UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Tema: "Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito"

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ingeniero, Luis Roberto Morales Alomoto

Director: Ingeniero, Carlos Israel Núñez Miranda Mg.

Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia, Mg., e integrado por los señores Ingeniero Hernán Fabricio Naranjo Ávalos, Mg., Ingeniero Félix Oscar Fernández Peña, PhD., Ingeniero Edison Homero Álvarez Mayorga, Mg., designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "BALANCED SCORECARD PARA SEGURIDAD DE LA INFORMACIÓN BAJO EL ESTÁNDAR ISO 27001 EN COOPERATIVAS DE AHORRO Y CRÉDITO", elaborado y presentado por el señor Ingeniero Morales Alomoto Luis Roberto, para optar por el Grado Académico de Magíster en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia, Mg.
Presidente del Tribunal

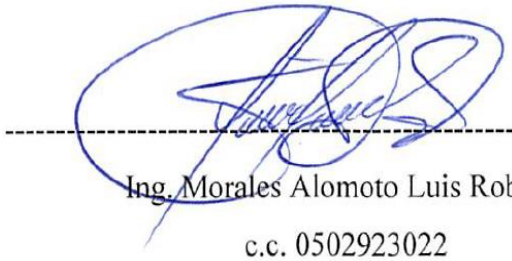
Ing. Hernán Fabricio Naranjo Ávalos, Mg.
Miembro del Tribunal

Ing. Félix Oscar Fernández Peña, PhD.
Miembro del Tribunal

Ing. Edison Homero Álvarez Mayorga, Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

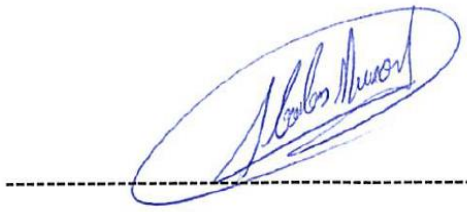
La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "BALANCED SCORECARD PARA SEGURIDAD DE LA INFORMACIÓN BAJO EL ESTÁNDAR ISO 27001 EN COOPERATIVAS DE AHORRO Y CRÉDITO", le corresponde exclusivamente a: Ingeniero, Morales Alomoto Luis Roberto, Autor bajo la Dirección del Ingeniero, Carlos Israel Núñez Miranda, Mg., Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. Morales Alomoto Luis Roberto

c.c. 0502923022

AUTOR



Ing. Carlos Israel Núñez Miranda Mg.

c.c. 1803459450

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Morales Alomoto Luis Roberto

c.c. 0502923022

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

Agradezco en primer lugar a Dios, porque por su gracia y su bendición he logrado alcanzar una meta más en mi vida y en mi vida profesional, a mi madre por su apoyo constante, su dedicación y motivación, a mis hermanos y sobrinos, a toda mi familia.

Agradecer también a mi amigo, profesor y director Ing. Carlos Nuñez, a la Ingeniera Katalina Coronel quien ha aportado con su conocimiento profesional para poder culminar con éxito este tema de investigación y un agradecimiento especial a la Universidad Técnica de Ambato por abrirme las puertas y brindarme la oportunidad de progresar con más conocimiento y su excelente trabajo para crear profesionales de valor.

Morales Alomoto Luis Roberto

DEDICATORIA

A Dios por todas sus bendiciones para mí y mi familia.

En especial a mi madre, pilar fundamental de mis sacrificios, por su amor y constancia y de lucha, pero sobre todo por haberme dado la vida, vida que no me alcanzará para agradecerle todo lo que ha sido para mí y mis hermanos.

Dedicarle también de manera especial este trabajo a Dolores Alomoto, mi abuelita a quien tengo la dicha y el honor de tenerla presente junto a nosotros, sus nietos, sus hijos, sus bisnietos, sus tataranietos y demás.

Morales Alomoto Luis Roberto

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"BALANCED SCORECARD PARA SEGURIDAD DE LA INFORMACIÓN BAJO EL ESTÁNDAR ISO 27001 EN COOPERATIVAS DE AHORRO Y CRÉDITO"

AUTOR: Ing. Morales Alomoto Luis Roberto
DIRECTOR: Ing. Carlos Israel Núñez Miranda, Mg.
FECHA: 24 de Octubre, 2018

RESUMEN EJECUTIVO

En este trabajo se plantea un modelo de Balanced ScoreCard que permita la toma de decisiones basadas en seguridad de información, es importante destacar que los activos que son analizados son aquellos que cumplen un rol importante dentro de uno o varios procesos, por lo tanto, merece de un tratamiento especial, ya que este es parte vital en la continuidad del negocio. Los datos fueron recopilados de la encuesta realizada a los empleados de las diferentes áreas, donde se ha desarrollado el tema de tesis propuesto. La percepción de los empleados y a su vez usuarios de los sistemas de información es que existen controles que previenen de los errores pero estos no son muy efectivos por lo tanto es de vital importancia crear lineamientos para el tratamiento de la registros, partiendo desde del inventario de los equipos informáticos con los que cuenta el departamento de TI distribuidos en las agencias y edificio matriz, análisis de los procesos más importantes, validando los dispositivos y software que hacen que un proceso fluya, realizar el análisis de riesgo a estos activos y construir el plan de seguridad, el mismo que es a su vez la entrada que representa al Balanced ScoreCard. Con la implementación del modelo de Balanced ScoreCard en la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., se genera un marco central y organizativo para los procesos y clarificación de las estrategias en cuanto a

seguridad de información, impactando positivamente en las jefaturas de Riesgo y TI de la entidad financiera.

Descriptores: Seguridad de información, plan de seguridad de información, tecnología, procesos, plan de acción, riesgo residual, riesgo inherente, nivel de riesgo, análisis de riesgo, sistemas de información.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"BALANCED SCORECARD PARA SEGURIDAD DE LA INFORMACIÓN BAJO EL ESTÁNDAR ISO 27001 EN COOPERATIVAS DE AHORRO Y CRÉDITO"

AUTHOR: Ing. Morales Alomoto Luis Roberto

DIRECTED BY: Ing. Carlos Israel Núñez Miranda, Mg.

DATE: October 24, 2018

EXECUTIVE SUMMARY

In this task, we plant a model of BalancScore card that allows decision making based on the information security. It is important to highlight that the active ones that are analysed are in fact those that play an important role within one or more processes, therefor it deserves a special treatment, because it is a vital part in the continuity of business. The data were gathered from the inquests that were submitted by the employees from different áreas, where the proposed thesis has been developed.The perception of the employees and users of the information systems, is that there are controls that prevent errors, But these aren't very effective, therefore is of vital importance creating guidelines as far as records, staring from the inventory of the informant equipment which the department of TI distributed in the agencies as well in the headquarters, análisis of the most impertinent process, validating the dispositives and software that allow a process to flow, realizing the risks on the analysis to the active and building a constructing a plan for security, the one that at the same time is what represents the balance scorecard. With the implementation of model balance scorecard in the company of savings and credit Maquita Cushunchic Ltda, it generates a central aim and organized in the process and clarifications of the

strategies as far as the information security, impacting positively in the risk headquarters and TI financial entity.

KEYWORDS: Information security, information security plan, technology, processes, action plan, residual risk, inherent risk, level of risk, risk analysis, information systems.

INTRODUCCIÓN

Las Cooperativas de Ahorro y Crédito, son instituciones de carácter financiero y sus servicios se enfocan básicamente en satisfacer las necesidades económicas a nivel empresarial o personal. Por lo que contar con un Balanced ScoreCard para la toma de decisiones en cuanto a Seguridad de información es muy importante, esto permitirá enfocar la inversión anual en los activos que muestren mayor riesgo y sean parte de los procesos más importantes.

La información es el activo más importante de cualquier organización, sea pública, privada o mixta, por lo que diseñar un Balanced ScoreCard enfocado a la norma ISO 27001 es muy importante, porque este a su vez permite identificar los riesgos y establecer controles para gestionarlos o eliminarlos.

En los últimos años las cooperativas de ahorro y crédito han tenido un crecimiento muy importante en la economía del Ecuador, convirtiendo al Ecuador en el segundo país con más número de este tipo de entidades después de Brasil como lo indica la SEPS (SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA) en su página web, publicado en el marco del décimo tercer aniversario de la Unión de Cooperativas de Ahorro y Crédito del Sur (Ucacsur), evento realizado el 11 de diciembre, en Cuenca (SEPS, 2015).

El titular de la SEPS, planteó la necesidad de integración de las entidades financieras, mediante fusiones y absorciones como uno de los retos a los que se enfrenta el sistema financiero popular y solidario, para consolidarse y fortalecerse (SEPS, 2015).

Enfatizó que estos procesos de integración, deben nacer dentro del sector, “como ha sucedido recientemente, lográndose fusiones exitosas”; sin embargo, dijo que la integración no sólo se concreta con fusiones o absorciones, sino que las entidades pueden constituir redes, en las que compartir imagen corporativa, estrategias, tarjetas de crédito y cajeros automáticos, que sin duda fortalecerán al sector (SEPS, 2015).

Actualmente se encuentran registradas dentro de este organismo 887 cooperativas de ahorro y crédito, sumando entre ellas 4.700.000 socios y generando activos de 8.300 millones de dólares, haciendo ver que el sector ha crecido en los últimos 3 años y medio muy notablemente, un 66% del microcrédito corresponden a estas instituciones financieras haciendo a este producto financiero, en algo distintivo del sistema financiero cooperativo frente a la banca, por lo que instó a protegerlo (SEPS, 2015).

El trabajo de investigación queda estructurado de la siguiente manera:

El capítulo I denominado "EL PROBLEMA DE INVESTIGACIÓN", se describe el problema que es el objeto de la investigación, que contempla el tema de investigación, el planteamiento del problema, la contextualización macro, meso y micro, el análisis crítico, la prognosis, la formulación del problema, las interrogantes, la delimitación del objeto de investigación, la justificación y los objetivos generales y específicos.

El capítulo II denominado "MARCO TEÓRICO", está estructurado por los antecedentes de la investigación, la fundamentación filosófica y legal, las categorías fundamentales y el señalamiento de variables.

El capítulo III denominado "METODOLOGÍA", se describe el enfoque, la modalidad básica de investigación, nivel o tipo de investigación, la población y muestra, la Operacionalización de variables, plan de recolección de información y el plan de procesamiento de la información

El capítulo IV denominado "ANÁLISIS E INTERPRETACIÓN DE RESULTADOS", se describe el análisis de resultados, la verificación de la prueba de hipótesis que se realizó utilizando el método estadístico – descriptivo.

El capítulo V denominado "CONCLUSIONES Y RECOMENDACIONES", se presentan las conclusiones y recomendaciones de la investigación del problema

planteado, están basados en la información y el análisis realizado en los capítulos anteriores.

El capítulo VI denominado “DESARROLLO DE LA PROPUESTA” (basada en la NORMA Internacional ISO 27001:2013), contempla la información detallada de la Normativa de Seguridad de la información; tema, datos informativos, antecedentes de la propuesta, la justificación, los objetivos, el análisis de factibilidad, la fundamentación científica y técnica, propuesta de la normativa que incluye las fases: situación actual, diseño de la normativa de seguridad, haciendo énfasis en los criterios: políticas de seguridad, principios de seguridad, proyección de resultados por la aplicación de la normativa de seguridad y el Plan de Seguridad.

Finalizando con los Anexos, que contiene la encuesta aplicada, las Políticas de Seguridad y procesamiento de la información de las encuestas por empresa.

CAPÍTULO I

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito.

1.2 Planteamiento del Problema

1.2.1 Contextualización

Según la (Financoop, 2018), las cooperativas de ahorro y crédito han tenido un crecimiento significativo cerrando el 2017 con 656 entidades financieras de cooperativas afiliadas observando un crecimiento del 7.3% con respecto al 2016 con una participación del 18.9% lo que corresponde a USD 11.186 millones de dólares por debajo del Sistema Privado Bancario que cuenta con el 65.9% correspondiente a USD 38.974 millones de dólares, considerando también el crecimiento en infraestructura, clientes y microcréditos, por lo que eso implica también un incremento muy importante en la información que las entidades financieras manejan por lo tanto proveerse de una herramienta informática que permita controlarla es cada vez más importante.

Figura 1. Participación de Activos a Diciembre 2017

Fuente: (Financoop, 2018)

Adquirir un Balanced ScoreCard para la gestión de la seguridad de la información y este a su vez permita controlar, prevenir, mitigar o eliminar los riesgos que puede incurrir en el tratamiento de los datos por parte de los empleados o clientes es muy complicado, es por eso que se plantea como tema **"Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito"**, en una época donde la tecnología informática brinda grandes herramientas que permitan poder realizar este tipo de actividades y normas técnicas que indican las mejores prácticas de hacerlo como es la ISO 2700 (Advisera).

Antes de optar por algún software de Balanced ScoreCard, se debe evaluar las mejores opciones que cumplan con los parámetros y características, siempre enfocadas en el usuario final (clientes, empleados), ya que, de la eficiencia, facilidad de uso, satisfacción del usuario y seguridad, dependerá el provecho que se obtenga de la misma, consecuentemente el grado de apoyo que ésta brinde a la organización en lo que es el tratamiento de la información. No existe una herramienta que evite los riesgos en el manejo de la información, pero si existen varias que permiten mantener prevenida a la empresa como es la IsoTools, Itson, Isolucion, entre otras, para la Gestión de la Seguridad de la Información, la implementación de la ISO 27001 en un Balanced ScoreCard permite mantener al tanto a todos los involucrados de las mejores prácticas en el tratamiento de incidentes que pueden ocurrir (Advisera).

Según ((Advisera, s.f.), La ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; a continuación, se puede ver la cantidad de certificados en los últimos años:

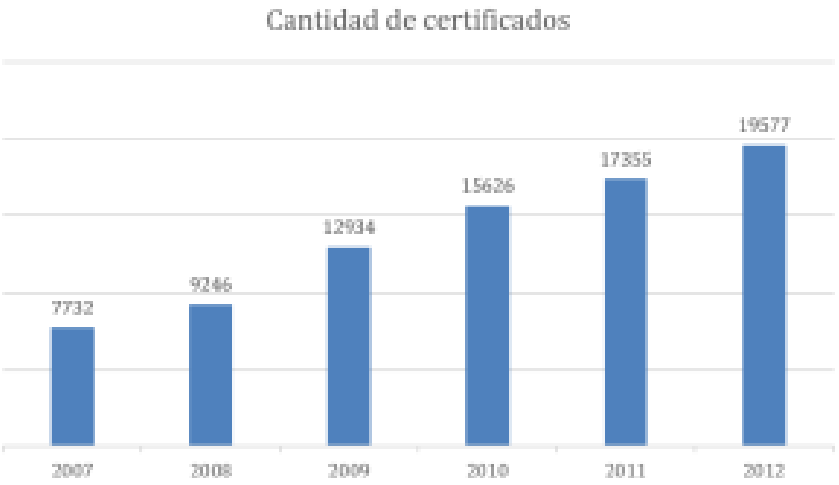


Figura 2. Cantidad de Empresas Certificados

Fuente: (Advisera, s.f.)

1.2.2 Análisis Crítico

En la actualidad el avance tecnológico y su apoyo constante en el manejo de la información y procesos del negocio han influenciado a las empresas a ofrecer sus servicios a través de sistemas informáticos cada vez más modernos ya sean estos en ambiente web, de escritorio o con infraestructura almacenada en la nube (Services, 2018).

La principal función de estos sistemas informáticos es tener la capacidad de almacenar información de la empresa, por lo mismo que se convierte en el activo más importante a salvaguardar, sin importar su naturaleza, debe ser gestionada y tratada de manera muy diferente por la criticidad que estos representan (Services, 2018).

Hoy en día asegurar los datos que se manejan es muy importante y esta a su vez se encuentra expuesta a ciberdelincuencia y espionaje cibernético actividades delincuenciales que actualmente operan a través del internet y tienen como principales víctimas a empresas públicas o privadas, personas naturales, gobiernos o negocios, dañando su imagen y reputación (Services, 2018).

Según (Services, 2018), la seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática (Services, 2018).

Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en riesgo los activos digitales ni tampoco que la información que manejan o almacenan sea vulnerable (Services, 2018).

La información: Es el principal activo. Mediante métodos y en diversos puntos se busca garantizar que la información esté disponible cuándo y cómo debe estarlo, sin que su tratamiento represente un riesgo económico para la empresa (Services, 2018).

Aspectos importantes a tomar en cuenta para la seguridad de la información.

- Protección de los datos y la privacidad de la información personal.
- Protección de los registros de la información.
- Derechos de la propiedad intelectual.
- Documentación de la política de seguridad de la información.
- Asignación de responsabilidades.
- Concienciación, formación y capacitación en seguridad de la información.
- Vulnerabilidad técnica.
- Gestión de incidentes de seguridad.
- Gestión de continuidad del negocio.

1.2.3 Prognosis

La información es un elemento crítico en el éxito y la supervivencia de las empresas y organizaciones y es por esa razón que las Cooperativas de Ahorro y Crédito del Ecuador buscan la administración efectiva de la misma y su resguardo considerando además la Tecnología de la Información (TI) relacionada y generada en esta sociedad global donde esta viaja a través de varios medios (Internet, Intranet) y dispositivos (Celular, laptop, Computador de escritorio, tablet,.., etc.). Es la información y la tecnología la que soporta la sobrevivencia de la empresa, motivo por el cual los responsables en su nivel jerárquico más elevado, optan por implantar métodos, modelos y sistemas de seguridad de la información, los mismos deben ser evaluados en su eficiencia y eficacia, es ahí donde la auditoria interviene permitiendo su revisión y análisis por medio de estándares, buenas prácticas, guías, etc., aceptadas y de aplicación internacional que permiten que se evidencie el estado de los Sistemas de Seguridad de la Información (Suñagua, 2013).

1.2.4 Formulación del problema

¿Cómo el balanced scorecard ayudará a la seguridad de la información en cooperativas de ahorro y crédito?

1.2.5 Interrogantes (Subproblemas)

- ¿Cuáles serían los parámetros a considerar y que permitan identificar los procesos críticos que necesiten la implementación de un modelo de seguridad?
- ¿Se puede desarrollar un Balance ScoreCard, que permita generar información de manera ágil y oportuna para la toma de decisiones en el área de TI?

1.3 Justificación

Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información.

Por lo antes expuesto vemos que el presente trabajo es de interés e incide directamente en que el mismo sea factible de ser realizado, al disponer de los

recursos necesarios para el cumplimiento de los objetivos y esto se lo hace posible mediante el diseño de un Balanced ScoreCard para la seguridad de información en las Cooperativas de Ahorro y Crédito.

Siendo la Superintendencia de Bancos una institución de regulación creada para supervisar y controlar las actividades que ejercen las entidades financieras y seguridad social, sea público o privado, con el fin de garantizar los intereses de la ciudadanía y fortalecerlas, es la misma que promueve a las instituciones financieras como es el caso de las cooperativas de ahorro y crédito a cumplir con las obligaciones impuestas por el ente de regulación antes mencionado.

Es importante que cada entidad financiera se acoja a las exigencias de la Superintendencia de Bancos, que, en la Codificación de Resoluciones, LIBRO UNO – SISTEMA FINANCIERO, SECCIÓN X - DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, Capítulo V, De la gestión del riesgo operativo. (Reformado mediante Resoluciones 285-2016-F y con 318-2016-F de la JPRMF), en el Art. 21 y 22, indican que se debe de gestionar la seguridad de la información y salvaguardarla, para satisfacer las necesidades de la entidad, ante revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya., base legal que se hace referencia en el MARCO TEÓRICO en el apartado 2.3 Fundamentación Legal.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar un Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito

1.4.2 Objetivos Específicos:

- Definir las políticas de seguridad.
- Identificar todos aquellos activos de información que tienen algún valor para la organización.

- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.
- Elaborar un plan de seguridad que permita a la Cooperativa evaluar los niveles de riesgo y cumplimiento de acuerdo a los planes de acción determinados.

CAPITULO II

2 MARCO TEÓRICO

2.1 Antecedentes Investigativos

Las Cooperativas de Ahorro y Crédito son instituciones que buscan ser un puente financiero solidario, canalizando ahorros de gente trabajadora y responsable hacia créditos que contribuyan al desarrollo de microempresas y al mejoramiento de la calidad de vida de sus prestatarios.

Su propiedad está dividida en miles de personas y su gestión está a cargo de un equipo de profesionales de primer nivel, altamente comprometidos con los objetivos financieros y sociales que persigue cada institución. El desarrollo de productos y servicios se realiza sobre un equilibrio REAL entre rentabilidad financiera y social.

Para el presente trabajo se toma en cuenta la creación y el fortalecimiento de controles existentes que se relacionan directamente con la seguridad física y lógica de la información, que maneja el personal responsable dentro de cada institución financiera, sea a través de políticas de seguridad de la información, seguridades implementadas en servidores como por ejemplo Active Directory, entre otras. Se tiene como finalidad crear una cultura organizacional en el empleado responsable, en cuanto al manejo y gestión de la información se refiere, para ello se plantea realizar charlas, planes de divulgación de seguridad de información y prevenciones de riesgos para reducir los mismos. Todo esto servirá para que la institución pueda dar cabida a una mejora en el rendimiento por parte de sus empleados, mejorando la satisfacción de sus clientes, de esta manera mejorará notablemente los ingresos económicos que los directivos esperan ver reflejados, para esto se toma en cuenta trabajar con la norma ISO 27001 que es la encargada de realizar ajustes que sirvan en el aseguramiento de sus datos.

Con lo antes mencionado se busca asegurar en lo posible los activos de información como:

- Hardware
- Software
- Redes LAN y WAN
- Servidor de Correo
- Servidor de Aplicaciones
- Servidor de Base de Datos
- Internet
- Infraestructura Y telecomunicaciones
- File Server
- Servidor de Archivos, ect.

Luego de realizar una revisión y análisis bibliográfico, en el repositorio de la Universidad Técnica de Ambato no se pudo encontrar referencias de estudios similares.

Al revisar la literatura en bases de datos científicas se encontraron los siguientes estudios relacionados a seguridad de información:

En la investigación de (Duque, 2017) se propone una metodología de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001, los controles de seguridad presentados en la ISO/IEC 27002, el esquema de riesgos de la ISO/IEC 27005 y los pasos recomendados en la ISO/IEC 27003. Se genera como resultado un proceso metodológico que da respuesta a cómo abordar un proyecto de este nivel de importancia en el contexto actual de las organizaciones y basado en estándares internacionales. Este proceso metodológico representa un aporte a los profesionales que emprenden esta labor, y que buscan un método para una implementación exitosa de un SGSI.

En la investigación de (Martelo, 2015) indica que el objetivo principal de este trabajo consiste en desarrollar un software para contribuir al control de los documentos generados a partir del proceso de implantación de un Sistema de Gestión de

Seguridad de la Información (SGSI). Dicho software permite recepcionar, administrar y organizar la documentación generada en el proceso de implantación del SGSI. Para soportar dicho software, se diseña e implementa un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. Lo anterior, produjo como resultado un módulo para gestión documental que permite el control de documentos durante el proceso de implantación de un SGSI, trabajando bajo procedimientos del estándar ISO 27001.

A continuación, se presenta la fundamentación teórica relacionada al tema de investigación:

ISO 27001.

> Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (Advisera, s.f.).
>
> ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001 (Advisera, s.f.).

Documentación obligatoria que solicita la norma ISO 27001 para la certificación de una Institución.

Según (Advisera, s.f.), requiere que se confeccione la siguiente documentación.

- Alcance del SGSI (punto 4.3)
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2)
- Declaración de aplicabilidad (punto 6.1.3 d)
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2)
- Informe de evaluación de riesgos (punto 8.2)
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4)
- Inventario de activos (punto A.8.1.1)
- Uso aceptable de los activos (punto A.8.1.3)

- Política de control de acceso (punto A.9.1.1)
- Procedimientos operativos para gestión de TI (punto A.12.1.1)
- Principios de ingeniería para sistema seguro (punto A.14.2.5)
- Política de seguridad para proveedores (punto A.15.1.1)
- Procedimiento para gestión de incidentes (punto A.16.1.5)
- Procedimientos para continuidad del negocio (punto A.17.1.2)
- Requisitos legales, normativos y contractuales (punto A.18.1.1) (Advisera, s.f.).

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2)
- Monitoreo y resultados de medición (punto 9.1)
- Programa de auditoría interna (punto 9.2)
- Resultados de auditorías internas (punto 9.2)
- Resultados de la revisión por parte de la dirección (punto 9.3)
- Resultados de medidas correctivas (punto 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3) (Advisera, s.f.).

Por supuesto que una empresa puede decidir confeccionar otros documentos de seguridad adicionales si lo considera necesario.

Otro atributo importante a tomar en cuenta es la integridad de los datos como lo detalla ISACA.

> La importancia de la integridad de los datos se puede ilustrar con un sencillo ejemplo: Una persona necesita un tratamiento hospitalario que incluye la administración diaria de un medicamento en dosis de 10 miligramos (mg). Accidental o intencionalmente, se produce una modificación en el registro electrónico del tratamiento y las dosis quedan establecidas en 100 mg, con consecuencias mortales. Para tomar otro ejemplo, podríamos imaginar una situación propia de una obra de ficción que antecediera al ataque del virus Stuxnet en 2010 y preguntarnos qué ocurriría si alguien interfiriera los sistemas de control de una central nuclear para que simularan condiciones de funcionamiento normal cuando, en realidad, se ha provocado una reacción en cadena. ¿Podemos afirmar que los profesionales reconocen las múltiples definiciones de la "integridad de los datos"? Veamos:

Para un encargado de seguridad, la "integridad de los datos" puede definirse como la imposibilidad de que alguien modifique datos sin ser descubierto. Desde la perspectiva de la seguridad de datos y redes, la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria. Si examinamos el concepto de "integridad", podríamos concluir que no solo alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurados [SDLC], revisión de códigos fuente por expertos, pruebas exhaustivas, etc.), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etc.) (Isaca, 2011).

Para un administrador de bases de datos, la "integridad de los datos" puede depender de que los datos introducidos en una base de datos sean precisos, válidos y coherentes. Es muy probable que los administradores de bases de datos también analicen la integridad de las entidades, la integridad de los dominios y la integridad referencial —conceptos que podría desconocer un experto en infraestructuras instruido en normas ISO 27000 o en la serie 800 de publicaciones especiales (SP 800) del Instituto Nacional de Normas y Tecnología (NIST, National Institute of Standards and Technology) de los EE. UU (Isaca, 2011).

Para un arquitecto o modelador de datos, la "integridad de los datos" puede estar relacionada con el mantenimiento de entidades primarias únicas y no nulas. La unicidad de las entidades que integran un conjunto de datos se define por la ausencia de duplicados en el conjunto de datos y por la presencia de una clave que permite acceder de forma exclusiva a cada una de las entidades del conjunto (Isaca, 2011).

Para el propietario de los datos (es decir, para el experto en la materia), la "integridad de los datos" puede ser un parámetro de la calidad, ya que demuestra que las relaciones entre las entidades están regidas por reglas de

negocio adecuadas, que incluyen mecanismos de validación, como la realización de pruebas para identificar registros huérfanos (Isaca, 2011).

Para un proveedor, la "integridad de los datos" es:

La exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro de datos. La integridad de los datos se establece en la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores.
En un diccionario disponible en línea, se define la "integridad de los datos" de este modo:

Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. La integridad de los datos es uno de los seis componentes fundamentales de la seguridad de la información (Isaca, 2011).

Análisis

Según (CONCEPTODEFINICION, 2018): "El Análisis es un estudio profundo de un sujeto, objeto o situación con el fin de conocer sus fundamentos, sus bases y motivos de su surgimiento, creación o causas originarias. Un análisis estructural comprende el área externa del problema, en la que se establecen los parámetros y condiciones que serán sujetas a un estudio más específico, se denotan y delimitan las variables que deben ser objeto de estudio intenso y se comienza el análisis exhaustivo del asunto de la tesis"

Riesgo

Según (CIIFEN, 2018), "El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. [1] Los factores que lo componen son la amenaza y la vulnerabilidad."

2.2 Fundamentación Filosófica

La presente investigación se enmarca en el paradigma Crítico Propositivo, es crítico por que realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al mismo.

2.3 Fundamentación Legal

El presente trabajo de investigación se sustenta en la siguiente base legal, publicada el 2 de Septiembre del 2014 por la SB (Superintendencia de Bancos):

LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO, SECCIÓN VII. (Superintendencia de Bancos del Ecuador, 2014).

ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014).

21.1 Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información.

El comité debe estar conformado como mínimo por: el miembro del directorio delegado al comité integral de riesgos, quien lo presidirá, el representante legal de la institución y el funcionario responsable de la seguridad de la información.
El organismo de control puede requerir la creación del comité y de una unidad especializada para la gestión de los sistemas de seguridad de la información en las instituciones del sistema financiero que por su complejidad y volumen de negocio lo requieran, así como en aquellas que no hubieren puesto en práctica de una manera adecuadas las disposiciones de esta sección;

21.2 Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de violación de éstas.

Los procesos, procedimientos y metodologías de seguridad de la información deben ser revisados por el comité de seguridad de la información y en caso de no tener dicho comité, por el comité de administración integral de riesgos; y

21.3 Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas.

ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014).

22.1 Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:

22.1.1 Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;

22.1.2 Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;

22.1.3 Autorizar los cambios funcionales a las aplicaciones; y,

22.1.4 Monitorear el cumplimiento de los controles establecidos;

22.2 Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión de riesgo operativo de la entidad; y, con los controles de seguridad de la información;

22.3 Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;

22.4 Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización;

22.5 Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes;

22.6 Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio;

22.7 Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica;

22.8 Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

22.9 Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;

22.10 Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;

22.11 Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;

22.12 Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;

22.13 Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades

22.14 Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;

22.15 Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información;

22.16 Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución;

22.17 Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información; y,

22.18 Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fin de tomar acciones orientadas a mejorarlo.”

2.4 Categorías Fundamentales

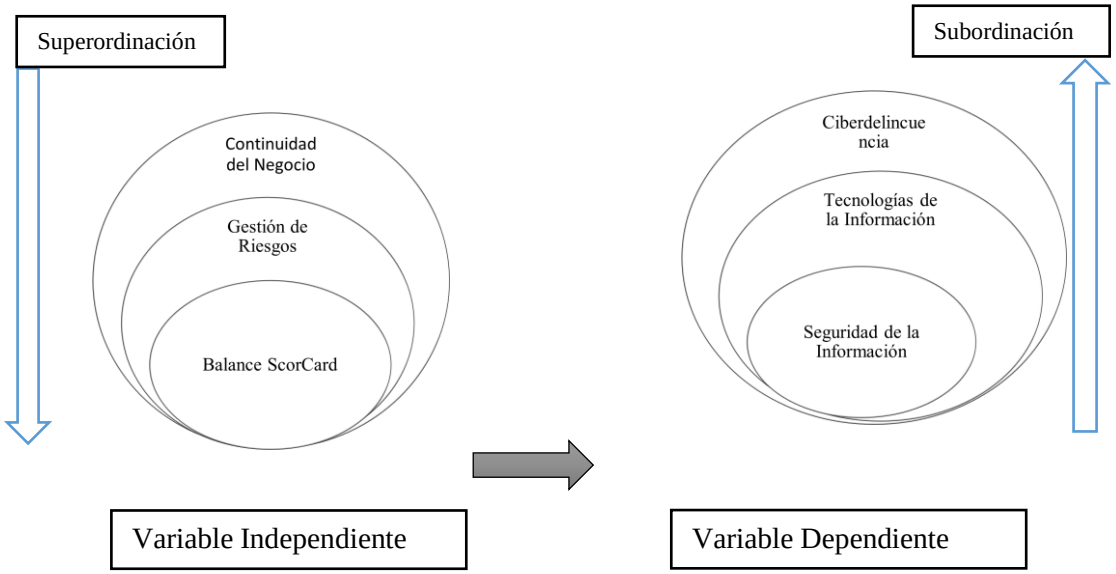


Figura 3. Inclusiones Conceptuales

Elaborado por: Investigador

Figura 4. Inclusiones Conceptuales

Elaborado por: Investigador

2.4.1 Categorías de la Variable Independiente

Continuidad del Negocio

La continuidad del negocio (conocida en inglés como Business Continuity) describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre. La Planificación de la Continuidad del Negocio (BCP) trata de evitar la interrupción de los servicios de misión crítica y restablecer el pleno funcionamiento de la forma más rápida y fácil que sea posible (searchdatacenter, s.f.).

Se establece que todas las instituciones financieras controladas deben de implementar planes de contingencia y continuidad del negocio las mismas que deben de ser capaces de garantizar su capacidad de operar en forma continua y minimizar las pérdidas en caso de interrupción del negocio (searchdatacenter, s.f.).

Estos mecanismos permitirán mantener el nivel de servicio en unos límites predefinidos, establecerán un periodo de recuperación mínimo, recuperarán la situación inicial anterior al incidente, analizarán los resultados y los motivos del incidente, y así evitarán la interrupción de las actividades corporativas (searchdatacenter, s.f.).

Gestión de Riesgos

Proteger la información es uno de los problemas más críticos que debe de enfrentar la empresa ya que no solo basta con la implementación de tecnología como fireware, gateways, antivirus y esperar lo mejor, sino más bien adoptar prácticas que ayuden a identificar, controlar y proteger los activos más importantes, incluida la información, la tecnología de la información y los procesos críticos del negocio (Sullivan, s.f.).

La gestión del riesgo de seguridad de la información permite a una organización evaluar lo que está tratando de proteger, y por qué, como elemento de apoyo a la decisión en la identificación de medidas de seguridad. Una evaluación integral del riesgo de seguridad de la información debería permitir a una organización evaluar sus necesidades y riesgos de seguridad en el contexto de sus necesidades empresariales y organizativas (Sullivan, s.f.).

Por lo tanto según (Sullivan, s.f.), la gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación del riesgo, un método y proceso de gestión del riesgo ayudará a:

- Identificar los activos críticos de información. Un programa de gestión de riesgos puede ampliarse para identificar también a personas críticas, procesos de negocio y tecnología.
- Comprender por qué los activos críticos escogidos son necesarios para las operaciones, la realización de la misión y la continuidad de las operaciones.

Para cumplir con la gestión de riesgos como componente de preparación para la ciberseguridad, una organización debe crear un sólido programa de evaluación y gestión del riesgo de la seguridad de la información. Si ya existe un programa de gestión del riesgo empresarial (ERM), un programa de gestión de riesgos de seguridad de la información puede soportar el proceso de ERM (Sullivan, s.f.).

Balance ScoreCard

El Balanced Scorecard (BSC / Cuadro de Mando Integral) es una herramienta que permite enlazar estrategias y objetivos clave con desempeño y resultados a través de cuatro áreas críticas en cualquier empresa: desempeño financiero, conocimiento del cliente, procesos internos de negocio y aprendizaje y crecimiento.

