistema de información	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	2	4	Alto
Sistema alfresco	Saturación de sistema de información	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	2	4	Alto
Anexo1 Requisitos según el tipo de crédito	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Anexo2 Tarifario de tasas de interés	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Anexo3 Ficha de productos de crédito	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Anexo4 Gestión de crédito	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Anexo5 Costo por asesoría en constitución y cancelación de garantías reales.	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Consulta de Buro de crédito Equifax	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Consulta de información de registro civil	Robo de medios o documentos	Copiado no controlado	3	3	Alto

Consulta de Función judicial	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Copias de documentos personales del socio (matricula).	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Rol mecanizado del IESS	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Registro 8 Solicitud de crédito	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Ficha de seguimiento	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Ubicación satelital de domicilio	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Análisis y decisión del comité	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Acta de comité crédito siacc	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Control de documentos para créditos	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Manual de créditos	Robo de medios o documentos	Copiado no controlado	3	3	Alto
Equipos de computo	Robo de equipamiento	Falta de control de activos fuera de las instalaciones	2	4	Alto
Impresora	Brecha en la capacidad de mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento de servicio	2	2	Medio
Escáner	Brecha en la capacidad de mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento de servicio	2	2	Medio
Correo electrónico	Fuga de información	Falta de configuración de parámetros en la consola de administración.	4	4	Alto
Mesa de ayuda ITOP	Brecha en la capacidad de mantenimiento del sistema de información	Falta o insuficiente Acuerdo de Nivel de Servicio	2	1	Medio
Enlaces de comunicación	Brecha en la capacidad de mantenimiento del sistema de información	Falta o insuficiente Acuerdo de Nivel de Servicio	2	2	Medio

Equipos de Comunicación	Falla en el equipo de telecomunicaciones	Punto único de falla	2	3	Medio
Proveedores de Core financiero	Espionaje remoto	Inseguridad en la arquitectura de la red	3	4	Alto
Central telefónica	Brecha en la capacidad de mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento de servicio	1	2	Medio
Personal de tecnología	Brecha de disponibilidad de personal	Ausencia de personal	2	2	Medio
Personal del área de crédito	Divulgación de información	Falta de conciencia de seguridad	2	2	Medio
Servidor bdd core financiero	Procesamiento ilegal de datos	Habilitación de servicios innecesarios	3	3	Alto
Servidor app core financiero	Procesamiento ilegal de datos	Habilitación de servicios innecesarios	3	3	Alto
Servidor sistema siacc	Procesamiento ilegal de datos	Habilitación de servicios innecesarios	3	3	Alto
Servidor sistema alfresco	Procesamiento ilegal de datos	Habilitación de servicios innecesarios	3	3	Alto

Fuente: Elaboración propia.

Figura 12. Mapa de calor riesgo inherente



Fuente: Elaboración propia.

Como se evidencia en el mapa de calor, la tendencia del riesgo de la mayor parte de activos es alto, debido a que no se aplican ningún control.

Tratamiento de Riesgo y definición de controles

Para el tratamiento de riesgo se hace referencia a las opciones de tratamiento de riesgo según la ISO 27005:

- Evasión del Riesgo
- Transferencia de Riesgo
- Aceptación del Riesgo
- Reducción del Riesgo

En esta sección se detalla los controles existentes según la ISO 27002 y planificados para el tratamiento del riesgo según la ISO 27005:

Tabla 22. Tratamiento de riesgo y asignación de controles aplicables.

