MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIONES

Tesis de grado previo a la obtención del título de magister.

"DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR."

Realizado por:

Ing. José Neptali Molina Alcocer

Director de Proyecto:

MGS. Luis Fabián Hurtado Vargas

Como requisito para la obtención del título de:

MAGISTER EN SEGURIDAD INFORMATICA CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIONES

DECLARACIÓN JURAMENTADA

Yo, JOSE NEPTALI MOLINA ALCOCER, con cédula de identidad # 171645433-3, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; se ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

José Neptali Molina Alcocer

C.C.: 1716454333

LOS PROFESORES INFORMANTES

MSC. CHRISTIAN DAVID PAZMIÑO FLORES

MSC. WALTER EDISON ESTRELLA MOGOLLON

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal examinador

Msc. Christian David Pazmiño Flores

Msc Walter Edison Estrella Mogollon

Quito, 3 de mayo de 2018

DEDICATORIA

Dedico el presente trabajo de investigación a mis padres quienes supieron inculcarme valores y principios que han guiado mi vida. Gracias Padres por estar siempre junto a mí.

A mi Esposa Diana, compañera de toda la vida, con quien he compartido los mejores momentos.

AGRADECIMIENTO

A la Ingeniero Fabián Hurtado Vargas por su acertada dirección de la tesis. Su profesionalismo y entrega fueron determinantes a la hora de conformar este documento.

A los profesores Christian Pazmiño y Edison Estrella, quienes con sus lecturas aportaron una visión diferente e integradora de mi investigación.

A la Universidad Internacional SEK, por su compromiso de formar profesionales íntegros.

TABLA DE CONTENIDO

Resumen..... xii

Palabras claves:..... xii

Abstract..... xiii

Key Word..... xiii

CAPÍTULO I. 1

INTRODUCCIÓN. 1

1.1 EL PROBLEMA DE INVESTIGACIÓN. 1

1.1.1 Planteamiento del Problema. 1

1.1.2 Formulación del Problema. 3

1.1.3 Sistematización del Problema. 4

1.1.4 Objetivo General. 4

1.1.5 Objetivos Específicos 4

1.1.6 Justificación 5

1.2 ESTADO DEL ARTE 6

1.2.2 Adopción de una Perspectiva Teórica 12

1.2.3 Marco Conceptual 13

1.2.4 Hipótesis 14

CAPÍTULO II. 15

MÉTODO 15

2.1 TIPO DE ESTUDIO. 15

2.2 MODALIDAD DE INVESTIGACIÓN. 15

2.3 MÉTODO 15

2.4 POBLACIÓN Y MUESTRA. 16

2.5 SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN. 16

2.6 VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS. 17

2.7 OPERACIONALIZACIÓN DE VARIABLES. 18
2.8 PROCESAMIENTO DE DATOS..... 19
CAPITULO III..... 20
RESULTADOS 20
3.1 DESCRIPCIÓN DE LA INSTITUCIÓN..... 20
3.1.1 Actos inapropiados 20
3.1.2 Gestión de seguridad de la información 21
3.2 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS 23
3.2.1 Análisis de la necesidad..... 23
3.2.2 Análisis de resultados 23
3.2.3 Tabulación de resultados 27
3.2.4. Interpretación de resultados..... 36
3.3 INTRODUCCIÓN 36
3.3.1 Planificación 37
3.3.2 Identificación y Clasificación..... 37
3.4 METODOLOGÍA DE GESTIÓN..... 38
3.4.1 PLANIFICACIÓN 38
3.5 IDENTIFICACIÓN Y CLASIFICACIÓN 41
3.5.1 Identificación 41
3.5.2 Pre clasificación de los activos..... 43
3.5.3 Análisis de Riesgos (Identificación y evaluación del Riesgo) 54
3.6 REVISIÓN Y MONITOREO 67
CAPITULO IV 70
4.1 CONCLUSIONES 70
4.2 RECOMENDACIONES..... 71
Bibliografía 73

ÍNDICE DE TABLAS

Tabla 1: Listado de entrevistas a los responsables del manejo de la información..... 2

Tabla 2: Población y Muestra 16

Tabla 3: Operacionalización de Variables 18

Tabla 4: Procesamiento de datos..... 19

Tabla 5 Matriz de resultados de la entrevista..... 24

Tabla 6: Pregunta 1 cuadro de porcentaje..... 27

Tabla 7: Pregunta 1 cuadro de porcentaje..... 28

Tabla 8: Pregunta 3 cuadro de porcentaje..... 29

Tabla 9: Pregunta 4 cuadro de porcentaje..... 30

Tabla 10: Pregunta 5 cuadro de porcentaje..... 31

Tabla 11: Pregunta 6 cuadro de porcentaje..... 32

Tabla 12: Pregunta 7 cuadro de porcentaje..... 33

Tabla 13: Pregunta 8 cuadro de porcentaje..... 34

Tabla 14: Pregunta 9 cuadro de porcentaje..... 35

Tabla 15 Definiciones nivel valor vs criterios de clasificación 40

Tabla 16 Matriz Levantamiento de activos..... 43

Tabla 17 Matriz de tipos de activos valorando su confidencialidad, integridad y disponibilidad 46

Tabla 18 Clasificación acuerdo a la confidencialidad 47

Tabla 19 Clasificación acuerdo a la Integridad..... 48

Tabla 20 Clasificación acuerdo a la disponibilidad 49

Tabla 21 Matriz para valor de impacto general del activo..... 50

Tabla 22 Valoración de activo 51

Tabla 23 Método de evaluación de amenazas..... 54

Tabla 24 Descripción de amenazas 55

Tabla 25 Método de evaluación de vulnerabilidades 58

Tabla 26 Descripción de vulnerabilidades 59

Tabla 27 Descripción nivel de riesgo 64

Tabla 28 Vulnerabilidad Residual 67

ÍNDICE DE FIGURAS

Figura 1. Sistema de actividades para la dirección de tecnologías de la información 6

Figura 2 Gráfico pregunta 1..... 27

Figura 3 Grafico pregunta 2..... 28

Figura 4: Gráfico pregunta 3 29

Figura 5: Gráfico pregunta 4..... 30

Figura 6: Gráfico pregunta 5 31

Figura: 7: Gráfico pregunta 6 32

Figura 8: Gráfico pregunta 7..... 33

Figura 9: Gráfico pregunta 8..... 34

Ilustración 10: Gráfico pregunta 9 35

Figura 11 Esquema de Planificación 38

Figura 12 Pasos para la identificación y clasificación..... 41

Figura 13 Elementos de la Identificación 42

Figura 14 Caracterización de los activos 43

Figura 15 Activos esenciales 44

Figura 16 Determinación nivel de riesgo..... 63

Figura 17 Seguimiento y Control 69

Resumen

En el presente proyecto se pretende examinar los procesos de cambio organizacional necesarios para una adecuada incorporación de gestión de riesgos y controles en la seguridad de la información mediante el "DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR" con el fin de reducir considerablemente las inconsistencias en la gestión de la información de la institución encargada de regular cooperativas y asociaciones, partiendo de un análisis comparativo entre diferentes normas y metodologías como son ISO 27001:2013 y MAGERIT, los cuales brindan un procedimiento frecuente para examinar los riesgos procedentes del empleo de medios tecnológicos de la información y comunicaciones. Una vez identificado el riesgo del activo se especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la información en el contexto de la organización, también se tomó como referencia la ISO 27002 considerado como una buena práctica para desarrollar y mantener normas de seguridad en una organización y así mejorar la confiabilidad de la seguridad de la información. De los resultados obtenidos en la investigación se desarrolló una política para la clasificación y etiquetado de la información la que se implementó en dos procesos claves dentro de la SUPER INTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Palabras claves:

Política, Clasificación, Etiquetado, Vulnerabilidad de la información, Disponibilidad de la información, Integridad de la información, Confiabilidad de la información, Activos de información, Riesgo

Abstract

This project aims wants to examine the required organizational processes changes for an adequate incorporation of risk management and controls in information security through the "DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR", in order to reduce inconsistences in the information management of the institution that is responsible of regulating cooperatives and associations, in based on a comparative analysis between different standards and methodologies such as ISO 27001: 2013 and MAGERIT, which provide a frequent procedure to examine to examine the risks arising from the use technology resources of information and communications. Once the risk of the asset was identified, the requirements was specified for establish, implement, maintain and continuously improve of an information management system according of the organization, also was taken the ISO 27002 standards like a reference, because it is considered a good practice to develop and maintain security standards in an organization and with this improve the confidentially of information security. From the results obtained in the research was develop a policy for the information classification and labeling and it was implemented within two key processes inside the SUPER INTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA.

Key Word

Policy, classification, labelling, information vulnerability, information availability, information integrity, information reliability, information assets, risk

CAPÍTULO I.

INTRODUCCIÓN.

1.1 EL PROBLEMA DE INVESTIGACIÓN.

1.1.1 Planteamiento del Problema.

Las instituciones públicas en el Ecuador generan una gran cantidad de información, basada en la producción de documentos físicos y electrónicos que son considerados como activos. Después de realizar las entrevistas a los responsables directos en la seguridad de la información se puede mencionar que existen interrupción de servicios, manipulación en la información, fugas, filtraciones de datos confidenciales y desorganización de documentación digital e impresa.

Diagnóstico del Problema.

La institución encargada de regular cooperativas y asociaciones gestiona diariamente la información física y digital. La información digital por su diversificación tiene una estructura compuesta. Esta puede ser procesada de dos formas; la primera, a través de software dispuestos en la plataforma web, la cual a su vez puede ser impresa y convertirse en información física; la segunda, mediante la utilización de dispositivos digitales como memorias extraíbles, base de datos y servidores en general.

Después de analizar las causas del problema con las autoridades competentes y personal responsable en el manejo de la información dentro de la institución, se puede determinar que existe vulnerabilidad; el cual se divide en tres aspectos: disponibilidad, integridad y confidencialidad.

A continuación, se detallan los síntomas en la primera etapa de análisis del problema:

- La carencia de la sistematización de la información reduce la productividad de la institución; generando caídas de servicio y prolongado tiempo de respuesta en la atención al público.
- La gestión de la institución se ve comprometida por una carencia en el control de acceso o que deriva en casos de información incorrecta y/o incompleta.

- La carencia en la jerarquización de la información en la institución; además del incumplimiento tanto de las leyes como de las reformas; trae como consecuencia la pérdida, alteración y divulgación no autorizada de la información.

Tabla 1: Listado de entrevistas a los responsables del manejo de la información.

Manejo de Reuniones y Entrevistas		
Fechas	Detalle	Conclusión
25/08/2017	Se respondió el oficio entregado para auspicio	Se obtiene carta de auspicio
29/08/2017	Presentación con el equipo de la dirección	Conocer el equipo de trabajo
01/09/2017	Reunión con el Director de Riesgos	Detección de riesgos en el manejo de la información.
05/09/2017	Entrevista con director de seguridad de la información en la que se trató sobre las necesidades que tiene la SEPS	Detección de vulnerabilidades
14/09/2017	Reunión con la experta en normativas donde se trató el manejo de la información actualmente y la visión a donde se quiere llegar	Detección del problema
28/09/2017	Reunión en la cual nos ayudó a responder preguntas y entender el manejo de la información dentro de la institución	se aclara el objetivo de la investigación
05/10/2017	Primera reunión para establecer procedimientos en levantamiento de activos	Realizar cronograma con los diferentes departamentos para levantamiento de activos

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Molina

Pronóstico

En la institución se genera un gran flujo de información; alrededor de 350 documentos físicos y 3.000 documentos digitales diarios, como por ejemplo oficios y memos. Mientras la información siga desordenada se incrementará la fuga de información, manipulación de datos y lentitud en el servicio que crecerá a medida que pase el tiempo ya que la información es requerida y generada diariamente.

Control de pronóstico

Para solucionar el problema en seguridad de la información de la institución encargada de regular cooperativas y asociaciones, se deben realizar las siguientes acciones:

a. Evaluar los procedimientos actuales de la institución, para detectar inconsistencias en los procesos de gestión de la información, en las condiciones de almacenamiento y en la distribución física medios de procesamiento y documentos.
b. Realizar una evaluación de las posibles alternativas que ayudara a disminuir el riesgo en la manipulación de la información.
c. Organizar la información digital o física de forma estructurada donde se pueda modificar y acceder a la misma de forma eficiente.

1.1.2 Formulación del Problema.

La institución pública que regula cooperativas y asociaciones, tiene la misión de supervisar y controlar su desempeño para garantizar el bienestar de todos los usuarios. Sin embargo, se ha detectado mediante el proceso de diagnóstico que existen inconsistencias en la gestión de la información; especialmente en jerarquización, accesibilidad y sistematización; evidenciando un nivel medio de vulnerabilidad lo cual afecta en la seguridad de todos los activos de información.

Tomando en cuenta que esta institución tiene a su cargo 716 cooperativas de ahorro y crédito en el sector financiero y 9.572 asociaciones, cooperativas y organizaciones comunitarias del sector no financiero; el impacto de la inconsistencia en la gestión de la información puede afectar directamente a cerca de 6’207.022 miembros o socios e indirectamente a todo el sistema financiero ecuatoriano ya que existe un volumen anual estimado de movimiento de activos de USD 9.556 millones (SEPS, 2017).

1.1.3 Sistematización del Problema.

- ¿Cuál es el estado actual de la gestión de la información de la institución encargada de regular cooperativas y asociaciones?
- ¿Cuáles son los activos de la información de la institución encargada de regular cooperativas y asociaciones?
- ¿Cómo puede la institución encargada de regular cooperativas y asociaciones mejorar la clasificación y etiquetado de la información?

1.1.4 Objetivo General.

Desarrollar una política para la clasificación y etiquetado de la información basado en riesgos, principalmente mediante el uso del conjunto de normas: ISO 27001:2013 y MAGERIT, posteriormente ISO 27002:2017 para generar mecanismos de control, con el fin de reducir considerablemente las inconsistencias en la gestión de la información de la institución encargada de regular cooperativas y asociaciones.

1.1.5 Objetivos Específicos

- Elaborar un diagnóstico preliminar de la situación actual de la gestión de la información de la institución encargada de regular cooperativas y asociaciones mediante una metodología basada en entrevistas y análisis documental para identificar los riegos que existe en la institución.
- Realizar un levantamiento detallado de activos de la información de la institución encargada de regular cooperativas y asociaciones para desarrollar una política de clasificación y etiquetado que permitirá identificar el nivel de confiabilidad, integridad y disponibilidad de la información.
- Evaluar las posibles amenazas y vulnerabilidades en los activos de la información ya organizado, para identificar el nivel de riesgo particular y así obtener una visión general del riesgo existente.

1.1.6 Justificación

En la actualidad, se genera una gran cantidad de información física y digital de alta relevancia para la institución encargada de regular cooperativas y asociaciones, en este contexto se ha considerado necesaria la implementación de controles mediante la metodología ISO 27001:2013 que nos ofrece un conjunto de normas para el análisis de riesgos derivados del uso de tecnologías de la información y comunicaciones TIC; mediante el levantamiento de activos, clasificación de la información, evaluación de riesgos, identificación de amenazas y vulnerabilidades. Lo que permitirá detectar y planificar la gestión oportuna para reducir los riesgos de la información.

El área encargada de la seguridad de la información de la institución ha considerado oportuno proteger y preservar la información que se genera dentro de la institución, mediante el desarrollo de la una política de clasificación y etiquetado de la información basada en riesgos.

Aprobada la carta de auspicio que permite la entrega de la información y colaboración del personal involucrado para el desarrollo de la investigación propuesta y dentro del acuerdo donde se menciona la confidencialidad con la que se debe manejar la información entregada por la institución, queda por lo tanto de manifiesto que el redactor de la tesis no puede mencionar el nombre de la institución dentro de la investigación.

Al existir leyes y normativas con respecto al manejo de la información pública que establecen categorías en la información. Se determina la necesidad de implementar una política de clasificación y etiquetado basada en riesgos, para mantener la organización de la información y salvaguardar los archivos durante 15 años después de su elaboración como dicta el artículo 2 del índice temático de documentos clasificados como reservados.

1.2 ESTADO DEL ARTE

Después de una minuciosa revisión de artículos, libros y revistas en inglés y español se puede determinar que la información generada y custodiada por la institución encargada de regular cooperativas y asociaciones tiene que ser clasificada por series documentales y reservadas como indica el índice temático de documentos clasificados(Estrella, 2012). A continuación, se detalla los diferentes criterios que se ha considerado para realizar la implementación de la política de clasificación y etiquetado.

La propuesta del desarrollo gestión de riesgos y controles de sistemas de información permite proponer diversos métodos y controles, que posteriormente podrá generar proyectos orientados a construir herramientas que permitan sistematizarlos, de manera que su utilización sea más amplia.