Kaplan y Norton (pp.38 y 39) explican que se trata de una estructura creada para integrar indicadores derivados de la estrategia. Aunque sigue reteniendo los indicadores financieros de la actuación pasada, el Cuadro de Mando Integral introduce los inductores de la actuación financiera futura. Los inductores, que incluyen los clientes, los procesos y las perspectivas de aprendizaje y crecimiento, derivan de una traducción explícita y rigurosa de la estrategia de la organización en objetivos e indicadores intangibles.

Sin embargo, es algo más que un nuevo sistema de medición. Las empresas innovadoras utilizan el Cuadro de Mando integral como el marco y estructura central y organizativa para sus procesos. Las empresas pueden desarrollar un Cuadro de mando Integral, con unos objetivos bastante limitados: conseguir clarificar, obtener el consenso y centrarse en su estrategia, y luego comunicar esa estrategia a toda la organización. Sin embargo, el verdadero poder del Cuadro de mando Integral aparece cuando se transforma de un sistema de indicadores en un sistema de gestión. A medida que más y más empresas trabajan con el Cuadro de Mando Integral, se dan cuenta de que puede utilizarse para:

- Clarificar la estrategia y conseguir el consenso sobre ella.
- Comunicar la estrategia a toda la organización.
- Alinear los objetivos personales y departamentales con la estrategia.

- Vincular los objetivos estratégicos con los objetivos a largo plazo y los presupuestos anuales.
- Identificar y alinear las iniciativas estratégicas.
- Realizar revisiones estratégicas periódicas y sistemáticas
- Obtener feedback para aprender sobre la estrategia y mejorarla.

El cuadro de mando integral llena el vacío que existe en la mayoría de sistemas de gestión: la falta de un proceso sistemático para poner en práctica la estrategia y obtener feedback sobre ella. Los procesos de gestión alrededor del Cuadro de Mando permiten que la organización se equipare y se centre en la puesta en práctica de la estrategia a largo plazo. Utilizado de este modo, el Cuadro de Mando Integeral se convierte en los cimientos para gestionar las organizaciones de la era de la información.

En la siguiente figura se presentan las cuatro perspectivas del Cuadro de Mando Integral, se puede apreciar que es un sistema que considera todos los procesos estratégicos de la organización:

Figura 5. Perspectivas del Cuadro de Mando Integral

Elaborado por: (gestiopolis, s.f.)

Métricas de usabilidad

Debido a que los atributos de una aplicación son conceptos abstractos, éstos no se pueden medir directamente. Para medirlos se les asocian distintas métricas, por ejemplo, el atributo eficiencia puede ser evaluado mediante la métrica que calcula el tiempo empleado por un usuario en terminar una tarea específica (Enríquez & Casas, 2013).

Una métrica (medida) es un valor numérico o nominal asignado a características o atributos de un objeto computado a partir de un conjunto de datos observables y consistentes con la intuición (Enríquez & Casas, 2013).

A la efectividad se asocian métricas como: Tareas en un tiempo determinado, porcentaje de tareas completadas. Una métrica de la eficiencia es por ejemplo el número de teclas presionadas por tarea o proceso que el usuario ejecuta en sus funciones diarias. Para la satisfacción se consideran métricas como agrada o no agrada, preferencias, etc.

2.4.2 Categorías de la Variable Dependiente

Seguridad de la Información

La Seguridad de la Información consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización (Pmg-Ssi, 2015).

Según (Pmg-Ssi, 2015), determina lo siguiente.

Los objetivos de la seguridad informática:

Los activos de información son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:

- **Información**: es el objeto de mayor valor para la empresa.
- **Equipos**: suelen ser software, hardware y la propia organización.
- **Usuarios**: son las personas que usan la tecnología de la organización.

Salvaguardar la información es una tarea muy difícil de hacerlo, ya que no solo implica implementar sistemas de gestión seguras, sino también mantener al usuario final muy bien capacitado en el proceso y en el negocio, por lo tanto, es una tarea de todos hacerlo.

Ciberdelincuencia

Según (Kaspersky, 2017), en las primeras fases del desarrollo de malware, la mayoría de los troyanos y virus informáticos fueron creados por estudiantes y programadores jóvenes, además de otros programadores con más experiencia algo más mayores. Hoy en día, aún existen cuatro tipos de ciberdelincuentes:

- **Estudiantes cualificados, a los que les gusta presumir**

En muchos casos, los estudiantes (que acaban de aprender a utilizar un lenguaje de programación) desean probar sus habilidades y demostrar su capacidad o su inteligencia. Por suerte, muchos de estos creadores de malware no distribuyen sus obras y, en su lugar, envían virus o gusanos a una compañía antivirus (Kaspersky, 2017).

- **Jóvenes sin experiencia, ayudados por Internet**

Los jóvenes que aún no dominan el arte de la programación también pueden convertirse en ciberdelincuentes para demostrar su valía. En el pasado, esto derivó en virus primitivos. No obstante, ahora existen numerosos sitios web que explican cómo crear y desarrollar virus informáticos, y cómo estos pueden eludir el software antivirus. Por lo tanto, Internet ha hecho mucho más sencillo para los jóvenes inexpertos la creación de sus propios virus (Kaspersky, 2017).

- **Desarrolladores profesionales**

A medida que los desarrolladores de virus jóvenes van madurando, su experiencia puede hacer que sus actividades sean mucho más peligrosas. Los programadores adultos y con talento pueden crear virus informáticos muy "profesionales". Puede tratarse de programas sofisticados que utilicen métodos innovadores para introducirse sin permiso en dominios de sistemas de datos o pueden explotar vulnerabilidades de seguridad de entornos operativos, aprovechar la ingeniería social o utilizar una amplia gama de trucos (Kaspersky, 2017).

- **Investigadores**

Se trata de programadores inteligentes capaces de crear nuevos métodos para infectar ordenadores, ocultar la infección y resistir las acciones de software antivirus. El objetivo del programador es investigar el potencial de "fauna informática". El programador puede optar por no compartir sus creaciones, pero puede promocionar activamente sus ideas a través de numerosos recursos de Internet dedicados a la creación de virus. Estas ideas y "virus de investigación" pueden ser utilizadas por cibecriminales (Kaspersky, 2017).

Tecnologías de la Información

La tecnología de la información (TI, o más conocida como IT por su significado en inglés: information technology) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas. El término es comúnmente utilizado como sinónimo para los computadores, y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos. Múltiples industrias están asociadas con las tecnologías de la información, incluyendo hardware y software de computador, electrónica, semiconductores, internet, equipos de telecomunicación, e-commerce y servicios computacionales (Pmg-Ssi, 2015).

Sistema de Gestión de la Seguridad de la Información

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (ISO 27000, 2012).

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO 27000, 2012).

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización (ISO 27000, 2012).

2.5 Hipótesis:

¿Cómo el balanced scorecard ayudará a la seguridad de la información?

2.6 Señalamiento de variables

Variable Independiente

- Balanced ScoreCard

Variable Dependiente

- Seguridad de la Información

CAPITULO III

3 METODOLOGÍA

3.1 Enfoque

El presente trabajo de investigación tiene un enfoque predominantemente cuantitativo, pues se aplicarán parámetros de medición en las variables.

3.2 Modalidad básica de la investigación

Investigación aplicada

La investigación es aplicada por que busca encontrar mecanismos que permitan tener las mejores prácticas en el tratamiento de la información en las Cooperativas de Ahorro y Crédito.

Descripción del experimento:

Para realizar al Balanced ScoreCard para Seguridad de Información se plantea los siguientes esquemas:

- Inventario de equipos informáticos
- Políticas de Seguridad basadas en el análisis de los equipos informáticos
- Catálogo de Procesos
- Análisis de Riesgos
- Cumplimiento de Políticas
- Plan de Seguridad
- Balanced ScoreCard

Inventario de Equipo Informáticos

En este apartado se recomienda considerar lo siguiente:

- **Código**. - Este se refiere al código de clasificación que representa el activo dentro de la cooperativa, ejemplo EC-2003-047-M01.
- **N° de Activo**. - Este corresponde al número que se le asigna al equipo dentro de su clasificación, ejemplo 286
- **Tipo. -** Corresponde al tipo de activo que se está representando, como por ejemplo servidor, cpu, monitor, switch…, etc.

- **Marca. -** Corresponde a la marca en cuanto a equipos de computación, por ejemplo, DELL, TOSHIBA, HP, CISCO…, etc.
- **Modelo**. - Es el modelo de equipo dependiendo de la marca y el tipo de activo, por ejemplo, POWER EDGE 1750 - 1 INTEL XEON 2.4 G, que corresponde a un servidor de marca DELL.
- **Función. -** Es la función para el que ha sido destinado el activo.
- **Ubicación. -** Se solicita en este punto indicar la agencia (Sucursal), piso y área (Negocios, cajas, contabilidad, …, etc.).
- **Custodio. -** Se indica a quien está asignado el equipo la persona puede ser un jefe de área.
- **Responsable. -** La persona que está usando el activo o a quien se le consta en el registro.
- **Fecha de Registro. -** Fecha en la que ha sido registrado como activo de la empresa.
- **Fecha de Compra. -** En qué fecha ha sido adquirida al proveedor dependiendo del activo requerido.
- **N° de Usuarios. -** Se indica el número de usuarios que ocupan el activo, puede ser un área o una sola persona.

Para quien está a cargo de realizar el análisis de riesgo de los equipos en cuanto a seguridad de información se trata, estas características pueden ser muy importantes, porque a través de estas puede tener una idea más clara del activo que está empleado en los procesos, sea este de importancia alta, mediana o baja.

Políticas de Seguridad

Las políticas deben considerar los procesos, la gestión de los activos, el personal, seguridad operativa, física y ambiental, telecomunicaciones, proveedores, pero sobretodo la gestión de la información que es lo que se va a salvaguardar y para ello se recomienda hacerlo mediante un análisis con la ISO 27001:2013(Véase ANEXO 3), a continuación, se presenta un modelo propuesto a seguir:

TABLA DE CONTENIDO

Tabla 1. Ficha de cambios

VERSION	FECHA DEL CAMBIO	DESCRIPCION DEL CAMBIO

Desarrollado por: Investigador

Tabla 2. Ficha de elaboración del documento

1.	Elaborado por:			
NOMBRE	CARGO	FECHA	VERSIÓN	FIRMA

Desarrollado por: Investigador

Tabla 3. Ficha de revisión

2.	Revisado por:		
NOMBRE	CARGO	FECHA	FIRMA

Desarrollado por: Investigador

Tabla 4. Ficha de Aprobación

3.	Aprobado por:	
NOMBRE	CARGO	FIRMA

Desarrollado por: Investigador

Catálogo de procesos

El catálogo de procesos será facilitado por la institución de acuerdo a su actividad comercial, de no contar se deberá definir los procesos más importantes en conjunto con el departamento de sistemas o la que la represente y deberá de constar del **Código, nombre del proceso y descripción**.

Ejemplo:

Tabla 5. Ficha de presentación de procesos

Código	Nombre del Procesos	Descripción
P.02.01.01	Análisis y Aprobación de Microcrédito	El Microcrédito pasa por varias fases antes de su aprobación, como son: - Análisis de información entregada por el aspirante a crédito - Visita en sitio para verificar su actividad comercial de ser necesario. - Análisis de información recopilada por los analistas en comité de crédito para su aprobación final. - Firma de documentos de préstamo asignado en caso de haber sido aprobado o entrega de documentos en caso de ser rechazado.

Desarrollado por: Investigador

Análisis de Riesgos

La norma ISO 27001:2013 para garantizar que la seguridad de la información sea gestionada correctamente indica que se debe identificar los aspectos relevantes adoptados para garantizar su C-I-D:

Disponibilidad (D). - Cuando el personal requiera la información y no se encuentre disponible, la carencia de este supone la interrupción del servicio, acceso y utilización de la misma.

Confidencialidad (C). - Se lo valora en cuanto la información llega solamente a las personas autorizadas mas no cuando lo requieran en secreto y sin permiso de una autoridad competente de la institución, en muchas ocasiones puede darse fugas y filtraciones.

Integridad (I). - El mantenimiento de la exactitud y completitud de la información y sus métodos de proceso es muy importante. Permite que la información no pueda aparecer manipulada, corrupta o incompleta, esto afecta directamente al correcto desempeño de las funciones de una Organización.

Escala de valores:

Lo más normal es que cada activo reciba una valoración en cada dimensión, este planteamiento puede y debe de ser enriquecido en el caso de dimensiones más complejas, como es el caso de la integridad, en la que la información no puede ser irreal a lo que la institución muestra y estos valores pueden ser propuestos mediante criterios de expertos.

Criterios de Evaluación. - Es importante para realizar la valoración de los activos, determinar criterios de evaluación que permitan obtener un criterio más acertado del riesgo que puede ocasionar un activo mal valorado, es por ello que se plantea la siguiente matriz para el análisis.

Atributos	Criterios y evaluación			
	Bajo	Moderado	Alto	Crítico
	1	2	3	4
Disponibilidad	Ningún otro activo depende de este para entregar servicios a usuarios	Pocos activos dependen de este para entregar servicio a usuarios	Una gran cantidad de activos dependen de este para entregar servicios a usuarios	Todos los activos dependen de este para entregar servicios a usuarios
Confidencialidad	La revelación de los datos que procesa o almacena el activo produce un impacto menor a la entidad	La revelación de los datos que procesa o almacena el activo produce un impacto parcial a la entidad	La revelación de los datos que procesa o almacena el activo produce un impacto significativo a la entidad en términos legales, económicos y/o de reputación e imagen	La revelación de los datos que procesa o almacena el activo impide dar cumplimiento a obligaciones legales y afecta a la reputación de la empresa
Integridad	La afectación a la integridad del activo puede afectar de forma insignificante la entrega de servicios a usuarios	La afectación a la integridad del activo puede afectar en parte la entrega de servicios a usuarios	La afectación a la integridad del activo puede afectar significativamente la entrega de servicios a usuarios	La afectación a la integridad del activo puede afectar totalmente la entrega de servicios a usuarios

Figura 6. Matriz de criterios y evaluación

Desarrollado por: Investigador

Dependiendo de la calificación tendremos la siguiente semaforización:

1	11	21	31	41	51	61
2	12	22	32	42	52	62
3	13	23	33	43	53	63
4	14	24	34	44	54	64
5	15	25	35	45	55	
6	16	26	36	46	56	
7	17	27	37	47	57	
8	18	28	38	48	58	
9	19	29	39	49	59	
10	20	30	40	50	60	

Figura 7. Colores de Semaforización

Elaborado por: Investigador

En donde:

- Del 1 al 23 se marca de color verde y tenemos la siguiente marca, esto significa que no existe riesgo en el activo por lo tanto no es crítico.
- Del 24 al 32 de color naranja y del 33 al 64 se marcará de color rojo esto indica que el riesgo del activo es crítico y merece determinar su nivel de riesgo

El nivel de riesgo se determina básicamente en este modelo, siguiendo la siguiente matriz:

Frecuencia / Probabilidad			
Alta	M	A	A
Media	B	M	A
Baja	B	B	M
Impacto	Bajo	Medio	Alto

Figura 8. Impacto de riesgo

Desarrollado por: Investigador

Según los resultados se analizarán los procedimientos necesarios que permitan que las procesos y equipos esenciales puedan continuar durante y después de un desastre y eso estará a cargo del investigador, sistemas y del departamento de riesgos de la institución o a su vez departamentos que hayan sido nominados.

Cumplimiento de Políticas

Para validar el cumplimiento de las políticas es recomendable basarse en la Norma ISO 15504, que establece una escala de calificación cuyos valores se basan en el porcentaje de logro de los atributos:

1. **NO CUMPLE**, no implementado (0-15%)
2. **PARCIAL**, Parcialmente implementado (16-50%)
3. **ALTO**, Ampliamente implementado (51-85%)
4. **TOTAL**, completamente implementado (86-100%)

Valores que se consideran también en los Criterios de Evaluación para el análisis de riesgo de los activos de información en cuanto a Disponibilidad, Confidencialidad e Integridad.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos), por lo tanto, los dominios que se tomaron para generar las políticas deben de organizarse y valorar sus criterios bajo esta normativa, por ejemplo:

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE		
			PARCIAL	ALTO	TOTAL
11.Gestión de incidentes en la seguridad de la información	11.1. La Cooperativa mantendrá un proceso específico para la Administración de incidentes y problemas, que incluya la definición de responsabilidades para el reporte, registro, clasificación, resolución y revisión de los eventos de seguridad de la información.			X	

Figura 9. Ejemplo políticas

Desarrollado por: Investigador

Dependiendo de la valoración que se le dé al análisis y verificación de las políticas, se le adjunta el Plan de Acción, Responsable y fecha de ejecución siempre y cuando esa valoración no sea **TOTAL.**

Plan de Seguridad

El Plan de Seguridad consiste por un lado valorar las políticas que no cumplieron en su totalidad, por otro lado, del Análisis de Riesgo realizado aquellas que tuvieron una calificación Media o Alta. El objetivo principal del Plan de Seguridad es crear un Plan de Acción mucho más fuerte que el que fue creado en el Análisis de Riesgo, en donde el Riesgo se convierte en Riesgo Inherente y este a su vez se busca convertirlo en un Riesgo Residual.

Balanced ScoreCard

Estará construido a partir del Plan de Seguridad, considerando las fechas propuestas en su análisis, por lo que es importante definir qué tipo de información permitirá dar seguimiento. (Ver la Fase 6. Diseño de Balanced ScoreCard a partir del Plan de Seguridad del Capítulo 6 que es el desarrollo de la propuesta).

Alcance y resultados esperados

Al tratarse de una propuesta que busca garantizar la información en cualquiera de sus fases, los documentos realizados para llegar a construir el Balanced ScoreCard para Seguridad de la Información, son muy relevantes, por que ayudan a identificar los riesgos a los que se encuentran expuestos los activos y a su vez los procesos más importantes. Es por eso que se crea un modelo genérico para el análisis de riesgo y a su vez el Plan de Seguridad, utilizando la NORMA ISO 27001:2013 como lo especifica la Superintendencia de Bancos, artículos expuestos en la Base Legal de este documento (2.3 Fundamentación Legal).

Investigación Bibliográfica

Se ha realizado una exhaustiva investigación bibliográfica apoyada en libros, artículos científicos, trabajos investigativos previos, revistas, artículos y leyes existentes para la elaboración de un Balanced ScoreCard para la Seguridad de la Información basadas en la Norma ISO 27001.

3.3 Nivel o tipo de investigación

Investigación Correlacional

La investigación será correlacional porque se asegura la información basándose en la norma ISO 27001.

3.4 Población y Muestra

Este trabajo se ha desarrollado utilizando una porción de la población total, siendo a su vez personas que directamente se encuentran con la información que se gestiona dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic.

Tabla 6. Población

Población	Número	Porcentaje
Gerente	1	3,23%
Jefaturas(Sistemas, Riesgo, Procesos, Crédito, Negocios, Financiero, Auditoria)	7	22,58%
Analista de Riesgos	1	3,23%
Cajeros/as	5	16,13%
Analistas de Crédito	4	12,90%
Oficiales de Cobranzas	6	19,35%
Asistente de Auditoría	1	3,23%
Oficiales de Campo	6	19,35
Total	31	100,00%

Elaborado por: Investigador

Este trabajo se ha desarrollado utilizando una muestra de 31 personas del total de 58 empleados, no se trabaja con el resto por tratarse de una población bastante amplia y a su vez se encuentra dispersa por varias partes de la Ciudad de Quito en diferentes agencias y también en Portoviejo.

3.5 Operacionalización de Variables

3.5.1 Árbol de Problemas

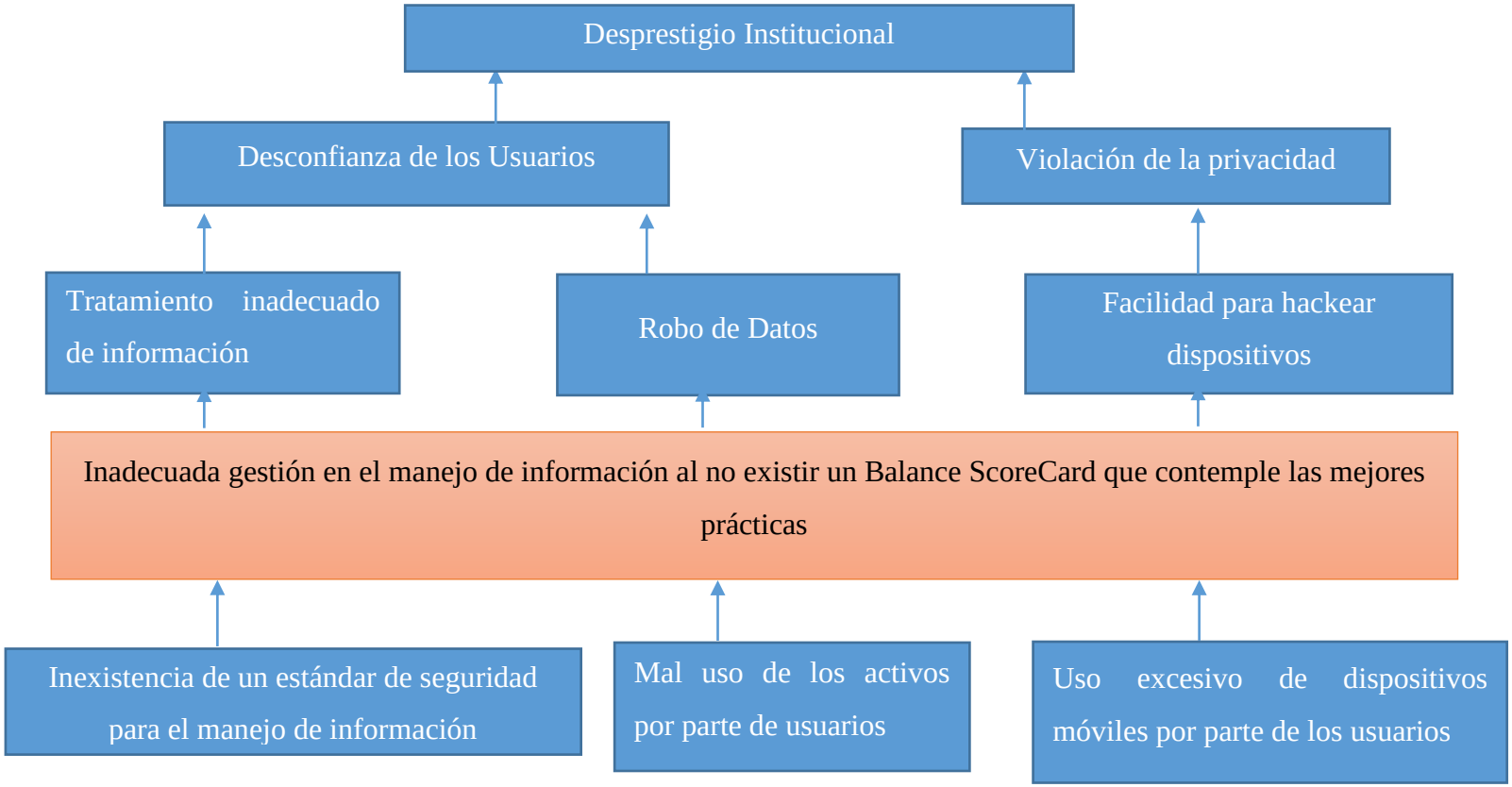


Figura 10. Árbol de Problemas

Elaborado por: Investigador

3.5.2 Variable independiente: Balanced ScoreCard

Tabla 7. Variable Independiente: Balanced ScoreCard

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
"El Balanced Scorecard (BSC / Cuadro de Mando Integral) es una herramienta que permite enlazar estrategias y objetivos clave con desempeño y resultados a través de cuatro áreas críticas en cualquier empresa: desempeño financiero, conocimiento del cliente, procesos internos de negocio y aprendizaje y crecimiento."	- Definir las políticas de seguridad. - Identificar los activos de información que tienen valor para la institución financiera y puedan presentar vulnerabilidades. - Diseñar un Plan de Seguridad que informe sobre el manejo de información y la pérdida de confidencialidad, integridad y disponibilidad para cada activo y que sirva de apoyo para el Balanced ScoreCard.	- Procesos - Inventario de la Institución - Activos en Riesgo	- Se define los procesos más importantes dentro de la Institución. - Se valoran los activos más importantes para los procesos. - Se define los riesgos que los activos pueden tener durante su tratamiento y las mejores políticas que garanticen la seguridad para la información.	- Encuesta - Entrevista, lista de Cotejo - Listas de Cotejo

Elaborado por: Investigador

3.5.3 Variable Dependiente: Seguridad de la Información

Tabla 8. Variable Dependiente: Seguridad de la Información

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Es el conjunto de medidas preventivas y reactivas que las organizaciones las toman al analizar sus sistemas tecnológicos, análisis que permite resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos a través de la aceptación o mitigación de los riesgos.	- Crear Políticas de Seguridad para los activos y procesos de riesgo de la institución financiera	- Registro de incidentes relacionado a los activos y procesos que involucran manejo de información.	- Políticas de seguridad que permitan conservar la confidencialidad, integridad y disponibilidad de la información de la Institución.	- Lista de Cotejo

Elaborado por: Investigador

3.6 Recolección de Información

La técnica a emplearse es la encuesta, necesario utilizar como instrumento el cuestionario a través de preguntas cerradas, lo que ayuda significativamente a la obtención más concreta de la información a obtener.

Tabla 9. Recolección de la Información

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Expertos en riesgos del negocio
¿Sobre qué aspectos?	Gestión de Riesgos, planes de continuidad del negocio, políticas de seguridad
¿Quién, Quiénes?	Investigador: Ing. Morales Roberto
¿Cuándo?	Cuarto trimestre del 2017
¿Dónde?	Cooperativa de Ahorro y Crédito Maquita Cushunchic
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Guía de observación, Cuestionario de interfaz atractiva Cuestionario de satisfacción dirigido a los usuarios
¿Con qué?	Cuestionario
¿En qué situación?	Dentro de la jornada laboral de la institución financiera, con profesionalismo investigativo, confidencialidad y reserva.

Elaborado por: Investigador

3.7 Procesamiento y Análisis

- Revisión crítica de la información recogida; es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente y otras fallas.
- Repetición de la recolección, en ciertos casos individuales para corregir errores de contestación.
- Tabulación o cuadros variables de la hipótesis y objetivos:

- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).
- Estudio estadístico de datos para presentación de resultados.

3.8 Análisis de Resultados

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados con apoyo del marco teórico en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPITULO IV

4 ANÁLISIS E INTERPRETACION DE RESULTADOS

4.1 Análisis e interpretación de los resultados

Los resultados que se presentan a continuación están basados en una encuesta realizada a jefes de área, analistas de crédito, oficiales de cobranzas y cajeros de la Cooperativa Maquita Cushunchic Ltda. La encuesta consta de 21 preguntas y fue aplicada a 31 personas con funciones administrativas y operativas de la institución. (Ver Anexo 1).

Pregunta 1: ¿Recibe mantenimiento periódico el computador asignado para el desarrollo de sus funciones?

Tabla 10. Mantenimiento periódico del computador

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	2	7 %
CASI NUNCA	5	16 %
REGULARMENTE	9	29%
BUENO FRECUENTEMENTE	7	23%
MUY BUENO CASI SIEMPRE	6	19%
EXCELENTE SIEMPRE	2	6%
TOTAL	31	100 %

Elaborado por: Investigador

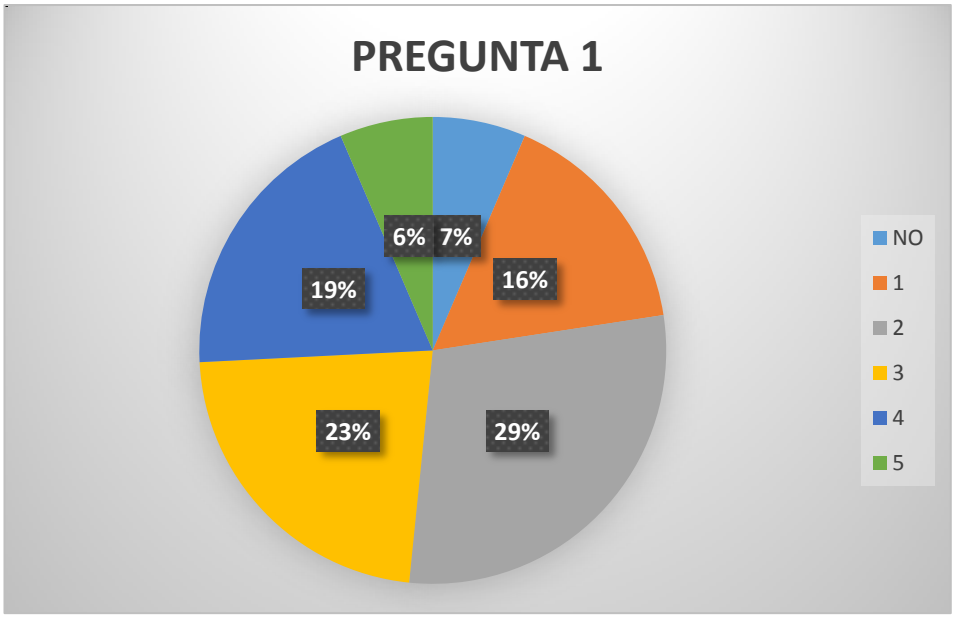


Figura 11. Mantenimiento periódico del computador

Elaborado por: Investigador

Análisis: El 7% de los encuestados, indican que no existe mantenimiento a sus computadores, mientras que el 16% indica que casi nunca lo realizan, el 29% dice que es muy regular, el 23% dice que es bastante frecuente, el 19% indica que casi siempre lo realizan y el 6% indica que siempre recibe mantenimiento a los computadores que maneja.

Interpretación: El departamento de sistemas de la Cooperativa de Ahorro y Crédito Maquita Cushunchic, realiza mantenimientos preventivos de los computadores cuando detecta anomalías en su funcionamiento y lo hace coordinadamente con el usuario para que no se vea afectado por mucho tiempo en las funciones que debe desempeñar.

Pregunta 2: ¿El computador asignado en el desarrollo de sus funciones posee antivirus actualizado?

Tabla 11. Computador posee antivirus

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	1	3%
REGULARMENTE	4	13%
BUENO FRECUENTEMENTE	2	6%
MUY BUENO CASI SIEMPRE	8	26%
EXCELENTE SIEMPRE	16	52%
TOTAL	31	100 %

Elaborado por: Investigador

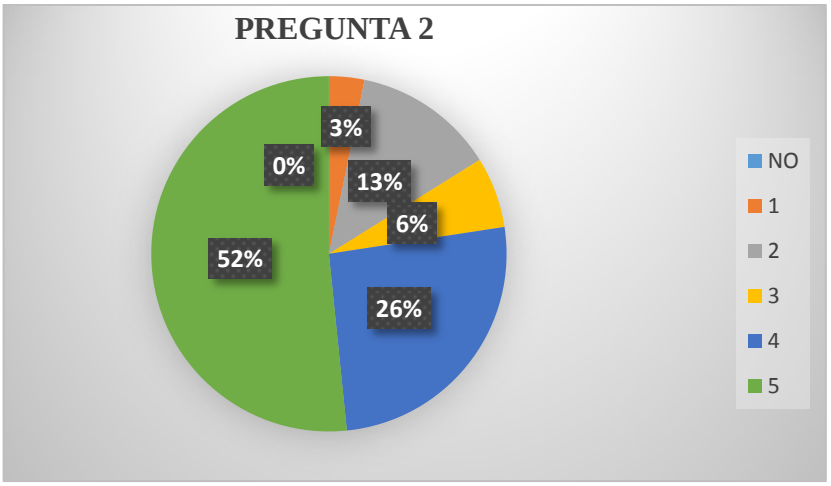


Figura 12. Computador posee antivirus

Elaborado por: Investigador

Análisis: Según estos resultados el 3% de los encuestados indican casi nunca ha tenido antivirus su computador, el 13% que es muy regular el antivirus, el 6% que frecuentemente, el 26% indica que casi siempre ha estado protegido su computador y el 52% afirma que siempre ha tenido antivirus en su computador.

Interpretación: El departamento de sistemas de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., tiene instalado y con actualización automática el Antivirus ESET32 tanto en computadores como en servidores, con el fin de salvaguardar la información que en las estaciones de trabajo se generan a diario y no ser víctimas de antivirus o delincuentes informáticos.

Pregunta 3: ¿Su equipo cuenta con las seguridades para restringir el acceso a personal no autorizado?

Tabla 12. Seguridad para restricción de acceso a personal no autorizado

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	2	7%
CASI NUNCA	1	3%
REGULARMENTE	3	10%
BUENO FRECUENTEMENTE	5	16%
MUY BUENO CASI SIEMPRE	10	32%
EXCELENTE SIEMPRE	10	32%
TOTAL	31	100 %

Elaborado por: Investigador

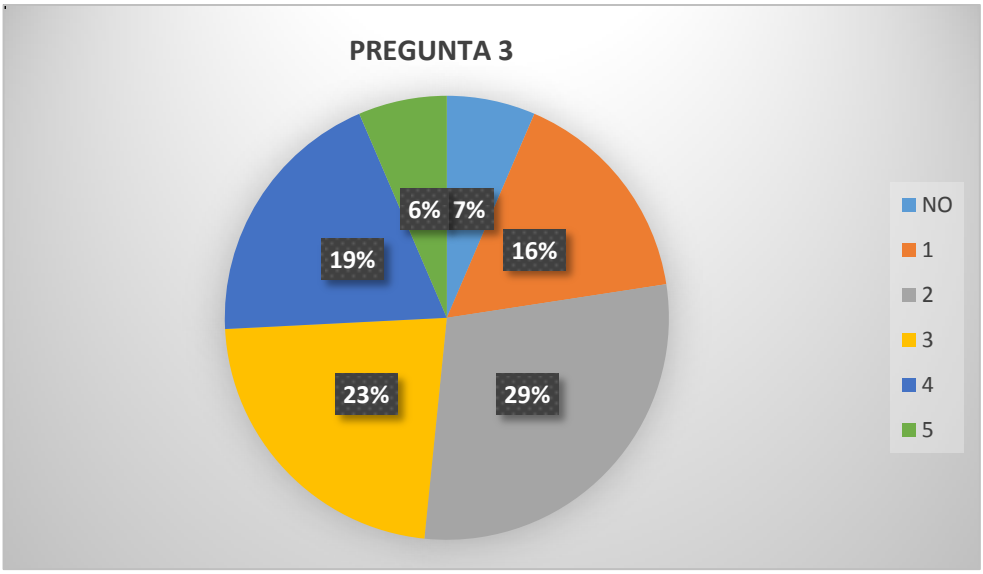


Figura 13. Seguridad para restricción de acceso a personal no autorizado

Elaborado por: Investigador

Análisis: Según la encuesta el 7% indica que no existen restricciones en sus áreas para el acceso de personal no autorizado, por otra parte el 16% indica que casi nunca ha existido, el otro 29% indica que regularmente las instalaciones cuentan con restricción, el 23% de los encuestados dice que es si frecuente, el 19% indica que casi siempre han tenido esta restricción y tan solo el 6% indica que siempre han tenido restricción y esto ocurre generalmente en el área de cajas.

