UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC.

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Sistemas

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Oscar Gabriel Muñoz Pinto

TUTOR: Dennis Vinicio Chicaiza Castillo

Ambato - Ecuador

Agosto – 2020

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC", desarrollado bajo la modalidad Proyecto de Investigación por el señor Oscar Gabriel Muñoz Pinto, estudiante de la Carrera de Ingeniería en Sistemas Electrónica e Industrial, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, agosto 2020.

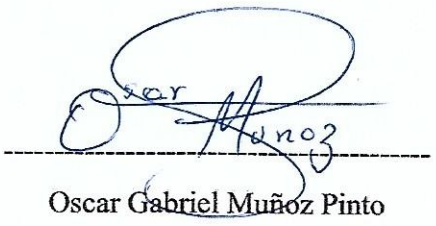
Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Chicaiza, Mg
TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC" es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2020.



Oscar Gabriel Muñoz Pinto

C.I. 180425737-4

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Oscar Gabriel Muñoz Pinto, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC", nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, agosto 2020.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Balarezo, PhD.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
VICTOR HUGO GUACHIMBOSA VILLALBA

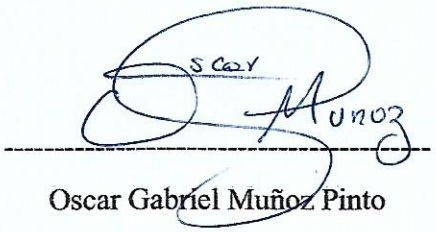
Ing. Víctor Guachimbosa, PhD.
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, agosto 2020.



Oscar Gabriel Muñoz Pinto

C.I. 180425737-4

AUTOR

DEDICATORIA

El presente trabajo está dedicado a todas las personas que creyeron en mi desde el primero momento.

En especial a mis padres Raúl y Rosa que fueron los pilares fundamentales en este pequeño logro de la vida

Mis hermanos Andrés y Mauricio por su apoyo en cada uno de los momentos compartidos.

Sobre todo, a mi sobrino Mateo y mi compañera de vida Verónica que fueron mi inspiración y ganas de superarme, hasta conseguir cada objetivo planteado.

Oscar Gabriel Muñoz Pinto

AGRADECIMIENTO

Quiero agradecer a Dios por la salud, el trabajo y la vida de mis padres sin él y ellos nada de esto sería posible.

Al ing. Dennis Chicaiza y al Ing. Ricardo Pilamunga por su apoyo en el desarrollo del trabajo de investigación.

A Verónica por todo su apoyo incondicional y aliento en cada uno de mis pasos

Oscar Gabriel Muñoz Pinto

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

RESUMEN EJECUTIVO

La seguridad de la información, es relevante dentro de cualquier entidad, empresa o institución. La Cooperativa de Ahorro y Crédito SAC, es una entidad financiera, que maneja información crítica y reservada para el resto, por lo que es primordial garantizar la seguridad de la información dentro de la misma, el siguiente proyecto se basa en la Norma ISO/IEC 27001, lo que se busca es mejorar y/o garantizar dicha información, a través del Sistema de Gestión de la Seguridad de la Información (SGSI), aplicando cada uno de las políticas de seguridad, como la gestión de activos, controles de acceso, seguridad física, etc. Dentro de cada uno de los dominios que la norma dicta, los cuales fueron analizados detalladamente.

Primeramente, se empezó analizando y evaluando el estado actual de seguridad en el departamento de tecnologías de la información dentro de la entidad financiera las cuales fueron obtenidas a través de entrevistas, encuestas, y levantamiento de la información con visitas al mismo, para poder obtener información certera que ayude a tener un punto de partida para la realización del sistema de gestión de calidad.

Después de que haber obtenido el estado actual de la entidad financiera, se procedió, a analizar en busca de posibles vulnerabilidades que afecten a la integridad de la seguridad de la información y problemas que afecten a la disponibilidad de ella, para definir el alcance esperado, finalmente se definieron las políticas de seguridad con una gestión adecuada para garantizar la seguridad de la información, estas fueron establecidas cumpliendo, los limites institucionales de la entidad financiera.

ABSTRACT

Information security is relevant within any entity, company or institution. The Cooperativa de Ahorro y Crédito SAC, is a financial entity that manages critical information reserved for the rest, so it is essential to guarantee the security of the information within it, the following project is based on the ISO / IEC Standard 27001, what is sought is to improve and / or guarantee said information, through the Information Security Management System (ISMS), applying each of the security policies, such as asset management, access controls, physical security, etc. Within each of the domains that the norm dictates, which were analyzed in detail.

Firstly, the analysis and evaluation of the current state of security in the information technology department within the financial institution began, which were obtained through interviews, surveys, and information gathering with visits to it, in order to obtain information certain that it helps to have a starting point for the implementation of the quality management system.

After having obtained the current status of the financial institution, we proceeded to analyze for possible vulnerabilities that affect the integrity of information security and problems that affect its availability, to define the expected scope, Finally, security policies were defined with adequate management to guarantee the security of the information, these were established in compliance with the institutional limits of the financial institution.

CAPITULO I
MARCO TEÓRICO

1.1 Antecedentes Investigativos

“Ramiro Alejandro Guevara en su proyecto de investigación “SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001” determina que existen diversos procedimientos que se llevan a cabo para la protección de los equipos, pero estos se descuidan en gran medida del mantenimiento que se debe realizar a los mismos con lo cual se expone tanto la integridad del equipo como la del personal.” [3]

“Tania Verónica Guachi Aucapiña en su proyecto de investigación “NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA” la información que se procesa en los sistemas de información y de comunicación manifiesta que no se encuentran protegidas con metodologías además que estos se encuentran expuestos a varios ataques informáticos.”[4]

“Mireya Elizabeth Ramírez Quintero en su trabajo de tesis presentada “IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO” concluye que en un sistema de seguridad se deben considerar aspectos técnicos debido a que el riesgo en una organización nunca se elimina por lo cual es importante mantenerse actualizado en cuanto a las nuevas amenazas que atenten contra la seguridad de los activos de la empresa.” [5]

“Cristian Ríos Criollo y Hugo Tinoco Silva en su proyecto de titulación “IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA INFORMACION, BAJO LA NORMA ISO/IEC 27001, EN UNA EMPRESA DE SERVICIOS”, concluyen que la seguridad de la información es muy importante ya que si no se le presta atención podría existir fuga de información sensible, que podría ocasionar consecuencias como pérdida de prestigio de la institución y litigios para la empresa.” [6]

1.1.1 Contextualización del problema

A través de los años la tecnología informática, como los sistemas de información han evolucionado de manera gigantesca en el mundo, así como métodos para su vulneración, es así como entes gubernamentales han alertado a organizaciones internacionales que se dedican a la seguridad de la información generen normas con el fin de proteger la información, las organizaciones están en un tiempo donde se han generado amenazas, malware, ataques cibernéticos dirigidos, esto sumada a una inadecuada inversión en dispositivos, aplicaciones y el poco uso de normas de seguridad, dan paso a una serie de vulnerabilidades que pueden provocar la pérdida de información mediante infiltraciones de intrusos en equipos que se encuentran conectados a la red, es por esto que es necesario, y de mucha importancia realizar un análisis de amenazas en un contexto, donde se pueda detectar las principales causas que pueden ocasionar los incidentes que las normas y estándares internacionales proporcionan, con el fin de garantizar un rendimiento más óptimo en cuanto a seguridad de la información en un departamento informático, con el fin de aumentar la confianza dentro del mismo, como a usuarios, negocios, socios de una manera sustentable. [1]

En Ecuador, existen empresas públicas y privadas que contextualizan a la información como un problema tecnológico, es por eso que es necesario tomar las medidas adecuadas con el fin de proteger uno de los activos más valiosos como es la información. La seguridad de la información tiene que ser entendida como un bien necesario dentro de cualquier empresa, esta permitirá tener una serie de lineamientos y respuestas a cualquier eventualidad maliciosa o catástrofe que pudiera poner en riesgo la pérdida o filtración de datos que son estrictamente confidenciales dentro de cualquier organización. [2]

La gestión de riesgos, así como la seguridad de la información informática son muy poco estudiadas, pese a ser una de los pilares más importantes dentro de cualquier empresa, que maneje un sistema informático.

Conforme avanza la tecnología, aparecen nuevos métodos que afectan a la seguridad de la información, por este motivo es necesario tener un análisis de vulnerabilidades que puedan existir en un sistema informático, con el fin que se pueda elaborar un sistema de gestión de seguridad de la información, el mismo que esta echo con el fin de minimizar los riesgos que pueda presentarse, de forma fraudulenta, ayudando a tener un mejor control sobre el mismo.

Dentro de la Cooperativa de Ahorro y Crédito Indígena SAC, se trabaja con información delicada y confidencial para cada uno de los socios de la entidad financiera, es por esto que es importante tener una seguridad de la información, en el sistema informático con la que se trabaja dentro de la misma, considerando los aspectos básicos como: confidencialidad, integridad y disponibilidad.

Actualmente la Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con medidas preventivas, pero no dispone con un sistema de seguridad de la información, que maneje alguna norma previamente establecida que ayude a mantener segura la información, dejándola vulnerable algún ataque malicioso.

1.1.2 Fundamentación Teórica

1.1.2.1 Seguridad de la información

- **Definición**

Podemos definir a la seguridad de la información, en la aplicación y normas de seguridad necesarias, para resguardar y asegurar la información, esta cumple con las tres siguientes dimensiones principales: la confidencialidad, disponibilidad e integridad [7].

Siendo así los tres pilares fundamentales de la seguridad de la información:

- **Confidencialidad:** Es una cualidad que se otorga a la comunicación de un mensaje de datos, y que estos sean entendidos, comprendidos o leídos, que estén autorizados.

- **Integridad:** Es una cualidad que obtienen el mensaje, comunicación o los datos, el cual permite comprobar y asegurar que este no haya sido modificado o alterado desde su origen, hasta la recepción del destino.

- **Disponibilidad:** Es la cualidad que se otorga a la capacidad de un servicio, de datos o de un sistema, siendo este accesible y utilizado por los usuarios autorizados, cuando ellos lo necesiten y/o requieran.

- **Riesgos**

- Podemos clasificar como riesgos a la detección de vulnerabilidades y/o amenazas sobre algún activo, después de su análisis de riesgo a los que se encuentre expuesto, y que este represente una amenaza a la seguridad de la información, tanto física como de software.

- **Tipos de Seguridad**

- **Activa**

  La seguridad activa se representa como una serie de medidas que son implementas con el fin de minimizar los efectos contrarios a cualquier incidente de seguridad, a estas medidas también se las puede clasificar como medidas de corrección.

- **Pasiva**

  La seguridad pasiva se representa al objetivo de prevenir y detectar los diferentes riesgos que pueden ser causados, por un accidente, un usuario o un malware, que ponga en peligro a los sistemas de información.

1.1.2.2 Normas ISO

- **Definición**

  Las normas ISO son el conjunto de normas que de una manera ordenada y orientada ayuda a las gestiones dentro de una empresa en diferentes ámbitos. [11]

  ISO (Organización Internacional para la Normalización) es la dedicada a la creación de los estándares para asegurar y mantener la calidad, así como la seguridad y eficacia de productos y servicios. [12]

  Las normas ISO, actualmente se encuentra presente en más de 150 países, a nivel mundial y es una organización no gubernamental e independiente. En la actualidad se encuentran creadas alrededor de 22.000 estándares que se distribuyen en diferentes industrias, como tecnología, agricultura, salud, etc. [12]

- **Normas ISO 27000**

  Estas normas son el conjunto de los estándares internacionales que existen para la seguridad de la información, dentro de las normas ISO 27000 se encuentra un conjunto de buenas prácticas, para establecer, implementar, mantener y mejorar los Sistemas de Gestión de la Seguridad de la Información (SGSI). [13]

  Dentro de los estándares ISO 27000, tenemos las dos principales normas que son las normas 27001 y 27002, entre estas dos su principal diferencia radica, en que la norma 27001 está basada en la seguridad de forma continua, con identificación de riesgos de forma permanente en el transcurso del tiempo, por otro lado, la norma 27002 es una guía de prácticas que describen la serie de objetivos de control y gestión que deben cubrir las organizaciones. [13]

- **ISO 27001**

  Esta norma internacional nos permite asegurar, la confidencialidad e integración de los datos y la información, así como los sistemas que los procesan. [14]

  Esta norma es importante y nos facilita el establecer, la implementación, el mantenimiento y la mejora de la seguridad los activos más valiosos que poseen las organizaciones, es decir la información. Esta lo hace por medio de un conjunto de procesos que se basan en los riesgos que cada una de las organizaciones se enfrentan en sus actividades diarias. [14]

  La norma 27001, es la mejor y la más adecuada actualmente para implementar en cualquier organización, sin que importe su tamaño, su mercado o la actividad que esta realice.