La investigación presentada en el artículo abre el camino a estudios relacionados con la cultura de la organizacional hacia los riesgos y controles en sistemas de información, que permiten indagar sobre los procesos de cambio organizacional necesarios para una adecuada incorporación de gestión de riesgos y controles en la seguridad de la información.(Guerrero Julio & Gómez Flórez, 2012)

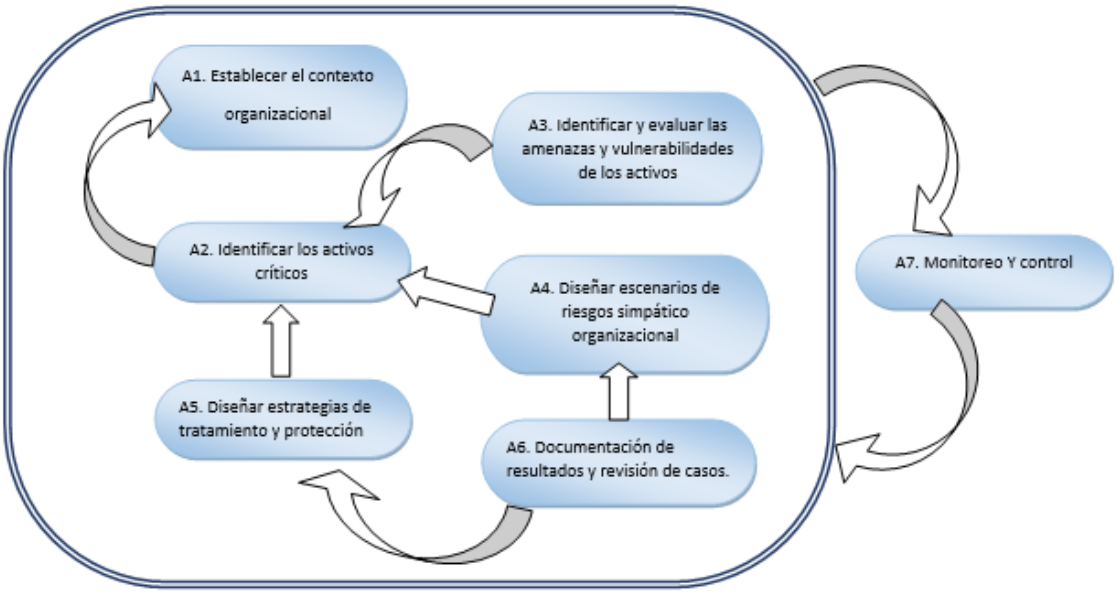

Figura 1. *Sistema de actividades para la dirección de tecnologías de la información*

Fuente: (Guerrero Julio & Gómez Flórez, 2012)

En el artículo de (Syalim, Hori, & Sakurai, n.d.) se realizó una elaboración de cuatro métodos para analizar el riesgo: Mehari, Magerit, NIST800-30 y la Guía de gestión de seguridad de Microsoft. Se encontró que todos los métodos siguen los tres primeros pasos generales para el análisis de riesgos: (1) Identificación de amenaza, (2) Identificación de vulnerabilidades y (3) Detección de riesgo. Se encontró que todos los métodos proporcionan una guía detallada para la evaluación de riesgo.

En el 2017 en Colombia se realiza un estudio de análisis y gestión de riesgo al sistema de información de la empresa AGESAGRO S.A.S utilizando la metodología MAMEGTIT (Varón Quiroga, 2017). Contribuyendo a la empresa conocimientos claros sobre los riesgos que puedan presentarse en el sistema de información, junto a los objetivos, estrategia y políticas de la organización.

Las principales perspectivas de este sistema están asociadas a sensibilizar a los responsables de las instituciones de información de la presencia de peligros y de la premura de planificar su gestión. De igual modo, la autora Aguilera (2010) señala que: "Magerit brinda un procedimiento frecuente para examinar los riesgos procedentes del empleo de medios tecnológicos de la información y comunicaciones (TIC)" (López, 2010, Pag. 21)Por otro lado, auxilia la identificación y proyección del procedimiento acertado para conservar los riesgos bajo vigilancia y de esta manera prepara a la estructura organizaciones para métodos de valoración, auditoría, legitimación o refrendación, de acuerdo con lo que se determine en cada caso.

De acuerdo a (Molina, 2015) en su trabajo *"Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del litoral*", MAGERIT se utilizó como una metodología para analizar la gestión de riesgos de los Sistemas de Información de la Escuela Politécnica del Litoral , el fin de esta fue disminuir los riesgos de la implementación y uso de las Tecnologías de la Información (TICS).

Octave se elige como una técnica de programación y consultoría táctica en seguridad fundada en el peligro. En contra de la distintiva consultoría direccionada en tecnología, que posee como finalidad los conflictos tecnológicos y la dirección en las temáticas estratégicas, la finalidad del OCTAVE es el riesgo en la organización y su centro de atención reside en los contenidos referentes a la habilidad y a la dinámica.

De acuerdo con las consideraciones del autor Giménez (2015) se delimita que:

Cuando se emplea OCTAVE, un pequeño grupo de gente desde las secciones ejecutantes o de negocios hasta los departamentos de tecnología de la información (IT) laboran juntos encaminados a las insuficiencias de seguridad, analizando tres elementos: inseguridades ejecutantes, habilidades de seguridad y tecnología.(Giménez, Pag 16).

En la investigación realizada por (Aucapiña, 2012), con el título "Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la cooperativa de ahorro y crédito San Francisco Ltda." Describe que la norma ISO 27001 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos; esto garantiza que ante recursos limitados las inversiones sean bien focalizadas, para lograr el objetivo se necesita de la concientización de la compañía ya que es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que despierten un interés y compromiso por parte de todos los empleados. Al tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significa contar con seguridad máxima en la información de la organización, sino que esto representa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

La norma ISO 27001 determina que todo contexto empresarial posee los conocimientos determinados acerca de la totalidad de los activos que tienen como parte transcendental de la administración de inseguridades. De acuerdo con esta norma los activos de información requieren estar catalogados de acuerdo a la sensibilidad y criticidad de la información que sujetan o que verifican con la finalidad de demarcar cómo ha de estar salvaguardada la información.(Aragón, 2009, Pag, 351).

Adicionalmente se tiene la investigación realizada por (Romo & Valarezo, 2012), con el título *"Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la universidad politécnica salesiana sede Guayaquil".* Presenta una guía para el cumplimiento de Políticas de Seguridad de la Información, basado en los controles de la normativa ISO 27002:2017, donde se detalla las buenas prácticas que el departamento de sistemas de la institución debe seguir y cumplir paso a paso para poder adquirir el

conocimiento necesario que le permitirá en base a las políticas establecer controles de seguridad, y a su vez, para mitigar riesgos como por ejemplo fuga de información.

DOCUMENTOS LEGALES DE LA REPÚBLICA DEL ECUADOR

A continuación, se detallan las leyes, artículos y códigos orgánicos que determinan los parámetros de confidencialidad de la información pública. A la vez serán utilizados como base para la clasificación de la información de acuerdo a las estipulaciones que dicta la normativa ecuatoriana.

LEY ORGÁNICA DE ECONOMÍA POPULAR Y SOLIDARIA

Art. 95.- Sigilo y Reserva. El sigilo y la reserva de los depósitos y las captaciones de las organizaciones del Sector Financiero Popular y Solidario, se regirá por las disposiciones del Código Orgánico Monetario y Financiero.

Artículo 95.- Sigilo y Reserva.- Los depósitos y demás captaciones de cualquier índole que se realicen en las organizaciones del sector financiero popular y solidario, determinadas por la Superintendencia, excluyendo las operaciones activas, estarán sujetos a sigilo, por lo cual las instituciones receptoras de los depósitos y captaciones, sus administradores, funcionarios y empleados, no podrán proporcionar información relativa a dichas operaciones, sino a su titular o a quien lo represente legalmente. Las organizaciones del sector financiero popular y solidario con el objeto de facilitar procesos de conciliación, darán acceso al conocimiento detallado de las operaciones anteriores y sus antecedentes a la firma de auditoría externa contratada por la institución, que también quedará sometida al sigilo bancario. Las organizaciones del sector financiero popular y solidario podrán dar a conocer las operaciones anteriores, en términos globales, no personalizados ni parcializados, solo para fines estadísticos o de información. Las organizaciones del sector financiero popular y solidario tendrán la obligación de proporcionar a la Superintendencia la información sobre las operaciones determinadas por ésta, por su naturaleza y monto, requieran de un informe especial. La Superintendencia proporcionará esta información a otras autoridades que por disposición legal expresa, previa determinación sobre su causa y fines, puedan requerirla, quienes también estarán sujetas al sigilo hasta que se utilice la información en los fines para los cuales se la requirió.(Asamblea, 2011)

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

TÍTULO TERCERO DE LA INFORMACIÓN RESERVADA Y CONFIDENCIAL

Art. 17.- De la Información Reservada. - No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos:

b) Las informaciones expresamente establecidas como reservadas en leyes vigentes. Art. 18.- Protección de la Información Reservada. - La información clasificada previamente como reservada, permanecerá con tal carácter hasta un período de quince años desde su clasificación. La información reservada será desclasificada cuando se extingan las causas que dieron lugar a su clasificación. Se ampliará el período de reserva sobre cierta documentación siempre y cuando permanezcan y se justifiquen las causas que dieron origen a su clasificación. El Consejo de Seguridad Nacional, en los casos de reserva por motivos de seguridad nacional y los titulares de las instituciones públicas, serán responsables de clasificar y desclasificar la información de conformidad con esta Ley. La clasificación de reserva no podrá efectuarse posteriormente a la solicitud de información. La información reservada que se haga pública antes del vencimiento del plazo de la reserva o de manera distinta a la prevista en el inciso anterior, podrá ocasionar responsabilidad civil, administrativa y/o penal según los casos, de la persona que por su función haya violado la reserva. Las instituciones públicas elaborarán semestralmente por temas, un índice de los expedientes clasificados como reservados. En ningún caso el índice será considerado como información reservada. Este índice de información reservada, detallará: fecha de resolución y período de vigencia de esta clasificación. La información reservada en temas de seguridad nacional, solo podrá ser desclasificada por el Consejo de Seguridad Nacional. La información clasificada como reservada por los titulares de las entidades e instituciones del sector público, podrá ser desclasificada en cualquier momento por el Congreso Nacional, con el voto favorable de la mayoría absoluta de sus integrantes, en sesión reservada.(Congreso, 2004)

ÍNDICE TEMÁTICO DE DOCUMENTOS CLASIFICADOS COMO RESERVADOS GENERADO POR LA SEPS

Artículo 1.- El índice temático por series documentales, de los expedientes clasificados como reservados por parte de la Superintendencia de Economía Popular y Solidaria, excluido del derecho de acceso a la información pública, es el siguiente:

a. Programas de supervisión de las entidades del sector financiero popular y solidario, y planes de regularización de las organizaciones de la economía popular y solidaria.
b. Informes de Auditorías internas y externas de las entidades del sector financiero popular y solidario y de las organizaciones de la economía popular y solidaria;
c. Informes de Auditorías, documentación e información que son parte del proceso de supervisión In Situ de las entidades del sector financiero popular y solidario, y de las organizaciones de la economía popular y solidaria;
d. Auditorías, análisis, informes y metodologías de supervisión extra situ de las entidades del sector financiero popular y solidario, y de las organizaciones de la economía popular y solidaria;
e. Inversiones (participación por tipo de instrumento y entidad, organización, emisores, inversionistas, por segmento o nivel);
f. Reportes, informes y estructuras realizadas en las entidades del sector financiero popular y solidario y de las organizaciones de la economía popular y solidaria, con excepción de los que se deban publicar de acuerdo a la normativa vigente;
g. Información remitida con carácter de reservado por las Superintendencias de Compañías, Valores y Seguros; Bancos; Control de Poder de Mercado; y, otros organismos de control;
h. Informes de supervisión, inspección, seguimiento y análisis de las entidades del sector financiero popular y solidario y de las organizaciones economía popular y solidaria, que emitan los administradores temporales, interventores y liquidadores de las entidades y organizaciones, según corresponda;
i. Informes y dictámenes jurídicos producidos por el Intendente (a) General de Procesos Jurídicos, asesores u otros abogados de la Institución contratados por ésta;

j. Información personal producida o que reposa en los expedientes de la Intendencia Administrativa y de Talento Humano de la institución, con excepción de aquella que se publica por transparencia en la gestión administrativa de las instituciones del Estado;
k. Planes o programas de supervisión o inspección, incluyendo el calendario anual de las visitas de inspección in situ y, los criterios o parámetros utilizados en las pruebas de esfuerzo y simulaciones;
l. Calificación de riesgo o de supervisión parcial y total de las entidades del sector financiero popular y solidario, y de las organizaciones de la economía popular y solidaria;
m. Informes de constitución de nuevas entidades, organizaciones y de apertura o traslado de oficinas o agencias;
n. Manuales operativos y de gestión;
o. Información individualizada sobre las operaciones activas y contingentes;
p. Información sujeta a sigilo y reserva conforme lo dispuesto en el artículo 353 del Código Orgánico Monetario y Financiero.(Estrella, 2012)

1.2.2 Adopción de una Perspectiva Teórica

Como producto de la investigación de fuentes fidedignas y con el fin de tener una visión macro lo suficientemente sólida para generar la política de clasificación y etiquetado; se decidió adoptar el fundamento teórico de Guerrero Julio y Gómez Flórez expuesto en el artículo del 2012

Cabe resaltar que para realizar la primera etapa del **análisis organizacional** también se adopta el fundamento teórico de Guerrero Julio y Gómez Flórez expuesto en el artículo del 2012(Guerrero Julio & Gómez Flórez, 2012).

Para la segunda etapa de **identificación de activos**, que se considera como eje en la creación de la política de clasificación y etiquetado se adopta la metodología Magerit versión 3, la cual se utiliza como instrumento que facilita la identificación de activos, dimensiones de valoración, criterios de valoración en la gestión de un activo (Amutio Gómez, 2012).

Para **el análisis de riesgo** que agrupa tres etapas: la tercera etapa de identificación y evaluación de amenazas y vulnerabilidades, la cuarta etapa de análisis de riesgo y quinta etapa de gestión de riesgo se adopta la norma ISO 27001:2013.

En la sexta y última etapa de **Seguimiento y control del riesgo**, se comprueba que todo el proceso general de clasificación y etiquetado se cumpla, formando un sistema de monitoreo de las vulnerabilidades que ayudan a identificar donde se encuentra el riesgo y entregando opciones para su control adoptando la norma ISO 27002:2017.

1.2.3 Marco Conceptual

A continuación, se detalla los conceptos que serán de investigación que nos va a llevar a cumplir el objetivo principal.

Activos: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.(Amutio Gómez, 2012)

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización (Amutio Gómez, 2012).

Política: Conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que, en un momento determinado, tanto los ciudadanos como el propio gobierno consideran prioritarios (Tamayo Saenz, 1997).

Clasificación: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización (ISO/IEC, 2017).

Seguridad de la información: La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad (Solarte, Enriquez, & Benavides, 2015).

Vulnerabilidad de la información: Son las posibilidades que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la

presencia de un factor que pueda posibilitar una amenaza o un ataque (Solarte et al., 2015).

Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones (Amutio Gómez, 2012).

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización (Amutio Gómez, 2012).

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos (Amutio Gómez, 2012).

1.2.4 Hipótesis

El desarrollo de una política de clasificación y etiquetado de la información basada en riesgos, garantizará el adecuado manejo de los activos de información dentro de la institución encargada de regular cooperativas y asociaciones permitiendo el cumplimiento de los estándares en la seguridad de la información. Lo que contribuirá con una mayor sistematización, jerarquización y accesibilidad de los activos.

CAPÍTULO II.

MÉTODO

2.1 TIPO DE ESTUDIO.

El enfoque de la investigación se realizó mediante un estudio **exploratorio** ya que se obtuvo información directa aplicando una entrevista a los responsables directos, definiendo normas para la seguridad de la información, que se adaptarán a los requerimientos de la institución encargada de regular cooperativas y asociaciones.

Este tipo de estudio servirá para elaborar la política de clasificación y etiquetado de la información basada en riegos, con el apoyo del área encargada de la seguridad de la información además del criterio de expertos en el tema y fuentes bibliográficas abaladas por organizaciones e instituciones especializadas en las áreas en cuestión.

2.2 MODALIDAD DE INVESTIGACIÓN.

Se utilizará la modalidad de investigación **documental** dentro de la institución en cuestión, en la cual las principales fuentes de información son las resoluciones, leyes, normas, registros impresos y electrónicos con el fin de mejorar la gestión del manejo de activos con información valiosa tomada como sustento científico del proyecto.

2.3 MÉTODO

El método que se utilizará en la investigación será el **deductivo-inductivo**, que está basado en la observación del manejo de la información dentro de la institución con respecto a la seguridad de la información para identificar: los diferentes activos, tipo de información, medio de difusión y tipo de almacenamiento; lo cual permite analizar el riesgo de cada activo y diseñar adecuadamente la política de clasificación y etiquetación según las necesidades detectadas en la institución.

2.4 POBLACIÓN Y MUESTRA.

El proyecto está orientado a una población constituida por 786 funcionarios en general, de los cuales 13 son responsables directos en la gestión de la información dentro la institución en las diferentes direcciones e intendencias, lo cual se detalla en el siguiente cuadro.

Tabla 2: Población y Muestra

Sujetos	Cantidad
Dirección nacional de la seguridad de la información	3
Intendencia de riesgo	10
Intendencia general de gestión	100
Intendencia general de técnica	400
Secretaria general	30
Otros usuarios de la institución	233
TOTAL	776

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Molina

2.5 SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN.

Para el levantamiento de información primaria se utilizará la técnica de la entrevista y como instrumento el **banco de preguntas**, el cual se aplicará a los responsables del manejo de la información dentro de la institución, esto permitirá conocer las falencias e inconsistencias en la gestión de activos.

La **observación directa**, es también un medio necesario para el desarrollo de la investigación, a través de esta se podrá identificar los lineamientos utilizados por la institución en la clasificación y manejo de la información donde se utilizará un juicio crítico de la observación. **Fotografías y notas de campos.**

En el análisis Documental, mediante esta técnica se podrán analizar los distintos instrumentos como **artículos, tesis, libros y documentos legales** que afecten a la institución, para poder identificar los posibles factores de riesgo existentes en la manipulación de archivos, sean físicos o digitales, y determinar la metodología adecuada basándonos en documentos publicados para la clasificación y etiquetado de la información basada en riesgos.

2.6 VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS.

Para realizar una entrevista eficaz se utilizará al grupo de expertos del departamento de seguridad de la institución encargada de regular cooperativas y asociaciones en la verificación del banco de preguntas orientadas a los intereses y necesidades para el levantamiento de activos y clasificación de la información.

Para el levantamiento de información primaria se utilizará la entrevista, acompañado del análisis documental el cual es validado por revistas, editoriales y entes reguladoras dependiendo del instrumento a utilizar. Brindando una información confiable que nos sirve como modelos a seguir para culminar con éxito la investigación.