Interpretación: Dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., existen algunas áreas con restricción como es el área de cajas de cada agencia y el edificio Matriz no permitiendo el acceso libre a áreas como por ejemplo UAC (Unidad de Análisis de Crédito), Riesgos, Sistemas, etc, pero si al área de NEGOCIOS.

Pregunta 4: ¿Conoce si dentro de la institución existen políticas, normativas o Sistema de Gestión de Seguridad de la Información?

Tabla 13. Existen políticas, normativas o Sistema de Gestión de Seguridad de la Información dentro de la Cooperativa

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	4	13%
BUENO FRECUENTEMENTE	2	6%
MUY BUENO CASI SIEMPRE	9	29%
EXCELENTE SIEMPRE	16	52%
TOTAL	31	100 %

Elaborado por: Investigador

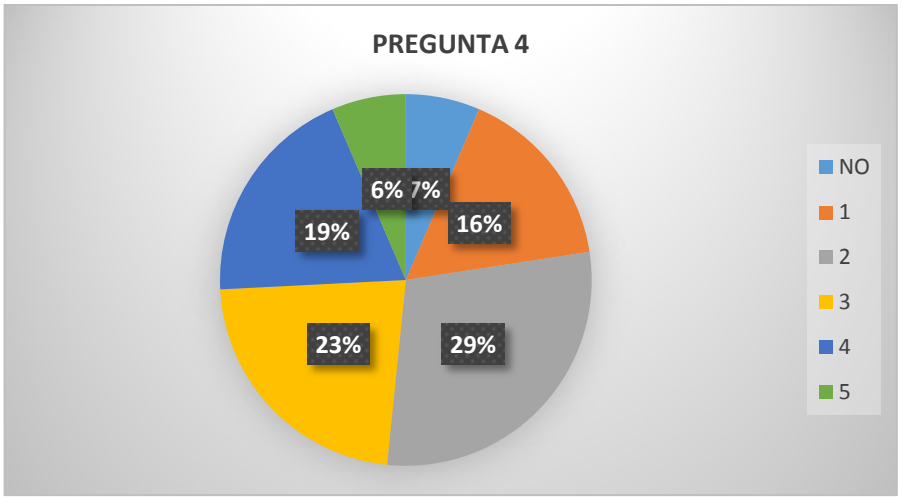


Figura 14. Existen políticas, normativas o Sistema de Gestión de Seguridad de la Información dentro de la Cooperativa

Elaborado por: Investigador

Análisis: En la encuesta realizada se puede validar que el 7% indica no conocer o que no existen ningún tipo de política, normativas o Sistemas de Gestión de Seguridad de Información dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., sin embargo el 6% indica que casi nunca ha existido, el otro 16% indica que eso es muy regular, el 29% dice que es algo regular que exista, mientras que el 23% indica que frecuentemente si ha existido, el 19% que casi siempre ha encontrado con algo de eso, y el 6% indica que siempre ha tenido que responder a este tipo de seguridades o políticas basadas en seguridad de información.

Interpretación: La Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., cuenta con políticas en cuanto a ciertos procesos, pero enfocadas a seguridad de información, no existe política alguna, por lo que se la encuesta es parte de ella.

Pregunta 5: ¿Considera necesario que la institución desarrolle e implante una normativa de Gestión de Seguridad de la información?

Tabla 14. La institución desarrolle e implante una normativa de Gestión de Seguridad de la información

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	2	6.5%
BUENO FRECUENTEMENTE	2	6.5%
MUY BUENO CASI SIEMPRE	13	42%
EXCELENTE SIEMPRE	14	45%
TOTAL	31	100 %

Elaborado por: Investigador

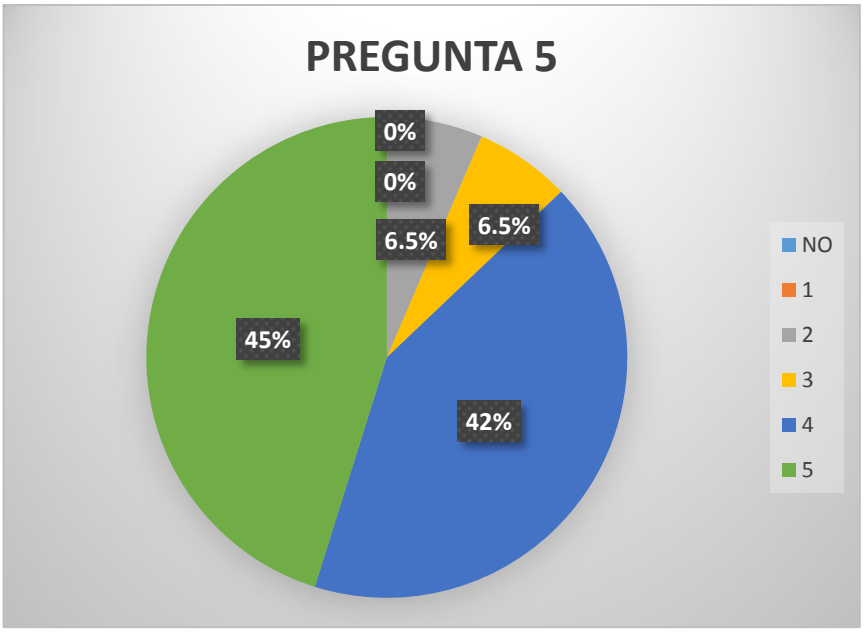


Figura 15. La institución desarrolle e implante una normativa de Gestión de Seguridad de la información

Elaborado por: Investigador

Análisis: El 6.5% de los encuestados indica que es regular y a su vez bueno implementar una normativa de Gestión de Seguridad de Información, el 42% dice que es muy buena la idea de hacerlo y el 45% indica que es excelente la idea de implementación.

Interpretación: Dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., no existe una normativa de gestión de seguridad de Información, por ende, tiende a generar errores en la gestión de esta, creando malestar en quienes trabajan para las fases siguientes del requerimiento solicitado por el cliente.

Pregunta 6: ¿La institución capacita al personal en temas de seguridad de la información?

Tabla 15. Capacitación a personal en temas de seguridad de información

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	2	7%
REGULARMENTE	5	16%
BUENO FRECUENTEMENTE	9	29%
MUY BUENO CASI SIEMPRE	6	19%
EXCELENTE SIEMPRE	9	29%
TOTAL	31	100 %

Elaborado por: Investigador

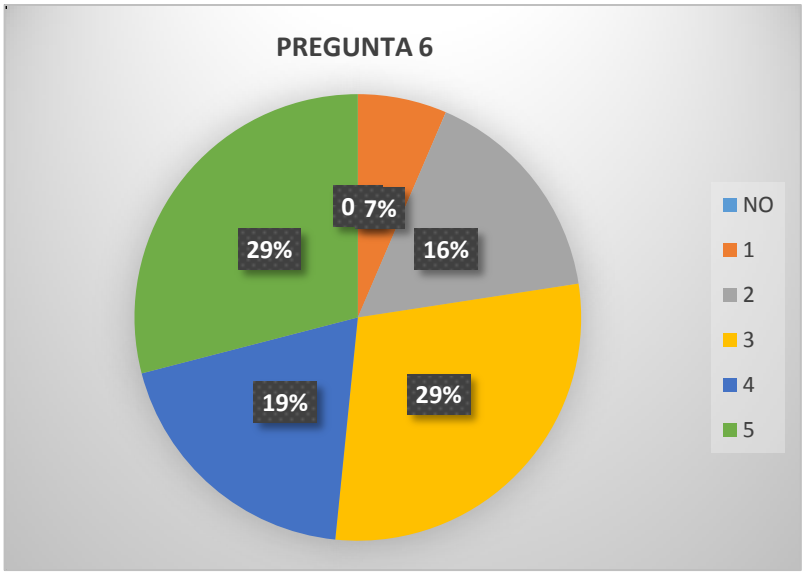


Figura 16. Capacitación a personal en temas de seguridad de información

Elaborado por: Investigador

Análisis: Según la encuesta realizada el 7% del personal indica que casi nunca se hace capacitación en estos temas, mientras que el 16% indica que es bastante regular, el 29% indica que es muy frecuente, el 19% indica que casi siempre ha sido capacitado, sin embargo, el 29% siempre ha recibido capacitación con respecto a este tema.

Interpretación: Dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., si bien es cierto no existe alguna herramienta de Gestión de Seguridad de Información, pero sin embargo la Gerencia y el Área de Riesgos se han preocupado por brindar charlas con respecto a este tema, brindando a su vez él apoyo para poder realizar el proyecto de tesis dentro de la misma.

Pregunta 7: ¿La institución capacita al personal en temas de riesgo operativo?

Tabla 16. Capacitación al personal en temas de riesgo operativo

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	1	3%
REGULARMENTE	4	13%
BUENO FRECUENTEMENTE	7	23%
MUY BUENO CASI SIEMPRE	8	26%
EXCELENTE SIEMPRE	11	35%
TOTAL	31	100 %

Elaborado por: Investigador

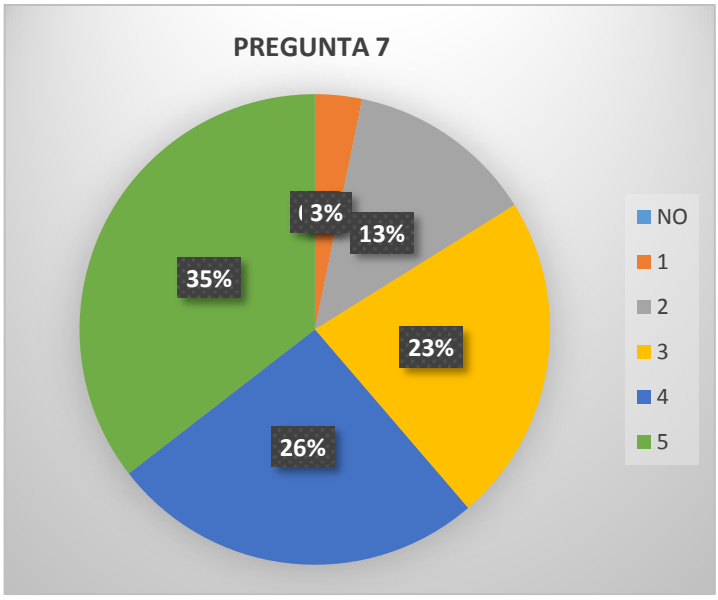


Figura 17. Capacitación al personal en temas de riesgo operativo

Elaborado por: Investigador

Análisis: Según la encuesta se puede validar que el 3% indica que casi nunca ha sido capacitado, el 13% indica que es muy regular la capacitación que recibe, sin embargo, el 23% indica que es muy frecuente la capacitación, el 26% indica que casi siempre ha recibido capacitación, y el 35% dice haber recibido capacitación sobre riesgo operativo siempre.

Interpretación: La Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., cuenta con un departamento encargado de contrarrestar el riesgo operativo y de estar muy al pendiente de cualquier incidente que ocurra y a su vez validar que se haya mitigado el incidente, es el área encargada de impartir charlas dentro de la cooperativa acerca de estos temas.

Pregunta 8: ¿Cuándo ocurre un evento relacionado con riesgo operativo sabe a quién reportarlo?

Tabla 17. Eventos relacionados con riesgo operativo

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	1	3%
BUENO FRECUENTEMENTE	3	10%
MUY BUENO CASI SIEMPRE	8	26%
EXCELENTE SIEMPRE	19	61%
TOTAL	31	100 %

Elaborado por: Investigador

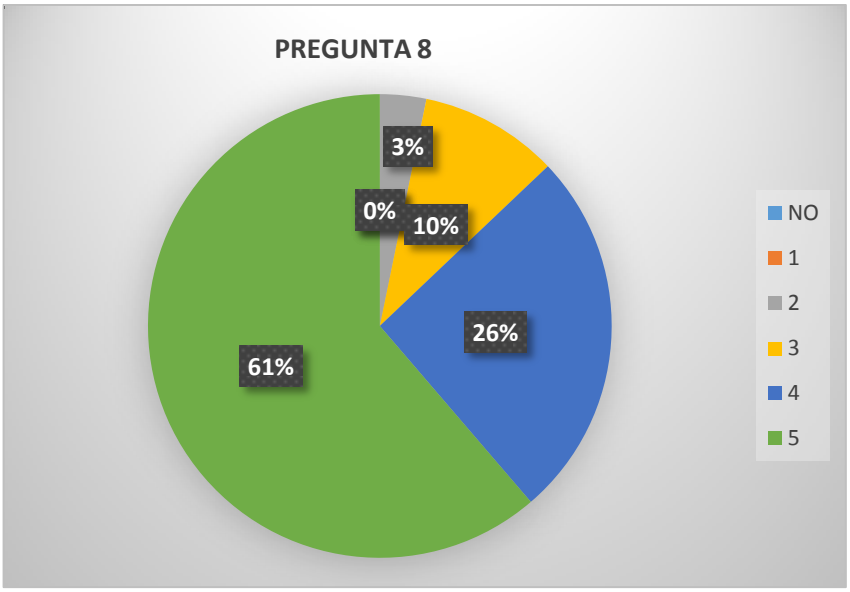


Figura 18. Eventos relacionados con riesgo operativo

Elaborado por: Investigador

Análisis: En la encuesta realizada se puede evidenciar que el 3% indica que no conoce con exactitud a quien reportar un riesgo operativo detectado, el 10% regularmente sabe a quién, mientras que el 26% casi siempre sabe a quién hacerlo y el 61% tiene claramente identificado a quien reportar si ocurre un incidente dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda.

Interpretación: Dentro de la Cooperativa de Ahorro y Crédito existe un departamento de Riesgo Operativo y es a donde se debe reportar cada uno de los incidentes, siendo que estos pueden afectar directa o indirectamente a los procesos críticos de la misma, a su vez está pendiente de todas las áreas y que dentro de ellas no ocurra ningún incidente que no haya sido reportado.

Pregunta 9: ¿Existe alguna restricción para navegar en internet?

Tabla 18. Restricciones para navegar en internet

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	2	6%
CASI NUNCA	2	6%
REGULARMENTE	0	0%
BUENO FRECUENTEMENTE	2	6%
MUY BUENO CASI SIEMPRE	8	27%
EXCELENTE SIEMPRE	17	55%
TOTAL	31	100 %

Elaborado por: Investigador

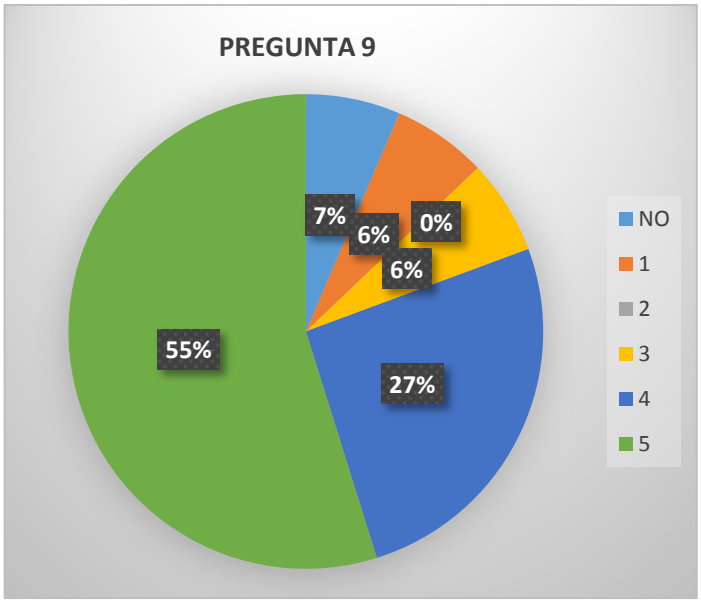


Figura 19. Restricciones para navegar en internet

Elaborado por: Investigador

Análisis: Según los encuestados el 6% indica que no tiene ninguna restricción para navegar en el internet, mientras que el otro 6% indica que casi nunca aplica esa restricción, el otro 6% que es muy frecuente, mientras que el 27% indica que casi siempre tiene restringido el acceso a varias páginas y el 55% tiene restricción a páginas web que no sean netamente de su uso para cumplir las funciones asignadas a su cargo.

Interpretación: En la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., existe una herramienta que controla el acceso a páginas de internet ya sea de manera individual como grupal y esta herramienta se llama FortiGate en su versión 6.0 y es administrada por el personal de Sistemas.

Pregunta 10: ¿Conoce de alguna restricción sobre el uso del correo electrónico?

Tabla 19. Restricción sobre el uso del correo electrónico

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	9	29%
CASI NUNCA	3	10%
REGULARMENTE	1	3%
BUENO FRECUENTEMENTE	6	20%
MUY BUENO CASI SIEMPRE	6	19%
EXCELENTE SIEMPRE	6	19%
TOTAL	31	100 %

Elaborado por: Investigador

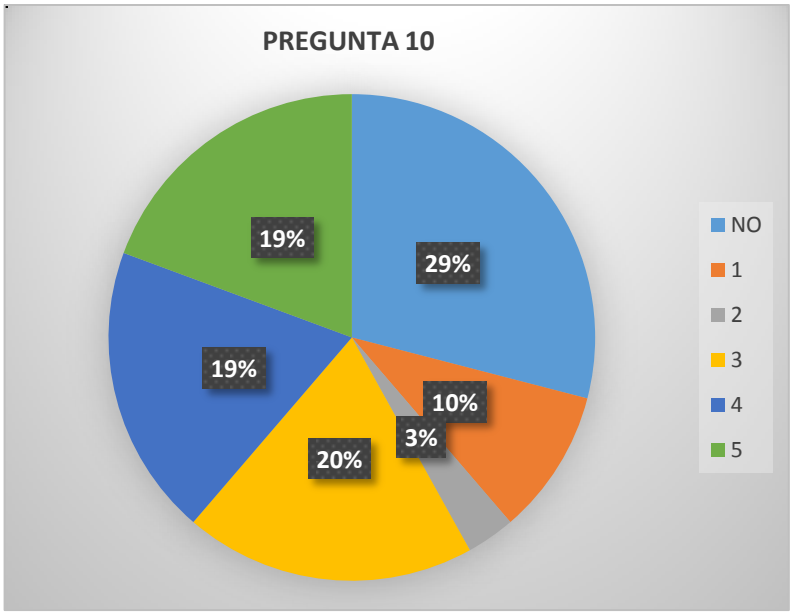


Figura 20. Restricción sobre el uso del correo electrónico

Elaborado por: Investigador

Análisis: Según la encuesta realizada al personal de la Maquita Cushunshic, se puede evidenciar que el 29% desconoce de la existencia de una herramienta de control de correos electrónicos, 10% casi nunca ha sabido de su existencia, el 3% regularmente ha sabido algo, el 20% frecuentemente ha escuchado o sabido de la existencia de esta herramienta, el 19% casi siempre trabaja bajo esta herramienta y el 19% final si sabe de la existencia de una herramienta que le permite tener un control de los correos maliciosos y que no tengan nada que ver con la información que necesita validar.

Interpretación: La Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., cuenta con dos herramientas que validan los correos maliciosos como es el FortiGate y el ESET32, herramientas que se encargar de gestionar la información que ingresa con los correos electrónicos y de ser necesario los bloquea automáticamente.

Pregunta 11: ¿Existe alguna política para el cambio regular de las contraseñas?

Tabla 20. Política para el cambio regular de las contraseñas

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	8	26%
CASI NUNCA	4	13%
REGULARMENTE	1	3%
BUENO FRECUENTEMENTE	2	6%
MUY BUENO CASI SIEMPRE	7	23%
EXCELENTE SIEMPRE	9	29%
TOTAL	31	100 %

Elaborado por: Investigador

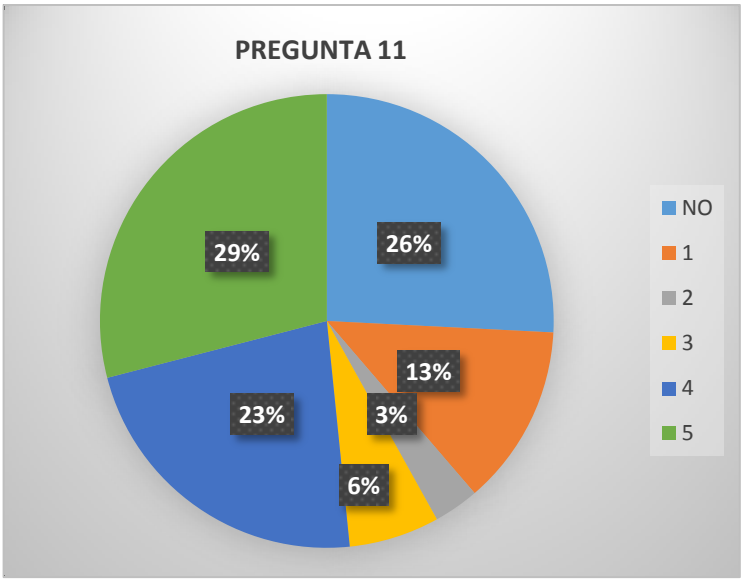


Figura 21. Política para el cambio regular de las contraseñas

Elaborado por: Investigador

Análisis: En la encuesta realizada al personal de la Cooperativa Maquita Cushunchic Ltda., se puede evidenciar que el 26% indica que no existe una política de cambio regular de contraseña, el 13% casi nunca ha tenido dicho control, el 3% regularmente cambia la contraseña de sus equipos y aplicaciones, el 6% frecuentemente cambia su contraseña, el 23% casi siempre hace el cambio de contraseñas en sus equipos y el 29% indica que siempre las realiza.

Interpretación: Dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., solo ciertas aplicaciones contienen políticas de gestión de contraseñas como es el Active Directory, las demás no cumplen con esta política y es el área de sistemas quien se encarga de manera manual gestionarla en el resto.

Pregunta 12: ¿Firmó usted un acuerdo de confidencialidad y de buen uso de sus claves de acceso?

Tabla 21. Firma de un acuerdo de confidencialidad y de buen uso de sus claves de acceso

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	1	3%
REGULARMENTE	3	10%
BUENO FRECUENTEMENTE	1	3%
MUY BUENO CASI SIEMPRE	4	13%
EXCELENTE SIEMPRE	22	71%
TOTAL	31	100 %

Elaborado por: Investigador

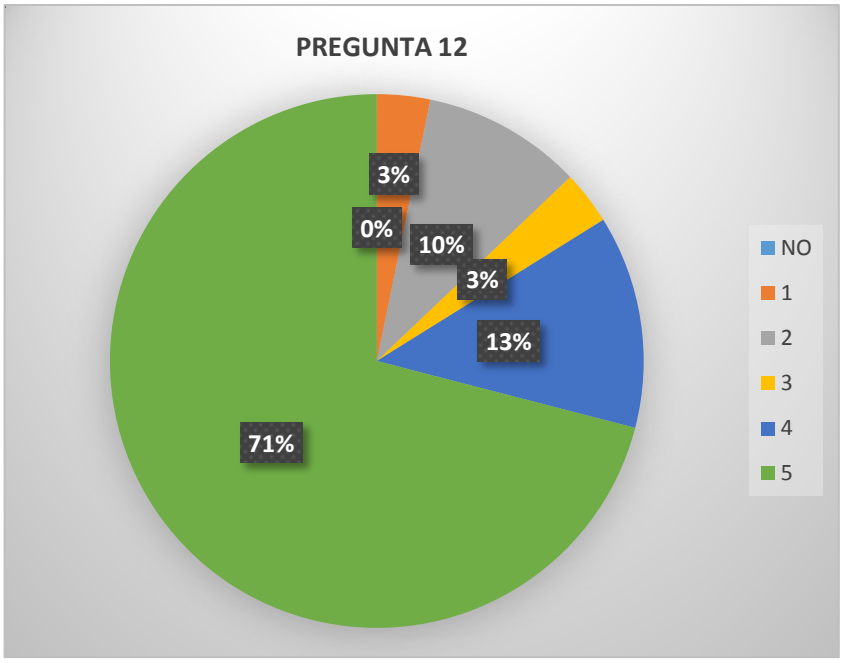


Figura 22. Firma de un acuerdo de confidencialidad y de buen uso de sus claves de acceso

Elaborado por: Investigador

Análisis: Según la encuesta realizada se puede validar que el 3% casi nunca ha firmado este tipo de acuerdos de confidencialidad, el 10% sin embargo lo ha hecho, el 3% frecuentemente, el 13% casi siempre firma un documento de esta naturaleza y el 71% si ha firmado este tipo de documentos.

Interpretación: En la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., es importante que las personas que ingresan a prestar sus servicios ya sea como empleados o proveedores, mantengan la privacidad de la información que maneja ya que por ser una entidad financiera, requiere de mucha privacidad con respecto a su información que es muy sensible.

Pregunta 13: ¿Ha detectado problemas en la integridad o exactitud de la información del core financiero?

Tabla 22. Problemas en la integridad o exactitud de la información del core financiero

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	10	32%
CASI NUNCA	6	19%
REGULARMENTE	2	7%
BUENO FRECUENTEMENTE	6	19%
MUY BUENO CASI SIEMPRE	4	13%
EXCELENTE SIEMPRE	3	10%
TOTAL	31	100 %

Elaborado por: Investigador

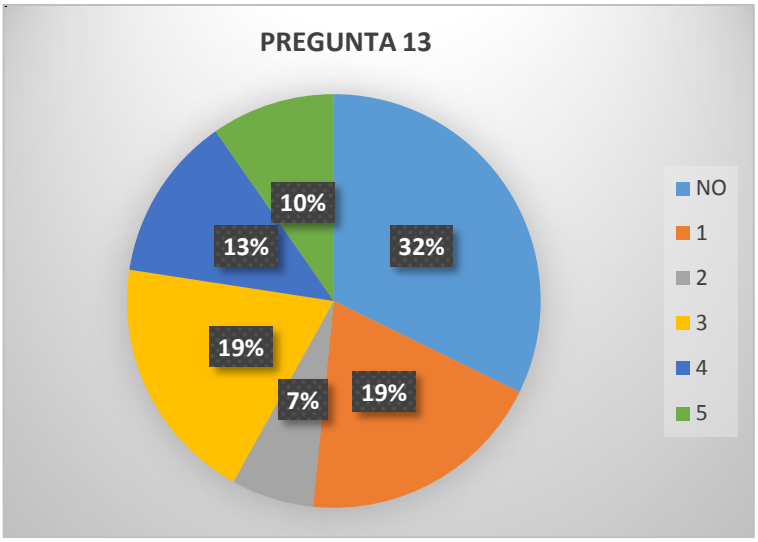


Figura 23. Problemas en la integridad o exactitud de la información del core financiero

Elaborado por: Investigador

Análisis: En la encuesta realizada la problemática que existe en cuanto a integridad e inexactitud de la información es la siguiente, el 32% de los encuestados no ha evidenciado tal situación, el 19% indica que casi nunca sucede eso, el 7% regularmente sucede, el 19% indica que frecuentemente sucede tal situación, el 13% indica que casi siempre encuentra fallas en la información que maneja y el 10% siempre encuentra fallas de este sentido en la información.

Interpretación: En la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., el core financiero es Cobis de la empresa CobisCorp, que es la aplicación que maneja toda la información de la cooperativa tanto de clientes como de transacciones y créditos de los mismos, sin embargo casi a menudo existen diferencias en la información, siendo un riesgo importante, ya que esos errores que ocasiona el sistema se ve reflejado en el trabajo que a diario cumple cada empleado, siendo el área de auditoría interna, contabilidad y operaciones quien se encarga de validar a diario los descuadres y reportarlo al resto de áreas para su corrección.

Pregunta 14: ¿La información que usted maneja para el desempeño de sus funciones se respalda periódicamente?

Tabla 23. Información que se maneja para el desempeño de las funciones se respalda periódicamente

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	1	3%
CASI NUNCA	0	0%
REGULARMENTE	5	16%
BUENO FRECUENTEMENTE	4	13%
MUY BUENO CASI SIEMPRE	9	29%
EXCELENTE SIEMPRE	12	39%
TOTAL	31	100 %

Elaborado por: Investigador

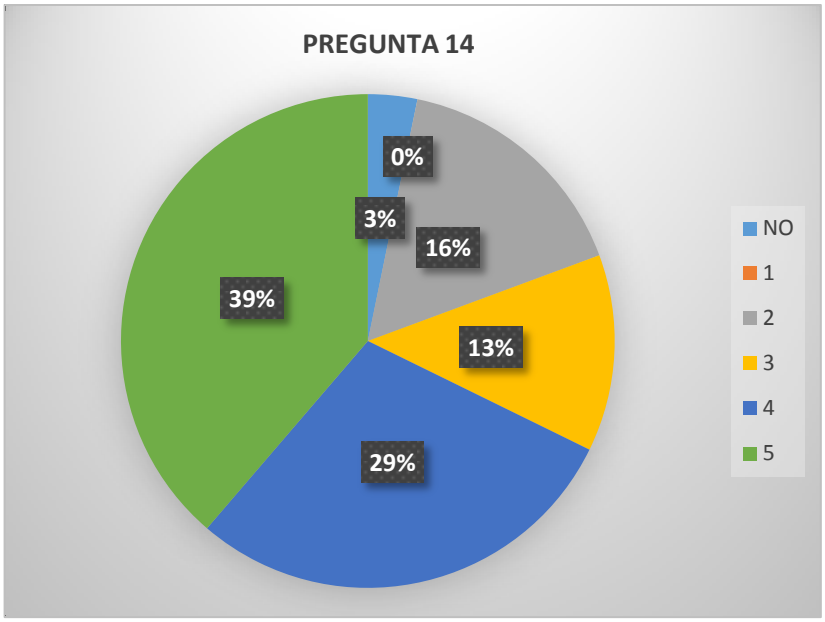


Figura 24. Información que se maneja para el desempeño de las funciones se respalda periódicamente

Elaborado por: Investigador

Análisis: Según la encuesta realizada al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., indican lo siguiente con respecto al respaldo de información, el 3% nunca ha respaldado su información, el 16% regularmente ha respaldado la información, el 13% frecuentemente lo hace, el 29% casi siempre realiza tal acción, el 39% siempre respalda la información.

Interpretación: En la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., se trabaja con Cloud Backup, servicio de respaldo que sirve de apoyo para salvaguardar información más sensible y se lo hace mediante un agente en usuarios con tareas más críticas, se considera antes de ser instalado, el área, procesos e información más importante a respaldar.

Pregunta 15: ¿El acceso que usted requiere a los datos para el desempeño de sus funciones está siempre disponible?

Tabla 24. Acceso a datos para el desempeño de sus funciones está siempre disponible

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	4	13%
BUENO FRECUENTEMENTE	11	36%
MUY BUENO CASI SIEMPRE	10	32%
EXCELENTE SIEMPRE	6	19%
TOTAL	31	100 %

Elaborado por: Investigador

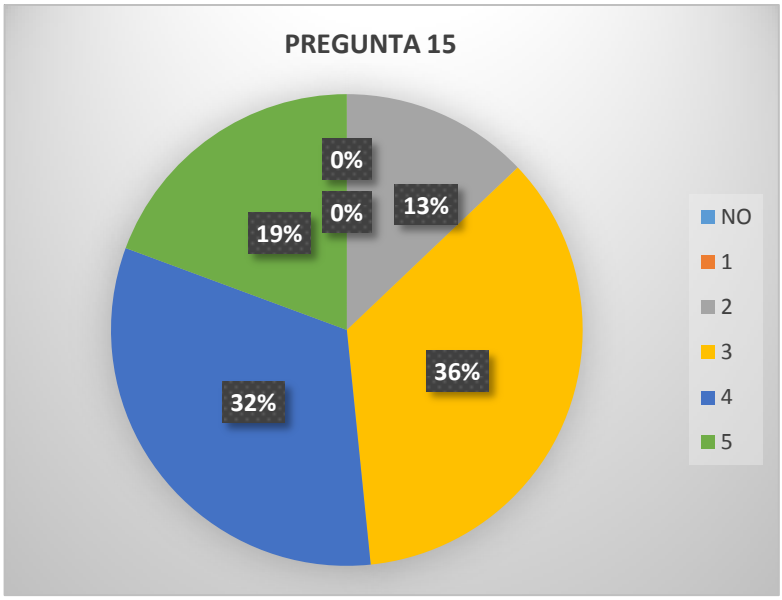


Figura 25. Acceso a datos para el desempeño de sus funciones está siempre disponible

Elaborado por: Investigador

Análisis: Según la encuesta realizada al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunchic, se ha validado lo siguiente, el 13% indica que regularmente no tiene el acceso a la información, el 36% indica que frecuentemente pierde acceso, mientras que el 32% indica que casi siempre le sucede tal situación y el 19% indica que siempre tiene problemas con el acceso a la información que maneja.

Interpretación: El acceso a los datos muchas de las veces están claramente disminuida por el ancho de banda que se maneja tanto para la agencia matriz, como para las demás agencias, es por ello que se ve afectada la consulta de información que se lo hace en el sistema financiero Cobis y es el área de sistemas la encargada de brindar el soporte necesario para que eso no suceda.

Pregunta 16: ¿El core financiero le permite identificar quién ha realizado cambios en la información?

Tabla 25. El core financiero le permite identificar quién ha realizado cambios en la información

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	4	13%
CASI NUNCA	2	6%
REGULARMENTE	0	0%
BUENO FRECUENTEMENTE	5	16%
MUY BUENO CASI SIEMPRE	11	36%
EXCELENTE SIEMPRE	9	29%
TOTAL	31	100 %

Elaborado por: Investigador

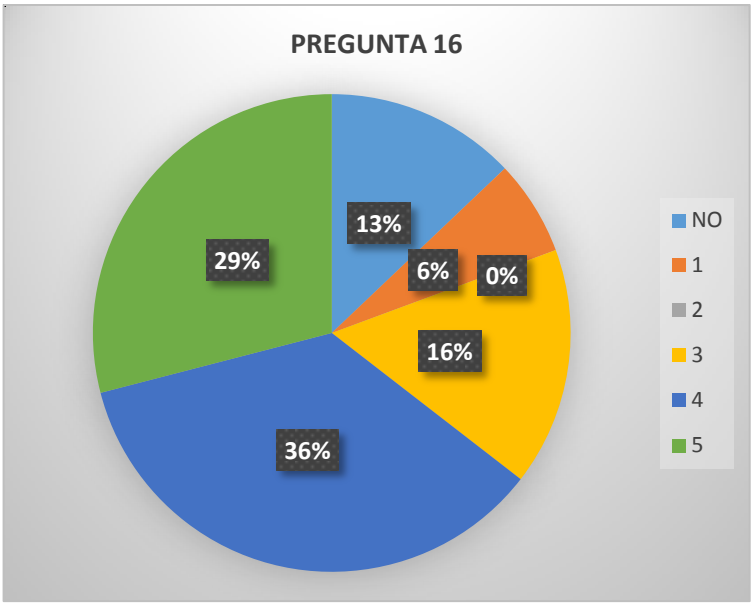


Figura 26. El core financiero le permite identificar quién ha realizado cambios en la información

Elaborado por: Investigador

Análisis: Según la encuesta realizada al personal de la Coioperativa de ahorro y Crédito Maquita Cushunchic Ltda., indica lo siguiente, el 13% no puede visualizar quien ha sido el usuario que ha manipulado la información, el 16% en cambio casi nunca lo visualiza, el 16% frecuentemente valida quien modifico tal información, el 36% casi siempre lo visualiza y el 29% siempre encuentra o valida quien fue el último usuario en manipular dicha información.