					Tratamiento del Riesgo				
Id	**Área / Dependencia**	**Codigo**	**Nombre del activo de información.**	**Calificación Riesgo (P+I)**	**Evasión del Riesgo**	**Transferencia de Riesgo**	**Aceptación del Riesgo**	**Reducción del Riesgo**	**Control (generalmente se aplica la ISO 27002)**
1	Tecnología	N/A	Sistema Core Financiero	Alto				x	11.2.1 Emplazamiento y protección de equipos.
2	Tecnología	N/A	Sistema SiaCC	Alto				x	11.2.1 Emplazamiento y protección de equipos.
3	Tecnología	N/A	Sistema Alfresco	Alto				x	11.2.1 Emplazamiento y protección de equipos.
4	Créditos	NGCR-A-01	Anexo1 Requisitos según el tipo de	Alto				x	8.2.3 Manipulación de activos.
5	Créditos	NGCR-A-02	Anexo2 Tarifario de tasas de interés	Alto				x	8.2.3 Manipulación de activos.
6	Créditos	NGCR-A-03	Anexo3 Ficha de productos de crédito	Alto				x	8.2.3 Manipulación de activos.
7	Créditos	NGCR-A-04	Anexo4 Gestión de crédito	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
8	Créditos	NGCR-A-05	Anexo5 Costo por asesoría en constitución y cancelación de garantías	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
9	Créditos	N/A	Consulta de Buro de crédito Equifax	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
10	Créditos	N/A	Consulta de información de registro civil	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
11	Créditos	N/A	Consulta de Función judicial	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
12	Créditos	N/A	Copias de documentos personales del socio (matricula).	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
13	Créditos	N/A	Rol mecanizado del IESS	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
14	Créditos	NG-R-8	Registro 8 Solicitud de crédito	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
15	Créditos	NG-R-6	FICHA DE SEGUIMIENTO	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
16	Créditos	NG-R-7	UBICACION SATELITAL DE DOMICILIO	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
17	Créditos	NG-R-3	ANALISIS Y DESICION DEL COMITE	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
18	Créditos	NG-R-1	ACTA DE COMITE CREDITO SIACC	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
19	Créditos	NG-R-2	CONTROL DE DOCUMENTOS PARA CREDITOS	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
20	Créditos	NG-M-01	MANUAL DE CRÉDITOS	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
21	Tecnología	N/A	Equipos de computo	Alto				x	11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
22	Tecnología	N/A	Impresora	Medio			x		11.2.4 Mantenimiento de los equipos.
23	Tecnología	N/A	Escáner	Medio			x		11.2.4 Mantenimiento de los equipos.
24	Tecnología	N/A	Correo Electrónico	Alto				x	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
25	Tecnología	N/A	Mesa de ayuda ITOP	Medio			x		17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
26	Tecnología	N/A	Enlaces de comunicación	Medio		x			13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
27	Tecnología	N/A	Equipos de Comunicación	Medio		x			13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.
28	Tecnología	N/A	Proveedores de Core financiero	Alto		x			13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.
29	Tecnología	N/A	Central Telefónica	Medio			x		11.2.4 Mantenimiento de los equipos.
30	Tecnología	N/A	Personal de tecnología	Medio			x		9.2.3 Gestión de los derechos de acceso con privilegios especiales.
31	Créditos	N/A	Personal del área de crédito	Medio				x	7.2.2 Concienciación, educación y capacitación en segur. de la informac.
32	Tecnología	N/A	Servidor BDD Core Financiero	Alto				x	11.2.1 Emplazamiento y protección de equipos.
33	Tecnología	N/A	Servidor APP Core Financiero	Alto				x	11.2.1 Emplazamiento y protección de equipos.
34	Tecnología	N/A	Servidor Sistema Siacc	Alto				x	11.2.1 Emplazamiento y protección de equipos.
35	Tecnología	N/A	Servidor Sistema Alfresco	Alto				x	11.2.1 Emplazamiento y protección de equipos.

Fuente: Elaboración propia.

Como se evidencia en la figura anterior, ciertos controles son aplicables para algunos activos, por lo que en el presente documento se considera los siguientes controles aplicables según el Anexo A de la ISO 27002, las mismas que serán considerados en la planificación de seguridad de la información anual, esto con el fin obtener mayor cumplimiento de las normas.

- 7.2.2 Concienciación, educación y capacitación en seguridad de la información.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

Ante los controles considerados en el presente proyecto se ejecuta el control de etiquetado de la información.

Etiquetado de la información

Para el etiquetado de la información se considera el primer pilar de seguridad que consiste en la confidencialidad, se hace referencia a la tabla de Criterios de clasificación de la Información, se considerar que la información es: Público, Uso interno, Restringida o Confidencial.

Para el tema de codificación de la información se coloca el criterio de clasificación seguido del nombre del activo como se muestra en el ejemplo:

- [PUBLICO] Nombre de activo de información.
- [USO INTERNO] Nombre de activo de información.
- [RESTRINGIDA] Nombre de activo de información.
- [CONFIDENCIAL] Nombre de activo de información.

Con referencia a los criterios descritos se elabora el etiquetado de la información del proceso de estudio:

Tabla 23. Etiquetado de Información

Etiquetado de activo
[RESTRINGIDA] Sistema Core Financiero
[USO INTERNO] Sistema SiaCC
[USO INTERNO] Sistema Alfresco
[USO INTERNO]NGCR-A-01 Anexo1 Requisitos según el tipo de crédito
[USO INTERNO]NGCR-A-02 Anexo2 Tarifario de tasas de interés
[USO INTERNO]NGCR-A-03 Anexo3 Ficha de productos de crédito
[USO INTERNO]NGCR-A-04 Anexo4 Gestión de crédito
[USO INTERNO]NGCR-A-05 Anexo5 Costo por asesoría en constitución y cancelación de garantías reales.
[USO INTERNO] Consulta de Buro de crédito Equifax
[USO INTERNO] Consulta de información de registro civil
[USO INTERNO] Consulta de Función judicial
[USO INTERNO] Copias de documentos personales del socio (matricula).
[USO INTERNO] Rol mecanizado del IESS
[USO INTERNO]NG-R-8 Registro 8 Solicitud de crédito
[USO INTERNO]NG-R-6 FICHA DE SEGUIMIENTO
[USO INTERNO]NG-R-7 UBICACION SATELITAL DE DOMICILIO
[RESTRINGIDA]NG-R-3 ANALISIS Y DESICION DEL COMITE
[USO INTERNO]NG-R-1 ACTA DE COMITE CREDITO SIACC
[USO INTERNO]NG-R-2 CONTROL DE DOCUMENTOS PARA CREDITOS
[RESTRINGIDA]NG-M-01 MANUAL DE CRÉDITOS
[USO INTERNO] Equipos de computo
[USO INTERNO] Impresora
[USO INTERNO] Escáner
[USO INTERNO] Correo Electrónico
[USO INTERNO] Mesa de ayuda ITOP
[USO INTERNO] Enlaces de comunicación
[USO INTERNO] Equipos de Comunicación
[USO INTERNO] Proveedores de Core financiero
[USO INTERNO] Central Telefónica
[USO INTERNO] Personal de tecnología
[USO INTERNO] Personal del área de crédito
[RESTRINGIDA] Servidor BDD Core Financiero
[RESTRINGIDA] Servidor APP Core Financiero
[USO INTERNO] Servidor Sistema Siacc
[USO INTERNO] Servidor Sistema Alfresco

Fuente: Elaboración propia.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Evaluación final del SGSI

En la presente fase se realiza el diagnóstico final del SGSI que permite demostrar el resultado posterior a la aplicación el modelo planteado.

