UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable.
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Morales Hidalgo Cristhian Gabriel
Tutores:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, **Toasa Guachi Renato Mauricio** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.

Elaborado por **Morales Hidalgo Cristhian Gabriel**, de C.I: **1717550287**, estudiante de la Maestría en Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, **Urdaneta Herrera Maryory** C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.

Elaborado por **Morales Hidalgo Cristhian Gabriel**, de C.I: **1717550287**, estudiante de la Maestría en Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

Firma

ORCID: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Morales Hidalgo Cristhian Gabriel con C.I: 1717550287, autor/a del proyecto de titulación denominado: Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., de marzo de 2024

Firmado electrónicamente por:
CRISTHIAN GABRIEL
MORALES HIDALGO

_____

Firma

ORCID: 0009-0002-8790-4143

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El siguiente proyecto de investigación se enmarca en el objetivo elaborar un plan de seguridad mediante la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001 para el análisis del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO. Esto a fin de contrarrestar los ataques y acciones ofensivas en su base de datos, orientado a la gestión de riesgo contenidos en la Norma de Seguridad de la Información del Sector Financiero, sobre los controles obligatorios de la seguridad de la información a través de la aplicación de los fundamentos metodológicos de riesgo y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001.

En este sentido el proyecto se enfoca en analizar los ataques informáticos como Phishing, Spear phishing, Whaling, Malware, Ransomware, Inyección SQL, los cuales son acciones ofensivas contra sistemas de información, como bases de datos y redes informáticas. Estos se pueden suscitar en sus dos modalidades; activos o pasivos. En el primer caso, es decir; los ataques activos modifican la información y la situación de los recursos del sistema. Y en el segundo caso, los ataques pasivos se limitan a registrar el uso de los recursos y a acceder a ellos.

La Cooperativa de Ahorro y Crédito CACPECO comprende una entidad financiera, la cual está regida por la Norma de Seguridad de la Información del Sector Financiero. Esta cuenta con oficinas en cinco provincias del Ecuador; sin embargo, la oficina que es objeto de investigación para este proyecto se localiza en Pichincha en la ciudad de Quito específicamente, prestando servicios financieros en colaboración de los emprendimientos y activación de los sectores productivos, por lo que posee un compromiso social que ha brindado confiabilidad y seguridad incentivando y potencializando el desarrollo socio-económico de sus clientes.

En esta línea, la entidad maneja gran flujo de información y dada la importancia de los datos que posee en sus sistemas y en las áreas financieras de índole privado, se hace necesario contar con componentes y mecanismos para el soporte de seguridad informática en la protección de dichos datos, así como en los procesos de la compartición de recursos desde la relación de registros de información y recursos ante exposiciones de vulnerabilidades provenientes de brechas de seguridad en las que se pueda acceder a información sensible.

El diseño de un plan de seguridad tal como refiere Beltrán (2022) “está enfocado en la configuración en la delimitación de normas, regulaciones y políticas a fin de lograr la protección informática” (p.24), lo que admitirá que el recurso informativo de dicha entidad financiera no sea vulnerada ni manipulada por terceros que transgredan dichas barreras a través de estrategias de ataques informáticos, implementando componentes y mecanismos de seguridad admitiendo que los datos sensibles sean seguros y libre de terceros intrusos para el correcto manejo de los servicios en red de la organización.

Este proyecto está enfocado en realizar una valoración del estado de las redes de comunicación para la confiabilidad de la información que maneja esta organización, empleando el Hacking ético para el análisis del sistema informático de la organización; el cuál se delimita en cuatro ejes fundamentales para su abordaje: El primero corresponde a la recopilación de estudios en relación a los diversos ataques informáticos como Phishing, Spear phishing, Whaling, Malware, Ransomware, Inyección SQL siendo los más comunes y sus características de ataque empleando indicadores como: tipo de economía o empresa, por su localidad y software, detallando de forma estadística el impacto a nivel general. Para ello se establecerán matrices referentes a las contenidas en los controles obligatorios de seguridad de la información establecida en la Norma de Seguridad de la Información del sector financiero en referencia a los estándares de la ISO 27001. Finalmente, a partir de la información recabada se realiza un plan de seguridad sistematizado en una matriz de técnicas de detección, prevención y mitigación de impactos ante ataques informáticos.

Es por ello, que para que este estudio valorativo de índole analítico se lleve a cabo de forma correcta, es fundamental el establecimiento de criterios de aceptación de amenazas y riesgos, así como también, la contextualización en cada uno de estos será medidos, tal como se detalló en el párrafo anterior. Los cuales posteriormente serán evaluados en relación a la probabilidad de ocurrencia y las consecuencias de los que se hayan identificado como posibles en el diagnóstico inicial (Recalde y Vallejo, 2023).

La aplicación de este estudio versa tanto en una valoración técnica como la configuración de estrategias en pro al establecimiento de políticas sobre la seguridad de la información lo que admite que los datos de la entidad no puedan ser operados por terceros que puedan llegar a violar los bloques de acceso a través de tácticas contra los ataques que generen pérdida de datos e informaciones.

Problema de investigación

A nivel mundial los sistemas de información se ven afectados por diversas vulnerabilidades como; una política de seguridad poco eficiente y la deficiente protección de las redes, lo que ha provocado fallos de seguridad informática. Debido a esto se producen grandes pérdidas a las organizaciones, situándose debilidades que pueden comprometer la información de sus clientes. En este sentido, muchas organizaciones, no toman como prioridad el análisis de impactos; por tanto, no adoptan estrategias de seguridad sostenidas en innovaciones tecnológicas que contribuyan a la delimitación de barreras de seguridad. Ante la proliferación de componentes tecnológicos concernientes a los SSI, si no se implementan elementos de seguridad certificados y no se realizan valoraciones pertinentes, estos serán vulnerables ante amenazas y ataques en la red.

Por su parte García y Morales (2022) establecen que este problema se sigue evidenciando por lo que aproximadamente "el 64% de las instituciones financieras optimizan sus sistemas, pero no los protegen de vulnerabilidades cibernéticas ya que no poseen una cultura de seguridad de la información" (p.18), creando sectores abiertos a la vulneración y riesgos respecto a la manipulación de información sensible por terceros no acreditados.

En Ecuador, se evidencia de forma constante vulneraciones y amenazas cibernéticas que afectan gravemente la integridad de los sistemas de datos de una determinada organización; considerándose una problemática creciente que influye en el resguardo de información sensible que pone en riesgo la confidencialidad de los usuarios que se sirven de los productos de dichas entidades. En este sentido, todo esto ocurre debido a la falta de implementación de políticas de seguridad y de privacidad desde la sistematización tecnológica en donde se implementen técnicas, componentes y mecanismos que contrarresten los ataques y violaciones a los sistemas de dichas organizaciones y que protejan la información que se maneja de red a red.

En la actualidad son muchas las organizaciones que fundamentan sus actividades operativas desde la transformación digital, la cual va de la mano con el crecimiento a nivel socioeconómico del país, por lo que la incorporación de tecnologías de vanguardia contribuye a tal crecimiento de su productividad, a desarrollar nuevos servicios y por tanto a posicionarse en el mercado y sector al que dedica tales actividades. Sin embargo, mientras muchos se enfocan por migrar a la digitalización de servicios, en el camino se descuidan aspectos fundamentales como la seguridad de esta información sensible que se está llevando hacia los formatos digitales.

La Cooperativa de Ahorro y Crédito CACPECO ha sido parte de las organizaciones que hoy en día la mayoría de sus servicios han sido sistematizados sin embargo dada la naturaleza de esto, la información que actualmente disponen en la red de datos es sensible ya que dentro de ellas se maneja la cartera de clientes e información sensible referente a identificaciones personales, registros económicos, etc.

El flujo de información y los datos que manejan y gestionan las organizaciones financieras como CACPECO, representan un papel fundamental y un activo esencial que deben ser resguardados y protegidos ante la estrategia de intrusión o hackeo, con el fin de mitigar debilidades o vulnerabilidades en sus sistemas que pongan en duda su confiabilidad. Es por ello que, las amenazas y ataques informáticos desde los dispositivos comunicativos y de la red de datos constituye una amenaza, especialmente cuando no se cuenta con protección informática, ocasionando riesgos tanto lógicos como físicos (Chango y Gualpa, 2023).

Las entidades bancarias son objeto constante a vulnerabilidades y ciberataques siendo los problemas más recurrentes a las que están expuestas especialmente por las redes de internet, en la cual las tecnologías son el medio por el cual causan grandes dificultades y daños en los sistemas, produciendo caída de estos; mientras se da un proceso de extracción de datos a través de la violación de las barreras de seguridad accediendo así a los servidores de la organización y migrando información confidencial hacia otros sistemas.

Esta información está de forma latente expuesta a ataques cibernéticos, de acuerdo con los datos aportados por el Ministerio de Telecomunicaciones (MINTEL) la penetración de “servicios de Banda Ancha representa solo un 8% para la fija y un 72% para la móvil, obteniendo como resultado un índice del 85% de conectividad” (p.2), lo que facilita el acceso a la red. En este sentido, desde el momento en el que toda la sociedad tiene la facilidad de poder acceder a esta y estar hiperconectada y aún más cuando se encuentra en auge tecnologías como la 5G, la IA (Inteligencia artificial) así como las infraestructuras de magnitudes habilitadores claves de tecnológicas referentes a la computación cuántica.

Sin embargo, al ser una nueva tendencia Ecuador se encuentra en una posición de desventaja respecto a otros países de la región y, por tanto, al primer mundo que en sintonía con este crecimiento sí están en vanguardia de sistemas de seguridad, por lo que en Ecuador se desea incorporar tecnologías, pero se están dejando a un lado los temas de seguridad informática para que el avance este sostenido en políticas de resguardo de datos

En cuanto a la gestión de la propuesta que versa sobre la entidad CACPECO, se promueve una intervención que aborde los problemas descritos anteriormente, respecto a la red de datos en donde se identifiquen las falencias críticas y se implanten políticas y programas de seguridad que coloquen fuera de alcance toda amenaza y vulnerabilidad de índole informática para el resguardo y protección de las infraestructuras de redes de datos locales, y que los procesos de tratamiento de información sensibles no sean deficientes, sino que se maneje bajo un monitoreo sistematizado para el control de los recursos compartidos en los sistemas comunicativos de la organización.