Interpretación: Es el sistema financiero o core financiero Cobis que se maneja dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltad., que se encarga de visualizar quien fue el último usuario que modificó o manipuló tal información.

Pregunta 17: ¿Se conoce en qué momento se cambió la información?

Tabla 26. Cambios en la información

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	1	3%
CASI NUNCA	4	13%
REGULARMENTE	3	10%
BUENO FRECUENTEMENTE	5	16%
MUY BUENO CASI SIEMPRE	10	32%
EXCELENTE SIEMPRE	8	26%
TOTAL	31	100 %

Elaborado por: Investigador

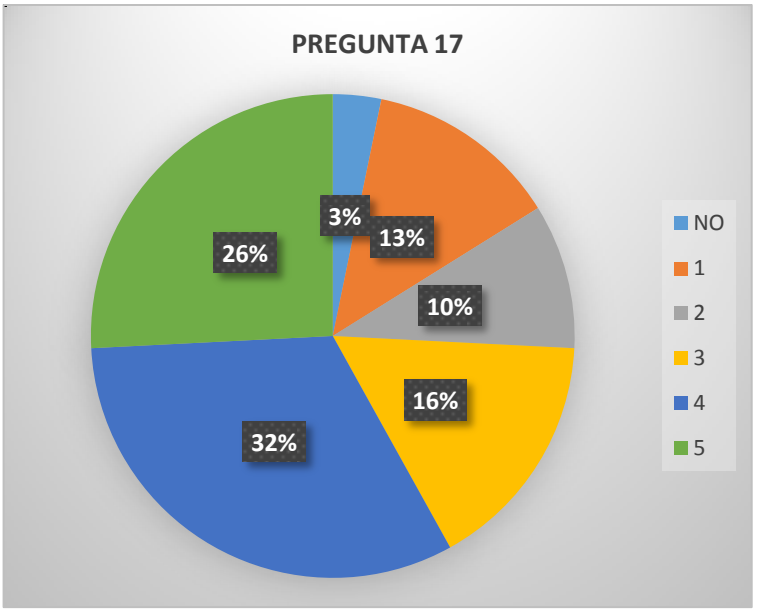


Figura 27. Cambios en la información

Elaborado por: Investigador

Análisis: Según la encuesta realizada, se indica que el 3% no puede ver en qué fecha y hora se modificó tal registro, el 13% casi nunca ha podido validar tal acción, el 10% regularmente lo puede ver o en algunos formularios, el 16% frecuentemente lo puede validar, el 32% casi siempre y el 26% siempre visualiza en qué fecha y hora se modificó tal registro.

Interpretación: El sistema financiero Cobis, brinda la posibilidad de visualizar en qué fecha y hora se manipuló un registro, permitiendo mantener un control sobre la información ingresada de los clientes.

Pregunta 18: ¿Se restringe el acceso de personal a opciones críticas del core financiero, donde se maneja transacciones sensibles de la Cooperativa?

Tabla 27. Restricción de acceso al personal a opciones críticas del core financiero

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	3	3%
CASI NUNCA	1	3%
REGULARMENTE	1	3%
BUENO FRECUENTEMENTE	1	3%
MUY BUENO CASI SIEMPRE	13	42%
EXCELENTE SIEMPRE	12	9%
TOTAL	31	100 %

Elaborado por: Investigador

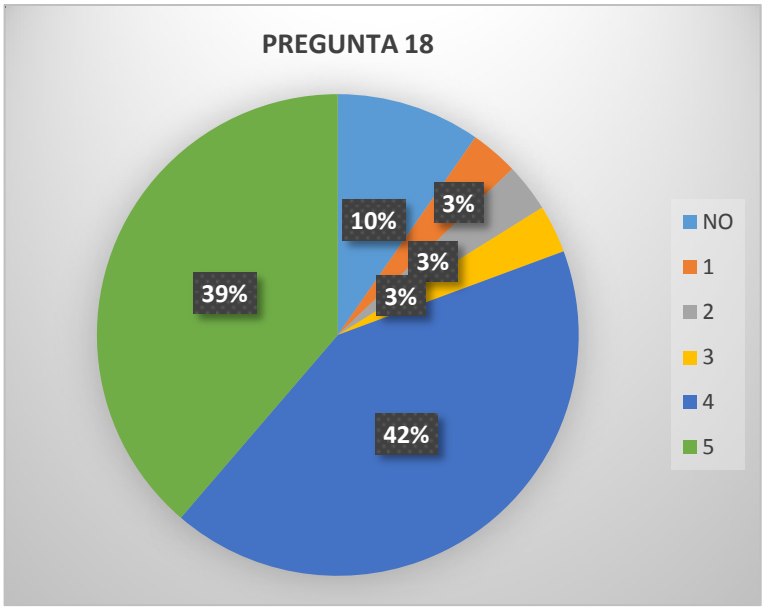


Figura 28. Restricción de acceso al personal a opciones críticas del core financiero

Elaborado por: Investigador

Análisis: Según la encuesta realizada el 10% de los encuestados, indican no tener restricción al sistema financiero, mientras que el 3% indica tener ciertas limitaciones, el 3% siguiente indica que regularmente se les restringe el acceso, el otro 3% indica que es frecuente la restricción, al 42% casi siempre lo limitan y al 39% siempre se le restringe el acceso al mismo.

Interpretación: El core financiero Cobis usado en la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., permite configurar el acceso personalizado a los usuarios mediante un usuario Administrador, por lo que es una gran ventaja al momento de crear funciones para cada uno de ellos.

Pregunta 19: ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?

Tabla 28. Sistemas de seguridad que impidan el acceso a lugares restringidos

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	1	3%
BUENO FRECUENTEMENTE	4	13%
MUY BUENO CASI SIEMPRE	12	39%
EXCELENTE SIEMPRE	14	45%
TOTAL	31	100 %

Elaborado por: Investigador

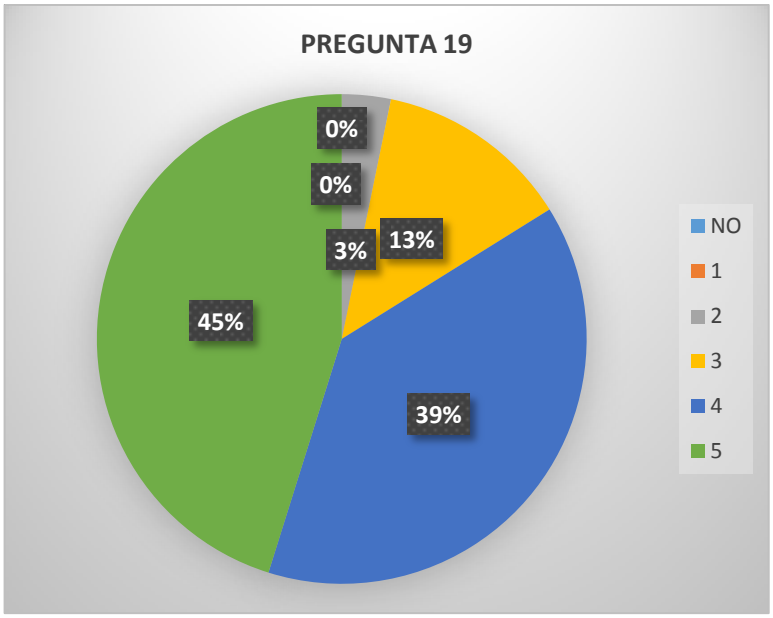


Figura 29. Sistemas de seguridad que impidan el acceso a lugares restringidos

Elaborado por: Investigador

Análisis: Según la encuesta realizada al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., el 3% indica que es muy regular la seguridad que se le brinda dentro de la Maquita Cushunchic, mientras que el 13% indica que es muy frecuente la seguridad, el 39 indica que casi siempre tiene seguridad en su área y el 45% indica tener siempre disponible la seguridad en los lugares críticos o de responsabilidad.

Interpretación: La Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., tiene un contrato con la empresa de seguridad RAVSEG quienes son los encargados de brindar la seguridad que corresponde tanto al edificio matriz, como a las agencias, con personas capacitadas para tal trabajo.

Pregunta 20: ¿Se cuenta con sistemas de alarma como detectores de humo, incendio?

Tabla 29. Sistemas de alarma como detectores de humo, incendio

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	0	0%
BUENO FRECUENTEMENTE	2	7%
MUY BUENO CASI SIEMPRE	6	19%
EXCELENTE SIEMPRE	23	74%
TOTAL	31	100 %

Elaborado por: Investigador

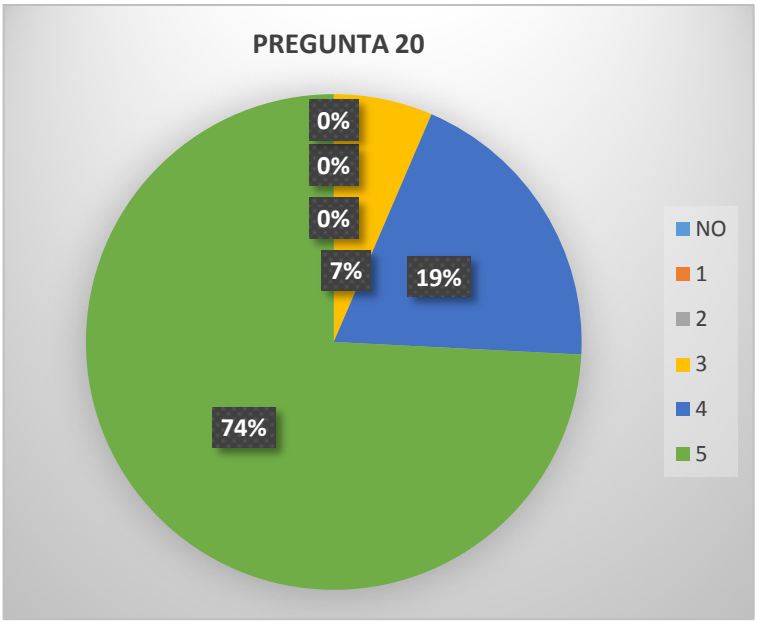


Figura 30. Sistemas de alarma como detectores de humo, incendio

Elaborado por: Investigador

Análisis: En la encuesta realizada al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., el 7% indica que frecuentemente encuentra que existan detectores dentro de su área de trabajo, el 19% indica que casi siempre existen estos detectores y el 74% indica que siempre existe este tipo de detectores dentro de su lugar de desempeño laboral.

Interpretación: La Cooperativa de Ahorro y Crédito cuenta con sistemas de alarma para incendios, detectores de humo y a su vez implementos que permitan mitigar en caso de existir un evento de esta naturaleza, como también realizar capacitaciones a través de Salud Ocupacional a todo su personal y la manera correcta de actuar ante tal situación.

Pregunta 21: ¿Existe vigilancia en la entrada del edificio donde Ud. labora?

Tabla 30. Vigilancia en la entrada del edificio

ALTERNATIVAS	GERENTE, JEFATURAS, ANALISTAS DE CRÉDITO Y RIESGOS, OFICIALES DE CAMPO Y COBRANZAS, CAJEROS	
	FRECUENCIA	%
NO	0	0%
CASI NUNCA	0	0%
REGULARMENTE	0	0%
BUENO FRECUENTEMENTE	1	3%
MUY BUENO CASI SIEMPRE	6	19%
EXCELENTE SIEMPRE	24	78%
TOTAL	31	100 %

Elaborado por: Investigador

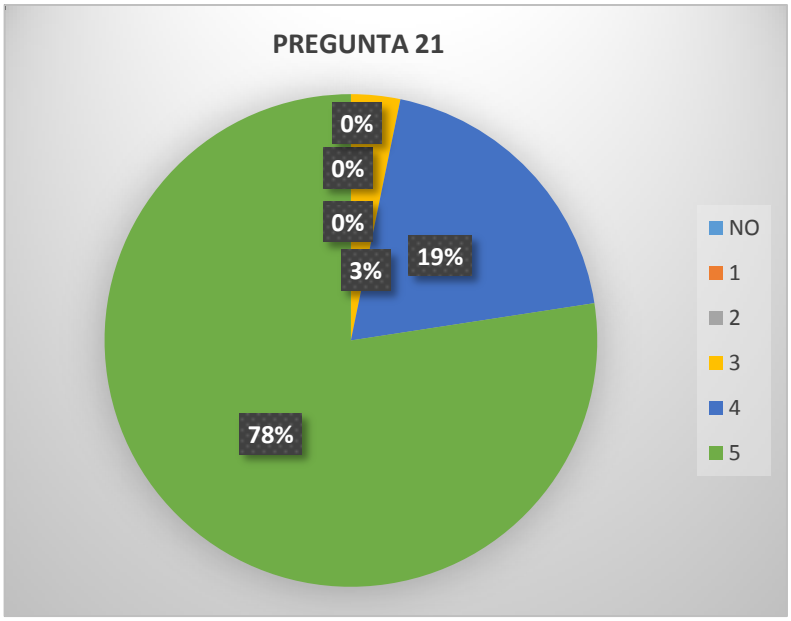


Figura 31. Vigilancia en la entrada del edificio

Elaborado por: Investigador

Análisis: En la encuesta realizada al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., el 3% indica que frecuentemente encuentra un vigilante en el acceso al edificio donde labora, el 19% casi siempre cuenta con seguridad al acceder al edificio y el 78% indica que siempre cuenta con seguridad para el acceso a cada uno de los edificios en donde debe de desempeñar.

Interpretación: El edificio Matriz y agencias de Quito como de Portoviejo cuenta con el servicio de seguridad de la empresa RAVSEG, quienes dependiendo del tamaño del lugar se distribuye al personal y existe una rotación segura de empleados cuando uno de ellos debe de ausentarse del sitio.

4.2 Verificación de la Hipótesis

4.2.1. Planteamiento de la hipótesis

El desarrollo de un Balanced ScoreCard impacta positivamente en el aseguramiento de la información en las Cooperativas de Ahorro y Crédito

4.2.1.1 Modelo Estadístico - Descriptivo

La encuesta se realiza a una muestra de 31 encuestados con la cual se puede identificar los principales factores de relevancia.

Se categorizan las preguntas en las personas que responden "No" y las personas que responden "Sí", aquellas que responden la segunda opción proceden a calificar el servicio del 1 al 5, con las siguientes etiquetas de datos:

- 1= Casi Nunca
- 2= Regularmente
- 3= Bueno/ Frecuentemente
- 4=Bueno/ Casi Siempre
- 5= Excelente/ Siempre

Se presenta el análisis descriptivo de las preguntas más relevantes del estudio.

1. **¿Recibe mantenimiento periódico el computador asignado para el desarrollo de sus funciones?**

La calificación promedio es de 2.5 es decir un servicio de mantenimiento regular, la moda por su parte es 2 que los encuestados eligieron mayoritariamente, la opción 2 de calificación regular, mientras que tiene un grado de dispersión o variabilidad de los datos de 1.33, es decir a partir de la media los datos se distribuyen en 1.33 de diferencia.

Tabla 31. Análisis Pregunta 1

Media	2.52
Mediana	2.00
Moda	2
Desviación estándar	1.338
Varianza	1.791

Elaborado por: Investigador

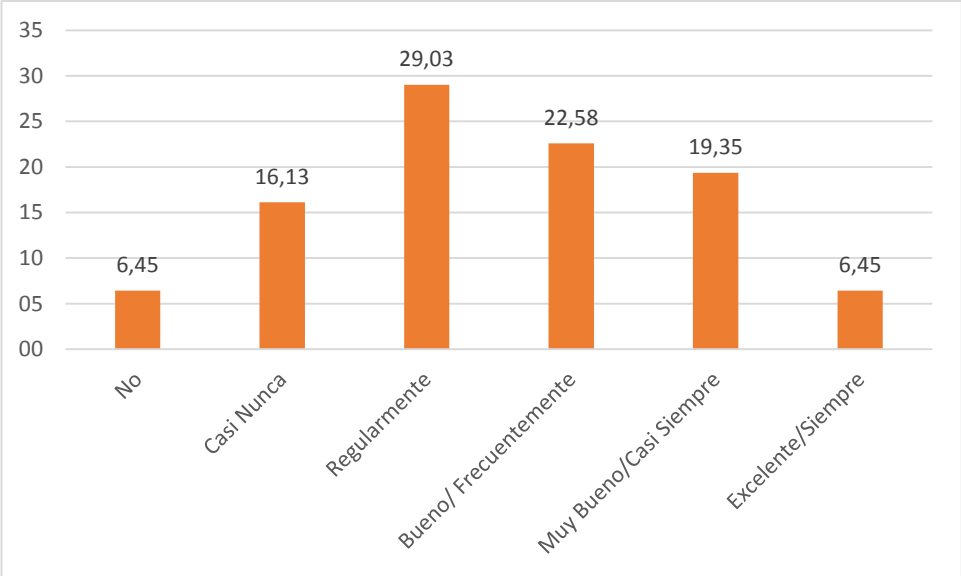


Figura 32. Histograma Pregunta 1

Elaborado por: Investigador

2. ¿El computador asignado en el desarrollo de sus funciones posee antivirus actualizado?

La Calificación promedio de las personas que si poseen antivirus actualizado es 4.1 con lo que se infiere que en promedio el personal casi siempre posee un antivirus actualizado en su equipo de trabajo. La. Moda por otra parte e s 5, equivalente a la. Opción "Siempre", es decir que es la opción con más número de veces elegida por el Personal. Por otro lado, esta pregunta tiene un grado de dispersión o variabilidad de datos de 1.1 osea que estos se distribuyen alrededor de la media en el valor antes mencionado.

Figura 33. Análisis Pregunta 2

Media	4.10
Mediana	5.00
Moda	5
Desviación estándar	1.193
Varianza	1.424

Elaborado por: Investigador

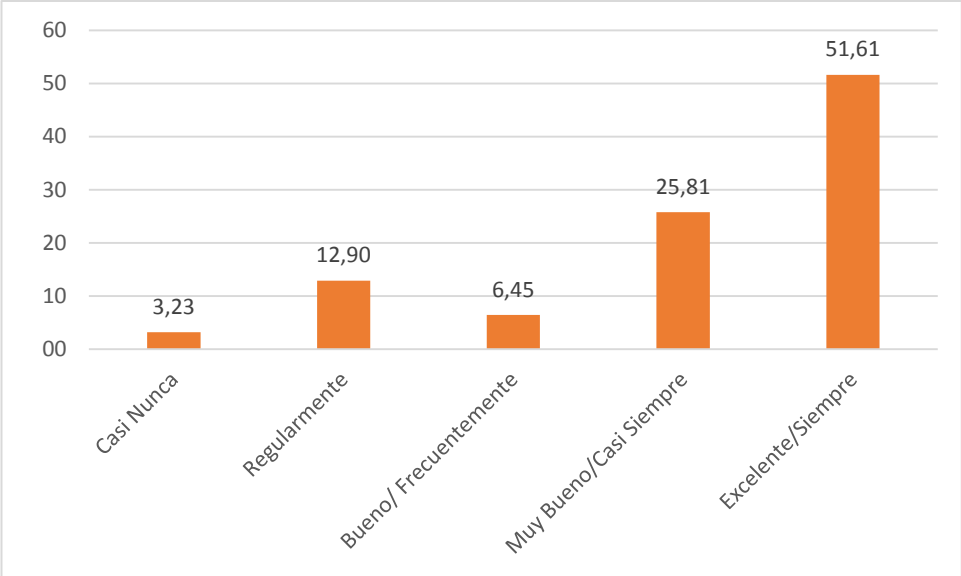


Figura 34. Histograma Pregunta 2

Elaborado por: Investigador

3. ¿Su equipo cuenta con las seguridades para restringir el acceso a personal no autorizado?

La calificación promedio es de 3.6, es decir que frecuentemente los computadores tienen seguridades para evitar el acceso de personal no autorizado en sus equipos de trabajo, la moda por su parte es 4 lo que indica que los encuestados eligieron mayoritariamente la opción 4 "casi siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.45, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 32. Análisis Pregunta 3

Media	3.61
Mediana	4.00
Moda	4
Desviación estándar	1.453
Varianza	2.112

Elaborado por: Investigador

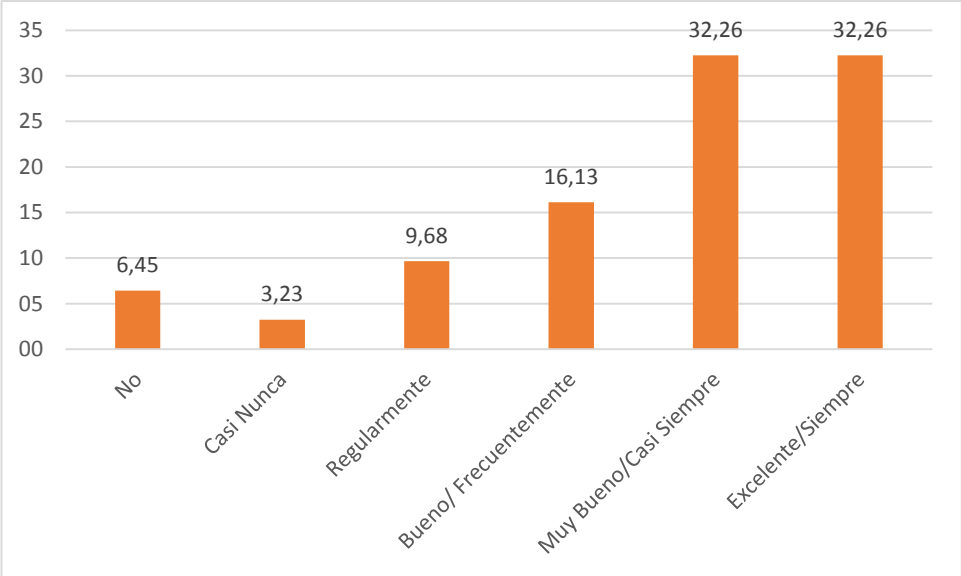


Figura 35. Histograma Pregunta 3

Elaborado por: Investigador

4. ¿Conoce si dentro de la institución existen políticas, normativas o Sistema de Gestión de Seguridad de la Información?

La calificación promedio es de 4.1 es decir casi siempre el personal conoce las políticas y normativas de la gestión de seguridad de la información, la moda por su parte es 5 es decir que los encuestados eligieron mayoritariamente la opción 5 "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.04, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 33. Análisis Pregunta 4

Media	4.19
Mediana	5.00
Moda	5
Desviación estándar	1.046
Varianza	1.095

Elaborado por: Investigador

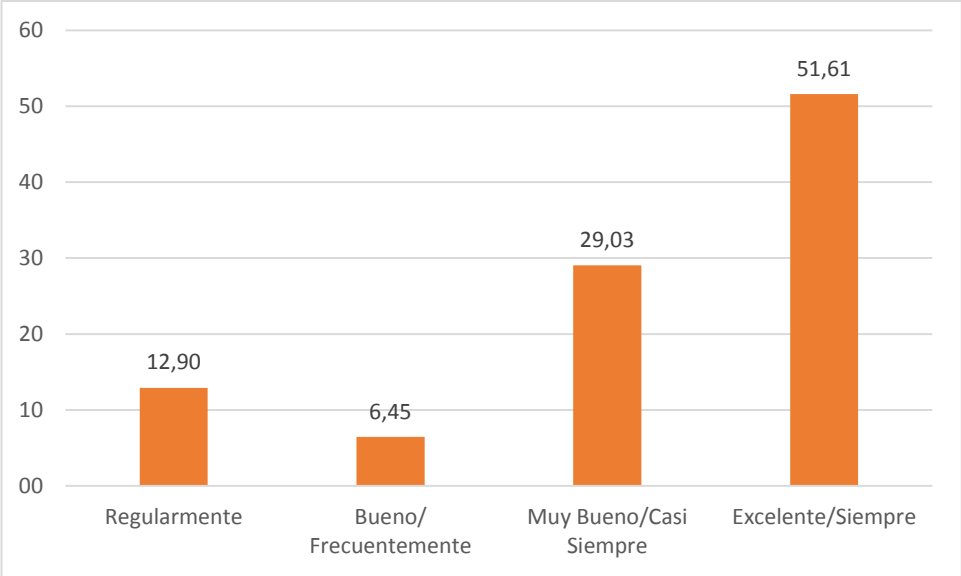


Figura 36. Histograma Pregunta 4

Elaborado por: Investigador

5. ¿Considera necesario que la institución desarrolle e implante una normativa de Gestión de Seguridad de la información?

La calificación promedio es de 4.2 es decir que casi siempre el personal considera necesario el desarrollo e implantación de normativas de gestión de la seguridad de la información, la moda por su parte es 5 lo que indica que los encuestados eligieron mayoritariamente la opción 5 "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 0.855, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 34. Análisis Pregunta 5

Media	4.26
Mediana	4.00
Moda	5
Desviación estándar	.855
Varianza	.731

Elaborado por: Investigador

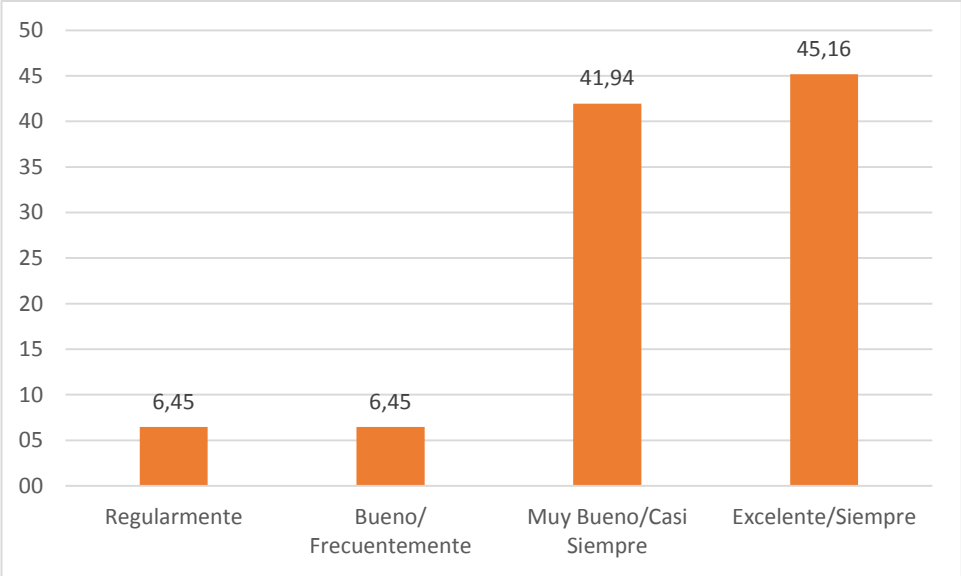


Figura 37. Histograma Pregunta 5

Elaborado por: Investigador

6. ¿La institución capacita al personal en temas de seguridad de la información?

La calificación promedio es de 3.8 eso indica que frecuentemente el personal es capacitado en temas de seguridad de la información por parte de la institución, la moda por su parte es 3, lo que los encuestados eligieron mayoritariamente la opción 3 "frecuentemente" y "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.26, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 35. Análisis Pregunta 6

Media	3.48
Mediana	3.00
Moda	3
Desviación estándar	1.262
Varianza	1.591

Elaborado por: Investigador

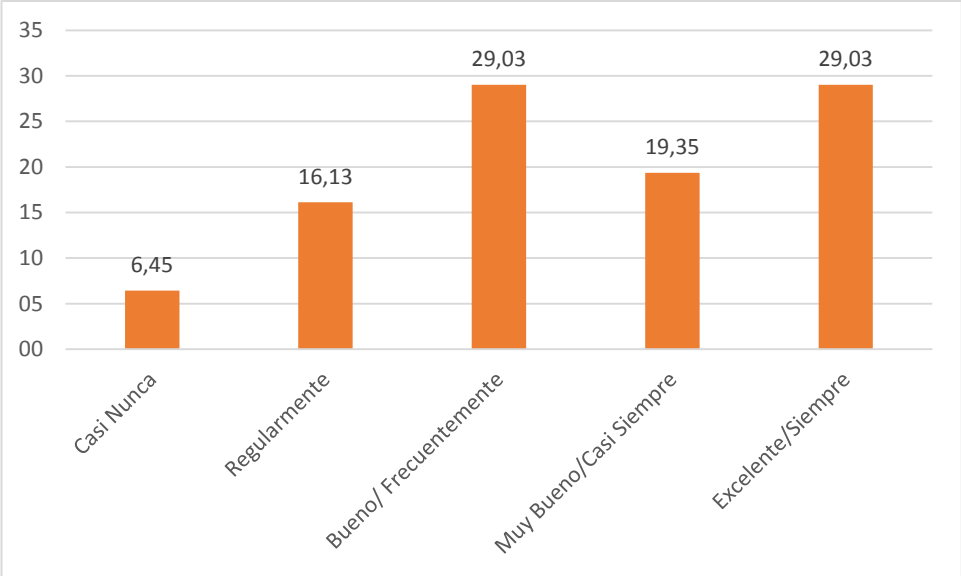


Figura 38. Histograma Pregunta 6

Elaborado por: Investigador

7. ¿Cuándo ocurre un evento relacionado con riesgo operativo sabe a quién reportarlo?

La calificación promedio es de 4.4 es decir que casi siempre el personal conoce a quien reportar un evento de riesgo operativo, la moda por su parte es 5 que los encuestados eligieron mayoritariamente la opción 5 "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 0.810, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 36. Análisis Pregunta 8

Media	4.45
Mediana	5.00
Moda	5
Desviación estándar	.810
Varianza	.656

Elaborado por: Investigador

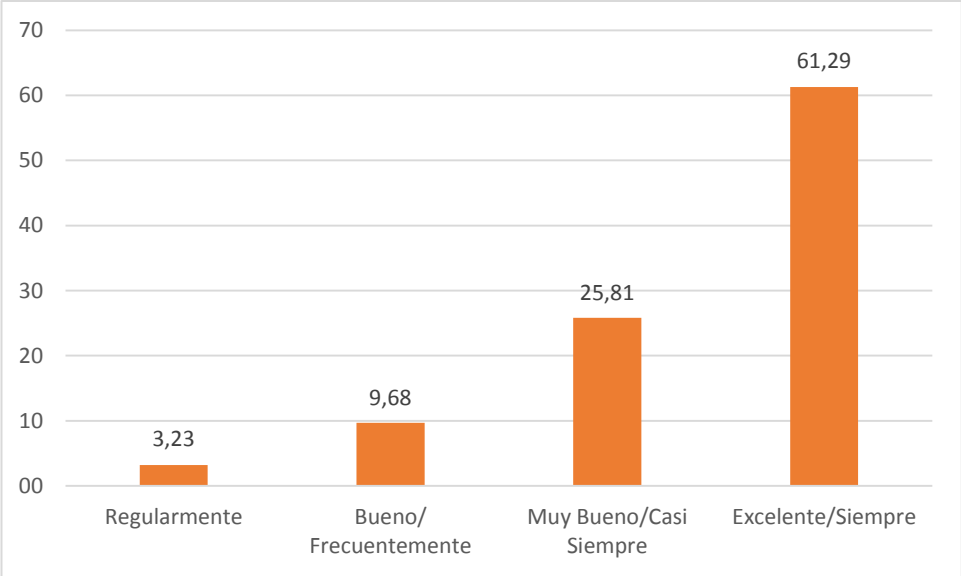


Figura 39. Histograma Pregunta 8

Elaborado por: Investigador

8. ¿Existe alguna política para el cambio regular de las contraseñas?

La calificación promedio es de 2.7, es decir que el personal realiza cambios de contraseñas, la moda por su parte es 5 es decir que los encuestados eligieron mayoritariamente la opción 5 "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 2.08, es decir que los datos se distribuyen alrededor de la media en dicho valor. Se observa que los datos se encuentran con una mayor variabilidad con respecto de la media.

Tabla 37. Análisis Pregunta 11

Media	2.74
Mediana	4.00
Moda	5
Desviación estándar	2.081
Varianza	4.331

Elaborado por: Investigador

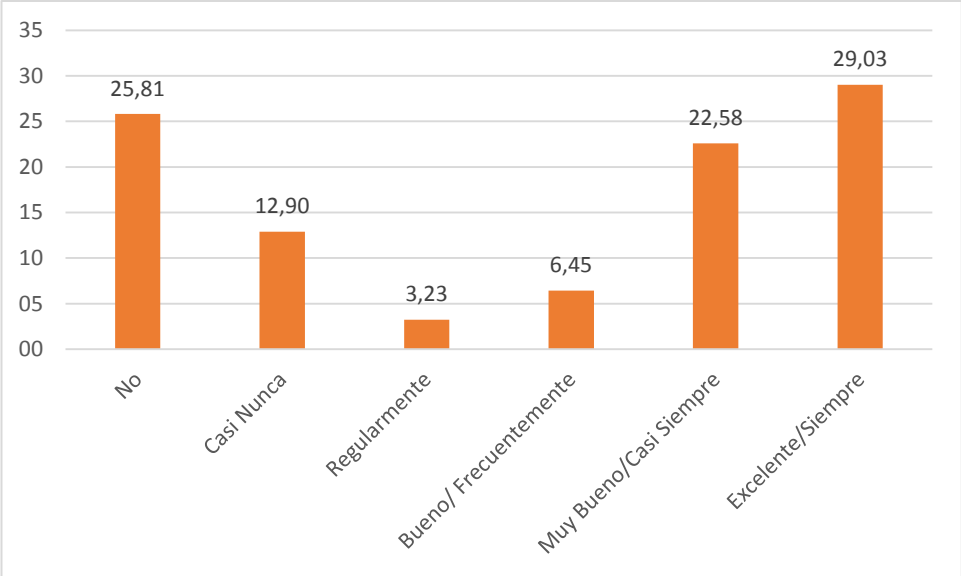


Figura 40. Histograma Pregunta 11

Elaborado por: Investigador

9. ¿Ha detectado problemas en la integridad o exactitud de la información del core financiero?

