República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Posgrado e Investigación

Tesis en opción al título de Magister en:

Sistemas de Información Gerencial

Tema de tesis:

Modelo de Gestión de la Seguridad de la Información adaptado a las Cooperativas de Ahorro y Crédito de la ciudad de Guayaquil.

Autor:

Ing. Carlos Eduardo Sánchez Paredes

Director de Tesis:

Ing. Xavier Mosquera

Agosto 2021

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

Yo, Carlos Eduardo Sánchez Paredes, declaro ser el autor exclusivo de esta tesis de posgrado y como tal me permito ceder los derechos a la Universidad Tecnológica Empresarial de Guayaquil UTEG.

Ing. Carlos Eduardo Sánchez Paredes

CI: 0930548409

Resumen

El presente trabajo tiene como objetivo contribuir con la optimización de los estándares de seguridad, a través de un modelo de gestión seguridad de información dirigido a un grupo de pequeñas cooperativas de ahorro y crédito que operan en la ciudad de Guayaquil. El mismo partió de una revisión bibliográfica, y un análisis situacional de estas cooperativas realizado a través de una matriz FODA, se aplicaron encuestas a un grupo de personas que poseen responsabilidad dentro de estas cooperativas. Los resultaron pusieron en evidencia que las principales dificultades afrontadas por estas organizaciones son infraestructura física y tecnológica insuficiente para proteger sus recursos, robo y alteraciones de la información y la inexistencia de sistemas aplicados para la seguridad de la información. Es por ello, que se desarrolló un modelo de sistema de seguridad de la información orientada a las cooperativas de ahorro y crédito de la ciudad de Guayaquil, el cual estuvo basado principalmente en la norma ISO 27001 con el propósito de establecer, implementar, operar, monitorear, revisar, mantener y mejorar la Seguridad de la Información. Es así como se espera que el modelo de gestión de seguridad de la información contribuya a establecer políticas y procedimientos relacionados con los objetivos comerciales de las cooperativas de ahorro y crédito de la ciudad de Guayaquil, para mantener niveles de exposición inferiores al nivel de riesgo que la propia organización pueda manejar y así garantizar que la seguridad de la información sea gestionada de forma correcta.

Palabras Clave: seguridad, información, modelo, gestión, cooperativas.

Abstract

The present objective is to contribute to the optimization of security standards, through an information security management model aimed at a group of small savings and credit cooperatives that operate in the city of Guayaquil. It started from a bibliographic review, situational analysis of these cooperatives, through a SWOT matrix, surveys were applied to a group of people who have responsibility within these cooperatives. The results showed that the main difficulties faced by these organizations are insufficient physical and technological infrastructure to protect their resources, theft and alteration of information and the lack of systems applied for information security. That is why an information security system model was developed aimed at savings and credit cooperatives in the city of Guayaquil, which was based mainly on the ISO 27001 standard with the purpose of establishing, implementing, operating, monitor, review, maintain and improve Information Security. This is how it is expected that the information security management model contributes to establishing policies and procedures related to the commercial objectives of the savings and credit cooperatives of the city of Guayaquil, to maintain exposure levels lower than the level of risk that the organization itself can manage and thus guarantee that information security is managed correctly.

Keywords: security, information, model, management, cooperatives.

ÍNDICE GENERAL

Índice de Tablas

Índice de Figuras

Índice de Anexos

INTRODUCCIÓN

Los sistemas informáticos llegaron para tomar posición en el mundo empresarial en relación con el desarrollo de los procesos comerciales. Tal es su presencia que este se ha ido incrementando a través del uso de diversos dispositivos electrónicos, a los que se puede tener acceso e intercambiar información, como transacciones, trasmisión de datos, etc., en tiempo real (Quiroz-Zambrano & Macías-Valencia, 2017).

En este contexto, el presente trabajo se enfoca en el desarrollo de un modelo de Gestión de Seguridad de Información dirigido a una muestra de Cooperativas de Ahorro y Crédito ubicadas en la ciudad de Guayaquil. Este modelo, se apoya en las orientaciones dadas por la Escuela Superior de Redes RED CEDIA, la cual establece un conjunto de orientaciones con adaptaciones al Estado ecuatoriano.

Además, se toman algunas referencias del Modelo de Seguridad y privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC de Colombia. En una apuesta por incorporar buenas prácticas desarrolladas en otros escenarios, cuyos procedimientos resultan de mucho valor como un marco de orientación. Y las referencias aportadas por (Moscaiza-Moncada, 2020); (Garcés, 2015).

Es importante destacar que el desarrollo de la gestión administrativa en la actualidad ha ido en franca aceleración, en la medida en la cual, las pequeñas empresas buscan calidad y excelencia en sus procesos administrativos, que les permita evolucionar con miras a lograr la eficiencia en cada uno de sus procesos. Dentro de estas organizaciones hacen presencia las Cooperativas de Ahorro y Crédito, las cuales, bajo su personalidad jurídica y propiedad social, establecen emprendimientos con sus socios para generar desarrollo en el país. Aunque, según algunos reportes por investigadores que se encuentran en líneas siguientes, estas estarían reportando algunas debilidades en sus sistemas de información.

Bajo este panorama, la información en cada una de estas organizaciones es actualmente un recurso clave, pues esta funciona como el mecanismo que permitirá a la empresa ser competitiva y mantenerse en el tiempo (Santamaría, 2017). En este sentido, la tecnología juega un papel clave en la creación, uso, almacenamiento, divulgación y destrucción de la información generada, eso la hace parte integral de todos los aspectos de la organización. Y esta perspectiva se basa en que la seguridad informática constituye en la actualidad un pilar esencial en la estabilidad de las empresas, no sólo de las Pymes sino cualquier tipo de empresa (Parra, 2014).

Por consiguiente, las organizaciones cada vez más se esfuerzan por garantizar que la tecnología brinde apoyo para ayudarlas a tomar decisiones y alcanzar objetivos estratégicos para minimizar el riesgo involucrado. Para este propósito, se requieren pautas de seguridad para regular la gestión adecuada de la copia de seguridad de la base de datos, la información contable, los datos administrativos, las copias de seguridad del correo electrónico y la información del usuario individual.

Es un requisito previo para que las instituciones logren una buena coordinación en el área de tecnología y la adapten a la estrategia institucional a través del cuadro de mando de Tecnología de Información (TI) y el ajuste de procesos que eviten que la información se vuelva vulnerable debido a la falta de pautas regulatorias. Para hacer esto, es importante analizar dentro del sistema de los riesgos de seguridad.

El presente trabajo se encuentra estructurado en cuatro capítulos:

En el primero se desarrolla todo el marco teórico conceptual sobre el cual parte y se sustenta la investigación. Este abarca los antecedentes de la investigación, formulación y sistematización del problema, la descripción y presentación del problema, los objetivos, y justificación del estudio. Los referentes empíricos o investigaciones afines al objeto que se investiga. Y el marco de referencia, compuesto por el teórico y el conceptual.

Seguidamente se presenta el capítulo dos. Este capítulo comprende el marco metodológico en el cual se expone el tipo, diseño, alcance y enfoque de la

investigación. Los métodos utilizados, las unidades de análisis la población y muestra seleccionada. Se presentan las variables, las fuentes y técnicas de investigación y los procedimientos que se llevaron a cabo para su desarrollo.

En el Capítulo tres se presentan los resultados generales del proceso de investigación realizada, así como su respectiva discusión, la cual comprende los análisis a cada una de las preguntas planteadas.

En el capítulo cuatro se encuentra la propuesta final como producto del estudio, con su respectiva presentación, justificación e importancia, propósito y desarrollo. Finalmente se presentan las conclusiones y recomendaciones.

CAPITULO I. MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes de la investigación

La seguridad de información en el mundo posee una larga data, esta puede ser tan antigua como la misma humanidad. Siendo diferente a los sistemas de gestión de información. En atención a este punto, la evolución de los sistemas de información y su seguridad empiezan a verse a finales del siglo XX. Especialmente en la postguerra, año 1969, cuando Peter Drucker introduce la llamada "sociedad del conocimiento", en la cual, se da valor al capital intelectual dentro del ámbito empresarial. Sin duda, uno de los hechos más importantes que condujo a la llamada Revolución Industrial (Chenche, 2020), o revolución de la denominada productividad de las economías, por cuanto el valor concedido al saber cómo factor productivo era esencial en el desarrollo industrial.

Bajo esta óptica, la sociedad del conocimiento se basaba en una gestión de la información física a través de ordenadores y mecanismos de almacenamiento de información, en la cual se pasaba por la seguridad de sistemas y redes de tecnologías de información, siendo posible a través de políticas y controles propios de cada empresa (Cárdenas-Solano, Martínez-Ardila, & Ardila, 2016).

En este sentido, a finales de la década de los años 80 en los EEUU, y principios de los 90, entran las tecnologías y el internet en los diferentes sectores y ámbitos de la sociedad, y con ella, todas sus implicaciones, como lo es la seguridad de sus procesos y su funcionamiento. Posteriormente, en el año 2000, se apreció el hecho de que las tecnologías digitales en el marco de una llamada revolución digital incursionaran en la estimulación del crecimiento económico y desarrollo de los países, pues, esta había llegado para brindar amplias posibilidades de incremento económico (Ministerio de Ciencia y Tecnología, 2020)

Bajo este marco, es en Europa, a partir de los años 2002 y 2005 que se desarrollaron un conjunto de propuestas orientadas hacia la implementación de las TIC y del internet en los procesos de desarrollo social, y en torno a las pymes, en el año 2003 se estableció una red europea de apoyo y refuerzo de los

negocios electrónicos (Ministerio de Ciencia y Tecnología, 2020). En España para el año 2005, un denominado hacker logró violar la seguridad de un conjunto de tarjetas de créditos, por lo que se tuvieron que alertar a muchos otros clientes del riesgo que representaba este hecho.

Posteriormente, según refiere Arguello (2020) se fueron presentando otros hechos que constituían amenazas cibernéticas a diferentes sistemas de información. Estos ataques resultaron de gran impacto para los sistemas, especialmente, cuando se trataban de estructuras de las cuales dependen áreas como la energía o el flujo del agua, industrias, procesos industriales, financieros, comerciales, entre otros. Y se acentuaban en pequeñas empresas cuya estructura no estaba lo suficientemente sólida para resistir a estos ataques en sus sistemas.

Vale destacar que, La Fundación Telefónica Española Ariel, en su informe sobre ciberseguridad indica que, así como las tecnologías han traídos grandes bondades a la vida de las personas, y especialmente al mundo de las empresas, también se deben considerar los problemas, que a la par se presentan, especialmente en el manejo de información sensible o de mucho valor para las organizaciones, situación que genera alarma para estas (Fundación Telefónica, 2016).

Muchos de los problemas que se presentan en la gestión de la información de las empresas se asocian con que, la mayoría de estas se encuentran en la incapacidad para predeterminar el tiempo y los eventos que puedan ocurrir en la realidad, razón por la cual, se debe alertar que, estas no deben confiarse (García, 2018). Pues, en cualquier momento puede estar bajo la vulnerabilidad o de alguna amenaza, como las cibernéticas, poniendo en riesgo la información de la que dependen muchas empresas.

Tal situación de riesgo, hace que sea cada vez mucho más importante, que se cuenten con sistemas de blindaje y protección de información que ayuden a minimizar los peligros, en la posible pérdida de datos de interés para las empresas y organizaciones. Pues, el uso del internet como sistema de comunicación, requiere de una actuación de prevención por parte de los

microempresarios, ya que la seguridad que puedan brindarle a la información que manejan es vital para que la organización pueda sobrevivir. Es de destacar que en la medida en la que pasa el tiempo, han ido surgiendo nuevos virus, amenazas y por tanto, se elevan los riesgos en los sistemas de información, pues si algo avanza y no se detiene, esas son las tecnologías apoyada con el sistema de conexión web.

Con respecto a ello, indica el informe de referencia CISO para el año 2020, que el 86% de las empresas han aumentado el uso de proveedores de seguridad, debido a que existe un incremento de ataques a los sistemas de información. En este sentido, el 46% con respecto al 30% del año pasado, han sufrido algún tipo de incidente o vulnerabilidad sin Parchear. Es decir, que este porcentaje va en aumento por lo cual, existen software malintencionados que afectan los sistemas de información, generando destrucción en los sistemas. Uno de los más comunes, según el informe es el ransomware, y su presencia puede estar en las microempresas como en las grandes empresas (Martino, 2020).

En América Latina las microempresas han tenido un rol importante en la economía de los países, especialmente, las cooperativas, pues estas han sumado a la generación de ambientes productivos, a la creación de empleos, y evidentemente, al desarrollo socioeconómico de los países en la región. Sin embargo, las mismas han tenido que sortear grandes dificultades en sus procesos. Al respecto, Mantilla indica que toda empresa ya sea micro o mediana, debe contar con un sistema de gestión de información, y estos no solo deben gestionarse ante un problema que afecte sus sistema de información, sino que debe tenerse de forma permanente como mecanismo de prevención (Mantilla, 2009).

En el Ecuador, las cooperativas y pequeñas empresas como las Pymes han tenido una importante participación en la economía nacional. Especialmente aquellas empresas familiares, las cuales surgen como emprendimientos, que van desarrollándose de generación en generación (Iglesias, 2017). No obstante, estas por sus múltiples ocupaciones, desconocen en su mayoría los procesos y mecanismos de seguridad que le permitan su subsistencia en el mercado. Sobre

este aspecto, el autor Mera indica que muchos son los pequeños empresarios de diversas modalidades de empresas, han tenido que sortear grandes dificultades en sus sistemas de información, principalmente, porque no han desarrollado políticas especializadas que le ayuden a enfrentar las amenazas a sus plataformas tecnológicas, haciéndolas menos competitivas en el mercado internacional (Mera, 2020).

Bajo esta idea, una empresa que invierte en seguridad de sus sistemas de información aumentará su valor, pues, estas deben preocuparse por la seguridad de sus sistemas de información, en la que pueden estar en riesgo información sobre finanzas, claves y contraseñas, correos electrónicos, interrupción de los servicios, caída de los sistemas, etc. En este contexto, según los informes de la RED CEDIA, la seguridad es fundamental para que las microempresas sobrevivan en esta era del internet y del comercio digital, en donde la información se maneja a través de dispositivos de almacenamiento, correos electrónicos, compras y transacciones en línea, etc., por ello, debe protegerse de cualquier tipo de amenaza que también transite a través de la conexión a internet (Silva, Segadas, & Kowask, 2014).

1.2. Referentes empíricos

Sánchez & Rebolledo, (2017) en su investigación denominada “Diseño de un sistema de gestión de la seguridad de información en el área de talento humano de la secretaría de educación”, en el que se propusieron realizar un modelo de gestión de seguridad para una institución pública, esta se llevó a cabo en Colombia, expusieron que, en toda organización existen riesgos como en el acceso, seguridad y claves para ingresar sistemas de información. Además indican que, otros de los posibles riesgos están asociados a la integridad del software y la información que se maneja dentro del sistema de la organización. Por lo cual, toda organización debe contar con una estructura de protección que permita funcionar sin mayores problemas, independientemente de cual sea su razón social o actividad económica.

Como parte de los resultados, encontraron, que uno de los mayores problemas ha sido la falta del establecimiento de una política de seguridad

robusta que logre mitigar los posibles riesgos a los que enfrenta la organización estudiada. De manera que, indican que, promover una cultura de seguridad y privacidad en el manejo de la información puede ayudar decisivamente en la mejora de los sistemas de las empresas. Esto se basa en el establecimiento de políticas y objetivos institucionales, los cuales deben ser de fiel cumplimiento por cada uno de los miembros de la organización. Además de establecer estas políticas, indicaron que se debe capacitar al personal especializado en esta materia para que mantenga el control preventivo de manera constante.

Los resultados que se generan de la precitada investigación constituyen un grandioso aporte al desarrollo teórico del presente estudio. Pues, como bien se puede evidenciar, independientemente del tipo de empresa u organización, es un imperativo que estas cuenten con sistemas de seguridad que le permitan su desarrollo y subsistencia en el tiempo. Es interesante además, indicar que, el estudio promueve el desarrollo de una cultura organizacional que favorezca un ambiente de seguridad de la información en los diferentes ámbitos de la empresa. Esto le concede mayor importancia al estudio, así como valor para comprender el desarrollo de este tema en el ámbito de las cooperativas.

Por su parte, Nieves, (2017) en su estudio denominado “Diseño de un sistema de gestión de la seguridad de la información basados en la norma ISO/IEC 27001:2013” propone el diseño de un (SGSI), bajo la mencionada norma, en virtud de la necesidad de contrarrestar los riesgos que presenta la organización en estudio. Es importante añadir, que el estudio área de una fase de planeación, análisis de la situación y descripción de cada uno de los procesos que se desarrollaban en la entidad, esto con el fin de valorar los riesgos a los que esta se encontraba expuesta.

Dentro de los resultados más resaltantes esta que, en relación a la organización de la seguridad de la información se pudo conseguir que esta cumplió solo en un 25%. Mientras que en criptado de información, o algún tipo de cifrado para proteger la entidad, se consiguió que el riesgo es elevado en un 100%, por cuanto no se encontró este tipo de mecanismo. Es relevante señalar, los datos que proporciona esta investigación para enriquecer el desarrollo de los fundamentos de la presente investigación, pues permite situar en torno

comportamiento que ha tenido este tema en otras esferas y contextos de investigación. De la cual se pueden tomar elementos de destacada importancia para el análisis de datos que den cuenta de una información clave para explicar el comportamiento del objeto de estudio.

Otro estudio interesante a destacar, es el presentado por Lara, (2015) en la cual destaca que, dentro de las principales amenazas encontradas que afectan a los sistemas de información de las empresas están: Los Virus con un 75%; la divulgación de contraseñas en un 57%, los Hackers en un 44%; los trabajadores insatisfechos en un 42%, seguidamente, los accesos indebidos con un 40%; la filtración de información en un 33%, seguido de las múltiples fallas en la seguridad física, la cual reportó un 30%; los accesos remotos indebidos con un 29% y finalmente están con un 27% los superpoderes que permiten acceso.

En el estudio, Lara señala las razones por las cuales un sistema se convierte en vulnerable y esto puede ser en gran medida, por algunos defectos internos de los equipos, que vienen con fallas de fábricas, seguido de la incorrecta configuración de los mismos. En esto se comprometen los hardware y los software, los medios de comunicación y de almacenaje. Por ello, considera que es de vital importancia para cualquier empresa, contar con sistemas políticas y medidas que permitan aminorar los riesgos, y protegerse contra posibles ataques y delitos informáticos, pero además gente capacitada para gestionar estos procesos de seguridad.

Por su parte, García (2015), en su investigación “Modelo de Gestión de la Seguridad de Información en los procesos críticos de las áreas financieras universitarias. Caso PUCE”, en el cual, planteó el diseño de un modelo de gestión de la seguridad de la información que se ajustara a la realidad de la dirección general financiera de la organización donde llevó a cabo el estudio.