A continuación, se presenta la entrevista aplicada al Oficial de Seguridad de la Información de la Cooperativa de Ahorro y Crédito Ambato Ltda., esto con referencia a las cláusulas principales del SGSI y el test de cumplimiento normativo ISO 27001 según el criterio de evaluación de la Tabla de Parámetros de evaluación del SGSI.

Tabla 24. Evaluación final del SGSI

CLÁUSULA	PREGUNTAS APLICADAS	NC	CP	CS	Observación
4	**La Organización y su Contexto**	**0**	**1**	**7**	
4.1	**Entende la Organización y su contexto**	**0**	**0**	**3**	Se defina el contexto de la organización, alcance, partes interesadas del SGSI.
1.-	¿Están identificados los objetivos del SGSI Sistema de Gestión de la Seguridad de la Información?			X	
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?			X	
3.-	¿Se han identificado como las partes internas y externas podrían suponer amenazas o riesgos para la seguridad de la Información?			X	
4.2	**Expectativas de las partes interesadas**	**0**	**0**	**3**	
1.-	¿Se han identificado las partes interesadas?			X	
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?			X	
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?			X	
4.3	**Alcance del SGSI**	**0**	**0**	**1**	
1.-	¿Se ha determinado el alcance del SGSI y se conserva información documentada?			X	
4.4	**SGSI Sistema de Gestión de la Seguridad de la información**	**0**	**1**	**0**	
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considera oportunidades de mejora?		X		
		0	**3**	**6**	
5.1	**Liderazgo y compromiso**	**0**	**2**	**1**	

1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?			X	Se mantiene un Comité de Seguridad de la Información.
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		X		
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		X		
5.2	**Política de la Seguridad de la Información**	**0**	**1**	**3**	
1.-	¿Se ha definido una Política de la Seguridad de la Información?			X	Se mantiene un manual de políticas de seguridad de la información.
2.-	¿Se ha establecido un marco que permita el establecimiento de objetivos?			X	
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?			X	
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		X		
5.3	**Roles y Responsabilidades**	**0**	**0**	**2**	
1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?			X	Se mantiene definido los roles y responsabilidades de seguridad de la información en el manual de cargos y perfiles de talento humano.
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?			X	
6	**Planificación**	**0**	**4**	**4**	
6.1	**Tratamiento de Riesgos y Oportunidades**	**0**	**2**	**3**	
1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?		X		Se levanta la metodología para el riesgo de seguridad de la información según la norma internacional iso27005
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?			X	
3.-	¿Se ha definido un proceso de tratamiento de riesgos?			X	
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?			X	
5.-	¿Se mantiene información documentada de los puntos anteriores?		X		
6.2	**Planificación para consecución de objetivos**	**0**	**2**	**1**	
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?		X		Se encuentra definido en el plan estratégico de la entidad.
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		X		
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización tene en cuenta las funciones principales dentro de la Organización?			X	

		1	**6**	**3**	
7.1	**Recursos**	**0**	**1**	**0**	
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?		X		Se contempla en el presupuesto anual.
7.2	**Competencia**	**1**	**0**	**1**	
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	X			Se emite mensualmente consejos de seguridad pero no se evalúa.
2.-	¿Se mantiene información actualizada sobre la competencia del personal?			X	
7.3	**Concienciación**	**0**	**0**	**2**	
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?			X	Anualmente se realiza la concientización de todo el personal de la entidad.
2.-	¿Existe conciencia de los daños que se podrían producir de no seguir las pautas de la Seguridad de la Información?			X	
7.4	**Comunicación**	**0**	**2**	**0**	
1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		X		Las políticas se dan a conocer mediante correo electrónico e intranet.
2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		X		
7.5	**Información Documentada**	**0**	**3**	**0**	
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluye? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluye registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)		X		Se mantiene documentado como buenas prácticas los manuales, procedimientos, registros y documentos externos alineados a la norma, sin embargo es necesario alinear estrictamente.
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección		X		
3.-	¿Se controlan los documentos de origen externo?		X		
		2	**2**	**4**	
8.1	**Control Operacional**	**2**	**1**	**1**	
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?		X		Se levanta la metodología para el riesgo de seguridad de la información según la norma internacional iso27005
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?			X	
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?	X			