2.7 OPERACIONALIZACIÓN DE VARIABLES.

Tabla 3: Operacionalización de Variables

Operacionalización de Variables			
Variable	Definición conceptual	Definición operacional	Indicadores de criterios de medición
Información Física	Es en medio por el cual se recibe información física que se distribuye en la institución.	Re refiere al proceso de ingreso de información mediante la recepción de documentos, y se medirá por tipo y tramite ingresado.	Promedio de ingreso de documentos físicos.
Información Digital / Aplicativo	Son medio de comunicación y utilización de aplicaciones de forma electrónica.	Se refiere a la interacción o intercambio que se realiza entre usuarios con los datos digitales y se medirá por los ingresos a los sistemas informáticos.	Promedio de ingreso de documentos digitales. Conectividad de unarios a los aplicativos.
Información Digital Pc/ USB	Son medios electrónicos que facilita la generación de información y traslado de información digital.	Se refiere a la creación de documentos que se genera al realizar el trabajado diario mediante el uso de herramientas tecnológicas se medirá a través del grado de importancia con respecto al tipo de actividad.	Informe de almacenamiento. Informe de respaldos.

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Molina

2.8 PROCESAMIENTO DE DATOS.

Tabla 4: Procesamiento de datos

Procesamiento de Datos		
Datos	Proceso	Salida
Periféricos de entrada	Procesamiento de información	Periféricos de salida
• Documentos Físicos • Documentos Digitales /aplicaciones • Documentos Físicos PC/USB	• Clasificación de activo • Clasificación por tipo de información.	• Políticas • Reglas • Proceso
• Red de datos • Correo Físico • Correo Electrónico • Impresos • Unidades Externas	• Clasificación por medio de difusión • Clasificación por nivel de impacto	• Políticas • Reglas • Proceso
• Servidores • Archivo Físico • PC / Laptop	• Clasificación por tipo de almacenamiento • Clasificación por nivel de impacto	• Políticas • Reglas • Proceso

Fuente: Institución encargada de regular cooperativas y asociaciones

Autor: José Molina

CAPITULO III.

RESULTADOS

3.1 DESCRIPCIÓN DE LA INSTITUCIÓN

Es una entidad técnica de supervisión y control que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario sean esta financieras o no financieras con procesos técnicos, trasparentes y confiables, para contribuir el bienestar de sus integrantes y de la comunidad en general pensando en la satisfacción de las necesidades de las personas. La superintendencia se ha propuesto para el año 2018 ser reconocida a nivel nacional e internacional como referente en supervisión y control de la economía popular y solidaria con procesos trasparentes, confiables y de excelencia que impulsan la consolidación de sus organizaciones en procura del buen vivir.

3.1.1 Actos inapropiados

Conflicto de interés

Intervenir directa o indirectamente, en actos en los cuales exista contraposición de intereses personales, laborales o financieros de las y los servidores públicos con los objetivos, deberes y funciones a su cargo y con los objetivos de la institución pública que regula cooperativas y asociaciones

Hacer mal uso de la información

Participar en actos no autorizados de cualquier índole, en los cuales se emplee o difunda información de la institución pública que regula cooperativas y asociaciones; o permitir el uso inapropiado de dicha información para beneficio personal o de terceros.

Abuso de autoridad

Sucede cuando las y los servidores de la institución pública que regula cooperativas y asociaciones se aprovechan del cargo o función que ejercen o representa en benéfico propio de cualquier índole.

3.1.2 Gestión de seguridad de la información

a. Misión:

Desarrollar y mantener el programa de seguridad de la información mediante la coordinación, asesoramiento, supervisión y preparación de políticas, planes, estrategias, controles y acciones que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de la información acorde a las necesidades institucionales; promoviendo un comportamiento responsable en la Seguridad de la Información.

b. Atributos y responsabilidades:

1. Diseñar, elaborar, ejecutar, actualizar las políticas, procedimientos, planes y controles concernientes a la seguridad de la información.
2. Diseñar, coordinar y actualizar planes de acción correctivos para mejorar el sistema de seguridad de la información y procedimientos para mejorar respuesta a incidentes de seguridad de la información.
3. Diseñar y coordinar la actualización y clasificación de los activos de información;
4. Diseñar y coordinar la estructura de gestión de la seguridad de la información para asignar roles, responsabilidades, facultades individuales y explícitas;
5. Sistematizar y coordinar la evaluación del riesgo y el plan de tratamiento de riesgo de seguridad de la información;
6. Proponer y coordinar planes de concienciación y capacitación sobre la seguridad de la información para el personal de la institución.
7. Monitorear y evaluar la efectividad de políticas, procedimientos y controles:
8. Coordinar, monitorear y evaluar los riesgos a los que están sometidos los activos de la información institucional;
9. Coordinar, monitorear y evaluar las acciones relacionados con los incidentes de seguridad en la información;
10. Coordinar, monitorear y evaluar las iniciativas de concienciación y capacitación sobre la seguridad de la información;
11. Validar, evaluar y mantener un registro de roles y perfiles de acceso a los activos de la información;

12. Evaluar el cumplimiento de las unidades funcionales de la institución en la implementación de controles de seguridad de la información, acorde las necesidades institucionales;
13. Coordinar planes, procedimientos y pruebas para brindar continuidad de las operaciones críticas institucionales.
14. Ejercer las demás funciones y atribuciones que le delegaren las autoridades

c. Productos y servicios

Gestión de planificación y normativa de seguridad de la información

1. Políticas, procedimientos, planes y controles de seguridad de la información;
2. Planes de acciones correctivas procedimientos para respuestas a incidentes de seguridad de la información;
3. Guías y metodologías para la clasificación de activos de la información;
4. Estructuras de roles y perfiles de acceso y privilegios que permitirá al uso los activos de información institucionales;
5. Plan de tratamiento de riesgo de Seguridad de la Información;
6. Plan de concienciación y capacitación en seguridad de la información;

Gestión de Seguimiento y Evaluación de la Información

1. Informes de seguimiento y evaluación de la aplicación de políticas procedimientos y controles relacionados con la seguridad de la información.
2. Informes de evaluación de riesgos de los activos de información.
3. Informes de evaluación de los incidentes de seguridad en la información;
4. Informes de evaluación de plan de concienciación y capacitación sobre la Seguridad de la información;
5. Informes de evaluación de la efectividad de la gestión de roles y perfiles de acceso a los activos y la información;
6. Informes de evaluación en el cumplimiento de controles de seguridad de la información de las unidades funcionales de la institución.
7. Informe de resultados de la aplicación de planes, procedimiento y pruebas de continuidad de las operaciones críticas institucionales.

3.2 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

3.2.1 Análisis de la necesidad

La institución en análisis es la encargada de la supervisión y control de cooperativas y asociaciones en el Ecuador, al ser una entidad que protege los activos de la información cuenta con una dirección de seguridad de la información que se encarga proteger los activos de información dentro de la institución.

La dirección de seguridad de la información busca crear, mejorar e implementar políticas de seguridad que permita salvaguardar la información entregada a la institución, por lo tanto, surge la necesidad de crear varios proyectos para la protección de la información basada en riesgos.

3.2.2 Análisis de resultados

La investigación se realizó mediante la aplicación de entrevistas y reuniones a las autoridades competentes dentro de la dirección de seguridad de la información y la dirección de riesgos de la institución encargada de regular cooperativas y asociaciones, lo que va a permitir conocer la situación actual en el manejo de la información.

Tabla 5 Matriz de resultados de la entrevista.

Entrevistado / Pregunta	Director	Analista de Seguridad	Seguridad	Mantenimiento
¿Cuentan con políticas de seguridad para la información?	Si, • PSI. • Acceso a Ethernet. • Acceso físico • Respaldos usuario final.	Si.	Si, • Control de accesos. • Respaldos. • PSI	Si, • Respaldos. • Antivirus.
¿Cómo se maneja el control de la seguridad de la información?	• Estrategias de negocio. • Políticas de seguridad de la información	• Políticas de seguridad de la información.	• Estrategias de negocio. • Políticas de seguridad de la información	• Políticas de seguridad de la información
¿Describa el control interno que realiza el área responsable en la seguridad de la información?	• Análisis de requisitos y especificaciones de seguridad de la información. • Normativa de seguridad.	• Análisis de requisitos y especificaciones de seguridad de la información • Aseguramiento de los servicios de aplicaciones en redes publicas • Protección de las transacciones de servicios de aplicación	• Análisis de requisitos y especificaciones de seguridad de la información.	• Análisis de requisitos y especificaciones de seguridad de la información.
¿La institución cuenta con un Sistema de Gestión de seguridad de la Información (SGSI)?	• NO	• NO	• NO	• NO

Entrevistado / Pregunta	Director	Analista de Seguridad	Seguridad	Mantenimiento
¿Cómo se garantiza la confiabilidad, integridad y disponibilidad de la información que se genera dentro de la institución?	• Planificación. • Evolución. • Normativa • Controles	• Planificación de la continuidad de la seguridad de la información • Implementación de la comunidad de la seguridad de la información • Revisión y evaluación de la comunidad de la seguridad de información.	• Normativa • Planificación • Control	• Revisión y evaluación de la comunidad de la seguridad de información.
¿Qué mecanismos, técnicas y/o herramientas de seguridad se aplican para salvaguardar la información confidencial?	• Identificación de las causas de incumplimiento. • Implementación de acciones correctivas necesarias.	• Identificación de las causas de incumplimiento. • Evaluación de acciones necesarias para el cumplimiento. • Implementación de acciones correctivas necesarias. • Revisión de acciones correctivas y verificar su efectividad.	• Identificación de las causas de incumplimiento. • Implementación de acciones correctivas necesarias.	• Implementación de acciones correctivas necesarias. • Revisión de acciones correctivas y verificar su efectividad.
¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?	Si, • Metodología basada en riesgos	NO	Si, • Metodología basada en riesgos	NO

Entrevistado / Pregunta	Director	Analista de Seguridad	Seguridad	Mantenimiento
¿Cómo se realiza el monitoreo a los sistemas de información y de comunicación?	• Revisión independiente de la seguridad de la información • Cumplimiento de las políticas y normas de seguridad	• Cumplimiento de las políticas y normas de seguridad • Comprobación del cumplimiento técnico	• Revisión independiente de la seguridad de la información • Cumplimiento de las políticas y normas de seguridad	• Comprobación del cumplimiento técnico
¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si……De qué manera se lo ha realizado; No……Porque?	SI, • Tenemos un plan de contingencia en TI aprobado.	NO	• Plan de continuidad solo aprobado,	NO

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

3.2.3 Tabulación de resultados

1. ¿Cuentan con políticas de seguridad para la información?

Objetivo:
Determinar si se aplican políticas de seguridad para la información.

Tabla 6: Pregunta 1 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
PSI.	3	30%
Acceso a Ethernet.	2	20%
Acceso físico	2	20%
Respaldos usuario final.	2	20%
Antivirus	1	10%
TOTAL	**10**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

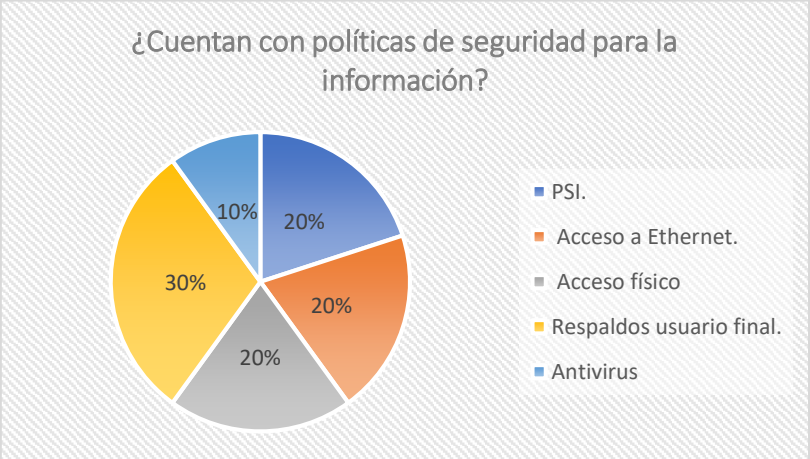

Figura 2 Gráfico pregunta 1

Autor: José Neptali Molina Alcocer

Interpretación:

Se puede concluir que la institución cuenta con políticas de seguridad alcanzando un 30% la comunicación de usuarios con gerentes (PSI), el 20 % podemos observar que corresponde al acceso a ethernet, accesos físicos y respaldos y con un 10% la aplicación de antivirus.

Análisis:

Se puede evidenciar que la institución cuenta con políticas de seguridad dirigida para los usuarios, pero la seguridad de la información se encuentra descuidada.

2. ¿Cómo se maneja el control de la seguridad de la información?

Objetivo:
Verificar la existencia de controles de seguridad de la información

Tabla 7: Pregunta 1 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
Estrategias de negocio.	2	40%
Políticas de seguridad de la información	3	60%
Normativas y contratos	0	0%
Asignación de responsables	0	0%
TOTAL	**5**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Figura 3 Grafico pregunta 2

Autor: José Neptali Molina Alcocer

Interpretación:

El 60% del personal manifiesta que se maneja políticas para la seguridad de la información acompañado con el control en estrategias del negocio con un 40% de las personas encuestadas.

Análisis:

Para el manejo de la seguridad de la información se puede constatar que se maneja dos aspectos: políticas de seguridad y estrategias de negocios

3. ¿Describa el control interno que realiza el área responsable en la seguridad de la información?

Objetivo: Identificar si se realiza un control por los responsables de la seguridad de la información.

Tabla 8: Pregunta 3 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
Análisis de requisitos y especificaciones de seguridad de la información	4	57%
Aseguramiento de los servicios de aplicaciones en redes publicas	1	14%
Protección de las transacciones de servicios de aplicación	1	14%
Normativa de seguridad	1	14%
TOTAL	**7**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

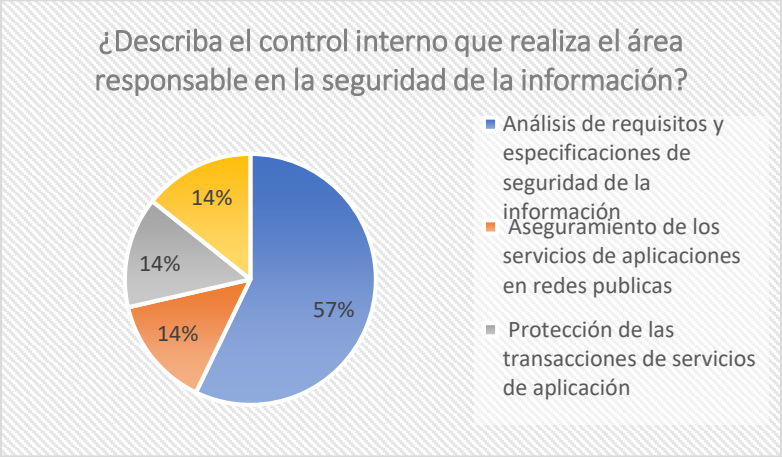

Figura 4: Gráfico pregunta 3

Autor: José Neptali Molina Alcocer

Interpretación:

Se puede interpretar que el 57% corresponde al análisis de requisitos y especificaciones de la seguridad de la información, acompañado con un 14% para el aseguramiento de los servicios de aplicaciones en redes públicas, protección de las transacciones de servicio de aplicación y normativa de seguridad.

Análisis:

No se mantiene un control apropiado de todas las actividades en el control interno para salvaguardar la información.

4. ¿La institución cuenta con un Sistema de Gestión de seguridad de la Información (SGSI)?

Objetivo:

Conocer si la institución cuenta con el sistema de gestión de la seguridad de la información.

Tabla 9: Pregunta 4 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
SI	0	0%
NO	4	100%
TOTAL	**4**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

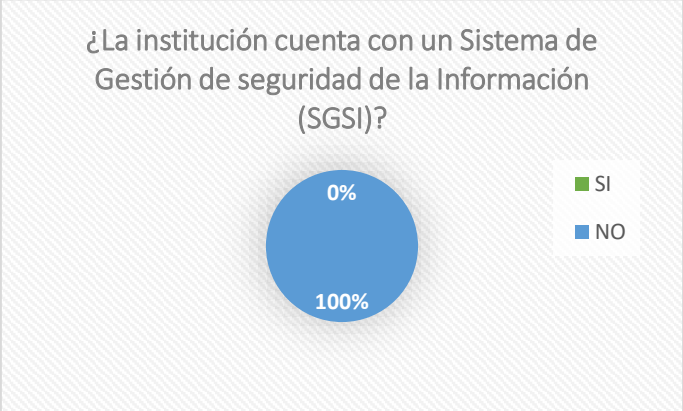

Figura 5: Gráfico pregunta 4

Autor: José Neptali Molina Alcocer

Interpretación:

Como se puede visualizar en el grafico la respuesta NO tienen un 100% en la encuesta realizada, quedando el sí con ninguna valoración.

Análisis:

Se puede evidenciar que la institución ni cuenta con un sistema de gestión de la información.

5. ¿Cómo se garantiza la confiabilidad, integridad y disponibilidad de la información que se genera dentro de la institución?

Objetivo:

Conocer la gestión que se realiza dentro de la institución para garantizar la integridad, confiabilidad y disponibilidad de la información procesada dentro de la empresa.