Objetivo general

Elaborar un plan de seguridad mediante la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001 para el análisis del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO

Objetivos específicos

- Estudiar los ataques y vulnerabilidades más existentes en el sector financiero mediante el análisis de los fundamentos relacionados a los diversos ataques informáticos.
- Diagnosticar la situación actual de la cooperativa sobre su sistema de seguridad informática respecto a los diversos ataques y vulnerabilidades en su base de datos mediante los fundamentos metodológicos establecidos por la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001.
- Proponer un plan de seguridad sistematizado en una matriz de técnicas de detección, prevención y mitigación de impactos ante ataques informáticos de la información sensible de la Cooperativa de Ahorro y Crédito CACPECO.
- Evaluar la efectividad del plan de seguridad del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO a través del criterio de especialistas en el área.

Vinculación con la sociedad y beneficiarios directos

Hoy en día con el avanzado desarrollo tecnológico, en el cual han incursionado las empresas y organizaciones para sistematizar su proceso y poder estar a la vanguardia en la oferta de servicios y productos han descuidado muchas veces el resguardo de la información que automatizan. Actualmente, la información es el activo más valioso para cualquier empresa; de la misma forma, los procesos y los sistemas informáticos trabajando conjuntamente, llegan a formar activos con más importancia. Por lo tanto, la integridad de la información, la disponibilidad y la confiabilidad de la misma

deben garantizarse, para de esta forma mantener niveles muy altos de imagen empresarial, conformidad y competitividad.

La vinculación con la sociedad de este proyecto reside en conocer e informar los diversos tipos de ataques y vulnerabilidades más existentes en el sector financiero mediante el análisis de los fundamentos relacionados a los diversos ataques informáticos, con el fin de elaborar una plan de seguridad mediante la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001 para el análisis del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO. Esto beneficiará en principio a la cooperativa CACPECO y sus colaboradores, así como sus clientes y a todos aquellos que tengan acceso al proyecto.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Antecedentes investigativos

El presente proyecto está enmarcado en la elaboración de un plan de seguridad mediante la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001 para el análisis del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO, para ello se ha delimitado un análisis de documentos de producción internacional y nacional (revisión literaria) a fin de obtener información sobre las normas empleadas en otros estudios y su eficacia, además de los métodos y técnicas que permitan la constitución teórica y sólida de este. A continuación, se detallan a

Según una investigación preliminar, el proyecto fue realizado por Tomás Alcántara, Marisa Panizzi e Iris Sattolo en la Escuela Superior de Ingeniería, Informática y Ciencias Agroalimentarias de la Universidad de Morón, Argentina. El objetivo de este proyecto, "Buenas prácticas para la seguridad informática en PyMES", fue crear un conjunto de pautas para la seguridad informática en pequeñas y medianas empresas. Los investigadores utilizaron un mapeo sistemático de la literatura, también conocido como "estudio de mapeo sistemático" o SMS, para realizar una revisión exhaustiva del estado actual de la seguridad informática en PyMES. La metodología empleada fue documental y los resultados principales mostraron los avances en la aplicación de los estándares establecidos por la Organización Internacional de Normalización (ISO), siendo la ISO 27001 la más importante. La mayoría de los estudios se centran en los problemas de seguridad informática relacionados con redes, aplicaciones y puntos finales. Se llega a la conclusión de que estos son los principales objetivos de ataque. Además, se destaca que el usuario es el principal punto débil en seguridad informática, y puede convertirse en un punto débil debido a la falta de conocimiento o al uso inadecuado de la tecnología. Por lo tanto, las primeras cosas que una organización debe proteger y considerar al desarrollar una arquitectura de seguridad son estas tres áreas mencionadas anteriormente (Alcántara et al., 2022).

En la Universidad Técnica de Ambato, Chicaiza Castillo, Dennis Vinicio y Torres Chango, Christian Damián, realizaron una segunda investigación. El objetivo principal de este estudio, denominado "Plan de seguridad informática basado en la norma ISO 27001 para proteger la información y los activos de la empresa privada Megaprofer S.A.", fue desarrollar un plan de seguridad estructurado de naturaleza preventiva, conocido como Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001(Chicaiza y Torres, 2020)

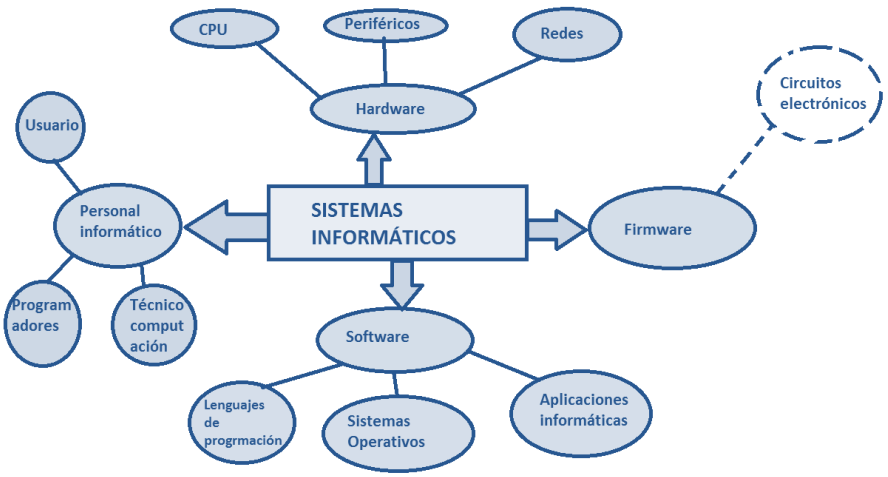
El tercer estudio consultado fue escrito por Vaca Benalcazar, Christian Patricio y Cueva Quintana, Jonathan Bryan, para la Universidad de Israel. Se tituló Propuesta De Un Modelo De Sistema De Gestión Seguridad De La Información Para La Unidad Educativa. Conforme a la Norma ISO 27001, Fray Jodoco Ricke La investigación se centró en contextualizar la importancia y los requisitos para implementar un modelo de gestión en una unidad educativa basada en esta norma ISO, que permitió la fijación de políticas (uso aceptable, cuentas de usuario, claves, correo y protección de la información) en los sistemas de automatización de los estudiantes de la unidad, protegiendo datos sensibles y fortaleciendo los criterios de confidencialidad, confiabilidad y protección de la información (Vaca y Cueva, 2022).

Sistema informático

Para Beltrán (2022) determina que un sistema informático (SI) constituye a un proceso automatizado encargado de almacenar, procesar y recuperar datos. Es síntesis, corresponde a un conjunto de elementos físicos y lógicos que recibe, guarda y procesa datos a fin de sistematizarlos en resultados. En cuanto a sus componentes fundamentales son: Hardware, Software, Personal informático (Ver figura 1).

Figura 1

Sistema informático



Nota: Esquematización sobre el concepto de sistema informático. Obtenido de (Sisti, 2019)

En síntesis, el/los sistema/as informáticos se componen de: ordenador, Teclado, Ratón, Monitor, Otros componentes llamados periféricos tal como se muestra en la figura 1. Estos últimos (periféricos)

comprenden elementos externos al propio ordenador, como puede ser la impresora (Garcia y Morales, 2022).

Seguridad de la información

La seguridad de la información ha sido conceptualizada por muchos autores, sin embargo, dentro del abordaje teórico, se considera que la definición más acertada es la de Hunter (citado por Dávila, 2021) como un conjunto de medidas - técnicas que se emplean para el control y resguardo de los datos manejada en una organización, con el fin de proteger la información sensible sobre empleados, socios, proveedores, clientes, etc.

Figura 2

Esquema seguridad de la información

Nota: Esquematización sobre el concepto de sistema informático. Obtenido de (Sisti, 2019)

En criterio Silva y Recalde (2022) comprende diversos aspectos, entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos, mediante las tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado.

Plan de seguridad

Un plan de seguridad informática es un documento que describe cómo implementar sistemas de seguridad y acciones para lograr la mayor seguridad cibernética posible en una empresa (Dávila, 2021).

Comprende una estrategia que determina las acciones digitales que protegen el flujo de datos recabados mediante plataformas, apps o software. Incluye acciones sencillas, como cambiar las contraseñas de vez en cuando, o tareas más complicadas, como hacer una copia de seguridad periódica de los recursos. Ha sido definido como un documento que contiene medidas que puedes tomar para proteger los recursos de tu negocio y minimizar los riesgos informáticos (Chango y Gualpa, 2023).

Norma de la seguridad informática -ISO 27001

La norma ISO 27001 comprende un lineamiento estándar internacional que detalla los requisitos para la implementación, mantenimiento y mejoramiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) (Silva y Recalde, 2022). Está basada en los siguientes principios:

- Confidencialidad: La información solo debe ser accesible para las personas autorizadas.
- Integridad: La información y los métodos de tratamiento deben ser exactos y completos.

En cuanto a los beneficios de la norma ISO 27001 se tienen:

Tabla 1

Beneficios de la seguridad informática -ISO 27001

Beneficios	Apoya a las organizaciones en la configuración de su política y objetivos de seguridad de la información, proporcionándoles el conocimiento para gestionar sus aspectos relevantes, aplicar los controles necesarios y establecer metas precisas para mejorar la seguridad de su información.
	Simplifica la administración de las obligaciones legales, como el Reglamento General de Protección de Datos (GDPR), junto con la norma ISO 27701, al incorporar la evaluación regular del grado de cumplimiento para una constante mejora del sistema, asegurando la seguridad y afrontando las posibles vulnerabilidades.
	Ofrece una perspectiva completa de la seguridad de la información al salvaguardar los recursos digitales, la documentación física, los activos materiales (como dispositivos y redes), así como el conocimiento del personal. Se aborda desde la mejora de las habilidades del personal hasta la aplicación de medidas técnicas para prevenir el fraude informático.
	La norma ISO 27001 ha sido desarrollada para ser compatible y coordinada con otras normas reconocidas de sistemas de gestión, lo que la hace más fácil de incorporar en los sistemas y procesos de gestión existentes.