4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?	X			
8.2	**Análisis de riesgos de la Seguridad de la Información**	**0**	**1**	**0**	
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia		X		Se levanta la metodología para el riesgo de seguridad de la información según la norma internacional iso27005
8.3	**Tratamiento de riesgos de la Seguridad de la Información**	**0**	**0**	**3**	
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados			X	En la metodología de riesgo se define el tratamiento de riesgo.
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justifica su aplicación?			X	
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?			X	
		7	**0**	**0**	
9.1	**Seguimiento y medición**	**2**	**0**	**0**	Como aún no se cuenta con el SGSI no se podría realizar el seguimiento correspondiente.
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información tiene en cuenta los controles para la seguridad de la información?	X			
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?	X			
9.2	**Auditorías Internas**	**3**	**0**	**0**	
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	X			
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	X			
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	X			
9.3	**Informe de Revisión por la Dirección**	**2**	**0**	**0**	
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	X			
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?	X			
10	**Mejora**	**3**	**0**	**0**	
10.1	**No Conformidades y acciones correctivas**	**2**	**0**	**0**	

1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	X			Como aún no se cuenta con el SGSI no se podría realizar el seguimiento correspondiente.
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	X			
10.2	**Mejora continua**	**1**	**0**	**0**	
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identifica las oportunidades de mejora?	X			

Fuente: Modificado a partir de la (MINTIC, 2016).

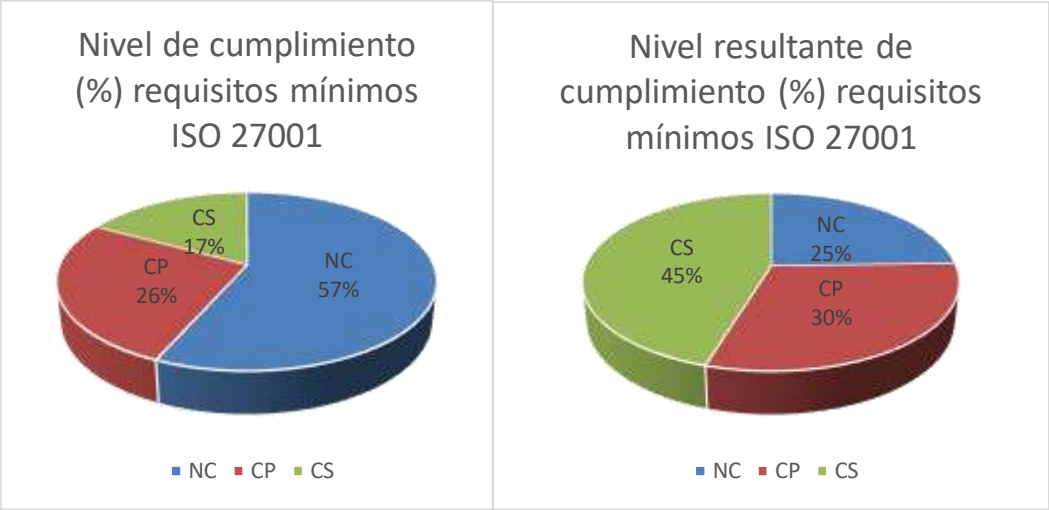
De acuerdo con la entrevista realizada referente a cada uno de las clausulas mínimas y obligatorias del numeral 4 al 10 de la norma ISO 27001:2013, a continuación, en la siguiente Tabla se presenta el resumen final del cumplimiento:

Tabla 25 Reevaluación de los puntos del SGSI.

DIAGNOSTICO INICIAL DEL SGSI					
CLÁUSULA	**DESCRIPCIÓN**	**NC**	**CP**	**CS**	**TOTAL PREGUNTAS**
4	La Organización y su Contexto	0	1	7	8
5	Liderazgo	0	3	6	9
6	Planificación	0	4	4	8
7	Soporte	1	6	3	10
8	Operación	2	2	4	8
9	Evaluación del desempeño	7	0	0	7
10	Mejora	3	0	0	3
TOTAL		**13**	**16**	**24**	**53**
		NC	**CP**	**CS**	**TOTAL PREGUNTAS**

Fuente: Elaboración propia.

Figura 13. Comparativo del nivel de cumplimiento resultante con respecto a los puntos principales del SGSI 27001.



Fuente: Elaboración propia.

Una vez implementado el proyecto y evaluado nuevamente los requisitos del estándar ISO 27001, se evidencia que en comparación al estado anterior se obtuvo un cumplimiento satisfactorio del 45% que es considerable, con respecto al cumplimiento parcial de un 30% , debido a que el porcentaje de incumplimiento se redujo del 57% al 25%.

3.2. Evaluación final del Anexo A de la Norma NTC-ISO-IEC 27001:2013

Con el fin de realizar el diagnóstico posterior a la aplicación del modelo de gestión de seguridad de la información propuesto, se realiza una reevaluación de los 114 objetivos de control y controles que se obtienen directamente del Anexo A de la norma ISO 27001:2013, en los numerales 5 al 18. Esta validación se lo realiza con los mismos criterios de evaluación inicial.

Tabla 26. Evaluación final del Anexo A ISO 27001:2013.