La calificación promedio es de 1.9 es decir que el personal encuentra problemas en la exactitud del core financiero de manera regular, la moda por su parte es 0 es decir que los encuestados eligieron mayoritariamente la opción 0 "no", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.77, indicando que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 38. Análisis Pregunta 13

Media	1.90
Mediana	1.00
Moda	0
Desviación estándar	1.777
Varianza	3.157

Elaborado por: Investigador

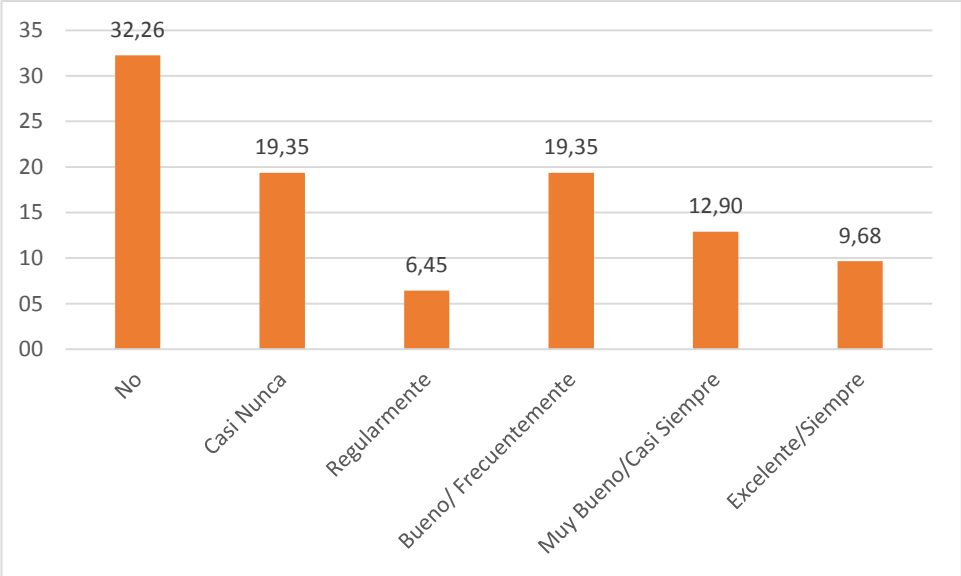


Figura 41. Histograma Pregunta 13

Elaborado por: Investigador

10. ¿La información que usted maneja para el desempeño de sus funciones se respalda periódicamente?

La calificación promedio es de 3.8, es decir que el personal casi siempre respalda la información de su trabajo para un mejor desempeño de sus funciones, la moda por su parte es 5 esto indica que los encuestados eligieron mayoritariamente la opción 5 "siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.302, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 39. Análisis Pregunta 14

Media	3.81
Mediana	4.00
Moda	5
Desviación estándar	1.302
Varianza	1.695

Elaborado por: Investigador

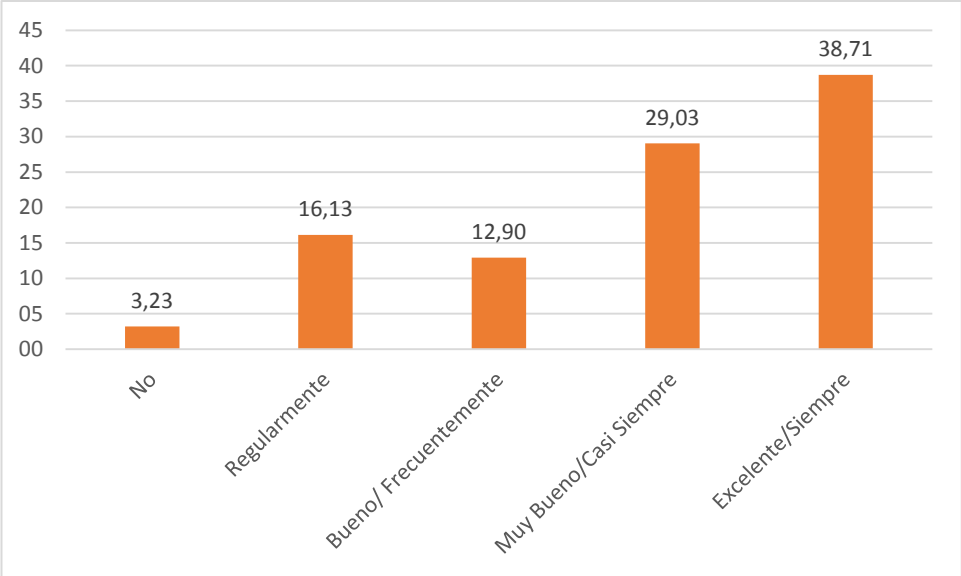


Figura 42. Histograma Pregunta 14

Elaborado por: Investigador

11. ¿Se restringe el acceso de personal a opciones críticas del core financiero, donde se maneja transacciones sensibles de la Cooperativa?

La calificación promedio es de 3.8 es decir que el personal casi siempre considera que se restringen el acceso del personal a opciones críticas del core financiero, la moda por su parte es 4, esto indica que los encuestados eligieron mayoritariamente la opción 4 "casi siempre", mientras que tiene un grado de dispersión o variabilidad de los datos de 1.55, es decir que los datos se distribuyen alrededor de la media en dicho valor.

Tabla 40. Análisis Pregunta 18

Media	3.81
Mediana	4.00
Moda	4
Desviación estándar	1.558
Varianza	2.428

Elaborado por: Investigador

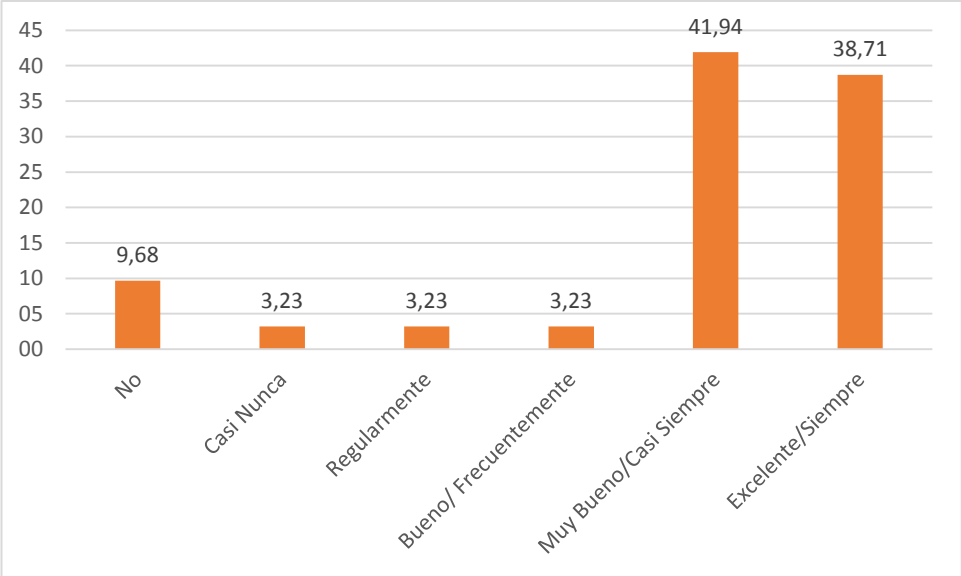


Figura 43. Histograma Pregunta 18

Elaborado por: Investigador

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones:

Con la información recopilada a través de las encuestas realizadas al personal de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., se puede concluir con que la información para el tipo de negocio que ejecuta la entidad financiera es muy importante, por lo que salvaguardarla es lo más primordial y para ello hay que iniciar identificando los activos más importantes para los diferentes procesos.

Con base en las estadísticas obtenidas por cada pregunta y luego de analizar su resultado, es importante dar propuestas a cada respuesta negativa, por tanto, definir un modelo que facilite el aseguramiento de la información que es el objetivo principal de este trabajo es muy importante.

La metodología planteada para este trabajo debe de permitir un esquema apropiado de seguridad para la información, ya que durante el mismo se determina que son varios los activos como por ejemplo el computador personal del empleado que muestra debilidades a la hora de gestionar la información en cada uno de sus estados de gestión. Un aspecto importante en la elaboración de este trabajo es la determinación de responsables para las acciones a ejecutar, ya que sin ello no se puede realizar el seguimiento y verificación de su cumplimiento, y constituir así un mecanismo de rendición de cuentas.

5.2 Recomendaciones

Partiendo de que la información es el activo principal de cualquier empresa sin importar la actividad comercial que este desempeñe, se recomienda definir los procesos más importantes para en base a eso determinar los activos tecnológicos que ayudan en la continuidad de cada uno de ellos. De esta manera se crea un análisis de riesgo hacia los activos de manera más eficaz y con un nivel de efectividad bastante alto, permitiendo mantener un control más efectivo de los riesgos que amenacen a la continuidad del negocio.

CAPITULO VI

6 PROPUESTA

6.1 Datos Informativos

Tema: Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito.

Institución: Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda.

Provincia: Pichincha

Cantón: Quito

Dirección: Oficina Matriz, Av. Cardenal de la Torre S15-111 y Ajaví

Beneficiarios: Gerente, Jefaturas, Analistas De Crédito Y Riesgos, Oficiales De Campo y Cobranzas, Cajeros.

Responsable: Ing. Morales Alomoto Luis Roberto

Director: Carlos Israel Núñez Miranda Mg.

6.2 Antecedentes de la propuesta

En el análisis realizado en el capítulo 2, se hizo referencia a varios trabajos realizados por varios autores, quienes proponen metodologías de desarrollo de sistemas de gestión de seguridad de información basándose en la norma ISO 27001:2013, aplicados en diferentes escenarios, como por ejemplo el trabajo de (Martelo, 2015), que desarrolla un Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI), permitiéndole implementar un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. (Advisera, s.f.), una empresa dedicada a la seguridad de información, en su página web explica cómo hacer que los estándares sean fáciles de entender antes y durante el desarrollo de metodologías basadas en la familia de las ISO.

La Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., es una entidad dedicada a generar fuentes de financiamiento directo a sus clientes, apoyándolos con productos basados en créditos para vivienda, negocios o nuevos emprendimientos, atiende a más de 200 clientes diarios, entregando créditos mensuales por más de 1 millón de dólares, por lo tanto es importante contar con procedimientos legales, organizativos, técnicos y tecnológicos aprobados que aseguren la información en todos sus niveles y estados.

El autor del presente trabajo de tesis desarrolla un modelo de Balanced ScoreCard que, basado en un plan de seguridad, pretende crear una herramienta que dé seguimiento a los procesos y activos que requieran mayor atención, mediante fechas planteadas a planes de acciones concretas y con responsables directos.

6.3 Justificación

Aun que en los trabajos revisados y mencionados en el capítulo 2, describen soluciones que hacen referencia a la seguridad de información basados en la norma ISO 27001, no se encontró un modelo que se adapte al que se plantea como modelo a seguir dentro de la Cooperativa de Ahorro y Crédito Maquita Cushunchic, por lo tanto es importante que el trabajo se base en los mencionados en el capítulo 3 de este documento.

6.4 Objetivos

- Establecer los principios, políticas, y responsabilidades que rijan el proceso de Seguridad de la Información en la Cooperativa
- Determinar la situación actual de la seguridad de la información.
- Diseñar una normativa de seguridad de seguridad de la información basada en la norma internacional ISO 27001:2013 que garantice el estado correcto de la información en todas sus etapas.

6.5 Análisis de Factibilidad

6.6.1. Factibilidad Técnica:

El proyecto técnicamente es factible de realizar ya que se cuenta con los recursos tecnológicos requeridos, haciendo referencia a la infraestructura, herramientas tecnológicas o software, acceso a datos e información requerida.

6.6.2. Factibilidad Operativa:

El presente proyecto es factible operativamente porque cuenta con el apoyo de las autoridades de la Cooperativa de Ahorro y Crédito Maquita Cushunshic Ltda., lo cual también permite tener la apertura necesaria con el personal de la institución financiera para proporcionar la información necesaria y asegura que los resultados del presente proyecto por su beneficio y utilidad sean aplicados.

6.6.3. Factibilidad Organizativa

Organizacionalmente es factible el proyecto ya que los Directivos de la Cooperativa muestran el interés por contar y disponer de medidas para la seguridad de la información, consientes que su aplicabilidad e implementación es a largo plazo.

6.6.4. Factibilidad Económica:

Cabe mencionar que económicamente el presente proyecto es factible ya que los costos que implican el análisis, estudio, tiempo empleado en estos temas serán asumidos por el investigador, mientras que los tiempos del personal de la institución involucrado será asumido por la Institución.

6.6 Fundamentación

El propósito de un Balanced Scorecard es llegar a ser un modelo de gestión integrado de alto nivel que aporta una visión conjunta e interrelacionada. A través de un BSC las organizaciones establecen la estrategia desde una perspectiva multidimensional y dinámica (de cambio continuo) frente a la definición más estática y unidimensional de otros modelos de gestión o planificaciones estratégicas (IsoTools, 2018).

A través de un balanced ScoreCard para la Seguridad de la Información, una organización conoce o está atento a los riesgos que se encuentra expuesto sus datos o registros y los asume, mitiga, elimina o controla de manera documental, esto le permite revisar y mejorar constantemente (IsoTools, 2018).

La Normativa de seguridad de información publicada por la SB (Superintendencia de bancos) establece que se debe de gestionar la seguridad de los datos de clientes, empleados y datos propios de su negocio, satisfaciendo las necesidades de la

institución financiera y salvaguardándola contra el mal uso, revelación y su modificación no autorizada. De esta manera promueve conseguir el nivel de protección adecuado mediante el cumplimiento legal en cuanto a parámetros tecnológicos, disponibilidad, confidencialidad e integridad de la información cuando se encuentre disponible en los sistemas informáticos o a través de la red (Superintendencia de Bancos, 2018).

6.7 Propuesta de Normativa de Seguridad

6.7.1. FASE 1: Situación Actual (Desarrollo de Políticas de Seguridad)

La primera etapa de este trabajo de investigación consiste en determinar la situación actual en la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., para ello se toma como referencia la norma ISO 27001:2013 (Ver Anexo 3), "Sistema de Gestión de Seguridad de la Información" para garantizar la aplicación de buenas prácticas internacionales, y se la complementará con la normativa vigente de la Superintendencia de Bancos, misma que se detalla en la Fundamentación Legal del Capítulo 2, por lo que a continuación se detallan los principios y políticas que regirán este proceso, por cada uno de los 14 dominios (Se consideran en el documento 13 dominios ya que una de ellas se refiere a Políticas de la Seguridad en general, que es todo el documento en sí. Ver Anexo 2) que conforman la norma ISO 27001 y que a continuación detalla:

1. No existe la correcta gestión de la información en su tratamiento en algunos de los aplicativos que maneja la Cooperativa (ejemplo. - Cobis, Coonecta), sin embargo, es el usuario quien tiene muchas fallas, por ejemplo, cuando ingresa los datos del cliente es fácil que las faltas de ortografía se vean dentro de los registros, es por ello que se plantea la revisión anual del cumplimiento de las políticas por parte del área de riesgos, auditoría interna y la unidad de tecnología. Ver Anexo 2.

2. Existe un control muy responsable en la contratación de nuevo personal para la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., sea con la revisión de antecedentes personales, profesionales y penales de los aspirantes y una vez incluidas en la nómina de la entidad financiera se le crea usuarios con sus respectivos roles dentro de las aplicaciones que por su función deberá de cumplir, de esto se encarga el Área de Soporte

3. El sistema financiero Cobis, adjunta dentro de sus módulos, la gestión de activos, mismo que es manipulada por el área contable, sin embargo, no cuenta con la correcta gestión de traslados de equipos de computación, encontrando bajo registros que un activo se encuentra en determinada agencia, pero físicamente está en otro lugar y como responsable el jefe o jefa de agencia.

4. El acceso a los sistemas y recursos de la Cooperativa se realiza según el perfil del usuario y las funciones a él asignadas, siendo el área de soporte los únicos responsables de gestionar tal actividad.

5. El área de tecnología es la encargada de validar procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

6. Las agencias como el edificio matriz de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda., cuenta con seguridad privada de la empresa RAVSEG, quienes son los encargados de no permitir el acceso a áreas restringidas, a no ser bajo la responsabilidad de uno de los empleados de la entidad financiera.

7. No cuenta con un área de desarrollo ni de ambiente de pruebas, ya que los servicios se manejan a través de varias empresas quienes venden el servicio de sus aplicaciones o infraestructura, tal es el caso del sistema financiero Cobis de CobisCorp, que se encarga de la gestión de datos de los clientes,

8. El área de Tecnología es el encargado de configurar los dispositivos y aplicaciones de tal manera que puedan evitar el acceso físico no autorizado.

9. Documentos de contrato de servicios u otros relacionados a los proveedores, son dirigidas al área de auditoria interna y son ellos los encargados junto al área de contabilidad de su custodia y validación de la renovación o finiquito de los mismos.

10. La gestión de amenazas en la seguridad de la información está a cargo del área de riesgos, pero no cuenta con la herramienta adecuada para llevar un control de los incidentes que afectan, amenazan la continuidad del negocio, por lo que es importante que se desarrolle un Balanced ScoreCard para la seguridad de la información.

Para más detalle las políticas de seguridad realizada para este trabajo se encuentran en el Anexo 2.

6.7.2. FASE 2: Valoración de Activos

Uno de los aspectos más importantes de la empresa es valorar los activos informáticos con los que la Cooperativa cuenta para salvaguardar los procesos que implican el manejo de información y por ende su seguridad.

Para poder cumplir esta fase se ha realizado lo siguiente:

1. **Identificar los procesos con los que cuenta la Cooperativa. -** Para identificar los procesos se tuvo apoyo del área de riesgos y procesos, quienes aportaron para su posterior análisis.

Tabla 41. Procesos

COOPERATIVA MAQUITA CUSHUNCHIC	
Código	**Procesos**
P.02.01.01	Negociación de Fuentes de Financiamiento
P.02.01.02	Gestión de Desembolso de Fuentes de Financiamiento
P.04.01.01	Negociación de Microcrédito
P.04.01.02	Análisis y Aprobación de Microcrédito
P.04.01.03	Otorgamiento de Microcrédito
P.04.02.01	Negociación de Crédito Consumo
P.04.02.02	Análisis y Aprobación de Crédito Consumo
P.04.02.03	Otorgamiento de Crédito Consumo
P.06.03.01	Ejecución de transacciones en ventanilla
P.06.03.02	Envío y recepción de transferencias
A.01.02.01	Administración y Control de Efectivo en Cajas

A.01.02.02	Apertura y Cierre de Agencias
A.02.02.01	Administración de la Disponibilidad y la Capacidad
A.02.02.02	Administración del Cambio
A.02.02.03	Administración de la Aceptación del Cambio y de la Transición
A.02.02.04	Administración de la Configuración
A.04.02.01	Pago de nómina
A.05.01.01	Elaboración y Presentación de Estados Financieros

Elaborado por: Investigador

2. **Identificar todos los activos que se involucran para llevar a cabo cada uno de los procesos encontrados. -** La identificación de los activos parte de la información que mantiene el área de sistemas a través del inventario y los mismos que han sido validados por el área contable.

INVENTARIO - ACTIVOS INFORMÁTICOS									
Nº	CODIGO	Nº ACTIVO	DESCRIPCIÓN	MARCA	MODELO	TIPO	FECHA DE REGISTRO	FECHA DE COMPRA	FUNCIÓN
145	31201701005700	1196	Localizador	GSM	GSM LOCALIZADOR GL-100 069095587-011874000533658,	Elegir Tipo..	08/01/2012	08/06/2012	
146		1585	LAPTOP	Toshiba	COMPUTADOR LAPTO TOSHIBA SATELLITE L55-C52205	Portatil		06/23/2016	
147	30800341005800	625	Impresora	HP	IMPRESORA LASER HP 1022 SERIE VNB3H74225	Láser	01/01/2008	01/09/2008	
148	30500291000600	394	Ipaq	HP	HP. IPAQ RX3715 152MB S3C 2440 SERIE TWC51807CX	Elegir Tipo..	06/01/2005	06/21/2005	
149	30500031003600	395	Ipaq	HP	HP IPAQ RX3715 152MB S3C 2440 SERIE TWC51807FJ	Elegir Tipo..	06/01/2005	06/21/2005	
150	30600011005400	426	LAPTOP	SONY	COMPUTADOR PORTÁTIL SONY VAIO VGN-FJL50F MODELO PC	Portatil	03/01/2006	02/22/2006	
151	30800361005400	686	LAPTOP	HP	COMPUTADOR PORTATIL HP 2710P SERIE 2CE81226K2	Portatil	06/01/2008	05/28/2008	
152	30600121005800	489	Ipaq	HP	IPAQ HP RX3715 152 MB 83C 2440 SERIE X11-15450	Elegir Tipo..	01/01/2007	12/27/2006	
153	21802851005900	1772	DVR	MARKVISION	DVR DIGITAL MARKVISION 16 CANALES CON DISCO DURO D	Digital	02/01/2018	01/31/2018	
154	31301931005900	1293	BLUERAY	Elegir Marca...	UNIDAD DE BLUERAY EXTERNO	Externo	11/01/2013	10/15/2013	
155	31602451005900	1573	Disco Duro	Elegir Marca...	WD RED 1TB NAS HARD DISK DRIVE 5400 RPM CLASS SATA	Elegir Tipo..	04/01/2016	04/13/2016	Dispositivo para agente de respaldos
156	31602471005900	1577	Servidor	HP	SERVIDOR HP ML110 G9 UBICADO EN CUARTO DE SISTEMAS	Elegir Tipo..	05/01/2016	04/29/2016	SRVANTIMALWARE- 192.0.0.130
157	31602481005900	1578	Servidor	HP	SERVIDOR HP ML110 G9 UBICADO EN CUARTO DE SISTEMAS	Elegir Tipo..	05/01/2016	04/29/2016	SRVRIESGOS - 192.0.0.104
158	31000751005900	814	Servidor	POWER EDGE	SERVIDOR CENTRAL DELL -MODELO POWER EDGE R710 - SER	Elegir Tipo..	03/01/2010	03/12/2010	

Figura 44. Ficha para inventario de equipos informáticos

Elaborado por: Investigador

No.	TIPO	ACTIVO
1	**BDD**	Sybase
2	**Hardware**	Servidor principal
3	**Hardware**	Servidor branch
4	**Instalaciones**	DC Century-Link
5	**Instalaciones**	DC local
6	**Instalaciones**	Agencias
7	**Personal**	Supervisor Operativo
8	**Personal**	Jefes de agencia
9	**Personal**	Jefe de Control Financiero
10	**Personal**	Asesoras
11	**Personal**	Analistas de crédito
12	**Personal**	Operador de Tecnología
13	**Personal**	Contadora General
14	**Personal**	Cajeros
15	**Proveedores**	Telconet
16	**Proveedores**	Eqysum
17	**Proveedores**	Cobiscorp
18	**Proveedores**	Seguridad privada RAV
19	**Proveedores**	Banco Central
20	**Proveedores**	Jefferson Arciniega
21	**Proveedores**	Diebold
22	**Proveedores**	Pago ágil
23	**Proveedores**	GYP Multiservicios
24	**Proveedores**	Casa Pazmiño
25	**Red**	Switch Telconet
26	**Red**	Switch Eqysum
27	**Red**	Switch local
28	**Red**	Proxy Fortigate
29	**Red**	Enlace de Internet
30	**Software**	Cobis
31	**Software**	SPI BCE
32	**Software**	Internet Explorer
33	**Software**	Outlook
34	**Software**	Pago ágil
35	**Software**	Ofimática
36	**Software**	Browser (Chrome, Mozilla)
37	**Software**	Thunderbird
38	**Software**	Invgate (mesa de servicios)

Figura 45. Catálogo de Activos por grupo

Elaborado por: Investigador

Código	Procesos	BDD	Hardware	Software	Red	Personal	Proveedores	Instalaciones
P.02.01.01	Negociación de Fuentes de Financiamiento	N/A	PC de usuario	Ofimática, Correo	Enlace de Internet	Jefe de Control, Financiero	Telconet, Eqysum, Externos	N/A
P.02.01.02	Gestión de Desembolso de Fuentes de Financiamiento	N/A	PC de usuario	Ofimática, Correo	Enlace de Internet	Jefe de Control Financiero	Externos	N/A
P.04.01.01	Negociación de Microcrédito	Sybase	Servidor branch, Servidor principal	Cobis, IE, correo	Enlace de Intranet	Asesoras	Cobiscorp	DC Century-Link
P.04.01.02	Análisis y Aprobación de Microcrédito	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Analistas de crédito	Cobiscorp, Telconet, Eqysum	DC Century-Link
P.04.01.03	Otorgamiento de Microcrédito	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Supervisor Operativo	Cobiscorp, Telconet, Eqysum	DC Century-Link
P.04.02.01	Negociación de Crédito Consumo	Sybase	Servidor branch, Servidor principal	Cobis, IE, correo	Enlace de Intranet	Asesoras	Cobiscorp	DC Century-Link
P.04.02.02	Análisis y Aprobación de Crédito Consumo	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Analistas de crédito	Cobiscorp, Telconet, Eqysum	DC Century-Link
P.04.02.03	Otorgamiento de Crédito Consumo	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Supervisor Operativo	Cobiscorp, Telconet, Eqysum	DC Century-Link
P.06.03.01	Ejecución de transacciones en ventanilla	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Cajeros	Cobiscorp, telconet, Eqysum, Produbanco	DC Century-Link
P.06.03.02	Envío y recepción de transferencias	Sybase	Servidor branch, Servidor principal	Cobis, IE, browser, correo	Enlace de Internet	Supervisor Operativo	Cobiscorp, telconet, Eqysum, Banco Central	DC Century-Link

Figura 46. Identificación de Activos - I

Elaborado por: Investigador

Código	Procesos	BDD	Hardware	Software	Red	Personal	Proveedores	Instalaciones
A.02.02.01	Administración de la Disponibilidad y la Capacidad	Sybase	Proxy Fortigate, Servidor branch, Servidor principal	Software monitoreo Fortigate	Enlace de Intranet	Operador de Tecnología	Cobiscorp	DC Local
A.02.02.02	Administración del Cambio	N/A	Proxy Fortigate, Servidor branch, Servidor principal	Ofimática, IE, correo, mesa de servicios	Enlace de Internet	Operador de Tecnología	Cobiscorp, la entidad, GYP Multiservicios , Jefferson Arciniega, Diebold, Casa Pazmiño	Agencias, DC Local
A.02.02.03	Administración de la Aceptación del Cambio y de la Transición	N/A	Proxy Fortigate, Servidor branch, Servidor principal	Ofimática, IE, correo, mesa de servicios	Enlace de Internet	Operador de Tecnología	Cobiscorp, la entidad, GYP Multiservicios , Jefferson Arciniega, Diebold, Casa Pazmiño	Agencias, DC Local
A.02.02.04	Administración de la Configuración	Sybase	Proxy Fortigate, Servidor branch, Servidor principal	Ofimática, IE, correo, mesa de servicios	Enlace de Internet	Operador de Tecnología	Cobiscorp, la entidad, GYP Multiservicios , Jefferson Arciniega, Diebold, Casa Pazmiño	Agencias, DC Local
A.04.02.01	Pago de nómina	Sybase	Servidor branch, Servidor principal	Cobis, IE, correo, ofimática	Enlace de Intranet	Contadora General	Cobiscorp	DC Century-Link
A.05.01.01	Elaboración y Presentación de Estados Financieros	Sybase	Servidor branch, Servidor principal	Cobis, IE, correo, ofimática	Enlace de Intranet	Contadora General	Cobiscorp	DC Century-Link

Figura 47. Identificación de Activos - II

Elaborado por: Investigador

Las categorías que involucran esta clasificación y análisis son: Bases de Datos (BDD), Hardware, Software, Red, Personal, Proveedores, Instalaciones. Y cada uno de ellos tiene su propio conjunto de activos que ayudan a que un proceso se ejecute de manera correcta o con fallas, y que el departamento de sistemas debe de controlar o mitigar.

3. Valorar los activos que más importancia tenga para la empresa.

3.1.Dimensiones de la valoración

Son aquellas que hacen valioso a un activo, por lo tanto, dimensionar significa darle un valor a un activo independientemente de otras.

Esto nos permitirá a su vez valorar las consecuencias de la materialización de una amenaza, ósea es la medida del perjuicio para la organización en el caso de que el activo se vea dañado con respecto a este aspecto.

Dependiendo del análisis y la calificación que se le da al cumplir o no estos parámetros, se obtienen los siguientes valores. Ver **Figura 48.**

ACTIVO	ATRIBUTOS			VALORACIÓN
	Disponibilidad	Confidencialidad	Integridad	
BDD				
Sybase	4	4	4	64
Hardware				
Servidor principal	4	3	4	48
Servidor branch	4	3	4	48
Red				
Switch Telconet	4	3	4	48
Switch Eqysum	4	3	4	48
Switch local	4	3	4	48
Proxy Fortigate	2	3	4	24
Software				
Cobis	4	3	4	48
Ofimática	2	2	2	8
Internet Explorer	3	2	3	18
Browser (Chrome, Mozill	2	2	2	8
Outlook	3	2	2	12
Thunderbird	2	2	2	8
Pago ágil	2	3	2	12
SPI BCE	2	3	4	24
Invgate (mesa de servicio	1	1	1	1
Personal				
Jefe de Control Financiero	2	4	4	32
Asesoras	2	4	4	32
Analistas de crédito	3	3	3	27
Cajeros	3	2	2	12
Supervisor Operativo	3	4	4	48
Contadora General	2	3	3	18
Jefes de agencia	3	4	4	48
Operador de Tecnología	2	3	4	24
Proveedores				
Cobiscorp	3	4	3	36
Telconet	4	3	4	48
Eqysum	4	3	4	48
Pago ágil	2	3	1	6
Banco Central	3	3	3	27
Seguridad privada RAV	3	3	4	36
GYP Multiservicios	3	1	3	9
Jefferson Arciniega	2	3	3	18
Diebold	2	2	4	16
Casa Pazmiño	2	1	2	4
Instalaciones				
DC Century-Link	4	3	3	36
DC local	4	3	3	36
Agencias	3	2	2	12

Figura 48. Valoración de activos

Elaborado por: Investigador

Una vez teniendo la matriz con la valoración hecha a cada uno de los activos procedemos a agrupar, los de puntaje a partir del 24 en adelante, que se determina como crítico y lo ordenamos desde el más alto al más bajo en puntuación, quedando como lo indica la siguiente figura.

			MÍNIMO
TIPO	ACTIVO	PUNTAJE	24
BDD	Sybase	64	Crítico
Hardware	Servidor principal	48	Crítico
Hardware	Servidor branch	48	Crítico
Red	Switch Telconet	48	Crítico
Red	Switch Eqysum	48	Crítico
Red	Switch local	48	Crítico
Software	Cobis	48	Crítico
Personal	Supervisor Operativo	48	Crítico
Personal	Jefes de agencia	48	Crítico
Proveedores	Telconet	48	Crítico
Proveedores	Eqysum	48	Crítico
Proveedores	Cobiscorp	36	Crítico
Proveedores	Seguridad privada RAV	36	Crítico
Instalaciones	DC Century-Link	36	Crítico
Instalaciones	DC local	36	Crítico
Personal	Jefe de Control Financiero	32	Crítico
Personal	Asesoras	32	Crítico
Personal	Analistas de crédito	27	Crítico
Proveedores	Banco Central	27	Crítico
Personal	Operador de Tecnología	24	Crítico
Red	Proxy Fortigate	24	Crítico
Software	SPI BCE	24	Crítico
Software	Internet Explorer	18	No crítico
Personal	Contadora General	18	No crítico
Proveedores	Jefferson Arciniega	18	No crítico
Proveedores	Diebold	16	No crítico
Software	Outlook	12	No crítico
Software	Pago ágil	12	No crítico
Personal	Cajeros	12	No crítico
Proveedores	Pago ágil	12	No crítico
Instalaciones	Agencias	12	No crítico
Proveedores	GYP Multiservicios	9	No crítico
Software	Ofimática	8	No crítico
Software	Browser (Chrome, Mozilla)	8	No crítico
Software	Thunderbird	8	No crítico
Proveedores	Casa Pazmiño	4	No crítico
Software	Invgate (mesa de servicios)	1	No crítico

Figura 49. Clasificación de activos en orden descendente

Elaborado por: Investigador

Una vez organizado nuestros activos procedemos a agruparlos de manera que nos permita crear matrices para su análisis de riesgo, como se lo puede observar en la siguiente imagen.

No.	TIPO	ACTIVO	PUNTAJE
1	**Instalaciones**	DC Century-Link	36
1	**Instalaciones**	DC local	36
2	**Red**	Switch Telconet	48
2	**Red**	Switch Eqysum	48
2	**Red**	Switch local	48
2	**Red**	Proxy Fortigate	24
3	**Hardware**	Servidor principal	48
3	**Hardware**	Servidor branch	48
4	**Software**	Sybase	64
4	**Software**	Cobis	48
4	**Software**	SPI BCE	24
5	**Personal**	Supervisor Operativo	48
5	**Personal**	Jefes de agencia	48
5	**Personal**	Jefe de Control Financiero	32
5	**Personal**	Asesoras	32
5	**Personal**	Analistas de crédito	27
5	**Personal**	Operador de Tecnología	24
6	**Proveedores**	Telconet	48
6	**Proveedores**	Eqysum	48
6	**Proveedores**	Cobiscorp	36
6	**Proveedores**	Seguridad privada RAV	36
6	**Proveedores**	Banco Central	27

Figura 50. Clasificación de activos según su ponderación y grupo

Elaborado por: Investigador

6.7.3. FASE 3: Análisis de Riesgos

Una vez realizada la valoración de cada uno de los activos que interactúan con los procesos se procede a realizar un análisis de riesgo a cada grupo identificado que son los siguientes:

TIPO	ACTIVO
Instalaciones	DC Century-Link
	DC local
Red	Switch Telconet
	Switch Eqysum
	Switch local
	Proxy Fortigate
Hardware	Servidor principal
	Servidor branch
Software	Sybase
	Cobis
	SPI BCE
Personal	Supervisor Operativo
	Jefes de agencia
	Jefe de Control Financiero
	Asesoras
	Analistas de crédito
	Operador de Tecnología
Proveedores	Telconet
	Eqysum
	Cobiscorp
	Seguridad privada RAV
	Banco Central

Figura 51. Clasificación de activos por grupos

Realizado por: Investigador

Luego de haber identificado los grupos de activos y obtenidos una valoración para cada uno de ellos, procedemos a realizar su análisis, en donde determinaremos el nivel de riesgo que implica dentro de cada proceso identificado, para esta fase nos apoyamos en el catálogo de amenazas de la **figura 52**.