Nota: Beneficios de la norma ISO 27001 – Adaptado de (Silva y Recalde, 2022)

La ISO 27001 también ha sido definido como una norma mundial que se aplica a todas las organizaciones, independientemente de su tamaño o sector lo que permite que se otorguen certificaciones que contribuye a la fidelidad de la organización (Recalde y Vallejo, 2023)

Cooperativas de ahorro y crédito (Sector financiero)

Las cooperativas de ahorro y crédito son todas aquellas organizaciones sin fines de lucro dedicadas a la prestación de servicios a sus socios, dentro de esta oferta se encuentra los depósitos, otorgamiento de préstamos y ofrecen una amplia variedad de otros servicios financieros. Dentro de sus objetivos se encuentra el de servir a sus miembros en lugar de buscar generar ganancias; por lo que ofrecen mejores tasas de ahorro, tasas de préstamo más bajas y tarifas reducidas (ASOBANCA, 2023).

Este tipo de organizaciones tienen un papel fundamental en la economía social del país, al ser gestores del desarrollo económico de los microempresarios, apoyando desde las más pequeñas iniciativas de negocio hasta los miles de hogares en el Ecuador (ASOBANCA, 2023).

1.2. Proceso investigativo metodológico

Enfoque y diseño de la investigación

La metodología de este estudio está apoyada de un enfoque cualitativo ya que no recurre a datos de medición numérica (Hernández, 2018), sino que admite descripciones profundas e interpretaciones de fenómenos que responde a la naturaleza de este estudio. Esto debido a que se centra en los aspectos culturales e ideológicos del resultado, en lugar de los numéricos o proporcionales.

El diseño del estudio se caracterizó por ser no experimental ya que se llevó a cabo sin la manipulación deliberada de los indicadores de estudio, se fundamentó en la observación de fenómenos en su contexto natural para luego analizarlos.

Este diseño fue no experimental ya que se empleó para describir, diferenciar y examinar el fenómeno de estudio lo que admitió diagnosticar la situación actual de la cooperativa sobre su sistema de seguridad informática respecto a los diversos ataques y vulnerabilidades en su base de datos mediante los fundamentos metodológicos establecidos por la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001.

Tipo de estudio

El tipo de estudio fue descriptivo ya que constituyó un método de investigación que describió las características del fenómeno o población estudiada, el cual se centró más en el "qué" del objeto de estudio que en el "por qué" (Hernández, 2018).

Se empleó este tipo de investigación descriptiva ya que admitió describir y explicar lo que se investiga, pero no dar las razones por las cuales eso tiene lugar, se acompañó del método observacional y fue adecuada al estudio, por su naturaleza concluyente lo que permitió establecer el diagnostico situacional de la cooperativa sobre su sistema de seguridad informática.

Universo de estudio

El universo de estudio comprende el conjunto de elementos, personas, objetos, sistemas y sucesos, finitos e infinitos, a los que pertenece la población. Es decir, representan los sujetos de estudio de donde se extraerá la información y hacia el que se generalizarán las conclusiones obtenidas (Hernández, 2018).

En este sentido, el universo de estudio está constituido por el gerente de la cooperativa y dos colaboradores del departamento informático de CACPECO a fin de recopilar información que permita realizar el diagnostico situacional de la organización para llevar a cabo la elaboración del plan de seguridad según sus necesidades y requerimientos.

Instrumentos y técnicas

En cuanto a los instrumentos para la recopilación de datos e información, se empleó el cuestionario semiestructurado que constó de 10 preguntas con dos indicadores que le delimitaron, la primera seguridad informática y el segundo normativa ISO 27001. En cuanto a la técnica se aplicó la entrevista ya que permitió una conversación abierta con los sujetos de estudio a fin de obtener la información para el posterior procesamiento de datos.

Proceso de análisis de datos

En cuanto al proceso de análisis de datos se llevó a cabo un análisis general en donde se identificó el problema y las falencias de la situación de la organización y se vincularon con los objetivos de la investigación lo que permitió analizar los datos contrastando la información teórica y se presentó el informe con los resultados de forma sistematizada en matrices, caracterizados por determinar los indicadores (preguntas realizadas a los sujetos de investigación) sus respuestas escritas sin modificación y la el establecimiento del diagnóstico que facilitó la interpretación y discusión de resultados finales.

1.3. Análisis de resultados

En conformidad con el objetivo de diagnosticar la situación actual de la cooperativa sobre su sistema de seguridad informática respecto a los diversos ataques y vulnerabilidades en su base de datos mediante los fundamentos metodológicos establecidos por la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001; se presentan los resultados obtenidos del procesamiento de información recopilados del gerente de la Cooperativa y dos de sus colaboradores:

Tabla 2

Sistematización de los datos obtenidos en las entrevistas

Entrevistado: Gerente general

Categorías / Indicadores	Diagnóstico
Seguridad y Norma ISO 27001	
1. ¿Está familiarizado con la seguridad de la información?	Está bien informado sobre la seguridad de la información.
2. ¿Está familiarizado con los estándares de seguridad de la información?	Con respecto a las normas de seguridad de la información el conocimiento es parcial
3. ¿Qué sabe sobre las Normas ISO 27001?	El conocimiento de la norma ISO 27001 es insuficiente.
4. ¿Qué sabe sobre la ley de protección de datos?	Muy poco conocimiento de la ley de protección de datos.
5. ¿Tienen licencias vigentes los equipos de computación?	Este año no tiene licencias.
6. ¿Cuál es el nivel de seguridad que cumple con los parámetros de ingreso al sistema?	El nivel de seguridad del acceso al sistema es moderado.
7. ¿Todos los usuarios autorizados de los sistemas tienen acceso a toda la información necesaria?	La información que se maneja es redundante y no se comparte a menudo.

8. ¿Hay información que se ha difundido fuera del departamento?	Si hay información filtrada (activos, activos informáticos)
9. ¿Existe documentación detallada y disponible en cualquier momento sobre los procesos que se manejan actualmente?	Algunos procesos están documentados de manera detallada y están disponibles en cualquier momento.
10. ¿Existen actualmente políticas de seguridad para la gestión de datos? Enumere	La gestión de la información carece de políticas de seguridad.
11. ¿Se lleva a cabo la gestión de riesgos en relación con la seguridad de la información?	La seguridad de la información carece de gestión de riesgos.

Nota: Datos obtenidos de la entrevista aplicada al gerente general de la Cooperativa CACPECO. 2024

Tabla 3

Sistematización de los datos obtenidos en las entrevistas

Entrevistados: Colaboradores

Categorías / Indicadores	Diagnóstico
Seguridad y Norma ISO 27001	
1. ¿Existe una sola persona responsable de la creación de usuarios?	Solo una persona está a cargo de crear usuarios.
2. ¿Hay algún registro de usuario creado?	No existe un registro completo de los usuarios creados.
3. ¿Se bloquean los usuarios que se encuentran en período de vacaciones o que ya no trabajan para la empresa?	A los usuarios que se encuentran en período de vacaciones no se les bloquea y a los usuarios que ya no laboran se hace un seguimiento para ser bloqueados.
4. ¿Es necesario obtener permisos para la creación de usuarios?	SI es de carácter obligatorio solicitar permiso para la creación de usuarios.
5. ¿Tienen validez las claves creadas?	Existe un tiempo estimado para que las claves creadas tengan caducidad. Pero generalmente siguen funcionando a menos que se bloqueen.

6. ¿Existen obligaciones para los usuarios con respecto al uso adecuado de los recursos?	El usuario es responsable del uso adecuado de los recursos. Pero no se definen.
7. ¿Existe un control de acceso no autorizado al usuario para proteger el equipamiento y los sistemas de la empresa?	No hay control sobre el acceso no autorizado.
8. ¿La contraseña es única para todos los usuarios?	Su contraseña como primer ingreso cuando un usuario crea una cuenta en un sistema específico es genérica.
9. ¿Cuál es el tamaño y la definición del password?	El código de clave se basa en la afinidad del usuario.
10. ¿El usuario está bloqueado por una clave incorrecta?	Luego de 3 intentos el usuario es bloqueado.
11. ¿Pueden los usuarios acceder al sistema desde cualquier equipo?	En ocasiones, los usuarios deben trabajar en otros lugares que no sean en la empresa.
12. ¿Es posible acceder a través de un equipo diferente si el usuario ya está en uso?	Se puede acceder desde múltiples equipos.

Nota: Datos obtenidos de la entrevista aplicada al Ingeniero Informático de la Cooperativa CACPECO. 2024

Autorización y administrador de sistemas: Información suministrada por los colaboradores

1. ¿Tienen permiso los usuarios creados para consultar, modificar o modificar la base de datos?	Los usuarios no tienen ningún tipo de permiso para alterar la BDD.
2. ¿Todos los usuarios tienen sus propios permisos definidos?	El control de permisos para cada usuario es confuso.
3. ¿Está permitido cambiar el usuario o la contraseña?	No, ya que es responsabilidad del usuario cambiar la contraseña.
4. ¿Es posible acceder a sitios web que no son de carácter institucional?	No, la Lista de Control de Acceso (ACL) controla el acceso a la Web.
5. ¿Es posible usar el teléfono móvil o cualquier otro dispositivo de almacenamiento mientras trabaja?	Las políticas de la empresa no tienen en cuenta este tema. Tanto las prohibiciones como el seguimiento son inexistentes.
6 . ¿Puede un administrador modificar la Base de Datos (BDD)?	Si, siempre y cuando esté autorizado.
7. ¿La sesión de los usuarios permanece activa durante largos períodos de tiempo cuando no se usa el sistema?	Sí
8. ¿Los usuarios pueden obtener datos a través de dispositivos externos?	Si, ya que no tiene un sistema para bloquear dispositivos extraíbles.
9. ¿Existe algún documento o registro de las personas que están autorizadas para realizar respaldos de sistemas?	Si, las personas responsables están registrando el proceso.

10. ¿Se llevan a cabo actividades de seguimiento de los sistemas de información que se manejan?	En sistemas cooperativos, si se realiza en algunas áreas con un proveedor que permite llevar el control.

Nota: Datos obtenidos de la entrevista aplicada al administrador de la Cooperativa CACPECO. 2024

Análisis entrevista aplicada

En cuanto a la sistematización de los datos obtenidos por el gerente y los colaboradores de la Cooperativa CAPECO, enfocados en el diagnóstico de la situación actual de la organización, se pudo conocer qué; se aplican algunas políticas para gestionar la información, sin embargo, son escuetas y atienden puntos básicos, tales como la gestión de usuarios o ciertas limitaciones en cuanto al uso de internet. Por lo tanto, se ha evidenciado que, este tipo de "políticas" son suficientes para garantizar que la información financiera de los usuarios de la entidad financiera esté asegurada.