	ANEXO A ISO 27001	NC	CP	CS	Observación
A5	**Políticas de Seguridad de la Información**	**0**	**0**	**2**	
A5.1	**Dirección de gestión para la seguridad de la información**	**0**	**0**	**2**	
1.-	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?			X	Actualmente la entidad su cuenta con un manual de seguridad de la información en la cual, se detallan las políticas internas.
2.-	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?			X	
A6	**Organización de la Seguridad de la Información**	**0**	**2**	**5**	
A6.1	Asignación de responsabilidades para la seguridad de la información.	**0**	**1**	**4**	
1.-	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?			X	Las responsabilidades se lo detallan en el manual de cargos y perfiles de talento humano, al igual que el oficial de seguridad de la información fue designado por el consejo de administración.
2.-	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?			X	
3.-	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		X		
4.-	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?			X	
5.-	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?			X	
A6.2	**Dispositivos Móviles y Teletrabajo**	**0**	**1**	**1**	
1.-	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?			X	La entidad cuenta con un procedimiento para el teletrabajo.
2.-	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?		X		
A7	**Seguridad en los Recursos Humanos**	**0**	**2**	**5**	
A7.1	**Antes de contratar a un empleado**	**0**	**0**	**2**	
1.-	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación -Referencias			X	Esta actividad se detalla en el manual de talento humano.
2.-	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?			X	
A7.2	**Durante el contrato**	**0**	**2**	**1**	
1.-	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?			X	

2.-	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		X		Se ejecuta la sensibilización pero no se cuenta con un proceso.
3.-	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		X		Se lo comunica mediante correo sin embargo no hay un plan.
A7.3	**Terminación del contrato**	**0**	**0**	**2**	
1.-	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?			X	Esta actividad se define en el manual de talento humano hace referencia al procedimiento de gestión de accesos de seguridad de la información.
2.-	¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?			X	
A8	**Gestión de Activos**	**3**	**2**	**5**	
A8.1	**Responsabilidad sobre los Activos**	**1**	**1**	**2**	
1.-	¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información?			X	Se levanta el inventario de activos de información del proceso crítico identificado.
2.-	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?			X	
3.-	¿Se han establecido normas para el uso de activos en relación a su seguridad?	X			
4.-	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?		X		Se realiza un acta entrega de equipos, sin embargo no hay un procedimiento.
A8.2	**Clasificación de la Información**	**0**	**0**	**3**	
1.-	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?			X	Se ejecuta la clasificación de información según estándares internacionales como la ISO 27001
2.-	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?			X	
3.-	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?			X	
A8.3	**Manipulación de Soportes**	**2**	**1**	**0**	
1.-	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado -Etc.	X			No se cuenta con ningún procedimiento de manipulación de soporte.
2.-	¿Existen procedimientos establecidos para la eliminación de soportes?	X			
Cláusula	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.		X		Seguridad física realiza el control de salida de equipos.
A9	**Control de Acceso**	**2**	**0**	**12**	
A9.1	**Requisitos generales para el control de acceso**	**0**	**0**	**2**	

1.-	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?			X	Se mantiene un procedimiento de control de accesos
2.-	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?			X	
A9.2	**Accesos de Usuario**	**1**	**0**	**5**	
1.-	¿Existen procesos formales de registros de usuarios?			X	Se mantiene un procedimiento de control de accesos
2.-	¿Existen procesos formales para asignación de perfiles de acceso?			X	
3.-	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?			X	
4.-	¿Se ha establecido una política específica para el manejo de información clasificada cono secreta ? en cuanto a: -Autenticación -Compromisos	X			Aun no se cuenta con la clasificación de la información.
5.-	¿Se establecen periodos concretos para renovación de permisos de acceso?			X	Renovación de claves
6.-	¿Existe un proceso definido para la revocación de permisos si se finalice una actividad, puesto de trabajo o cese de contratos?			X	Talento Humano lo mantiene
A9.3	**Responsabilidades de los usuarios**	**0**	**0**	**1**	
1.-	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?			X	Se detalla en el Manual de Seguridad de la Información
A9.4	**Control de acceso a sistemas y aplicaciones**	**1**	**0**	**4**	
1.-	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?			X	Se lo controla mediante el Directorio activo.
2.-	¿Se han implementado procesos de acceso seguro para el inicio de sesión considera limitaciones de intentos de acceso, controla la información en pantalla etc.?			X	
3.-	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?			X	
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?	X			No se controla a los usuarios privilegiados.
5.-	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?			X	Tecnología mantiene un control de cambios.
A10	**Criptografía**	**2**	**0**	**0**	
A10.1	**Control criptográfico**	**2**	**0**	**0**	
1.-	¿Existe una política para el establecimiento de controles criptográficos?	X			No se mantiene ningún procedimiento en tema criptográfico
2.-	¿Existe un control del ciclo de vida de las claves criptográficas?	X			
A11	**Seguridad Física y del entorno**	**1**	**1**	**12**	