  Uno de los principales objetivos dentro de un Sistema de Gestión de Seguridad de la información, es favorecer y ayudar al desempeño de cada una de las organizaciones, para esto es necesario que este alineada con los objetivos de negocio. [14]

La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001. Considerando los avances y las preocupaciones actuales, esta escala se compondría de los siguientes niveles:

- Nivel 0, el "sentido común".
- Nivel 1, el cumplimiento de la legislación obligatoria.
- Nivel 2, evaluación del proceso de Gestión de Seguridad.
- Nivel 3, analizar el riesgo y la gestión de su resolución.
- Nivel 4, adquisición de productos para integrarlos en los Sistemas de Gestión.
- Nivel 5, integración de los componentes certificados en sistemas compuestos y su certificación

  Los niveles de madurez se pueden jerarquizar de la siguiente manera:

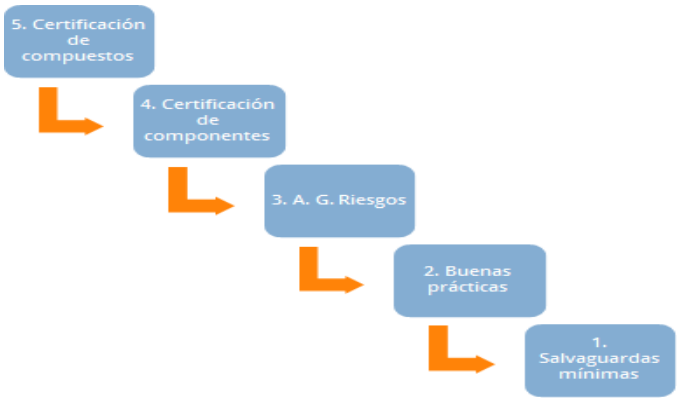


Grafico 1 Niveles de madurez de la empresa

- **Etapas de la seguridad de la información**

  Los Sistemas de gestión de seguridad están basados en la mejoría continua, para su desarrollo en este proyecto será utilizado el ciclo DEMING (PDCA)

1.1.2.3 Propuesta de solución

En este proyecto se propone establecer un Sistema de Gestión de la Seguridad de la Información basada en la norma ISO/IEC 27001, que permita mediante un plan mejorar la seguridad con el fin de tener confidencialidad, integridad y disponibilidad de la información, con niveles altos de eficiencia y protección.

1.2 Objetivos

1.2.1 Objetivo General

- Establecer un Sistema de Gestión de Seguridad de la Información basado en las Normas de la ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indígena SAC.

1.2.2 Objetivos Específicos:

- Realizar un diagnóstico de los procesos informáticos que actualmente se manejan en el Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC, con el fin de evidenciar falencias en el manejo de los mismos.

- Diagnosticar la existencia de políticas de seguridad y el cumplimiento de normas en los procesos de seguridad informática, en el Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Diseñar un Sistema de Gestión de la Seguridad de la Información basado en la norma IS0/IEC 27001 para el Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC.

CAPÍTULO II
METODOLOGÍA

2.1 Materiales

Institucionales

- Universidad Técnica de Ambato.
- Facultad de Ingeniería en Sistemas Computacionales e Informáticos.
- Cooperativa de Ahorro y Crédito Indígena SAC.
- Biblioteca Física.
- Biblioteca Digital.
- Repositorio Institucional.

Humano

- Docente Tutor del Proyecto
- Jefe del Departamento de Tecnologías de la Información de la Cooperativa.
- Autor del Proyecto.

Recursos

- Computador – 8GB RAM – INTEL CORE i3
- Libros
- Transporte
- Internet
- Energía eléctrica
- Suministros de oficina
- Dispositivos de almacenamiento

Económico (presupuesto y financiamiento)

El investigador será quien se encargará del financiamiento del proyecto de investigación. En la siguiente tabla se detalla el presupuesto:

N°	Detalle	Unidad	Cantidad	Valor Unitario	Total
1	Internet	Horas	400	1	400
2	Transporte	c/u	120	5	600
3	Computadora	c/u	1	900	900
4	Medios de almacenamiento				
	* Flash Memory	c/u	1	16	16
5	Resma hojas A4	c/u	2	5	10
6	Carpetas	c/u	5	0,5	2,5
7	Impresiones	c/u	600	0,05	30
				SubTotal	1958,5
				Imprevistos(10%)	195,85
				Total	2154,35

Tabla 1:Materiales

2.2 Métodos

2.2.1 Modalidad de la Investigación

2.2.1.1 Investigación Bibliográfica- Documental

Este proyecto fue de investigación bibliográfica y documental, debido a que se recolecto información y posteriormente estos fueron analizados, con el fin de recomendar las medidas que se tomarán para mejorar la seguridad de la información, en base a diferentes fuentes como libros, documentos, artículos, revistas, etc., las mismas que ayudarán a tener un mejor enfoque sobre el problema.

2.2.1.2 Investigación de campo

Sera una investigación de campo ya que se obtuvo información en el Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC, con el fin de entender los procesos que se realizan actualmente y obtener información que nos ayudara a la identificación de debilidades y fortalezas en la seguridad de la información.

2.2.1.3 Investigación Aplicada

Sera una investigación aplicada, ya que el problema es establecido y conocido por el investigador, con el fin de establecer un Sistema de Gestión de Seguridad de la Información, para ayudar a mantener confidencialidad y eficacia en el manejo de la seguridad de la información.

2.2.2 Población y Muestra

- **Población**

Para la presente investigación se tomó como población al personal del departamento de tecnologías de la información de la Cooperativa de Ahorro y Crédito Indígena SAC.

N	Cargo	Departamento
1	Jefe del Departamento de Sistemas	Tecnologías de la Información
2	Desarrollador 1	Tecnologías de la Información
3	Desarrollador 2	Tecnologías de la Información
4	Asistente de Tecnología	Tecnologías de la Información
	Total	100%

Tabla 2 : Población encuestada

- **Muestra**

No es necesario realizar un muestreo debido a que la población es reducida y se puede acceder a ella sin restricciones. Por tanto, la muestra viene a ser la misma población definida anteriormente.

2.2.3 Recolección de Información

Para poder tener un diagnóstico de los procesos informáticos que se manejan actualmente en el Departamento de Tecnologías de la Información en la entidad financiera, se realizó una encuesta, a cada uno del personal dentro del departamento, para así poder evidenciar cómo se manejaban los procesos y poder encontrar falencias de seguridad en el mismo.

Con el fin de poder determinar si existían actualmente políticas de seguridad, se mantuvo visitas al departamento, se hizo un levantamiento de información y se realizó una auditoria de madurez a cada uno de los objetivos que establece la norma.

La documentación de la norma ISO 27001, así como su incidencia en la seguridad de la información, fue realizada con una investigación documental en las áreas y dominios de dicha norma.

2.2.4 Procesamiento y análisis de datos

Cada una de la información que se obtuvo fue clasificada, revisada, organizada e interpretada, de manera que los resultados obtenidos fueron representados en forma de gráficos, porcentajes y diagramas que fueron de ayuda para el desarrollo de la solución del problema planteado aplicando los siguientes procedimientos:

1. Elaboración de instrumentos para entrevista y encuestas.

2. Elaboración de matriz de evaluación del nivel de madurez de los controles de seguridad conforme norma ISO/IEC 27001.

3. Tabulación de la información obtenida

4. Estudio estadístico de datos para presentación de resultados.

CAPÍTULO III
RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados.

Una de los puntos más importantes para el desarrollo del proyecto es la investigación para determinar la situación actual del Departamento de Tecnologías de la Información dentro de la Cooperativa de Ahorro y Crédito Indígena SAC, con respecto a las políticas y normas de la seguridad de la información.

Para el procesamiento y análisis de los datos se realizó una encuesta a cada uno de los integrantes del departamento, con el fin de determinar la situación de la seguridad en la Cooperativa de Ahorro y Crédito Indígena SAC.

Después será importante realizar un análisis de cada una de las preguntas de la encuesta, para tener un punto de partida y generar una gestión adecuada, poniendo interés necesario en aquellos puntos negativos de políticas y normas de seguridad de la información.

Se procederá a evaluar cada uno de los activos informáticos, como equipos de cómputo, routers, impresoras y servidores dentro del departamento, aplicando una auditoria de madurez con cada uno de los puntos que marca la norma ISO 27001, al fin de encontrar políticas y normas existentes dentro de el departamento.

Entrevistado Pregunta	Jefe del Departamento de Sistemas	Desarrollador 1	Desarrollador 2	Asistente de Tecnología
1.- ¿Actualmente existen políticas que gestionen la seguridad de la información?	Si, se aplican políticas de seguridad El acceso al internet es limitado, tiene restricciones. Control de usuarios y accesos al core financiero. La instalación y modificación de software es restringido. El uso de dispositivos extraíbles solo puede ser usados previa autorización y desbloqueo	No, no se utilizan políticas para gestionar la seguridad de la información	No, no se utilizan políticas para gestionar la seguridad de la información	Si se aplican varias políticas de seguridad El acceso al core financiero es inaccesible desde fuera de las instalaciones Únicamente se puede acceder desde matriz y las agencias El control de dispositivos es restringidos
2.- ¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?	Si, el personal recibe capacitaciones.	Si, el personal está totalmente capacitado en el uso del software	Si, ya que se dictan capacitaciones sobre los recursos tecnológicos	Si, el personal esta capacitado y recibe capacitaciones frecuentes

3.- ¿Existen controles sobre el acceso de personal interno y externo al equipamiento y sistemas que maneja dentro de la institución financiera?	Si, se entrega actas de confidencialidad de ingreso al core financiero El equipamiento se entrega con acta de responsabilidad de equipamiento. Existe control de acceso a las diferentes áreas.	Si, se lleva actas de confidencialidad de ingreso al core financiero	Si, los equipamiento se llevan un control mediante actas de entrega de los equipos informáticos Existe control sobre el uso del sistema mientas actas de confidencialidad	Si, con actas de entrega de Hardware y Software Control de Acceso a bóvedas, cajas fuertes, como a otras áreas de alto riesgo para la institución.
4.- ¿Existe un plan de mantenimiento para los equipos informáticos dentro de la institución financiera?	Si, los equipos informáticos reciben mantenimiento a través de un manual.	Si, existe un plan de mantenimiento que se desarrolla anualmente	Si, a través de manual de mantenimiento preventivo y correctivo	Si, existe un manual de mantenimiento.

Entrevistado Pregunta	Jefe del Departamento de Sistemas	Desarrollador 1	Desarrollador 2	Asistente de Tecnología
5.- ¿Existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución financiera?	Si, existe un plan de contingencia que se realiza anualmente, aprobada por la **SEPS** (Superintendencia de Economía Popular y Solidaria) Las bases de datos son respaldadas periódicamente en almacenamiento interno como externo.	Si, las bases de datos se realizan respaldos periódicamente tanto internamente como externamente	Existe un plan de contingencia anual.	Si, existe un plan de contingencia que se realiza cada año
6.- ¿Se realizan tareas de monitoreo a los sistemas de información con los empleados en la institución?	Si, se realiza un monitoreo a los sistemas y empleados a través de la red.	No, no se realiza monitoreo.	Si, se realiza a diario el monitoreo de los servidores sobre los cuales están funcionando los servicios principales.	Si, parcialmente se realizan monitoreo, especialmente cuando son sistemas nuevos.

Entrevistado Pregunta	Jefe del Departamento de Sistemas	Desarrollador 1	Desarrollador 2	Asistente de Tecnología
7.- ¿Cuáles son las técnicas, mecanismo y/o herramientas que se apliquen para la seguridad de los sistemas de información de la institución financiera?	Existe una doble autentificación para cualquier uso del sistema de información de la institución financiera Control de antivirus y firewall	Factores de doble autentificación. Existe encriptación de contraseñas	Para el acceso al sistema de información de la institución se requiere una doble autenticación. Uso de antivirus	Si, factores de doble autentificación.
8.- ¿Se lleva un control y administración adecuado para el inventario de activos informáticos de la institución?	Si, existe un manual de control de procesos inventarios. Existe un control con el valor económico de los activos informáticos de la institución.	Si, existe un manual y procesos de inventarios.	Si, se realiza a diario el monitoreo de los servidores sobre los cuales están funcionando los servicios principales.	Si, un manual de procesos, codificación y valor económico.
9.- ¿Conoce Ud. Acerca de algún Sistema de Gestión de Seguridad de la Información (SGSI)?	No	No	No	No

Tabla 3 Desarrollo encuesta

3.1.1 Tabulación de resultados

1.- ¿Actualmente existen políticas que gestionen la seguridad de la información?