Tabla 10: Pregunta 5 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
Planificación.	3	27%
Evolución.	1	9%
Normativa	2	18%
Controles	4	36%
Implementación de la comunidad de la seguridad de la información	1	9%
TOTAL	**11**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

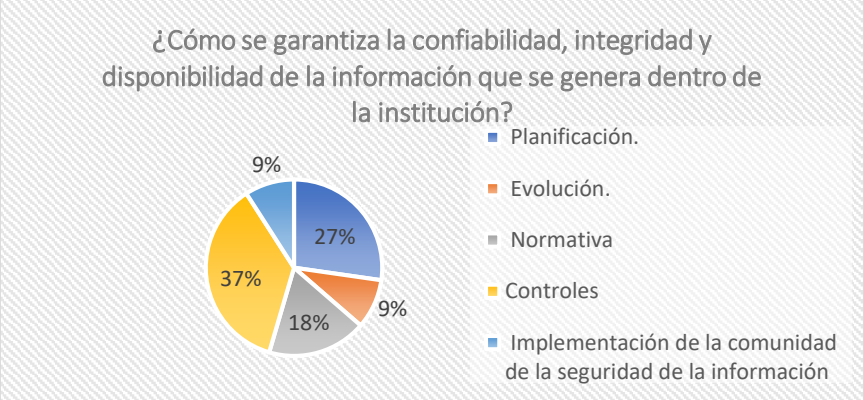

Figura 6: Gráfico pregunta 5

Autor: José Neptali Molina Alcocer

Interpretación:

Dentro de las cinco respuestas para garantizar la confiabilidad, integridad y disponibilidad de la información, la que más se destaca dentro del proceso con un 37% son los controles acompañado con un 27% la planificación, 18% normativa y finalmente con un 9% planificación e implementación de la comunidad de la seguridad de la información.

Análisis:

La institución carece de medidas técnicas preventivas y reactivas lo cual permite resguardar y proteger la información que vela por los principales objetivos de seguridad de los activos.

6. ¿Qué mecanismos, técnicas y/o herramientas de seguridad se aplican para salvaguardar la información confidencial?

Objetivo:

Conocer el proceso que me maneja dentro de la institución para salvaguardar la información confidencial generada en el trabajo diario.

Tabla 11: Pregunta 6 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
Identificación de las causas de incumplimiento.	3	30%
Evaluación de acciones necesarias para el cumplimiento.	1	10%
Implementación de acciones correctivas necesarias.	4	40%
Revisión de acciones correctivas y verificar su efectividad.	2	20%
TOTAL	**10**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

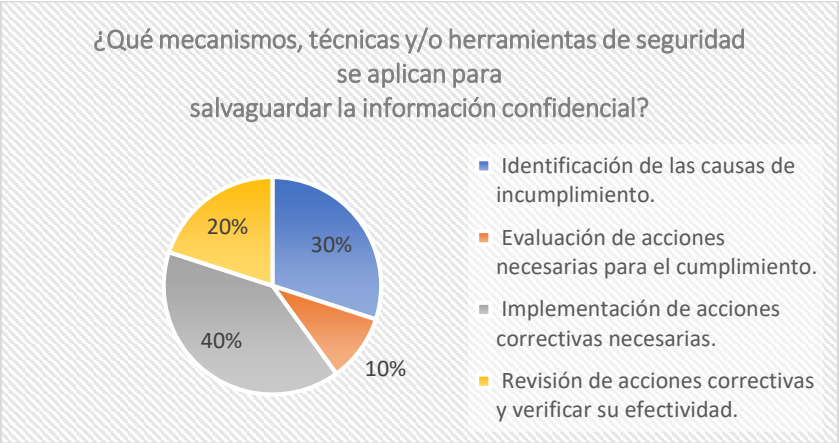

Figura: 7: Gráfico pregunta 6

Autor: José Neptali Molina Alcocer

Interpretación:

En el grafico se puede visualizar que se considera como lo más importante con un 40% la implementación de acciones correctiva, seguido con un 30% con la identificación de las causas de incumplimiento, 20 % revisión de acciones y con un 10% evaluación de las acciones necesarias para el cumplimiento.

Análisis:

La institución cuenta con un conjunto de mecanismo y técnicas, sin embargo, no se tiene claro el proceso a seguir para salvaguardar la información.

7. ¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?

Objetivo:

Verificar si la institución dispone de un proceso para la administración y control de riesgos en la seguridad de la información.

Tabla 12: Pregunta 7 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
SI.	2	50%
NO.	2	50%
Total	**4**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

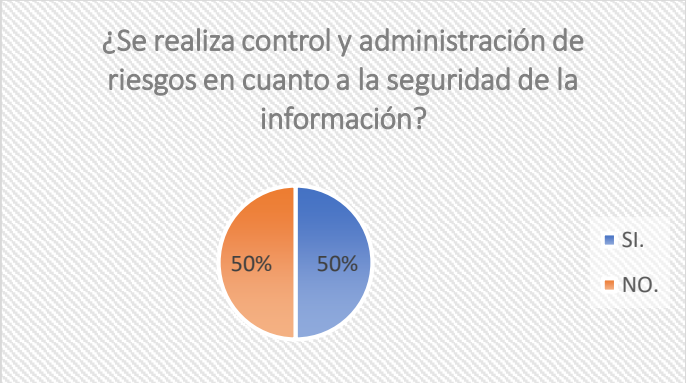

Figura 8: Gráfico pregunta 7

Autor: José Neptali Molina Alcocer

Interpretación:

Se puede observar que los colaboradores responsables en el manejo de la información dentro de la institución el 50% conoce sobre los controles para la gestión de riesgo y el 50% restante desconocen de su uso.

Análisis:

El control y administración de riesgo que se gestiona dentro de la institución no es conocido por todo el personal para lo cual se sugiere socializar el proceso de gestión de riesgos.

8. ¿Cómo se realiza el monitoreo a los sistemas de información y de comunicación?

Objetivo:

Conocer si la institución cuenta con procesos de monitoreo a los sistemas de información y comunicación.

Tabla 13: Pregunta 8 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
Revisión independiente de la seguridad de la información	2	24%
Cumplimiento de las políticas y normas de seguridad	3	38%
Comprobación del cumplimiento técnico	3	38%
Total	**8**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Figura 9: Gráfico pregunta 8

Autor: José Neptali Molina Alcocer

Interpretación:

Se puede interpretar que existe una gestión en comprobación de cumplimiento técnico y cumplimiento de políticas y normas de seguridad con un 38% cada una y con un 24% la revisión independiente de la seguridad de la información dentro del monitoreo a los sistemas de información y de comunicación.

Análisis:

Se puede describir que existe monitoreo a los sistemas de información y de comunicación dentro de la institución.

9. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si……De qué manera se lo ha realizado; ¿No……Por qué?

Objetivo:

Definir si en la institución se realiza simulacros frente a la caída de los sistemas de información y de comunicación para identificación de vulnerabilidades.

Tabla 14: Pregunta 9 cuadro de porcentaje

Respuesta	Cantidad	Porcentaje
SI.	2	50%
NO.	2	50%
Total	**4**	**100%**

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

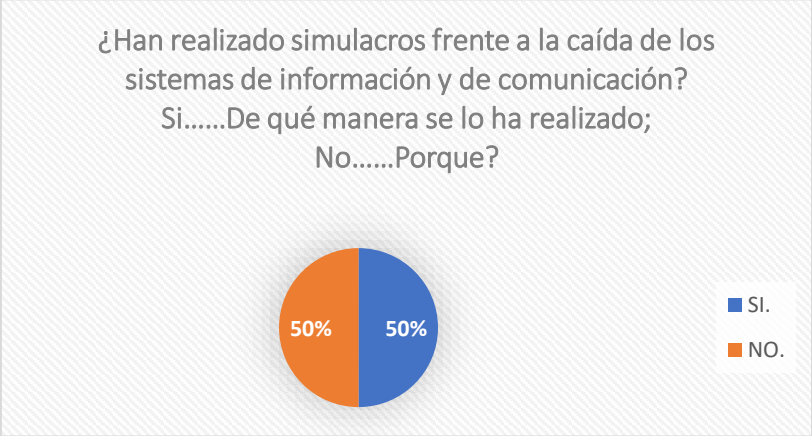

Ilustración 10: Gráfico pregunta 9

Autor: José Neptali Molina Alcocer

Interpretación:

Se puede visualizar en el gráfico que el conocimiento de simulacros frente a la caída de los sistemas esta divididos con una igualdad el 50%

Análisis:

La institución cuenta con un plan de contingencia aprobado por el departamento de TI para enfrentar caídas de sistemas de información y comunicación.

3.2.4. Interpretación de resultados

Después de realizar un análisis minucioso a cada pregunta y cada entrevistado que maneja directamente la seguridad de la información se pude determinar o siguiente:

Conclusiones del análisis de resultados:

- No existe políticas de clasificación y etiquetado de la información que se genera y recopila dentro de la institución.
- La institución no cuenta con un sistema de gestión de seguridad de la información.
- La institución cuenta con la dirección de seguridad de la información la cual se encarga de proteger los activos de información.
- No se utiliza metodologías para garantizar la confiabilidad, integridad y disponibilidad de los activos de la información.

Recomendaciones del análisis de resultados:

- Crear una política de clasificación y etiquetado de la información basada en riesgos, adoptando normas y reglas establecidas en la institución.
- Utilizar metodologías como Magerit y ISO 27001 para el levantamiento de activos y evolución de riesgo ya que se las normas mencionadas se aplican a instituciones públicas y la evaluación es basada en riesgos.

3.3 INTRODUCCIÓN

La gestión de activos de información contempla los siguientes elementos: planificación, identificación de los activos, seguimiento y control.

Figura 1 Ciclo de la Gestión de Activos de Información
Autor: José Neptali Molina Alcocer

3.3.1 Planificación

Dentro de la planificación se establece cuáles serán las políticas y lineamientos para realizar la gestión de activos de información, las valoraciones para identificación de riesgos, definición de alcance y cada uno de los activos a identificar dividiendo a la organización en unidades de negocio desde las de mayor importancia criticidad y valor para la institución a las de menores, la misma que debe ser determinada con la aprobación de la máxima autoridad de la institución encargada de regular cooperativas y asociaciones.

3.3.2 Identificación y Clasificación

Identificación: una vez definido los alcances y los lineamientos de gestión, se debe seguir con la identificación y clasificación de los activos de información.

En esta etapa podremos realizar un levantamiento de información e identificar:

- Los recursos de información.
- Ubicación de los datos.
- Determinar los propietarios, usuarios, custodios de los datos.
- Datos que los proveedores y terceros poseen.
- Identificar los niveles de accesos, los cuales deben ser mínimos.
- Que activos se podrían agrupar con una misma estrategia de seguridad.

Pre-Clasificación: en la etapa de pre-clasificación se debe tomar en cuenta los parámetros que sirven para medir los valores en función a la importancia relativa de los activos de información, considerando la confidencialidad, integridad y disponibilidad que se requiere en la institución.

El resultado de realizar esta preclasificación es un inventario de todos los activos de información. Junto con este inventario se definen los propietarios, custodios de la información (que no necesariamente son los mismos), los medios de almacenamiento de la información, forma de distribución y los componentes tecnológicos.

Clasificación: con este inventario de activos preclasificados se procede a la identificación de posibles vulnerabilidades, la evaluación y ponderación del riesgo al cual están sometidos los mismos, a través de la valoración definida en esta metodología.

Seguimiento y Control: con el inventario final de activos, se procede con cada uno de los propietarios a definir un mapa integral de riesgos por activo; se establecen los controles a implementar para mitigar los riesgos definidos, así como las estrategias para la implementación. En esta fase se realiza un seguimiento a la implementación de los controles y estrategias para mitigar los riesgos definidos, los informes relativos a dicha implementación se darán a conocer al Comité de Seguridad de la Información.

3.4 METODOLOGÍA DE GESTIÓN

3.4.1 PLANIFICACIÓN

Para que se realice una adecuada gestión deben seguirse los elementos definidos dentro de la planificación. Cuando se realiza la planificación debe tomarse en cuenta lo siguiente (figura 11):

Figura 11 Esquema de Planificación

Autor: José Neptali Molina Alcocer

Definición del alcance: Deben establecerse las metas claras que se van a gestionar en el contexto organizacional, para la planificación se tomará en consideración los siguientes aspectos:

- Identificar la estrategia de la institución en torno a los sistemas de información, utilizando las técnicas de recolección de información como: Entrevistar a los jefes del Dpto. de Sistemas administradores de TI y revisar la documentación sobre las políticas organizacionales de adquisición, implementación y uso de los SI.
- Especificar los sistemas de información que apoyan los procesos determinando la dependencia de los procesos con respecto a los sistemas de información.
- Especificar los roles de los actores y sus responsabilidades en los riesgos asociados a los sistemas de información, se puede identificar mediante entrevistas a los actores de los sistemas de información sobre la conducta anti riesgos

Definición de las políticas de clasificación: Es importante que se definan las políticas de clasificación bajo qué criterios deben establecerse. En ese sentido las políticas o criterios de clasificación deben identificar al activo dentro de la confidencialidad, integridad y disponibilidad considerando los valores, los niveles y etiquetas que se exponen en la tabla15.

Tabla 15 Definiciones nivel valor vs criterios de clasificación

Tipo	Nivel / Valor	Confidencialidad	Integridad	Disponibilidad
TOP SECRET	5	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de servidores o funcionarios, generalmente de la alta dirección.	Información cuya modificación no autorizada no podría recuperarse, ocasionando pérdidas graves a la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la SEPS o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas a entes externos.
SECRETA	4	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios. Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar efectos negativos sobre la Entidad	Información cuya modificación no autorizada es de difícil recuperación y podría ocasionar pérdidas significativas para la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la institución o a terceros. podría ocasionar pérdidas significativas a la SEPS o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen moderado a entes externos.
CONFIDENCIAL	3	Información que puede ser conocida y utilizada por todos los servidores y funcionarios de la SEPS. Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones	Información cuya modificación no autorizada puede recuperarse aunque podría ocasionar pérdidas leves para la institución o a terceros. La información cuya modificación o eliminación puede ocasionar un impacto significativo dentro de las direcciones.	Información cuya inaccesibilidad permanente durante un mes o más, podría ocasionar pérdidas significativas para la institución o para terceros. La no disponibilidad de la información puede afectar a la operación normal pero no conlleva ampliaciones legales, económicas o pérdida de imagen.
RESTRINGIDA	2	Información que puede ser conocida y utilizada, sin autorización por cualquier persona. Podrá ser utilizada por todos los empleados directos de la SEPS y por empleados temporales, contratistas y/o terceros a la SEPS	Información cuya modificación no autorizada puede recuperarse fácilmente, o no afecta a la operatividad. La pérdida de información conlleva un impacto NO significativo para la entidad o entes externos	Información cuya inaccesibilidad no afecta la operatividad. La no disponibilidad de la información no conlleva implicaciones legales, ecuménicas o pérdida de imagen
PUBLICA	1	Información de disponible para cualquier persona externa a la institución. Información Publica	información que puede ser usado como informativa o material de investigación. Los activos de información que deben ser incluidos en el inventario como activos de información de integridad	Información que se encontrara publicada en medios digitales. La información puede acceder personas ajenas a la institución

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Lineamiento a los objetivos institucionales. - La gestión de clasificación de información debe estar alineada al plan estratégico de la organización. Para esto debe verificarse en el alcance que es lo que se va a identificar, clasificar y que se encuentre dentro de los procesos que soportan los objetivos institucionales.

3.5 IDENTIFICACIÓN Y CLASIFICACIÓN

Una vez planteado los lineamientos y objetivos de la gestión de activos de información, procedemos con la identificación y clasificación de activos, los pasos a seguir se ilustran en la figura #12:

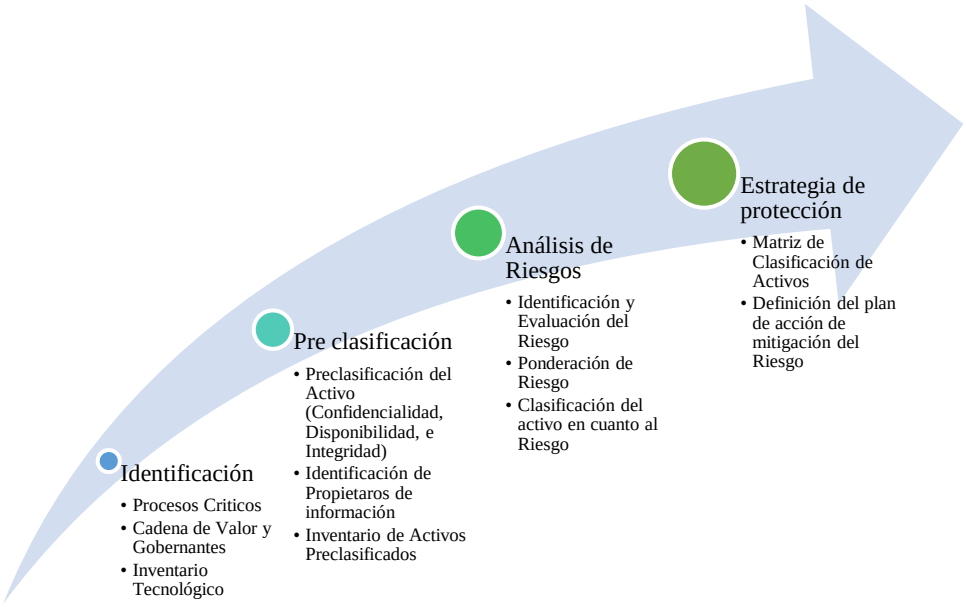

Figura 12 Pasos para la identificación y clasificación

Autor: José Neptali Molina Alcocer

3.5.1 Identificación

Para lograr la identificación es necesario contar dos elementos previos, la definición de los procesos críticos que generalmente son los procesos de la cadena de valor, algunos gobernantes y de apoyo. Dentro de los procesos de apoyo se encuentran los procesos de tecnologías de la información, aquellos procesos se vuelven importantes e inclusos críticos. De allí depende que, por la implementación de buenas prácticas y de estándares internacionales se cuente con

varios elementos derivados de esa gestión tales como: un portafolio de servicios, un inventario tecnológico, procesos documentados y demás. Para esta etapa de identificación se utilizará el inventario tecnológico, y como referencia el portafolio de servicios.

Todos los activos de información durante la fase de análisis del proceso de implantación de la norma, se someterán a un análisis de impacto en el negocio en los que se consideran los atributos de Confidencialidad, Integridad y Disponibilidad.

La metodología de evaluación de riesgos evalúa los riesgos resultantes de amenazas de carácter interno y externo, ya sean deliberadas o accidentales, sobre los activos de información documentados en la lista de activos y su vulnerabilidad frente a éstas.