A11.1	**Áreas de Seguridad**	**0**	**0**	**5**	
1.-	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?			X	Se detalla en el Manual de Seguridad Física
2.-	¿Existen controles de acceso a personas autorizadas en áreas restringidas?			X	
3.-	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas accesibles a personal externo?			X	
4.-	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?			X	
5.-	¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?			X	
A11.2	**Seguridad de los equipos**	**1**	**1**	**7**	
1.-	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?			X	Se detalla en el Manual de Seguridad Física
2.-	¿Se protegen los equipos contra fallos de suministro de energía?			X	
3.-	¿Existen protecciones para los cableados de energía y de datos?			X	
4.-	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			X	
5.-	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información?		X		
6.-	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?			X	Configuración de antivirus.
7.-	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?	X			No se cuenta con el procedimiento de destrucción de información
8.-	¿Se establecen normas para proteger la información de equipos si los usuarios abanan el puesto de trabajo?			X	Cierre de sesión en 5 min de inactividad
9.-	¿Se establecen reglas de comportamiento para abanos momentáneos o temporales del puesto de trabajo?			X	
A12	**Seguridad en las Operaciones**	**3**	**3**	**10**	
A12.1	**Procedimientos y responsabilidades**	**2**	**0**	**3**	
1.-	¿Se documentan los procedimientos y se establecen responsabilidades?			X	Se detalla en el manual de talento humano
2.-	¿Se controla que la información sobre procedimientos se mantenga actualizada?			X	Mediante la intranet
3.-	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	X			
4.-	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?			X	Monitoreo con zabbix
5.-	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	X			No hay vlans

A12.2	**Protección contra software malicioso**	**0**	**0**	**1**	
	¿Existen sistemas de detección para Software malicioso o malware?			X	Antivirus
A12.3	**Copias de Seguridad**	**0**	**0**	**1**	
1.-	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?			X	Tecnología mantiene un procedimiento
A12.4	**Registros y supervisión**	**1**	**2**	**1**	
1.-	¿Se realiza un registro de eventos? -Intentos de acceso fallidos/exitosos -Desconexiones del sistema -Alertas de fallos Etc.		X		firewall, Waf
2.-	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?		X		Matriz de roles
3.-	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?	X			No hay sistema de control de acceso para administradores.
4.-	¿Existe un control de sincronización de los distintos sistemas?			X	Lo mantiene con el Directorio Activo
A12.5	**Control del Software**	**0**	**1**	**0**	
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?		X		No todos los sistemas mantienen un ambiente de pruebas
A12.6	**Vulnerabilidad Técnica**	**0**	**0**	**2**	
1.-	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?			X	Se maneja con un proveedor anualmente.
2.-	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evita las instalaciones por parte de usuarios finales?			X	Controla con el AD
A12.6	**Auditorias de Sistemas de Información**	**0**	**0**	**2**	
1.-	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?			X	1 vez al año
2.-	¿Se establecen protocolos específicos para desarrollo de auditorías Software considera su impacto en los sistemas?			X	
A13	**Seguridad en las Comunicaciones**	**1**	**3**	**3**	
A13.1	**Seguridad de Redes**	**1**	**2**	**0**	
1.-	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?		X		Se mantiene un Waf, firewall perimetral
2.-	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?		X		
3.-	¿Existe separación o segregación de redes toma en cuenta condiciones de seguridad y clasificación de activos?	X			
A13.2	**Intercambio de Información**	**0**	**1**	**3**	

1.-	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?		X		Manual de Seguridad de la Información
2.-	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?			X	Acuerdos de confidencialidad.
3.-	¿Se establecen normas o criterios de seguridad en mensajería electrónica?			X	Manual de Seguridad de la Información
4.-	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades			X	Acuerdos de confidencialidad.
A14	**Adquisición, desarrollo y mantenimiento de sistemas de información**	**1**	**3**	**10**	
A14.1	**Intercambio de Información**	**0**	**1**	**3**	
1.-	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?			X	En todo proyecto se considera la participación de seguridad de la información
2.-	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?			X	
3.-	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?			X	VPN
4.-	¿Se establecen medidas de protección para transacciones Online?		X		WAF, Firewall aún no se cuenta con una solución antifraude
A14.2	**Seguridad en los procesos de Soporte**	**1**	**2**	**6**	
1.-	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?	X			No existe procedimiento de desarrollo seguro
2.-	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?			X	Tecnología mantiene un procedimiento de control de cambios
3.-	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?			X	
4.-	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?			X	
5.-	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?			X	
6.-	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?		X		
7.-	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?		X		
8.-	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?			X	
9.-	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?			X	
A14.3	**Datos de prueba**	**0**	**0**	**1**	
1.-	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?			X	
A15	**Relación con Proveedores**	**0**	**1**	**4**	
A15.1	**Seguridad en la Relación con Proveedores**	**0**	**1**	**2**	

1.-	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?			X	Se detalla en el procedimiento de gestión de proveedores críticos.
2.-	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?			X	
3.-	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?		X		
A15.1	**Gestión de servicios externos**	**0**	**0**	**2**	
1.-	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?			X	
2.-	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?			X	
A16	**Gestión de incidentes de seguridad de la información**	**7**	**0**	**0**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	**7**	**0**	**0**	
1.-	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	X			Tecnología mantiene un procedimiento de incidentes de tecnología mas no de seguridad de la información
2.-	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?	X			
3.-	¿Se promueve y se ha establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	X			
4.-	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	X			
5.-	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	X			
6.-	¿La información proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?	X			
7.-	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?	X			
A17	**Gestión de la Continuidad del Negocio**	**0**	**1**	**3**	
A17.1	**Continuidad de la seguridad de la información.**	**0**	**1**	**2**	
1.-	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?		X		Plan de continuidad de negocio
2.-	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?			X	
3.-	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?			X	Al menos dos veces al año
A17.2	**Redundancias**	**0**	**0**	**1**	
1.-	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?			X	Se mantiene redundancia de los sistemas críticos.
A18	**Cumplimiento**	**4**	**2**	**2**	
A18.1	**Cumplimiento de los requisitos legales y contractuales.**	**4**	**0**	**1**	
1.-	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su			X	Entes de control aun no cuentan con normas para

	cumplimiento? -LOPD -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad -Ley general de Telecomunicaciones				entidades financieras sin embargo se hace referencias a normas internacionales por buenas prácticas.
2.-	¿Existen procedimientos implementados sobre la propiedad intelectual?	X			
3.-	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	X			
4.-	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	X			
5.-	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	X			
A18.2	**Revisiones de la Seguridad de la Información**	**0**	**2**	**1**	
1.-	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?			X	Se ejecuta mediante Auditorías internas y externas.
2.-	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?		X		
3.-	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?		X		