CATÁLOGO DE AMENAZAS	
Categoría	**Amenaza**
Daño físico	Fuego
	Daño en tuberías
	Contaminación
	Destrucción
	Corrosión, polvo
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Inundación
Pérdida de servicios	Falla del aire acondicionado
	Falla de provisión de agua
	Pérdida de provisión de luz
	Falla de telecomunicaciones
Disturbio por radiación	Radiación electromagnética
	Radiación termal
	Pulsos electromagnéticos
Compromiso de la información	Intercepción de señales de interferencia comprometedoras
	Espionaje remoto
	Robo de medios o documentos
	Robo de equipos
	Recuperación de medios descartados o reciclados
	Revelación
	Datos de fuentes no confiables
	Detección de posición
Daños técnicos	Falla de equipos
	Mal funcionamiento de equipos
	Saturación del sistema
	Mal funcionamiento del software
	Brecha de mantenimiento de sistemas
Acciones no autorizadas	Uso no autorizado de equipos
	Copia fraudulenta de software
	Uso de software pirata
	Corrupción de datos
	Procesamiento ilegal de datos
Compromiso de funciones	Error en el uso
	Abuso de privilegios
	Denegación
	Brecha de disponibilidad de personal
Fraudes o ataques	Hacking, cracking
	Delitos informáticos
	Terrorismo
	Espionaje industrial
	Intrusión, negligencia

Figura 52. Catálogo de amenazas

Elaborado por: Investigador

Con lo anterior se procede al análisis de riesgo de cada activo, dependiendo del grupo al que pertenece, como se muestra en las siguientes figuras.

Instalaciones – DC Century Link

DC Century-Link	36	CONTROL	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA AMENAZA	IMPACTO EN EL NEGOCIO	NIVEL DE RIESGO	ESTRATEGIA DE RESPUESTA	CONTROL A IMPLEMENTAR	RESPONSABLE	FECHA PLAZO
Daño físico	Fuego	Sistema contra incendios y enfriamiento	N/A	Baja	Medio	BAJO	Aceptar			
	Daño en tuberías	Tuberia diseñada para agua(caliente o fría) y monitoreo de instalaciones	N/A	Baja	Bajo	BAJO	Aceptar			
	Inundación	Monitoreo de instalaciones	N/A	Baja	Bajo	BAJO	Aceptar			
	Contaminación	Sistema de Ventilación	NA	Baja	Bajo	BAJO	Aceptar			
	Corrosión, polvo	Monitoreo y limpieza de instalaciones	N/A	Baja	Bajo	BAJO	Aceptar			
Eventos naturales	Fenómenos climáticos	Control de sumideros y desagues en las instalaciones	N/A	Baja	Bajo	BAJO	Aceptar			
	Fenómenos sísmicos	Edificio antisismico, rutas seguras de evacuación	N/A	Baja	Alto	MEDIO	Mitigar	Implementación de un Sitio alterno de contingencia	Century Link	
	Fenómenos volcánicos	Implementación de Sistemas de Alerta Volcánico, Rutas seguras de evacuación	El DC se encuentra ubicado en las laderas del volcán Guagua Pichincha	Baja	Alto	MEDIO	Mitigar	Implementación de un Sitio alterno de contingencia	Century Link	
Pérdida o falla de servicios	Falla del aire acondicionado	Sistema de enfriamiento controlado	N/A	Baja	Bajo	BAJO	Aceptar			
	Pérdida de provisión de luz	Implementación de UPS (Sistema de Energía Ininterrumpida)	N/A	Baja	Bajo	BAJO	Aceptar			
	Variación de voltaje	Implementación de Reguladores, Elevadores de energía, UPS (Sistema de Energía Ininterrumpida)	N/A	Baja	Bajo	BAJO	Aceptar			
Compromiso de la información	Intercepción de señales de interferencia comprometedoras	Encriptadores de información	N/A	Baja	Medio	BAJO	Aceptar			
	Espionaje remoto	Antivirus y proxys	N/A	Baja	Medio	BAJO	Aceptar			
	Robo de medios o documentos	Politicas de documentación	N/A	Baja	Medio	BAJO	Aceptar			
	Robo de equipos	Póliza de seguros para equipos contra todo riesgo; fuertes procedimientos de seguridad para el ingreso físico, CCTV	N/A	Baja	Medio	BAJO	Aceptar			
	Recuperación de medios descartados o	Politicas de documentación	N/A	Baja	Bajo	BAJO	Aceptar			
	Revelación	Acuerdos de confidencialidad	N/A	Baja	Medio	BAJO	Aceptar			
	Datos de fuentes no confiables	Politicas de Seguridad	N/A	Baja	Bajo	BAJO	Aceptar			

Figura 53. Análisis Instalaciones – DC Century Link

Elaborado por: Investigador

Instalaciones – DC Local

DC Local	36	CONTROL	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA AMENAZA	IMPACTO EN EL NEGOCIO	NIVEL DE RIESGO	ESTRATEGIA DE RESPUESTA	CONTROL A IMPLEMENTAR	RESPONSABLE	FECHA PLAZO
Daño físico	Fuego	Detectores de Fuego y uso de materiales inherentes del fuego	Espacio reducido para controlar el fuego enj caso de tal evento, existe un detector de humo que no se ha probado	Baja	Alto	MEDIO	Mitigar	Probar el funcionamiento óptimo del detector de humo, si emite algún tipo de alerta para que el personal tome acción inmediata ante la ocurrencia de fuego		
	Daño en tuberías	Tuberias de plástico adecuadas para agua caliente o fría según sea el caso	N/A	Baja	Medio	BAJO	Aceptar			
	Inundación	Ubicación de Datacenter en lugares altos	N/A	Baja	Medio	BAJO	Aceptar			
	Contaminación		N/A	Baja	Bajo	BAJO	Aceptar			
	Corrosión, polvo	Instalación y uso de ventiladores de aire, limpieza periodica		Baja	Medio	BAJO	Aceptar			
Eventos naturales	Fenómenos climáticos	Sistema de enfriamiento controlado	Existe uno solo y no existe sensor de temperatura o humedad	Baja	Alto	MEDIO	Mitigar	Instalar un sensor de temperatura y humedad que emita alertas para acción inmediata del personal	Sistemas	
	Fenómenos sísmicos		El espacio se encuentra dividido por vidrios	Baja	Bajo	BAJO	Aceptar			
	Fenómenos volcánicos	El espacio no cuenta con ventanas	N/A	Baja	Medio	BAJO	Aceptar			
Pérdida o falla de servicios	Falla del aire acondicionado	Sistema de enfriamiento controlado	Existe un solo equipo de enfriamiento y no existe sensor de temperatura o humedad	Baja	Alto	MEDIO	Mitigar	Instalar un sensor de temperatura y humedad que emita alertas para acción inmediata del personal	Sistemas	
	Pérdida de provisión de luz	Se cuenta con APS	Cortes de energía recurrentes en el sector	Media	Bajo	BAJO	Aceptar			
	Variación de voltaje	Conexión a tierra, APS, Elevadores de energía	N/A	Baja	Medio	BAJO	Aceptar			

Figura 54. Análisis Instalaciones – DC Local

Realizado por: Investigador

Red

Switch Telconet	48	Control	Vulnerabilidad	Probabilidad de ocurrencia de la	Impacto en el negocio	Nivel de Riesgo	Estrategia de	Control a implementar	Responsable	Fecha Plazo
Pérdida de servicios	Falla de telecomunicaciones	Monitoreo de Servicios, acceso restringido	Los cables no están etiquetados y están expuestos a manipulación incorrecta	Baja	Alto	MEDIO	Mitigar	Solicitar a los proveedores que etiqueten los cables de sus equipos, bajo un	Sistemas	
Pérdida de servicios	Falla de telecomunicaciones	Monitoreo de Servicios, acceso restringido	Existe un proveedor alterno de Internet, pero no se ha probado el funcionamiento	Baja	Alto	MEDIO	Mitigar	Probar el servicio alterno de Internet	Sistemas	
Switch Eqysum	**48**	**Control**	**Vulnerabilidad**	**Probabilidad de ocurrencia de la**	**Impacto en el negocio**	**Nivel de Riesgo**	**Estrategia de**	**Control a implementar**	**Responsable**	**Fecha Plazo**
Pérdida de servicios	Falla de telecomunicaciones	Monitoreo de Servicios, acceso restringido	Los cables no están etiquetados y están expuestos a manipulación incorrecta	Baja	Medio	BAJO	Aceptar			
Pérdida de servicios	Falla de telecomunicaciones	Monitoreo de Servicios, acceso restringido	Su funcionamiento no ha sido validado	Baja	Medio	BAJO	Aceptar			
Switch local	**48**	**Control**	**Vulnerabilidad**	**Probabilidad de ocurrencia de la**	**Impacto en el negocio**	**Nivel de Riesgo**	**Estrategia de**	**Control a implementar**	**Responsable**	**Fecha Plazo**
Daños técnicos	Falla de equipos	Equipo de marca reconocida, Acceso restringido	Se cuenta con un único dispositivo, no tiene mantenimiento	Baja	Alto	MEDIO	Mitigar	Configurar Switch Alterno	Sistemas	
	Saturación del sistema		N/A			BAJO	Aceptar			
	Brecha de mantenimiento de sistemas	Acceso restringido	Los equipos no cuentan con un plan de mantenimiento	Baja	Alto	MEDIO	Mitigar	Configurar Switch Alterno y contratar servicio de mantenimiento	Sistemas	
Proxy Fortigate	**24**	**Control**	**Vulnerabilidad**	**Probabilidad de ocurrencia de la**	**Impacto en el negocio**	**Nivel de Riesgo**	**Estrategia de**	**Control a implementar**	**Responsable**	**Fecha Plazo**
Daños técnicos	Falla de equipos	Equipo de marca reconocida, Acceso restringido, Control de respaldos de configuraciones	Es el unico dispositivo que controla el flujo de información	Baja	Alto	MEDIO	Mitigar	Implementar un equipo espejo redundante para contingencia	Sistemas	
	Saturación del sistema		N/A			BAJO	Aceptar			
	Brecha de mantenimiento de sistemas	Equipo de marca reconocida, Acceso restringido, Control de respaldos de configuraciones	El personal no cuenta con capacitación acerca de su uso y configuración, no se cuenta con mantenimiento del	Baja	Alto	MEDIO	Mitigar	Capacitación al personal de Tecnología, y/o contratar mantenimiento del proveedor	Sistemas	

Figura 55. Análisis de equipos de Red

Realizado por: Investigador

Equipos Físicos – Servidor principal

Servidor principal	48	Control	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza	Impacto en el negocio	Nivel de Riesgo	Estrategia de respuesta	Control a implementar	Responsable	Fecha Plazo
Daños técnicos	Falla de equipos	Monitoreo del proveedor	Equipo descontinuado y sin mantenimiento	Media	Alto	ALTO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
	Saturación del sistema	Revisión de archivos log y procesos abiertos, capacidad técnica adecuada		Baja	Alto	MEDIO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
	Brecha de mantenimiento de sistemas	Monitoreo del proveedor	Equipo descontinuado y sin mantenimiento	Media	Alto	ALTO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
Acciones no autorizadas	Uso no autorizado de equipos	Bitácoras de control de acceso a áreas restringidas	N/A	Baja	Bajo	BAJO	Aceptar			
	Copia fraudulenta de software	Acceso restringido	N/A	Baja	Bajo	BAJO	Aceptar			
	Uso de software pirata	Inventario de Software con licencias y Software Libre	N/A	Baja	Bajo	BAJO	Aceptar			
	Corrupción de datos	Monitoreo del proveedor	N/A	Baja	Bajo	BAJO	Aceptar			
	Procesamiento ilegal de datos	Acceso restringido	N/A	Baja	Bajo	BAJO	Aceptar			
Compromiso de funciones	Error en el uso	Acceso restringido	N/A	Baja	Bajo	BAJO	Aceptar			
	Abuso de privilegios	Control mediante bitácora de actividades	N/A	Baja	Bajo	BAJO	Aceptar			
	Denegación	Monitoreo del proveedor	N/A	Baja	Bajo	BAJO	Aceptar			
	Brecha de disponibilidad de personal	Monitoreo del proveedor	N/A	Baja	Bajo	BAJO	Aceptar			
Fraudes o ataques	Hacking, cracking	Seguridad perimetral provista por el proveedor del housing	N/A	Baja	Bajo	BAJO	Aceptar			
	Delitos informáticos	Control en los accesos al computador tanto físicos como lógicos	N/A	Baja	Bajo	BAJO	Aceptar			
	Terrorismo	N/A	N/A	Baja	Bajo	BAJO	Aceptar			
	Espionaje industrial	N/A	N/A	Baja	Bajo	BAJO	Aceptar			
	Intrusión, negligencia	N/A	N/A	Baja	Bajo	BAJO	Aceptar			

Figura 56. Análisis Equipos Físicos - Servidor principal

Realizado por: Investigador

Equipos Físicos – Servidor Branch

Servidor branch	48	Control	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza	Impacto en el negocio	Nivel de Riesgo	Estrategia de respuesta	Control a implementar	Responsable	Fecha Plazo
Daños técnicos	Falla de equipos		Servidor Branch descontinuado y sin mantenimiento	Media	Alto	ALTO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
	Saturación del sistema	Revisión de archivos log y procesos abiertos	Módulos del sistema que consumen recursos altos dentro del servidor, disco cercano al máximo de su capacidad de almacenamiento	Media	Alto	ALTO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
	Brecha de mantenimiento de sistemas		Servidor Branch descontinuado y sin mantenimiento	Media	Alto	ALTO	Mitigar	Migración al nuevo core financiero	Tecnología	01-ene-19
Acciones no autorizadas	Uso no autorizado de equipos	Bitácoras de control de acceso a áreas restringidas, cámaras de vigilancia	El control de acceso al data center local es manual	Baja	Bajo	BAJO	Aceptar			
	Copia fraudulenta de software	Bitácoras de control de acceso a áreas restringidas, cámaras de vigilancia	Puertos USB habilitados	Baja	Bajo	BAJO	Aceptar			
	Uso de software pirata	Inventario de Software con licencias y Software Libre	No se cuenta con un inventario de software instalado	Media	Medio	MEDIO	Mitigar	Efectuar un inventario de software instalado, con un snifer	Tecnología	
	Corrupción de datos	Bitácoras de control de acceso a áreas restringidas, cámaras de vigilancia	N/A	Baja	Bajo	BAJO	Aceptar			
	Procesamiento ilegal de datos	Acceso restringido	N/A	Baja	Bajo	BAJO	Aceptar			
Compromiso de funciones	Error en el uso	Acceso restringido	N/A	Baja	Media	BAJO	Aceptar			
	Abuso de privilegios	Control mediante bitácora de actividades	N/A	Baja	Media	BAJO	Aceptar			
	Denegación	Control de usuarios en el terminal	N/A	Media	Media	BAJO	Aceptar			
	Brecha de disponibilidad de personal	N/A	N/A	Baja	Bajo	BAJO	Aceptar			

Figura 57. Análisis Equipos Físicos – Servidor Branch

Realizado por: Investigador

Software – SyBase

Sybase	64	Control	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza	Impacto en el negocio	Nivel de Riesgo	Estrategia de respuesta	Control a implementar	Responsable	Fecha Plazo
Daños técnicos	Mal funcionamiento del software	Control de acceso a los módulos mas pesados que implican conexión a las tablas con mas información	Consultas muy pesadas para los módulos	Baja	Medio	BAJO	Aceptar			
	Saturación del sistema	Control del rendimiento del CPU y memoria RAM del servidor branch	Saturación de la BDD al realizar consultas	Baja	Baja	BAJO	Aceptar			
	Brecha de mantenimiento de sistemas	Solicitudes de mejora en el rendimiento de la BDD a través de la mesa de ayuda	No existe una planificación para mantenimientos de BDD y su rendimiento de manera física	Baja	Media	BAJO	Aceptar			
Acciones no autorizadas	Uso no autorizado de equipos	Acceso a la Base de Datos por perfil de usuario	N/A	Baja	Media	BAJO	Aceptar			
	Copia fraudulenta de software	Bloqueo de copias de bases de datos	N/A	Baja	Baja	BAJO	Aceptar			
	Uso de software pirata	Bloqueo de permisos de instalación de software y que solo el departamento de sistemas pueda realizarlo	N/A	Baja	Baja	BAJO	Aceptar			
	Corrupción de datos	Base de Datos normalizada bajo estandares internacionales	N/A	Baja	Alto	MEDIO	Mitigar	Implementar controles de validación de información	Cobis Corp.	
	Procesamiento ilegal de datos	Validar tablas de auditoria regularmente	N/A	Baja	Alto	MEDIO	Mitigar	Implementar controles de validación de información	Cobis Corp.	
Compromiso de funciones	Error en el uso	Acceso de administrador a la base de datos contralada	Desconocimiento de las tablas en el área de sistemas de la Cooperativa.	Baja	Media	BAJO	Aceptar			
	Abuso de privilegios	Acceso a la Base de Datos por perfil de usuario	Fácil ejecución de scripts que afecten a la base de datos y su información	Baja	Baja	BAJO	Aceptar			
	Denegación	Disponibilidad del servicio de BDD	N/A	Baja	Media	BAJO	Aceptar			
	Brecha de disponibilidad de personal	Configuración del control del servidor de manera remota	N/A	Baja	Media	BAJO	Aceptar			
Compromiso de la información	Revelación	Contratos de confidencialidad de información entre el proveedor y el cliente	N/A	Baja	Alto	MEDIO	Mitigar	Crear compromiso de confianza	Coop. Maquita Cushunchic Ltda.	
	Datos de fuentes no confiables	Scripts y reportes validadospor proveedor y cliente	N/A	Baja	Media	BAJO	Aceptar			

Figura 58. Análisis Software – SyBase

Realizado por: Investigador

Software – Cobis

Cobis	48	Control	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza	Impacto en el negocio	Nivel de Riesgo	Estrategia de respuesta	Control a implementar	Responsable	Fecha Plazo
Daños técnicos	Mal funcionamiento del software	Controlar los procesos que se ejecutan a través del terminal del servidor	Conexiones lentas hacia las agencias	Media	Media	BAJO	Aceptar			
	Saturación del sistema	Control de consumo de ancho de banda mediante proxy	Saturación del enlace principal hacia las agencias	Media	Media	BAJO	Aceptar			
	Brecha de mantenimiento de sistemas	Limpieza preventiva de impresoras, escaner y cpu	No se realiza ningún plan de mantenimiento de equipos de computo de los clientes	Baja	Media	BAJO	Aceptar			
Acciones no autorizadas	Uso no autorizado de equipos	Acceso mediante Active Directory	N/A	Baja	Baja	BAJO	Aceptar			
	Copia fraudulenta de software	Uso de software libre	Existe acceso libre para conexión de dispositivos externos	Baja	Baja	BAJO	Aceptar			
	Uso de software pirata	Uso de software libre	Instalación de nuevos software no se encuentra controlado en equipos de los clientes	Baja	Baja	BAJO	Aceptar			
	Corrupción de datos	Control de información de clientes y empleados se protege a través del software FINEWARE	Ingreso de información falsa a través de los asesores	Baja	Alto	MEDIO	Mitigar	Validación diaria de información ingresada	Coop. Maquita Cushunchic Ltda.	
	Procesamiento ilegal de datos	La información antes de ser registrada se procesa a través de varios filtros	N/A	Baja	Baja	BAJO	Aceptar			
Compromiso de funciones	Error en el uso	Accesos controlados a cada uno de los módulos	N/A	Baja	Media	BAJO	Aceptar			
	Abuso de privilegios	Acceso por perfiles a los módulos	N/A	Baja	Baja	BAJO	Aceptar			
	Denegación	N/A	N/A	Baja	Baja	BAJO	Aceptar			
	Brecha de disponibilidad de personal	Personal backup para cada área	Vacaciones por ley de los trabajadores	Baja	Baja	BAJO	Aceptar			
Compromiso de la información	Revelación	Convenios de confidencialidad de información entre el proveedor y el cliente	Venta de información de clientes por parte del proveedor del servicio	Baja	Baja	BAJO	Aceptar			
	Datos de fuentes no confiables	Manejo de fuentes controladas por el proveedor del servicio	N/A	Baja	Baja	BAJO	Aceptar			

Figura 59. Análisis Software – Cobis

Realizado por: Investigador

Software – SPI Banco Central

SPI BCE	24	Control	Vulnerabilidad	Probabilidad de ocurrencia de la amenaza	Impacto en el negocio	Nivel de Riesgo	Estrategia de respuesta	Control a implementar	Responsable	Fecha Plazo
Daños técnicos	Mal funcionamiento del software	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Saturación del sistema	Control de consumo de ancho de banda mediante proxy	N/A	Baja	Media	BAJO	Aceptar			
	Brecha de mantenimiento de sistemas	N/A	N/A	Baja	Media	BAJO	Aceptar			
Acciones no autorizadas	Uso no autorizado de equipos	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Copia fraudulenta de software	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Uso de software pirata	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Corrupción de datos	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Procesamiento ilegal de datos	N/A	N/A	Baja	Media	BAJO	Aceptar			
Compromiso de funciones	Error en el uso	Personal calificado para el manejo del software	N/A	Baja	Media	BAJO	Aceptar			
	Abuso de privilegios	Personal calificado para el manejo del software	N/A	Baja	Media	BAJO	Aceptar			
	Denegación	N/A	N/A	Baja	Media	BAJO	Aceptar			
	Brecha de disponibilidad de personal	N/A	N/A	Baja	Media	BAJO	Aceptar			
Compromiso de la información	Revelación	Manejo de fuentes controladas por el proveedor del servicio	N/A	Baja	Media	BAJO	Aceptar			
	Datos de fuentes no confiables	N/A	N/A	Baja	Media	BAJO	Aceptar			

Figura 60. Software – SPI Banco Central

Realizado por: Investigador

Personal

		Supervisor Operativo	Jefes de agencia	Jefe de Control Financiero	Asesoras	Analistas de crédito	Operador de Tecnología			
		48	48	32	32	27	24			
Personal	**GRUPO 1**	**Control**	**Vulnerabilidad**	**Probabilidad de ocurrencia de la amenaza**	**Impacto en el negocio**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Control a implementar**	**Responsable**	**Fecha Plazo**
Acciones no autorizadas	Procesamiento ilegal de datos	Firma de acuerdos de confidencialidad y accessos unicos a los usuarios de cada sistema	N/A	Alta	Alta	MEDIO	Mitigar	Generar perfiles de accesos a los usuarios en cada sistema que se usa y sus módulos	Procesos, Recursos Humanos	
Personal	Enfermedad	Chequeos priódicos del personal	Los espacios de trabajo no se encuentran temperados	Alta	Alta	MEDIO	Mitigar	Mantener personal backup para las áreas afectadas	Procesos, Recursos Humanos	
	Accidentes industriales	Capacitación Salud Ocupacional	No todos los espacios de trabajo se encuentran señalizados	Bajo	Bajo	BAJO	Aceptar			
	Alta rotación del personal	Capacitación en los procesos del core financiero y proveedores	El personal de las agencias lejanas recorren varios kilometros para llegar a sus lugares de trabajo	Bajo	Medio	BAJO	Aceptar			
	Clima laboral	Evaluaciones periódicas de satisfacción del empleado	S/N	Bajo	Bajo	BAJO	Aceptar			
	Negligencia	Pruebas de conocimiento	Falta capacitación en el personal acerca del uso adecuado de equipos de información	Bajo	Bajo	BAJO	Aceptar			
Compromiso de funciones	Error en el uso	Validación en campos de entrada y generación de procesos	S/N	Bajo	Bajo	BAJO	Aceptar			
	Abuso de privilegios	Generar perfiles de acceso por usuario o por grupo de usuarios	S/N	Bajo	Medio	BAJO	Aceptar			
	Denegación	Generar perfiles de acceso por usuario o por grupo de usuarios	S/N	Bajo	Medio	BAJO	Aceptar			
	Brecha de disponibilidad de personal	Mantener capacitado al personal denominado backup para su desempeño en cualquier área	S/N	Bajo	Bajo	BAJO	Aceptar			

}

Figura 61. Personal

Realizado por: Investigador

Proveedores

	Proveedores	Telconet	Eqysum	Cobiscorp	Seguridad privada RAV	Banco Central
		48	48	36	36	27
CONTROLES	Contrato formal	SI	SI	SI	SI	SI
	Cláusula / Acuerdo de confidencialidad	SI	SI	SI	NO	NO
	Propiedad intelectual	NO	NO	SI	NO	NO
	Está contratado otro proveedor para el mismo servicio	SI	NO	NO	NO	NO
	Existen otros proveedores en el mercado	SI	SI	SI	SI	SI
	Se ha probado con el proveedor su plan de contingencia	NO	NO	NO	NO	NO
	Se ha realizado transferencia de conocimiento	NO	NO	SI	NO	SI
	Se ha entregado documentación técnica y de usuario	NO	NO	SI	NO	SI
	Se verifica cada mes la entrega de los niveles de servicio	SI	NO	SI	SI	SI
	Existe garantía técnica, de mantenimiento o de otro tipo	NO	NO	SI	NO	SI

Figura 62. Cumplimiento proveedores

Realizado por: Investigador

	COMENTARIOS	Riesgo de incumplimiento en la entrega del servicio debido a que no existe validación de un plan de contingencia que permita solventar algún tipo de incidente. Alta dependencia del proveedor	Existe riesgo de que como servicio alterno no funcione ya que no se encuentra validado su disponibilidad al suscitarse un incidente	Alta dependencia del proveedor, riesgo de incumplimiento en la entrega del servicio por no existir un plan de contingencia ante algún incidente.	Alta dependencia del proveedor por restricción contractual	Riesgo de demoras en la entrega del soporte por falta de SLA
	Probabilidad de ocurrencia de la amenaza	Baja	Baja	Baja	Baja	Baja
	Impacto en el negocio	Alto	Alto	Alto	Baja	Alto
	Nivel de Riesgo	MEDIO	MEDIO	MEDIO	BAJO	MEDIO
	Estrategia de respuesta	Mitigar	Mitigar	Mitigar	Aceptar	Mitigar
	Control a implementar	Implementar un plan de contingencia con otro proveedor y validar su funcionamiento	Realizar puruebas constantes de su correcto funcionamiento	Implementar un plan de contingencia, validando tiempos de respuesta en caso de que el servicio se mantenga caído por mas de 4 horas		Validar conexiones y su tiempo de respuesta a la Central
	Responsable	Sistemas	Sistemas	Sistemas		Sistemas
	Fecha Plazo					

Figura 63. Análisis de Proveedores

Realizado por: Investigador

El análisis realizado a cada activo permite obtener una visión más clara de aquellos que requieren mayor atención y por ende gestionar los métodos o técnicas que permitan mitigar sus riesgos.

6.7.4. FASE 4: Declaración de Aplicabilidad

La declaratoria de Aplicabilidad se refiere a que, una vez generado las políticas de seguridad de información, se pueda validar si se están aplicando o no dentro de la Cooperativa y de no ser así, se procede a generar un plan de acción, el responsable de la ejecución y la fecha.

Un plan de acción no se aplica siempre y cuando el cumplimiento de la política sea en su totalidad, de lo contrario se genera uno y a su vez se le asigna un responsable y la fecha de máxima de ejecución. Con esto se busca obtener un nivel de efectividad superior al riesgo inherente y este último a su vez se busca convertir en riesgo residual.

A continuación, se muestra cual es el análisis de cumplimiento de las políticas de seguridad validado (**Ver Anexo 2**) de acuerdo a cada uno de los dominios.

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
1. Aspectos organizativos de la seguridad de la información	1.1. Toda la información generada, ingresada, almacenada, procesada, transmitida u obtenida por cualquier medio en los equipos de la Cooperativa, es de propiedad de la Cooperativa Maquita Cushunchic, por lo que todo usuario de la misma deberá suscribir un Acuerdo de Confidencialidad previo a su acceso.				X		Area de Procesos	
	1.2. Las necesidades de seguridad en la información, así como sus medidas de protección, serán definidas en conjunto por la Unidad de Riesgos y el Comité Gerencial, de acuerdo con su grado de criticidad y sensibilidad.				X			
	1.3. La Unidad de Tecnología implementará las medidas de seguridad informática requeridas, y realizará el monitoreo permanente de su correcto funcionamiento.		X			Coordinar con la Jefatura de Riesgos la implementación de las medidas de seguridad informática requeridas y definir el procedimiento de monitoreo	Jefe de Tecnología	
	1.4. La Jefatura de Riesgos deberá monitorear al menos anualmente el cumplimiento y efectividad de las políticas de seguridad de la información en las personas, procesos y tecnología de información de la Cooperativa, y coordinará la verificación de la efectividad de las medidas de seguridad informática implementadas, a través del análisis y gestión de vulnerabilidades.Cooperativa, y coordinará la verificación de la efectividad de las medidas de seguridad informática implementadas.		X			Elaborar un inventario de las medidas de seguridad a ser monitoreadas y definir el procedimiento periódico de monitoreo	Jefe de Riesgos	
	1.5. Auditoría Interna realizará el seguimiento hasta su regularización, de los casos de incumplimiento detectados por el área de Riesgos.			X		Impulsar el uso de la mesa de ayuda y definir procedimientos de monitoreo		
	1.6. La presente Política será revisada al menos de forma anual, para verificar su rendimiento, efectividad y alineamiento a los objetivos estratégicos institucionales.		X			Aprobar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	Jefe de Procesos	
	TOTAL	**0**	**3**	**1**	**2**			

Figura 64. Cumplimiento política de aspectos organizativos de la seguridad de la información

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
2. Seguridad relacionada con los recursos humanos	2.1. La Jefatura de Soporte deberá asegurarse de que se realice la verificación de antecedentes de las personas a ser contratadas, para aquellos cargos que manejen información crítica o sensible de la Cooperativa.				**X**			
	2.2. La Jefatura de Riesgos será la responsable de capacitar al personal en todos los temas relacionados a seguridad de información, como parte de la creación de una cultura organizacional para la gestión de riesgos.				**X**			
	2.3. La Jefatura de Soporte conjuntamente con Tecnología eliminarán todos los accesos y documentos de identificación corporativos al empleado, y verificarán la devolución de los activos a su cargo, al momento de su desvinculación de la Cooperativa.				**X**			
	2.4. El incumplimiento de la política de seguridad será considerado falta grave cuando ocasione riesgos de tipo económico, legal, operacional o reputación para la Cooperativa, y conllevará las sanciones establecidas en el Reglamento de Trabajo.				X			
	TOTAL	**0**	**0**	**0**	**4**			

Figura 65. Cumplimiento política de seguridad relacionada con los recursos humanos

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
3. Gestión de activos	3.1. La identificación de necesidades de seguridad se inicia con la elaboración y mantenimiento del inventario de activos de información, por lo que su actualización debe ser permanente.		X			Documentar los activos que mantiene cada usuario, con sus nombres, area, sucursal, serie, marca y modelo del activo y que se mantenga actualizado al finalizar el año		
	3.2. El área de Tecnología se encargará de mantener actualizado el inventario de los activos tecnológicos y los que permiten la gestión de la información de la cooperativa, durante su creación, procesamiento, almacenamiento, transmisión, uso o eliminación de los datos, en cualquier plataforma que decida utilizar la Cooperativa.	X				Coordinar con la Jefatura de Soporte que el parque informático sea actualizado en el sistema periódicamente Elaborar el plan de seguridad de la información para cubrir las necesidades de protección de los activos	Jefe de Tecnología Jefe de Riesgos	
	3.3. El registro contable de todos los activos de la Cooperativa y su cuadre con el inventario actualizado será de responsabilidad del área de Contabilidad.				X			
	3.4. El esquema de clasificación de la información será definido por la Jefatura de Riesgos, y considerará la criticidad y sensibilidad de la misma, así como los medios de almacenamiento físico y magnético.			X		Implementar un sistema de respaldos de información y que este se encargue de salvaguardar la información que en su configuración haya sido predeterminada	Jefe de Tecnología Jefe de Riesgos	
	3.5. La clasificación y determinación de las medidas de protección a implementar en la información, será de responsabilidad del Comité Gerencial conjuntamente con la Jefatura de Riesgos, mientras que el etiquetado, manipulación y gestión de los activos que se relacionan con TI será responsabilidad del área de Tecnología.		X			Implementar un control de Vida útil del activo, el mismo permita llevar un control de todas las actividades realizadas en el mismo y validado una vez al año	Jefe de Tecnología Jefe de Riesgos Comité Gerencial	
	3.6. Los puertos de conexión para medios extraíbles de información estarán inhabilitados en los equipos de la Cooperativa, salvo que su uso esté justificado y aprobado formalmente por la Gerencia.		X			Implementar politicas de acceso y restricción el en servidor de Active Directory y definir el procedimiento de monitoreo	Jefe de Tecnología	
	3.7. Los dispositivos móviles que no sean de propiedad de la Cooperativa y requieran conectarse a su red o recursos tecnológicos, serán previamente autorizados por la Gerencia, y deberán incorporar las protecciones mínimas definidas por el área de Tecnología para evitar intrusiones de terceros.			X		Aprobar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	Jefe de Procesos	
	TOTAL	1	2	2	1			

Figura 66. Cumplimiento política de gestión de activos

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO	CUMPLE			PLAN DE ACCIÓN
			PARCIAL	ALTO	TOTAL	
4. Control de accesos	4.1. Todo acceso a los sistemas y recursos de la Cooperativa se realizará según el perfil del usuario y las funciones a él asignadas. Los permisos de acceso asignados a cada perfil de usuario deberán estar documentados y actualizados para posteriores revisiones de las áreas de control.				X	
	4.2. El acceso no autorizado a información sensible de la Cooperativa, será imputado al responsable de su custodia, o dueño del usuario con el que se realizó el acceso.				X	
	4.3. La Jefatura de Soporte será la responsable de otorgar, modificar y revocar los permisos de acceso a los sistemas y recursos de red de la Cooperativa, los cuales se asignarán según el rol de cada persona y bajo los principios de la necesidad de saber y del mínimo privilegio para el cumplimiento de sus funciones.				X	
	4.4. La Jefatura de Tecnología será responsable de establecer esquemas de seguridad para el acceso del personal a los recursos tecnológicos y de red de la Cooperativa, tanto para usuarios internos como externos.				X	
	4.5. En el acceso a información sensible de sistemas o recursos de la Cooperativa se aplicará doble factor de autenticación (dos de tres: algo que sabe, algo que tiene, algo que es).		X			Aprobar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento
	4.6. Las contraseñas de usuarios deberán cambiarse al menos cada 90 días, tanto para el acceso a la red como a los sistemas, y deberán configurarse con al menos 8 caracteres que incluyan mayúsculas, minúsculas y números.		X			Aprobar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento
	4.7. No se permitirá reutilizar contraseñas históricas que se hayan utilizado en los últimos 6 meses.		X			Aprobar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento
	4.8. No se otorgarán usuarios compartidos, excepto en el caso de abogados externos de una misma firma, o auditores externos en cuyo caso el acceso será exclusivamente de consulta.				X	
	4.9. Auditoría Interna controlará al menos anualmente, que los accesos a los sistemas y recursos de la Cooperativa se hayan concedido considerando las autorizaciones otorgadas por el área de Soporte.				X	
	4.10. El acceso de terceros a reportes o listados con información sensible de la Cooperativa, deberá ser solicitado por la línea de supervisión del área a la Gerencia, y será otorgado previo la firma de una cláusula o acuerdo de confidencialidad.				X	
	TOTAL	0	3	0	7	