RESPUESTA	CANTIDAD	PORCENTAJE
Políticas para los usuarios	1	25%
Políticas para los sistemas de información	1	25%
No	2	50%
Total	4	100%

Tabla 4 Cuadro porcentual pregunta 1

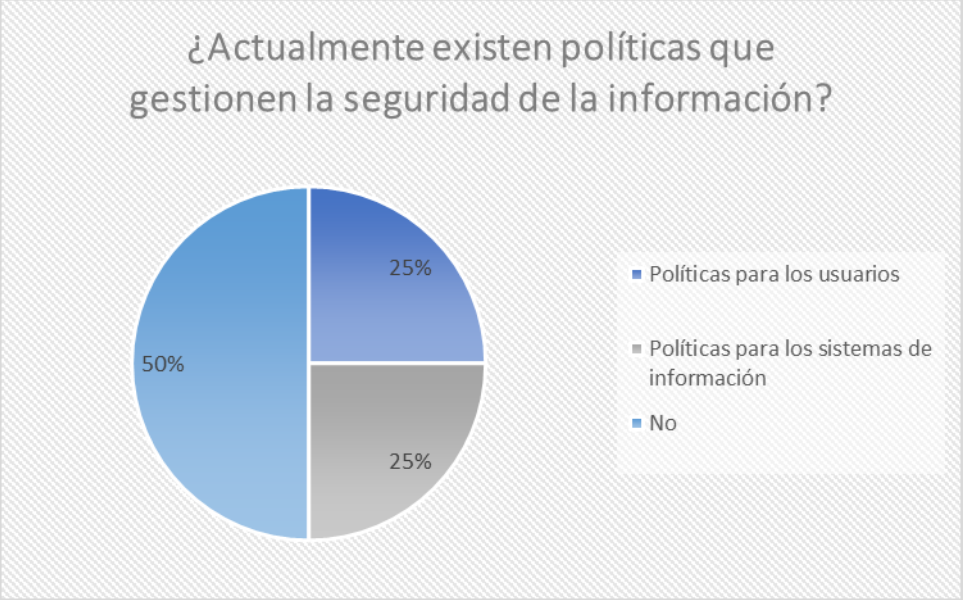


Grafico 2 pregunta 1

Interpretación. – Del total de los entrevistados, el 25% afirma que existen políticas para los usuarios, otro 25% afirma que existen políticas para los sistemas de información, mientras el 50% de los entrevistados afirma que no existen políticas que gestionen la seguridad de la información dentro de la entidad financiera.

Análisis. – Existen políticas para la seguridad de información dirigidas a usuarios y a los sistemas de información, sin embargo, se puede concluir que los sistemas de información no tienen un nivel confiable de protección.

2.- ¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	100%
No	0	0%
Total	4	100%

Tabla 5 Cuadro porcentual pregunta 2

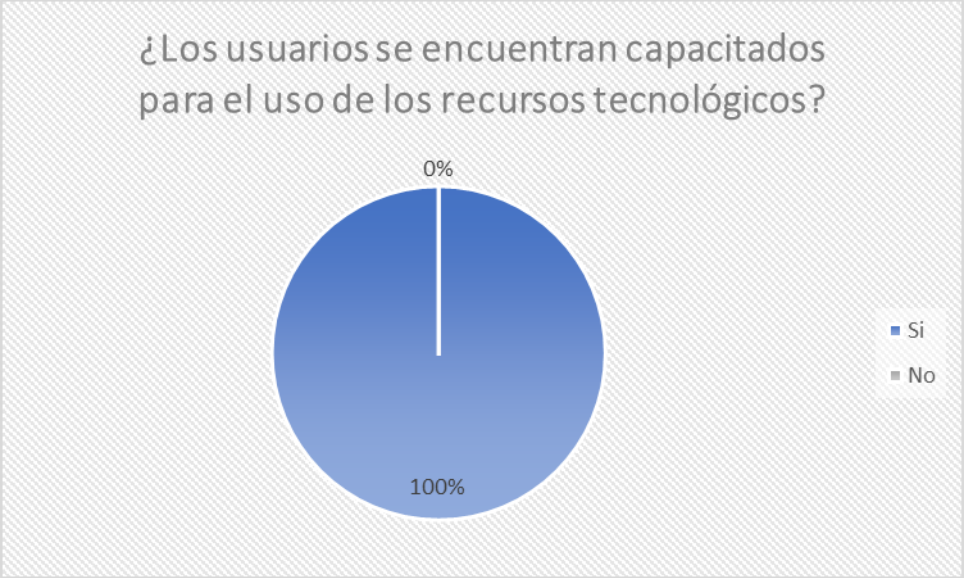


Grafico 3 pregunta 2

Interpretación. – Del total de los entrevistados, el 100% afirma que el personal se encuentra debidamente capacitado para la utilización de los recursos tecnológicos, así también se dictan capacitaciones permanentes para los usuarios dentro de la entidad financiera.

Análisis. – Los usuarios dentro de la entidad financiera se encuentra capacitado, así como a su vez reciben capacitación permanentemente y oportunamente esto ayuda en un mejor desempeño y mayor eficacia a la hora de realizar las funciones asignadas para cada usuario, cabe mencionar que la capacitación es necesaria para que los usuarios actualicen sus conocimientos periódicamente para colaborar con el éxito de la entidad financiera.

3.- ¿Existen controles sobre el acceso de personal interno y externo al equipamiento y sistemas que maneja dentro de la institución financiera?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	100%
No	0	0%
Total	4	100%

Tabla 6 Cuadro porcentual pregunta 3

Grafico 4 pregunta 3

Interpretación. – Del total de los entrevistados, el 100% de los entrevistados afirman que existen controles sobre el acceso para personal interno y externo al equipamiento, así como a los sistemas que se maneja dentro de la entidad financiera.

Análisis. – Existe un control debidamente controlado para personas internas como externas dentro de la institución financiera ya que los datos que maneja son de absoluta reserva, aun así los sistemas de información dentro de la entidad financiera pueden ser vulnerados y pueden generar algún tipo de riesgo.

4.- ¿Existe un plan de mantenimiento para los equipos informáticos dentro de la institución financiera?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	100%
No	0	0%
Total	4	100%

Tabla 7 Cuadro porcentual pregunta 4

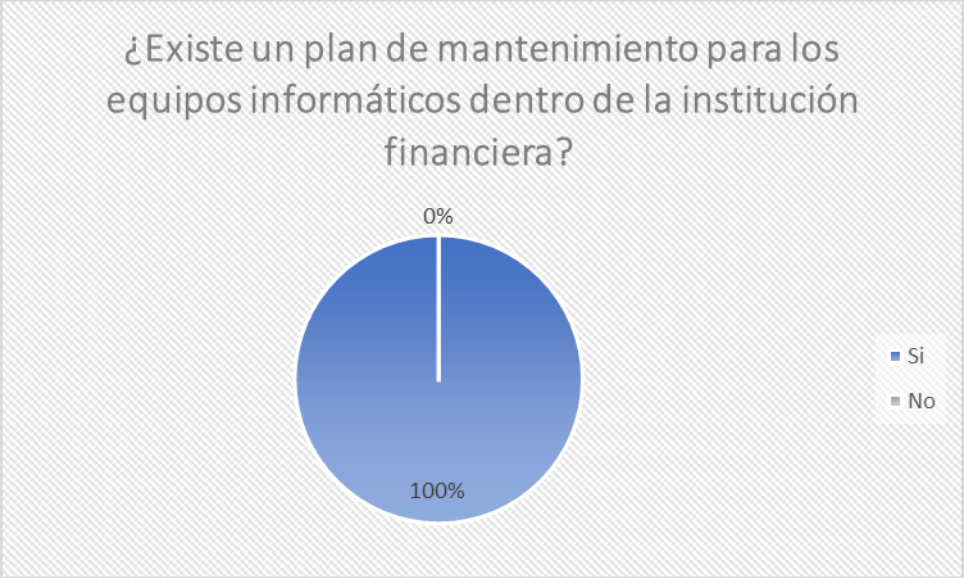


Grafico 5 pregunta 4

Interpretación. – Del total de entrevistados, el 100% de los entrevistados afirman que existe un plan de mantenimiento para los equipos informáticos dentro de la institución financiera, además de el soporte que se da en los problemas que pudiera suscitarse a cualquiera de los usuarios dentro de la entidad financiera.

Análisis. – Los mantenimientos tanto correctivos como preventivo en los equipos informáticos son muy importantes dentro de la entidad financiera, lo que prolonga un mejor desempeño de los equipos informáticos así como su duración lo que permite llevar un desempeño favorable por parte del usuario.

5.- ¿Existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución financiera?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	100%
No	0	0%
Total	4	100%

Tabla 8 Cuadro porcentual pregunta 5

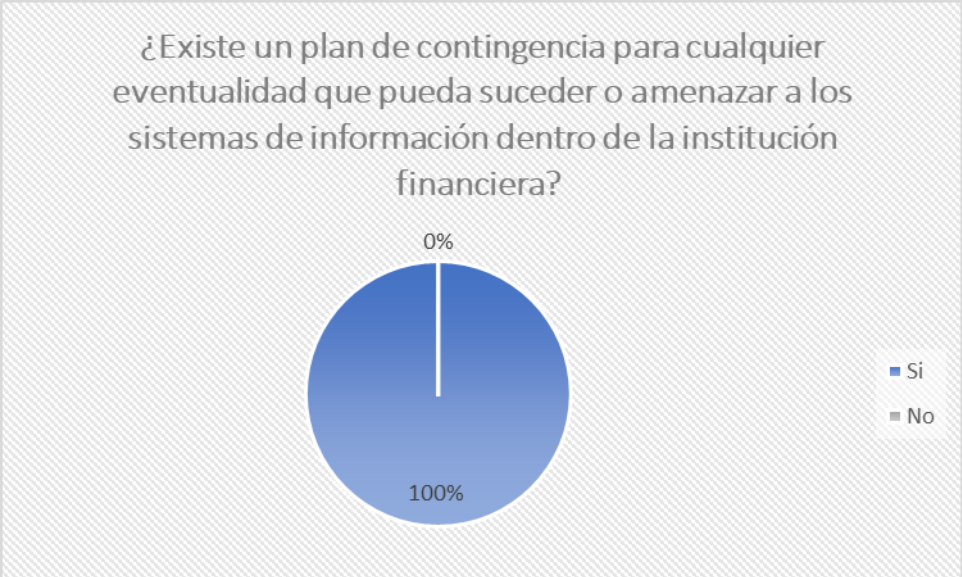


Grafico 6 pregunta 5

Interpretación. – Del total de entrevistados, el 100% de los entrevistados afirma que existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución financiera, el cual es creado anualmente, así como supervisado por la **SEPS** (Superintendencia de Economía Popular y Solidaria).

Análisis. – El desempeño correcto de la entidad financiera depende del correcto funcionamiento del sistema de información que maneja la entidad financiera por lo que es necesario tener un plan de contingencia para cualquier eventualidad que pudiera suscitarse en cualquier momento dentro de la institución.

6.- ¿Se realizan tareas de monitoreo a los sistemas de información con los empleados en la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	3	75%
No	1	25%
Total	4	100%

Tabla 9 Cuadro porcentual pregunta 6

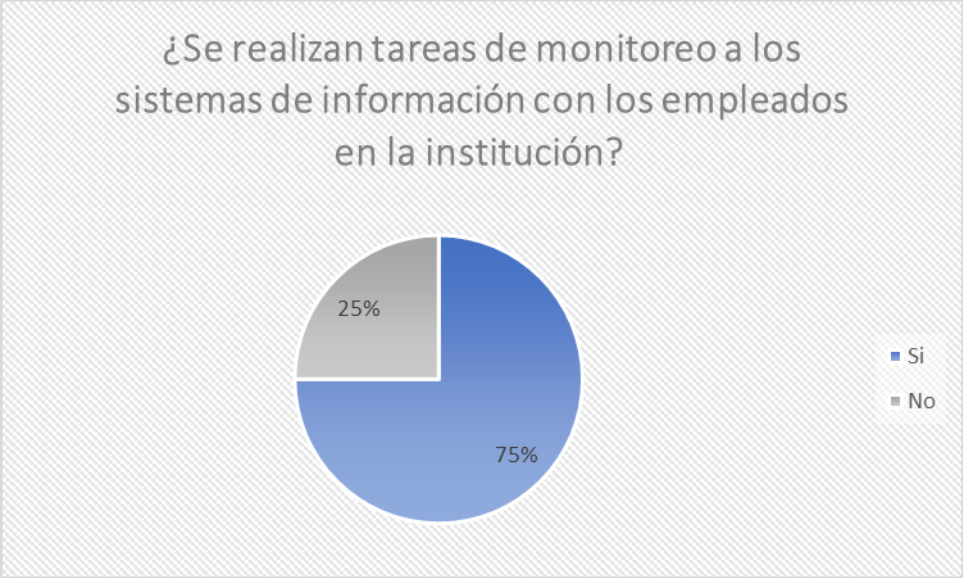


Grafico 7 pregunta 6

Interpretación. – Del total de entrevistados, el 100% de los entrevistados afirma que existe un plan de contingencia para cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución financiera, el cual es creado anualmente, así como supervisado por la **SEPS** (Superintendencia de Economía Popular y Solidaria).