Fuente: Modificado a partir de la (MINTIC, 2016).

De acuerdo con la entrevista realizada referente al Anexo A de la ISO27001:2013 A5 hasta la A18, a continuación, en la siguiente tabla se presentan los resultados obtenidos:

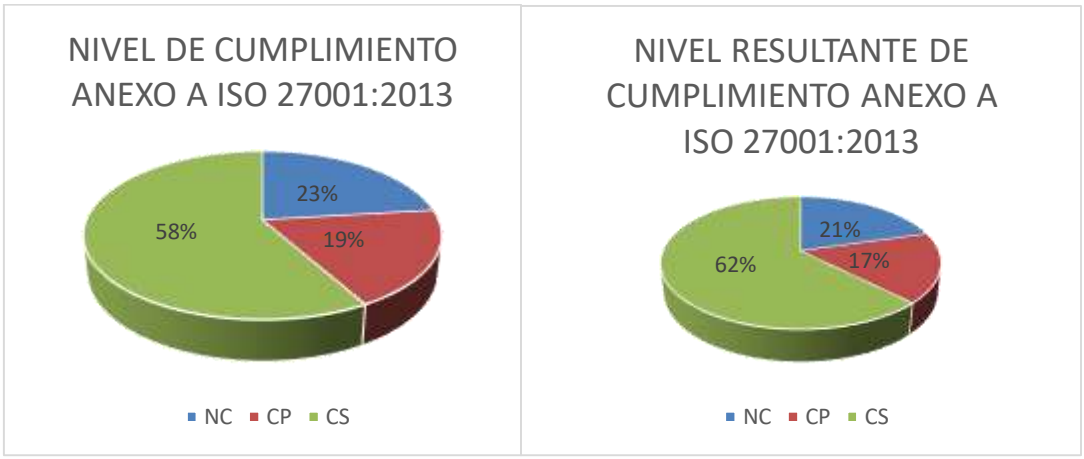
Tabla 27. Resumen resultados Anexo A ISO 27001:2013

Cláusula	ANEXO A ISO 27001	NC	CP	CS	TOTAL PREGUNTAS
A5	Políticas de Seguridad de la Información	0	0	2	2
A6	Organización de la Seguridad de la Información	0	2	5	7
A7	Seguridad en los Recursos Humanos	0	2	5	7
A8	Gestión de Activos	3	2	5	10
A9	Control de Acceso	2	0	12	14
A10	Criptografía	2	0	0	2
A11	Seguridad Física y del entorno	1	1	12	14
A12	Seguridad en las Operaciones	3	3	10	16
A13	Seguridad en las Comunicaciones	1	3	3	7
A14	Adquisición, desarrollo y mantenimiento de sistemas de información	1	3	10	14
A15	Relación con Proveedores	0	1	4	5
A16	Gestión de incidentes de seguridad de la información	7	0	0	7
A17	Gestión de la Continuidad del Negocio	0	1	3	4
A18	Cumplimiento	4	2	2	8
TOTAL		24	20	73	117
		NC	**CP**	**CS**	**TOTAL PREGUNTAS**

Fuente: Elaboración propia.

El comparativo del nivel de cumplimiento y madurez general referente al Anexo A de la ISO27001:2013 es:

Figura 14. Comparativo del nivel de cumplimiento resultante del anexo A de la ISO27001:2013.



Fuente: Elaboración propia.

Con referencia al nivel de cumplimiento inicial del anexo A, se evidencia claramente que en la institución cuenta con ciertos controles aplicados de manera empirica, debido a que no se han realizado ningun analisis de riesgos previos, por ende el cumplimiento resultante incrementa un porcentaje minimo en el cumplimiento. Para obtener mayor cumplimiento en cada uno de los controles, es necesarios que se le de prioridad a los controles identificados según los riesgos de cada activo.

CONCLUSIONES

- El diagnóstico es el proceso más crítico a nivel de seguridad de la información en la organización, en conclusión, la evaluación realizada determina que si bien existen varios procesos que conjuntamente aportan a la entidad financiera, también, existen procesos considerados críticos como lo es el otorgamiento de crédito que contribuyen significativamente al giro del negocio y cumplimiento de los objetivos estratégicos de la Cooperativa de Ahorro y Crédito Ambato Ltda.

- El análisis de las vulnerabilidades de la organización del proceso crítico, incide mayormente, a la gestión de los activos de información, la misma que son vulnerados por procesos ajenos o entes externos a la entidad.