En su análisis indica que, las tecnologías forman parte integral de la organización o la empresa, por ello, es indispensable que se revisen los procesos que se dan a través de sus usos. Este, agrega que, dentro de la gestión, la información es fundamental, esta forma parte de un recurso clave que le permite a la empresa desarrollar el intercambio comercial, así como también, es la que

permite llevar el control de los archivos, sean estos administrativos o financieros. Los resultados de la investigación destacaron que la PUCE no dispone de un sistema de seguridad financiera, por el contrario, las políticas que se manejan en la institución distan de estos objetivos. De manera que, como aporte establecieron la viabilidad para implementar un modelo que permitiera brindar seguridad al sistema financiero.

De allí que, se puede inferir que las tecnologías y el manejo del internet en las pequeñas empresas son factores claves en la creación, organización, difusión de información. Además, estas permiten darle soporte a la empresa, en cuanto a las decisiones que se deban tomar, ayudan al cumplimiento de los objetivos y metas. Tomando en cuenta el precitado trabajo, vale indicar que, en un escenario que es movido a través de las tecnologías y la conexión a internet, no es posible, o más bien es impensable, desarrollar procesos empresariales y comerciales, sin tomar la previsión en cada una de las unidades que conforman la microempresa. Así pues, las reflexiones que se generan como parte del estudio referido, son de capital importancia para ampliar los análisis expresados en líneas posteriores.

En el marco de estas consideraciones, autores como Granada (2018) en su investigación sobre “Diseño de un Plan de Gestión de Seguridad de la Información para una cooperativa de ahorro y crédito”, cuyo objetivo principal se orientó hacia la creación de un Plan de Gestión de Seguridad de la Información en el área tecnológica de la Cooperativa de Ahorro y Crédito Kullki Wasi. Este proyecto surge por las debilidades presentadas en esta cooperativa en el manejo de los activos internos, los cuales se manipulaban sin ningún tipo de prevención de riesgos.

En este sentido, en la investigación se señala que la información que se maneja en las cooperativas depende la base del negocio, y de ella también depende el logro de los objetivos a corto o mediano plazo. Pues, sostiene que uno de los grandes problemas que presentan las Pymes es que no cuentan con el personal capacitado en esta área, razón por la cual, están expuestas cada día a nuevas amenazas a sus sistemas de información.

El estudio fue concluyente al indicar que, es una necesidad muy grande, el que estas microempresas inviertan recursos en capacitaciones y desarrollo de prácticas sobre seguridad de información. Los autores sostienen que la función de la toma de este tipo de medidas es que, se debe prever que los posibles riesgos en una empresa o cooperativa deben conocerse, entenderlos y gestionarlos con total responsabilidad en los términos del manejo y control de toda la información que se dispone en la empresa.

Otra investigación desarrollada por Bedón, (2019) denominada “Sistemas de información para la seguridad de datos de los socios de la cooperativa Tapeco”, indica que los mayores problemas de gestión de seguridad de información de la cooperativa estudiada es que tenían información en ficheros digitales sin ningún mecanismo de seguridad. Se encontró que la mayoría de los socios de las cooperativas desconoce en el tema de la gestión de la seguridad de información, lo cual eleva el riesgo de inseguridad de los sistemas que se manejan en la cooperativa estudiada.

Sarmiento, (2020) en su investigación denominada “Modelo de sistema de información gerencial para la gestión del riesgo operativo en las cooperativas de ahorro y crédito, segmento 3 de la economía popular y solidaria en la provincia del Azuay” presentado a la UTEG como requisito de titulación. El estudio propone en su objetivo principal, Diseñar el modelo de un SIG, para gestionar los posibles riesgos operativos que se presentan en la Cooperativa de Ahorro y Crédito en la provincia del Azuay, Ecuador.

El mismo se desarrolló bajo una metodología de análisis de campo, de tipo experimental, en el cual se profundizó en la cooperativa para conocer de la fuente primaria los riesgos a los que esta enfrentaba. Consiguiéndose que, de las cooperativas estudiadas, la mayoría presentaron riesgos elevados en sus sistemas de finanzas principalmente. Estas organizaciones para el investigador, no aplican Sistemas de Información, lo cual las pone bajo riesgo y vulnerabilidad, así como limitadas en sus gestiones operativas.

Las conclusiones indican que estas se encuentran transitando por procesos muy complejos, los cuales, las ponen frente a diversos desafíos, pero que están

obligadas a asumir para poder sobrevivir en un mundo lleno de dificultades. En lo que respecta a sus sistemas tecnológicos, estas manifiestan problemas como caídas prolongadas de sus sistemas, un pobre almacenamiento de información y transacciones que se interrumpen por presentar fallas de tipo técnico en sus equipos. De esta investigación se extrae información relevante sobre el comportamiento de un número importante de cooperativas, además, acerca de forma general a sus principales problemas, los cuales se pudiera inferir que pueden repetirse en otras empresas de esta economía popular y solidaria.

En atención todas las investigaciones y aportes de los autores revisados, se puede evidenciar, que sin lugar a dudas, existe un amplio consenso en que las empresas deben tener dentro de su estructura de gestión administrativa como operativa un sistema de seguridad de información, que le permita poner a resguardo los datos, registro y toda información de importancia para la empresa, seguidamente coinciden en que, para ello es un imperativo invertir en una plataforma de prevención como programas adecuados que bloqueen cualquier tipo de amenaza que ataque el sistema de información de la empresa.

También se debe agregar que, la capacitación del personal técnico y expertos es una necesidad, pues estos poseen un rol muy importante en la empresa. Un elemento adicional que se desprende de las investigaciones anteriores es que independientemente del tipo de empresa sea, su modalidad o condición organizativa esta debe tener este sistema de prevención de riesgo, porque es un hecho que las amenazas van a estar siempre presentes en la web, en el intercambio de la información, trasmisión de datos, transacciones, etc.

Por ello, es condición indispensable, que estas vayan implementando dentro de su estructura las políticas, líneas estratégicas, controles, acciones, objetivos, entre otros que marquen las pautas a seguir en la organización, así como el orden administrativos de rigor que se deben seguir en todas las unidades administrativas y departamentos de las microempresas.

Estas aunque sean pequeñas, es necesario que inicien de una forma adecuada, si es que desean crecer y enfrentar de la forma más correcta los

embates que se presentan en el camino del intercambio comercial, y de los procesos de gestión de información.

1.3. Planteamiento del problema de investigación

En la actualidad, las cooperativas de ahorro y crédito en el país, poseen dominio de una cantidad importante de información y datos relacionados con el segmento que desarrollan. Uno de las más importantes se asocia a los datos financieros, así como el manejo de transacciones electrónicas, que le dan comodidad, agilidad y ahorro del tiempo en sus operaciones. Sin embargo, estas no cuentan con un sistema de información que les ayude en el desarrollo y administración de estos procesos operativos (Sarmiento, 2020). Esta situación puede afectar el control de los sistemas informáticos y de resguardo de la información que le permita evitar posibles riesgos, pérdidas o alteración en sus sistemas.

Las cooperativas cada vez más, poseen mayor presencia en el ámbito empresarial de Ecuador, pues estas han tenido el acceso al desarrollo comercial, encontrándose dentro de la modalidad de economía social y solidaria establecida en la constitución nacional y en el plan de desarrollo económico del país. Y aunque, la Superintendencia de Economía popular y Solidaria ha hecho grandes esfuerzos por apoyar en el control y supervisión del sector cooperativista, y en ese marco, apoyar en el desarrollo y modernización tecnológica en el dominio de la gestión de los procesos de estas entidades y organizaciones.

Así se ha planteado en la 9na jornada de Supervisión de la Economía Popular y Solidaria en la que se informó de un importante número de cooperativas que llevan su estructura de información de manera organizada, aún falta mucho camino que recorrer, pues el trabajo debe ampliarse en este sector, y deben ser los mismos socios los que se esfuercen por propiciar las condiciones para que sus sistemas de información estén a salvo y con ello, les permita su evolución (Superintendencia de Economía Popular y Solidaria, 2020).

Por otra parte, es importante destacar que la gestión de la información es la clave para el crecimiento y el éxito de una empresa, pues esta permite y orienta hacia la correcta toma de decisiones. Por ello, las pequeñas empresas deben

prestar más atención a asegurar su información y asignar los recursos necesarios para implementar políticas de seguridad para prepararlos para posibles ataques cibernéticos. En este contexto, la dimensión de la seguridad en las microempresas y cooperativas ha sido uno de los factores que se convierte en un desafío. Esto debido a que, en muchos casos estas no cuentan con los recursos disponibles que les permitan blindar sus sistemas, así como invertir en preparación técnica de sus miembros (Parra, 2014).

Según la Revista ED Digital Economy Magazine, los ataques cibernéticos aumentaron un 130% en 2016, siendo las pequeñas empresas los objetivos más vulnerables. Según este medio, los números son preocupantes y es posible que grandes números puedan estar ocultos porque las compañías no informan de todos los ataques, porque un ataque cibernético puede comprometer su marca (Capital Online, 2015).

El tema no es nuevo, particularmente en Ecuador, El Diario El Comercio dice que "Ecuador es vulnerable a los ataques cibernéticos" y que se ha encontrado que el país tiene vulnerabilidades en sus sitios web oficiales de empresas privadas; por esta razón, el gobierno, junto con las empresas privadas, deberían involucrarse en el asunto tomando medidas preventivas para evitar que ocurra este tipo de ataque (Bravo, 2015), protegiendo así, los recursos de información de las organizaciones.

Este es el caso de las Pymes en Ecuador, debido a sus limitaciones, no pueden implementar políticas de seguridad o medidas preventivas para proteger sus recursos de información. Por lo tanto, es aconsejable que estas empresas puedan realizar mayores esfuerzos con el fin de fortalecer sus sistemas de comunicación.

Por tanto, las empresas deben tomar medidas de seguridad para proteger su información de posibles ataques de seguridad. Esto debido a que la complejidad de los nuevos sistemas informáticos y los datos procesados en los mismos, demandan de procesos que deben desarrollarse por estas microempresas. De igual forma, la problemática de la falta de conocimiento sobre los mecanismos tecnológicos que permiten la protección de la información y las tendencias

tecnológicas para protegerse de las amenazas y ataques internos y externos han llevado a la necesidad de mejorar el área de seguridad de la pequeña empresa para proteger su información.

A medida que se multiplican las amenazas a la información que circula en los sistemas de las pequeñas empresas, bajo la modalidad de cooperativas, se hace más necesario el uso de un modelo para realizar la gestión de la seguridad de la información. Pues, este permitirá un cambio sociocultural con responsabilidad y eficiencia en estas pequeñas empresas o Pymes.

Por otra parte, existen estándares de seguridad informática implementados por grandes empresas, pero esto dificulta la implementación en pequeñas empresas, debido a que estas no cuentan con las condiciones financieras, logísticas y humanas para alcanzarlos. Por esta razón, es importante crear un modelo de gestión para aplicar a las pequeñas y medianas empresas, que cuente con la respectiva adecuación para estas.

Por ello, es un imperativo que las empresas deban disponer de un mejor sistema para gestionar la información de sus archivos, documentos, etc, ya que los ciberataques y distintas amenazas cibernéticas constituyen un problema global, permanente, inminente, y que se acentúa mucho más en las pequeñas y medianas empresas.

Si no se implementa un modelo de gestión para la seguridad de los recursos de información, las pequeñas empresas corren el riesgo de ataques internos y externos con el riesgo de perder información, lo que se refleja en pérdidas económicas, y en los casos más extremos podrían llevarlas a la quiebra o pérdida total de información.

1.3.1. Formulación del problema de investigación

¿Un modelo de gestión de seguridad de la información para pequeñas cooperativas de ahorro y crédito en la ciudad de Guayaquil garantizará la seguridad de los recursos de información?

1.3.2. Sistematización del problema de investigación

- ¿Cuáles son los problemas de seguridad de la información en las pequeñas cooperativas de ahorro y crédito en Guayaquil?
- ¿Qué modelo se puede considerar como parte del estudio de caso seleccionado?
- ¿Cuál sería el diseño del modelo de gestión de seguridad de la información para pequeñas empresas en Guayaquil?

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Optimizar los estándares de seguridad mediante un modelo de gestión seguridad de información en una muestra de las pequeñas cooperativas de ahorro y crédito de la ciudad de Guayaquil.

1.4.2. Objetivos específicos

- Identificar los problemas de seguridad de la información que tienen las pequeñas cooperativas ahorro y crédito de la ciudad de Guayaquil.
- Evaluar varios modelos de gestión de seguridad de la información que se ajusten a pequeñas cooperativas ahorro y crédito.
- Diseñar un modelo GSI dirigido a las pequeñas empresas o cooperativas de ahorro y crédito de la ciudad de Guayaquil.

1.5. Justificación de la investigación

1.5.1. Justificación teórica

La mayoría de las pequeñas empresas tienen una infraestructura tecnológica creciente de la que dependen muchos de sus procesos productivos y administrativos. Gran parte de la información que generan (sistemas de información, buzones, documentos, PDF, etc.) no está protegida adecuadamente. Esto evidencia la falta de pautas de control que permitan el procesamiento adecuado de la información. Esas pautas deben sustentarse en políticas de control y manejo adecuado de información que se pueda ajustar a las necesidades de la empresa.

1.5.2. Justificación práctica

La gestión de la seguridad de información es un tema que ha cobrado capital importancia durante los últimos años, y a la vez, ha ido avanzado con gran rapidez (Echeverría, 2020). Esto movido por los incesantes cambios que se presentan, producto de la globalización y de aspectos como la economía, y con ella, la interconexión de la que dependen muchos procesos y sistemas que mueven una abultada cantidad de información a diario.

En este sentido, las premisas anteriores admiten que esta propuesta se justifique desde una perspectiva práctica, pues, técnicamente factible porque tiene los recursos tecnológicos necesarios, relacionados con la infraestructura, herramientas tecnológicas o software, acceso a los datos e información necesaria. Puesto que las pequeñas cooperativas de ahorro y crédito trabajan al límite en términos de seguridad de información, por ello, se considera aconsejable implementar estándares que se adapten al tamaño y a la operación de este tipo de instalación para garantizar, que la información sea accesible para aquellos que estén debidamente autorizados.

1.6. Marco de referencia de la investigación

1.6.1. Marco teórico

1.6.1.1. Contextualización de la investigación

El sector de Cooperativas de Ahorro y Crédito en Ecuador

Las cooperativas en el Ecuador han tenido un importante papel en la economía durante los últimos tiempos, pues estas han permitido la expansión de la participación de ciudadanos como socios en su desarrollo. En este sentido, estas nacen dentro de la política de implementación de una economía popular y solidaria en el país, pues su intención fue agrupar personas que encontrándose unidos por lazos de parentalidad, vecindad, contratos, en función de unir esfuerzos para emprender el desarrollo de actividades económicas para para la producción, obtención y distribución de bienes o servicios y con ello, satisfacer necesidades en común (Caicedo & Vásquez, 2020).

Coraggio, (2014), expone al respecto que: “entendemos por Economía Solidaria el sector de la economía que se rige interna y externamente por relaciones de cooperación, intercambio, financiamiento y consumo solidarios” (p. 9), el mismo la concibe como aquella forma de economía que se desarrolla en un ambiente democrático, participativo y simétrico, donde se asume un enfoque de responsabilidad propia y servicio hacia lo social, asume una cultura de derechos humanos, que se centra en el servicio y apoyo mutuo como sociedad.

Bajo esta perspectiva, las cooperativas de ahorro y crédito en el Ecuador de acuerdo con la Superintendencia de Economía Popular y Solidaria (2020) las cuales poseen como objetivo primordial desarrollar actividades de intermediación en el financiamiento y de responsabilidad social para con sus respectivos socios, terceros o con clientes. Estas se crearon bajo la resolución Nº 038-2015-F de febrero, 13 del año 2015, bajo cargo de la figura de la Junta de Política y Regulación Monetaria y Financiera. Estableciendo la regulación de los segmentos y entidades de este sector con base en el saldo de los activos y del tipo. La cual se muestra en la tabla siguiente:

Tabla 1
Saldos activos establecidos para las Cooperativas de Ahorro y Crédito, según resolución Nº 038-2015-F

Segmento	Activos ($)
1	Mayor a 80´000.000
2	Mayor a 20´000.000 hasta 80´000.000
3	Mayor a 5´000.000 hasta 20´000.000
4	Mayor a 1´000.000,00 hasta 5´000.000
	Hasta 1´000.000
5	Cajas de ahorro, bancos comunales y cajas comunales

Fuente: (Superintendencia de Economía Popular y Solidaria, 2020, p. s/p)

De acuerdo con información suministrada por Gestión Digital, (2019) las Cooperativas de Ahorro y Crédito (COAC) se han posicionado de forma importante en el país, puesto que, según reporta el informe de esta revista informativa digital que, para el año 2012 estas tenían unos activos igual a $6.077 millones y al cierre del año 2018, estaos se incrementaron a 14.016 millones de dólares, cifra que coincide con la reportada por la Superintendencia de la Economía Popular y Solidaria (SEPS). Como es posible evidenciar un importante incremento en las cifras en el comportamiento de estos activos.

Breves antecedentes en el país

De acuerdo con la Ley Orgánica de Economía Popular y Solidaria, establece en su artículo 21 que el sector de cooperativas se comprende como sociedades voluntarias que buscan satisfacer necesidades sociales, económicas, etc, para las cuales establecen una empresa con la figura de propiedad conjunta y de una gestión de principios democráticos y personalidad juridicial de interés social y derecho particular (Ley Orgánica de Economía Popular y Solidaria, 2018).

En El Estado ecuatoriano, La Constitución de la República establece dentro de su texto, la modalidad de Economía Popular y Solidaria en los términos de libre ejercicio, siempre que se cumpla con las disposiciones y regulaciones establecidas para tal fin. En este sentido, este sector forma parte de un grupo financiero importante en el país, al cual están adscritas las cooperativas de ahorro y crédito. Estas se encuentran conformadas por una asociación de personas que poseen un aporte importante al capital social, que también puede

ser conocido como integración social, en la que todos trabajan por fines y beneficios comunes (García, Prado, Salazar, & Mendoza, 2018).

De acuerdo con las ideas de Ortega-Pereira, Borja-Borja, Aguilar-Rodríguez, y Montalván-Burbano, (2017), los cuales indican, que posterior a la dolarización del país, el Sistema Financiero Nacional se convirtió en el más importante en la economía, así en paralelo, las Cooperativas de Ahorro y Crédito demostraron un incremento del 34,48%, cuyo aporte fue considerado el más significativo para el momento en el país.

Bajo este panorama económico en el país, las Cooperativas de Ahorro y Crédito poseen su presencia, bajo un sistema que buscaba satisfacer las necesidades de los ciudadanos, quienes se conformaban con la figura de socios de manera voluntaria para desarrollar actividades comerciales que le permitiera tener progreso y desarrollo en el país.

Las cooperativas fueron impulsadas por el efecto de las crisis económicas vividas en Ecuador, especialmente posterior a la entrada en vigencia de un nuevo texto constitucional (Santillán, y otros, 2016). Esto llevó a una nueva empresa con cuidado y diligencia, basada en el compromiso de la familia, de los socios, este negocio floreció y fue heredado a los nietos y las nuevas generaciones que vinieron en ese momento, aunque estas iniciativas no se conocían formalmente como Pymes o pequeñas empresas ya se venía desarrollando una especie de emprendimientos familiares.