Se observó durante la sesión de conversación con los participantes de la investigación que han surgido problemas internos, que incluyen correos electrónicos con archivos adjuntos diseñados para eliminar datos hasta la filtración de datos de ciertos usuarios. Debido a la falta de capacitación para abordar estos ataques y, especialmente, para gestionar los problemas de contraseñas poco seguras, estos incidentes han representado un problema de alto impacto que ha afectado negativamente a la organización.

Además, se descubrió que no hay un documento oficial que describa las responsabilidades de los funcionarios en relación a los equipos, ya que las propiedades de la entidad no están claramente definidas. Solo se socializa a los funcionarios que son responsables de un recurso específico, lo cual no es recomendable. Esto demostró la importancia de implementar la propuesta que consiste en crear un plan de seguridad integral que incluya una serie de métodos para detectar, prevenir y reducir los efectos de los ataques informáticos a la información confidencial de la Cooperativa de Ahorro y Crédito CACPECO. Este plan deberá ser difundido a toda la Cooperativa.

Se descubrió, entre otros aspectos evaluados, que no existe una forma de limitar el acceso de los usuarios al equipamiento de la institución, aunque en cierta medida se utiliza una contraseña para proteger contra usuarios malintencionados. En este mismo orden, la ubicación del centro de datos no cumple con las especificaciones de seguridad, lo que lleva

a un incorrecto control de acceso para el personal no autorizado. El acceso a este medio solo debería ser permitido mediante una documentación detallada que registre los ingresos y salidas del personal.

En conclusión, solo se maneja un plan de mantenimiento básico y no hay controles ni seguimientos de normas de seguridad de la información. Tampoco hay un cronograma de mantenimiento para los equipos que utilizan los usuarios. No tienen un plan de emergencia para casos de fallas en los sistemas que controlan, ni para situaciones en las que no puedan acceder a Internet. No se implementan medidas de gestión de riesgos en caso de robos o ataques a la información financiera controlada, lo que ha llevado a las situaciones descritas por los participantes del estudio.

CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

Un plan de seguridad basado en la norma de seguridad informática para el sector financiero y en la ISO 27001 para el análisis del sistema informático es fundamental para garantizar la protección de la información sensible y crítica en las instituciones financieras. La seguridad de la información en el sector financiero es de suma importancia debido a la naturaleza confidencial de los datos financieros y personales que manejan estas entidades (Chicaiza y Torres, 2020). A continuación, se proporciona una fundamentación teórica sobre este enfoque de seguridad:

- Normativa de seguridad informática para el sector financiero:

Las instituciones financieras están sujetas a regulaciones específicas relacionadas con la seguridad de la información. Estas regulaciones suelen incluir medidas específicas para proteger la integridad, confidencialidad y disponibilidad de los datos financieros. El cumplimiento de estas regulaciones es crucial para evitar sanciones legales, pérdida de confianza por parte de los clientes y daños a la reputación de la institución financiera (Beltrán, 2022).

- ISO 27001:

ISO 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Proporciona un marco sistemático y proactivo para administrar la seguridad de la información y aborda aspectos como la gestión de riesgos, la seguridad física, la gestión de incidentes y la continuidad del negocio. La implementación de la ISO 27001 permite a las instituciones financieras identificar y mitigar los riesgos de seguridad de la información de manera efectiva, garantizando así la protección de los datos confidenciales y la continuidad de las operaciones comerciales (Sisti, 2019).

- Beneficios del enfoque combinado:

Al combinar la normativa de seguridad informática específica del sector financiero con la norma ISO 27001, las instituciones financieras pueden obtener una cobertura integral de los requisitos de seguridad. La normativa específica del sector financiero aborda los desafíos y riesgos particulares que enfrentan estas instituciones, mientras que ISO 27001 proporciona un marco generalmente aceptado y probado para la gestión de la seguridad de la información. Este enfoque combinado ayuda a las instituciones financieras a fortalecer su postura de seguridad,

mejorar la resiliencia ante amenazas y demostrar el cumplimiento de los estándares de seguridad tanto a los reguladores como a los clientes (Beltrán, 2022).

En resumen, un plan de seguridad basado en la normativa de seguridad informática para el sector financiero e ISO 27001 proporciona un marco sólido y completo para proteger los activos de información crítica en las instituciones financieras. Al cumplir con estos estándares, las organizaciones pueden mitigar los riesgos de seguridad, fortalecer la confianza del cliente y cumplir con las regulaciones pertinentes.

1.2. Descripción de la propuesta

Actualmente en la era digital, la seguridad de la información se ha convertido en una preocupación crítica para organizaciones de todos los tamaños y sectores, especialmente las entidades financieras cuyo manejo de datos es sensible.

Con la creciente amenaza de ciberataques, filtraciones de datos y regulaciones cada vez más estrictas en materia de privacidad, garantizar la protección de la información sensible es fundamental para el éxito y la supervivencia de cualquier empresa. En este contexto, la normativa ISO 27001 emerge como un estándar internacional ampliamente reconocido para la gestión de la seguridad de la información.

La presente propuesta está enmarcada en desarrollar un Plan de Seguridad para la Cooperativa CACPECO vinculado a la normativa ISO 27001 ya que establece un marco de trabajo integral para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) para la entidad financiera objeto de este estudio.

Este estándar proporciona a las organizaciones una metodología estructurada para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información, asegurando así la confidencialidad, integridad y disponibilidad de los activos de información críticos.

Una de las principales ventajas de adoptar la normativa ISO 27001 para el sustento y validez de este plan de seguridad, es su enfoque basado en el riesgo. En lugar de ofrecer soluciones genéricas, la norma insta a las organizaciones a realizar una evaluación exhaustiva de los riesgos de seguridad de la información que enfrentan, así como a implementar controles y medidas de seguridad adecuadas para mitigar estos riesgos de manera efectiva. Este enfoque proactivo no

solo ayuda a prevenir incidentes de seguridad, sino que también permite a las organizaciones adaptarse rápidamente a los cambios en el panorama de amenazas.

Por tanto, desarrollar un plan de seguridad basado en la norma de seguridad informática para el sector financiero e ISO 27001 implica combinar las mejores prácticas de ambos marcos para garantizar la protección de los activos de información crítica en el entorno financiero. A continuación, se detallan los elementos claves que fundamentaran este plan de seguridad como eje propositivo de este proyecto:

- Evaluación de riesgos y análisis de impacto: Se realizará una evaluación exhaustiva de los riesgos de seguridad de la información específicos del sector financiero, considerando amenazas como ataques cibernéticos, fraudes financieros, robo de identidad, entre otros. Utilizar el enfoque basado en riesgos de ISO 27001 para identificar y priorizar los riesgos más significativos y evaluar su impacto potencial en la confidencialidad, integridad y disponibilidad de la información financiera.
- Desarrollo de políticas y procedimientos de seguridad: Se definirán políticas y procedimientos de seguridad de la información que cumplan con los requisitos de ISO 27001 y aborden las necesidades específicas del sector financiero. Esto puede incluir políticas de acceso seguro, gestión de contraseñas, cifrado de datos, monitoreo de seguridad, gestión de incidentes, entre otros.
- Implementación de controles de seguridad: se implementarán controles de seguridad técnicos y organizativos para mitigar los riesgos identificados. Esto puede incluir medidas como firewalls, sistemas de detección de intrusiones, cifrado de datos, autenticación de dos factores, políticas de gestión de parches, entrenamiento de concientización en seguridad para empleados, entre otros.
- Gestión de accesos privilegiados: Se establecerá dentro del plan un sistema de gestión de accesos privilegiados robusto para limitar y controlar el acceso a la información financiera confidencial. Esto implica asignar privilegios de acceso de manera adecuada, monitorear y auditar las actividades de los usuarios privilegiados, y garantizar la revisión regular de los derechos de acceso.

- Protección de datos personales y confidenciales: se implementarán medidas de seguridad adicionales para proteger los datos personales y financieros de los clientes, en cumplimiento con regulaciones como GDPR, CCPA y normativas locales aplicables. Esto puede incluir el cifrado de datos, controles de acceso reforzados y procedimientos de gestión de incidentes específicos para la protección de datos.
- Preparación para la respuesta a incidentes: se desarrollará dentro del plan, acciones de respuesta a incidentes detallado que establezca los roles y responsabilidades del equipo de respuesta, los procedimientos de notificación, la comunicación con las partes interesadas y las medidas de mitigación de incidentes. Realizar ejercicios periódicos de simulación de incidentes para garantizar la efectividad del plan.
- Formación y concienciación en seguridad: Proporcionar formación regular en seguridad de la información para todos los empleados del sector financiero, destacando la importancia de las políticas de seguridad, las mejores prácticas de manejo de datos y la identificación de posibles amenazas.