Figura 67. Cumplimiento política de control de accesos

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
5. Cifrado	5.1. Los sistemas que requieran cifrado o encriptación para la transmisión de datos mantendrán su contraseña compartida bajo la custodia de dos jefaturas, cada una de las cuales conocerá solo su mitad de la contraseña.				X			
	5.2. Las mitades de las contraseñas se almacenarán en un sobre sellado en la bóveda de la oficina matriz, y su acceso será autorizado por la Gerencia.				X			
	TOTAL	0	0	0	2			

Figura 68. Cumplimiento política de cifrado

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
6. Seguridad física y ambiental	6.1. Las áreas restringidas de la Cooperativa son los centros de procesamiento de datos, tanto el interno como el provisto por terceros, a los cuales solo tendrán acceso los Jefes de Tecnología y Soporte, y el Operador de Sistemas. Los proveedores o terceros que requieran acceso para mantenimiento o soporte de los equipos, únicamente ingresarán acompañados por uno de los funcionarios autorizados, quienes registrarán el acceso en una bitácora de visitas.				X			
	6.2. El acceso a las oficinas y agencias de la Cooperativa estará custodiado y registrado por el personal de seguridad. Todo tercero que requiera acceso a las oficinas deberá presentar una identificación previo a su ingreso, el cual deberá estar autorizado por la jefatura del área que visita.				X			
	6.3. Las agencias mantendrán operativas las cámaras de seguridad en las áreas donde se realicen transacciones u operaciones con los socios y clientes, las cuales serán monitoreadas por el Supervisor Operativo.				X			
	6.4. Todo incidente externo que afecte a la seguridad del personal de la Cooperativa y/o de su información, será notificado inmediatamente al personal de seguridad de cada oficina, y a las jefaturas de Riesgos y Soporte mediante correo electrónico. Tales incidentes pueden referirse a desastres naturales, ataques maliciosos, daños de equipos o accidentes.				X			

Figura 69. Cumplimiento política de seguridad física y ambiental - I

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
6. Seguridad física y ambiental	6.5. Las estaciones de trabajo deberán mantener condiciones seguras para trabajar, por lo que sus responsables se asegurarán de que no se encuentren cajones abiertos u obstáculos para la salida del personal, ni exista material combustible, líquidos u otras sustancias que puedan afectar a las personas, y los equipos y soportes de información.				X			
	6.6. Los equipos y dispositivos portátiles estarán en todo momento bajo la custodia de su responsable. De ser necesario, su información estará encriptada y protegida con contraseña para su acceso.				X			
	6.7. Los equipos y dispositivos críticos para la entrega de servicios a los socios y clientes de la Cooperativa, contarán con un suministro de energía alterno, que entrará en funcionamiento en caso de presentarse un corte de energía eléctrica, y tendrá capacidad para soportar la				X			
	6.8. El cableado de energía y de telecomunicaciones deberá estar protegido contra interceptación, interferencia o daño.				X			
	6.9. Los equipos, impresoras y dispositivos de la Cooperativa deberán estar sujetos a un proceso de mantenimiento preventivo a realizarse al menos de forma anual, que garantice su correcto y oportuno funcionamiento.		X			Implementar un cronograma de actividades que permita de manera anual dar mantenimiento a las computadoras e impresoras, tanto de la agencia matriz como de sucursales, debiendo ser reportado anualmente su realización mediante la hoja de vida de cada activo	Jefe de Sistemas	
	6.10. El retiro y traslado de equipos entre diferentes áreas de la Cooperativa deberá ser autorizado previamente por la Jefatura de Soporte, y actualizado por el área de Tecnología en el inventario de activos.		X			Implementar una bitácora de movimiento de activos, el mismo que permita mantener un control sobre los activos removidos entre agencias		

Figura 70. Cumplimiento política de seguridad física y ambiental – II

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
	6.11. Antes de descartar o reutilizar un equipo, se deberá garantizar el borrado seguro de la información sensible o software con licencia que éste pudiera contener.				X			
	6.12. Cada usuario será responsable de no dejar desatendido su equipo, y en caso de requerir ausentarse, deberá dejarlo bloqueado para impedir el acceso no autorizado.				X			
	6.13. Los escritorios y estaciones de trabajo no deberán mantener documentación sensible desprotegida, que pueda ser visualizada o sustraída por personas ajenas a dicha estación de trabajo.				X			
	TOTAL	0	2	0	11			

Figura 71. Cumplimiento política de seguridad física y ambiental

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
7. Seguridad operativa	7.1. Las políticas, procesos e instructivos operativos de la Cooperativa, deberán estar documentados y disponibles para su consulta por parte de todos los usuarios que los necesiten.		X			Implementar el ambiente de SharePoint en donde se encuentren todos los procesos y archivos, permita el acceso por perfiles de usuario	Jefe de Tecnología Jefe de Procesos	
	7.2. Todos los cambios a la documentación, procesos, sistemas o instalaciones de la institución que afectan a la confidencialidad, integridad o disponibilidad de la información deberán ser controlados, autorizados y documentados.				X			
	7.3. Para garantizar el adecuado desempeño de los sistemas, el área de Tecnología deberá ejecutar el proceso de Administración de la Disponibilidad y Capacidad de los recursos, de forma proactiva.		X			Implementar un plan de capacitación técnica máximo de forma anual para el personal del área de sistemas	Jefe de Soporte	
	7.4. El área de Tecnología deberá garantizar la provisión de ambientes separados para los entornos de pruebas y producción para evitar cambios no autorizados en el entorno operacional.			X		Implementar el ambiente de pruebas en el nuevo core financiero	Jefe de Tecnología	
	7.5. El área de Tecnología mantendrá actualizado el software y procedimientos que permitan detectar, prevenir y recuperarse de afectaciones de código malicioso.				X	Implementar una bitácora de actividades para el monitoreo del antivirus y que se lo haga al menos una vez a la semana	Jefe de Tecnología	
	7.6. El área de Riesgos promoverá en el personal la concientización en el uso adecuado de los recursos de la Cooperativa.				X			

Figura 72. Cumplimiento política de seguridad operativa -I

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
	7.7. El área de Tecnología realizará pruebas regulares de las copias de respaldo de la información, del software y de las imágenes del sistema, para validar su integridad y recuperación de los datos.				X			
	7.8. El área de Riesgos definirá y revisará regularmente las pistas de auditoría para identificar excepciones, fallas y eventos de seguridad de la información, y coordinará la implementación de medidas de seguridad para su protección.				X			
	7.9. El área de Tecnología mantendrá sincronizados los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Cooperativa así como del servidor de dominio, con relación a una fuente de sincronización única de referencia.				X			
	7.10. El área de Tecnología deberá mantener procedimientos para identificar el software no autorizado que se encontrare en los equipos de la Cooperativa, así como mantener control sobre la instalación de software a través del Directorio Activo.		X			Implementar políticas de permisos de instalación de software dentro del Active Directory	Jefe de Tecnología	
	7.11. El área de Riesgos planificará con la Gerencia el alcance, duración y fechas para la realización de las actividades periódicas de auditoría informática para minimizar las interrupciones en los procesos del negocio.				X			
	TOTAL	**0**	**3**	**1**	**7**			

Figura 73. Cumplimiento política de seguridad operativa -II

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
8. Seguridad en las telecomunicaciones	8.1. El área de Tecnología coordinará la configuración y arquitectura de los servicios de red de manera que se evite el acceso físico no autorizado, daños e interferencias a la información y las instalaciones de procesamiento de la Cooperativa, a través de la segmentación, diseño de seguridad en profundidad, y otros controles apropiados.				X			
	8.2. El área de Tecnología mantendrá el control y monitoreo de todos los accesos a servicios internos (LAN / LAN) y externos (LAN / WAN) conectados a la red, manteniendo el equilibrio entre controles de seguridad y niveles de servicio en el desempeño.				X			
	8.3. La provisión de servicios de telecomunicaciones considerará la transferencia segura de información, así como acuerdos o cláusulas de confidencialidad.				X			
	TOTAL	0	0	0	3			

Figura 74. Cumplimiento de política de seguridad en las telecomunicaciones

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
9. Adquisición, desarrollo y mantenimiento de sistemas	9.1. Los proyectos de desarrollo de sistemas nuevos o de mejoras a los existentes, establecerán las necesidades de seguridad de la información en la etapa de definición de requisitos, en los que se incluirá la aplicación de procedimientos de desarrollo seguros.				X			
	9.2. En la contratación de aplicaciones de terceros se incluirán medidas de protección contra fraudes, divulgación o modificación no autorizada de información, transmisión incompleta de datos, duplicación o reproducción de transacciones no autorizada, y enrutamiento alterado, según aplique.				X			
	9.3. Los análisis de vulnerabilidades a realizar periódicamente, deberán incluir la verificación de que sea hayan aplicado procedimientos de desarrollo seguros en los sistemas críticos de la Cooperativa.				X			
	9.4. El área de Tecnología verificará la aplicación de un proceso formal para el control de cambios, tanto en sistemas internos como en los provistos por terceros, y coordinará una revisión post-implementación con los usuarios para asegurar el correcto funcionamiento y evitar impactos no deseados.				X			
	9.5. En el plan de pruebas de los sistemas se incluirán criterios mínimos de aceptación del usuario, así como los requisitos de seguridad identificados				X			
	9.6. Los datos utilizados para la realización de pruebas de los sistemas, deberán contar con seguridades tales como enmascaramiento o sanitización para evitar la revelación no autorizada de datos sensibles de la Cooperativa o de sus socios.				X			
	TOTAL	0	0	0	6			

Figura 75.Cumplimiento de política de adquisición, desarrollo y mantenimiento de sistemas

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
10. Relaciones con proveedores	9.1. La Cooperativa mantendrá una política específica para la Administración de Proveedores, que incluirá lineamientos para garantizar la seguridad de la información.				X			
	TOTAL	**0**	**0**	**0**	**1**			

Figura 76. Cumplimiento política de relaciones con proveedores

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
11.Gestión de incidentes en la seguridad de la información	11.1. La Cooperativa mantendrá un proceso específico para la Administración de incidentes y problemas, que incluya la definición de responsabilidades para el reporte, registro, clasificación, resolución y revisión de los eventos de seguridad de la información.			X		La jefatura de Riesgos deberá presentar un informe mensual de registro de incidentes a través de la mesa de ayuda implementada por el área de tecnología	Jefatura de Riesgos	
	TOTAL	**0**	**0**	**1**	**0**			

Figura 77. Cumplimiento de política de gestión de incidentes en la seguridad de la información

Desarrollado por: Investigador

POLÍTICA	CRITERIO	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
12. Gestión de la continuidad del negocio	12.1. La Cooperativa mantendrá una política específica para la gestión de la Continuidad del Negocio, que incluirá lineamientos para garantizar la aplicación de medidas para proteger la confidencialidad, integridad y disponibilidad de los datos durante situaciones de contingencia o desastre, así como la revisión periódica de la validez y eficacia de los controles establecidos.				X			
	TOTAL	**0**	**0**	**0**	**1**			

Figura 78. Cumplimiento de política de gestión de la continuidad del negocio

Desarrollado por: Investigador

POLÍTICA	CRITERIOS	NO CUMPLE	CUMPLE			PLAN DE ACCIÓN	RESPONSABLE	FECHA
			PARCIAL	ALTO	TOTAL			
13. Cumplimiento	13.1. El área de Riesgos deberá identificar, documentar y mantener actualizados todos los requisitos estatutarios, normativos y contractuales relativos a la seguridad de la información, junto a los planes de la Cooperativa para cumplirlos.				X			
	13.2. En la identificación de riesgos de los procesos de la Cooperativa, se incluirán los escenarios de pérdidas, destrucción, falsificación, accesos y publicación no autorizados de la información.				X			
	TOTAL	**0**	**0**	**0**	**2**			

Figura 79. Política de Cumplimiento

Desarrollado por: Investigador

ATRIBUTOS DE CLASIFICACIÓN SEGÚN LA ISO 15504					
Se establece una escala de calificación cuyos valores se basan en el porcentaje de logro de los					
NO CUMPLE, no implementado (0-15%)					
PARCIAL, Parcialmente implementado (16-50%)					
ALTO, Ampliamente implementado (51-85%)					
TOTAL, completamente implementado (86-100%)					
DOMINIOS ISO 27001:2013	**TOTAL CRITERIOS**		**CUMPLEN**		
		NO CUMPLE	**PARCIAL**	**ALTO**	**TOTAL**
1. Aspectos organizativos de la seguridad de la información	6	0	3	1	2
2. Seguridad relacionada con los recursos humanos	4	0	0	0	4
3. Gestión de activos	7	1	2	2	1
4. Control de accesos	10	0	3	0	7
5. Cifrado	2	0	0	0	2
6. Seguridad física y ambiental	13	0	2	0	11
7. Seguridad operativa	11	0	3	1	7
8. Seguridad en las telecomunicaciones	3	0	0	0	3
9. Adquisición, desarrollo y mantenimiento de sistemas	6	0	0	0	6
10. Relaciones con proveedores	1	0	0	0	1
11.Gestión de incidentes en la seguridad de la información	1	0	0	1	0
12. Gestión de la continuidad del negocio	1	0	0	0	1
13. Cumplimiento	2	0	0	0	2
TOTAL	**67**	**1**	**13**	**5**	**47**
Porcentaje(%)	**111,67%**	**1,49%**	**19,40%**	**7,46%**	**70,15%**

Figura 80.Reporte de Cumplimiento por Política

Desarrollado por: Investigador

En la gráfica se puede validad que se cuenta con 67 políticas agrupadas en cada uno de los dominios de la ISO 27001, según corresponda, la misma que indica que 1 **NO CUMPLE** y eso corresponde al 1.49%, siendo necesario generar un plan de acción que permita que siempre se esté ejecutando, 13 políticas que corresponde al 19.40% si cumplen de manera **PARCIAL**, pero aun así requiere de un plan de acción, 5 políticas que corresponde al 7.46% ,tienen un cumplimiento **ALTO,** pero aun así requiere de un plan de acción, y 47 políticas cumplen al 100 por ciento y estas corresponden al 70.15% por lo tanto no requieren plan de acción, de la matriz obtenemos la siguiente gráfica.

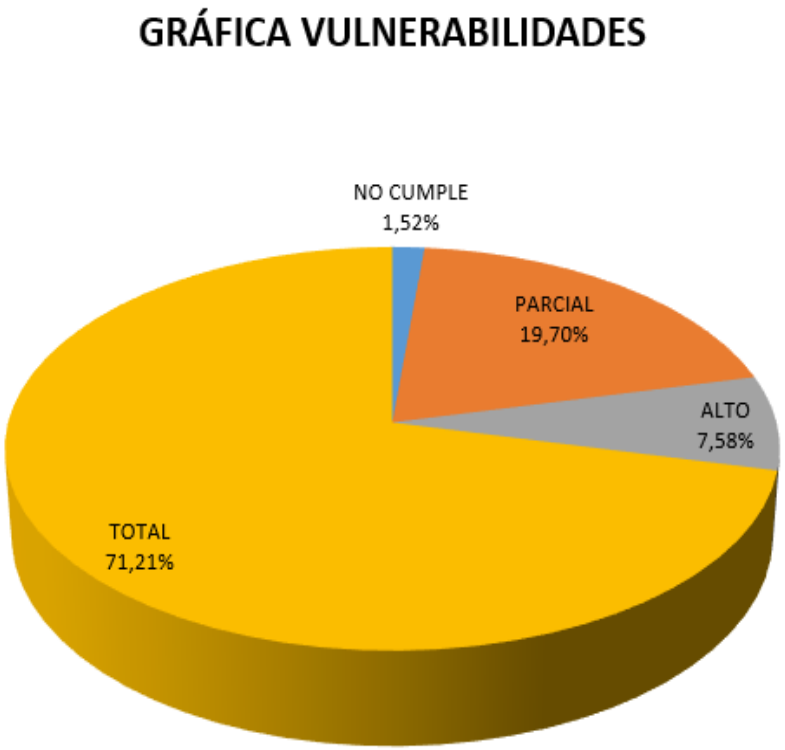


Figura 81. Gráfica Resumen General de Aplicabilidad

Desarrollado por: Investigador

6.7.5. FASE 5: Elaboración del Plan de Seguridad

Según (pmg-ssi, 2018), El Plan de seguridad supone:

"llevar a cabo los objetivos estratégicos que se identificaron en la política de seguridad y en las normativas vigentes de seguridad en la empresa, con el fin de ubicar a la organización, a nivel mundial, en un entorno de riesgo aceptable.".

Luego del análisis de riesgo realizado, se procede a realizar el Plan de Seguridad, encontrando que necesitamos aplicar Planes de Acción a los siguientes grupos de Activos:

- **INSTALACIONES FÍSICAS**
  - Data Center Century-Link
  - Data Center Local

- **COMPONENTES DE RED**
  - Switch Telconet
  - Switch Local
  - Proxy Fortigate

- **EQUIPOS FÍSICOS**
  - Servidor Principal
  - Servidor Branch

- **BASES DE DATOS Y SISTEMAS TRANSACCIONALES**
  - SyBase
  - Cobis

- **PERSONAL**
  - Personal

- **PROVEEDORES**
  - Telconet
  - Eqysum
  - Cobiscorp
  - Banco Central

- **CUMPLIMIENTO DE POLÍTICAS**

Para cada una de ellas, dependiendo su grado de Riesgo Inherente se aplicará un Plan de Acción que mitigue el Riesgo, en donde también se mide en Nivel de Efectividad para el mismo, estas acciones indican que el Riesgo Residual sea más bajo que el Inherente, como muestran las siguientes figuras.

Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Fenómenos sísmicos	MEDIO	Crear y ejecutar planes de contingencia que pemitan obtener tiempos de respuesta en el levantamiento del servicio Backup	ALTO	BAJO	Century Link	27/11/2018
Fenómenos volcánicos	MEDIO	Monitorear documentadamente el cumplimiento del cronograma de implementación del sitio de contingencia	MEDIO	BAJO	Century Link	18/02/2019
Fuego	MEDIO	Monitorear y revisar periodicamente las instalaciones y documentar las novedades encontradas que requieran acción inmediata	ALTO	BAJO	Sistemas	19/01/2019
Fenómenos climáticos	MEDIO	Monitorear la temperatura y humedad de forma periodica y documentar las observaciones que requieran acción inmediata para su control	ALTO	BAJO	Sistemas	20/03/2019
Falla del aire acondicionado	MEDIO	Mantenimiento preventivo según contrato entregado por el proveedor	ALTO	BAJO	Sistemas	21/04/2019
Espionaje remoto	MEDIO	Validación de las políticas de seguridad DOMINIO DE CIFRADO	ALTO	BAJO	Sistemas	22/05/2019
Datos de fuentes no confiables	MEDIO	Validar políticas de seguridad del Fortigate y documentar los cambios realizados	ALTO	BAJO	Sistemas	23/06/2019

Figura 82. Planes de Acción para Instalaciones Eléctricas

Desarrollado por: Investigador

Switch Telconet	Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Pérdida de servicios	Falla de telecomunicaciones	MEDIO	Control de etiquetado de cables que instalan los proveedores y documentar las observaciones	ALTO	BAJO	Sistemas	
Pérdida de servicios	Falla de telecomunicaciones	MEDIO	Validar el servicio de internet tanto el principal como el alterno y su documentar cada una de sus acciones	ALTO	BAJO	Sistemas	
Switch local	**Amenaza**	**Riesgo Inherente**	**Plan de Acción**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
Daños técnicos	Falla de equipos	MEDIO	Documentar los cambios realizados en cada uno de los equipos	ALTO	BAJO	Sistemas	
	Brecha de mantenimiento de sistemas	MEDIO	Implementar una hoja de vida de cada uno de los activos de computación	ALTO	BAJO	Sistemas	
Proxy Fortigate	**Amenaza**	**Riesgo Inherente**	**Control a implementar**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
Daños técnicos	Falla de equipos	MEDIO	Configurar un equipo de contingencia	ALTO	BAJO	Sistemas	
	Brecha de mantenimiento de sistemas	MEDIO	Presentar un plan de capacitación técnica para el área de sistemas	ALTO	BAJO	Sistemas	

Figura 83. Planes de Acción para Componentes de Red

Desarrollado por: Investigador

Servidor principal	Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Daños técnicos	Falla de equipos	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Saturación del sistema	MEDIO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Brecha de mantenimiento de sistemas	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	MEDIO	Sistemas	01-ene-19
Servidor branch	**Amenaza**	**Riesgo Inherente**	**Plan de Acción**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
Daños técnicos	Falla de equipos	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Saturación del sistema	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Brecha de mantenimiento de sistemas	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Uso de software pirata	MEDIO	Documentar el inventario de software instalado mediante un snifer	ALTO	BAJO	Sistemas	
Fraudes o ataques	Hacking, cracking	MEDIO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19
	Terrorismo	MEDIO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01-ene-19

Figura 84. Planes de Acción para Equipos Físicos

Desarrollado por: Investigador

Sybase	Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Acciones no autorizadas	Corrupción de datos	MEDIO	Documentar los controles de validación de información implementados	ALTO	BAJO	Cobis Corp.	
	Procesamiento ilegal de datos	MEDIO	Documentar los controles de validación de información implementados	ALTO	BAJO	Cobis Corp.	
Compromiso de la información	Revelación	MEDIO	Crear compromiso de confianza	MEDIO	BAJO	Coop. Maquita Cushunchic Ltda.	
Fraudes o ataques	Hacking, cracking	MEDIO	Configuración de equipos de encriptación de datos	ALTO	BAJO	Coop. Maquita Cushunchic Ltda.	
	Delitos informáticos	MEDIO	Configuración de equipos de encriptación de datos	ALTO	BAJO	Coop. Maquita Cushunchic Ltda.	
	Terrorismo	MEDIO	Configurar un equipo de contingencia	MEDIO	BAJO	Coop. Maquita Cushunchic Ltda.	
Cobis	**Amenaza**	**Riesgo Inherente**	**Plan de Acción**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
Acciones no autorizadas	Corrupción de datos	MEDIO	Documentar en una bitácora de la validación diaria de información ingresada los que se hayan encontrado con errores	ALTO	BAJO	Coop. Maquita Cushunchic Ltda.	

Figura 85. Planes de Acción para Bases de Datos y Sistemas Transaccionales

Desarrollado por: Investigador

Personal	Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Acciones no autorizadas	Procesamiento ilegal de datos	MEDIO	Documentar los perfiles de accesos a los usuarios para los módulos que han sido c reados	ALTO	BAJO	Procesos, Recursos Humanos	
Personal	Enfermedad	MEDIO	Crear un historial de enfermedades mas comunes que ocurren en las agencias	MEDIO	BAJO	Procesos, Recursos Humanos	
Fraudes o ataques	Hacking, cracking	MEDIO	Configuración de equipos de encriptación de datos	ALTO	BAJO	Sistemas	

Figura 86. Planes de Acción para Personal

Desarrollado por: Investigador

Telconet	Amenaza	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
	Desconexión del enlace principal	MEDIO	Validar el servicio del enlace tanto el principal como el alterno y documentar cada una de sus acciones	ALTO	BAJO	Sistemas	
Eqysum	**Amenaza**	**Riesgo Inherente**	**Plan de Acción**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
	Desconexión del enlace secundario	MEDIO	Validar el servicio del enlace tanto el principal como el alterno y documentar cada una de sus acciones	ALTO	BAJO	Sistemas	
Cobiscorp	**Amenaza**	**Riesgo Inherente**	**Plan de Acción**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
	Desconexión del sistema bancario	MEDIO	Documentar en una bitácora de actividadades las novedades encontradas durante el proceso de contingencia	ALTO	BAJO	Sistemas	
Banco Central	**Amenaza**	**Riesgo Inherente**	**Control a implementar**	**Nivel de Efectividad**	**Riesgo Residual**	**Responsable**	**Fecha Plazo**
	Desconexión del enlace del sistema c	MEDIO	Configurar el servidor proxy y medir tiempos de respuesta	ALTO	BAJO	Sistemas	

Figura 87. Planes de Acción para Proveedores

Desarrollado por: Investigador

Criterio	Amenaza	Riesgo Inherente	Control a implementar	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Medidas de seguridad Informática	Riesgo legal	MEDIO	Ejecutar en conjunto con la Jefatura de Riesgos la implementación de las medidas de seguridad informática requeridas y definir el procedimiento de monitoreo	ALTO	BAJO	Sistemas	
Cumplimiento de las políticas de seguridad	Riesgo legal	MEDIO	Publicar el inventario de las medidas de seguridad a ser monitoreadas y ejecutar un procedimiento periódico de monitoreo	ALTO	BAJO	Jefe de Riesgos	
Alineamiento de las políticas a alineamiento a los objetivos estratégicos institucionales	Riesgo legal	MEDIO	Aplicar la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	ALTO	BAJO	Jefe de Procesos	
Elaboración y mantenimiento del inventario de activos de información	Riesgo legal	MEDIO	Verificar los activos que mantiene cada usuario, con sus nombres, area, sucursal, serie, marca y modelo y que se mantenga actualizado al finalizar el año	ALTO	BAJO	Contabilidad	
Actualización del inventario de los activos tecnológicos	Riesgo legal	MEDIO	Implementar con la Jefatura de Soporte que el parque informático sea actualizado en el sistema periódicamente	ALTO	BAJO	Sistemas Jefe de Riesgos	
Clasificación y determinación de las medidas de protección a implementar en la información	Riesgo legal	MEDIO	Ejecutar el control de Vida útil del activo, el mismo que permita llevar un control de todas las actividades realizadas en el mismo y validado una vez al año	ALTO	BAJO	Sistemas Jefe de Riesgos Comité Gerencial	
Inhabilitación para medios extraíbles de información	Riesgo legal	MEDIO	Implementar politicas de acceso y restricción en el servidor de Active Directory y definir el procedimiento de monitoreo	ALTO	BAJO	Sistemas	

Figura 88. Planes de Acción para Cumplimiento de Políticas – I

Desarrollado por: Investigador

Criterio	Amenaza	Riesgo Inherente	Control a implementar	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo
Acceso a información sensible de sistemas o recursos de la Cooperativa	Riesgo legal	MEDIO	Ejecutar y monitorear la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	ALTO	BAJO	Jefe de Procesos	
Política de cambio periódico de contraseñas	Riesgo legal	MEDIO	Ejecutar y monitorear la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	ALTO	BAJO	Jefe de Procesos	
No reutilización de contraseñas históricas	Riesgo legal	MEDIO	Ejecutar y monitorear la Política de Seguridad de la Información y su proceso, y verificar anualmente su actualización y cumplimiento	ALTO	BAJO	Jefe de Procesos	
Disponibilidad de las políticas, procesos e instructivos operativos de la Cooperativa	Riesgo legal	MEDIO	Publicar el ambiente de SharePoint en donde se encuentren todos los procesos y archivos, y permita el acceso por perfiles de usuario	ALTO	BAJO	Sistemas Jefe de Procesos	
Adecuado desempeño de los sistemas de Información	Riesgo legal	MEDIO	Ejecutar un plan de capacitación técnica máximo de forma anual para el personal del área de sistemas	ALTO	BAJO	Jefe de Soporte	
Identificación de software no identificado	Riesgo legal	MEDIO	Ejecutar políticas de permisos de instalación de software dentro del Active Directory	ALTO	BAJO	Jefe de Soporte	

Figura 89. Planes de Acción para Cumplimiento de Políticas - II

Desarrollado por: Investigador

6.7.6. FASE 6: Diseño de Balanced ScoreCard a partir del Plan de Seguridad

El Balanced ScoreCard de este proyecto se encuentra dirigido al área gerencial para la toma de decisiones, de esta manera se podrá dar seguimiento a las actividades que se encuentran pronto a ejecutar, así como las actividades que ya han sido validadas. Es importante indicar que se encuentra distribuido de varias partes, como son:

1. Al ejecutar la combinación de **Actividades por vencer** y **Fecha de Control** de la **figura 90**, podremos observar los planes de acción prontas a llegar a esa fecha y saber si han sido ejecutadas y que nivel de cumplimiento se le ha asignado.

2. En este juego de opciones de la **figura 90** podremos ver las actividades que están a ejecutarse o ejecutadas en el **mes** y **año** indicado

3. En la **figura 91** podemos observar **una** gráfica de pastel que indica el nivel de porcentaje sumado a las varias opciones que mantiene cada plan de acción, sea este **NO, PARCIAL, ALTO y TOTAL.**

4. En la **figura 92 se** puede observar los planes de acción que pertenecen al juego de opciones realizadas en el punto 1 o 2, dependiendo de lo seleccionado.

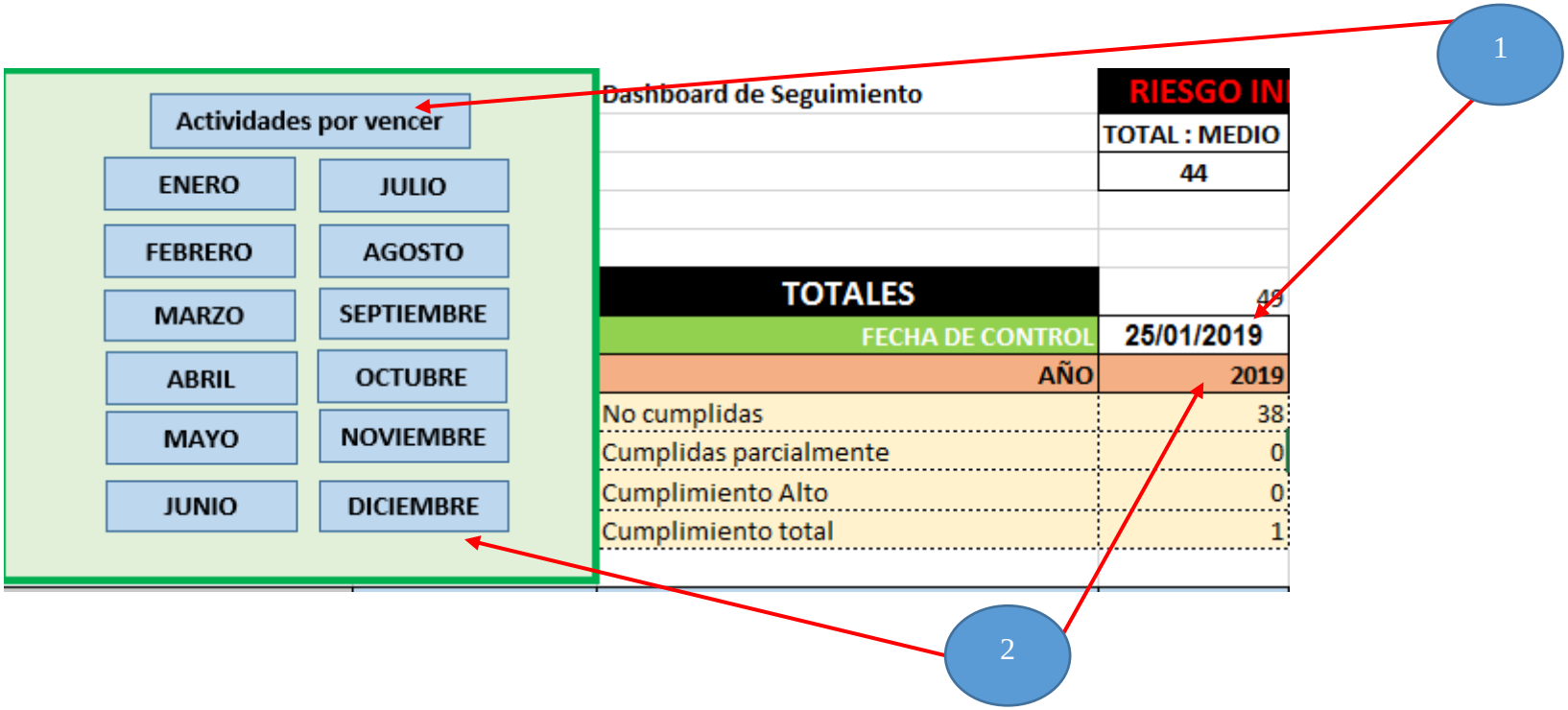


Figura 90. Opciones de Consulta

Desarrollado por: Investigador

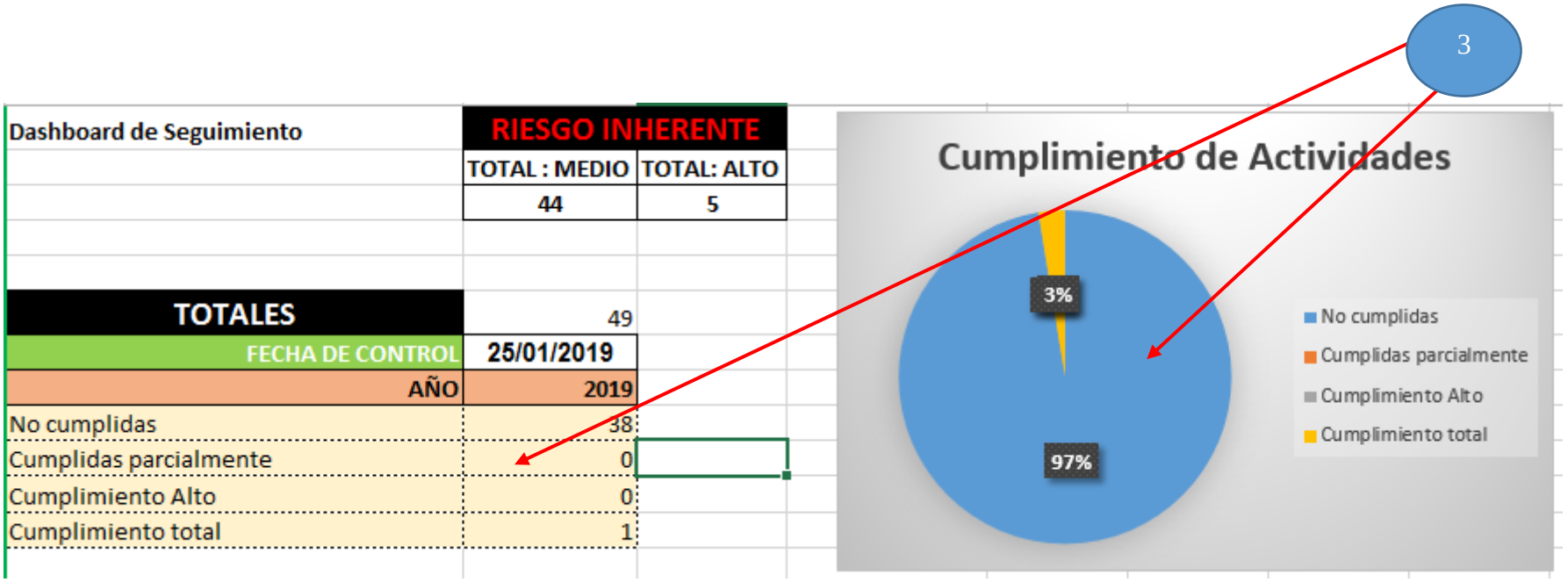
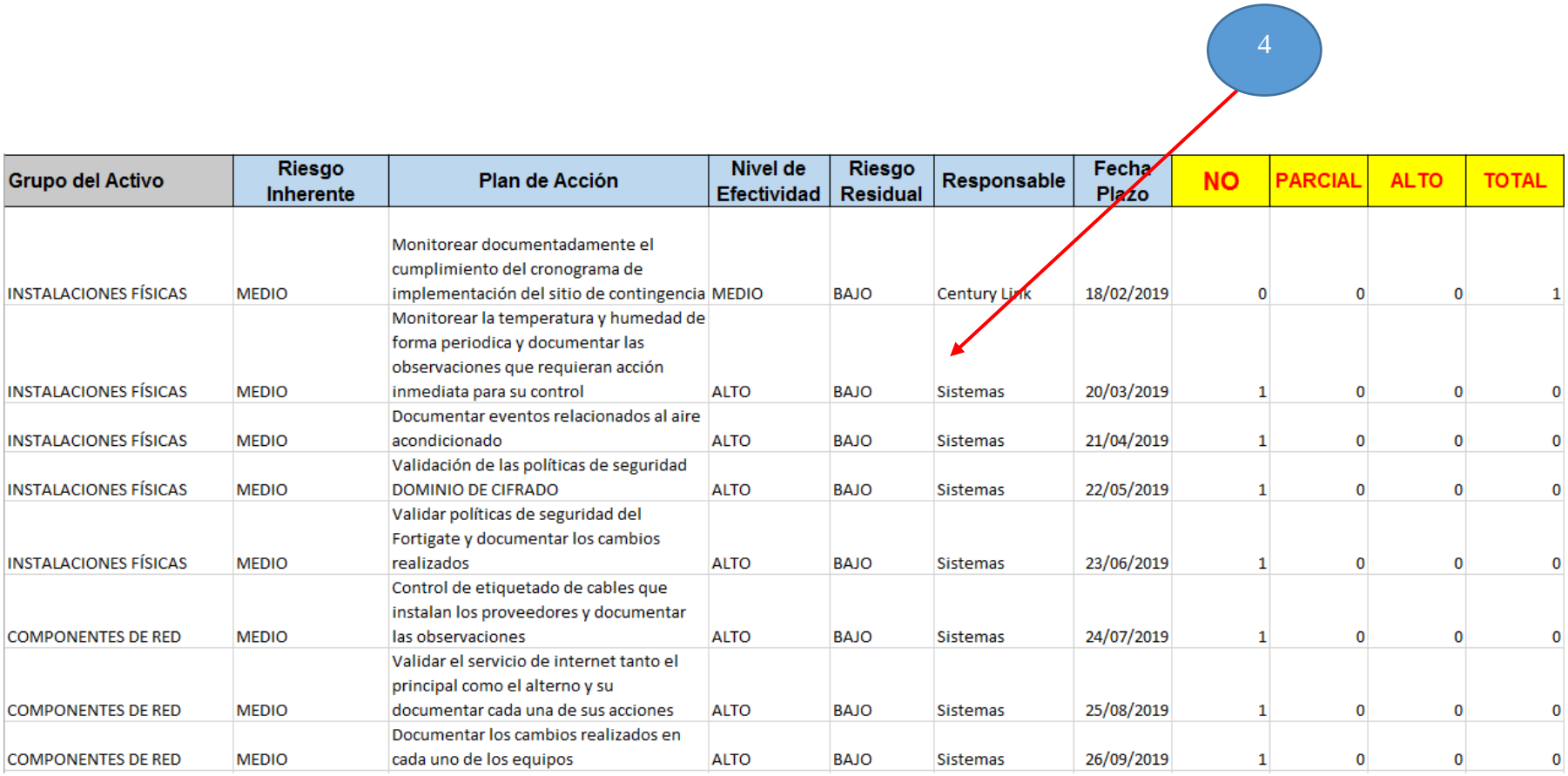