Posteriormente, algunas microempresas fueron creciendo en la medida en que se diversificó la economía, sin embargo, otras debido a que no pudieron cumplir con los requisitos, ni alcanzar los estándares de un buen producto se quedaron atrás, mientras que otras se han creado, y en la actualidad estas pequeñas empresas en Ecuador representan un porcentaje importante en la producción nacional. Se destaca que aquellas microempresas, que han podido adaptarse o mantenerse, es porque han hecho esfuerzos importantes en el mejoramiento de sus sistemas, esto ha hecho que puedan convertirse en grandes empresas.

Las cooperativas, especialmente de microempresas familiares, enfrentan dos desafíos permanentes que pueden representar una grave amenaza para su supervivencia. Por un lado, aprenden y practican nuevas formas de gestión, y por el otro, realizan una reinvención constante de los negocios debido a factores internos y externos que afectan el mercado y la necesidad de pasar de una empresa nacional a una gran empresa. Experimentan cambios fundamentales en la forma en que se gestiona, ingresando a un proceso de integración y automatización de información, estandarizando los flujos del proceso para ser cien por ciento eficiente (Ordóñez, 2014).

Clasificación de las cooperativas en Ecuador

En correspondencia con la Ley Orgánica de Economía Popular y Solidaria, (2018), el sector de cooperativas se clasifica en:

- Producción: llevan a cabo actividad productiva, agrícola, textil, pesquera e industrial.
- Consumo: Estas se dedican al suministro de bienes varios por parte de los socios
- Vivienda: Se dedican a la adquisición de materiales para la construcción de viviendas o conjuntos residenciales.
- Ahorro y crédito: Este rubro se encarga de las entidades solidarias, los bancos, las cajas y el ahorro solidario.
- Servicios: Los servicios son todos aquellos orientados a la salud, la educación transporte, ventas.

Según reporta la Caja Central de Crédito Cooperativa (FINANCOOP) (2019), que para la fecha se tenían registradas 120 cooperativas de ahorro y crédito en todo el país. Esta cifra fue presentada en un evento público en el cual analizaron los grandes desafíos que posee el sistema financiero de la economía popular y solidaria, en el que observaron de forma positiva, el panorama de las cooperativas. Esto debido a que, de acuerdo a sus análisis, las mismas han ido en franco crecimiento a pesar de las crisis económicas suscitadas en el país durante los últimos años.

1.6.1.2. Conceptualización de Información

El concepto de información se refiere a un conjunto de datos que se encuentran de forma organizada y que se procesan con fines determinados. Estos constituyen un sistema de elementos que permiten la realización de operaciones en el trabajo, así como también, el cumplimiento de las funciones.

De acuerdo con Castro, (2016), la información se puede definir como un recurso muy importante que posee mucho valor para una determinada organización, por tanto, debe protegerse. Esta puede ser de diversas maneras, y almacenada en diferentes formatos y modalidades como de forma digital o impresa.

Según Baader, (2017) La información hace referencia a cualquier comunicación o formato de representación que admite el conocimiento de datos, los cuales pueden tener diversas presentaciones, formas, tipos, etc. En este sentido, la información puede tener una forma de presentaciones como numéricas, graficas, audiovisuales etc, y se puede representar en forma física o digital, sean estos informes, archivos, sistemas de datos, los cuales poseen gran importancia para la empresa.

Un sistema de información se refiere al conjunto de elementos informativos sobre la empresa, en los que se mencionan datos, estadísticas, reportes financieros, etc, los cuales se encuentran organizados de una forma en la que pueden ser procesados con facilidad, así como mantenerlos y transmitirlos, según la necesidad que se presente.

Estas definiciones anteriores permiten indicar que la información forma parte interna como externa de una empresa, y es de vital importancia para su funcionamiento. Por ello, su organización y gestión correcta es necesaria para que asegure calidad en el proceso.

1.6.1.3. La seguridad de información

La seguridad de información se conoce como el conjunto de medidas preventivas que están orientadas a la detección de posibles riesgos y amenazas,

vulnerabilidades del sistema general de seguridad de una determinada empresa u organización. Esta definición amplia permite hacer una clara distinción en seguridad de información y seguridad informática, la cual, evidentemente, hace referencia a dos cosas distintas (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2017).

Así pues, la seguridad de información se refiere a la protección y resguardo integral de un sistema que se maneja en una determinada organización, en el cual se aplican técnicas de protección de la información. Su evaluación posee un amplio alcance en torno al análisis de riesgos, amenazas, así como una evaluación de escenarios. Mientras que la seguridad informática es aquella que se refiere al resguardo de datos dentro de un sistema informático propiamente (Linux, 2020).

Por su parte, Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, y Saltos-Gómez (2017) sostienen que la seguridad informática se refiere a la protección que se le brinda a la información que está dentro de un dispositivo informático, es decir, al tipo de seguridad interna, que brinda soluciones específicas a una falla en su sistema de seguridad. Esta diferenciación permite poner en contexto el tema que se desarrolla, y con ello, sentar las bases que admiten un punto de partida claro en relación con el objeto de estudio.

La seguridad de información debe ser una intervención amplia que contemple la protección no solo de la información, sino del sistema en general, los recursos, los posibles errores y el posible impacto que se pueda generar de algún evento de inseguridad. Estas medidas le permiten a la organización su permanencia y continuidad en el tiempo. Así como la minimización de los riesgos, esto, evidentemente, favorecerá la inversión y la protegerá de las amenazas.

La seguridad de información está conformada por los siguientes aspectos que se vinculan con la necesidad de un sistema de gestión que permita desarrollarla en el marco de una visión general: Son estos:

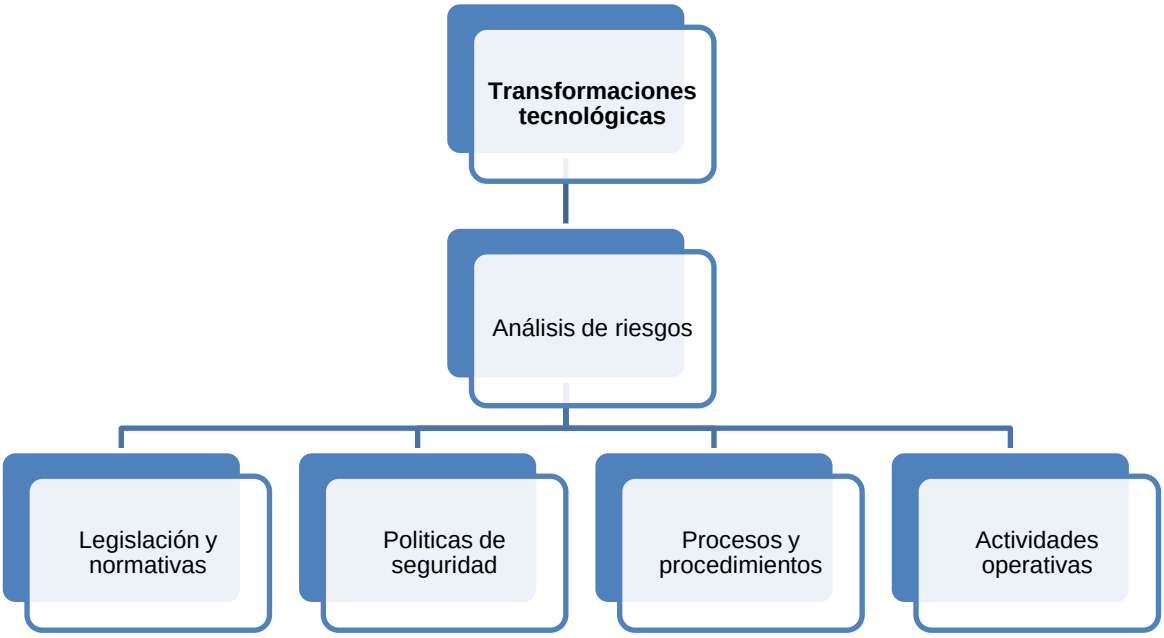

Figura 1 Perspectiva general de un Sistema de Seguridad de la Información
Fuente: Modelo tomado de la Escuela Superior de Redes RED CEDIA (Silva, Segadas, & Kowask, 2014, p. 29)

Los aspectos que se evidencian en la figura 1, se relacionan con la gestión de la seguridad de la información. En ese sentido, con respecto a las transformaciones tecnológicas, estas son permanentes en el sistema de información, pues siempre saldrán actualizaciones que se deben considerar en la gestión y operaciones de la información. En torno a ello, cada vez que estos cambios aparecen, también surgen nuevas amenazas y riesgos, esto hace que las evaluaciones deban hacerse de forma permanente.

Otro de los aspectos claves en el manejo de un sistema de gestión es la normativa que orienta todo el proceso que se lleva a cabo en la organización, considerando cada una de las unidades administrativas, como por ejemplo: finanzas, la cual es una de las instancias más importantes, y debe regirse por pautas y normativas que establece el Estado para su manejo y cumplimiento de lo relativo a impuestos, es decir, toda la parte de regulación y de las reglas del juego e intercambio comercial y en lo relativo a contratación de personal, etc.

1.6.1.4. El Sistema de Gestión de Seguridad de Información

Según García, Aguirre, y Delgado, (2015) un SGSI hace referencia a un modelo de Gestión que se basa en el desarrollo de políticas de seguridad, y se plantea estrategias propias de una determinada organización con la finalidad de establecer los lineamientos o directrices a seguir para el resguardo de la información. Dentro de este se contemplan algunos patrones a seguir, de comportamiento y actuación frente a situaciones, las prohibiciones y lo permitido, la seguridad lógica y física, la definición de los roles, atribuciones de cada miembro de la organización.

Por lo general, un sistema de gestión de seguridad se basa en un plan de seguridad, el cual se diseña tomando en consideración las directrices previamente establecidas en las políticas. En este sentido, dentro de la política se establece el gran lineamiento, que luego se materializará a través del plan de seguridad, el cual puede partir por una evaluación de los principales riesgos a los que está expuesta la microempresa. En este sentido, advierte Mantilla, (2009) que en toda organización se debe contar con este sistema, con el fin de proteger la información, así como mantener los controles en las diferentes unidades del sistema.

Las políticas de seguridad de la información se basan en objetivos, sanciones, organización de la información, y todos los procesos que están planteados para favorecer el sistema que se maneja en la determinada organización. Su desarrollo corresponde a un determinado modelo que se puede construir a partir de un conjunto de políticas, procedimientos, controles, procesos, acciones que se fundamentan en estándares y prácticas adecuadas que ayuden a minimizar los riesgos en una determinada organización.

Por su parte, Areitio, (2008) subraya que dentro de los grandes objetivos de la seguridad de información se pueden indicar los siguientes:

- Disponibilidad y accesibilidad de la información y sistemas de datos, este permite que se trabaje cabalmente

- Integridad, esta fase da garantía de no alteración de la información por personas no autorizadas. La misma incluye la integridad del sistema y de los datos.
- Confidencialidad
- Responsabilidad: Presenta registros de auditoria
- Confiabilidad: esta es una de las importantes, pues, esta hace que se pueda tener tranquilidad con el funcionamiento de la información.

Por otra parte, Silva, Segadas, y Kowask, (2014) indican que existen ciertos requisitos que se consideran muy importantes, los cuales se sustentan en tres fuentes primordiales:

- La evaluación y el análisis de los posibles riesgos: la cual parte de la valoración de los objetivos y las líneas estratégicas que posee la organización como resultado de la detección de las vulnerabilidades, de allí que, se puede mantener el control de las posibles amenazas. En este sentido, la gestión de riesgos involucra actividades que puedan controlar y dirigir acciones para mantener la estabilidad del sistema y los activos que esta representa. Por tanto, su evaluación es una necesidad, pues los resultados de esta son los que permitirán la intervención con el tratamiento adecuado.
- El ordenamiento jurídico vigente: se refiere a los reglamentos, resoluciones, estatutos, clausulas y resoluciones, cuyo cumplimiento debe hacer la organización, los colaboradores, los socios y todos los agentes se encuentren vinculados a la misma. Este aspecto indica los códigos y formalidades que ayudan a las buenas prácticas dentro de la organización, y especialmente de los procesos y procedimientos que en ella se desarrollen. Fundamentalmente las políticas.
- Los principios: referidos a los requerimientos y los objetivos del negocio que sirven de sustento para el procesamiento de la información de base para la definición y soporte de las operaciones correspondientes. Los principios son los que orientan las acciones y estos deben cocerse tanto los empleados, como a los clientes.

1.6.1.5. Elementos claves que debe presentar el modelo de seguridad de la información.

La seguridad se refiere a la preservación de la información que se posee en el sistema de una determinada organización. También se contempla la disponibilidad de información, la responsabilidad y confiabilidad de todo lo que se mantienen en el sistema. En este orden, plantean Silva, Segadas, y Kowask (2014) se poseen determinados elementos:

- Tener una política orientadora de seguridad de la información (esta debe contar con objetivos bien definidos en función de la actividad o el segmento de la cooperativa)
- Establecer la seguridad a nivel organizacional (corresponde al enfoque y la estructura que se defina para la implementación, es decir, que este modelo coincida y sea coherente con la cultura organizacional de la cooperativa)
- Plantear seguridad en cada una de las instancias administrativas de la cooperativa (todas las instancias administrativas deben estar y asumir el compromiso con la mejora de la seguridad de la información, por tanto estar dispuestos a cumplir con cada uno de los procesos que se plantean en la organización para cada actividad o tarea a realizar)
- La seguridad debe ser a nivel físico como digital (archivos y libros, como en los dispositivos electrónicos que manejan información de relevancia)
- Control en los accesos, así como en las salidas
- Gestionar los posibles riesgos y accidentes fortuitos en el sistema de la seguridad de la información (emplear un procedimiento eficaz, en función de la realidad que presentan las cooperativas y del escenario en el cual se desenvuelven)
- Gestionar de la seguridad de forma permanente (esto implica un proceso de evaluación, se deben medir los resultados de la gestión de seguridad). Este es una de las fases más importantes del proceso.

El modelo de SGSI depende además de los siguientes factores que ayudarán al éxito en el resguardo de la información:

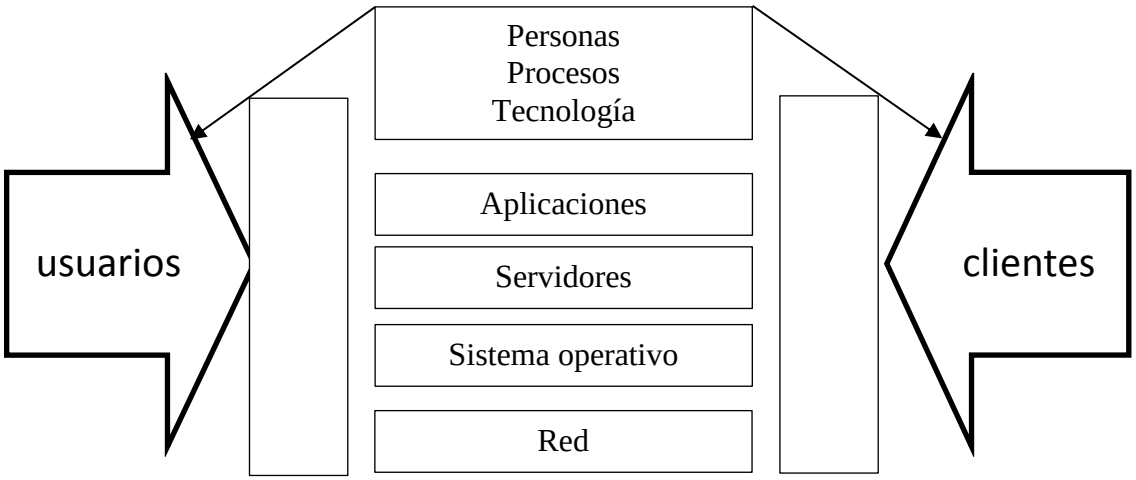

Figura 2 factores para el resguardo de la información
Fuente: Elaboración propia con adaptaciones de (Moscaiza-Moncada, 2020).

Estos factores permiten entender con claridad, que en toda organización existe una entrada de usuarios que pasarán por un proceso operativo, bajo el cual se encuentra un sistema que ordena todos los procedimientos y acciones a realizar. En este proceso intervienen o se pasa por un servidor, sus aplicaciones, así como sistemas operativos, los cuales son accionados bajo un escenario en red, en la cual, pueden estar presentes amenazas y riesgos que deben ser detectados y controlados por un buen sistema o modelo de gestión de seguridad de información.

De manera que, existen tres aspectos esenciales que son indispensables en el sistema, estos son las personas, las cuales deben ser sensibilizadas, responsabilizadas, además deben controlar y supervisar todas las áreas de las entidades.

Los procesos, que incluyen la organización bajo los parámetros formales y normativos que exige la legislación, es decir, se debe procesar y dar cumplimiento de lo que establecen las leyes vigentes. Así también la organización incluye el ordenamiento y ejecución de las políticas, procedimientos, planes y las relaciones con los clientes y proveedores. Y la tecnología que ayuda el proceso y es manejada por las personas y expertos en el área. Esta abarca la selección e instalación de los equipos, su debida actualización, configuración y dar la solución a los problemas de Software y

Hardware. La criptografía, y desarrollo seguro de las aplicaciones que se requieran (Moscaiza-Moncada, 2020).

1.6.1.6. Importancia de la Seguridad de información

Hoy no hay duda de que se está viviendo en una nueva era, que se caracteriza por el uso masivo de los sistemas de información, esto con mayor fuerza que en épocas anteriores, por lo que, es esencial considerar dentro de las organizaciones, la identificación de las debilidades del sistema de información. Así también, se haga frente a las amenazas y los riesgos que se pudieran experimentar, por la gran cantidad de usuarios con potencial de ataque, que se centran no solo en el entorno y fuera de la empresa, sino también en los usuarios normales que trabajan. Representando una amenaza de seguridad si no hay pautas de acceso claras a la información.

Después de conocer las amenazas y debilidades ambientales identificadas en el análisis de riesgos, y de definir formalmente las intenciones y actitudes de la organización establecidas en la política de seguridad de la información, se debe tomar algunos mecanismos, para implementar las medidas de seguridad recomendadas y adecuadas. Tomando en consideración que las amenazas son agentes que pueden explotar vulnerabilidades. Como resultado, pueden causar pérdidas o daños a los activos de una empresa, afectando de forma importante el negocio.

Es importante alertar, que conocer las debilidades del área o tener una política de seguridad escrita no es suficiente, por ello, se deben instalar las herramientas, se deben publicar las reglas, se debe informar a los usuarios sobre el valor de la información, la configuración de entornos, etc., se tiene que seleccionar e implementar todas las medidas de protección para ayudar a reducir las vulnerabilidades. Cada medida debe seleccionarse para que logre los objetivos definidos en operación.