Análisis. – El desempeño correcto de la entidad financiera depende del correcto funcionamiento del sistema de información que maneja la entidad financiera por lo que es necesario tener un plan de contingencia para cualquier eventualidad que pudiera suscitarse en cualquier momento dentro de la institución.

7.- ¿Cuáles son las técnicas, mecanismo y/o herramientas que se apliquen para la seguridad de los sistemas de información de la institución financiera?

Respuesta. – La entidad financiera cuenta con varios mecanismos o técnicas para la seguridad de los sistemas de información, así como la encriptación de datos en especial las de mayor vulnerabilidad como las contraseñas de los usuarios, así como

se utiliza la doble autentificación para el ingreso al core financiero, mientras que como herramientas se utiliza el antivirus y firewall para un mayor control y seguridad.

Análisis. – La utilización de técnicas o mecanismos, como el de herramientas nos permite tener una mayor seguridad de los sistemas de información de la entidad financiera.

8.- ¿Se lleva un control y administración adecuado para el inventario de activos informáticos de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	100%
No	0	0%
Total	4	100%

Tabla 10 Cuadro porcentual pregunta 8

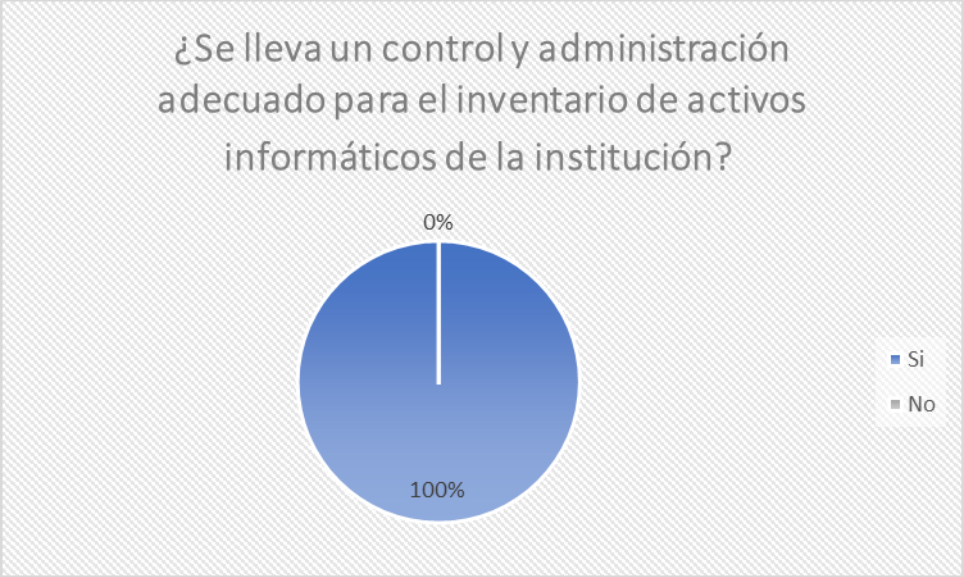


Grafico 8 pregunta 8

Interpretación. – Del total de entrevistados, el 100% de los entrevistados afirma que se lleva un control y una adecuada administración para el inventario de activos informáticos dentro de la entidad financiera con un manual de procesos, así como el valor económico de cada uno de los activos.

Análisis. – La entidad financiera lleva el control adecuado de los activos informáticos, lo que le permite una mejor estructura, así como un mayor control sobre los equipos y cada uno de los usuarios al saber el responsable del manejo de cada uno de los activos.

9.- ¿Conoce Ud. Acerca de algún Sistema de Gestión de Seguridad de la Información (SGSI)?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	0	0%
No	4	100%
Total	4	100%

Tabla 11 Cuadro porcentual pregunta 9

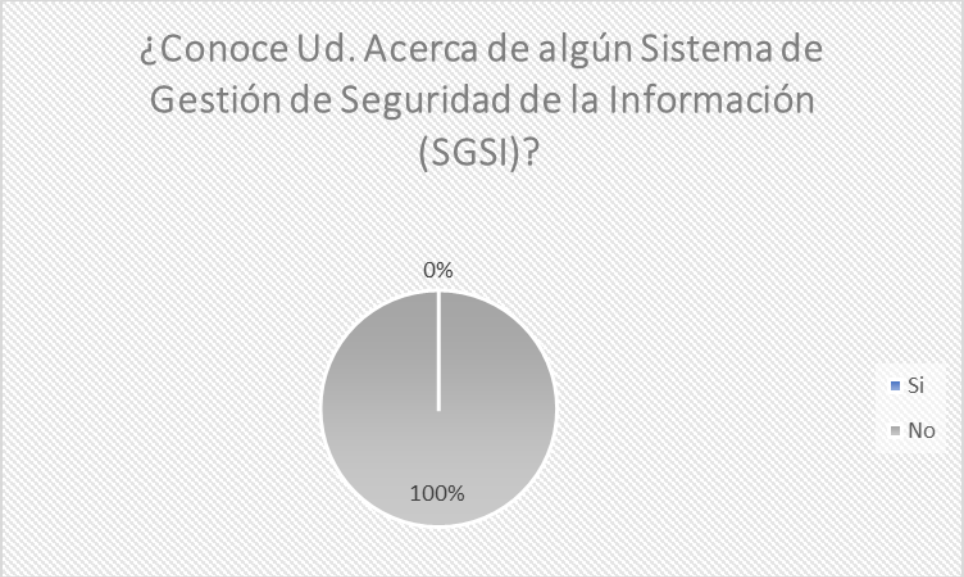


Grafico 9 pregunta 9

Interpretación. – Del total de entrevistados, el 100% de los entrevistados no conoce acerca de algún sistema de seguridad de la información.

Análisis. – El departamento de tecnologías de información de la entidad financiera desconoce sobre los sistemas de gestión de seguridad de la información, entonces desconocen tanto las ventajas como los múltiples beneficios que se puede obtener al contar con un sistema de seguridad.

3.1.2 Desarrollo de la propuesta

Antes de establecer un sistema de gestión de seguridad, es necesario aclarar que el término "sistema", no necesariamente se asocia con el desarrollo o implementación de un software o aplicativo informático.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados

por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para el siguiente proyecto se adoptó la metodología del ciclo Deming o también conocido como ciclo continuo (PDCA), tradicional en los sistemas de gestión de seguridad.

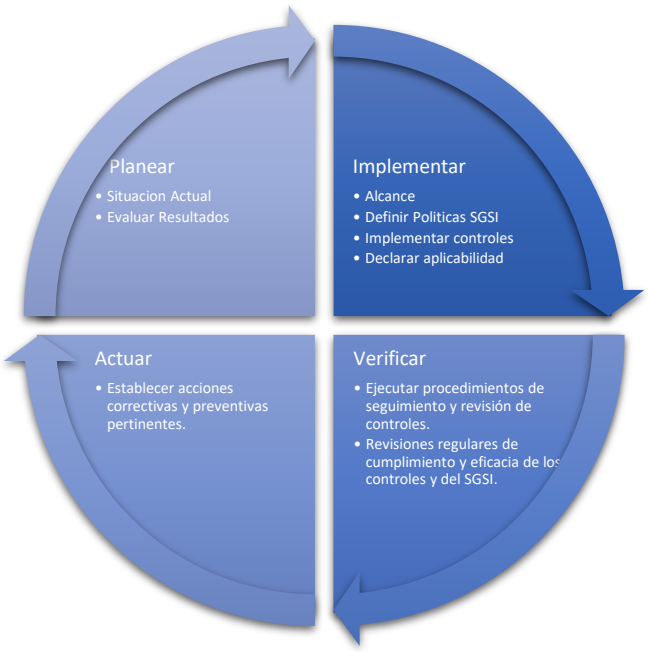


Grafico 10 Metodología de aplicación – ciclo de Deming

3.1.2.1 Políticas existentes en el Departamento de Tecnologías de la Información

El Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC, al momento no tiene políticas establecidas para realizar los diferentes técnicas y procesos que garanticen la seguridad de la información dentro del departamento, existen varias pautas o reglas que se implementaron para cubrir los diferentes procesos los cuales deberían tener y contar con una política estructurada con las diferentes normas para la seguridad de la información.

Entre las normas que se encontraron en el departamento de tecnologías de la información, podemos detallar las siguientes:

- Los usuarios se encuentran capacitados de forma permanente para la utilización de os diferentes recursos informáticos.

- El uso de actas de confidencialidad para el ingreso al core financiero.

- Existe un plan de mantenimiento anual de los recursos informáticos.
- Existe un plan de contingencia que es realizada anualmente, previamente aprobada por la SEPS (Superintendencia de Economía y Popular).
- Para el ingreso del sistema de información de la institución financiera se requiere una doble autentificación.
- Control de manual de procesos.
- Control de inventarios
- Respaldo de la información internamente como externamente.

3.1.2.2 Situación Actual de la Seguridad de la Información

Para determinar el estado actual de la seguridad de la información dentro del departamento se realizó un examen con la utilización de varias herramientas de vulnerabilidades, las cuales permitieron comprobar infraestructura, puertos, etc.

3.1.2.3 Herramientas para la ejecución del análisis de vulnerabilidades

Para el análisis de debilidades o vulnerabilidades se realizó pruebas con varias herramientas que permitieron obtener resultados específicos los mismos que serán analizados más adelante detalladamente, dentro de las herramientas que se escogieron tenemos las que se especifican a continuación:

Herramientas de reconocimiento

Herramienta / Características	Maltego	Visual Route	The Harvester
Costo	Libre/Pagada	Pagada	Libre
Plataforma	Windows Mac Linux	Windows Mac	Linux
Actualizaciones Soporte	Si	Si	Si
Dificultad utilidad	Medio	Fácil	Medio

Tabla 12 Herramientas de reconocimiento

The Harvester y Maltego son dos muy buenas herramientas ya que tienen su versión libre a la vez que se puede obtener actualizaciones inmediatas ya que vienen en el sistema operativo Kali Linux, ambas herramientas se utilizaron para reconocimiento dentro de la Cooperativa de Ahorro y Crédito Indígena SAC.

Herramienta de sondeo de puertos

Herramienta / Características	Nmap	SuperScan4	NetScan6
Costo	Gratuita	Libre/Pagada	Libre/Pagada
Plataforma	Windows Mac Linux Unix	Windows Mac	Linux
Actualizaciones Soporte	Si	Si	Si
Dificultad utilidad	Medio	Fácil	Fácil

Tabla 13 Herramientas de sondeo de puertos

Tras el análisis de la tabla 13, Nmap es la herramienta con la que se realizara el análisis dado que es la más adecuada además la misma cuenta con varias funciones como escaneo de puertos abiertos, servicios y aplicaciones que se ejecutan dentro de ellos además de scripts que permiten tener resultados más precisos y completos.

Herramientas de detección de vulnerabilidades

Herramienta / Características	Nexpose	OpenVAS	Nessus
Costo	Libre	Libre	Libre/Pagada
Plataforma	Windows Linux	Windows Linux	Windows Mac Linux
Actualizaciones Soporte	Si	Si	Si
Dificultad utilidad	Fácil	Fácil	Medio

Tabla 14 Herramientas de detección de vulnerabilidades

3.1.2.4 Identificación de vulnerabilidades

A continuación, identificaremos las vulnerabilidades de la institución financiera, por medio de las herramientas informáticas, que fueron analizadas y estudiadas, en la Tabla 12.

La herramienta Maltego, nos permitió la exploración del dominio **coopsac.fin.ec,** con el que se pudo determinar las cuentas relacionadas a este dominio.