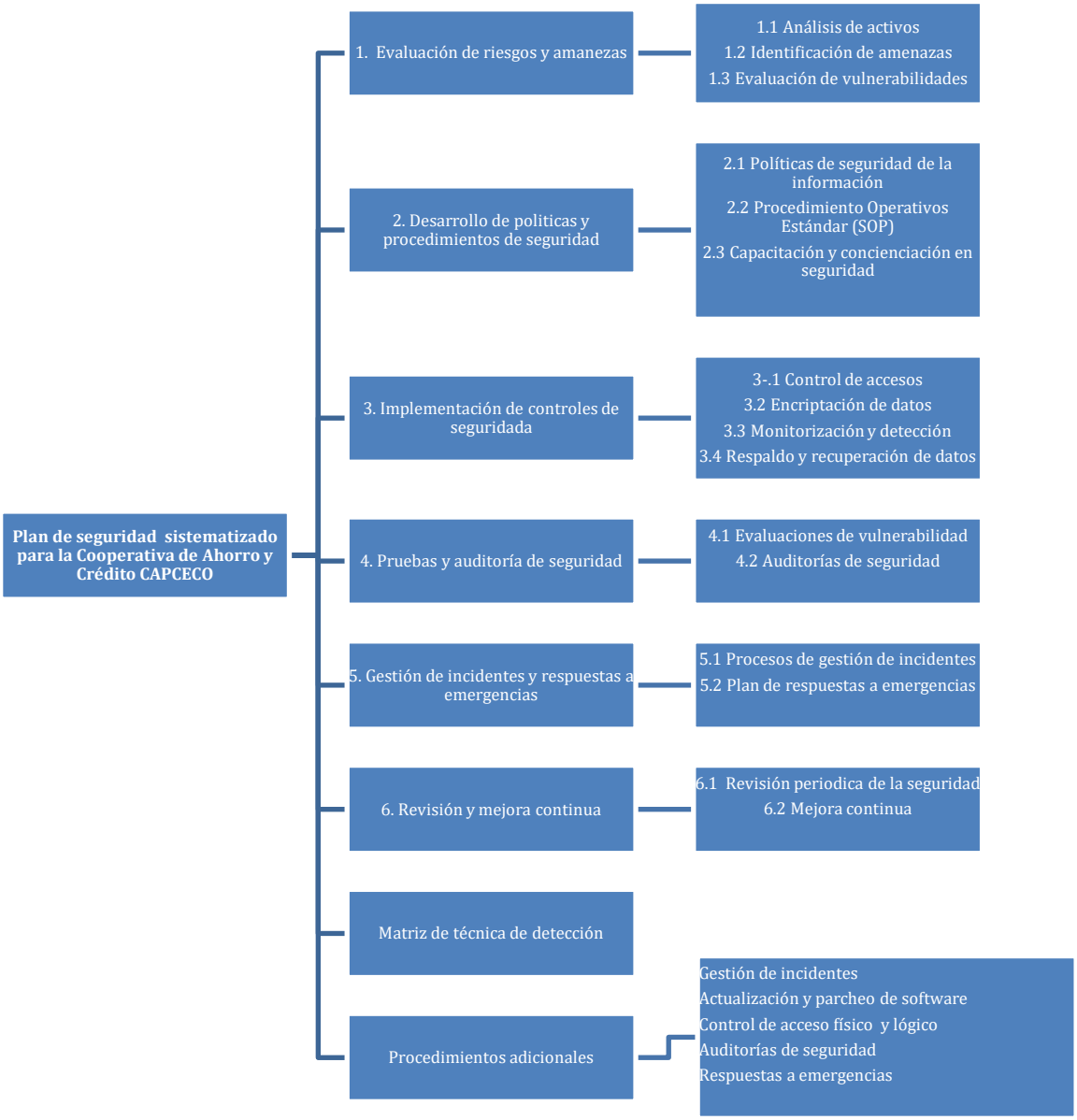
Al integrar los principios y prácticas de la norma de seguridad informática para el sector financiero con los requisitos de ISO 27001, este plan de seguridad proporciona una base sólida para proteger los activos de información crítica y garantizar la confianza y seguridad en las operaciones financieras. Es importante adaptar y personalizar este plan según las necesidades específicas de cada organización y su entorno operativo.

a. Estructura general

La propuesta abordará diferentes aspectos clave de la seguridad de la información, incluyendo la evaluación de riesgos y amenazas, el desarrollo de políticas y procedimientos de seguridad, la implementación de controles técnicos y organizativos, la capacitación del personal en seguridad, las pruebas y validación de los controles implementados, y la revisión continua y mejora del plan de seguridad. A través de esta propuesta, se busca proporcionar a la organización una guía detallada y estructurada para fortalecer la postura de seguridad y proteger los activos de información crítica contra amenazas y ataques cibernéticos de la organización.

Tabla 4

Indicador gráfico de la estructura general de la propuesta



Elaboración propia

b. Explicación del aporte

Plan de seguridad sistematizado detallado para la Cooperativa de Ahorro y Crédito CACPECO:

1. Evaluación de Riesgos y Amenazas

1.1 Análisis de Activos: Identificar y clasificar los activos de información crítica, como datos financieros de los clientes, información de cuentas y transacciones, sistemas de procesamiento de pagos, entre otros.

1.2 Identificación de Amenazas: Realizar un análisis exhaustivo de las posibles amenazas que podrían afectar a la cooperativa, como ataques de phishing, malware, ataques de fuerza bruta, ingeniería social, denegación de servicio, entre otros.

1.3 Evaluación de Vulnerabilidades: Identificar y evaluar las vulnerabilidades en la infraestructura de TI, aplicaciones y procedimientos operativos que podrían ser explotadas por los atacantes.

2. Desarrollo de Políticas y Procedimientos de Seguridad

2.1 Políticas de Seguridad de la Información: Establecer políticas claras y detalladas que aborden aspectos como el acceso a la información, la gestión de contraseñas, el uso aceptable de los recursos informáticos, la gestión de dispositivos móviles, entre otros.

2.2 Procedimientos Operativos Estándar (SOP): Desarrollar procedimientos operativos estándar para actividades clave relacionadas con la seguridad de la información, como la gestión de incidentes, la respuesta a emergencias, la administración de parches, entre otros.

2.3 Capacitación y Concienciación en Seguridad: Implementar programas de capacitación y concienciación en seguridad para el personal, que aborden las mejores prácticas de seguridad, la identificación de amenazas y la respuesta adecuada a incidentes de seguridad.

3. Implementación de Controles de Seguridad

3.1 Control de Acceso: Implementar controles de acceso adecuados para proteger los activos de información crítica, incluyendo autenticación multifactor, gestión de identidades y acceso basado en roles.

3.2 Encriptación de Datos: Utilizar técnicas de encriptación para proteger la confidencialidad de los datos sensibles en reposo y en tránsito, especialmente durante la transmisión de datos a través de redes no seguras.

3.3 Monitorización y Detección de Amenazas: Implementar sistemas de monitoreo de seguridad y detección de amenazas para identificar y responder rápidamente a actividades sospechosas o maliciosas en la red y sistemas de información.

3.4 Respaldo y Recuperación de Datos: Establecer procedimientos para realizar copias de seguridad regulares de los datos críticos y desarrollar un plan de recuperación ante desastres para garantizar la disponibilidad y la integridad de la información en caso de incidentes de seguridad.

4. Pruebas y Auditorías de Seguridad

4.1 Evaluaciones de Vulnerabilidad: Realizar evaluaciones periódicas de vulnerabilidad en la infraestructura de TI y las aplicaciones para identificar y remediar posibles debilidades de seguridad.

4.2 Auditorías de Seguridad: Realizar auditorías de seguridad internas y externas de forma regular para evaluar el cumplimiento de las políticas de seguridad, identificar posibles áreas de mejora y garantizar el cumplimiento de las regulaciones y estándares de seguridad relevantes.

5. Gestión de Incidentes y Respuesta a Emergencias

5.1 Proceso de Gestión de Incidentes: Establecer un proceso formalizado para la gestión de incidentes de seguridad, que incluya la notificación, la escalada y la respuesta rápida y eficaz a los incidentes de seguridad.

5.2 Plan de Respuesta a Emergencias: Desarrollar un plan de respuesta a emergencias que establezca los pasos a seguir en caso de incidentes graves de seguridad, incluyendo la coordinación con las autoridades competentes, la gestión de la comunicación con los clientes y la restauración de los servicios afectados.

6. Revisión y Mejora Continua

6.1 Revisión Periódica de la Seguridad: Realizar revisiones periódicas del plan de seguridad y los controles implementados para garantizar su eficacia y relevancia en un entorno cambiante de amenazas.

6.2 Mejora Continua: Identificar áreas de mejora a partir de las lecciones aprendidas de incidentes de seguridad, auditorías y evaluaciones de seguridad, y realizar ajustes en el plan de seguridad y los controles de acuerdo con las mejores prácticas y estándares de seguridad emergentes.

Este plan de seguridad sistematizado proporciona una estructura integral para proteger los activos de información crítica de la Cooperativa de Ahorro y Crédito CACPECO, garantizando la confidencialidad, integridad y disponibilidad de la información y fortaleciendo la postura de seguridad de la organización.

Matriz de técnicas de detección, prevención y mitigación de impactos ante ataques informáticos a la información sensible Cooperativa de Ahorro y Crédito CACPECO:

Tabla 5

Matriz de técnicas de detección

Tipo de Ataque	Técnicas de Detección	Técnicas de Prevención	Técnicas de Mitigación
Phishing	Monitoreo de correos electrónicos y URLs sospechosas.	Capacitación regular en conciencia de seguridad para el personal.	Implementación de filtros de correo electrónico y URL que bloqueen sitios maliciosos.
Malware	Uso de software de detección de malware actualizado.	Restricción de la instalación de software no autorizado en los sistemas.	Aislamiento de sistemas afectados, eliminación del malware y restauración desde copias de seguridad.
Ataque de Fuerza Bruta	Monitoreo de intentos de acceso	Implementación de políticas de	Bloqueo automático de cuentas después de

	repetidos o no autorizados.	contraseña fuerte y autenticación multifactor.	múltiples intentos fallidos y revisión de logs para detectar patrones de ataque.
Ingeniería Social	Capacitación en conciencia de seguridad y políticas de manejo de información confidencial.	Políticas estrictas de divulgación de información y verificación de identidad.	Implementación de procedimientos para verificar la autenticidad de solicitudes de información confidencial.
Denegación de Servicio (DoS/DDoS)	Monitoreo del tráfico de red y sistemas para detectar patrones inusuales o sobrecarga.	Implementación de sistemas de protección contra DoS/DDoS (como firewalls y sistemas de detección de intrusos).	Redireccionamiento de tráfico, filtrado de paquetes maliciosos y escalado de recursos para mitigar la sobrecarga.
Robo de Datos	Monitoreo de accesos y actividades inusuales en bases de datos y sistemas de almacenamiento.	Encriptación de datos sensibles en reposo y en tránsito.	Bloqueo de accesos no autorizados, revisión forense para determinar el alcance del robo y notificación a las partes afectadas.

Elaboración propia

Procedimientos Adicionales:

1. Gestión de Incidentes: Establecer un proceso formalizado para la gestión de incidentes de seguridad, incluyendo la notificación, escalado y respuesta a incidentes de seguridad.

2. Actualización y Parcheo de Software: Implementar un proceso regular de actualización de software y aplicar parches de seguridad para mitigar vulnerabilidades conocidas.

3. Control de Acceso Físico y Lógico: Implementar controles de acceso físico y lógico para proteger los recursos críticos de la cooperativa, incluyendo el uso de tarjetas de acceso, biometría y políticas de acceso basadas en roles.

4. Auditorías de Seguridad: Realizar auditorías de seguridad periódicas para evaluar el cumplimiento de las políticas de seguridad y detectar posibles debilidades en la infraestructura y procesos de seguridad.