Gran parte de esta labor, está en manos de los responsables de la seguridad de la información, a quienes la gerencia apoya de manera explícita y activa en todo momento. Por lo tanto, es importante no solo establecer cuáles son las

principales amenazas en todo momento, sino también, lo que debe hacer para poder resolver la situación. Bajo esta línea, es imperioso que se considere la capacitación, un entrenamiento adecuado y constante en el tema de seguridad de información, esto debe ser parte de la gestión estratégica de toda organización. Pues el ampliar y potenciar las competencias del personal amplía las posibilidades de mejorar la seguridad de la organización.

1.6.1.7. Los ataques y su clasificación

De acuerdo con Soriano, los ataques se conocen como aquellas acciones que se ejecutan de forma sistemática para corromper la seguridad de un sistema determinado (Soriano, 2019). Se conoce también como una amenaza sistemática, siendo las redes de los ordenadores unas de las más vulnerables a estos ataques.

Estos ataques pueden ser pasivos y activos

Pasivos

Son aquellos que se relacionan con el contenido que conllevan los mensajes y su relación con el análisis del tráfico de información (Soriano, 2019). Estos ataques se presentan cuando el atacante lleva el monitoreo del canal de comunicación sin alterarlo, aunque en esta acción está vulnerando la privacidad y confidencialidad de la información que se maneja. Sus formas son el espionaje y el análisis del tráfico de información o datos.

Otro de estos ataques es el análisis de tráfico, el cual tienen que ver con la interceptación de información y examinación de los mensajes enviados, para deducir información de interés. Esta acción es posible cuando los mensajes se encuentran cifrados.

Activos

Este tipo de ataque es aquel que se realiza con el propósito de alterar el funcionamiento de un sistema o afectar su proceso. En estos ataques se pueden borrar datos, cambiar o modificar información (Figueroa-Suárez, Rodríguez-

Andrade, Bone-Obando, & Saltos-Gómez, 2017). Dentro de los ataques de esta naturaleza se conocen seis categorías de análisis:

- Suplantación de identidad
- Repetición
- Cambio de mensajes
- Denegación en el acceso a servicios.
- Amenazas persistentes, estos atacantes pueden estar en el sistema o red sin ser descubiertos por mucho tiempo.
- Elemento en el medio, se trata del interceptor de información

El escenario de aplicación de esta seguridad de información posee determinados niveles y un alcance:

- El desarrollo
- La integración
- La operación
- La administración
- El mantenimiento preventivo y correctivo
- La evolución de sistemas
- Las aplicaciones

Todas las anteriores representan el ciclo de vida de las operaciones de los negocios. De manera que, en cada aspecto, etapa o nivel debe existir un mecanismo de seguridad que permita el desarrollo cabal y óptimo del servicio o producto, según sea el caso.

1.6.1.8. La Gestión de Riesgos

Hasta este apartado se han desarrollado algunas ideas iniciales sobre la gestión de riesgos, esta involucra la evaluación, que se realiza a partir de la consideración de posibles amenazas, o vulnerabilidades a los sistemas de información. En este sentido, se refiere a la valoración de los riesgos y gestionarlos de manera que se pueda visualizar el contexto y comportamiento de una forma general. De modo que, para la evaluación de riesgos, se debe

iniciar, atendiendo a las siguientes consideraciones tomando como referencia, los aportes de Silva, Segadas, y Kowask, (2014):

- Se incluyen todas las acciones y medidas establecidas para el control de los posibles riesgos
- Este análisis contempla los posibles riesgos, los identifica y estima su alcance y posible impacto a la información.
- Se establecen los criterios para las acciones a implementar
- Los riesgos se identifican dependiendo del cómo afectan la información o en qué medida representan realmente un riesgo importante para la organización.
- Implica la iniciativa y una correcta toma de decisiones.

Para la prevención de riesgos, son muchas las medidas que se emplean hoy en día para prevenir el posible ataque a los sistemas de información de las microempresas, dentro de ellos se mencionan:

- Disponer de equipos especializados en torno al tema de seguridad informática
- Se debe usar un software legal
- Los equipos y dispositivos de una empresa deben tener un constante mantenimiento
- Se deben usar programas que ayuden a prevenir riesgos, como antivirus y antimalware
- Siempre las empresas deben tener respaldo de información
- Además del uso de contraseñas seguras
- El personal a cargo debe estar constantemente capacitado
- Las empresas invierten tiempo y recursos valiosos.

1.6.1.9. Normas ISO 27001:2013

La gestión de un sistema de información implica tomar en consideración que existen factores o elementos que pueden vulnerar sus procesos y archivos, dentro de los que se puede mencionar los malware o los piratas informáticos, los cuales producen alteraciones, causando fallas. En ese sentido, se puede señalar

que todas las empresas sean de las características que se encuentran expuestas a sufrir este tipo de ataques, y presentar fallas importantes en sus procesos.

Por ello, Organizaciones como la ISO (Organización Internacional de Estandarización) se ha especializado en proveer un sistema con orientaciones técnicas a través de modelos estandarizados de seguridad, los cuales están adaptados para implementar en cualquier tipo de empresas. Las siglas ISO que en inglés significan *International Organization for Standardization,* corresponde a una organización internacional de normalización que se encarga de crear normas para brindar seguridad y eficiencia en los diversos servicios que poseen las empresas y organizaciones (ISO27000.ES, 2021).

Este sistema de normas estandarizadas orienta sobre los requisitos que deben cumplir o tener para poder tener sus servicios, bajo estándares de seguridad. Aunque se sabe, que cada empresa posee su propia realidad, de allí que estas normas son de carácter general, y deben ser adaptadas a las características de las organizaciones. Estas normas de acuerdo con los lineamientos que poseen se encargan de orientar hacia buenas prácticas para poder contar con una gestión de seguridad en los procesos y sistemas de información (Colegio Oficial de Ingenieros de Telecomunicación, 2021).

Estas a lo largo de los años, han tenido una serie de actualizaciones en sus estándares. En relación a las normas ISO-27001:13, esta posee antecedentes de aparición en el año 1995, en la que se planteaba presentar un conjunto de normas para favorecer las prácticas y procesos en la gestión de la seguridad de la información. Seguidamente, en el año 98 especifica el SGSI, un año más tarde, se presentan otras actualizaciones BS 7799-1:1999 y la 2. En el año 2000 se adopta el ISO, posteriormente en el 2002, se hicieron revisiones de la parte 2. En el año 2005 se actualizó como ISO/IEC 177799:2005, y revisión de ISO 177799. En ese mismo año, la segunda parte asume ISO (ISO27000.ES, 2021).

Las normas ISO han tenido una trayectoria de actualización de estándares de seguridad según las características que demanden las empresas en el mundo, pues, los procesos son cambiantes, y por ello, se debe mantener bajo actualización en los sistemas y servicios. De acuerdo con el portal oficial de las

ISO.ORG, (2021) los estándares de normas ISO/IEC 27001 se basan en la gestión de seguridad de sistemas de información, y se ha diseñado para implementar en cualquier organización.

Estas se orientan a:

- Tecnologías de información
- Técnicas de seguridad
- Sistemas de gestión de seguridad de información y sus requisitos generales.

Su última revisión y/ actualización de estas normas se hizo en el año 2019.

Indica ISOtools Excelence, (2021) que estas normas se enfocan en la preservación de la confidencialidad, la integralidad y disponibilidad de información a través de la implementación de la gestión de riesgos, que puedan gestionarse adecuadamente. Toman en consideración en su aplicación, el diseño de procesos, el sistema de información, y los respectivos controles. Evaluar interna y externamente la empresa y las propias capacidades para responder a los objetivos. Aunque el orden para su aplicación va a depender de las necesidades reales de la organización.

De acuerdo con el sistema de normas ISO, (2021) se contempla:

1. El alcance
2. Referencias normativas
3. Términos y definiciones
4. El contexto de la organización (necesidades, alcances, expectativas e intereses, sistema de gestión de la seguridad)
5. Liderazgo (liderazgo y compromiso, políticas, funciones, responsabilidades y organización)
6. Planificación (acciones para abordar los riesgos y las oportunidades, objetivos de seguridad, alcances)
7. Soporte (recursos, competencia, conciencia, comunicación, información documentada)

8. Funcionamiento (planificación y control de operacional, evaluación de riesgos de seguridad, tratamiento de riesgo de seguridad)
9. Evaluación del rendimiento (monitoreo, medición y análisis y evaluación, auditoría interna, revisión de gestión)
10. Mejora (Acción de inconformidad y corrección, mejora continua.

1.6.1.10. COBIT

Esta es una metodología que se conoce como COBIT 5, se trata de la última versión publicada en el año 2012. Ayuda a través de lineamientos y políticas a cumplir con las normas establecidas, los acuerdos contractuales y generar con ello, un sistema de equilibrio que le permita un buen funcionamiento a la organización.

De acuerdo con Ruíz, (2018) COBIT se fundamenta en 5 principios:

1. Satisfacción de necesidades de las partes interesadas
2. Cubrimiento integral de la compañía
3. Aplicación de un solo marco integrado
4. Enfoque holístico en su aplicación
5. Se retira el gobierno de la administración.

Su metodología es por procesos, a través de cuatro dominios:

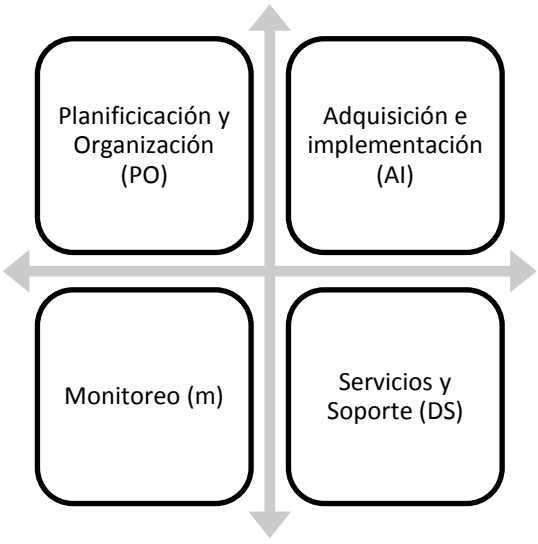

Figura 3 cuatro dominios del modelo COBIT
Fuente: Ruíz, (2018, p. 53)

Karczewska, (2017) indica que se trata de un marco general de estándares de tipo integral para la gestión de las organizaciones corporativas. Su objetivo se orienta fundamentalmente a la generación de valor, optimizando niveles de riesgo, sumando beneficios y el buen uso de los recursos. Se conoce como un marco integrador de auditoría.

1.6.2. Marco conceptual (Glosario de términos)

Activos: Hace referencia a la aquella información que se encuentra relacionada con el tratamiento de la información, sean sistemas, soportes, archivos, etc.

Amenaza: la posible causa de daño a un objeto de información. Son agentes que invaden y explotan los mecanismos de seguridad de un sistema (Lara, 2015). La amenaza en el lenguaje informático hace referencia a una determinada acción que se hace bajo el aprovechamiento de la vulnerabilidad para atentar con un sistema de información. Estas pueden tipificarse como robos, fraudes, entre otros.

Análisis de riesgos: uso sistemático de la información disponible para identificar y evaluar riesgos. Cuando se hace análisis de riesgo es por la probabilidad de presentarse una alteración en el sistema de seguridad de una determinada organización. Y este se materializa en amenaza, toda vez que se ha consumado, es decir, cuando ya se está ante la presencia de las pérdidas o el robo (INCIBE, 2017). El sistema de protección antivirus puede comprender: una Unidad de Evaluación de Comportamiento de Procesos para identificar los programas existentes en los equipos del usuario y clasificarlos en programas normales y programas sospechosos; una Unidad de Monitoreo de Programas para monitorear y registrar las acciones y / o comportamientos de los programas

Antivirus: Según Nachenberg (2000), El antivirus constituye un sistema que se maneja a través de un método y tienen como propósito examinar archivos para detectar amenazas o ataques que puedan alterar su funcionamiento. Estos se encuentran asociados a computadoras. Sirven además para detectar y bloquear algún tipo de virus que intente afectar el sistema de una computadora.

Ataques: se refiere a aquella agresión, en cuyo caso, el atacante monitorea los canales de comunicación no ingresando datos ni modificando nada. De acuerdo a los aportes de Hernández y Mejía, (2015) los ataques son agresiones potenciales que se realizan al sistema informático de una determinada organización, empresa, los cuales son perpetrados principalmente cuando el sistema esta vulnerable o cuando estos presentan fallas.

Cooperativas: Asociación voluntaria de grupos o personas que se unen con el fin de buscar satisfacción a necesidades en común, sean estas económicas, sociales, culturales entre otras. Agrupación que se hace mediante la figura de una empresa con personalidad jurídica, propiedad social y derecho privado, en igualdad de condiciones y en un espacio de relaciones democráticas y trasparente (Ley Orgánica de Economía Popular y Solidaria, 2018).

Confidencialidad: propiedad que determina que la información no está disponible para personas no autorizadas.

Controles: Estos son los mecanismos para monitorear y controlar acciones que se consideran sospechosas y pueden tener un impacto en los recursos de información.

Disponibilidad: la propiedad determina que la información es accesible y utilizable por la persona debidamente autorizada.

Fuente de información: qué es válido y contiene información importante de la compañía que necesita ser protegida.

Hackers: Son personas o agentes que se encargan de hacer robos de información o ingresan a los sistemas de manera irregular para alterar o hurtar información, estos pueden generar daños, desconfiguración y alteración de los sistemas informativos a través de la web (Lara, 2015)

Hardware: Este se refiere a la plataforma física del computador, es decir, a las máquinas, los cables, conexiones, etc. Está compuesto por el sistema de almacenamiento, el procesador, los dispositivos de entrada y de salida. Estos son dispositivos o sistemas que están diseñados para el procesamiento de una cantidad importante de información.

Información: Hace referencia a cualquier tipo de datos o comunicación encartada en archivos, documentos, sean físicos o digitales.

Integridad: se refiere a aquel sistema en donde cada una de sus partes se encuentra engranadas de forma correcta.

Riesgo: nivel de exposición de un activo que permite que ocurra una amenaza.

Seguridad: se conoce como una interrelación de forma dinámica entre lo quien protege y quien agrede con el fin de conservar el valor tratado. Su objetivo se orienta hacia el mantenimiento de la integridad y la privacidad de los datos.

Seguridad de información 1: agrupa la tecnología, y la organización, en relación a la primera, esta se soporta en los equipos y dispositivos tecnológicos. Y en cuanto a la organización está la desarrollan las personas. Se basa en los principios de integridad, confidencialidad y disponibilidad.

Seguridad de la información 2: La seguridad de la información hace referencia a los riesgos, a las amenaza, análisis de prácticas de escenarios e implementación de los esquemas normativos que permitan asegurar un nivel de confianza en el sistema de información de una determinada empresa. Esta se enfoca en analizar los posibles riesgos, se refieren a las normativas que orienta los pasos y procesos a seguir de forma general y en cada una de las instancias que conforman la organización empresarial, y responde además, al plan de la máxima autoridad.

Sistema de la información: Este hace referencia a una línea estratégica de seguridad que se desarrollan en las empresas a manera de prevención e intervención de los sistemas. Además, se orienta a la agrupación no dependiente de recursos informativos sistematizados, procesados, transmitidos y definidos a través de diversos mecanismos pudiendo ser digitales o no.

Seguridad informática: Está a diferencia de la anterior, hace referencia a la implementación de un conjunto de procesos, técnicas y métodos que buscan la protección de la información en un dispositivo electrónico. Es decir, implementan tecnologías como los antivirus para proteger los sistemas operativos de las amenazas que se encuentran latentes en la nube. Posee tres características

importantes que lo diferencian de la seguridad de información: que se refiere a la configuración de una forma segura, es una técnica que implica brindar protección a los equipos. Y se realiza en un acto de auditoria de los sistemas operativos de los equipos tecnológicos.

SGSI: Se trata de una perspectiva o enfoque de gestión sistemática de la información de importancia para la empresa, que le permita a estar alcanzar los estándares de seguridad requeridos. Este Sistema abarca procesos, personas, sistemas a través de aplicaciones de procesos y evaluaciones de riesgos.

Software: Estos son programas que poseen en su estructura las órdenes según la cual trabaja un computador. Existen diversos, pueden ser de sistemas o de aplicaciones específicas empresariales. Poseen sistemas operativos a través de los cuales administrar los recursos del computador y a la vez poseen control o dominio en su funcionamiento (Ponte, 2015). El más usado es el Windows, aunque hoy por hoy, existen otros que se relacionan con aplicaciones y dispositivos inteligentes. Así también, aplicaciones, sistemas operativos, CPU (Borghello, 2001).

Virus: Los virus informáticos constituyen un software que altera el normal funcionamiento de un equipo informático. En atención a Prieto & Pan, (2007)**,** estos ingresan y se alojan por lo general, en la memoria del computador y de esta manera, se podrán ejecutar, y por ende, mantener el control de las operaciones del sistema. Los más comunes se les llama gusanos y los troyanos, se ocultan y se reproducen en los ficheros de los archivos, pudiendo llegar a destruir datos, o el control remoto del sistema.

Vulnerabilidad: Este concepto está asociado a la debilidad presentada por el sistema, activo o control de estos, generando un escenario en el que puede ser invadida por amenazas (MINTIC, 2020).

CAPITULO II. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de investigación

El diseño de una investigación de conformidad con lo que establece Hernández, Fernández, y Baptista, (2014), se refiere al plan o estrategia sobre los procedimientos en general, planeados por el investigador para lograr los objetivos propuestos en el estudio. En tal sentido, la presente investigación se planteó optimizar los estándares de seguridad de una muestra de cooperativas de ahorro y crédito, localizadas en la ciudad de Guayaquil, a través de un modelo de GSI.

Pero para ello, fue necesario empezar por analizar e identificar los problemas de seguridad que estas cooperativas presentaban en sus sistemas internos de información. Para lograr estos objetivos se planteó un diseño de tipo no experimental, por cuanto no se sometieron las variables a experimentos, ni se manipularon deliberadamente.

2.1.1. Alcance del estudio

En relación con el alcance del estudio, este posee un nivel descriptivo-analítico de la información, porque en primera instancia, se definieron y describieron las variables establecidas, en función de la información recolectada de las cooperativas, documentos y archivos oficiales, así como de algunos funcionarios de estas organizaciones. Seguidamente, de la descripción se pasó en segunda instancia, al análisis y contrastación de la información, en la búsqueda e identificación de los principales problemas, que, en el orden de seguridad de la información, poseen las cooperativas de ahorro y crédito que se ubican en la ciudad de Guayaquil.

Es importante señalar, que la información provendrá de los informes de gestión, y páginas oficiales en donde estas dejan ver sus datos principales. Además, se realizará un análisis interno de estas cooperativas de ahorro y crédito a través de una matriz FODA, para valorar los factores internos y externos que inciden en su funcionamiento. Se tomarán ideas de varios enfoques y

modelos de SGSI para establecer el modelo a seguir en la propuesta de este trabajo.