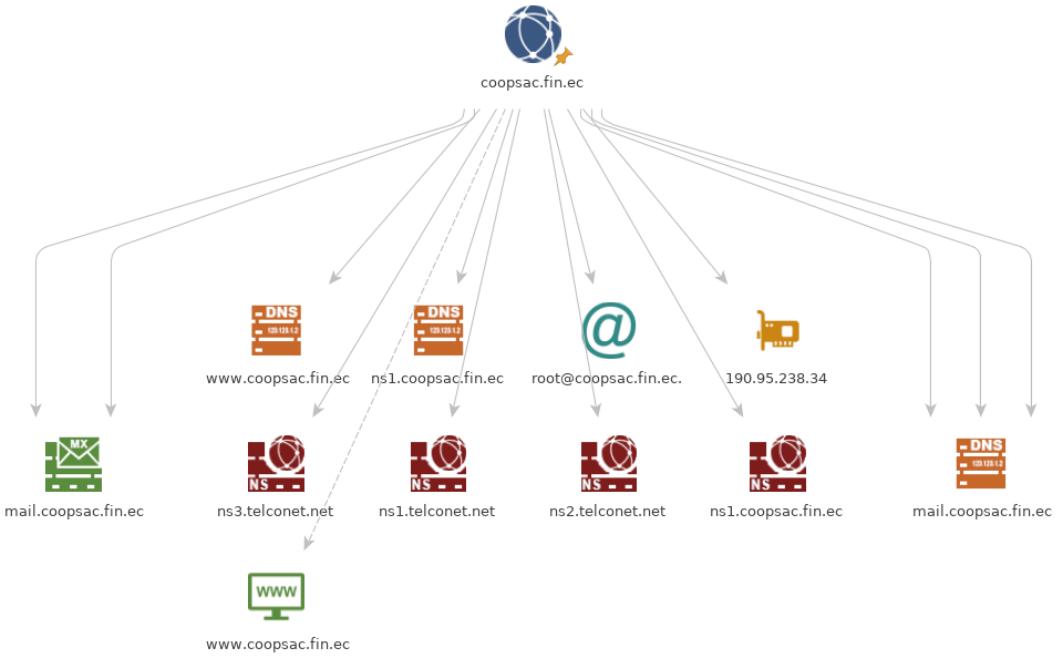


Grafico 11 Maltego, transformación en torno al dominio coopsac.fin.ec

Se puede observar en la Fig. 9, algunas transformaciones del dominio, en el que podemos apreciar, NS RECORD, DNS from Domain ,MX Record además podemos observar servidores de los correos, los servidores DNS, algunos servidores relacionados, como también la IP del dominio.

Así también con la herramienta **TheHarvester** obtendremos información que se relaciona al dominio coopsac.fin.ec.

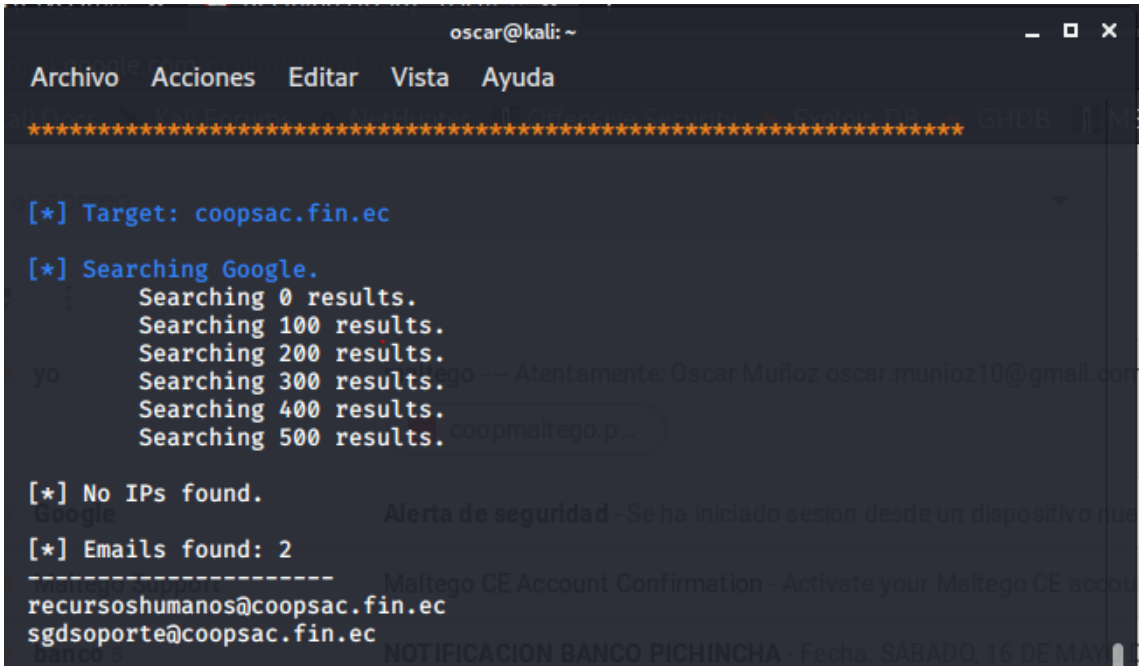


Grafico 12 TheHarvester a dominio coopsac.fin.ec

Se puede observar en la Fig.10 que, tras analizar, con la herramienta, obtuvimos algunos correos electrónicos, después de un nuevo análisis, como se presenta en la Fig. 11, obtuvimos hosts relacionados al dominio, como se presenta a continuación.

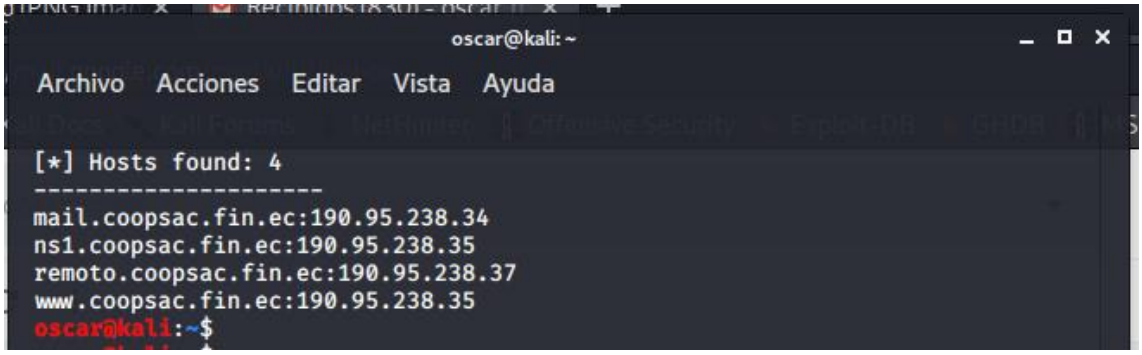


Grafico 13 TheHarvester a dominio coopsac.fin.ec

Resultados obtenidos con Maltego:

Nombre	Dirección IP	Servicio
www.coopsac.fin.ec	190.95.238.35	Web Site
www.coopsac.fin.ec	190.95.238.35	DNS Name
ns1.telconet.net	200.93.238.138	NS Record
ns2.telconet.net	200.93.238.139	NS Record
ns3.telconet.net	200.93.238.137	NS Record
ns1.coopsac.fin.ec	190.95.238.35	NS Record
mail.coopsac.fin.ec	190.95.238.34	MX Record

Tabla 15 Listado de servidores relacionados al dominio

3.1.2.5 Sondeo de Red

Obtenemos direcciones IP, estas fueron proporcionadas por el departamento de sistemas de la institución financiera, las mismas que van a ser auditadas, para esto se realizara una búsqueda en la red, se debe mencionar que el auditor no puede

obtener información que es confidencial para la Cooperativa de Ahorro y Crédito Indígena SAC.

3.1.2.6 Listado de Servidores de la institución

N°	Dirección	Nombre	Sistema Operativo
1	192.168.1.5	APP SERVER	Microsoft Windows Server 2003
2	192.168.1.13		Microsoft Windows Server 2016
3	192.168.1.205		Microsoft Windows Server 2016
4	192.168.1.250		Western Digital My Cloud (Linux 3.10)
5	192.168.122.1	10.10.0.20	Cisco 827H ADSL (IOS 12.2)

Tabla 16 Listado de Servidores a auditar

3.1.2.7 Identificación de Servicios y Sistemas

Se realizó una exploración , con los puertos de cada servidor para poder saber los servicios que se están ejecutando.

Para la exploración de los puertos utilizamos las herramientas NMAP, la misma que fue escogida anteriormente, la interfaz de esta herramienta es ZENMAP, la misma que nos indica los puertos como los servicios que esta en cada uno de los servidores.

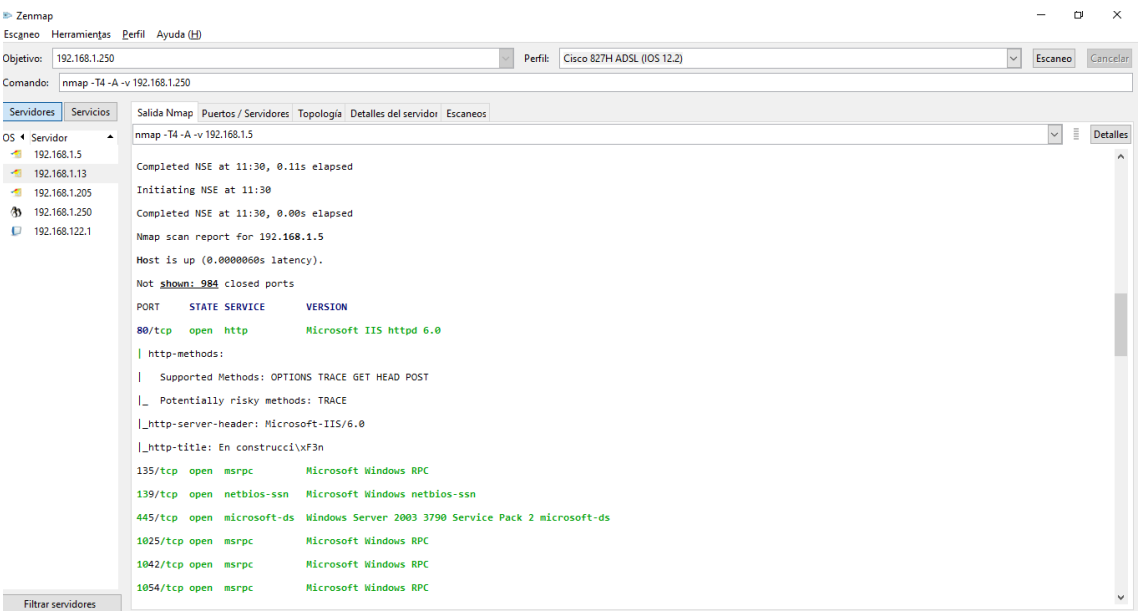


Grafico 14 Sondeo de puertos con NMAP

Servidor 192.168.1.5

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Microsoft IIS httpd 10.0
135	tcp	msrpc	t Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows Server 2008
1025	tcp	msrpc	Microsoft Windows RPC
1042	tcp	msrpc	Microsoft Windows RPC
1054	tcp	msrpc	Microsoft Windows RPC
1801	tcp	msmq	
2103	tcp	msrpc	Microsoft Windows RPC
2105	tcp	msrpc	Microsoft Windows RPC
2107	tcp	msrpc	Microsoft Windows RPC
3389	tcp	ms-wbt-server	Microsoft Terminal Services
4899	tcp	radmin	Famatech Radmin
5800	tcp	vnc-http	RealVNC E4
5900	tcp	vnc	RealVNC Enterprise 5.3
7007	tcp	remoting	MS.NET Remoting services

Tabla 17 NMAP a 192.168.1.5

Servidor 192.168.1.13

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Microsoft IIS httpd 10.0
135	tcp	msrpc	t Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows Server 2008
1801	tcp	msmq	
2103	tcp	msrpc	Microsoft Windows RPC
2105	tcp	msrpc	Microsoft Windows RPC
2107	tcp	msrpc	Microsoft Windows RPC
3389	tcp	ms-wbt-server	Microsoft Terminal Services
7070	tcp	realserver	
8085	tcp	http	Microsoft IIS httpd 10.0

Tabla 18 NMAP a 192.168.1.13

Servidor 192.168.1.205

Puerto	Protocolo	Servicio	Detalle
135	tcp	msrpc	t Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows Server 2008
1433	tcp	ms-sql-s	Microsoft SQL Server 2017
2383	tcp	ms-olap4	
3389	tcp	ms-wbt-server	Microsoft Terminal Services
7070	tcp	realserver	

Tabla 19 NMAP a 192.168.1.205

Servidor 192.168.1.250

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd
111	tcp	rpcbind	#1000000)
139	tcp	netbios-ssn	Samba smbd 3.x -4.x
443	tcp	http	Apache httpd
445	tcp	netbios-ssn	Samba smbd 4.3.11
548	tcp	afp	Netatalk 3.0.5
2049	tcp	nfs_acl	2-3 (RPC #100227)
3306	tcp	mysql	MySQL
8181	tcp	http	Plex Media Server
49152	tcp	upnp	Portable SDK

Tabla 20 NMAP a 192.168.1.250

Servidor 192.168.122.1

Puerto	Protocolo	Servicio	Detalle
135	tcp	msrpc	
139	tcp	netbios-ssn	
445	tcp	microsoft-ds	
593	tcp	http-rpc-epmap	

Tabla 21 NMAP a 192.168.122.1

En los escaneos a los servidores de la institución con la herramienta NMAP se puede observar lo siguiente:

- Se utilizan los protocolos SMTP para correo de salida e IMAP para el correo entrante.