5. Respuesta a Emergencias: Desarrollar planes de respuesta a emergencias que establezcan los pasos a seguir en caso de incidentes de seguridad graves, incluyendo la coordinación con las autoridades competentes y la gestión de la comunicación con los clientes y el público en general.

c. Estrategias y/o técnicas

En cuanto a las estrategias y técnicas empleadas para el plan de seguridad para la Cooperativa de Ahorro y Crédito CACPECO, se tienen que, constituyeron una serie de importantes aportes que benefician tanto a la organización como a sus partes interesadas:

1. Protección de Activos de Información

El plan de seguridad garantiza la protección de los activos de información crítica de la cooperativa, incluyendo datos financieros de clientes, información de cuentas y transacciones, sistemas de procesamiento de pagos, entre otros. Esto ayuda a prevenir la pérdida, robo o compromiso de información sensible, protegiendo la reputación y la confianza de los clientes.

2. Reducción de Riesgos y Amenazas

Al identificar y mitigar los riesgos y amenazas potenciales a los que está expuesta la cooperativa, el plan de seguridad ayuda a reducir la probabilidad y el impacto de incidentes de seguridad, como ataques cibernéticos, fugas de datos y fraudes. Esto contribuye a minimizar las interrupciones en las operaciones comerciales y los costos asociados con la recuperación de incidentes de seguridad.

3. Cumplimiento de Regulaciones y Estándares

El plan de seguridad asegura que la cooperativa cumpla con las regulaciones y estándares de seguridad de la industria financiera, como la Ley de Protección de Datos Personales, normativas específicas del sector financiero y estándares internacionales de seguridad de la información

como ISO 27001. Esto evita sanciones legales, multas y pérdida de confianza por parte de los reguladores y los clientes.

4. Mejora de la Conciencia y la Cultura de Seguridad

A través de programas de capacitación y concienciación en seguridad, el plan de seguridad ayuda a mejorar la conciencia y la cultura de seguridad dentro de la cooperativa. Esto fomenta una mayor responsabilidad y diligencia por parte del personal en la protección de la información sensible y en la detección y reporte de posibles incidentes de seguridad.

5. Fortalecimiento de la Postura de Seguridad

La implementación de controles de seguridad técnicos y organizativos fortalece la postura de seguridad de la cooperativa, aumentando su capacidad para detectar, prevenir y responder eficazmente a las amenazas de seguridad. Esto mejora la resiliencia de la organización frente a posibles ataques y contribuye a la confianza de los clientes y socios comerciales.

6. **Continuidad del Negocio y Resiliencia**

El plan de seguridad incluye medidas para garantizar la continuidad del negocio y la rápida recuperación ante incidentes de seguridad. Esto ayuda a minimizar el tiempo de inactividad y las pérdidas financieras asociadas con interrupciones en las operaciones comerciales, asegurando la resiliencia de la cooperativa frente a eventos adversos.

En resumen, el plan de seguridad proporciona una serie de aportes significativos que fortalecen la capacidad de la Cooperativa de Ahorro y Crédito CACPECO para proteger sus activos de información crítica, cumplir con las regulaciones y estándares de seguridad, mejorar la conciencia y la cultura de seguridad, y garantizar la continuidad del negocio y la resiliencia ante amenazas de seguridad.

Técnicas y métodos para la construcción del Plan de Seguridad

Para desarrollar un plan de seguridad completo y efectivo para la Cooperativa de Ahorro y Crédito CACPECO, se puede utilizar una metodología estructurada que abarque diferentes etapas, desde la evaluación inicial de riesgos hasta la implementación y revisión continua. A continuación, se detalla una metodología general que puede ser adaptada a las necesidades específicas de la cooperativa:

1. Evaluación Inicial

1.1 Recolección de Información: Obtener información detallada sobre los activos de información crítica, las infraestructuras de TI, los procesos operativos y las regulaciones aplicables.

1.2 Identificación de Stakeholders: Identificar a las partes interesadas clave dentro de la cooperativa, incluyendo la alta dirección, los equipos de TI, los usuarios finales y los reguladores.

1.3 Análisis de Riesgos y Amenazas: Realizar un análisis de riesgos y amenazas para identificar las vulnerabilidades y los riesgos potenciales que podrían afectar a la cooperativa y su información sensible.

2. Desarrollo de Políticas y Procedimientos

2.1 Definición de Objetivos de Seguridad: Establecer objetivos claros y medibles para el plan de seguridad, alineados con los objetivos estratégicos de la cooperativa y las regulaciones aplicables.

2.2 Desarrollo de Políticas de Seguridad: Crear políticas de seguridad de la información que aborden aspectos como el acceso a la información, la gestión de contraseñas, la gestión de riesgos, la continuidad del negocio y el cumplimiento de las regulaciones.

2.3 Elaboración de Procedimientos Operativos Estándar (SOP): Desarrollar procedimientos operativos estándar detallados que describan cómo implementar y mantener las políticas de seguridad en la práctica.

3. Implementación de Controles de Seguridad

3.1 Selección de Controles de Seguridad: Identificar y seleccionar los controles de seguridad apropiados para mitigar los riesgos identificados durante la evaluación inicial, teniendo en cuenta factores como el costo, la efectividad y la viabilidad técnica.

3.2 Implementación de Controles Técnicos y Organizacionales: Implementar controles técnicos (por ejemplo, firewalls, sistemas de detección de intrusiones, encriptación) y controles organizativos (por ejemplo, capacitación en seguridad, políticas de acceso) para proteger los activos de información crítica.

4. Capacitación y Concienciación en Seguridad

4.1 Desarrollo de Programas de Capacitación: Diseñar programas de capacitación y concienciación en seguridad para el personal de la cooperativa, que aborden aspectos como la identificación de amenazas, el uso seguro de la tecnología y la respuesta a incidentes de seguridad.

4.2 Implementación de Sesiones de Capacitación: Realizar sesiones periódicas de capacitación en seguridad para todo el personal, asegurándose de que estén actualizados sobre las últimas amenazas y las mejores prácticas de seguridad.

5. Pruebas y Validación

5.1 Pruebas de Penetración y Simulacros de Incidentes: Realizar pruebas de penetración regulares para evaluar la resistencia de los controles de seguridad implementados y realizar simulacros de incidentes para validar la efectividad del plan de respuesta a emergencias.

5.2 Auditorías de Seguridad: Realizar auditorías de seguridad internas y externas para evaluar el cumplimiento de las políticas de seguridad y las regulaciones aplicables, identificar posibles áreas de mejora y garantizar la eficacia de los controles de seguridad.

6. Revisión Continua y Mejora

6.1 Revisión Periódica del Plan de Seguridad: Realizar revisiones periódicas del plan de seguridad para evaluar su efectividad y relevancia en un entorno de amenazas en constante evolución.

6.2 Mejora Continua: Identificar áreas de mejora a partir de las lecciones aprendidas de incidentes de seguridad, auditorías y pruebas de seguridad, y realizar ajustes en el plan de seguridad y los controles de acuerdo con las mejores prácticas y estándares emergentes.

Al seguir esta metodología estructurada, la cooperativa puede desarrollar un plan de seguridad integral que proteja sus activos de información crítica y garantice la confidencialidad, integridad y disponibilidad de la información, fortaleciendo así su postura de seguridad y cumpliendo con las regulaciones y estándares de seguridad aplicables.

Estrategias y técnicas para la socialización del plan de seguridad

Para socializar el plan de seguridad de la Cooperativa de Ahorro y Crédito CACPECO, es crucial contar con una estrategia de comunicación efectiva que involucre a todas las partes interesadas

de manera adecuada. Aquí tienes una planificación detallada para llevar a cabo esta socialización:

1. Identificación de Partes Interesadas

1.1 Equipo Directivo: Involucrar a los líderes y tomadores de decisiones de la cooperativa para obtener su apoyo y compromiso con el plan de seguridad.

1.2 Personal de TI y Seguridad: Informar y capacitar al equipo de tecnología y seguridad sobre los detalles y la importancia del plan de seguridad.

1.3 Empleados de la Cooperativa: Brindar capacitación y concienciación en seguridad a todos los empleados para asegurar su comprensión y compromiso con las políticas y procedimientos de seguridad.

1.4 Clientes y Socios Comerciales: Comunicar de manera transparente y proactiva las medidas de seguridad implementadas para generar confianza y tranquilidad entre los clientes y socios comerciales.

2. Desarrollo de Materiales de Comunicación

2.1 Presentaciones Ejecutivas: Preparar presentaciones ejecutivas para el equipo directivo que destaquen los aspectos clave del plan de seguridad y su importancia para la cooperativa.

2.2 Material Informativo: Crear material informativo, como folletos, correos electrónicos y cartelería, para distribuir entre el personal y clientes, explicando de manera clara y concisa las políticas y procedimientos de seguridad.

2.3 Sesiones de Capacitación: Diseñar sesiones de capacitación interactivas y prácticas para el personal de la cooperativa, que aborden temas relevantes de seguridad y proporcionen orientación sobre cómo cumplir con el plan de seguridad.

3. Implementación de Actividades de Socialización

3.1 Reuniones Informativas: Organizar reuniones informativas con el equipo directivo y el personal de TI para presentar y discutir los detalles del plan de seguridad.

3.2 Seminarios y Talleres: Realizar seminarios y talleres prácticos sobre seguridad de la información para el personal de la cooperativa, con ejemplos y casos de estudio relevantes.

3.3 Campañas de Concienciación: Lanzar campañas de concienciación en seguridad a través de correos electrónicos, intranet y redes sociales internas, destacando la importancia de la seguridad de la información y proporcionando consejos prácticos para mantenerla.

4. Evaluación y Retroalimentación

4.1 Encuestas de Satisfacción: Realizar encuestas de satisfacción para recopilar comentarios y opiniones del personal y clientes sobre la efectividad y la comprensión del plan de seguridad.

4.2 Sesiones de Retroalimentación: Organizar sesiones de retroalimentación con el equipo directivo y el personal de TI para revisar el proceso de socialización e identificar áreas de mejora.

5. Seguimiento y Actualización

5.1 Monitoreo de Cumplimiento: Implementar mecanismos de monitoreo para evaluar el cumplimiento de las políticas y procedimientos de seguridad por parte del personal y clientes.

5.2 Actualización Continua: Mantener actualizado el plan de seguridad y las actividades de socialización en respuesta a cambios en el entorno operativo y las amenazas de seguridad.