2.1.2. Enfoque de investigación

El enfoque de la investigación busca tener una amplia panorámica de la información que se obtenga de estas cooperativas, por ello, asume un enfoque mixto, el cual de acuerdo con Núñez-Moscoso, (2017), combina de manera simultánea, métodos y técnicas cualitativas como cuantitativas en la recolección de la información, como en su tratamiento. Y en la que se plantea el diseño documental como el de campo.

Este enfoque es complementario porque se alimenta mutuamente de ambos procedimientos, es riguroso y se enfoca en el objeto de estudio. De allí que, la información de origen cualitativa será la que se extraiga del análisis interno de las cooperativas, buscando la conformación de un diagnóstico lo más completo posible. Y la información cuantitativa, se extrajo de los documentos, informes, de páginas oficiales como la Superintendencia de Economía Popular y Solidaria. Así como de la información de las encuestas aplicadas a los funcionarios y responsables de la seguridad de algunas cooperativas.

2.2. Método de investigación

Como parte de este proceso de investigación se contemplaron dos grupos de métodos:

2.2.1. Métodos empíricos

En el marco de este método, se aplicó una investigación de campo, en la cual se desarrolló la experiencia y contacto con la fuente primaria. En este acto, se aplicó la encuesta a una muestra de funcionarios y encargados de la seguridad de la información de algunas cooperativas muestreadas.

De igual forma, se plantea la búsqueda de información en fuentes secundarias, constituyendo en una investigación documental. En donde se

aplicará la sistematización de la información, atendiendo a las variables seleccionadas.

2.2.2. Métodos lógicos:

En el análisis y la contrastación de la información requirió de dos métodos:

2.2.2.1. Hipotético-deductivo

En el análisis de la información se empleará el método hipotético-deductivo, el cual, a partir de las premisas, variables y objetivos buscará explicar las causas y razonar sobre estas, en función de darle una respuesta adecuada a la problemática, y llegar con ello, a unas conclusiones precisas.

2.2.2.2. El Método inductivo

Este método permite profundizar en algunos aspectos subjetivos que se desprenderán de los análisis cualitativos de la información, se combina con el sintético, en el cual se realiza un ejercicio de reducción, e interpretación de la información seleccionada.

La investigación se realizó enfocada en la factibilidad del modelo de gestión de seguridad de la información para pequeñas empresas. Del mismo modo, se formuló la hipótesis: el modelo de gestión de seguridad de la información diseñado para que las pequeñas empresas garanticen la seguridad de los recursos informáticos.

Además, se aplicó la investigación descriptiva porque esta permitió describir y analizar el problema en sus partes como delimitación temporal y espacial, para proceder con la generación de análisis críticos, contextualizaciones y antecedentes de investigación.

Estos métodos de investigación se ajustan al presente trabajo, puesto que ayudan a conocer y describir la información de interés. Además, los resultados obtenidos del estudio, fueron contrastados con los diferentes modelos de gestión de seguridad de información, con el fin de comparar y analizar las principales

ventajas y desventajas de cada uno de ellos, para la selección de un modelo que se ajuste con las características necesidades que presentaron las cooperativas en el diagnóstico.

2.3. Unidades de análisis, población y muestra

Las unidades de análisis están compuestas por las muestras de cooperativas que se encuentran ubicadas en la ciudad de Guayaquil, estas son 07 en total:

Tabla 2
Cooperativas de ahorro y crédito ubicadas en la ciudad de Guayaquil

Cooperativas de ahorro y crédito ubicadas en la ciudad de Guayaquil				
Nº	**Identificación**	**Segmento**	**Área observada**	**Contacto o informantes**
01	COOPERATIVA DE AHORRO Y CRÉDITO LA DOLOROSA LTDA.	4	Área de gestión de información	Gerente Responsable de sistemas y soporte Jefe de seguridad y riesgos
02	COOPERATIVA DE AHORRO Y CRÉDITO DR. CORNELIO SÁENZ VERA LTDA.	2		
03	COOPERATIVA DE AHORRO Y CRÉDITO EL DISCAPACITADO	2		
04	COOPERATIVA DE AHORRO Y CRÉDITO GUARUMAL DEL CENTRO LTDA.	2		
05	COOPERATIVA DE AHORRO Y CRÉDITO CUNA DE LA NACIONALIDAD LTDA.	1		
06	COOPERATIVA DE AHORRO Y CRÉDITO LOS ANDES LATINOS LTDA.	1		
07	COOPERATIVA DE AHORRO Y CRÉDITO DEL EMIGRANTE ECUATORIANO Y SU FAMILIA LTDA.	1		

Fuente: (Banco Central de Ecuador, 2021)

La población de estudio estará compuesta por 07 cooperativas, de las cuales, se estudiarán a tres (3) personas por cada cooperativa, compuestos por los gerentes, el jefe de soporte y sistema, y el de gestión de riesgo, para un total de 21 personas. De manera que, al estar identificada la población objeto de estudio, y ser una baja población de estudio, no se aplicó una técnica de muestreo probabilístico.

2.4. Variables de investigación y operacionalización

Variable independiente: Modelo de gestión

Variable dependiente: Seguridad de la información para las cooperativas AC.

Tabla 3
Operacionalización de variables

Variables	Definición conceptual	Definición operacional	Indicadores
Variable independiente: Modelo de gestión	Conjunto de políticas, procesos, lineamientos de seguridad que se establecen para resguardar la información	Contribuyen a elevar los niveles de seguridad en la organización	• Sistemas • Políticas • Normas • Principios • Procesos • Objetivos • Sanciones • Regulaciones • Procedimientos
Variable dependiente: Seguridad de la información para las cooperativas AC.	La seguridad se refiere a la preservación de la información que se posee en el sistema de una determinada organización. También se contempla la disponibilidad de información, la responsabilidad y confiabilidad de todo lo que se mantienen en el sistema.	Garantizan la seguridad del sistema	• Análisis de riesgos • Amenazas • Medidas preventivas • Controles de acceso • Los equipos • Recursos • Archivos, libros • Dispositivos electrónicos • Datos • Antivirus, antimalware

Fuente: elaboración propia

2.5. Fuentes y técnicas para la recolección de información

Las fuentes de investigación provienen de tres lugares:

- Directamente de las personas o informantes de las cooperativas
- De los documentos y archivos de páginas oficiales
- Directamente de la gestión administrativa interna de las cooperativas

La técnica usada es la encuesta, y el cuestionario tipo de preguntas tipo escala para la obtención de la información.

2.6. Tratamiento de la información

- Revisión crítica de la información recopilada; es decir, la limpieza de información incorrecta, contradictoria, incompleta, irrelevante y otros errores.
- Recopilación, en ciertos casos individuales para corregir los errores de respuesta.
- Gestión de la información (adaptación de principales ideas, opiniones y percepciones durante la encuesta)
- Análisis de datos para presentar los resultados.

CAPITULO III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual

En este capítulo, se lleva a cabo un análisis de la situación actual de las Cooperativas de Ahorro y Crédito del segmento en cuanto a la utilización de los Sistemas de seguridad de información Gerencial.

En Ecuador, la seguridad de la información se encuentra amparada por diversas leyes, cuando demanda la implementación de la misma en todas las instituciones financieras del país, las cuales están orientadas a sostener de forma efectiva los procesos de las entidades que deben incluir la administración adecuada de sus recursos humanos, procesos y tecnología de información, para garantizar la continuidad de sus operaciones ante eventos de contingencia. En este sentido, algunas de las leyes que respaldan la seguridad de la información de las cooperativas de ahorro y crédito en Ecuador se muestran a continuación:

- Ley del Sistema Nacional de Registro de Datos Públicos.
- Normas técnicas de seguridad adoptadas por Ecuador de las ISO 27000.
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
- Ley de Comercio Electrónico, firmas electrónicas y mensaje de datos
- Código de procedimiento Penal de Ecuador, infracciones informáticas

En Ecuador, las cooperativas y las pequeñas empresas, que se clasifican como Pymes, tienen una participación importante en la economía nacional. En particular, las cooperativas de ahorro y crédito que nacen como un emprendimiento orientado a la gestión financiera. Sin embargo, debido a la falta de procesos establecidos y recursos limitados, la mayoría de estas cooperativas desconoce estos procesos y mecanismos de seguridad que les permiten adaptarse y mantenerse en el mercado. En este sentido, muchas de las pequeñas cooperativas de ahorro y crédito, han tenido que sortear grandes dificultades en sus sistemas de información, principalmente, porque no han establecido políticas especializadas que les facilite a enfrentar las amenazas a las que están expuestas sus plataformas tecnológicas, lo que conlleva a que sean menos competitivas en el mercado.

Cada evento de riesgo identificado acerca de la información debe ser monitoreado y seguido para una adecuada gestión. Para ello, se le debe otorgar la misma importancia que a otros tipos de riesgos gestionados por las instituciones financieras. Esto se debe a que, dentro de su control, puede ser difícil de cuantificar por la falta de información histórica que permita establecer claramente la frecuencia con la que ocurren los eventos de riesgo y el impacto que causan.

Por ello, a continuación, se expone una matriz DAFO que describe las fortalezas, oportunidades, debilidades y amenazas que presentan algunas cooperativas de ahorro y crédito de este sector, además del análisis de los resultados de las entrevistas de la visita de campo y comprender el estado actual de las cooperativas. Esto proporciona la base para la implementación de mejoras en beneficio de las cooperativas pertenecientes a este sector.

Tabla 4
Matriz FODA de Cooperativas de ahorro y crédito

	Fortalezas	Debilidades
Interno	Confianza y aceptación de socios Compromiso de los gerentes Contribución al desarrollo por parte de autoridades regionales; Proporciona servicios financieros y no financiero Atención a segmentos de mercado donde no llegan los bancos.	Escasa planificación estratégica No existen procesos a nivel institucional Alto índice de activo improductivos Dispone de poca información para análisis Insuficiente infraestructura tecnológica Poca o nula seguridad informática. No existen plan de capacitaciones
	Oportunidades	**Amenazas**
Externo	Avances tecnológicos que permite integrar información a la infraestructura Control de las redes de la Cooperativa Brindar seguridad a los asociados Plena confidencialidad de datos	Normativas sobre la seguridad de la información Cooperativas de ahorro y crédito con mejor seguridad de la información Deserción de socios Fuga de información de clientes Fuga de información sobre la institución. Ciberataques

Fuente: Elaboración propia

De acuerdo a lo reflejado en la matriz FODA, se puede observar que actualmente las cooperativas de ahorro y crédito no aplican sistemas o modelos

de gestión de la seguridad de la información, lo cual las vuelve vulnerables debido a que se encuentran expuestas a numerosos riesgos en sus sistemas informativos o de información que podrían implicar diversos problemas, que van desde la fuga de información hasta la deserción de usuarios. Por lo que, sus metas a corto, mediano y largo plazo pueden verse profundamente limitadas. Adicionalmente las cooperativas de este sector, generalmente no emplean herramientas apropiadas que les permitan una adecuada toma de decisiones.

En este panorama, en la actualidad las cooperativas de ahorro y crédito en Guayaquil, afrontan diversos riesgos en relación a la información, principalmente por:

- Infraestructura física que no tiene la seguridad necesaria para proteger los recursos y cumplir con los requisitos establecidos por las autoridades.
- Infraestructura tecnológica insuficiente para automatizar los procesos.
- Existencia de procesos indocumentados o mal diseñados en la gestión de la información.
- Capacidad insuficiente para la implementación de nuevos productos y servicios a los asociados.
- Competencia elevada de otras cooperativas más grandes y con más recursos físicos y tecnológicos.
- Regulaciones más amplias impuestas por los organismos de control.
- Ataques por hacker o software maliciosos.
- Fuga o extravío de información.

3.2. Análisis comparativo, evolución, tendencias y perspectivas

Se espera que: La gestión y administración de la información generada por las pequeñas empresas del sector de cooperativa de ahorro y crédito de la ciudad de Guayaquil muestre exiguo interés por parte de los directores de las empresas de este sector, ya sea por desconocimiento o falta de recursos para invertir en temas de seguridad de la información. Por lo tanto, con base en estándares internacionales, se deben definir pautas de seguridad que estén vinculadas a este tipo de empresa y que permitan la gestión correcta y segura de los recursos de información.

3.3. Presentación de resultados y discusión

1. ¿Cree que es importante la seguridad de la información de la institución?

Tabla 5
Importancia de la seguridad de información

Categoría	Frecuencia	Porcentaje
Si	19	90%
No	2	10%
Total	21	100%

Fuente: elaboración propia

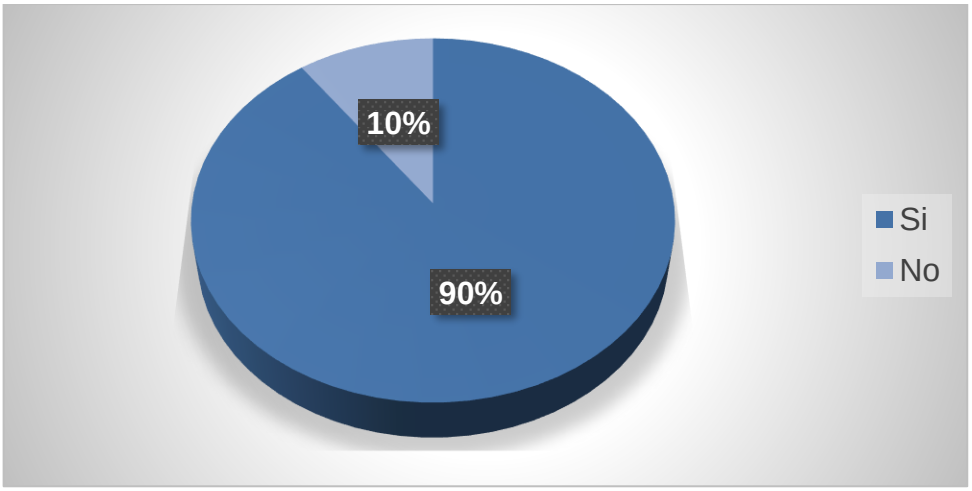

Figura 4 Importancia de la seguridad de información
Fuente: elaboración propia

Análisis: con base a las respuestas se evidenció que, el 90% de los encuestados considera importante la seguridad informática, mientras que el 10% restante no lo considera relevante. Lo cual demuestra la importancia que le atribuyen los gerentes de las instituciones financieras seleccionadas a la seguridad de información.

2. **¿Considera que la infraestructura informática de la institución es vulnerable?**

Tabla 6
Vulnerabilidad de la infraestructura informática

Categoría	Frecuencia	Porcentaje
Vulnerable	3	14%
Medianamente vulnerable	10	48%
Muy vulnerable	8	38%
Total	21	100%

Fuente: elaboración propia

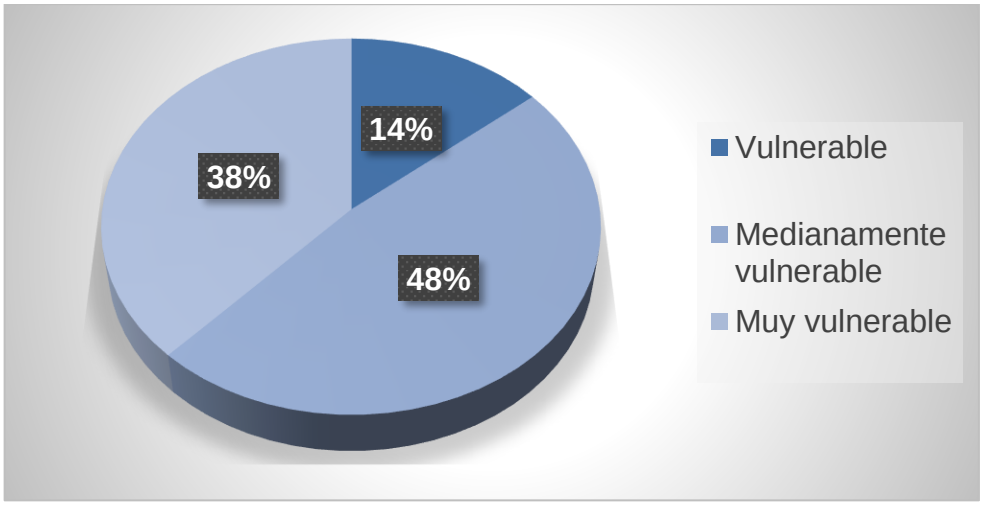

Figura 5 Vulnerabilidad de la infraestructura informática
Fuente: elaboración propia

Análisis: En relación a la vulnerabilidad de la infraestructura informática de las cooperativas de ahorro y crédito, de la totalidad de los encuestados, el 48% afirmó que la entidad financiera para la que labora, posee una infraestructura informática medianamente vulnerable, por su parte el 38% la considera muy vulnerable y el 14% restante cree que es vulnerable. Estos datos permiten reconocer la poca seguridad de información que manejan los entes financieros seleccionados.

3. ¿La empresa posee estrategias para la protección de información?

Tabla 7
Estrategias de protección de información

Categoría	Frecuencia	Porcentaje
Si	2	10%
No	19	90%
Total	21	100%

Fuente: elaboración propia

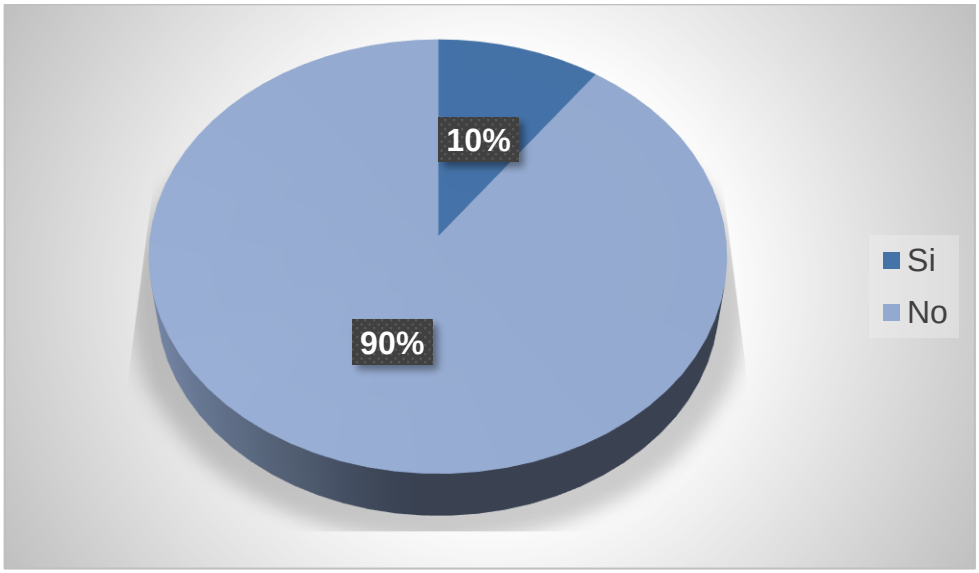

Figura 6 Estrategias de protección de información
Fuente: elaboración propia

Análisis: del 100% de los encuestados, se encontró que el 90% afirman que la institución financiera para la cual laboran no aplica estrategias para la protección de información de los activos del Ente, mientras que el 10% de ellos manifiesta que sí se emplean estrategias para resguardar los datos. De estos resultados se puede señalar que la falta de estrategias para la protección de información refleja la ausencia de la aplicación de procesos de seguridad en la organización.