- Se utilizan diferentes servicios de base de datos como por ejemplo MySQL y SQL

SERVER.

- Se utiliza el servidor Samba smbd para compartir archivos a través de la red.

- Se utilizan Apache httpd, IIS, para los servidores web, Apache es de código abierto para diferentes plataformas como por ejemplo Unix (BSD, GNU/Linux) mientras que IIS es exclusivo del sistema operativo Microsoft Windows.

3.1.2.8 Búsqueda y verificación de vulnerabilidades

A continuación, se buscaron errores o vulnerabilidades, dentro de todos los sistemas operativos que se encuentran en la entidad financiera, para esto se utilizó las herramientas que se escogieron con anterioridad, OpenVAS y Nessus, las mismas que fueron instalados en el sistema operativo Kali Linux Análisis de vulnerabilidades con OpenVAS

OpenVAS se encuentra disponible como para escritorio y para web, para este análisis utilizamos la versión web, que es el Asistente de Seguridad Greenbone, para esto primero se crea un Target(objetivo) que este es la IP que vamos a escanear, a su vez se crea también una tarea, para que analice todos los objetivos, que se desea, esta vez escogimos la opción de Full and very Deep, esta nos dará un resultado completo después del escaneo.

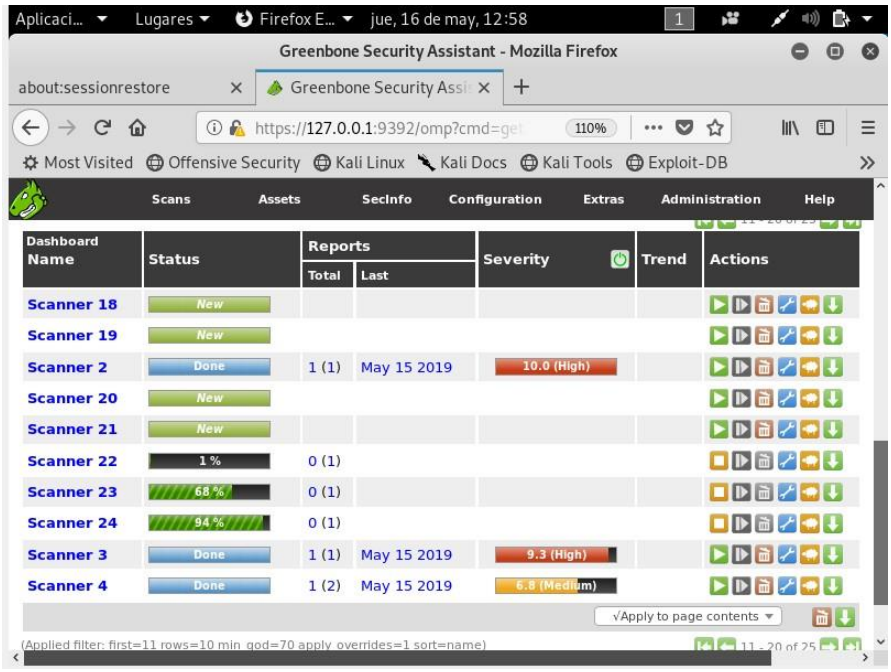


Grafico 15 Escaneo de vulnerabilidades con OpenVAS

Se detallan las vulnerabilidades detectadas con OpenVAS en las tablas de a continuación:

Servidor 192.168.1.5

Servicio	Vulnerabilidad	Riesgo	Observación
msrdp	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
msrdp	Certificado SSL firmado con un algoritmo de hash débil.	Medio	Un algoritmo de firma débil es vulnerable a los ataques de colisión, un atacante puede generar otro certificado con la misma firma digital.
Microsotf- ds	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
Msrdp	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140

Tabla 22 Vulnerabilidades detectadas en 192.168.1.5 OpenVAS

Servidor 192.168.1.13

Servicio	Vulnerabilidad	Riesgo	Observación
80/http	Detección de versiones no compatibles con Microsoft IIS 6.0	Alto	La falta de soporte que en los nuevos parches de seguridad para el producto será por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.
microsotf- ds	MS 17-010: Actualización de seguridad para Microsoft Windows SMB Server	Alto	Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a la gestión impropia de ciertas solicitudes.
microsotf- ds	Autenticación de sesión nula de Microsoft Windows SMB	Medio	Según la configuración, es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.
Ms-wbt-server	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
Ms-wbt-server	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140

Tabla 23 Vulnerabilidades detectadas en 192.168.1.13 OpenVAS

Servidor 192.168.1.205

Servicio	Vulnerabilidad	Riesgo	Observación
msrdp	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
msrdp	Certificado SSL firmado con un algoritmo de hash débil.	Medio	Un algoritmo de firma débil es vulnerable a los ataques de colisión, un atacante puede generar otro certificado con la misma firma digital.
Microsotf- ds	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
Msrdp	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140

Tabla 24 Vulnerabilidades detectadas en 192.168.1.205 OpenVAS

Servidor 192.168.1.250

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.12	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
domain	Divulgación de información remota de indagación de caché del servidor DNS	Medio	El servidor DNS remoto responde a las consultas de los dominios de terceros que no tienen establecido el bit de recursión.
Ms-wbt-server	Terminal Services no usa autenticación de nivel de red (NLA)	Medio	NLA utiliza el protocolo del Proveedor de soporte de seguridad de credenciales (CredSSP) para realizar una autenticación sólida a través de mecanismos TLS / SSL o Kerberos.
	Divulgación de IP interna del encabezado HTTP del servidor web	Bajo	Esto puede exponer las direcciones IP internas que generalmente están ocultas o enmascaradas detrás de un servidor de seguridad o servidor proxy de traducción de direcciones de red (NAT).

Tabla 25 Vulnerabilidades detectadas en 192.168.1.250 OpenVAS

Servidor 192.168.122.1

Servicio	Vulnerabilidad	Riesgo	Observación
Samba smbd 4.6.2	Microsoft Windows SMB comparte acceso sin privilegios	Medio	El control remoto tiene uno o más recursos compartidos de Windows a los que se puede acceder a través de la red con las credenciales proporcionadas.
OpenSSH 7.5 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
Nfs	NFS recursos compartidos de lectura mundial	Medio	El servidor NFS remoto está exportando uno o más sin restringir el acceso (según la IP del nombre de host o el rango de IP).
Samba smbd 4.6.2	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
OpenSSH 7.5 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).

Tabla 26 Vulnerabilidades detectadas en 192.168.122.1 OpenVAS

Análisis de vulnerabilidades con Nessus

Para usar Nessus, se debe crear un nuevo escaneo para el cual definimos primero la política ya existente, que es la Avanced Scan que es la recomendada, ingresamos cada uno del host que vamos a analizar, estos se guardan, y posteriormente se analizan las vulnerabilidades de cada objetivo.

Servidor 192.168.1.5

Servicio	Vulnerabilidad	Riesgo	Observación
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Ms-wbt-server	Informe de suites de cifrado débil	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.
TCP	Marcas de tiempo TCP	Bajo	El host remoto implementa las marcas de tiempo TPC y, por lo tanto, permite calcular el tiempo de actividad

Tabla 27 Vulnerabilidades detectadas en 192.168.1.5 Nessus

Servidor 192.168.1.13

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft SQL Server 2008	Detección de fin de vida de Microsoft SQL Server	Alto	La versión de Microsoft SQL Server en el host remoto ha llegado al final de su vida útil y ya no debe utilizarse.
Microsoft- ds	Microsoft Windows SMB Server Múltiple vulnerabilidades remotas	Alto	A este host le falta una actualización de seguridad crítica según Microsoft Bulletin MS17-010.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Microsoft IIS httpd 6.0	Vulnerabilidad en la divulgación de información de carácter de tilde de Microsoft IIS	Medio	Este host ejecuta el servidor web Microsoft IIS y es propenso a la divulgación de información.

Tabla 28 Vulnerabilidades detectadas en 192.168.1.13 Nessus

Servidor 192.168.1.205

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft- ds	MS 17-010: Actualización de seguridad para Microsoft Windows SMB Server	Alto	Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a la gestión impropia de ciertas solicitudes.
Ms-wbt-server	MS12-020: Vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código	Medio	Existe una vulnerabilidad de código arbitrario en la implementación del Protocolo de escritorio remoto (RDP) en los hosts remotos de Windows.
Msrpc	MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD	Medio	El host de Windows de seguridad remota se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Gestor de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación de nivel de autenticación inadecuada a través de los

Tabla 29 Vulnerabilidades detectadas en 192.168.1.205 Nessus

Servidor 192.168.1.250

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.12 (Win32)	Varias vulnerabilidades del servidor HTTPD de Apache	Alto	Este host ejecuta el servidor HTTP Apache y es propenso a múltiples vulnerabilidades.
Apache httpd 2.4.12 (Win32)	Vulnerabilidad de ataque del Apache HTTP Server Man-in-the-Middle	Medio	Este host se instala con el servidor HTTP Apache y es propenso a la vulnerabilidad de ataque del hombre en el medio.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Ms-wbt-server	Informe de suites de cifrado débil	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.

Tabla 30 Vulnerabilidades detectadas en 192.168.1.250 Nessus

Servidor 192.168.122.1

Servicio	Vulnerabilidad	Riesgo	Observación
ProFTPD	FTP sin cifrar inicio de sesión de texto claro	Medio	El host remoto está ejecutando un servicio FTP que permite inicios de sesión de texto simple en conexiones no cifradas.
ngnix	Transmisión de texto claro de información sensible a través de HTTP	Medio	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto sin cifrar a través de HTTP
OpenSSH 7.5(protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.

Tabla 31 Vulnerabilidades detectadas en 192.168.122.1 Nessus

3.1.2.9 Diseño del SGI

Un modelo SGSI basado en la ISO/IEC 27001 está estructurado bajo el siguiente modelo, con el que se pretende que los riesgos encontrados en la seguridad de la información, se minimicen en la Cooperativa de Ahorro y Crédito Indígena SAC.

Aspectos SGSI:

- Definición del alcance
- Definición de las políticas de seguridad
- Gestión de riesgos
- Declaración de aplicabilidad
- Cumplimiento de procedimientos y controles

3.1.2.10 Alcance del SGSI

El alcance será definido de acuerdo a las características que se tienen en la cooperativa, siendo estas las que cubren cada uno de los aspectos involucrados tales como recursos, activos, procesos, etc.

El alcance del SGSI estará definido como se detalla a continuación:

- Control de activos. - Un control adecuado de todos los activos con los que cuenta la cooperativa, ayudara a un mejor manejo de la seguridad de la información, así como lindar responsabilidades al personal que hace uso de

cada una de los activos en relación a las vulnerabilidades y riesgos dentro de la institución financiera.

- Control de recursos humanos. – Un control adecuado y capacitaciones oportunas dentro de la institución financiera, así como el compromiso del recurso humano ayudara a que exista un mejor control de la seguridad de la información, como una mejor gestión en los recursos durante el periodo laboral o culminación del mismo.
- Gestión de acceso. – Un mejor control y una adecuada verificación previo a ingresar, así como el control de acceso a cualquiera de los recursos de la institución financiera ayudara a la integridad y confianza de la información.
- Control de las operaciones y comunicación. – Es fundamental garantizar la comunicación y la funcionalidad de los sistemas de información, ante cualquier eventualidad que pudiera suscitarse dentro de la institución financiera.

3.1.2.11 Política de seguridad

Para establecer una política de seguridad que comprenda todas las necesidades que estén relacionadas con la gestión de la seguridad de la información en la institución financiera la misma que ayudara a la implementación del SGSI dentro de Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indígena SAC, es la siguiente.

"Fomentar hábitos y destrezas dentro de la institución para asegurar el manejo adecuado de los procesos del departamento de Tecnologías de la Información a través de un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y de mejora constante que mantenga la integridad, confidencialidad y disponibilidad de la información".

3.1.2.12 Enfoque de evaluación de riesgos

Es fundamental investigar y analizar los diferentes riesgos que pueden suscitarse y que afecten los procesos que se llevan a cabo en la institución y más aún si dichos procesos cuentan con información relevante.

El objetivo de la evaluación es determinar si un riesgo es aceptable o infringe las normas institucionales, para lo cual se definió una metodología a través de la que se analizara y evaluara los riesgos existentes.