Al seguir esta planificación detallada, la Cooperativa de Ahorro y Crédito CACPECO puede garantizar una adecuada socialización de su plan de seguridad, involucrando de manera efectiva a todas las partes interesadas y fortaleciendo la cultura de seguridad dentro de la organización.

1.3. Validación de la propuesta

Para evaluar la propuesta descrita, se ha seleccionado especialistas con un perfil que tenga una formación académica acorde al tema propuesto, que tenga la experiencia laboral y/o académica orientada a la seguridad informática y que este dispuesto a participar en esta evaluación. La tabla a continuación muestra información detallada de lo especialistas seleccionados para la validación del plan (Ver Tabla 6).

Tabla 6

Descripción de perfil de validadores

NOMBRES Y APELLIDOS	AÑOS DE EXPERIENCIA	TITULACIÓN ACADÉMICA	CARGO
RIVERA TOALA RUTH JENNIFFER	12	Máster en Dirección y Gestión de Tecnologías de la Información (TI)	**ANALISTA**
PEREZ DEFRANC HÉCTOR DANIEL	**22**	MÁSTER EN DIRECCIÓN DE SISTEMAS DE INFORMACIÓN Y GESTIÓN EMPRESARIAL	**EXPERTO**

Elaboración propia

Los objetivos perseguidos mediante la validación son los siguientes:

- Validar la metodología de trabajo aplicada en el desarrollo de la investigación.
- Aprobar los resultados, conclusiones y recomendaciones obtenidas.
- Redefinir (si es necesario) el enfoque de los elementos desarrollados en la propuesta, considerando la experiencia de los especialistas.
- Constatar las posibilidades potenciales de aplicación del Plan de negocios propuesto.

Tabla 7

Resultados de la validación

Criterios	Experto 1	Experto 2	Total	Porcentaje
Impacto	4	5	9	**12,86%**
Aplicabilidad	4	4	8	**11,43%**
Conceptualización	5	5	10	**14,29%**
Actualidad	5	5	10	**14,29%**
Calidad Técnica	5	4	9	**12,86%**

Factibilidad	5	5	10	**14,29%**
Pertinencia	5	5	10	**14,29%%**
Total	**28**	**28**	**56**	**94.29%**

Se han establecido los niveles de importancia y representatividad de acuerdo con una escala de Likert en la cual el valor máximo es de 5 puntos (Totalmente de acuerdo) que será otorgado según el desempeño adecuado del criterio; y un valor mínimo de un 1 punto (Totalmente en desacuerdo) en el caso de observarse un cumplimiento insuficiente (Ver anexo 4 y 5).

1.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 8

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Estudio de la Norma de la Seguridad de la información para el sector financiero	Norma basada en la ISO 27000 para proteger la información confidencial, crítica y sensible que manejan las entidades financieras (SEPS, 2022)	Metodología Bibliográfica (SEPS, 2022)	Análisis de la norma que se encuentra vigente	Permite identificar las vulnerabilidades y deficiencias en sus sistemas y procesos de seguridad	Investigación Bibliográfica
Estudio de la ISO 27001	Norma que permite implementar un SGSI para ayudar a proteger la información (ISO/IEC, 2022)	Metodología Bibliográfica (ISO/IEC, 2022)	Análisis de la norma que se encuentra vigente	Protege la confidencialidad, integridad y disponibilidad de la información	Investigación Bibliográfica

Encuesta y entrevista a personal de la cooperativa	Proceso de investigación cuantitativa	Encuesta	Elaboración de entrevista	Se realiza entrevista para verificar el conocimiento sobre la norma técnica para entidades financieras y la ISO 27001	Entrevista

Fuente: Elaboración propia

CONCLUSIONES

El presente proyecto abordó la elaboración de un plan de seguridad mediante la Norma de Seguridad de la Información del Sector Financiero y en conformidad a los criterios básicos señalados en la norma técnica ISO 27001 para el análisis del sistema informático de la Cooperativa de Ahorro y Crédito CACPECO, por lo que se concluye:

A través de un exhaustivo análisis de los fundamentos relacionados con los ataques informáticos más comunes en el sector financiero, hemos logrado identificar las amenazas y vulnerabilidades a las que la Cooperativa de Ahorro y Crédito CACPECO podría estar expuesta. Este conocimiento nos proporciona una base sólida para el desarrollo de estrategias de seguridad informática efectivas y adaptadas a las necesidades específicas de la cooperativa.

La aplicación de metodologías establecidas por la Norma de Seguridad de la Información del Sector Financiero y los criterios de la norma técnica ISO 27001 nos ha permitido diagnosticar de manera precisa la situación actual del sistema de seguridad informática de la Cooperativa de Ahorro y Crédito CACPECO. Identificamos áreas de mejora y vulnerabilidades que necesitan ser abordadas para fortalecer la postura de seguridad de la organización y proteger sus activos de información crítica.

La propuesta de un plan de seguridad sistematizado, basado en una matriz de técnicas de detección, prevención y mitigación de impactos, representa un enfoque integral y proactivo para proteger la información sensible de la Cooperativa de Ahorro y Crédito CACPECO. Este plan establece medidas claras y efectivas para mitigar los riesgos identificados y fortalecer la resiliencia de la organización frente a posibles ataques informáticos.

La evaluación de la efectividad del plan de seguridad, mediante el análisis de indicadores para la mitigación de impactos, nos permite medir el grado de protección de la información sensible de la cooperativa y la eficacia de las medidas implementadas. Esto nos permite identificar áreas de mejora y ajustar el plan de seguridad de manera continua, garantizando así la protección y confidencialidad de los datos de la organización en un entorno en constante evolución.

RECOMENDACIONES

1. Recomendaciones basadas en el estudio de los ataques y vulnerabilidades más comunes en el sector financiero:

- Mantenerse actualizado sobre las últimas tendencias y técnicas de ataques informáticos mediante la participación en cursos de formación y la suscripción a fuentes de información confiables en seguridad cibernética.

- Implementar un sistema de alerta temprana para detectar posibles amenazas emergentes y vulnerabilidades críticas en el entorno de seguridad de la cooperativa.

- Establecer alianzas estratégicas con otras organizaciones del sector financiero para compartir información y mejores prácticas en materia de seguridad informática.

2. Recomendaciones basadas en el diagnóstico de la situación actual del sistema de seguridad informática:

- Realizar auditorías de seguridad de forma regular para evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles implementados.

- Implementar un sistema de gestión de incidentes de seguridad para facilitar la detección, respuesta y recuperación de posibles incidentes de seguridad de manera oportuna y efectiva.

- Realizar evaluaciones de vulnerabilidad periódicas para identificar y remediar posibles debilidades en la infraestructura de TI y las aplicaciones críticas de la cooperativa.

3. Recomendaciones basadas en la propuesta del plan de seguridad sistematizado:

- Capacitar al personal de la cooperativa sobre las políticas y procedimientos de seguridad establecidos en el plan, asegurando que comprendan su importancia y cómo implementarlas en su trabajo diario.

- Establecer un sistema de monitoreo continuo de la efectividad del plan de seguridad, utilizando métricas y KPIs para evaluar su rendimiento y realizar ajustes según sea necesario.

- Fomentar una cultura de seguridad dentro de la cooperativa, promoviendo la responsabilidad compartida de todos los empleados en la protección de la información sensible y la detección de posibles amenazas.

4. Recomendaciones basadas en la evaluación de la efectividad del plan de seguridad:

- Realizar revisiones periódicas del plan de seguridad para asegurarse de que esté alineado con los cambios en el entorno operativo y las nuevas amenazas de seguridad.

- Involucrar a todas las partes interesadas en el proceso de evaluación de la efectividad del plan de seguridad, fomentando la colaboración y el intercambio de ideas para mejorar continuamente la postura de seguridad de la cooperativa.

- Establecer un proceso formalizado para la gestión de lecciones aprendidas de incidentes de seguridad, utilizando esta información para mejorar los procesos y controles de seguridad de manera proactiva.

BIBLIOGRAFÍA

Acos, M., & Recalde, P. (2023). *PROPUESTA DE ESTRATEGIA PARA EVITAR LA FUGA DE INFORMACIÓN EN EMPRESAS CONSTRUCTORAS UTILIZANDO DETECCIÓN POR COMPORTAMIENTO (UEBA) CASO DE ESTUDIO: SCMI INC (USA)*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3544

Alcántara, T., Panizzi, M., & s Sattolo, I. (2022). *Buenas prácticas para la Seguridad Informática en*. Obtenido de https://sedici.unlp.edu.ar/bitstream/handle/10915/149450/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

ASOBANCA. (2023). *Cooperativas de Ahorro y Crédito*. Obtenido de https://asobanca.org.ec/wp-content/uploads/2023/09/Evolucion-de-Cooperativas-Agosto-2023-2.pdf

Beltrán, L. (2022). *PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN PARA PEQUEÑAS EMPRESAS EN LA CIUDAD DE PUYO*. Obtenido de https://repositorio.pucesa.edu.ec/bitstream/123456789/3541/1/77836.pdf

Chango, R., & Gualpa, D. (2023). *IMPLEMENTACIÓN DE PRUEBAS DE HACKEO ÉTICO PARA EVALUAR EL SISTEMA DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RHELEC*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/24450/1/TTS1228.pdf

Chicaiza, D., & Torres, C. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* Obtenido de https://repositorio.uta.edu.ec/handle/123456789/30690

Chilán, K. (2022). *APLICACIÓN DE HACKING ÉTICO*. Obtenido de https://www.google.com/search?q=SEGURIDAD+INFORM%C3%81TICA+MEDIANTE+HACKING+%C3%89TICO+EN+LA+APLICACI%C3%93N+DE+PENTESTING+PARA+EL+AN%C3%81LISIS+DE+VULNERABILIDADES+EN+LAS+REDES+DE+DATOS+DE+LA+COOPERATIVA+SIERRA+CENTRO+SUCURSAL+LA+MAN%C3%81%2C+PROVINCIA+D

Cortijo, R., & Arellano, L. (2020). *SISTEMA DE VIDEO VIGILANCIA MEDIANTE VISIÓN POR COMPUTADOR PARA EL CENTRO DE EDUCACIÓN INICIAL N°1 DEL MINISTERIO DE EDUCACIÓN*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2433

Dávila, J. (2021). *"Implementación de hacking ético para mejorar la detección y evaluación de vulnerabilidades de la seguridad en la infraestructura minera en la ciudad de Lima -*