Se requiere que los propietarios de los activos evalúen el efecto que tendría en el negocio (empleados, clientes, proveedores o accionistas) la pérdida de confidencialidad, integridad y disponibilidad, de dichos activos, en el peor caso posible. Para facilitar una interpretación estándar de esta evaluación, se ha confeccionado una matriz de riesgos que tiene que estar aprobada por la dirección de la empresa.

Con los insumos y entregables (información) de los procesos críticos y el inventario tecnológico se puede seguir con la siguiente etapa, la pre clasificación de los activos.

Figura 13 Elementos de la Identificación

Autor: José Neptali Molina Alcocer

3.5.2 Pre clasificación de los activos

En la actividad se busca detectar los activos más relevantes dentro del proceso que se va analizar, diferenciando por tipo de activo, identificando las relaciones entre los distintos activos, definiendo las dimensiones de seguridad y valorando la importancia.

Figura 14 Caracterización de los activos

Autor: José Neptali Molina Alcocer

Lo primero que se debe hacer en esta etapa es identificar a los propietarios de información, al contar con procesos documentados será fácil su identificación; debido a que los propietarios de la información son por lo general los responsables de los procesos, o los responsables de la información de los insumos de dicho proceso.

Tabla 16 Matriz Levantamiento de activos

Activo	Descripción	Ubicación	Área	Propietario	Tipo	Cantidad

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Tipos de Activos

La tipificación de los activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

Activos esenciales

Dentro de sistema de información en la clasificación de activos se existen dos cosas esenciales, la información que se gestiona y los servicios que se prestan, marcando los requerimientos de seguridad para todos los componentes del sistema donde se puede considerar algunas características como se describe en la figura número 15

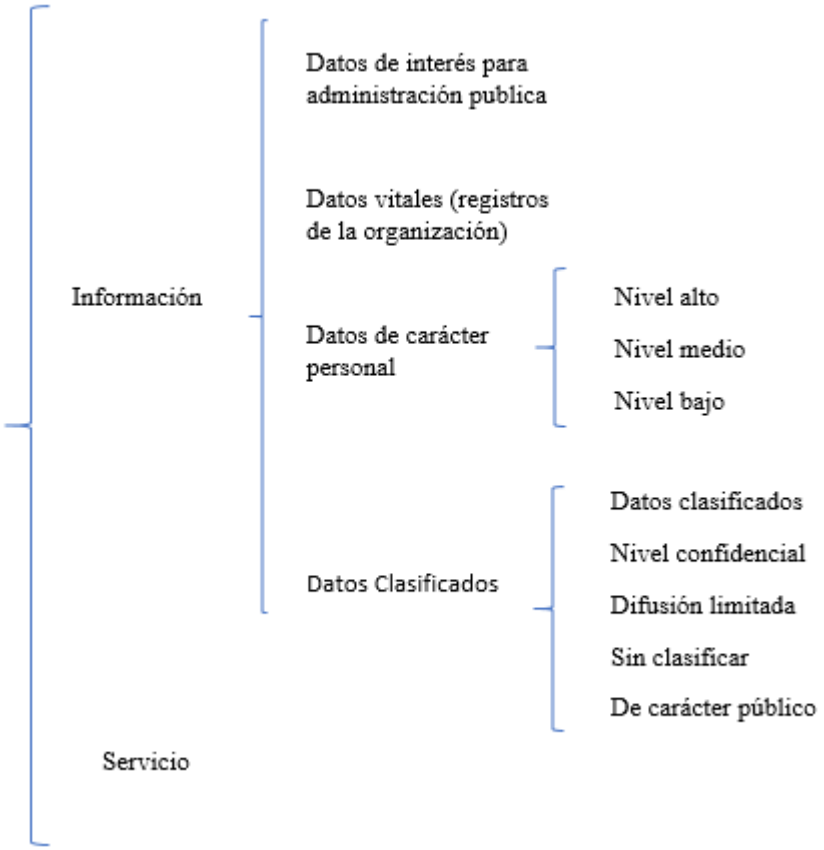

Figura 15 Activos esenciales

Autor: José Neptali Molina Alcocer

Físico

Elementos físicos que soportan los procesos de tratamiento de información y del negocio.

Información

Información vital para el negocio. Información personal privada según la ley orgánica de protección de datos. Información estratégica requerida para alcanzar objetivos. Información de alto costo económico o en dedicación de recursos para conseguirla, almacenarla o procesarla.

Personal

Puesto de personal clave para la toma de decisiones relacionadas con la seguridad.

Procesos

Procesos cuya pérdida o degradación pueda hacer imposible llevar adelante la misión de la organización. Procesos que sean secretos o utilicen tecnología propietaria. Procesos necesarios para el cumplimiento legal, regulatorio o contractual

Red

Elementos de la infraestructura de telecomunicaciones.

Servicios

Servicios relacionados con la seguridad o sus procesos.

Software

Programas informáticos, adquiridos, desarrollados o mantenidos. Los atributos mencionados son los más comunes, pero se puede agregar nuevos criterios si el responsable de la seguridad de la información lo cree necesario.

Con estos propietarios de la información se procederá en la matriz respectiva a clasificar la información y los activos que sirven de custodios, es decir se irá identificando cada información dentro del proceso midiendo su nivel de confidencialidad, integridad y disponibilidad, conforme se ha definido en la política de clasificación, por ejemplo:

Tabla 17 Matriz de tipos de activos valorando su confidencialidad, integridad y disponibilidad

Clasificación de un Activo							
Tipos de Activo	Descripción	Global	De Empresa	De Cliente	Confidenciabilidad	Integrida	Disponibilidad
Físico		X					X
Información		X			X	X	X
Personal		X					X
Procesos		X			X		X
Red		X					X
Servicios		X					X
Software		X					X

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Con esa caracterización, se tiene una idea bastante clara de ¿Qué tipo de información es?, ¿Por dónde circula?, ¿Dónde se almacena?; si es física o electrónica o ambas, y a que riesgos se enfrenta. Esto permite poner controles o planes de seguridad no solo al activo tecnológico, sino a la información en sí, donde sea que esta se genere, transmita, custodie o almacene. En esta etapa debe identificarse el activo de TI que soporta esta información, para esto es necesario contar con el inventario tecnológico. Esta etapa una vez caracterizada, se la realiza en conjunto con el área tecnológica.

Para finalizar la pre clasificación, es necesario tener un grado de clasificación de seguridad de cada activo identificado en conjunto con los responsables en la gestión de la información, es decir se toman los valores de cada factor de acuerdo a su confidencialidad, integridad y disponibilidad.

Dimensiones de valoración

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas.

Niveles de clasificación de acuerdo a la confidencialidad

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

¿Qué importancia tendría que el dato si fuera conocido por personas no autorizadas?

> Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización y los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

Tabla 18 Clasificación acuerdo a la confidencialidad

Etiqueta	Descripción acuerdo confidencialidad
Top Secret	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de servidores o funcionarios, generalmente de la alta dirección. información de alta importancia para la institución encargada de regular cooperativas y asociaciones que solo puede ser accedida por quienes ejerzan las funciones de: • Super Intendente • Directores
Secreta	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios seleccionados. Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar efectos negativos sobre la Entidad
Confidencial	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios de una dirección o intendencia. Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones
Restringida	Información que puede ser conocida y utilizada por todos los servidores y funcionarios de la institución encargada de regular cooperativas y asociaciones. Podrá ser utilizada por todos los empleados directos y por empleados temporales, contratistas y/o terceros a la institución encargada de regular cooperativas y asociaciones
Pública	Información que puede ser conocida y utilizada sin autorización por cualquier persona. Información Publica

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Niveles de clasificación de acuerdo a la integridad.

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización que puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.

Tabla 19 Clasificación acuerdo a la Integridad

Etiqueta	Descripción acuerdo integridad
Top Secret	Información cuya modificación no autorizada no podría recuperarse, ocasionando pérdidas graves a la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Pérdida de imagen severa de la entidad.
Secreta	Información cuya modificación no autorizada es de difícil recuperación y podría ocasionar pérdidas significativas para la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.
Confidencial	Información cuya modificación no autorizada puede recuperarse, aunque podría ocasionar pérdidas leves para la institución o a terceros. La información cuya modificación o eliminación puede ocasionar un impacto significativo dentro de las direcciones.
Restringida	Información cuya modificación no autorizada puede recuperarse fácilmente, o no afecta a la operatividad. La pérdida de información conlleva un impacto NO significativo para la entidad o entes externos.
Pública	La información que puede ser usado como informativa o material de investigación. Los activos de información que deben ser incluidos en el inventario como activos de información de integridad.

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Nivel de clasificación de acuerdo a la disponibilidad

Propiedad o característica de los activos. consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad ya que si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

Tabla 20 Clasificación acuerdo a la disponibilidad

Etiqueta	Descripción acuerdo disponibilidad
Top Secret	La información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la institución encargada de regular cooperativas y asociaciones o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Pérdida de imagen severas a entes externos.
Secreta	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la institución o a terceros. Podría ocasionar pérdidas significativas a la institución encargada de regular cooperativas y asociaciones o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • Retraso en sus funciones. • Pérdida de imagen moderado a entes externos.
Confidencial	Información cuya inaccesibilidad permanente durante un mes o más, podría ocasionar pérdidas significativas para la institución o para terceros. La no disponibilidad de la información puede afectar a la operación normal pero no conlleva ampliaciones legales, económicas o pérdida de imagen.
Restringida	Información cuya inaccesibilidad no afecta la operatividad. La no disponibilidad de la información no conlleva implicaciones legales, económicas o pérdida de imagen
Pública	Información que se encontrara publicada en medios digitales La información puede acceder personas ajenas a la institución

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Criterio de valoración:

Como siguiente paso de la política después de la identificación de se debe realizar una valoración de los mismos, identificando por los propietarios las consecuencias que tendría para el negocio la pérdida de su confidencialidad, integridad o disponibilidad, en el peor caso posible, sin tener en cuenta medidas de seguridad existentes en la institución.

El valor promedio de los tres valores asignados para cada activo de información determinará el valor de impacto general del activo, estableciendo su importancia para el estudio realizado. En el presente análisis se ha definido que aquellos activos con un valor promedio de impacto con la escala de valoración de acuerdo con la siguiente codificación:

Tabla 21 Matriz para valor de impacto general del activo

Valoración	Descripción	Justificación
5	Supervivencia del negocio amenazada	Requiere
4	Daño grave	No requiere
3	Daño considerable	No requiere
2	Daño menor	No requiere
1	Daño insignificante	No requiere

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Tabla 22 Valoración de activo

Descripción	Cantidad	Tipo	Ubicación	Área	Propietario	Valoración Parcial			Valoración Final	Valor de Impacto
						C	D	I		
Archivo Word de la resolución con la finalidad de realizar la publicación en el registro oficial.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	4	4	4	Daño Grave
Documento de extracto de la resolución.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	1	1	3	2	Daño Menor
El archivo Word de la resolución tiene la finalidad de realizar la publicación en el registro oficial.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	2	2	4	3	Daño considerable
Convocatoria a calificación de acreencias para remitirlo a la Dirección Nacional de Comunicación.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	4	5	4	Daño Menor
Correo electrónico al analista de liquidaciones del sector financiero.	1	Software	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	2	2	2	Daño Menor
El director recibirá y revisará el memorando y los artes adjuntos	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Director Nacional de Liquidación del Sector Financiero	3	2	2	2	Daño Menor
Correo electrónico a la prensa	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Director Nacional de Liquidación del Sector Financiero	2	1	1	1	Daño insignificante

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Dependencia de Activos

Para una correcta obtención de impactos sobre el negocio a partir de la pérdida de los atributos de los activos, es necesario establecer las dependencias entre los mismos. La dependencia puede establecerse con un único nivel de relaciones:

- Información
    - Software
    - Físicos
    - Red
    - Personal
    - Etc.

O bien tener más niveles según el criterio del responsable de seguridad:

- Información
    - Software
        - Físicos
    - Red
    - Procesos
        - Personal
        - Etc.

Para evitar duplicidad en las tareas de valoración, se establecerán criterios generales de agrupación de activos, de forma que luego se valoren amenazas y vulnerabilidades comunes a los activos que conforman el grupo.

En este sentido, para asegurarse que se aplican todas las amenazas, vulnerabilidades y controles al análisis de riesgos, será necesario que exista al menos un activo de cada tipo. Esto se aplica particularmente al activo tipo "Proceso" que apunta a amenazas y vulnerabilidades relacionadas con los aspectos organizativos y de cumplimiento de la Seguridad de la Información, que de otra forma no tendrían un tipo de activo donde aplicarlos de forma eficaz. Por ello, deberá existir en todo análisis de riesgos un único activo "Proceso" al que llamaremos "Seguridad de la Información".

Los beneficios de clasificar la información son:

- Identificar Qué información es sensible y vital para la institución encargada de regular cooperativas y asociaciones.
- Identificar Quiénes son los propietarios de la información y los responsables de la asignación de los permisos de acceso a la misma.
- Definir niveles apropiados de protección de la información y segregación de acceso a la misma.
- Controlar qué usuarios tienen acceso a la información.

Riesgos de no clasificar la información:

- Asignación de niveles y/o permisos de acceso a la información errada
- Pérdida de Información por acciones de usuarios mal intencionadas.
- Modificación de la información sin previa autorización.
- Uso de la información por parte de usuarios con fines personales.

Amenazas y vulnerabilidades

La organización se basa en una evaluación de amenazas y vulnerabilidades en una lista de amenazas extraída de norma de referencia ISO/IEC 27005:2008 y la experiencia de la empresa. Con el fin de priorizar dichas amenazas de acuerdo a los requisitos del negocio, el Responsable de Seguridad, junto con expertos en las áreas auditadas, evaluarán la importancia de la amenaza de acuerdo a la siguiente tabla:

Tabla 23 Método de evaluación de amenazas

Nivel de Amenaza	Descripción	Justificación
3	La amenaza se considera presente y con alta probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
2	La amenaza se considera presente y con media probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
1	La amenaza se considera presente y con baja probabilidad de que explote vulnerabilidades dentro del alcance.	Requiere
0	La amenaza no está presente en el entorno del alcance de la implantación.	Requiere

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

3.5.3 Análisis de Riesgos (Identificación y evaluación del Riesgo)

En esta fase se realiza la autoevaluación de riegos. Ahora, la evaluación de riesgos se la hace al activo de información, es decir a la información, o al activo tecnológico que genera, procesa, transmite o custodia esa información. Dependiendo del alcance definido en la planificación, podremos hacer a la información, al activo tecnológico o a ambos. En cualquiera de los casos los pasos que se dan aplican igual.

Lo primero que se debe realizar es la identificación de amenazas y vulnerabilidades que están expuestos los activos de información, que consiste en ir describiendo cada uno de los eventos que pueden afectar negativamente a los activos. Por ejemplo, un activo, puede ser, el informe de hallazgos y la matriz de los mismos encontrados en una organización controlada, puede sufrir un riesgo como que esa información sea accedida y divulgada por un tercero no autorizado al público, pudiendo provocar problemas reputacionales y credibilidad. Ahora también puede verse afectado.

Tabla 24 Descripción de amenazas

Amenaza	Descripción	Global	Confidencialidad	Integridad	Disponibilidad
Abuso de los derechos	Compromiso de las funciones. Accidental, deliberado.	true	true	true	true
Acceso a soportes no autorizado	Compromiso de la información. Deliberado.	true	true	true	true
Acceso no autorizado	Compromiso de la información. Deliberado.	true	true	true	true
Atentado terrorista	Daño físico. Deliberado.	true	false	false	true
Daño por agua	Daño físico. Accidental, intencionado o ambiental.	true	false	false	true
Daño por pruebas de intrusión	Compromiso de la información. Fallos técnicos. Accidental.	true	true	true	true
Daño por tercera parte	Compromiso de la información. Fallos técnicos. Accidental, deliberado.	true	true	true	true
Denegación de acciones	Compromiso de las funciones. Deliberado.	true	false	false	true
Destrucción	Daño físico. Accidental, intencionado o ambiental.	true	false	false	true
Deterioro de los soportes	Compromiso de la información. Ambiental.	true	false	true	true
Elevación de privilegios	Compromiso de las funciones. Deliberado.	true	true	true	true
Error en el uso	Compromiso de las funciones. Accidental.	true	true	true	true
Escuchas no autorizadas	Compromiso de la información. Deliberado.	true	true	false	false
Espionaje	Compromiso de la información. Intencionado.	true	true	false	false
Fallo de equipos	Fallos técnicos. Accidental.	true	false	false	true
Fallo de sistemas	Compromiso de la información. Accidental.	true	true	true	true
Fallo del aire acondicionado	Pérdida de servicios esenciales. Accidental, deliberado.	true	false	false	true
Fallo en equipamiento de telecomunicaciones	Fallos técnicos. Accidental.	true	false	false	true
Fallo en la provisión	Pérdida de servicios esenciales. Accidental, delibrado.	true	false	false	true
Falta de disponibilidad del personal	Compromiso de las funciones. Accidental, deliberado, ambiental.	true	true	false	true
Falta de mantenimiento de equipos	Fallos técnicos. Accidental, deliberado.	true	false	false	true

Amenaza	Descripción	Global	Confidencialidad	Integridad	Disponibilidad
Fuego	Daño físico. Accidental, intencionado o ambiental.	true	false	false	true
Gestión ineficiente de la seguridad de la información	Compromiso de las funciones. Accidental	true	true	true	true
Hacktivismo	Ataques por grupos de Hacking	false	true	true	true
Hacktivismo	Amenaza externa a Hacktivismo	false	true	true	true
Hacktivismo	Amenaza externa a Hacktivismo	false	true	true	true
Incumplimiento legal, reglamentario o contractual	Acciones no autorizadas. Accidental, deliberado.	true	true	true	true
Información de fuentes no confiables	Compromiso de la información. Accidental, deliberado.	true	false	true	false
Interrupción de los procesos	Compromiso de las funciones. Accidental.	true	false	false	true
Inundación	Evento natural. Daño físico. Ambiental.	true	false	false	true
Manipulación de los equipos	Compromiso de la información. Deliberado.	true	false	false	true
Manipulación de los registros	Compromiso de la información. Deliberado.	true	false	true	false
Manipulación de sistemas de información	Compromiso de la información. Accidental, deliberado.	true	true	true	true
Pérdida de la información	Compromiso de la información. Accidental.	true	false	false	true
Pérdida de los registros	Compromiso de la información. Accidental, deliberado.	true	false	false	true
Pérdida de servicio de comunicaciones de datos	Pérdida de servicios esenciales. Accidental, deliberado, ambiental.	true	false	false	true
Pérdida de servicio de comunicaciones de voz	Pérdida de servicios esenciales. Accidental, deliberado, ambiental.	true	false	false	true
Pérdida de suministro eléctrico	Pérdida de servicios esenciales. Accidental, deliberado, ambiental.	true	false	false	true
Pérdida o corrupción de la información	Acciones no autorizadas. Deliberado.	true	false	true	true
Polvo, humedad, corrosión	Daño físico. Ambiental.	true	false	false	true
Recuperación de medios reciclados o descartados	Compromiso de la información. Deliberado.	true	true	false	true
Revelación de contraseñas	Compromiso de la información. Accidental, deliberado.	true	true	true	false

Amenaza	Descripción	Global	Confidencialidad	Integridad	Disponibilidad
Revelación de información	Compromiso de la información. Accidental, deliberado.	true	true	false	false
Robo de documentación	Compromiso de la información. Deliberado.	true	true	false	true
Robo de equipamiento	Compromiso de la información. Deliberado.	true	true	false	true
Robo de información	Compromiso de la información. Deliberado.	true	true	false	true
Saturación de los sistemas de información	Fallos técnicos. Accidental, deliberado.	true	true	true	true
Suplantación de identidad	Compromiso de las funciones. Deliberado.	true	true	true	true
Terremoto	Evento natural. Daño físico. Ambiental.	true	false	false	true
Uso de código fuente no autorizado	Compromiso de la información. Accidental, deliberado.	true	true	true	true
Uso de sistemas por usuarios no autorizados	Compromiso de las funciones. Deliberado.	true	true	true	true
Uso no autorizado de equipos	Acciones no autorizadas. Deliberado.	true	true	true	true
Uso no autorizado de instalaciones de procesamiento	Compromiso de la información. Deliberado.	true	true	true	true

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

El Responsable de Seguridad utilizará la información contenida en la siguiente tabla para evaluar cada vulnerabilidad en función del grado de cumplimiento de los controles que la mitigan, según guías de implantación UNE-ISO/IEC 27002:2005.