4. ¿La empresa ha sufrido de robos de información?

Tabla 8
Robos de información

Categoría	Frecuencia	Porcentaje
Si	5	24%
No	16	76%
Total	21	100%

Fuente: elaboración propia

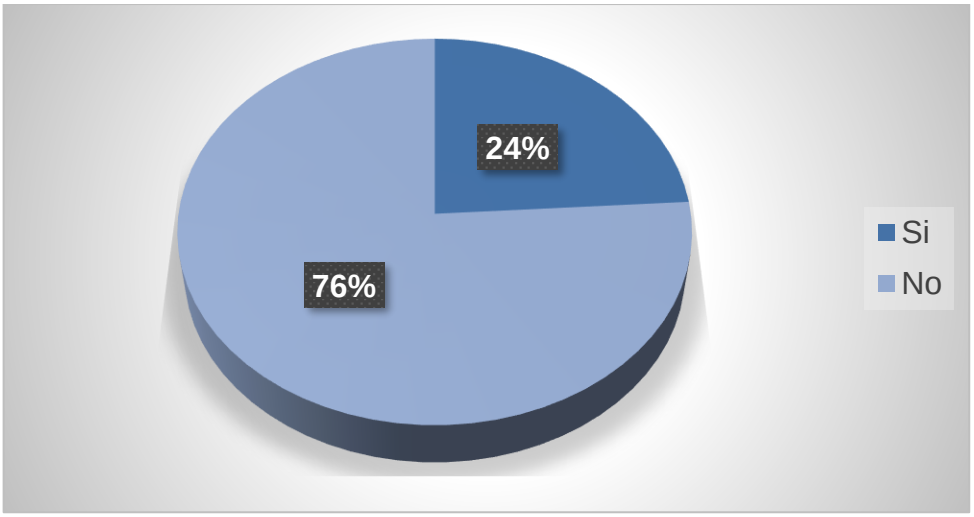

*Figura 7 R*obos de información
Fuente: elaboración propia

Análisis:

Del 100% de los sujetos estudiados, se pudo encontrar que el 76% de ellos opinó que no se han presentado robos de información en los sistemas de sus empresas, sin embargo, un 24% indicó que sí, esto permite inferir que sí se ha visto amenazado en algún momento el sistema de seguridad de información de algunas cooperativas. Requiriendo que se implemente mejoras en los procesos y políticas que se llevan a cabo en las mismas.

5. ¿Quiénes tienen acceso a la información de los activos?

Tabla 9
Personal con acceso a información de activos

Categoría	Frecuencia	Porcentaje
Gerente	11	52%
Encargado de sistema y soporte	7	33%
Jefe de seguridad y riesgo	3	14%
Gerente de contabilidad	0	0%
Gerente de caja	0	0%
Gerente de planeación financiera	0	0%
Total	21	100%

Fuente: elaboración propia

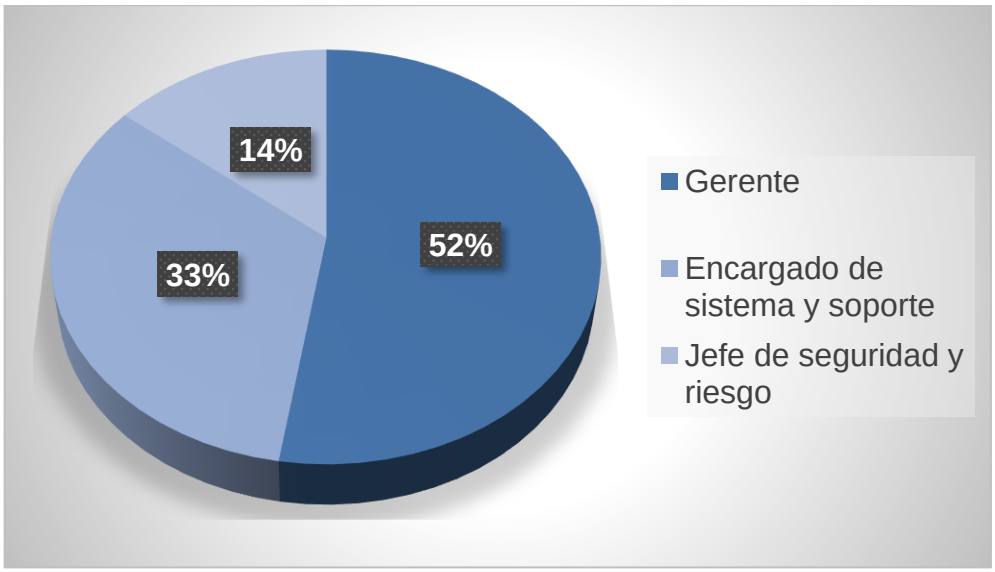

Figura 8 personal con acceso a información de activos
Fuente: elaboración propia

Análisis:

En relación con el acceso de las personas a los sistemas de seguridad de las empresas, se pudo conocer que el 52% lo tienen los gerentes, seguido de un 33% con acceso, el personal encargado de sistema y soporte, y solo un 14% tienen acceso al sistema, que son los jefes de seguridad. Esto permite indicar que la mayor responsabilidad recae en los gerentes en cuanto a la salvaguarda de datos e información de las cooperativas.

6. ¿La empresa ha sufrido de alteración de información?

Tabla 10
Alteraciones de información en institución

Categoría	Frecuencia	Porcentaje
Si	17	81%
No	4	19%
Total	21	100%

Fuente: elaboración propia

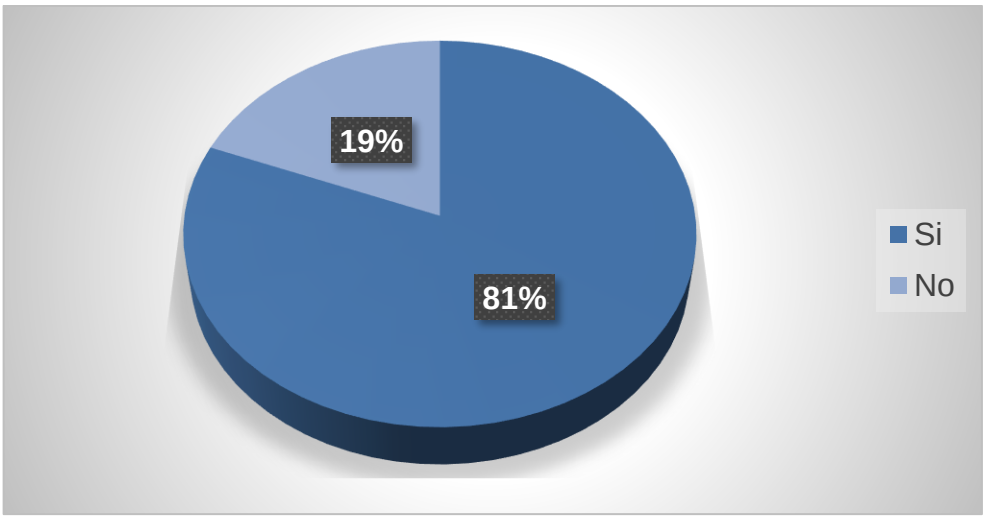

Figura 9 Alteraciones de información en institución
Fuente: elaboración propia

Análisis:

En relación con las alteraciones sufridas por las cooperativas, se encontró que el 89% si ha tenido en algún momento este tipo de alteraciones, mientras que el 19% indicó que no. Es importante destacar que estas alteraciones podrían ser frecuentes, y en muchos casos se pueden manejar, sin embargo, de no tener un sistema de seguridad sólido, estas alteraciones podrían convertirse en incontrolables, y generarían grandes amenazas para el sistema.

7. **¿La red empleada por la entidad financiera posee un sistema de seguridad de información?**

Tabla 11
Seguridad de la red empleada por la institución

Categoría	Frecuencia	Porcentaje
Si	9	43%
No	12	57%
Total	21	100%

Fuente: elaboración propia

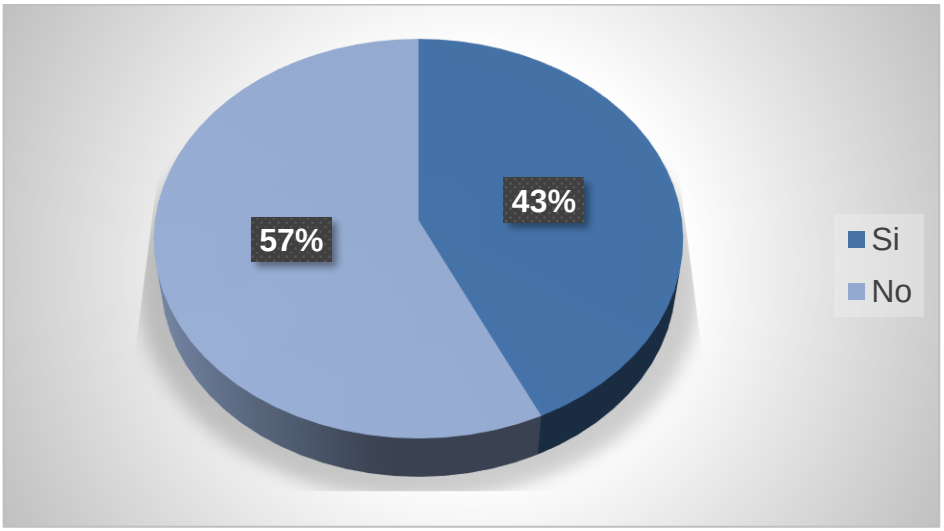

Figura 10 Seguridad de la red empleada por la institución
Fuente: elaboración propia

Análisis:

Al momento de realizar la encuesta acerca de la existencia de algún sistema de seguridad de la información en la entidad, se pudo comparar que, un 57 % de la población manifestó no tener alguno, mientras que un 43 % expresó que sí poseía alguno. Esto demuestra que un mayor porcentaje de cooperativas de ahorro y crédito no poseen sistemas que les ayude al resguardo de su información.

8. **¿Considera que la información de activos tiene amenazas relevantes?**

Tabla 12
Amenazas a información de activos

Categoría	Frecuencia	Porcentaje
Si	18	86%
No	3	14%
Total	21	100%

Fuente: elaboración propia

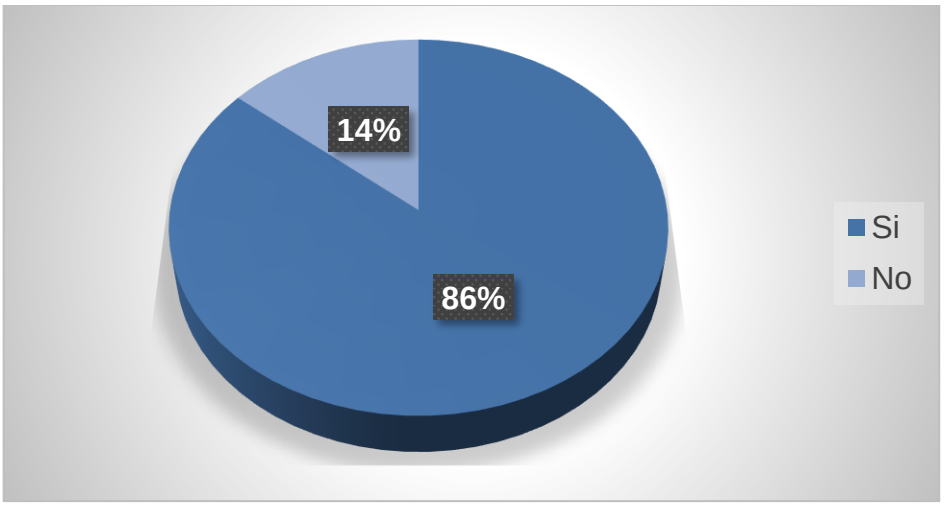

Figura 11 amenazas a información de activos
Fuente: elaboración propia

Análisis:

En cuanto a la pregunta número 8, sobre las amenazas relevantes de los activos, se pudo constatar que, un 86 % de la población considera que, si existen amenazas en este sentido en su entidad, por otro lado, solo el 14 % de la población manifestó no presentar este tipo de amenazas. Como los activos se encuentran asociados directamente con el funcionamiento y las metas de cada organización, este tema debe tener muy en cuenta para que una entidad logre sus objetivos establecidos.

9. **¿La institución financiera aplica controles adecuados a la información que maneja?**

Tabla 13
Controles aplicados al manejo de información en institución financiera

Categoría	Frecuencia	Porcentaje
Si	8	38%
No	13	62%
Total	21	100%

Fuente: elaboración propia

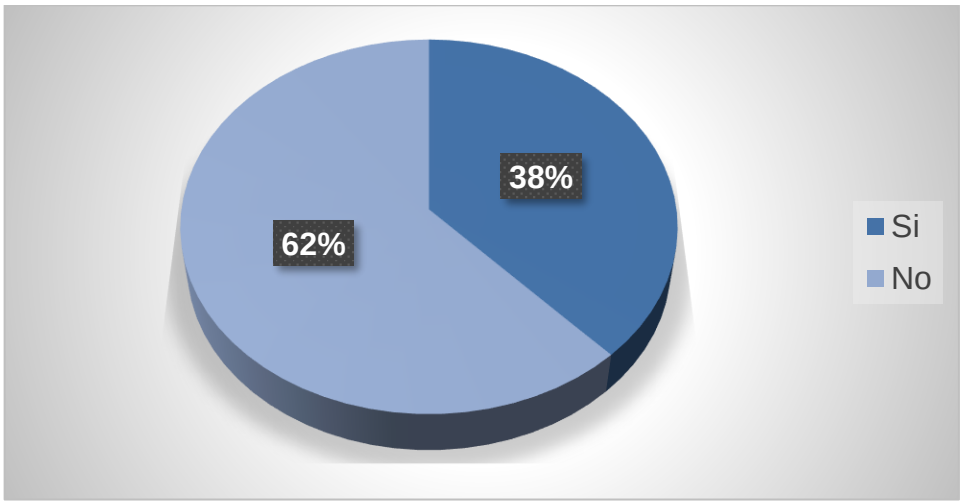

Figura 12 Controles aplicados al manejo de información en institución financiera
Fuente: elaboración propia

Análisis:

Sobre los controles a la información aplicados en las entidades que expuesto que, un 62 % de la población manifestó que no se realiza control alguno, mientras que el restante 38 % manifestó que si se aplican. El control sobre la información es un punto crucial para toda organización si quieren en materia de seguridad informativa, esto contribuye al correcto funcionamiento de todo sistema de seguridad de información de todo sistema aplicado.

10. ¿La institución posee políticas para el tratamiento y manejo de la información?

Tabla 14
Políticas y manejo de información

Categoría	Frecuencia	Porcentaje
Si	6	29%
No	15	71%
Total	21	100%

Fuente: elaboración propia

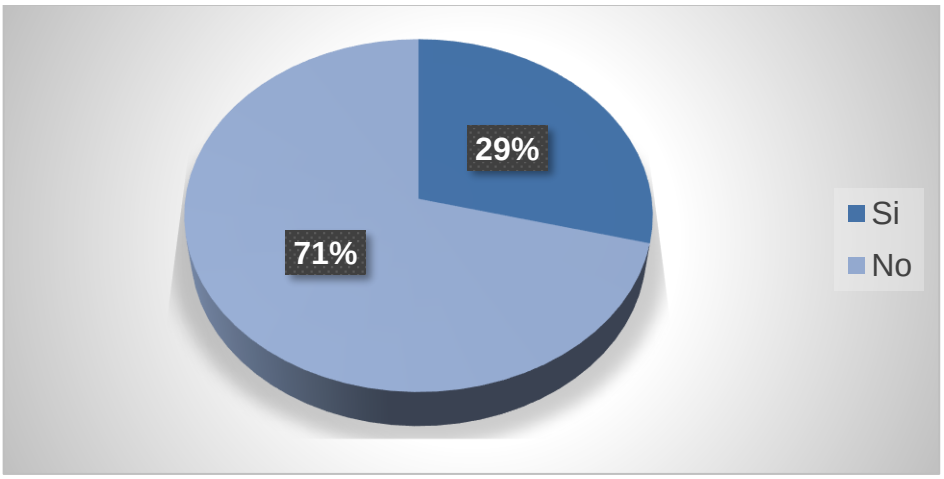

Figura 13 Políticas y manejo de información
Fuente: elaboración propia

Análisis:

En relación a la pregunta 10 sobre la existencia de políticas para el manejo de información se encontró que, un 71 % de la población manifestó que sus instituciones no poseen dichas estrategias, y solo un 29 % manifestó que si las posee. Sobre este punto, es importante destacar que las políticas resultan de vital importancia para una correcta seguridad de la información, al ser una declaración de reglas para acceder a la información y a los recursos.

3.4. Discusión de los resultados

Como se ha expuesto anteriormente las encuestas fueron dirigidas a las cooperativas de ahorro y crédito de la ciudad de Guayaquil que, en este caso, fueron un total de 7, de las cuales se encuestaron a 3 personas que estuvieran relacionadas o tuvieren conocimientos acerca de la seguridad de la información en su entidad. Es así como la población encuestada estuvo comprendida por gerentes, jefes de soporte y jefes de gestión de riesgos.

La encuesta estuvo orientada a exponer la situación actual de las entidades en relación a la seguridad de la información de manera que sirva como marco referente para el desarrollo del modelo. En este sentido, sobre la importancia que asignaban los encuestados a la seguridad de la información se observó una alta frecuencia (90%) en la respuesta positiva, lo que deja ver que los encuestados reconocen la trascendencia que puede tener la seguridad informativa dentro de sus entidades.

Pese a lo mencionado, a medida que avanzaba la encuesta se pudo constatar que las entidades no poseían sistemas, estrategias o políticas orientadas al resguardo de su información y que les ayudará a conseguir sus objetivos de forma óptima. Así, por ejemplo, al preguntar sobre si la entidad poseía estrategias para la protección de la información, quedó expuesto que un alarmante 90 % manifestó no tenerlas. De esta forma, aunque las personas encargadas reconozcan la importancia del tema tratado, es evidente la carencia de aplicación de sistemas o modelos para la seguridad de la información.

Este tipo de situación podrían se perjudiciales para las entidades, que pueden ser victimas de robos o alteraciones de su información. En este caso, quedó registrado una baja frecuencia de robos de información, solo el 24 %, sin embargo, no es un porcentaje que hay que menospreciar, considerando las repercusiones que esto podría acarrear a toda la entidad. Por otro lado, si se registró una alta frecuencia en las alteraciones de la información, un total de 81 % de toda la población encuestada manifestó haber sufrido esto en su institución, lo que nuevamente refleja las consecuencias de no poseer sistemas orientados al resguardo de la información.

Por otro lado, al preguntar sobre si la entidad poseía sistemas de seguridad de información, un 57 % manifestó no tenerla, lo denota que un mayor porcentaje de cooperativas de ahorro y crédito no poseen sistemas que les ayude al resguardo de su información. Es así, como todos los resultados muestran la imperativa necesidad en las cooperativas de ahorro y crédito de la ciudad de Guayaquil de la aplicación de modelos, sistemas, políticas o estrategia dirigidas al aseguramiento de su seguridad informativa, a fin de que puedan tener un control pleno de sus activos, reducir amenazas y lograr metas establecidas.