2021". Obtenido de https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5189/J.Davila_Trabajo_de_Suficiencia_Profesional_Titulo_Profesional_2021.pdf?sequence=1

Garcia, A., & Morales, J. (2022). *SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI*. Obtenido de https://repositorio.utc.edu.ec/bitstream/27000/8458/1/UTC-PIM-000410.pdf

Hurtado, L., & Calero, H. (2020). *Análisis de vulnerabilidades para la infraestructura de red de la bolsa de valores de Quito, aplicando una metodología de Ethical Hacking*. Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3811

Ramos, A., & Recalde, P. (2023). *Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3560

Recalde, P., & Cahueñas, C. (2019). *MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO Explotación de vulnerabilidades y análisis brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en un proceso estratégico.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/1863

Recalde, P., & Cevallos, O. (2023). *PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN EN SERVIENTREGA ECUADOR S.A*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3555

Recalde, P., & Garzón, E. (2023). *Análisis de funcionalidad y utilidad de herramientas de seguridad instaladas en un Security Operation Center (SOC)*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3556

Recalde, P., & Gavilanes, C. (2023). *Guía de análisis de brechas de seguridad para entornos de hipervisores.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3612

Recalde, P., & Ortega, S. (2022). *ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3364

Recalde, P., & Páez, M. (2023). *Descripción del ataque del Ransomware Exx bajo un entorno controlado en máquinas virtuales.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3614

Recalde, P., & Pérez, F. (2023). *INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN PYMES*. Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/3559

Recalde, P., & Vallejo, L. (2023). *Modelo de evaluación del nivel de madurez de la seguridad de la información*. Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/3563

Sarango, D., & Recalde, P. (2023). *PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3561

Silva, E., & Recalde, P. (2022). *Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3365

Sisti, M. (2019). *SEGURIDAD INFORMÁTICA: LA PROTECCIÓN DE LA INFORMACIÓN EN UNA EMPRESA VITIVINÍCOLA DE MENDOZA*. Obtenido de https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Vaca, C., & Cueva, J. (2022). *PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA FRAY JODOCO RICKE BAJO LA NORMA ISO 27001.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3358

Villacís, M., & Recalde, P. (2023). *ANÁLISIS DE BRECHAS DE SEGURIDAD EN REDES LPWAN: SIGFOX Y LORAWAN EN BASE A LA NORMA ISO 27001:2013*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3564

Vivanco, H., & Quintana, A. (2019). *Diseño de un Modelo de Gestión de Seguridad de la Información para la Universidad Iberoamericana del Ecuador.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2019

ISO/IEC. (2022). ISO/IEC 27001. Obtenido de https://www.iso.org/standard/27001

SEPS. (2022). Obtenido de https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTA

Entrevistado: _____

Gerente

1. ¿Está familiarizado con la seguridad de la información?
2. ¿Está familiarizado con los estándares de seguridad de la información?
3. ¿Qué sabe sobre las Normas ISO 27001?
4. ¿Qué sabe sobre la ley de protección de datos?
5. ¿Tienen licencias vigentes los equipos de computación?
6. ¿Cuál es el nivel de seguridad que cumple con los parámetros de ingreso al sistema?
7. ¿Todos los usuarios autorizados de los sistemas tienen acceso a toda la información necesaria?
8. ¿Hay información que se ha difundido fuera del departamento?
9. ¿Existe documentación detallada y disponible en cualquier momento sobre los procesos que se manejan actualmente?
10. ¿Existen actualmente políticas de seguridad para la gestión de datos? Enumere
11. ¿Se lleva a cabo la gestión de riesgos en relación con la seguridad de la información?

Colaboradores

1. ¿Existe una sola persona responsable de la creación de usuarios?
2. ¿Hay algún registro de usuario creado?
3. ¿Se bloquean los usuarios que se encuentran en período de vacaciones o que ya no trabajan para la empresa?
4. ¿Es necesario obtener permisos para la creación de usuarios?

5. ¿Tienen validez las claves creadas?
6. ¿Existen obligaciones para los usuarios con respecto al uso adecuado de los recursos?
7. ¿Existe un control de acceso no autorizado al usuario para proteger el equipamiento y los sistemas de la empresa?
8. ¿La contraseña es única para todos los usuarios?
9. ¿Cuál es el tamaño y la definición del password?
10. ¿El usuario está bloqueado por una clave incorrecta?
11. ¿Pueden los usuarios acceder al sistema desde cualquier equipo?
12. ¿Es posible acceder a través de un equipo diferente si el usuario ya está en uso?

Anexo 2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Pérez DeFranc Héctor Daniel

Título obtenido
Máster en Dirección de sistemas de Información y Gestión Empresarial y Auditor Líder ISO 27001:2013
Cédula de Identidad
1802553584
E- mail
hd.perezd@gmail.com
Institución de Trabajo
Ministerio de Relaciones Exteriores y Movilidad Humana
Cargo
Experto 2
Años de experiencia en el área
22

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		X			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos consideradas en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		X			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		*25*	*8*			

Observaciones: Es fundamental contar con un plan de respuesta a incidentes que defina los pasos a seguir en caso de un ataque o brecha de seguridad. Este plan debe incluir roles y responsabilidades, procedimientos de comunicación y estrategias de recuperación.

El panorama de las amenazas cibernéticas está en constante evolución. Es importante mantenerse actualizado sobre las últimas amenazas y vulnerabilidades para poder tomar medidas preventivas.

Recomendaciones

Es vital realizar copias de seguridad regulares de los datos críticos de la organización para garantizar la disponibilidad en caso de un ataque o desastre. Se recomienda implementar una solución de copia de seguridad que sea confiable y segura.

Lugar, fecha de validación: Quito, 9 de marzo de 2024

_____

Firma del especialista

Anexo 3

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Rivera Toala Ruth Jenniffer

Título obtenido
Máster en Dirección y Gestión de Tecnologías de la Información (TI)
Cédula de Identidad
0921790366
E- mail
r_jenniffer@hotmail.com
Institución de Trabajo
Ministerio de Relaciones Exteriores y Movilidad Humana
Cargo
Analista
Años de experiencia en el área
12

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Plan de seguridad basado en la norma de la seguridad informática para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		X			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		X			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		*25*	*8*			

Observaciones: Es importante realizar un análisis exhaustivo de los riesgos a los que está expuesta la organización para poder identificar las vulnerabilidades y amenazas más críticas. Esto permitirá priorizar las medidas de seguridad y enfocar los recursos de forma eficiente.

Es crucial controlar quién tiene acceso a los datos y sistemas de la organización. Esto incluye implementar medidas de autenticación y autorización fuertes, así como segmentar la red para limitar el acceso a los recursos críticos.

Recomendaciones

Es vital mantener los sistemas y software actualizados con los últimos parches de seguridad para evitar vulnerabilidades conocidas. Una solución de gestión de parches automatiza este proceso y ayuda a garantizar que todos los dispositivos estén protegidos.

Lugar, fecha de validación: Quito, 9 de marzo de 2024

Firma del especialista

Anexo 4

Instrumento para validar

Criterios	Descripción	Preguntas	Escala de estimación				
			En Total Desacuerdo	En desacuerdo	Neutral	De acuerdo	Totalmente de acuerdo
Impacto	Representa el alcance que tendrá el modelo de gestión y su representatividad en la generación de valor público.	¿Considera que el Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO propuesto representará un impacto significativo en la generación de valor público?				X	
Aplicabilidad	La capacidad de implementación del modelo considerando que los contenidos de la propuesta sean aplicables	¿Los contenidos de la propuesta son aplicables?				X	
Conceptualización	Los componentes de la propuesta tienen como base conceptos y teorías propias de la gestión de manera sistémica y articulada.	¿Los componentes de la propuesta tienen como base conceptos y teorías de la gestión?					X
Actualidad	Los contenidos de la propuesta consideran los procedimientos actuales y los cambios científicos y tecnológicos que se producen en la nueva gestión pública.	¿Los contenidos de la propuesta consideran los procedimientos actuales y nuevos cambios que puedan producirse?					X
Calidad Técnica	Miden los atributos cualitativos del contenido de la propuesta.	¿El modelo propicia el cumplimiento de los protocolos de atención analizados desde la óptica técnico-científica?					X
Factibilidad	Nivel de utilización del modelo propuesto por parte de la Entidad	¿Es factible incorporar un modelo de gestión por resultados en el sector?					X
Pertinencia	Los contenidos de la propuesta son conducentes, concernientes y convenientes para solucionar el problema planteado.	¿Los contenidos de la propuesta pueden dar solución al problema planteado?					X

Nombre: Ruth Rivera

CC: 0921790366

Firma:

Anexo 5

Instrumento para validar

Criterios	Descripción	Preguntas	Escala de estimación				
			En Total Desacuerdo	En desacuerdo	Neutral	De acuerdo	Totalmente de acuerdo
Impacto	Representa el alcance que tendrá el modelo de gestión y su representatividad en la generación de valor público.	¿Considera que el Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO propuesto representará un impacto significativo en la generación de valor público?					X
Aplicabilidad	La capacidad de implementación del modelo considerando que los contenidos de la propuesta sean aplicables	¿Los contenidos de la propuesta son aplicables?				X	
Conceptualización	Los componentes de la propuesta tienen como base conceptos y teorías propias de la gestión de manera sistémica y articulada.	¿Los componentes de la propuesta tienen como base conceptos y teorías de la gestión?					X
Actualidad	Los contenidos de la propuesta consideran los procedimientos actuales y los cambios científicos y tecnológicos que se producen en la nueva gestión pública.	¿Los contenidos de la propuesta consideran los procedimientos actuales y nuevos cambios que puedan producirse?					X
Calidad Técnica	Miden los atributos cualitativos del contenido de la propuesta.	¿El modelo propicia el cumplimiento de los protocolos de atención analizados desde la óptica técnico-científica?				X	
Factibilidad	Nivel de utilización del modelo propuesto por parte de la Entidad	¿Es factible incorporar un modelo de gestión por resultados en el sector?					X
Pertinencia	Los contenidos de la propuesta son conducentes, concernientes y convenientes para solucionar el problema planteado.	¿Los contenidos de la propuesta pueden dar solución al problema planteado?					X

Nombre: Héctor Pérez

CC: 1802553584

Firma:

HECTOR DANIEL PEREZ DEFRANC