Tabla 25 Método de evaluación de vulnerabilidades

Vulnerabilidad	Descripción	Justificación
5	La vulnerabilidad ha sido explotada en el pasado, más allá del nivel de implantación del control.	No requiere
4	Es muy probable que la vulnerabilidad sea explotada en el futuro ya que el control no se ha implantado.	No requiere
3	Es probable que la vulnerabilidad sea explotada en el futuro, ya que el control se ha implantado parcialmente.	Requiere
2	Es poco probable que la vulnerabilidad sea explotada en el futuro, ya que el control está implantado.	Requiere
1	Es muy improbable que la vulnerabilidad sea explotada, ya que el control está implantado y auditado.	Requiere
0	La vulnerabilidad no aplica al activo, por lo que el control no se aplica.	Requiere

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Tabla 26 Descripción de vulnerabilidades

Vulnerabilidad	Descripción	Global
Acceso remoto no seguro	Software. Red.	True
Arquitectura de red no segura	Red.	True
Asignación errónea de derechos de acceso	Software.	True
Cableado desprotegido	Información.	True
Capacitación en seguridad insuficiente	Personal.	True
Comunicaciones a través de redes públicas o desprotegidas	Información.	True
Conexiones a red pública desprotegidas	Información. Software.	True
Configuración de parámetros errónea.	Software.	True
Configuraciones incorrectas	Físicos. Software.	True
Control de acceso al edificio y a las salas ineficiente	Físicos.	True
Descargas y uso de software no controlados	Software.	True
Eliminación o reutilización de soportes sin borrar	Información. Software.	True
Equipos de comunicaciones desprotegidos	Físicos. Red.	True
Error en la fecha	Software.	True
Especificaciones para desarrolladores incompletas o confusas	Software.	True
Exposición a humedad, polvo, suciedad	Físicos.	True
Exposición a temperaturas extremas	Físicos.	True
Fallos conocidos en versiones	Software.	True
Falta puesta protección a tierra	Físico	True
Frecuencia de cambio de contraseñas insuficiente	Software.	True
Gestión de actualizaciones de seguridad ineficiente	Software.	True
Gestión de cambios ineficiente	Físicos. Software.	True
Gestión de contraseñas débil	Software.	True
Gestión de políticas de seguridad de la información insuficiente	Procesos.	True
Gestión de red ineficiente	Red. Software.	True
Gestión del control de acceso ineficiente	Software. Personal.	True
Gestión inadecuada de terceras partes	Personal.	True
Gestión ineficiente de contraseñas	Software.	True
Habilitación de servicios innecesarios	Software.	True
Inicio de sesión inseguro	Software.	True
Instalación desprotegida	Físicos.	True
Interfases de usuarios complejas	Software.	True
Mala instalación de medios de almacenamiento	Físicos.	True
Mantenimiento insuficiente	Físicos.	True
No existe asignación de responsabilidades relacionadas a la seguridad de la información	Personal.	True
No existe cambio sobre cuentas y contraseñas de fábrica	Software.	True
No existe concienciación y formación en seguridad	Personal.	True

Vulnerabilidad	Descripción	Global
No existe contacto con otras organizaciones y grupos de interés	Procesos.	True
No existe control de cambios en configuraciones	Físicos. Software.	True
No existe control de entrada y salida de datos	Software.	True
No existe control de los activos fuera de las instalaciones	Físicos. Personal.	True
No existe control de procesamiento de datos	Software.	True
No existe control para copia de información	Información.	True
No existe control sobre el uso de shareware o freeware	Software.	True
No existe control sobre el uso de utilidades de sistema	Software.	True
No existe protección en puertas y ventanas	Físicos.	True
No existe documentación	Software. Procesos.	True
No existe esquema de reemplazo periódico	Físicos.	True
No existe evaluación de riesgos en el plan de continuidad	Procesos.	True
No existe generador o sistema de alimentación ininterrumpida	Físicos.	True
No existe gestión de activos	Físicos.	True
No existe identificación del remitente o receptor del mensaje	Procesos.	True
No existe plan de continuidad	Procesos.	True
No existe política de control de accesos	Información. Software.	True
No existe política de controles criptográficos	Software. Procesos.	True
No existe política de puesto de trabajo y pantallas limpias	Personal.	True
No existe procedimiento para el control de cambios	Físicos. Software. Servicios.	True
No existe procedimiento para la gestión de incidencias de seguridad	Procesos.	True
No existe protección contra código malicioso	Software.	True
No existe protección contra código malicioso	Información.	True
No existe revisión de la política de seguridad	Procesos.	True
No existe separación de entornos de prueba y operación	Software.	True
No existe separación de funciones	Personal. Procesos.	True
No existe sistema estabilizador de tensión	Físicos.	True
No existe supervisión de los empleados que trabajan fuera de horario de oficina	Personal.	True
No existe supervisión de terceros dentro de la organización	Personal.	True
No existe un comité de seguridad	Procesos.	True
No existe una política de seguridad de alto nivel	Procesos.	True
No existen acuerdos de calidad de servicio (SLA)	Servicios.	True
No existen acuerdos de confidencialidad	Personal.	True
No existen auditorías regulares	Información. Software.	True
No existen equipos de detección de incendios	Físicos.	True

Vulnerabilidad	Descripción	Global
No existen equipos de extinción de incendios	Físicos.	True
No existen mecanismos de autenticación y validación del usuario	Software.	True
No existen mecanismos de monitorización	Personal.	True
No existen políticas para el correcto uso de telecomunicaciones	Personal.	True
No existen políticas para el uso de dispositivos portátiles	Físicos. Personal.	True
No existen procedimiento para devolución de activos	Físicos. Personal.	True
No existen procedimiento para eliminar permisos de acceso	Personal. Procesos.	True
No existen procedimientos de autorización de sistemas para producción	Físicos. Software.	True
No existen procedimientos de autorización para la información pública	Información.	True
No existen procedimientos de copia de seguridad	Información.	True
No existen procedimientos de monitorización de las instalaciones	Físicos.	True
No existen procedimientos de pruebas para el plan de continuidad	Procesos.	True
No existen procedimientos de tratamiento de la información	Información. Procesos.	True
No existen procedimientos formales de revisión de accesos	Información. Software. Procesos.	True
No existen procedimientos formales para alta y baja de usuarios	Información. Software. Procesos.	True
No existen procedimientos para cumplimiento de la propiedad intelectual	Software. Personal.	True
No existen procedimientos para el etiquetado y manejo de la información	Información.	True
No existen procedimientos para identificación y tratamiento de riesgos	Procesos.	True
No existen procedimientos para la comunicación de incidentes de seguridad de la información	Personal.	True
No existen procesos disciplinarios claros para incidentes de seguridad de la información	Personal.	True
No existen registros de auditoría	Software.	True
No existen registros de auditoría al enviar o recibir mensajes	Procesos.	True
No existen reportes sobre la actividad de los administradores y operadores	Personal.	True
No existen requisitos de seguridad de la información en planes de continuidad	Procesos.	True
No existen requisitos de seguridad en contratos con terceros	Procesos.	True
No existen requisitos de seguridad en contratos de empleados	Personal.	True
No existen responsabilidades de seguridad de la información en puestos de trabajo	Personal.	True
Personal clave de seguridad no disponible	Personal.	True

Vulnerabilidad	Descripción	Global
Personal disconforme o desmotivado	Personal.	True
Planificación y monitorización de capacidad inadecuada	Físicos. Software. Personal. Red. Servicios.	True
Proceso de contratación ineficiente	Personal.	True
Protección de claves criptográficas insuficiente	Software.	True
Pruebas de software insuficientes	Software.	True
Puesto de trabajo desatendido con sesión abierta	Software.	True
Punto único de fallo	Físicos. Red.	True
Respuesta inadecuada del servicio de mantenimiento	Físicos. Software.	True
Segregación de redes inapropiadas	Físicos. Red.	True
Segregación de redes inapropiadas	Red.	True
Selección de datos de prueba erróneos	Software.	True
Sistemas nuevos o inmaduros	Software.	True
Susceptibilidad a inestabilidad de voltajes	Físicos.	True
Susceptibilidad a inestabilidad térmica	Físicos.	True
Susceptibilidad a polvo, humedad.	Físicos.	True
Tabla de contraseñas desprotegidas	Software.	True
Tráfico de red especialmente sensible desprotegido	Red.	True
Transferencia de contraseñas en claro	Información. Software.	True
Ubicaciones susceptibles a inundación	Físicos.	True
Uso incorrecto de equipos	Físicos.	True
Uso incorrecto de software	Software.	True
Uso no aceptable de activos	Físicos. Software.	True
Uso soportes removibles no controlado	Información. Físicos.	True
Violación de la legislación aplicable	Procesos.	True

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Determinación del nivel de riesgo

Para determinar el valor del nivel de riesgo de los activos de información de la organización debidamente clasificados se obtiene por medio del resultado de multiplicar el valor del activo por el nivel de amenaza por la probabilidad de la vulnerabilidad como se puede visualizar a continuación:

Valor del Activo * Amenaza * Vulnerabilidad = Nivel de Riesgo

El valor de los activos de información es estático, tal y como lo han determinado los propietarios de dichos activos. Anualmente se revisará esta valoración sobre activos existentes por si la pérdida de alguno de sus atributos representase un impacto mayor por cambios en el sistema, por ejemplo, debido a nuevas regulaciones legales o contractuales. La metodología de evaluación de riesgos consiste en comparar las medidas de seguridad implantadas actualmente con los controles de seguridad de la información establecidos en la norma UNE-ISO/IEC 27001:2007 e identificar y gestionar las vulnerabilidades existentes o potenciales en los procesos y sistemas de información de la organización.

	Nivel de Amenaza	1					2					3				
	Nivel de Vulnerabilidad	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Valor del Activo	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75
		Nivel de Riesgo														

Figura 16 Determinación nivel de riesgo

Autor: (Alvarez Zurita, García Guzman, Flores, Oidor González, & Carlos, 2017)

Los datos reflejados en la tabla anterior se interpretarán de la siguiente manera:

Tabla 27 Descripción nivel de riesgo

Nivel de Riesgo	Descripción
1 – 24	No es necesario adoptar ninguna medida. El nivel de riesgo es suficientemente bajo y no justifica la implantación de controles adicionales.
25 – 48	La dirección de la empresa, o un delegado de esta, determinará el nivel de los riesgos que son aceptables o no a su juicio.
49 – 75	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la dirección de la empresa. El Responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

Gestión del riesgo

Se establecen cuatro métodos para la gestión de riesgos:

- Aceptar.
- Tratar.
- Transferir.
- Evitar.

Aceptar el riesgo

La Dirección puede aceptar riesgos que no tratará de ninguna manera en los casos que:

- El riesgo sea menor o igual al nivel de riesgo aceptable.
- El costo de tratar el riesgo sea mayor que el daño que pueda causar su impacto.
- El costo de tratar el riesgo no pueda ser asumido económicamente por la empresa. En este caso deberán considerarse opciones adecuadas al presupuesto para el tratamiento, aunque no sean las idóneas.

Para cualquiera de estas situaciones, se justificará debidamente las razones por las que el riesgo se acepta.

Tratar el riesgo

La Dirección decidirá, a su juicio, la prioridad en la implantación de las medidas de tratamiento de riesgo, en proporción al nivel de riesgo, la facilidad de la implantación, el costo o a los cambios en la organización.

1. Riesgo ALTO: Si el nivel de riesgo resultante para un activo es igual o superior a 49, la Dirección se remitirá a la norma UNE-ISO/IEC ISO 27001:2007 **Anexo A** para seleccionar los objetivos de control y controles que mitiguen el riesgo a un nivel aceptable y que encajen con los requisitos establecidos por la organización. En relación a los activos y a sus vulnerabilidades/amenazas asociadas, se implantarán todos los controles adicionales que tengan un efecto positivo en el negocio o en los procesos existentes y cuyo costo sea aceptable.
2. Riesgo MODERADO: El Comité de Seguridad puede aceptar un riesgo con un nivel entre 25 y 49 por cualquiera de las razones expuestas a continuación:

    a) El control o el proceso asociado no está alineado con la cultura de la organización.

    b) El personal necesario para su operación no está disponible.

    c) Los recursos económicos necesarios no están disponibles.

    d) No existe un beneficio claro para la organización.

    e) El costo de implantación del control supera el costo del activo que protege o el costo de una brecha de seguridad actual o futura.

    La aceptación del riesgo debe quedar documentada en las actas de reunión del Comité de Seguridad, en caso de no aceptación del riesgo, se actuará, como se indica para el caso de riesgo ALTO, seleccionando los procedimientos, mejores prácticas y mecanismos que mitiguen el riesgo a un nivel aceptable.

3. Riesgo BAJO: Los niveles de riesgo entre 1 y 24 son bajos y no requieren actuación ninguna.

    Se determina que un riesgo ALTO es inaceptable para la organización, a menos que así lo decida la Dirección y sobre el que dependa la propiedad

y el derecho de uso del activo afectado mediante la justificación de dicha decisión.

Transferir el riesgo

Cuando sea conveniente, la organización podrá transferir el riesgo a otras entidades. El Responsable de Seguridad es el responsable de asegurarse de que las responsabilidades que han sido transferidas son proporcionales al riesgo y de que sus colaboradores, proveedores o socios de negocio están conscientes de dichas responsabilidades. En caso de optar por transferir un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas por el Responsable de Seguridad de la Información. Las responsabilidades transferidas se reflejarán en acuerdos de nivel de servicio.

Se registrarán las actuaciones llevadas adelante en la transferencia de los riesgos.

Evitar el riesgo

La organización también puede optar por evitar el riesgo cesando un proceso o actividad o modificando la forma en que este se lleva a cabo. En caso de optar por evitar un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas por el responsable de seguridad, si el proceso o actividad son modificados, deberá realizarse el análisis de riesgos para el proceso o actividad modificada, no así en caso de cese del mismo.

Aceptación del riesgo residual

Como se ha definido, el riesgo residual para cualquiera de los activos y una vez aplicados las medidas de control previstas deberían situarse en un rango de valores por debajo del valor de riesgo aceptable determinado por la dirección de la empresa.

Para aquellos casos en que, tras el tratamiento con los controles previstos, se determine un nivel de riesgo moderado, se deberá obtener la aprobación de la Dirección para aceptar el riesgo residual resultante, lo que se documentará mediante Acta de reunión del Comité de Seguridad.

Tabla 28 Vulnerabilidad Residual

Vulnerabilidad Residual	Descripción	Justificación
3	La vulnerabilidad residual es parcial ya que el activo ha sido evaluado metodológicamente y se ha decidido aceptar su riesgo.	No Requiere
2	Es poco probable que la vulnerabilidad residual sea explotada en el futuro, ya que el conjunto de controles estará implantado.	No Requiere
1	Es muy improbable que la vulnerabilidad residual sea explotada, ya que el conjunto de controles estará implantado y auditado.	No Requiere
0	La vulnerabilidad residual no aplica al activo porque la amenaza no aplica, o porque el conjunto de controles no aplica (ver 4.3 Determinación de Amenazas y Vulnerabilidades).	No Requiere

Fuente: La institución encargada de regular cooperativas y asociaciones

Autor: José Neptali Molina Alcocer

3.6 REVISIÓN Y MONITOREO

El análisis de riesgos se repetirá con un intervalo anual, partiendo de los niveles de riesgo residual del análisis anterior teniendo en cuenta las incidencias, no conformidades, auditorías internas, nuevos requisitos de seguridad de las partes interesadas, cambios en la legislación, riesgos no contemplados, nuevos riesgos por cambios en los sistemas de información, indicadores de la efectividad de los controles implantados y el valor de riesgo aceptable definido por la dirección para el año se modifican los valores de vulnerabilidad en el nuevo análisis revisión del anterior. Esta revisión requiere información del ciclo de mejora continua del SGSI.