Dicha evaluación se basa en un método cualitativo en la que se detallan los activos de la institución, se identifican las amenazas relacionado con cado uno de ellos y la posibilidad de que dichas amenazas se cumplan.

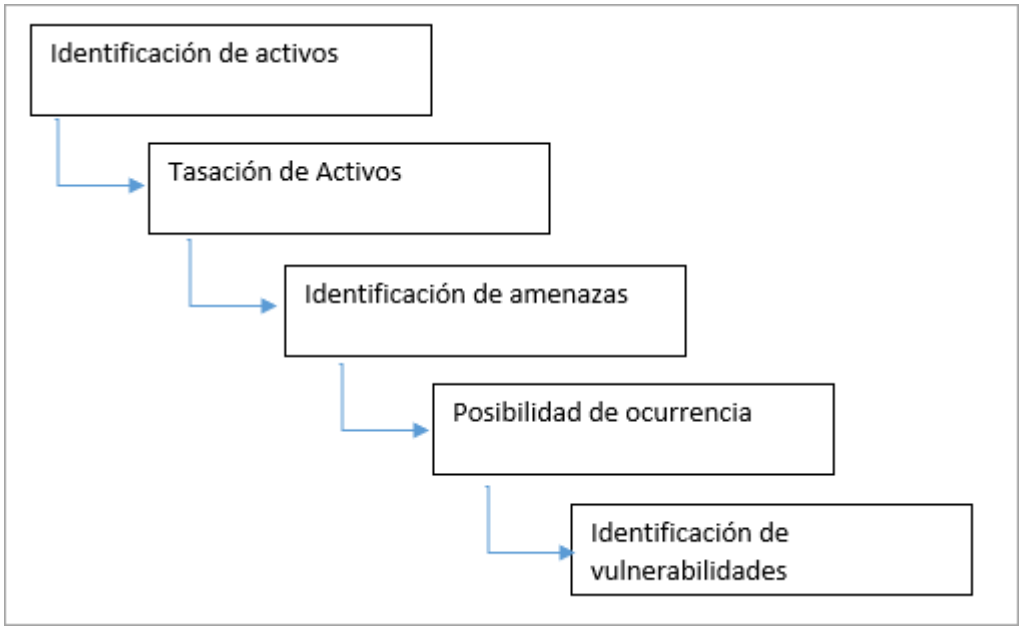


Grafico 16 Metodología evaluación de riesgos

Elaborado por: Investigador

3.1.2.13 Identificación y tasación de activos

Entre lo más importante dentro de la institución están los activos ya que son los canales por los cuales se transmite la información, debido a esto es importante la protección suficiente de los mismos, una vez identificados los activos que existen, estos deben ser tasados para establecer los de mayor importancia, basados en los niveles de integridad, disponibilidad y confidencialidad de la información.

Después de la tasación se establece la probabilidad de incidencia de las amenazas, asumiendo el impacto en el caso de suscitarse, lo que implicaría riesgo en la confiabilidad, integridad y disponibilidad de la información.

La fórmula para establecer el riesgo es la siguiente:

Riesgo = Valoración total del activo × Probabilidad de amenaza

3.1.2.14 Inventario de Activos Informáticos

Dentro los activos que forman parte de todos los procesos que se lleva a cabo en la institución existen varios tipos de activos informáticos, como son los del sistema de información, los de tipo software y los de tipo físico.

Para la evaluación de estos activos tenemos un rango de 1 a 5 para después obtener el promedio para cada uno de los niveles.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Archivos	4	4	4	4
Computadores de oficina	3	4	3	3
Switch	2	3	3	3
Central Telefónica IP	2	4	3	3
Router	4	4	4	4
Cuentas de usuario	4	4	3	4
Correo Institucional	2	3	2	2
Core Financiero (Sistema Financiero)	4	4	4	4
Impresora Multifunción	3	3	4	3

Tabla 32 Identificación y tasación de riesgos

Lo siguiente es determinar todos los activos con un resultado mayor o igual a 3 para evaluar los riesgos correspondientes.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Servidor de archivos	Información no verificada o alterada	Las medidas de seguridad no sean las adecuadas o carezcan de estas	4	3	12
	Hurto de información	Falta de mantenimiento			
Computadores de escritorio	Virus	Falta de mantenimiento	3	4	12
	Malware	Uso inadecuado del internet			
		Libre acceso en la internet			
	Spyware	Falta de controles			
	Phishing	Carencia de herramientas de monitoreo			
Switch	Sobrecalentamiento	Problemas de alimentación eléctrica	3	3	9
	Perdida o daño irreparable				

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Central Telefónica IP	Perdida de conexión	Configuración inadecuada en central telefónica	3	3	9
Router	Rendimiento	Tráfico de Datos	3	3	9
		Mala ubicación			
	Sobrecalentamiento	Problemas de alimentación eléctrica			
Cuenta de usuarios	Perdida de usuario	Control de acceso inadecuado	3	3	9
	Modificación de cuenta				

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Core Financiero (Sistema Financiero)	Robo de Información	Falta políticas de seguridad	4	3	12
		Falta de control de acceso			
Impresoras Multifunción	Atasco de papel	Papel incompatible	3	3	9
	Avería de cabezales	Falta de mantenimiento			
	Cartuchos incompatibles	Falta de control de calidad			

Tabla 33 Activos de mayor importancia

Una vez finalizado el análisis y evaluación de riesgos de los activos informáticos pertenecientes a la institución se puede identificar los activoscon las tasas más altas de afectación dado posibles ataques, daños y/o vulnerabilidades.

3.1.2.15 Selección de objetivos de Control

A continuación, se procede a relacionar los controles definidos en la norma ISO 27001, tomando como referencia los activos con mayor índice de riesgo en las tablas elaboradas anteriormente. – Posteriormente se enuncia los 11 dominios que conforman la norma IS0 27001.

3.1.2.16 Áreas o Dominios de la ISO 27001:

- A.5 Políticas de seguridad de la información.
- A.6 Organización de seguridad de la información.
- A.7 Seguridad relativa a los recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y del entorno.
- A.12 Seguridad de las operaciones.
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.15 Relación con proveedores.
- A.16 Gestión de incidentes de seguridad de la información.
- A, 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
- A.18 Cumplimiento

A continuación, tenemos la columna de “Objetivo de Control” la misma que tiene los dominios de la ISO con las amenazas que corresponden a cada una de las amenazas que se detalla en los activos informáticos.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivo de Control
Servidor de archivos	Información no verificada o alterada	Las medidas de seguridad no sean las adecuadas o carezcan de estas	4	3	12	A.11 Seguridad física y del entorno
	Hurto de información	Falta de mantenimiento				
Computadores de escritorio	Virus	Falta de mantenimiento	3	4	12	A.9 Control de acceso A.11 Seguridad física y del Entorno A.12 Seguridad de las operaciones
	Malware	Uso inadecuado del internet				
		Libre acceso en la internet				
	Spyware	Falta de controles				
	Phishing	Carencia de herramientas de monitoreo				
Switch	Sobrecalentamiento	Problemas de alimentación eléctrica	3	3	9	A.11 Seguridad física y del Entorno A.13 Seguridad de las comunicaciones
	Perdida o daño irreparable					

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivo de Control
Central Telefónica IP	Perdida de conexión	Configuración inadecuada en central telefónica	3	3	9	A.11 Seguridad física y del Entorno A.13 Seguridad de las comunicaciones
Router	Rendimiento	Tráfico de Datos	3	3	9	A.11 Seguridad física y del Entorno A.13 Seguridad de las comunicaciones
		Mala ubicación				
	Sobrecalentamiento	Problemas de alimentación eléctrica				
Cuenta de usuarios	Perdida de usuario	Control de acceso inadecuado	3	3	9	A.9 Control de acceso
	Modificación de cuenta					

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivo de Control
Core Financiero (Sistema Financiero)	Robo de Información	Falta políticas de seguridad	4	3	12	A.9 Control de acceso A.5 Políticas de seguridad de la Información
		Falta de control de acceso				
Impresoras Multifunción	Atasco de papel	Papel incompatible	3	3	9	A.8 Gestión de activos A.11 Seguridad física y del entorno
	Avería de cabezales	Falta de mantenimiento				
	Cartuchos incompatibles	Falta de control de calidad				

Tabla 34 Activos de mayor importancia

3.1.2.17 Declaración de aplicabilidad

Entre los puntos más importantes dentro del SGSI es la Declaración de Aplicabilidad - SOA (Arquitectura Orienta a Servicios) que es la que da el punto de partida para la instauración del SGSI con una alta escalabilidad dentro de la institución financiera, esta se encuentra basada en las áreas y los dominios de la ISO 27001.

Para este paso que tiene como finalidad la de identificar y analizar cada uno de todos los controles aplicables dentro del departamento de la información de la Cooperativa de Ahorro y Crédito Indígena SAC para su uso, así también la identificación de cada uno de los controles que no son aplicables los cuales no se usan con la debida justificación.

Todo este proceso de aplicabilidad tendrá que ser revisada para su posterior aprobación por el Jefe del departamento de tecnologías de la información, fundamentalmente esta consistirá en:

- Área o Dominio de control de la norma ISO 27001.
- Objetivos de control de cada Dominio.
- Justificación de controles de cada Objetivo de control escogido.

A.5 Políticas de seguridad de la Información

Política	**Análisis**			
A.5 Políticas de seguridad de la información	**Sección**		A.5.1 Directrices de gestión de la seguridad de la información	
	Control de la ISO 27001		5.1.1	5.1.2
			Políticas para la seguridad de la información	Revisión de las políticas para la seguridad de la información
	Aplicabilidad	**Si**	X	X
		No		
	Justificación		Es muy importante la creación de un documento con las políticas de seguridad para la entidad financiera ya que una de las cosas más importantes dentro de esta es la información, que se almacena, así mismo es fundamental su revisión periódica .	

Tabla 35 Políticas de seguridad de la información

A.8 Gestión de activos

Política	Análisis					
A.8 Gestión de activos	**Sección**		8.1 Responsabilidad sobre los activos			
	Control de la ISO 27001		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 los activos
	Aplicabilidad	**Si**	X	X	X	X
		No				
	Justificación		La entidad financiera actualmente cuenta con un control de activos			

Tabla 36 Gestión de activos – responsabilidad sobre los activos

A.8 Gestión de activos	**Sección**		8.2 Clasificación de la información		
	Control de la ISO 27001		8.2.1	8.2.2	8.2.3
			Clasificación de la información	Etiquetado de la información	Manipulado de la información
	Aplicabilidad	**Si**	X	X	X
		No			
	Justificación		Es muy importante que la información que se maneja en la entidad financiera tenga una adecuada protección.		

Tabla 37 Gestión de activos – clasificación de la información

A.8 Gestión de activos	**Sección**		8.3 Manipulación de los soportes		
	Control de la ISO 27001		8.3.1	8.3.2	8.3.3
			Gestión de soportes extraíbles	Eliminación de soportes	Soportes físicos en tránsito
	Aplicabilidad	**Si**			
		No	X	X	X
	Justificación		La entidad financiera ya cuenta con este apartado		

Tabla 38 Gestión de activos - manipulación de los soportes

- **A.9 Control de Acceso**

Política	**Análisis**			
A.9 Control de acceso	**Sección**		A.9.1 Requisitos de negocio para el control de acceso	
	Control de la ISO 27001		9.1.1	9.1.2
			Política de control de acceso	Acceso a las redes y a los servicios de red
	Aplicabilidad	**Si**	X	X
		No		
	Justificación		Es importante también mantener vigilado los recurso de la red y que estos sean utilizados para el bien común de la empresa	

Tabla 39 Control de Acceso- requisitos de negocio para el control de acceso

Política	**Análisis**							
A.9 Control de acceso	**Sección**		A.9.2 Gestión de acceso de usuario					
	Control de la ISO 27001		9.2.1	9.2.2	9.2.3	9.2.4	9.2.5	9.2.6
			egistro y baja de usuario	Provisión de acceso de usuario	Gestión de privilegios de acceso	Gestión de la información secreta de autenticación de los usuarios	Revisión de los derechos de acceso de usuario	Retirada o reasignación de los derechos de acceso
	Aplicabilidad	**Si**	X	X	X	X	X	X
		No						
	Justificación		o la red de un posible acceso no autorizado ya que este sería un inconveniente en la red y servicio de la entidad financiera					

Tabla 40 Control de acceso - gestión de acceso de usuario

Política	Análisis		
A.9 Control de acceso	**Sección**		A.9.3 Responsabilidades del usuario
	Control de la ISO 27001		9.3.1 Uso de la información secreta de autenticación
	Aplicabilidad	**Si**	X
		No	
	Justificación		Es importante una política para salvaguardar toda la información de los usuarios y que estos sean debidamente autenticados así evitar ingresos no adecuados de otros usuarios.