Figura 91. Cumplimiento de Actividades

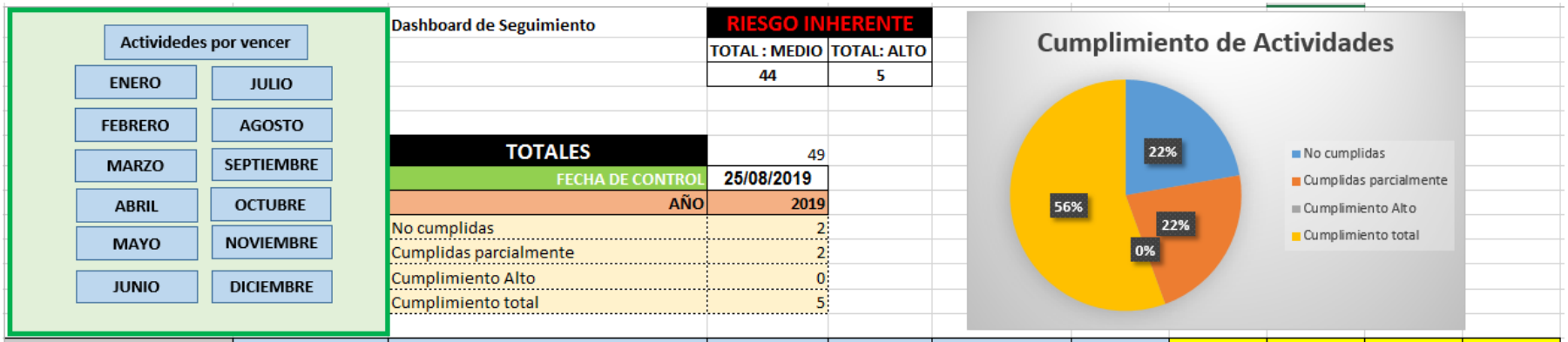
Desarrollado por: Investigador



Grupo del Activo	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo	NO	PARCIAL	ALTO	TOTAL
INSTALACIONES FÍSICAS	MEDIO	Monitorear documentadamente el cumplimiento del cronograma de implementación del sitio de contingencia	MEDIO	BAJO	Century Link	18/02/2019	0	0	0	1
INSTALACIONES FÍSICAS	MEDIO	Monitorear la temperatura y humedad de forma periodica y documentar las observaciones que requieran acción inmediata para su control	ALTO	BAJO	Sistemas	20/03/2019	1	0	0	0
INSTALACIONES FÍSICAS	MEDIO	Documentar eventos relacionados al aire acondicionado	ALTO	BAJO	Sistemas	21/04/2019	1	0	0	0
INSTALACIONES FÍSICAS	MEDIO	Validación de las políticas de seguridad DOMINIO DE CIFRADO	ALTO	BAJO	Sistemas	22/05/2019	1	0	0	0
INSTALACIONES FÍSICAS	MEDIO	Validar políticas de seguridad del Fortigate y documentar los cambios realizados	ALTO	BAJO	Sistemas	23/06/2019	1	0	0	0
COMPONENTES DE RED	MEDIO	Control de etiquetado de cables que instalan los proveedores y documentar las observaciones	ALTO	BAJO	Sistemas	24/07/2019	1	0	0	0
COMPONENTES DE RED	MEDIO	Validar el servicio de internet tanto el principal como el alterno y su documentar cada una de sus acciones	ALTO	BAJO	Sistemas	25/08/2019	1	0	0	0
COMPONENTES DE RED	MEDIO	Documentar los cambios realizados en cada uno de los equipos	ALTO	BAJO	Sistemas	26/09/2019	1	0	0	0

Figura 92. Resultado de Búsquedas

Desarrollado por: Investigador



Grupo del Activo	Riesgo Inherente	Plan de Acción	Nivel de Efectividad	Riesgo Residual	Responsable	Fecha Plazo	NO	PARCIAL	ALTO	TOTAL
INSTALACIONES FÍSICAS	MEDIO	Monitorear y revisar periodicamente las instalaciones y documentar las novedades encontradas que requieran acción inmediata	ALTO	BAJO	Sistemas	19/01/2019	0	0	0	1
EQUIPOS FÍSICOS	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01/01/2019	0	0	0	1
EQUIPOS FÍSICOS	MEDIO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01/01/2019	0	0	0	1
EQUIPOS FÍSICOS	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	MEDIO	Sistemas	01/01/2019	0	0	0	1
EQUIPOS FÍSICOS	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01/01/2019	0	0	0	1
EQUIPOS FÍSICOS	ALTO	Documentar el proceso y brechas del nuevo core financiero	ALTO	BAJO	Sistemas	01/01/2019	0	1	0	0

Figura 93. Balanced ScoreCard

Desarrollado por: Investigador

6.7.7. Conclusiones

En el presente trabajo se ha definido un modelo de Balanced ScoreCard para Seguridad de Información, este modelo está basado en la norma ISO 27001:2013, la misma que determina cuales son objetivos de control a validar en cada una de las áreas donde la información es parte vital de su actividad.

Este modelo cubre los activos dependiendo de la actividad económica, por lo tanto considerando de que el lugar donde se lo ejecutó el proyecto es una entidad financiera, es posible aplicar el mismo modelo en otras de las mismas características, garantizando que el área que gestiona los riesgos de la empresa pueda dar seguimiento fácilmente a los planes de acción que se encuentran en curso o aquellos que se encuentran próximos a alcanzar su fecha de ejecución o a su vez aquellos que ya han cumplido su plazo, garantizando a la entidad financiera y a sus clientes información segura y por ende confianza en ellos.

BIBLIOGRAFÍA

Advisera. (s.f.). *advisera.com*. Recuperado el 12 de 11 de 2017, de advisera.com: https://advisera.com/27001academy/es/

Alvarez, P. (2009). *Modelo de Administración de Riesgos de Liquidez y Mercado en la Cooperativa de Ahorro y Crédito san francisco de Asis Ltda.* Quito, Ecuador: Escuela Politécnica Nacional.

Ascanio, J. G. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*.

BSI. (julio de 2017). *Balanced Score Card Institute*. Obtenido de http://www.balancedscorecard.org/About/About-BSI

CIIFEN. (29 de 8 de 2018). *CIIFEN*. Obtenido de http://www.ciifen.org/index.php?option=com_content&view=category&id=84&Itemid=111&lang=es

CONCEPTODEFINICION. (29 de 08 de 2018). *CONCEPTODEFINICION*. Obtenido de https://conceptodefinicion.de/analisis/

Cushunchic, M. (2017).

Dávila, A. (1999). Nuevas herramientas de control: El Cuadro de Mando. *IESE, Revista de nuevos alumnos*.

Duque, F. J. (22 de 6 de 2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Rua Quinta do Roseiral*.

Enríquez, J., & Casas, S. (2013). Usabilidad en Aplicaciones móviles. *ICT-UNPA-62-ISSN: 1852-4516.*

Financoop. (12 de 12 de 2018). *Financoop*. Obtenido de https://www.financoop.net/index.php/nosotros/memoria-2017

gestiopolis. (s.f.). Recuperado el 04 de 12 de 2017, de https://www.gestiopolis.com/que-es-el-balanced-scorecard-y-para-que-sirve/

Godsulting. (2017). *Integrale, Cuadro de mando: Aplicativo Balanced Score Card.* Quito.

Hernández Trasobares, A. (2003). *Los Sistemas de Información: Evolución y Desarrollo.* Articulo, Universidad de Zaragoza, Zaragoza.

Isaca. (2011). *Isaca*. Recuperado el 12 de 11 de 2017, de Isaca: https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx?utm_referrer=

ISO 27000. (2012). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/sgsi.html

IsoTools. (10 de 11 de 2018). *IsoTools*. Obtenido de https://www.isotools.org/soluciones/estrategia/balanced-scorecard/

Kaspersky. (2017). *Kaspersky*. Recuperado el 13 de 11 de 2017, de https://www.kaspersky.es/resource-center/threats/computer-vandalism

Martelo, R. J. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *La Serena*.

Muñoz Vizhñay, J. P. (06 de enero de 2014). Balanced Scorecard-BSC o Cuadro de Mando Integral-CMI para la Universidad Nacional de Loja. https://es.slideshare.net/jorgemunozv/bsc-cmi-para-unl. Loja, LOja, Ecuador. Obtenido de https://es.slideshare.net/jorgemunozv/bsc-cmi-para-unl

Newing, R. (1994). Benefits of a balanced scorecard. *Accountancy*, pp. 52-3.

Pmg-Ssi. (21 de 05 de 2015). *Pmg-Ssi*. Recuperado el 13 de 11 de 2017, de Pmg-Ssi: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

pmg-ssi. (14 de 10 de 2018). *pmg-ssi*. Obtenido de https://www.pmg-ssi.com/2014/12/iso-27001-el-plan-de-seguridad/

searchdatacenter. (s.f.). *searchdatacenter*. Recuperado el 13 de 11 de 2017, de searchdatacenter: http://searchdatacenter.techtarget.com/es/definicion/Continuidad-de-negocios-BC

SEPS. (2015). *Ecuador tiene un total de 887 cooperativas de ahorro y crédito.* Quito.

Services, B. I. (2018). *Binaria IT Services*. Obtenido de http://www.binaria.com.ec/seguridad-de-informacion

Sullivan, P. (s.f.). *searchdatacenter*. Recuperado el 13 de 11 de 2017, de searchdatacenter: http://searchdatacenter.techtarget.com/es/consejo/Gestion-

de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Suñagua, Á. F. (Septiembre de 2013). *Auditoria de Seguridad de Información*. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2013000100004

Superintendencia de Bancos. (22 de 11 de 2018). *Superintendencia de Bancos*. Obtenido de https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2017/06/L1_X_cap_V.pdf

Superintendencia de Bancos del Ecuador. (2014). *Libro I.- Normas Generales para las Instituciones del Sistema Financiero.*

ANEXO 1

ESTRUCTURA DEL CUESTIONARIO

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Encuesta dirigida a gerentes, jefaturas, analistas de crédito, oficiales de cobranzas y cajeros de la Cooperativa Maquita Cushunchic Ltda.

Objetivo: Conocer el criterio acerca de la seguridad de información por quienes hacen parte de la Cooperativa de Ahorro y Crédito Maquita Cushunchic Ltda.

Instrucciones:

- Al ser anónima la encuesta, responda con toda libertad y sinceridad.
- Antes de contestar las preguntas, lea detenidamente.
- Marque con una X dentro del cuadro que Ud. considere en caso de tener una respuesta positiva y **No** en caso de dar una respuesta negativa, según la siguiente escala.

1	2	3	4	5
Casi Nunca	Regularmente	Bueno Frecuentemente	Muy Bueno Casi Siempre	Excelente Siempre

Cuestionario

No	Preguntas	No	**Si**				
			1	2	3	4	5
1	¿Recibe mantenimiento periódico el computador asignado para el desarrollo de sus funciones?						
2	¿El computador asignado en el desarrollo de sus funciones posee antivirus actualizado?						
3	¿Su equipo cuenta con las seguridades para restringir el acceso a personal no autorizado?						
4	¿Conoce si dentro de la institución existen políticas, normativas o Sistema de Gestión de Seguridad de la						

	Información?						
5	¿Considera necesario que la institución desarrolle e implante una normativa de Gestión de Seguridad de la información?						
6	¿La institución capacita al personal en temas de seguridad de la información?						
7	¿La institución capacita al personal en temas de riesgo operativo?						
8	¿Cuándo ocurre un evento relacionado con riesgo operativo sabe a quién reportarlo?						
9	¿Existe alguna restricción para navegar en internet?						
10	¿Conoce de alguna restricción sobre el uso del correo electrónico?						
11	¿Existe alguna política para el cambio regular de las contraseñas?						
12	¿Firmó usted un acuerdo de confidencialidad y de buen uso de sus claves de acceso?						
13	¿Ha detectado problemas en la integridad o exactitud de la información del core financiero?						
14	¿La información que usted maneja para el desempeño de sus funciones se respalda periódicamente?						
15	¿El acceso que usted requiere a los datos para el desempeño de sus funciones está siempre disponible?						
16	¿El core financiero le permite identificar quién ha realizado cambios en la información?						
17	¿Se conoce en qué momento se cambió la información?						
18	¿Se restringe el acceso de personal a opciones críticas del core financiero, donde se maneja transacciones sensibles de la Cooperativa?						

19	¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?						
20	¿Se cuenta con sistemas de alarma como detectores de humo, incendio?						
21	¿Existe vigilancia en la entrada del edificio donde Ud. labora?						

ANEXO 2

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVOS Y ALCANCE

1.1.Introducción

La información en la actualidad es considerada como el activo más importante de una organización después del talento humano, lo que genera la necesidad de gestionar un trato especial de mantenimiento y respaldo, previniéndola de incidentes naturales, físicos o humanos durante todo su ciclo de vida, de manera que se garantice su disponibilidad, integridad y confidencialidad, requeridas para una adecuada toma de decisiones.

En este contexto, y con el fin de garantizar una adecuada gestión de la Seguridad de la Información, la Cooperativa de Ahorro y Crédito Maquita Cushunchic ha desarrollado la presente Política, basada en las mejores prácticas que establece la norma ISO 27001, así como la referencia de la normativa de la Superintendencia de Bancos, con lo cual se promueve la protección de los activos de información y por ende, del valor patrimonial de la organización.

1.2.Objetivos

Objetivo General: Establecer los principios, políticas, y responsabilidades que rijan el proceso de Seguridad de la Información en la Cooperativa.

Objetivos Específicos

- Orientar la aplicación de controles de seguridad de la información para garantizar la provisión de los servicios financieros de la Cooperativa.
- Impulsar la eficiencia en la mitigación de riesgos de seguridad de la información, considerando los activos más importantes de la institución.
- Establecer la línea base para la ejecución del Proceso de Gestión de Seguridad de la Información.
- Dar cumplimiento a las disposiciones y normativas internas y externas asociadas con la Seguridad de la Información.
- Mantener la reputación e imagen institucional y su marca.

1.3.Alcance

La presente Política será de aplicación obligatoria para todo el personal de la Cooperativa que esté relacionado con la provisión de información y recursos, y la

ejecución de los procesos críticos de la institución, así como la gestión con proveedores externos de los mismos.

Su no aplicación será considerada falta grave, y conllevará las sanciones establecidas en el Reglamento de Trabajo.

La contratación de productos o servicios provistos por terceros, también estará sujeta al cumplimiento de la presente Política.

1.4.Términos y definiciones

La siguiente es la principal terminología a utilizar, la cual se encuentra fundamentada en las definiciones dadas por la norma ISO 27001, la normativa de Riesgo Operativo de la Superintendencia de Bancos y por ISACA[1]:

- **Gestión de la Seguridad de la Información**: políticas y procedimientos para administrar sistemáticamente los datos sensibles de una organización, minimizar el riesgo y asegurar la continuidad del negocio mediante la limitación proactiva del impacto ante una brecha de seguridad, incluyendo la gestión del comportamiento del personal, los procesos y la tecnología, de forma comprensiva para convertirse en parte de la cultura organizacional.

- **Incidente de seguridad de la información**: Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

[1] ISACA (www.isaca.org) es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento.

- **Plan de contingencia**: plan usado por una organización o unidad de negocios para dar continuidad a sus operaciones luego de una falla en los sistemas o interrupción específica.

- **Plan de Seguridad de la Información**: Herramienta que permite definir y priorizar todas las acciones y proyectos para cumplir las directrices establecidas en la Política de Seguridad de la Información, para reducir su riesgo a un nivel aceptable para la Cooperativa.

- **Proceso crítico**: Es el indispensable para la Seguridad de la Información y las operaciones de la institución, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo o poner en riesgo su sostenibilidad en el tiempo.

- **Seguridad de la Información**: conjunto de mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

- **Seguridad informática**: medidas de protección de la información en los sistemas, medios, redes y equipos tecnológicos y de comunicaciones.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Sistema holístico y sistemático para la Gestión de la Seguridad de la Información. (ISMS en inglés, siglas de Information Security Management System).

  En este contexto, se entiende por información al conjunto de datos organizados que posean valor para la institución, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

2. Políticas generales

La Cooperativa adoptará como referencia para la Gestión de la Seguridad de la Información a la norma ISO 27001:2013 "Sistema de Gestión de Seguridad de la Información" para garantizar la aplicación de buenas prácticas internacionales en el mismo, y la complementará con la normativa vigente de la Superintendencia de Bancos, por lo que a continuación se detallan los principios y políticas que regirán este proceso, por cada uno de los dominios de la norma ISO 27001:

2.1.Aspectos organizativos de la seguridad de la información

1. Toda la información generada, ingresada, almacenada, procesada, transmitida u obtenida por cualquier medio en los equipos de la Cooperativa, es de propiedad de la Cooperativa Maquita Cushunchic, por lo que todo usuario de la misma deberá suscribir un Acuerdo de Confidencialidad previo a su acceso.
2. Las necesidades de seguridad en la información, así como sus medidas de protección, serán definidas en conjunto por la Unidad de Riesgos y el Comité Gerencial, de acuerdo con su grado de criticidad y sensibilidad.
3. La Unidad de Tecnología implementará las medidas de seguridad informática requeridas, y realizará el monitoreo permanente de su correcto funcionamiento.
4. La Jefatura de Riesgos deberá monitorear periódicamente el cumplimiento de las políticas de seguridad de la información en las personas, procesos y tecnología de información de la Cooperativa, y coordinará la verificación de la efectividad de las medidas de seguridad informática implementadas.
5. La presente Política y el Proceso de Gestión de la Seguridad de la Información serán evaluados al menos de forma anual, para verificar su rendimiento, efectividad y alineamiento a los objetivos estratégicos institucionales.

2.2.Seguridad relacionada con los recursos humanos

1. La Jefatura de Soporte deberá asegurarse de que se realice la verificación de antecedentes de las personas a ser contratadas, para aquellos cargos que manejen información crítica o sensible de la Cooperativa.
2. La Jefatura de Soporte será la responsable de otorgar, modificar y revocar los permisos de acceso al sistema core financiero de la Cooperativa, los cuales serán otorgados según el rol de cada persona y bajo los principios de la necesidad de saber y del mínimo privilegio para el cumplimiento de sus funciones.
3. La Jefatura de Tecnología será responsable de establecer esquemas de seguridad para el acceso del personal a los recursos tecnológicos de la red de la Cooperativa. Los permisos para el acceso a estos recursos serán autorizados por la Jefatura de Soporte.
4. La Jefatura de Riesgos será la responsable de capacitar al personal en todos los temas relacionados a seguridad de información, como parte de la creación de una cultura organizacional para la gestión de riesgos.
5. La Jefatura de Soporte conjuntamente con Tecnología, eliminarán todos los accesos al empleado, al momento de su desvinculación de la Cooperativa.

2.3.Gestión de activos

1. El área de Tecnología se encargará de mantener actualizado el inventario de los activos tecnológicos y los que permiten la gestión de la información de la cooperativa, durante su creación, procesamiento, almacenamiento, transmisión, uso o eliminación de los datos, en cualquier plataforma que decida utilizar la Cooperativa.
2. La clasificación y determinación de las medidas de protección a implementar en la información, será de responsabilidad del responsable del proceso conjuntamente con la Jefatura de Riesgos, mientras que el etiquetado, manipulación y gestión de los activos que se relacionan con TI será responsabilidad del área de Tecnología.

2.4.Control de accesos

1. El acceso a los sistemas y recursos de la Cooperativa se realizará según el perfil del usuario y las funciones a él asignadas.
2. La Jefatura de Soporte será la única responsable de conceder autorizaciones de ingreso, según el perfil que haya definido para cada usuario. No se permitirá el acceso de usuarios que no hayan sido asignados a un perfil.
3. Todos los usuarios creados deberán contar con la identificación de su propietario.
4. No se otorgarán usuarios compartidos, excepto en el caso de abogados externos de una misma firma, o auditores externos en cuyo caso el acceso será exclusivamente de consulta.
5. El área de Tecnología será la responsable de:
    - Implementar procedimientos formales para el control de acceso a la red y servicios asociados tanto a usuarios como a proveedores.
    - Gestionar eficientemente las altas y bajas de un usuario en todo su ciclo de vida dentro de la cooperativa, previa autorización documentada de la Jefatura de Soporte.
6. Auditoría Interna controlará al menos anualmente, que los accesos a los sistemas y recursos de la Cooperativa se hayan concedido considerando las autorizaciones otorgadas por el área de Soporte.

2.5.Cifrado

1. El área de tecnología es la encargada de validar que los servicios informáticos que brinda la Cooperativa sean propios o de proveedores externos, utilicen controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.
2. El área de tecnología será la encargada de validar procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

2.6.Seguridad física y ambiental

1. El área de Tecnología y de Riesgos deberán definir y utilizar perímetros de seguridad para el acceso y protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica mediante sistemas de seguridad físicas y lógicas, debiendo estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone del permiso de acceso.
2. El área de Tecnología deberá:
   - Diseñar y aplicar procedimientos para proteger físicamente la información en caso de desastres naturales, ataques maliciosos o incidentes.
   - Proteger los equipos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo y mantener su disponibilidad e integridad continua.
   - Proteger contra la intercepción, interferencia o posibles daños a los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información.
   - Prevenir y garantizar que los equipos, la información o software no se puedan retirar del sitio sin previa autorización.

2.7.**Seguridad operativa**

1. El área de Tecnología deberá:
   - Documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.
   - Separar los entornos de desarrollo, pruebas y operaciones para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
   - Implementar controles para la detección, prevención y recuperación ante afectaciones de software dañino en combinación con la concientización adecuada de los usuarios.
   - Realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida y planificada.
   - Producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, administradores y operadores del sistema, excepciones, fallas y eventos de seguridad de la información, protegiéndolos contra posibles alteraciones y accesos no autorizados a sus registros.
   - Mantener sincronizado los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la cooperativa, así como del servidor de dominio, con relación a una fuente de sincronización única de referencia
   - Implementar procedimientos para controlar la instalación de software en sistemas operacionales con previo análisis de riesgo a los cambios en atención al posible impacto por situaciones adversas y realizando actualizaciones por cada cambio implementado, tanto en manuales de usuario como en documentación operativa.

- Obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
- Establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
- Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

2.8.Seguridad en las telecomunicaciones

1. El área de Tecnología será el encargado de configurar los dispositivos y aplicaciones de tal manera que puedan evitar el acceso físico no autorizado, daños e interferencias a la información de la organización y las instalaciones de procesamiento de la misma.
2. El área de Tecnología deberá de controlar todos los accesos a servicios internos (LAN/ LAN) y externos (LAN/ WAN) conectados a la red, manteniendo el equilibrio entre controles de seguridad, frente a controles de seguridad en aplicaciones.

2.9.Adquisición, desarrollo y mantenimiento de sistemas

1. Es responsabilidad del área de Tecnología:
   - Incluir todos los requisitos relacionados con la seguridad de la información en los requisitos para los nuevos sistemas o en las mejoras a los ya existentes.
   - Proteger la información de los servicios de aplicación que pasan a través de redes públicas contra actividades fraudulentas, de disputa de contratos y/ o modificación no autorizada, evitar también la transmisión y enrutamiento incorrecto, alteración, divulgación y/ o duplicación no autorizada de mensajes o su reproducción.
   - Establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la cooperativa, mediante uso de procedimientos formales de control de cambios durante el ciclo de vida de su desarrollo.
   - Evitar modificación en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios.

2. Es responsabilidad del área de Riesgos en conjunto con Auditoria revisar y aprobar los cambios realizados en las aplicaciones críticas para el negocio para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la información.
   Aplicar pruebas de funcionalidad en aspectos de seguridad durante las etapas de desarrollo de nuevos sistemas de información, actualizaciones y/ o nuevas versiones.

3. Es responsabilidad del área de Tecnología seleccionar cuidadosamente las bases de datos e información de prueba, estableciendo solicitudes de

autorización formal al área de Auditoria para realizar copias de bases de datos y su eliminación inmediata una vez terminada sus pruebas, estas deben de contemplar la prohibición del uso de bases de datos operativas.

2.10. Relaciones con proveedores

1. Auditoria interna deberá chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con proveedores y terceras personas.
2. El área de Tecnología deberá garantizar la protección de los activos de información de la cooperativa que son accesibles a proveedores y terceras personas.

2.11. Gestión de incidentes en la seguridad de la información

1. El área de Riesgos deberá:
   - Establecer responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información identificados.
   - Informar los eventos de seguridad de información ocurrido lo antes posible utilizando los canales de administración posible.
   - Anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información dentro de la cooperativa.
   - Evaluar los eventos de seguridad de información y decidir su clasificación como incidentes.
   - Responder ante los incidentes en atención a los procedimientos documentados.
   - Generar una base de conocimientos con el análisis y resolución de incidentes más frecuentes que permitan reducir la probabilidad y/o impacto en el futuro y sirva de evidencia mediante su preservación.

2.12. Gestión de la continuidad del negocio

1. La organización deberá:
   - Determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastres, estableciendo, documentando, implementando y manteniendo los procesos, procedimientos y controles para garantizar el mantenimiento de los niveles necesarios de seguridad durante estas situaciones.
   - Verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
   - El área de Tecnología deberá de implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad necesarios.

2.13. Cumplimiento

1. El área de riesgos deberá:
   - Identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.
   - Proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
   - Revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

2. El área de Auditoria deberá:
   - Implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.
   - Revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
   - Revisar los sistemas de información regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

3. El área de Tecnología deberá:
   Garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan, así como el uso de controles de cifrado de información.

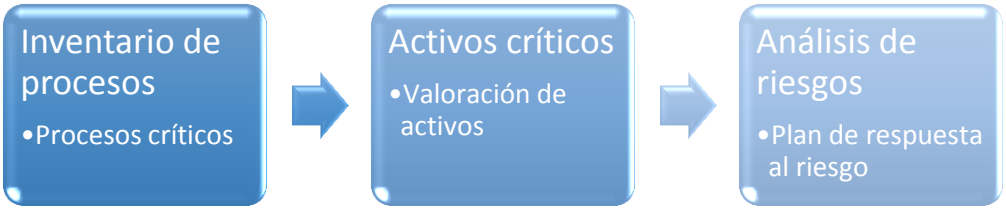
3. METODOLOGÍA PARA EL PLAN DE SEGURIDAD DE LA INFORMACIÓN

El plan de seguridad de la información se enfoca en asegurar que, dentro de la Cooperativa, la información esté protegida contra revelación a usuarios no autorizados (confidencialidad), modificación inapropiada (integridad), y falta de acceso cuando es requerido (disponibilidad). Para ello, la identificación, evaluación y

análisis de riesgos permite enfocar los esfuerzos en mitigar la exposición a amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información para la oportuna provisión de servicios por parte de la Cooperativa a sus socios.

a. Inventario de activos de información

El primer paso para elaborar el Plan de Seguridad de la información es la identificación de los procesos críticos de la Cooperativa, los cuales se encuentran identificados en el Plan de Continuidad del Negocio.



De éstos, se analiza las dependencias tecnológicas y de personal para el funcionamiento de cada uno de ellos, con lo cual se obtiene el detalle de recursos tecnológicos agrupados en las siguientes categorías:

- Instalaciones
- Red
- Equipos
- Software
- Personal
- Proveedores

Para los activos con mayor puntaje o importancia para la Cooperativa, se realiza el análisis de riesgos, identificando las amenazas, vulnerabilidades, controles y nivel de riesgo, y para los riesgos de nivel medio, alto o crítico se elabora el plan de riesgos, el cual debe contener al menos los siguientes datos:

- Descripción del riesgo
- Nivel de riesgo inherente
- Plan de respuesta
- Nivel de riesgo residual

- Fecha de implementación
- Cargo del responsable

La Jefatura de Riesgos realizará el seguimiento al cumplimiento del plan de riesgos por parte de cada responsable, y pondrá en conocimiento del Comité de Administración Integral de Riesgos los resultados y avances obtenidos cada mes, así como los incumplimientos.

b. Cumplimiento normativo

Una vez realizado el análisis de riesgos, se realiza una revisión de todos los controles establecidos en la Política de Seguridad de la Información y se valora si cada uno de ellos se ha cumplido a cabalidad en toda la organización. A partir de esta evaluación, se elaborará el Plan de Seguridad de la Información, en el que se incorpore:

- Objetivo de control (política)
- Porcentaje de implementación o cumplimiento
- Actividad a realizar para lograr un 100% de cumplimiento
- Entregable de la actividad (verificable)
- Fecha de implementación
- Cargo del responsable

Previo a su ejecución, el Comité de Administración Integral de Riesgos validará que la estrategia planteada en el Plan de Seguridad de la Información satisfaga las necesidades institucionales, e incorporará nuevas medidas o mejoras que considere pertinentes, luego de lo cual la Gerencia aprobará el presupuesto del plan y resolverá los conflictos de recursos que pudieran presentarse.

Al igual que con el Plan de respuesta al riesgo, la Jefatura de Riesgos realizará el seguimiento al cumplimiento del Plan de Seguridad de la Información por parte de cada responsable, y pondrá en conocimiento del Comité de Administración Integral de Riesgos los resultados y avances obtenidos cada mes, así como los incumplimientos.

4. TRATAMIENTO DE EXCEPCIONES

Las instancias que podrán autorizar excepciones a lo establecido en la presente Política, serán:

- Gerente General o su delegado
- Consejo de Administración

Se podrán excepcionar únicamente aquellas definiciones o situaciones que no pongan en riesgo operacional, financiero o reputacional a la Cooperativa, ni ocasionen incumplimiento a la normativa legal vigente u otras obligaciones con terceros.

Toda situación que pueda representar conflicto de intereses con los Consejos o funcionarios de la Cooperativa, deberá ser previamente analizada y aprobada por la Gerente General o por quien ésta designe.

5. BASE LEGAL Y NORMATIVA RELACIONADA

La presente Política está basada en:

- Sección IV "Seguridad de la Información", Capítulo V, Título X "De la Gestión y Administración de Riesgos", Libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y de la Junta Bancaria.
- Norma ISO 27001:2013 Sistema de Gestión de la Seguridad de la Información.

ANEXO 3

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

5. POLÍTICAS DE SEGURIDAD.

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

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

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

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

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

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

Octubre-2013