Si el valor de los riesgos que se obtienen a partir de este análisis excede el valor aceptable, se determina que controles es necesario implantar o reforzar, incluyendo sólo estos en el PTR asociado con este análisis de riesgos, definiendo el valor del riesgo residual tras su implantación.

Las revisiones podrán llevarse a cabo antes de la fecha prevista si hay factores determinantes que lo aconsejen. En cualquier caso, se tendrán en cuenta las situaciones que pueden requerir que se revise el análisis de riesgos incluyendo:

1. Cambios en la organización, los objetivos de negocio, los procesos o en el alcance del SGSI.
2. Cambios tecnológicos.
3. Cambios en las amenazas identificadas o en los requisitos externos (legales, contractuales).
4. Efectividad de los controles implantados.
5. Nuevos requisitos de seguridad de las partes interesadas.

Al cabo de 3 años, se debe realizar un nuevo análisis de riesgos completo. cada análisis realizado se guarda como registro y se realiza una comparación del valor de riesgo máximo anual de forma de representar la evolución del riesgo.

Seguimiento y Control

Debe elaborarse un mecanismo de control de cumplimiento de los planes de mitigación aprobados. Esto permitirá detectar desvío de información en forma temprana pudiendo alertar a los altos niveles directivos del impacto de estos en relación a la sensibilidad del activo que se desea proteger.

Para esto la Unidad de Seguridad de la Información deberá programar las siguientes actividades:

- Reuniones mensuales con las áreas propietarias para verificar la implementación de las estrategias de mitigación. Debe elaborar una matriz que indique la estrategia, el porcentaje de avance y la fecha de corte. Esto permitirá elaborar reportes estadísticos de los avances.
- Reuniones con el Comité de Seguridad para informar de los avances y el seguimiento respectivo.

Figura 17 Seguimiento y Control

Autor: José Neptali Molina Alcocer

CAPITULO IV

DISCUSIÓN

4.1 CONCLUSIONES

La institución encargada de regular cooperativas y asociaciones al generar información confidencial necesita un proceso de gestión de información: para el levantamiento de activos, clasificación de activos, evaluación de riesgos, identificación de amenazas y vulnerabilidades al que están expuesto. Evaluando la confidencialidad, integridad y disponibilidad con normas y reformas que cuenta la institución, para realizar de forma estructurada, sistemática y metodológica la gestión de la seguridad de la información.

Para la implementación de un estándar de la seguridad de la información basada en riesgos es necesario contar con una política de clasificación y etiquetado para gestionar de forma adecuada los activos de información basada en lineamientos, buenas prácticas y estándares internacionales de seguridad de la información, aplicando procedimientos integrados, eficientes y bajo una metodología de gestión basada en riesgos cumpliendo los lineamientos institucionales.

Para aplicar la política de clasificación y etiquetado de la información basada en riesgos es necesario identificar los procesos principales dentro de la institución donde se encuentren la mayor cantidad de actividades relacionadas con la gestión de información, lo que genera un grupo de activos importantes para realizar la evaluación de riesgos que permitirá garantizar el cumplimiento de atributos y responsabilidades del proceso.

Para garantizar una respuesta efectiva a incidencias de seguridad de la información, es necesario tener claro un proceso de notificación de incidencias que sea de conocimiento de todos los responsables del proceso a evaluar, para poder minimizar la probabilidad de ocurrencia.

La planificación es parte fundamental para una adecuada implementación de clasificación y etiquetado de la información, donde se analiza los procesos relevantes para determinar los activos más importantes de la institución encargada de regular cooperativas y asociaciones, posteriormente se realiza un análisis de riesgos identificando las amenazas y vulnerabilidades los cuales serán gestionados con controles apropiados.

En la institución encargada de regular cooperativas y asociaciones se considera que la tecnología, procesos y las personas forman un trípode que sostienen la seguridad de la información: las instituciones públicas comúnmente cuentan con grandes presupuestos para la implementación tecnológica y definición de procesos, descuidando el talento humano y transformándose en el pilar más débil de la cadena de seguridad, por lo que es fundamental motivar a las personas que se integren en la cultura de la seguridad de la información.

Al desarrollar una política para la clasificación y etiquetado de la información basado en riesgos, principalmente mediante el uso del conjunto de normas: ISO 27001:2013 y MAGERIT, posteriormente ISO 27002:2017 para generar mecanismos de control, se disminuyó considerablemente las inconsistencias en la gestión de la información de la institución encargada de regular cooperativas y asociaciones. La dirección de seguridad de la información expreso mediante un oficio su satisfacción por los resultados entregados con la investigación realizada.

4.2 RECOMENDACIONES

Realizar la identificación de activos de forma minuciosa teniendo claro el proceso que se va analizar, describiendo el nombre del activo, asignándole una calificación promedio de los factores de seguridad con el criterio del responsable del activo; para lograr mantener un inventario completo de activos y poder asignar una adecuada protección.

Es importante conocer el proceso que se va analizar para realizar el levantamiento de activos de forma minuciosa dentro de la institución, detallando el nombre del activo, descripción, ubicación, propietario y tipo de activo, posteriormente se calificara el activo según su confiabilidad, integridad y disponibilidad con la colaboración del propietario del activo y responsables del proceso. Si el levantamiento de información es eficaz todo el proceso de evaluación de riesgo será satisfactorio.

Se recomienda crear un comité de seguridad de la información el cual incrementará la protección de activos en las entidades públicas con políticas, gestión de los activos, seguridad de los recursos humanos, seguridad física y del entorno, control de accesos, gestión de los incidentes de la seguridad de la información y cumplimiento.

El activo al ser un bien tangible o intangible esencial para que funcione una empresa se recomienda la utilización de la norma ISO 27001:2013 para mejorar confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación acompañado de Magerit en el levantamiento de activos, y no verlo como un gasto sino como una inversión, ya que son muchos los beneficios obtenidos gracias a la aplicación de la norma.

La institución encargada de regular cooperativas y asociaciones genera una gran cantidad de activos de información por lo que se recomienda adquirir un SGSI (sistema de gestión de la información), para llevar un enfoque de riesgo de cada proceso que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información ayudando a la visualización y administración mejorando el desempeño en la institución

Es recomendable implementar un ciclo de mejora continua en los sistemas de gestión de la información. El Planificar, Hacer, Verificar y Actuar es una metodología que ha demostrado su aplicabilidad y ha permitido establecer cambios positivos en organizaciones de todas clases. La metodología cuenta una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización.

Bibliografía

Albacetev Giménez, J. F. (n.d.). *Seguridad en equipos informáticos MF0486_3*.

Alvarez Zurita, F. M., García Guzman, P. A., Flores, F., Oidor González, J. C., & Carlos, J. (2017). Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud, 298. Retrieved from http://repository.unad.edu.co/handle/10596/11907

Amutio Gómez, M. A. (2012). *MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. (Ministerio de Hacienda y Administraciones Públicas, Ed.) (Libro 1). España. Retrieved from http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Aragon, A. (2009). *Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços* (Brasport). Sao Paulo.

Asamblea, N. (2011). Ley Organica De Economia Popular Y Solidaria Del Sistema Financiero. *República Del Ecuador*, 1–39.

Aucapiña, T. V. G. (2012). Norma de Seguridad Informática ISO 27001, 162.

Congreso, N. (2004). LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. Quito- Ecuador.

Estrella, H. J. (2012). Resolución N°. SEPS_AD_SGE-2012-028. Quito- Ecuador.

Guerrero Julio, M. L., & Gómez Flórez, L. C. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Estudios Gerenciales*, *28*(125), 87–95. https://doi.org/10.1016/S0123-5923(12)70011-6

ISO/IEC. (2017). *ISO/IEC 27002:2017. Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información*. Madrid-España: Asociación Española de Normalización. Retrieved from https://www.iso.org/standard/54533.html

López, A. (2010). *Seguridad informática* (Editex).

Molina, M. F. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado*

en la Escuela Superior Politécnica del Litoral. Universidad Politécnica de Madrid Escuela.

Romo, D., & Valarezo, J. (2012). *Analisis e implementacio de la norma ISO 27002 para el departamento de sistemas de la Universidad Politecnica Salesiana sede Guayaquil*. Retrieved from http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

SEPS. (2017). Información Publica SEPS. Retrieved October 29, 2017, from http://www.seps.gob.ec

Solarte, N., Enriquez, E., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO / IEC 27001, *28*(Diciembre), 16.

Syalim, A., Hori, Y., & Sakurai, K. (n.d.). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.6972&rep=rep1&type=pdf

Tamayo Saenz, M. (1997). El Análisis de las políticas públicas. *La Nueva Administración Pública*, 2–22.

Varón Quiroga, J. C. (2017). Estudio de análisis y gestión de riesgo al sistema de información de la empresa Agesagro S.A.S utilizando la metodología Magerit. Retrieved from http://repository.unad.edu.co/handle/10596/11915

ANEXOS

Anexos A

Controles que mitiguen el riesgo a un nivel aceptable.

Numeración	Control	Descripción	Global
5.1.1	Políticas para la seguridad de la información	Se deben definir, aprobar por la dirección, publicar y comunicar a empleados y partes externas relevantes el conjunto de políticas para la seguridad de la información.	true
5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información deben revisarse a intervalos planificados o si existen cambios significativos para garantizar su eficacia, adecuación y conveniencia.	true
6.1.1	Roles y responsabilidades de la seguridad de la información	Se deben definir y asignar todas las responsabilidades sobre la seguridad de la información.	true
6.1.2	Segregación de tareas	Las responsabilidades y tareas que puedan entrar en conflicto deben segregarse para evitar oportunidades de modificación no autorizada o accidental o mal uso de los activos de la organización.	true
6.1.3	Contacto con las autoridades	Debe mantener contacto apropiado con autoridades relevantes.	true
6.1.4	Contacto con grupos de interés especial	Debe mantener contacto apropiado con grupos de interés especial u otros foros especializados en seguridad o asociaciones profesionales.	true
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe aplicarse en la gestión de proyectos, sin importar el tipo de proyecto.	true
6.2.1	Política de dispositivos móviles	Debe adoptarse una política y medidas de apoyo a la seguridad para gestionar el riesgo introducido por el uso de dispositivos móviles con acceso a la información del negocio.	true
6.2.2	Teletrabajo	Se debe implementar una política para proteger la información accedida, procesada y almacenada en sitios de teletrabajo.	true
7.1.1	Selección	Los antecedentes laborales de los candidatos a puestos de trabajo deben ser verificados de acuerdo a la legislación vigente, de acuerdo al requisito de negocio, la clasificación de la información y el riesgo percibido.	true
7.1.2	Términos y condiciones del puesto de trabajo	Los contratos con el personal y los proveedores deben establecer sus responsabilidades y la de la organización sobre la seguridad de la información.	true
7.2.1	Responsabilidades de la dirección	La dirección debe requerir al personal y a contratistas que apliquen la seguridad de la información de acuerdo a las políticas y procedimientos establecidos en la organización.	true

Numeración	Control	Descripción	Global
7.2.2	Concienciación, educación y capacitación de la seguridad de la información	Todo el personal y contratistas cuando resulte relevante, deben recibir concienciación y formación, y actualizaciones periódicas sobre las políticas y procedimientos, en relación a la seguridad de la información.	true
7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y ser comunicado al personal, para ser aplicado en el caso de que provoquen una brecha en la seguridad de la información.	true
7.3.1	Finalización o cambios en las responsabilidades del puesto de trabajo	Las responsabilidades y deberes que se mantengan tras la terminación de la relación con empleados o contratistas deben estar definidas, comunicadas y procurar su cumplimiento.	true
8.1.1	Inventario de activos	Los activos asociados a la información y a las instalaciones de procesamiento de información deben estar identificados e incluidos en un inventario.	true
8.1.2	Propiedad de los activos	Los activos incluidos en el inventario deben tener un propietario.	true
8.1.3	Uso aceptable de los activos	Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información, los activos y las instalaciones de procesamiento.	true
8.1.4	Devolución de los activos	Todo el personal y partes externas que tengan en su poder activos de la organización, deben devolverlos ante la finalización de su empleo, contrato o acuerdo.	true
8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad a modificación o revelación no autorizadas.	true
8.2.2	Etiquetado de la información	Se debe desarrollar e implementar procedimientos apropiados para el etiquetado de información de acuerdo al esquema de clasificación de la información establecido en la organización.	true
8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de la información establecido en la organización.	true
8.3.1	Gestión de medios removibles	Deben implementarse procedimientos para la gestión de los medios removibles de acuerdo al esquema de clasificación de la información establecido en la organización.	true
8.3.2	Desecho de medios	Los medios deben desecharse de manera segura cuando ya no tengan uso, mediante procedimientos formales.	true
8.3.3	Tránsito de medios físicos	Los medios que contengan información deben protegerse de accesos no autorizados, usos indebidos o daño durante el transporte.	true

Numeración	Control	Descripción	Global
9.1.1	Política de control de acceso	La organización debe establecer, documentar y revisar en base a los requisitos del negocio y de la seguridad de la información, una política de control de acceso.	true
9.1.2	Acceso a redes y servicios de red	El acceso a las redes y a los servicios de red deben otorgarse únicamente a los usuarios específicamente autorizados a utilizarlos.	true
9.2.1	Alta y baja de usuario	Debe implementarse un proceso formal de alta y baja de usuarios que permita la asignación de derechos de acceso a la información.	true
9.2.2	Provisión de acceso a usuarios	Debe implementarse un proceso formal de provisión para otorgar o retirar derechos de accesos a todos los tipos de usuarios sobre todos los sistemas de información.	true
9.2.3	Gestión de derechos de acceso privilegiado	Debe controlarse y restringirse la entrega y uso de derechos de acceso privilegiados.	true
9.2.4	Gestión de información secreta de autenticación	La ubicación de la información secreta de autenticación de los usuarios debe controlarse mediante un proceso formal de gestión.	true
9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar periódicamente los derechos de acceso de los usuarios.	true
9.2.6	Retirada o ajuste de los derechos de acceso	Los derechos de acceso a la información y a las instalaciones de procesamiento de información de empleados y partes externas deben ser retirados ante la finalización de la relación o modificados ante cambios de la misma.	true
9.3.1	Uso de información secreta de autenticación	El personal debe tener la responsabilidad de cumplir las prácticas definidas por la organización para el uso de la información secreta de autenticación.	true
9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de los sistemas de información debe estar restringido de acuerdo a la política de control de acceso.	true
9.4.2	Procesos de inicio seguro de sesión	Cuando sea requerido por la política de control de acceso, el acceso a los sistemas de información y aplicaciones deben estar controlados por procedimientos de inicio de sesión seguros.	true
9.4.3	Sistema de gestión de contraseña	El sistema de gestión de contraseña debe ser interactivo y garantizar la calidad de las mismas.	true
9.4.4	Uso de programas privilegiados de utilidad	El uso de aplicaciones utilitarias que puedan anular control de seguridad de los sistemas debe estar restringido y firmemente controlado.	true
9.4.5	Control de acceso a código fuente de programa	El acceso a código fuente debe estar restringido.	true
10.1.1	Política en el uso de controles criptográficos	Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.	True

Numeración	Control	Descripción	Global
10.1.2	Gestión de claves de criptografía	Una política sobre el uso, protección y duración de las llaves criptográficas deben desarrollarse e implementarse durante todo su ciclo de vida.	true
11.1.1	Perímetro de seguridad física	Deben definirse y utilizarse perímetros de seguridad para la protección de áreas que contengan información crítica o sensible e instalaciones de procesamiento de información.	true
11.1.2	Controles de acceso físico	Las áreas seguras deben protegerse por controles de entrada adecuados que otorguen acceso solo al personal autorizado.	true
11.1.3	Seguridad de oficinas, salas e instalaciones	Debe diseñarse y aplicarse seguridad física para oficinas, salas e instalaciones.	true
11.1.4	Protección contra amenazas externas y ambientales	Debe diseñarse y aplicarse seguridad para la protección física contra desastres naturales, ataques maliciosos o accidentes.	true
11.1.5	Trabajo en áreas seguras	Deben diseñarse y aplicarse procedimientos para el trabajo en áreas seguras.	true
11.1.6	Áreas de entrega y carga	Los puntos de acceso para entrega y carga de material, como cualquier otro punto vulnerable al acceso no autorizado deben ser controlado, y de ser posible aislado de las áreas de procesamiento de información.	true
11.2.1	Ubicación y protección de equipos	Los equipos deben ubicarse y protegerse para reducir el riesgo de amenazas ambientales y de accesos no autorizados.	true
11.2.2	Servicios de suministro	Los equipos deben estar protegidos contra fallas de alimentación eléctrica y otros fallos de suministro.	true
11.2.3	Seguridad del cableado	El cableado de potencia que alimente los sistemas y de comunicaciones que transporte información debe protegerse de intercepciones, interferencias o daños.	true
11.2.4	Mantenimiento de equipos	Los equipos deben ser correctamente mantenidos para garantizar su disponibilidad e integridad.	true
11.2.5	Retirada de activos	El equipamiento, aplicaciones e información no deben llevarse fuera de las instalaciones seguras sin la debida autorización.	true
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Debe aplicarse la seguridad sobre equipos fuera de las instalaciones considerando los diferentes riesgos del trabajo fuera de las instalaciones de la organización.	true
11.2.7	Seguridad en el desecho o reutilización de equipos	Los elementos de equipamiento que contengan medios de almacenamiento de información deben ser verificados para asegurar la eliminación o sobreescritura de información sensible, licencias antes de su desecho o reúso.	true
11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurar que sus equipos tengan apropiada protección cuando queden desatendidos.	True