- La norma ISO 27001 es una herramienta efectiva para la gestión adecuada de un sistema de gestión de seguridad de la información, la misma que podría ser aplicada en cualquier organización sin importar a la actividad económica a la que se dedique, además, de ser una norma global y certificable.

- La implementación el modelo de gestión de seguridad de la información en el área de crédito, permite mejorar los tres pilares fundamentales de seguridad como son: confidencialidad, integridad y disponibilidad de la misma, permitiendo así mejorar el aseguramiento de los datos valiosos tanto de la entidad financiera como de los clientes.

RECOMENDACIONES

- Se recomienda, para futuros trabajos aplicar el mismo modelo de gestión de seguridad de la información en todos los procesos del giro de negocio de la entidad financiera.

- Se sugiere, actualizar periódicamente la matriz de inventario y valoración de activos de información, debido a que en los procesos podría haber cambios en el transcurso del tiempo.

- Se sugiere, obtener la certificación de la norma ISO 27001 de todos los procesos del giro del negocio.

- Se recomienda, realizar revisiones periódicas del sistema de gestión de seguridad de la información y sus controles que ayudan a mejorar el manejo de la información dentro de la entidad financiera.

BIBLIOGRAFÍA

Bailón-Lourido, W. A. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. *[Revista]*, 173

COAC AMBATO. (2021). *Manual de Calidad.* Ambato.

COAC AMBATO. (2021). *Mapa de procesos de la entidad.* Obtenido de [Gráfico]: www. cooperativaambato.fin.ec

COAC AMBATO. (2021). *Organigrama Estructural de la entidad.* Obtenido de [Gráfico]: www.cooperativaambato.fin.ec

Dejan Kosutic. (s.f.). *¿Qué es norma ISO 27001?* Recuperado el 26 de 04 de 2022, de https://advisera.com/27001academy/es/que-es-iso-27001/

EditorR. (22 de 02 de 2016). *Software ISO*. (EditorR) Recuperado el 26 de 04 de 2022, de https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cual,es-son-sus-elem ento s-esenciales/

Guzman Silva, C. (2015). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO. *Seguridad de la Información.* INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO, Bogotá.

Hurtado Pérez, A. J., & Robayo Gonzales, O. (2019). DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN -SGSI- PARA LOS PROCESOS CRÍTICOS DE LA COOPERATIVA FEBOR BASADO EN LA NORMA ISO 27001:2013. *Seguridad de la Información.* UNIVERSIDAD PILOTO DE COLOMBIA, Bogotá.

INCIBE. (27 de 06 de 2016). *Sigue el camino del análisis de riesgos.* Recuperado el 02 de 05 de 2022, de https://www.incibe.es/protege-tu-empresa/blog/sigue-camino-analisis-riesgos.

INTEKEL. (3 de Junio de 2019). *Caracteristicas de Seguridad de la Información.* Obtenido de [Gráfico]: www.intekel.com

Intekel. (03 de 06 de 2019). Tu información segura con un Sistema de Gestión de Seguridad de la Información(SGSI). Recuperado el 02 de 04 de 2022, de https://www.intekel. com/blog/tu-informacion-segura-con-un-sgsi/

ISO. (2018). *ISO/IEC 27005:2018. Information Technology - Security Techniques - Information Security Risk Management.*

ISO27000. (s.f.).*Ciclo de mejora continua.*Obtenido de[Gráfico]: Obtenido de https://www.iso 27000.es/sgsi.html

Juan A. Figueroa-Suárez, R. F.-A.-O.-G. (15 de 12 de 2017). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, 190. doi:10.23857/pc.v2i12.420

L. (01 de 10 de 2020). *OSTEC | Segurança digital de resultados*. Recuperado el 28 de 04 de 2022, de Buenas prácticas para gestión de la seguridad de la información: https://os tec.blog/es/generico/iso-27002-buenas-practicas-gsi/

López, A. (14 de 04 de 2022). *SGSI*. Obtenido de https://www.iso27000.es/sgsi.html

Mejía Caguasango, K. (23 de 11 de 2017). Norma de control de las seguridades en el uso de transferencias electrónicas. págs. https://www.seps.gob.ec/wp-content/ uploads/R esolucion-No.-SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.pdf. Obtenido de https://ww w.seps.gob .ec/wp-content/uploads/Resolucion-No.-SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.pdf

MINTEL. (10 de Enero de 2020). *Ciclo de Deming (PDCA).* Obtenido de [Gráfico]: Recuperado de www.gobiernoelectronico.gob.ec

MINTEL. (10 de 02 de 2020). *EGSI.* Obtenido de Esquema Gubernamental de Seguridad de la Informacion: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

MINTIC. (2016). Controles de Seguridad y Privacidad de la Información. *Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia*, 18.

SEPS. (23 de 11 de 2017). NORMA DE CONTROL DE LAS SEGURIDADES EN EL USO DE TRANSFERENCIAS ELECTRÓNICAS. *RESOLUCION No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017- 103.*

SEPS. (31 de 03 de 2021). *Boletin Financiero.*

Velásquez, S. (2018). COMPARATIVA ENTRE LAS METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DEL RIESGO NTC-ISO/IEC 27005 Y MAGERIT. *Metodología de análisis y gestión de riesgo*, 13.

ANEXO

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Octubre-2013