CAPITULO IV. PROPUESTA

4.1. Justificación

Debido a que las cooperativas de ahorro y crédito en Guayaquil presentan eventualidades que repercuten en las operaciones, las cuales tiene su origen en la insuficiencia o incapacidad de una buena gestión sobre los incidentes de seguridad de la información, se hace necesario el desarrollo de un modelo de gestión de seguridad de la información en las empresas de este sector. Es por ello que, la investigación expuso algunas de las necesidades de las cooperativas y las diferentes formas de gestionar los incidentes de seguridad de la información alrededor del mundo.

Basados en los resultados de la investigación se propone como alternativa o solución viable la adopción de un modelo de gestión de seguridad de la información que contemple sobre todo lo establecido en las series de la norma ISO 27000, que tratan sobre todo de la prevención, detección y tratamiento de tiempo las eventualidades que expongan la información de una institución, así como del establecimiento de políticas y roles que garanticen el desarrollo y continuidad del modelo adoptado.

4.2. Propósito General

El objetivo de realizar un modelo con un enfoque estructurado paso a paso para la implementación de políticas orientadas a la gestión de incidentes de seguridad de la información para proteger a las cooperativas de ahorro y créditos de posibles incidentes, riesgos y amenazas. Por lo que, el propósito es que puede ser implementado o tomado como ejemplo de otra organización de la misma o similar naturaleza.

La política de seguridad tiene como objetivo comprometer a la administración y a todo el personal involucrado en las actividades de las organizaciones a quien se dirige el modelo a una cultura de seguridad que crea un entorno más creíble para lograr los objetivos de la organización. Por otro lado, los controles seleccionados tienen como objetivo mejorar los aspectos vulnerables que podrían ser explotados por las amenazas que actualmente están siendo

detectadas por las investigaciones realizadas en las cooperativas de ahorro y crédito.

4.3. Desarrollo

4.3.1. Mecanismos y medidas en la seguridad informática

La seguridad informática debería, en principio, estar respaldada por la creencia de que el equipamiento desde el que se envía y recibe la información debe estar debidamente protegido. Las implementaciones de seguridad de la información deben basarse en estándares y normas que guíen la correcta ejecución de la seguridad de la información.

De manera que, todas las instituciones financieras deben cumplir con normas y estándares específicos que regulen su funcionamiento. En este sentido, el proceso técnico también debe cumplir con las normas y estándares. Gran parte de estos estándares están fundamentados en las normas ISO correspondientes, junto con metodologías establecidas para la gestión de los distintos procesos dentro de una organización. Es por ello que, mediante los fundamentos de las Normas ISO 27001 se presentan cada uno de los procedimientos para la planeación, diseño e implementación de la seguridad informática dentro de las redes de datos de las cooperativas de ahorro y crédito.

ISO 27001, su propósito, es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma menciona la siguiente importancia:

- Comprender los requisitos de seguridad de la información de la organización.
- Implementar y operar áreas relacionadas con la gestión de riesgos de seguridad, controles de seguridad generales definidos y seguridad de los recursos físicos, ambientales y humanos.
- Monitorear y verificar el desempeño y la efectividad del SGSI.

El propósito de un sistema de gestión de seguridad de la información es reconocer, asumir, gestionar y minimizar los riesgos de seguridad de la información de una organización de forma documentada, sistemática, estructurada, reproducible, eficiente y adaptada a cambios en riesgo de medio ambiente y tecnología.

Los sistemas de gestión de seguridad de la información contribuyen a establecer políticas y procedimientos relacionados con los objetivos comerciales de una organización para mantener un nivel de exposición que siempre es inferior al nivel de riesgo que la propia organización prevé. Para garantizar que la seguridad de la información se gestione correctamente, primero debe identificar su ciclo de vida y los aspectos relevantes empleados:

- **Confidencialidad**: No se proporcionará ni divulgará información a personas, entidades o procesos no autorizados.
- **Integridad**: Mantener la precisión e integridad de la información y cómo se procesa.
- **Disponibilidad**: Acceso y uso de la información y sistemas de procesamiento por personas, entidades o procesos autorizados, según sea necesario.

Para el establecimiento y control de un Sistema de Gestión de la Seguridad de la Información fundamentado en la norma ISO 27001, se utiliza el ciclo continuo PDCA:

- **Plan** (planificar): establecer el SGSI.
- **Do** (hacer): implementar y utilizar el SGSI.
- **Check** (verificar): monitorizar y revisar el SGSI.
- **Act** (actuar): mantener y mejorar el SGSI.

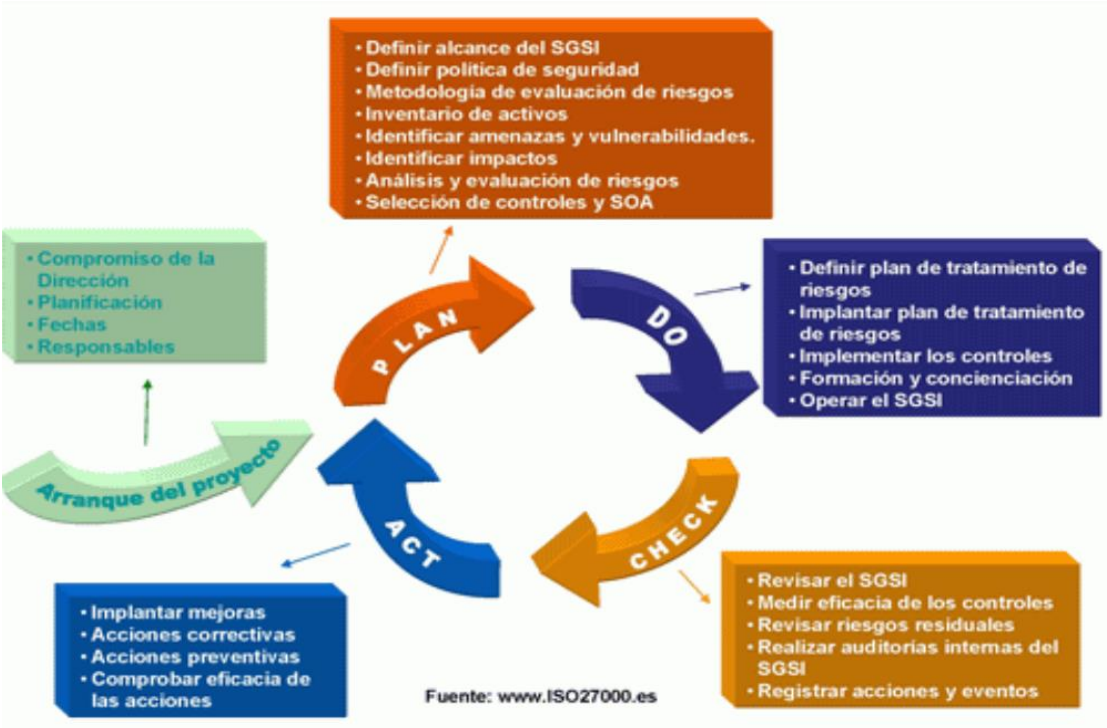

Figura 1 Ciclo PDCA
Fuente: tomado de (ISO27000.es, 2020)

4.3.1.1. Plan = Establecer con planificación

Establecer el alcance del SGSI en términos de negocio, organización, ubicación, activos y tecnología, incluyendo, además, los detalles y la legitimidad de alguna exclusión en caso de existir. Es importante definir los límites del SGSI, ya que dicho sistema no tiene que abarcar toda la organización. Es recomendable más bien, comenzar con un rango limitado, además de crear un mapa de procesos del negocio, definir claramente la interfaz fuera del alcance, identificar a los terceros (proveedores, clientes, etc.) que pueden afectar la seguridad de la información del alcance, y crear mapas de alto nivel de redes y sistemas, ubicaciones físicas, organigramas, definición clara de los requisitos legales y contractuales, relacionados con la seguridad de la información.

En este sentido, las políticas del SGSI son un documento generalizado, que funciona como una especie de "declaración de intenciones" de la administración general, la cual que debe:

- Contener el marco general de la organización y los objetivos de seguridad de la información.
- Considerar las necesidades de la organización de negocio además de considerar los requerimientos legales o contractuales acerca de la seguridad de la información.
- Alinearse con el contexto estratégico de gestión de riesgos de la organización en la cual se establecerá el SGSI.
- Establecer criterios para la evaluación de los riesgos.
- Tener aprobación por la dirección.

Determinar un enfoque de evaluación, utilizando SGSI y métodos de evaluación de riesgos que sean apropiados para los requisitos de la organización. Se deben establecer criterios de aceptación de estos riesgos y definir estrategias de aceptación de los mismos que especifiquen niveles de riesgo aceptables. Existen muchas metodologías estandarizadas para la evaluación de riesgos y las organizaciones pueden elegir una de ellas, aplicar varias combinaciones o crear la propia.

- **Identificación de riesgos:**

1. Identificar todos los activos de información dentro del alcance del SGSI y los administradores directos (llamados propietarios) que sean de valor para la organización.
2. Identificar las amenazas asociadas con los activos identificados.
3. Identificar las amenazas relevantes asociadas a los activos identificados.
4. Identificar vulnerabilidades que podrían ser explotadas por las amenazas.
5. Identificar el impacto potencial de la pérdida de confidencialidad, integridad y disponibilidad en cada activo.

- **Análisis y evaluación de riesgos:**

1. Evaluar el impacto en la organización de las brechas de seguridad con pérdida de confidencialidad, integridad o disponibilidad de los activos de información.

2. Evaluar, de manera realista, posibles brechas de seguridad en relación con amenazas, vulnerabilidades, impactos de activos y controles ya implementados.
3. Estimar el nivel de riesgo.
4. Determinar si un riesgo es aceptable o debe ser abordado de acuerdo con los criterios de tolerancia al riesgo previamente establecidos.

- **Identificar y evaluar diferentes opciones para el tratamiento de los riesgos:**

1. Aplicar una gestión adecuada (mitigación).
2. Aceptar el riesgo (de forma consciente), siempre que se sigan cumpliendo las políticas y estándares establecidos para la aceptación del riesgo.
3. Evitar riesgos.
4. Transferir total o parcialmente el riesgo a terceros.

Figura 2 Gestión de riesgos basado en la serie de ISO 27000
Fuente: tomado de (ISO27000.es, 2020)

Los riesgos de seguridad de la información son peligros para el negocio y no solo los administradores también, los cuales pueden tomar decisiones sobre la

aceptación final en cada revisión y / o acción de tratamiento que deban incorporar para la mejora.

En este sentido, resulta conveniente determinar una declaración de aplicabilidad también denominada SOA (Statement of Applicability) en la que se incluya:

- El propósito y control de los controles seleccionados y por qué fueron seleccionados.
- Metas y controles de gestión ya establecidos.
- Los objetivos de manejo y los casos excluidos y el por qué fueron excluidos. Este es un mecanismo que también permite detectar la posibilidad de abandonos involuntarios.

4.3.1.2. Implementar el SGSI

En correspondencia con la implementación es necesario:

- Estipular un plan de tratamiento de riesgos donde se definan acciones, recursos, responsabilidades y prioridades en la gestión de estos riesgos de seguridad de la información.
- Implementar el plan de tratamiento de riesgos para lograr las metas de gestión identificadas, como la asignación de recursos, las responsabilidades y las prioridades.
- Implementar el control previamente seleccionado.
- Definir un sistema métrico que pueda tomar resultados reproducibles y comparables para medir la efectividad de un control o grupo de controles. Este es uno de los mecanismos de gran importancia para el sistema de gestión de información interno.
- Adquirir programas de formación y sensibilización coherentes con la seguridad de la información para todo el personal.
- Gestionar las operaciones del SGSI.
- Administrar los recursos necesarios asignados al SGSI para mantener la seguridad de la información.

- Implementar procedimientos y controles en los procesos que faciliten una rápida detección y respuesta de incidentes relacionados a la seguridad de la información.
- Desarrollar los marcos regulatorios requeridos: relativos a los estándares, procedimientos, manuales de instrucciones correspondientes de las organizaciones.

4.3.1.3. Monitoreo y revisión

La organización deberá realizar procedimientos de supervisión y revisión para hacer lo siguiente:

- Detectar a tiempo los errores resultantes que se generaron en el procesamiento de la información.
- Identificar incidentes y brechas de seguridad.
- Ayudar a los administradores a determinar si las actividades que realizan las personas o los equipos técnicos para garantizar la seguridad de la información se realizan en relación a lo esperado.
- Utilizar indicadores para detectar y prevenir eventos e incidentes de seguridad.
- Determinar si las acciones tomadas para resolver la brecha de seguridad fueron eficaces y eficientes.

En cuanto a la revisión constante es necesario:

- Revisar periódicamente la eficacia del SGSI, prestando atención al cumplimiento de las políticas y objetivos de este, los resultados de las auditorías de seguridad, los incidentes, las mediciones de eficacia y las sugerencias y observaciones de todos los involucrados.
- Medir la eficacia del control para asegurarse de que se cumplen sus requisitos de seguridad.
- Evaluar riesgos, y sus niveles de tolerancia, teniendo en cuenta, los cambios que puedan haber ocurrido en la organización, la tecnología, los

objetivos y procesos comerciales, las amenazas identificadas y la efectividad de los controles implementados y el entorno externo.

- Verificar periódicamente a intervalos planificados los requisitos legales, obligaciones contractuales, etc.
- Realizar auditorías internas del SGSI de forma regular a Intérvalos planificados para garantizar que los controles, procesos y procedimientos del SGSI cumplen con los requisitos de ISO 27001, el entorno legal y las exigencias y objetivos de seguridad de la organización.
- Verificar periódicamente por parte del administrador el SGSI para asegurarse de que el alcance definido sea apropiado y que pueda mejorar su proceso, la política de seguridad o los objetivos de seguridad de la información del sistema.
- Mantener actualizado el plan de seguridad, en función de las conclusiones y los nuevos descubrimientos encontrados, esto durante sus actividades de supervisión y revisión.
- Registrar acciones y eventos que puedan haber afectado el desempeño del SGSI.

4.3.1.4. Mantener y mejorar

La organización de forma regular deberá:

- Implantar las mejoras identificadas previamente en el SGSI.
- Tomar las precauciones adecuadas y las acciones correctivas para prevenir posibles no conformidades antes de que ocurran, y resolver las no conformidades detectadas e incorporadas.
- Comunicar las acciones y mejoras a todas las partes interesadas de forma detallada y pormenorizada.
- Asegurarse que las mejoras realizadas hayan alcanzado los objetivos planificados. Siempre es importante verificar la validez de acciones, mediciones o cambios.

4.3.2. Recomendaciones NIST serie 800-53

La misión del NIST es desarrollar y promover métricas, estándares y tecnologías para aumentar la productividad, promover el comercio y mejorar la calidad de vida.

La serie NIST 800 es un conjunto de documentos de interés general en seguridad de la información. Estas publicaciones son un esfuerzo de la industria, el gobierno y las organizaciones académicas para todos aquellos interesados en la seguridad. La serie 800 incluye una lista de documentos que se pueden descargar de forma gratuita desde el sitio web oficial.

En este orden de ideas, la NIST SP800-53 Recommended Security Controls for Federal Information Systems. Son los controles de seguridad recomendados para los sistemas de información, los cuales especifican los controles necesarios para proteger el sistema de información. Entre ellos están:

- Vigilancia y control del acceso.
- Concientización y adiestramiento.
- Responsabilidad y Auditoría.
- Administración de la seguridad.
- Planes de contingencia.
- Identificación y autenticación.
- Respuesta a incidentes.
- Mantenimiento.

A continuación, se muestra un diagrama esquemático de los pasos que pueden seguir las cooperativas de ahorro y crédito, como modelo para la implementación de sistemas de seguridad de la información que les ayude a prever y reducir amenazas. Bajo esta línea, las entradas corresponden a un diagnóstico inicial, las actividades son los pasos a seguir de forma estructurada y las salidas son los resultados obtenidos.

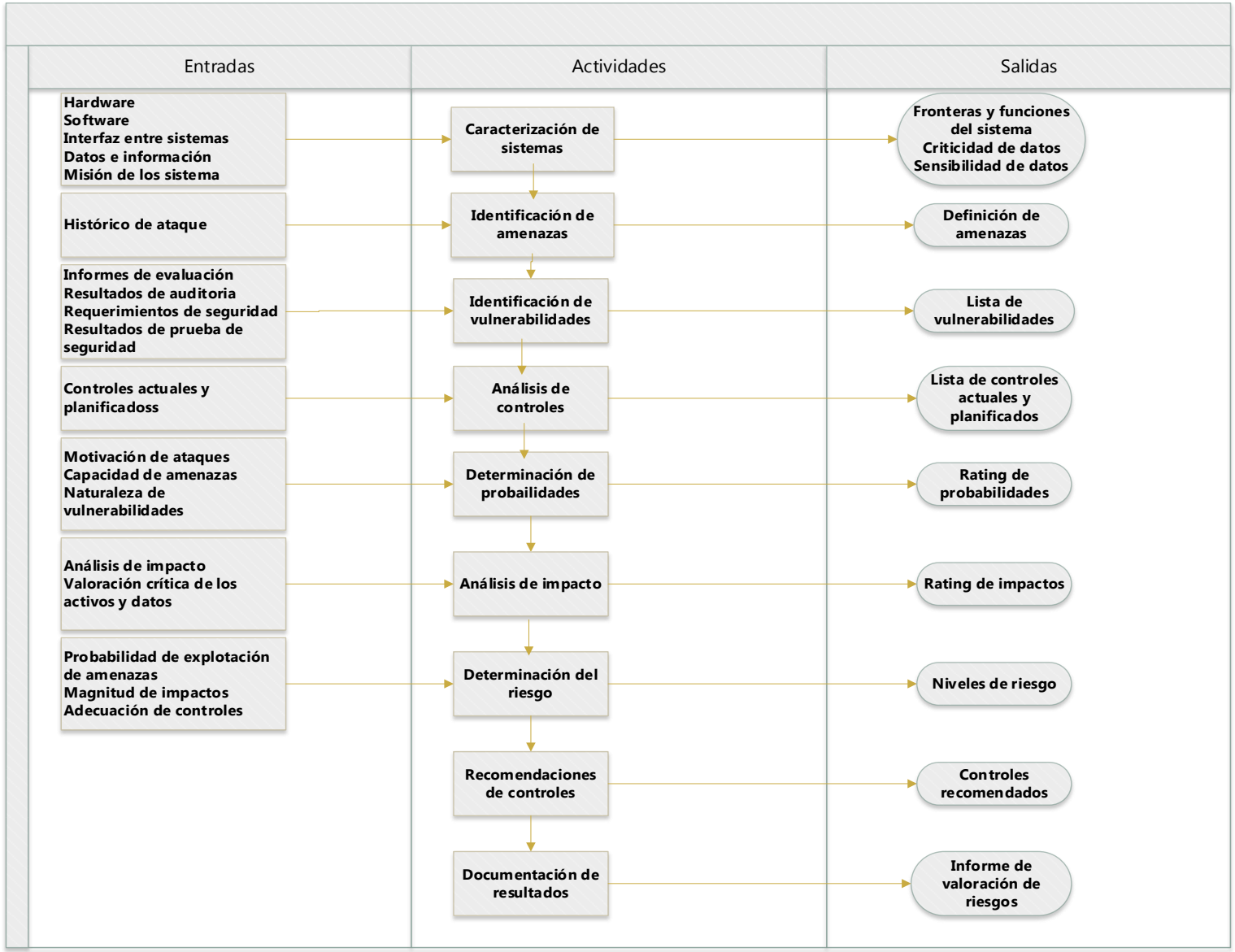

Figura 3 Modelo esquemático para la implementación de sistemas de seguridad de información
Elaboración propia

CONCLUSIONES

- En la actualidad las cooperativas de ahorro y crédito en la ciudad de Guayaquil no aplican sistemas o modelos de gestión de la seguridad de la información, lo cual las vuelve vulnerables debido a que se encuentran expuestas a numerosos riesgos en sus sistemas informativos o de información que podrían implicar diversos problemas, que van desde la fuga de información hasta la deserción de usuarios. Además, las cooperativas de este sector, generalmente no emplean herramientas apropiadas que les permitan una adecuada toma de decisiones, por lo que, sus metas a corto, mediano y largo plazo pueden verse profundamente limitadas.
- Las implementaciones de seguridad de la información deben basarse en estándares y normas que guíen la correcta ejecución de la seguridad de la información. De esta forma, las instituciones financieras como las cooperativas de ahorro y crédito deben cumplir con normas y estándares específicos que regulen su funcionamiento. Gran parte de los estándares para el resguardo de la información están fundamentados en las normas ISO en la serie 27000, junto con metodologías establecidas para la gestión de los distintos procesos dentro de la organización.
- El diseño del modelo estuvo basado principalmente en la norma ISO 27001 con el propósito de establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Es así como se espera que el modelo de gestión de seguridad de la información contribuya a establecer políticas y procedimientos relacionados con los objetivos comerciales de las cooperativas de ahorro y crédito de la ciudad de Guayaquil, para mantener un nivel de exposición que siempre es inferior al nivel de riesgo que la propia organización prevé y para garantizar que la seguridad de la información se gestione correctamente.