Numeración	Control	Descripción	Global
11.2.9	Política de pantalla y escritorio despejado	Una política de escritorio despejado de papeles y medio removibles y de pantalla de equipos de procesamiento limpia debe definirse y adoptarse.	True
12.1.1	Procedimientos operativos documentados	Los procedimientos de operación deben estar documentados y puestos a disposición de los usuarios que los necesiten.	True
12.1.2	Gestión del cambio	Deben controlarse los cambios en la organización, en los procesos de negocio, en las instalaciones de procesamiento y sistemas, cuando afecten a la seguridad de la información.	True
12.1.3	Gestión de la capacidad	Debe monitorizarse, ajustarse y proyectarse los requisitos futuros de capacidad del uso de los recursos para garantizar su correcto desempeño.	True
12.1.4	Separación de entornos de desarrollo, prueba y operación	Los entornos de desarrollo, prueba y operación deben estar separado para reducir el riesgo de accesos no autorizados o cambios sobre el entorno de operaciones.	True
12.2.1	Controles contra código malicioso	Deben implementarse controles de detección, prevención y recuperación contra código malicioso, combinados con la debida concienciación de los usuarios.	True
12.3.1	Copia de seguridad de la información	Copias de seguridad de la información, los sistemas, imágenes deben realizarse y probadas de forma regular de acuerdo a la política de copia de seguridad de la organización.	true
12.4.1	Registro de eventos	Deben producirse, mantenerse y revisarse periódicamente los registros de la actividad de los usuarios, los fallos en los sistemas y los eventos de seguridad.	true
12.4.2	Protección de la información del registro de eventos	Las instalaciones de registro y la información de registros deben protegerse contra manipulación y accesos no autorizados.	true
12.4.3	Registro de administrador y operador	La actividad de los administradores y operadores de sistemas debe registrarse, protegiendo estos registros y revisándolos periódicamente.	true
12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información relevantes, ya sea de la organización o del dominio de seguridad, deben sincronizarse respecto de una única fuente.	true
12.5.1	Instalación de programas en sistemas en producción	Deben implementarse procedimientos para controlar la instalación de aplicaciones en sistemas en operación.	true
12.6.1	Gestión de vulnerabilidades técnicas	La información sobre vulnerabilidades técnicas sobre los sistemas de la organización debe ser obtenida tan pronto como esté disponible de manera de evaluar la exposición y aplicar medidas apropiadas para reducir riesgos.	true
12.6.2	Restricciones en la instalación de programas	Deben establecerse e implementarse reglas que controlen la instalación de aplicaciones por parte de los usuarios.	true

Numeración	Control	Descripción	Global
12.7.1	Controles de la auditoría de sistemas de información	Los requisitos y actividades de auditoría que involucren la verificación de sistemas en producción deben planificarse cuidadosamente y estar acordados para reducir interrupciones sobre los procesos de negocio.	true
13.1.1	Controles de red	Las redes deben gestionarse y controlarse para proteger la información de sistemas y aplicaciones.	true
13.1.2	Seguridad de servicios de red	Los requisitos gestión, nivel de servicio y mecanismos de seguridad sobre todos los servicios de red deben estar identificados y ser incluidos tanto sean servicios internos o externos.	true
13.1.3	Segregación de redes	Deben segregarse los grupos de servicios de información, sistemas de información y usuarios en redes.	true
13.2.1	Políticas y procedimientos para el intercambio de información	Deben aplicarse políticas, procedimientos y controles formales para proteger la transferencia de información a través de cualquier tipo de medio de comunicación.	true
13.2.2	Acuerdos de intercambio de información	Deben definirse acuerdos que atiendan la seguridad sobre la transferencia de información del negocio entre la organización y las partes externas.	true
13.2.3	Mensajería electrónica	La información incluida en mensajería electrónica debe ser protegida de forma apropiada.	true
13.2.4	Acuerdos de confidencialidad y no divulgación	Debe identificarse, revisarse regularmente y documentarse los requisitos de confidencialidad y no divulgación de la organización sobre la protección de la información del negocio.	true
14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	Los requisitos relacionados con la seguridad de la información deben incluirse para los nuevos sistemas de información o para la mejora de sistemas existentes.	true
14.1.2	Seguridad del servicio de aplicación en redes públicas	La información trasmitida por aplicaciones o servicios a través de redes públicas debe ser protegida de actividades fraudulentas, disputas contractuales y modificación o divulgación no autorizada.	true
14.1.3	Protección de transacciones en servicio de aplicación	La información involucrada en transacciones de servicios debe ser protegida para evitar transmisiones incompletas, ruteo erróneo, así como alteración, revelación, duplicación y repetición no autorizadas.	true
14.2.1	Política de desarrollo seguro	Deben establecerse y aplicarse reglas al desarrollo de sistemas de información en la organización.	true
14.2.2	Procedimiento de control de cambio en sistemas de información	Los cambios sobre los sistemas de información durante su ciclo de vida deben estar controlados mediante procedimientos formales de control de cambio.	true

Numeración	Control	Descripción	Global
14.2.3	Revisión técnica de las aplicaciones ante cambios en la plataforma de operación	Cuando las plataformas operativas sufran cambios, las aplicaciones críticas de negocio deben ser revisadas y probadas para garantizar que no existen impactos adversos sobre la operación o la seguridad de la información.	true
14.2.4	Restricciones en cambios a paquetes de aplicaciones	La modificación de paquetes de aplicaciones debe restringirse y limitarse únicamente a cambios necesarios y estos deben ser controlados de forma estricta.	true
14.2.5	Principios para la ingeniería de sistemas seguros	Deben establecerse principios para la ingeniería de sistemas seguros, que sean documentados, mantenidos y aplicados a los esfuerzos de la organización para la implementación de cualquier sistema de información.	true
14.2.6	Entorno seguro de desarrollo	La organización debe establecer y proteger los entornos seguros de desarrollo que cubran todo el ciclo de vida.	true
14.2.7	Desarrollo externalizado	La organización debe supervisar y monitorizar las actividades de los proveedores de los desarrollos externalizados.	true
14.2.8	Pruebas de seguridad del sistema	Las pruebas de seguridad funcional de las aplicaciones deben ser llevadas adelante durante el período de desarrollo.	true
14.2.9	Pruebas de aceptación del sistema	Deben definirse y establecerse programas de pruebas y criterios de aceptación para nuevos sistemas de información, nuevas versiones y actualizaciones.	true
14.3.1	Protección de la información de prueba	Los datos de prueba deben ser seleccionados, cuidadosamente, estar protegidos y controlados.	true
15.1.1	Política de seguridad en la relación con proveedores	Los requisitos de seguridad de la información para reducir riesgos asociados con el acceso de proveedores a los activos de la organización, deben acordarse y documentarse.	true
15.1.2	Seguridad en el acuerdo con proveedores	Todos los requisitos de seguridad de la información relevantes deben definirse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar información y proveer infraestructuras IT.	true
15.1.3	Tecnología de la información y comunicación en la cadena de suministro	Los acuerdos con proveedores deben incluir requisitos que reduzcan los riesgos asociados a la información, tecnologías de la comunicación y cadena de suministros.	true
15.2.1	Monitorización y revisión de la provisión de servicios	La organización debe monitorizar, revisar y auditar la provisión de servicios regularmente.	true
15.2.2	Gestión de cambios en la provisión de servicios	Los cambios en la provisión de servicio, incluyendo el mantenimiento y mejoras de las políticas, procedimientos y procesos de seguridad de la información existentes, deben gestionarse considerando la evaluación de riesgos.	true

Numeración	Control	Descripción	Global
16.1.1	Responsabilidades y procedimientos	Deben establecerse las responsabilidades de la dirección y sobre los procedimientos para garantizar una respuesta rápida, eficaz y ordenada ante incidencias de seguridad de la información.	true
16.1.2	Reporte de eventos sobre la seguridad de la información	Los incidentes de seguridad de la información deben ser reportados tan pronto como sea posible a través de canales de comunicación debidamente gestionados.	true
16.1.3	Reporte de debilidades en la seguridad de la información	El personal y los contratistas que utilicen los sistemas de información y los servicios de la organización deben ser responsables de notificar cualquier debilidad en la seguridad que observen o de la que sospechen.	true
16.1.4	Valoración y decisión sobre los eventos de seguridad de la información	Los eventos en la seguridad de la información deben ser evaluados para determinar si serán clasificados como incidencias de seguridad de la información para ser gestionados de forma adecuada.	true
16.1.5	Respuesta a los incidentes de seguridad de la información	Las incidencias de seguridad de la información deben tener una respuesta acorde a los procedimientos documentados a tal fin.	true
16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido de análisis y la resolución de los incidentes de seguridad de la información debe ser utilizado para procurar reducir la probabilidad y el impacto de incidencias futuras.	true
16.1.7	Recolección de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que pueda servir de evidencia.	true
17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe definir los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información ante situaciones adversas.	true
17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener los procesos y procedimientos para garantizar el nivel requerido de continuidad de seguridad de la información durante situaciones adversas.	true
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar la continuidad de la seguridad de la información establecida e implementada a través de los controles en intervalos regulares para garantizar su validez y efectividad.	true
17.2.1	Disponibilidad de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben tener una redundancia suficiente para contar con sus requisitos de disponibilidad.	true

	Control	Descripción	Global
18.1.1	Identificación de legislación aplicable y requisitos contractuales	Deben identificarse de forma explícita, documentarse y mantenerse actualizados todos los requisitos legales, regulatorios, contractuales relevantes para cada sistema de información y la operación de la organización.	true
18.1.2	Derechos de propiedad intelectual	Deben implementarse procedimientos apropiados para asegurar el cumplimiento de requisitos legales, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de sistemas de información.	true
18.1.3	Protección de registros	Los registros deben protegerse de pérdida, destrucción, falsificación y acceso no autorizado de acuerdo a requisitos legales, regulatorios, contractuales y de negocio.	true
18.1.4	Privacidad y protección de información de identificación personal	La protección de la privacidad de la información de identificación personal debe aplicarse de acuerdo a la legislación aplicable.	true
18.1.5	Regulación de controles de criptografía	Los controles criptográficos deben utilizarse de acuerdo a los acuerdos, legislación y regulaciones relevantes.	true
18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización con la seguridad de la información (objetivos de control, controles, políticas, procedimientos y procesos) deben revisarse de manera independiente en períodos planificados o ante cambios.	true
18.2.2	Cumplimiento de políticas y normas de seguridad	Los responsables de áreas de negocio deben identificar como revisar el cumplimiento del procesamiento de la información y procedimientos de seguridad, de acuerdo a políticas, estándares y requisitos de seguridad.	true
18.2.3	Revisión de cumplimiento técnico	Los sistemas de información deben ser revisados periódicamente para garantizar el cumplimiento de las políticas y estándares de seguridad de la información.	true

Anexo B

ENTREVISTA

Los datos generados por la entrevista determinarán las condiciones en la clasificación de la información basada en riesgos en la institución encargada de regular cooperativas y asociaciones.

Nombre: _____

Cargo: _____

1. **¿Cuentan con políticas de seguridad para la información?**

SI ☐ Enúncielas; NO ☐

……
……
……

2. ¿Cómo se maneja el control de la seguridad de la información? ☐ Estrategias de negocio
☐ Normativas y contratos
☐ Políticas de seguridad de la información
☐ Asignación de responsabilidades
☐ Otros

_____

3. ¿Describa el control interno que realiza el área responsable en la seguridad de la información?

☐ Análisis de requisitos y especificaciones de seguridad de la información
☐ Aseguramiento de los servicios de aplicaciones en redes publicas
☐ Protección de las transacciones de servicios de aplicación
☐ Otros _____

4. ¿La institución cuenta con un Sistema de Gestión de seguridad de la Información (SGSI)?

SI ☐ Describir; NO ☐

……
……

5. ¿Cómo se garantiza la confiabilidad, integridad y disponibilidad de la información que se genera dentro de la institución?

☐ Planificación de la continuidad de la seguridad de la información
☐ Implementación de la comunidad de la seguridad de la información

☐ Revisión y evaluación de la comunidad de la seguridad de información.
☐ Otros _____

6. ¿Qué mecanismos, técnicas y/o herramientas de seguridad se aplican para salvaguardar la información confidencial?

☐ Identificación de las causas de incumplimiento.
☐ Evaluación de acciones necesarias para el cumplimiento.
☐ Implementación de acciones correctivas necesarias.
☐ Revisión de acciones correctivas y verificar su efectividad.

7. ¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?

SI ☐ Describir; NO ☐

……
……

8. ¿Cómo se realiza el monitoreo a los sistemas de información y de comunicación?

☐ Revisión independiente de la seguridad de la información
☐ Cumplimiento de las políticas y normas de seguridad
☐ Comprobación del cumplimiento técnico
……
……

9. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si……De qué manera se lo ha realizado; No……Por qué?

……
……
……
……
……

Anexo C

Carta de auspicio

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

OFICIO No. SEPS-SGD-SEPS-DNSI-2017-21315

Quito, D.M., 25 de agosto de 2017

Ing
Juan Grijalva
Facultad de Arquitectura e ingenierías
UNIVERSIDAD INTERNACIONAL SEK
Alberto Einstein s/n 5ta Transversal
Fono: 023974800 / 0987057359
Quito, Pichincha

Asunto: Administración de proyectos y servicios tecnológicos

De mi consideración:

En respuesta al trámite SEPS-UIO-2017-001-49960, donde se solicita el permiso para que el Sr. Ing. José Neptalí Molina Alcócer, realice su proyecto de tesis titulado " ", cuya aceptación implica permitir al mencionado realizar los levantamientos de procesos e información requeridos, bajo los esquemas de confidencialidad establecidos por la SEPS; se comunica que, con base el compromeitimiento de la SEPS con la comunidad expresado en nuestro Plan Estratégico Institucional que menciona: "Implementar un sistema de gestión de seguridad de la información" dentro del pilar estratégico de ciudadanía, se ha considerado dar la apertura para que el Sr. Ing. José Neptalí Molina Alcócer desarrolle su proyecto de tesis en la SEPS.

En consecuencia el tesista deberá acogerse a la normativa institucional y reglamentos que regulan el tratamiento de la información, además se deberá firmar un acuerdo de confidencialidad entre las partes que garantice el resguardo de la información.

Adicionalmente dicha tesis deberá ser clasificada con carácter de reservado de modo que no podrá ser publicada en la web ni sus versiones físicas extraídas de la universidad SEK. Este documento y todas sus copias deberán reposar con todas las seguridades que ameritan este caso bajo custodia de la máxima autoridad quien adicionalmente al Sr José Neptalí Molina, serán los únicos custodios por parte de la Universidad SEK.

Por parte de la SEPS, se recibirán dos copias, mismas que serán custodiadas por Secretaría General y por el Director Nacional de Seguridad de la Información, respectivamente.

Sin otro particular me suscribo.

1/2

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Atentamente,

Firmado electrónicamente por:
Cristian Fabián Aguirre Martínez
DIRECTOR NACIONAL DE SEGURIDAD DE LA INFORMACION
2017-08-25 09:22:00

DIRECTOR NACIONAL DE SEGURIDAD DE LA INFORMACION

2/2

Anexo D

Certificado de finalización de proyecto

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Quito 13 de junio del 2018

Señores
UNIVERSIDAD INTERNACIONAL SEK
Presente.

Asunto: "Finalización Proyecto"

De mis consideraciones:

Como es de su conocimiento el Ing. José Neptali Molina Alcocer portador de la cedula de identidad 1716454333, realizó su proyecto de tesis de la Maestria en Tecnologias de la Información con Mención en Seguridad de Redes y Comunicación denominado **"DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR"** en la SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, desde diciembre 2017 a junio 2018, el mismo que llegó a su etapa final cumpliendo los objetivos esperados por parte del maestrante.

De antemano agradecemos el tiempo y esmero que le dedico al proyecto

Sin otro particular me suscribo.

Atentamente,

Msg. Cristian Aguirre
Director Nacional de Seguridad de la Información
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Av. Amazonas y Mariana de Jesús • www.seps.gob.ec •contactenos@seps.gob.ec • (593) 2 394 88 40

Anexo E

Acuerdo de confidencialidad

Quito 20 de noviembre del 2017

ACUERDO DE CONFIDENCIALIDAD

Por la parte reveladora
Nombre: **Superintendencia De Economía Popular Y Solidaria**
Dirección: Av. Amazonas y Av. Mariana de Jesús
Teléfono: (593)23948840
E-mail: contactenos@seps.gob.ec

Por la parte receptora de la información
Nombre: **José Neptalí Molina Alcocer**
Dirección: Juan de Obando 454 y Pedro de Zumarraga
Teléfono: (593)984354160
E-mail: soi_solucoines@hotmail.com

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la **Superintendencia de Economía Popular y Solidaria,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo de una política para la gestión de la seguridad de la información.

2. Que la información de propiedad de la **Superintendencia de Economía Popular y Solidaria** ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación y por otro lado Ing. José Neptalí Molina Alcocer que, para el presente caso actual como **revelador, guarda y administrados de la información de propiedad de la Superintendencia de Economía Popular y Solidaria.**

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad, la parte receptora,** se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a la **Superintendencia de Economía Popular y Solidaria,** así como también a no utilizar dicha información en beneficio propio ni de terceros.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial,** para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios y/o cualquier otra relacionada con el **proyecto de investigación** lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma la **Superintendencia de Economía Popular y Solidaria**, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de la **Superintendencia de Economía Popular y Solidaria.**

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información como confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora**, esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la

inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo**. En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia.

Novena. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Como Parte Receptora:

Ing. José Molina

Estudiante de la Universidad Internacional Sek

Por la parte reveladora:

Firmado electrónicamente por:
CRISTIAN FABIÁN AGUIRRE MARTÍNEZ
DIRECTOR NACIONAL DE SEGURIDAD DE LA INFORMACION
2019-06-14 11:53:03

Msg. Cristian Aguirre

Director Nacional de Seguridad de la Información