RECOMENDACIONES

- Las entidades deben mantener la implementación de políticas de seguridad sugeridas para garantizar la integridad confidencialidad y disponibilidad de la información. Es condición indispensable, que estas vayan implementando dentro de su estructura las políticas, líneas estratégicas, controles, acciones, objetivos, entre otros que marquen las pautas a seguir en la organización, así como el orden gerencial de rigor que se deben seguir en todas las unidades administrativas y departamentos de las microempresas.

- Es necesario que se realicen estudios acerca de la factibilidad de la implementación de un Sistema de Gestión de la Seguridad de la Información en la Cooperativas de ahorro y crédito de la ciudad de Guayaquil.

- Llevar a cabo programas y capacitaciones al personal en materia de seguridad informativa. En esencia, a empleados de nivel técnico informático.

- Independientemente del tipo de empresa sea, su modalidad o condición organizativa, ésta debe tener un sistema de prevención de riesgo, porque es un hecho que las amenazas van a estar siempre presentes en la web, en el intercambio de la información, trasmisión de datos, transacciones, entre otros.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre, M. d., Aguirre, J. R., & Delgado, M. d. (2015). Fundamentos de Seguridad de la Información. Lima, Lima, Perú. Recuperado el 29 de Diciembre de 2020

Areitio, B. J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Cengage Learning Paraninfo S.A.

Areitio, J. (2018). *Seguridad de la Información, redes, informática y Sistemas de Información.* Madrid: Ediciones Praninfo S.A.

Arguello, G. (28 de Diciembre de 2020). *Historia de la seguridad de información.* Obtenido de https://www.academia.edu/19202037/Historia_de_la_seguridad_de_la_informacion

Baader, R. (2017). Seguridad de la Información. Buenos Aires, Argentina: Departamento de co mputación de la Facultad de Ciencias exactas y naturales de la univerisdad de la UBA. Recuperado el 28 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Seguridad_de_la_Informacion%20(2).pdf

Banco Central de Ecuador. (10 de Febrero de 2021). *Listado de cooperativas de ahorro y crédito calificadas.* Obtenido de https://www.bce.fin.ec/documents/pdf/proyecto_bid_bce/Coacsaprobadasxregionact.pdf

Bedón, Z. O. (2019). Sistemas de información para la seguridad de datos de los socios de la cooperativa Tapeco. *Facultad de sistemas mercantiles de la UNIANDES*, 1-17. Recuperado el 23 de Diciembre de 2020, de http://dspace.uniandes.edu.ec/bitstream/123456789/10326/1/ACTFMFG008-2019.pdf

Borghello, C. (2001). *Tesis Seguridad informática: sus implicaciones e implementación.* webmaster.

Bravo, D. (26 de Julio de 2015). El Ecuador se muestra vulnerables a ciberataques. *Actualidad*.

Caicedo, G. M., & Vásquez, C. E. (2020). Sostenibilidad de la economia popular y solidaria en Ecuador. *Revista Mapa*, 1-13.

Capital Online. (04 de Enero de 2015). *Capital Online.* Obtenido de https://www.capital.cl/negocios/2015/01/04/99010/aumento-de-ciberataques-se-instala-como-nueva-amenaza-en-economia-global/

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Ardila, L.-E. B. (Noviembre-diciembre de 2016). Gestión de Seguridad de la información: revisión bibliográfica. *El profesional de la información, 25*(6), 931-948. Recuperado el 23 de Diciembre de 2020, de http://profesionaldelainformacion.com/contenidos/2016/nov/10.pdf

Castro, S. (2016). Seguridad de Información. Lima, Lima, Perú: Political Science. Recuperado el 28 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Seguridad_de_la_Informacion%20(3).pdf

Catalunya, U. P. (2018). *Sistemas de Información.* Barcelona: Facultatad d'Informàtica de Barcelona.

Chenche, J. W. (2020). *Formar docentes de infromática, usando las TIC como entorno de aprendizaje, en todas las disiciplinas de la malla curricular.* Universidad del Rosario. Rosario, Argentina: Universidad del Rosario.

Clavijo, C. A. (2016). *Políticas de Seguridad Informática. Red de Revistas Científicas de América Latina y el Caribe, España y Portugal.* Madrid.

Colegio Oficial de Ingenieros de Telecomunicación. (11 de Febrero de 2021). *Guía de Iniciación a Actividad profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) segun la norma ISO 27001.* Obtenido de https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Coraggio, L. J. (Martes de Diciembre de 2014). *hdl.handle.net.* Recuperado el Lunes de Diciembre de 2018, de La presencia de la economia social y solidaria y su institucionalización en América Latina: http://hdl.handle.net/10419/148805

Echeverría, M. d. (23 de Diciembre de 2020). *Seguridad de la información de las empresas PyME. Cuáles son los 10 errores típicos de las empresas PYME en materia de seguridad de su información*. Obtenido de http://www.forodeseguridad.com/artic/discipl/4208.htm

Figueroa-Suárez, J., Rodríguez-Andrade, R., Bone-Obando, C., & Saltos-Gómez, J. (Diciembre de 2017). La seguridad informática y la seguridad de información. *Polo del conocimiento, 2*(12), 146-155. Recuperado el 23 de Diciembre de 2020, de file:///C:/Users/user/Downloads/420-1655-2-PB.pdf

FINANCOOP. (19 de Enero de 2019). *Las cooperativas de ahorro y crédito alistan sus estrategias para enfrentar el 2019*. Recuperado el 01 de Enero de 2021, de https://revistagestion.ec/empresas/las-cooperativas-de-ahorro-y-credito-alistan-sus-estrategias-para-enfrentar-el-2019

Fundación Telefónica. (2016). *Ciberseguridad, La protección de la información en un mundo digital.* (Ariel, Ed.) Recuperado el 23 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Ciberseguridad%20(1).pdf

Garcés, U. S. (2015). *Seguridad Informática para la Red de datos en la Cooperativa de Ahorro y Crédito Unión Popular LTDA.* Ambato: Universidad técnica de Ambato.

García, P. F. (2018). *Capitulo 7. Ingeniería del Software.* Recuperado el 23 de diciembre de 2020, de https://repositorio.grial.eu/bitstream/grial/1228/1/07-rep.pdf

García, P. Y. (2015). *Modelo de Gestión de la seguridad de información en los procesos críticos de las áreas financieras universitarias. Caso PUCE.* Quito: Escuela politécnica Nacional.

García, R. K., Prado, V. É., Salazar, C. R., & Mendoza, R. J. (Marzo de 2018). Cooperativas de Ahorro y Crédito del Ecuador y su incidencia en la conformación del Capital Social (2012-2016). *Revista Espacios, 39*(28), 1-6. Recuperado el 31 de Diciembre de 2020, de https://www.revistaespacios.com/a18v39n28/a18v39n28p32.pdf

Gestión Digital. (17 de Junio de 2019). *Las cooperatiovas de ahorro y crédito crecieron 132% en 7 años*. Recuperado el 01 de Enero de 2021, de https://revistagestion.ec/noticias/las-cooperativas-de-ahorro-y-credito-crecieron-132-en-7-anos

Granada, G. E. (2018). *Plan de gestión de seguridad de la información para la cooperativa de ahorro y crédito Kullki Wasi.* Quito: Escuela Politécnica Nacional.

Hernández, S. A., & Mejía, M. J. (Febrero de 2015). Guia de ataques, vulneraciones, técnicas y herramientas para aplicaciones web. *Recibe, año 4*(1), 1-18. Recuperado el 01 de Enero de 2021, de https://www.redalyc.org/pdf/5122/512251501005.pdf

Hernández, S. R., Fernández, C. C., & Baptista, L. P. (2014). *Metodología de la investigación 6a edición.* México D.F: McGraw Hill.

Iglesias, M. P. (Octubre-marzo de 2017). Diseño de un modelo de gestión para la permanencia de las empresas familiares en el mercado global. caso Ecuador. *Revista de Ciencia y Tecnología*(12), 31-42. Recuperado el 23 de Diciembre de 2020

INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Recuperado el 01 de Enero de 2021, de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO. (11 de Febrero de 2021). *Plataforma de navegación en línea (OBP) - ISO/IEC 27001:2013(es)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO.ORG. (12 de Febrero de 2021). *ISO/IEC 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

ISO27000.es. (2020). *Integración y uso de ISO 31000 en organizaciones con uno o más estándares de sistemas de gestión ISO e IEC*. Obtenido de www.iso27000.es: https://www.iso27000.es/sgsi.html

ISO27000.ES. (11 de Febrero de 2021). *Serie 27000* . Obtenido de https://www.iso27000.es/iso27000.html

ISOtools Excelence. (13 de Febrero de 2021). *Sistemas de Gestión de Riesgos y Seguridad ISO 27001*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

Karczewska, J. (19 de Mayo de 2017). *COBIT 5 y el reglamento RGPD - ISACA*. Obtenido de https://www.isaca.org/es-es/resources/news-and-trends/industry-news/2017/cobit-5-and-the-gdpr

Lara, S. N. (Domingo de Agosto de 2015). Seguridad en los Sistemas de Información Cap.8. Lima, Peru, Perú. Recuperado el 28 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Seguridad_de_los_sistemas_de_informacion.pdf

Ley Orgánica de Economía Popular y Solidaria. (2018). *Ley Orgánica de Economía Popular y Solidaria* (Vols. Última modificación: 23-oct.-2018). Quito, Pichincha, Ecuador: Registro Oficial 444 de 10-may.-2011. Recuperado el 29 de Diciembre de 2020, de http://www.seps.gob.ec/documents/20181/25522/LEY%20ORGANICA%20DE%20ECONOMIA%20POPULAR%20Y%20SOLIDARIA%20actualizada%20noviembre%202018.pdf/66b23eef-8b87-4e3a-b0ba-194c2017e69a

Linux. (23 de Diciembre de 2020). *Seguridad de la Información: Historia, Terminología y Campo de acción*, on line. Recuperado el 23 de Diciembre de 2020, de https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/

Mantilla, G. A. (2009). *Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base da las normas ISO 27001.* Quito: Escuela Politécnica Nacional.

Martino, S. (24 de Febrero de 2020). *Una visión 20/20 para la ciberseguridad*, on line. (CISCO) Recuperado el 23 de Diciembre de 2020, de https://blogs.cisco.com/security/a-20-20-vision-for-cybersecurity

Mera, B. A. (2020). *Diseño de un modelo de gestión de seguridad de la infromación del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5.* Sangolgí: ESPE. Recuperado el 27 de diciembre de 2020, de http://repositorio.espe.edu.ec/bitstream/21000/8152/1/AC-GRT-ESPE-047641.pdf

Ministerio de Ciencia y Tecnología. (23 de Diciembre de 2020). *La Sociedad de la Información en el siglo XXI: un requisito para el desarrollo. Buenas prácticas y lecciones aprendidas.* Obtenido de https://www.itu.int/net/wsis/stocktaking/docs/activities/1103547250/sociedad-informacion-sigloxxi-es.pdf

MINTIC. (23 de Diciembre de 2020). *Seguridad y privacidad de la información. Modelo*.

Moscaiza-Moncada, O. I. (2020). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013.* Lima: Universidad Peruana de Ciencias Aplicadas (UPC).

Nachenberg, C. (2000). *U.S Patent Nº 6,021,510. .* Washington DC. US: Patent and Trademark Office.

Neira, S. (2016). *Inclusión financiera de las pymes en el Ecuador.* Quito.

Nieves, A. C. (2017). *Diseño de un sistema de gestión de la seguyridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013.* Institución universitaria politécnico Grancolombiano. Recuperado el Diciembre de 2020, de file:///C:/Users/user/Downloads/Seguridad_de_la_informacion%20(4).pdf

Núñez-Moscoso, J. (junio de 2017). Los métodos mxtos en la investigación en educación: hacia un uso reflexivo. *Artigos. :Cuadernos de pesquisa, vol. 47*(num 164), 632-649. Obtenido de https://www.scielo.br/pdf/cp/v47n164/1980-5314-cp-47-164-00632.pdf

Ordóñez, D. (2014). *Pymes ecuatorianas: comercio exterior y fortalecimiento de mercados internacionales .* Guayaquil: Universidad de Guayaquil, Facultad de Ciencias económicas .

Ortega-Pereira, J., Borja-Borja, F., Aguilar-Rodríguez, I., & Montalván-Burbano, R. (Octubre-diciembre de 2017). Evolución de las cooperativas de ahorro y crédito en Ecuador, 2000-2015. *Semestre Económico, 20*(45), 187-216. Recuperado el 31 de Diciembre de 2020, de http://www.scielo.org.co/pdf/seec/v20n45/0120-6346-seec-20-45-00187.pdf

Parra, Á. (2014). *ISO 27001 para Pymes.* Medellín - Colombia: Universidad Internacional de la Rioja.

Ponte, R. M. (19 de Abril de 2015). Gestión de la información. Lima, Lima, Perú: Universidad de Lima. Recuperado el 28 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Gestion_de_la_Informacion_Semana_3_Gesti.pdf

Prieto, Á. V., & Pan, C. R. (2007). *Virus informaticos. Master en informática.* Recuperado el 01 de Enero de 2021, de Universidad de Coruña: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Revista cientifica dominio de las ciencias*, 676-688. Recuperado el 23 de Diciembre de 2020, de file:///C:/Users/user/Downloads/Dialnet-SeguridadEnInformatica-6137824.pdf

Ruíz, P. J. (2018). *Diseño de un sistema de Gestión de seguridad de la información (SGSI) bajo la norma ISO/27001:2013, en la cooperativa multiactiva del personal del Sena Bogotá.* Bogotá: Universidad Nacional Abierta y a Distancia.

Sánchez, P. E., & Rebolledo, H. F. (2017). *Diseño de un sistema de gestion de la seguridad de información en el área de talento humano de la secretaría de educación.* Arauca: Politécnico Grancolombiano.

Santamaría, P. R. (2017). Factores críticos de la gestión de la calidad determinantes del éxito sostenido empresarial en las PYMES. *Ingenieria industrial*, 105-118.

Santillán, X. L., Toalombo, R. A., Rocafuerte, H. C., Núñez, D. T., Bernal, M. M., & Milagro, U. E. (2016). Una mirada a la globalización de las Pymes ecuatorianas . *Observatorio de Economía* , 1-17.

Sarmiento, O. D. (2020). *Modelo de sistema de información gerencial para la gestión del riesgo operativo en las cooperativas de ahorro y crédito del segmento 3 de la economía popular y solidaria de la provincia del Azuay.* Guayaquil: Universidad Tecnológica Empresarial de Guayaquil.

Silva, C. F., Segadas, d. A., & Kowask, B. E. (2014). *Gestión de la seguridad de la información.* Bogotá: RENATA Colombia. Recuperado el 23 de Diciembre de 2020, de https://www.cedia.edu.ec/es/

Soriano, M. (2019). *Seguridad en redes y seguridad de la información.* Technická 2, Praha 6, Czech Republic : Innovative Methodology for Promising VET Areas.

Superintendencia de Economía Popular y Solidaria. (31 de Diciembre de 2020). *El control y la supervisión fortalecen al sector cooperativista*. Obtenido de https://www.seps.gob.ec/noticia?el-control-y-la-supervision-fortalecen-al-sector-cooperativista

Superintendencia de Economía Popular y Solidaria. (31 de Diciembre de 2020). *Situación y perspectivas de las cooperativas de ahorro y crédito en Ecuador*. Recuperado el 31 de Diciembre de 2020, de https://www.seps.gob.ec/noticia-medio?situacion-y-perspectivas-de-las-cooperativas-de-ahorro-y-credito-en-ecuador

Zamora, G. (2018). *Caracterización de la PYME .* México.

ANEXOS

Anexos 1 Instrumento de medición (encuesta)

1. ¿Cree que es importante la seguridad de la información de la institución? Si ___ no ___
2. ¿Considera que la infraestructura informática de la institución es vulnerable?
   Vulnerable ____
   Medianamente vulnerable ____
   Muy vulnerable _____
3. ¿La empresa posee estrategias para la protección de información? Si ____ no___
4. ¿La empresa ha sufrido de robos de información? Si ____ no___
5. ¿Quiénes tienen acceso a la información de los activos?
   Gerente _____
   Encargado de sistema y soporte _____
   Jefe de seguridad y riesgo _____
   Gerente de contabilidad _____
   Gerente de caja _____
6. ¿La empresa ha sufrido de alteración de información? Si ____ no___
7. ¿La red empleada por la entidad financiera posee un sistema de seguridad de información? Si ____ no___
8. ¿Considera que la información de activos tiene amenazas relevantes? Si ____ no___
9. ¿La institución financiera aplica controles adecuados a la información que maneja? Si ____ no___
11. ¿La institución posee políticas para el tratamiento y manejo de la información?