Tabla 41 Control de acceso - responsabilidades de usuario

Política	Análisis						
A.9 Control de acceso	Sección		A.9.4 Control de acceso a sistemas y aplicaciones				
	Control de la ISO 27001		9.4.1 Restricción del acceso a la información	9.4.2 Procedimientos seguros de inicio de sesión	9.4.3 Sistema de gestión de contraseñas	9.4.4 Uso de utilidades con privilegios del sistema	9.4.5 Control de acceso al código fuente de los programas
	Aplicabilidad	Si	X	X	X	X	X
		No					
	Justificación		Es importante la creación de roles en el departamento de sistemas para que estos sean restringidos a cada una de las tareas que el usuario necesite para su desempeño diario, así evitar accesos a información crítica de la entidad financiera.				

Tabla 42 Control de acceso - control de acceso a sistemas y aplicaciones

- **A.11 Seguridad física y del entorno**

Política	**Análisis**							
A.11 Seguridad física y del entorno	**Sección**		A.11.1 Áreas seguras					
	Control de la ISO 27001		A.11.1.1	A.11.1.2	A.11.1.3	A.11.1.4	A.11.1.5	A.11.1.6
			Perímetro de seguridad física	Controles físicos de entrada	Seguridad de oficinas, despachos y recursos	Protección contra las amenazas externas y ambientales	El trabajo en áreas seguras	Áreas de carga y descarga
	Aplicabilidad	**Si**	X	X	X	X	X	X
		No						
	Justificación		Es importante evita el acceso no autorizado de la información y todos los recursos de la entidad financiera					

Tabla 43 Seguridad física y del entorno - áreas seguras

Política	**Análisis**									
A.11 Seguridad física y del entorno	**Sección**		A.11.2 Seguridad de los equipos								
	Control de la ISO 27001		A.11.2.1	A.11.2.2	A.11.2.3	A.11.2.4	A.11.2.5	A.11.2.6	A.11.2.7	A.11.2.8	A.11.2.9
			Emplazamiento y protección de equipos	Instalaciones de suministro	Seguridad del cableado	Mantenimiento de los equipos	Retirada de materiales propiedad de la empresa	Seguridad de los equipos fuera de las instalaciones	Reutilización o eliminación segura de equipos	Equipo de usuario desatendido	Política de puesto de trabajo despejado y pantalla limpia
	Aplicabilidad	**Si**	X	X	X	X	X	X	X	X	X
		No									
	Justificación		Es importante ya que se evita que los activos de la entidad financiera estén comprometidos tanto en robos, perdidas o daños, y ayudaría para la desactivación o interrupción dentro de la empresa.								

Tabla 44 Seguridad física y del entorno - seguridad de los equipos

- **A.12 Seguridad de las operaciones**

Política	**Análisis**					
A.12 Seguridad de las operaciones	**Sección**		A.12.1 Procedimientos y responsabilidades operacionales			
	Control de la ISO 27001		12.1.1	12.1.2	12.1.3	12.1.4
			Documentación de procedimientos operacionales	Gestión de cambios	Gestión de capacidades	Separación de los recursos de desarrollo, prueba y operación
	Aplicabilidad	**Si**	X		X	
		No		X		X
	Justificación		Es importante mantener una adecuada documentación para que cualquier persona que se cumpla su ciclo dentro de la entidad financiera pueda desempeñar su trabajo normalmente			

Tabla 45 Seguridad de las operaciones - procedimientos y responsabilidades operacionales

Política	Análisis		
A.12 Seguridad de las operaciones	**Sección**		A.12.2 Protección contra el software malicioso (malware)
	Control de la ISO 27001		12.2.1 Controles contra el código malicioso
	Aplicabilidad	**Si**	X
		No	
	Justificación		Es importante una adecuada prevención y aseguramiento contra cualquier tipo de malware.

Tabla 46 Seguridad de las operaciones - protección contra el software malicioso (malware)

Elaborado por: Investigador

Política	Análisis		
A.12 Seguridad de las operaciones	**Sección**		A.12.3 Copias de seguridad
	Control de la ISO 27001		12.3.1 Copias de seguridad de la información
	Aplicabilidad	**Si**	X
		No	
	Justificación		Es muy importante los respaldos o aseguramiento de la información para evitar pérdidas de información

Tabla 47 Seguridad de las operaciones - copias de seguridad

Política	Análisis					
A.12 Seguridad de las operaciones	**Sección**		A.12.4 Registros y supervisión			
	trol de la ISO 27001		12.4.1	12.4.2	12.4.3	12.4.4
			Registro de eventos	Protección de la información del registro	Registros de administración y operación	Sincronización del reloj
	Aplicabilidad	**Si**				
		No	X	X	X	X
	Justificación		La entidad financiera ya cuenta con este apartado			

Tabla 48 Seguridad de las operaciones - registros y supervisión

Política	Análisis		
A.12 Seguridad de las operaciones	**Sección**		A.12.5 Control del software en explotación
	Control de la ISO 27001		12.5.1
			Instalación del software en explotación
	Aplicabilidad	**Si**	
		No	X
	Justificación		La entidad financiera ya cuenta con este apartado

Tabla 49 Seguridad de las operaciones - control de software en explotación

Política	Análisis			
A.12 Seguridad de las operaciones	**Sección**		A.12.6 Gestión de la vulnerabilidad técnica	
	Control de la ISO 27001		12.6.1	12.6.2
			Gestión de las vulnerabilidades técnicas	Restricción en la instalación de software
	Aplicabilidad	**Si**	X	X
		No		
	Justificación		Es importante ya que reduce en la totalidad un riesgo de alguna vulnerabilidad de explotación .	

Tabla 50 Seguridad de las operaciones - gestión de la vulnerabilidad técnica

Política	Análisis		
A.12 Seguridad de las operaciones	**Sección**		A.12.7 Consideraciones sobre la auditoria de sistemas de información
	Control de la ISO 27001		12.7.1 Controles de auditoria de sistemas de información
	Aplicabilidad	**Si**	X
		No	
	Justificación		Es importante que se haga periódicamente una auditoria en los sistemas de información para un mejor control de esta

Tabla 51 Seguridad de las operaciones - consideraciones sobre la auditoría de sistemas de la información

- **A.13 Seguridad de las comunicaciones**

Política	**Análisis**				
A.13 Seguridad de las comunicaciones	**Sección**		A.13.1 Gestión de la seguridad de las redes		
	Control de la ISO 27001		13.1.1	13.1.2	13.1.3
			Controles de red	Seguridad de los servicios de red	Segregación en redes
	Aplicabilidad	**Si**	X	X	X
		No			
	Justificación		Es importante que todos los activos, como los recursos y las redes tengan un tratamiento adecuado de la información.		

Tabla 52 Seguridad de las comunicaciones - gestión de la seguridad de las redes

Política	Análisis					
A.13 Seguridad de las comunicaciones	**Sección**		A.13.2 Intercambio de información			
	Control de la ISO 27001		13.2.1	13.2.2	13.2.3	13.2.4
			Políticas y procedimientos de intercambio de información	Acuerdos de intercambio de información	Mensajería electrónica	Acuerdos de confidencialidad o no revelación
	Aplicabilidad	**Si**				
		No	X	X	X	X
	Justificación		La entidad financiera ya cuenta con este apartado			

Tabla 53 Seguridad de las comunicaciones - intercambio de la información

Una vez analizado y justificado los controles de uno en uno en la institución financiera, se procede, a porcentual izar el cumplimiento de cada uno de los controles con el fin de tener una visualización sobre el cumplimiento de estos, y así se podrá realizar una propuesta de mejora para cada uno de los mencionados controles que actualmente se manejan.

3.1.2.18 Análisis de cumplimiento de controles

Esta valoración porcentual del cumplimiento de cada uno de los controles se realiza conjuntamente con el Ing. Ricardo Pilamunga desarrollador de software en el Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Indígena SAC.

Para esto se elaboró una gráfica con el cumplimiento para cada una de las áreas, las cuales detallan porcentualmente los resultados obtenidos, adicionalmente detallamos cada control, y a su vez como están establecidos en el momento de la investigación.

3.1.2.19 Políticas de seguridad de la información

A.5.1 Directrices de gestión de la seguridad de la información

- **A.5.1.1 Políticas para la seguridad de la información**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente carece de una documentación con políticas de seguridad de la información, aun así, se lleven varios de los diferentes procesos para tener a salvo la información, estos cumplen apenas algunas normativas básicas, pero esto, no garantiza una apropiada aseguración de la información.

Por esto es de suma importancia la implantación de políticas de seguridad de la información, están deben a su vez estar documentadas y socializadas con todas las áreas y personal de la institución financiera, y este deberá aplicar las debidas sanciones a quienes no las cumplan, este documento debería realizarse con la participación del Departamento de Tecnologías de la Información y la Gerencia de la institución financiera.

- **A.5.1.2 Revisión de las políticas para la seguridad de la información**

La entidad financiera al no contar con un documento con políticas de seguridad, como ya se lo menciono anteriormente, por ende no podemos obtener una revisión de políticas de seguridad dentro de la entidad financiera.

A continuación, ya definidas y documentadas cada una de las políticas de seguridad, juntamente el Departamento de Tecnologías de la Información y la gerencia se deben comprometer con la revisión periódica de las políticas de seguridad, para garantizar la efectividad y a su vez las examinaciones de cada una de las políticas de seguridad definidas se cumplan todas sin discusión alguna.

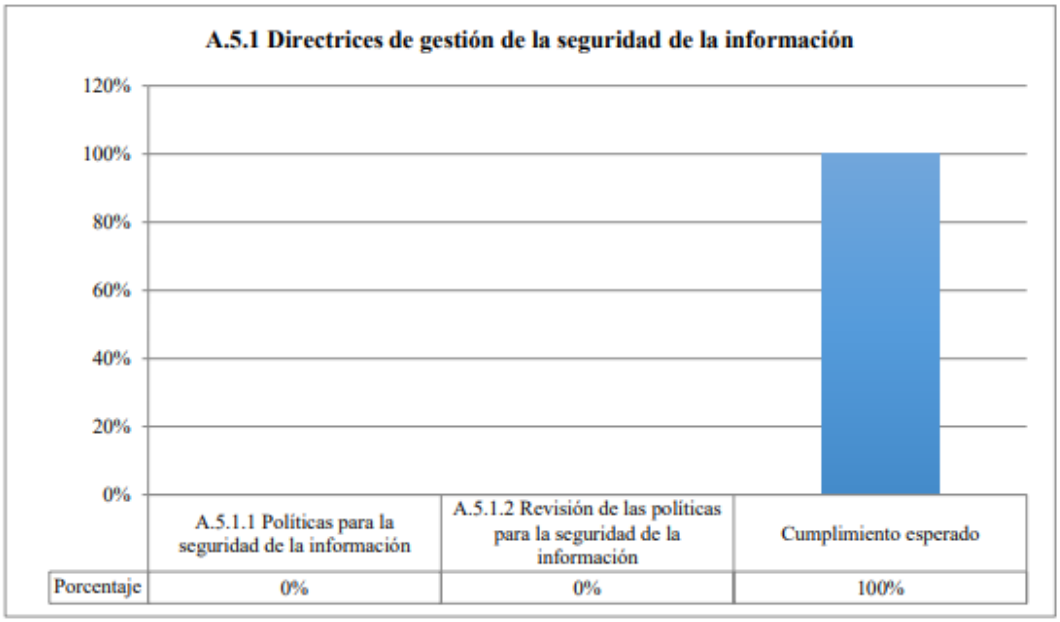


Grafico 17 Análisis porcentual - directrices de gestión de la seguridad de la información

A. 8 Gestión de activos

A.8.2 Clasificación de la información

- **A.8.2.1 Clasificación de la información**

El Departamento de Tecnologías de la Información, es el departamento que se encarga de la gestión y clasificación de los activos dentro de la entidad financiera, este departamento también es el encargado de etiquetar por su importancia la información de la entidad financiera, así mismo asigna un adecuado rol y usuario al personal.

- **A.8.2.2 Etiquetado de la información**

El Departamento de Tecnologías de la Información, es el que se encarga de un adecuado etiquetado para clasificar y gestionar los activos de la entidad financiera, este departamento también es el encargado de establecer una etiqueta de acuerdo a la clasificación que decidió adoptar la entidad financiera.

- **A.8.2.3 Manipulación de la información**

El Departamento de Tecnologías de la Información, es el que se encarga de los procesos de control, manejo y la manipulación de toda la información, esto de

acuerdo la clasificación que decidió adoptar la entidad financiera.

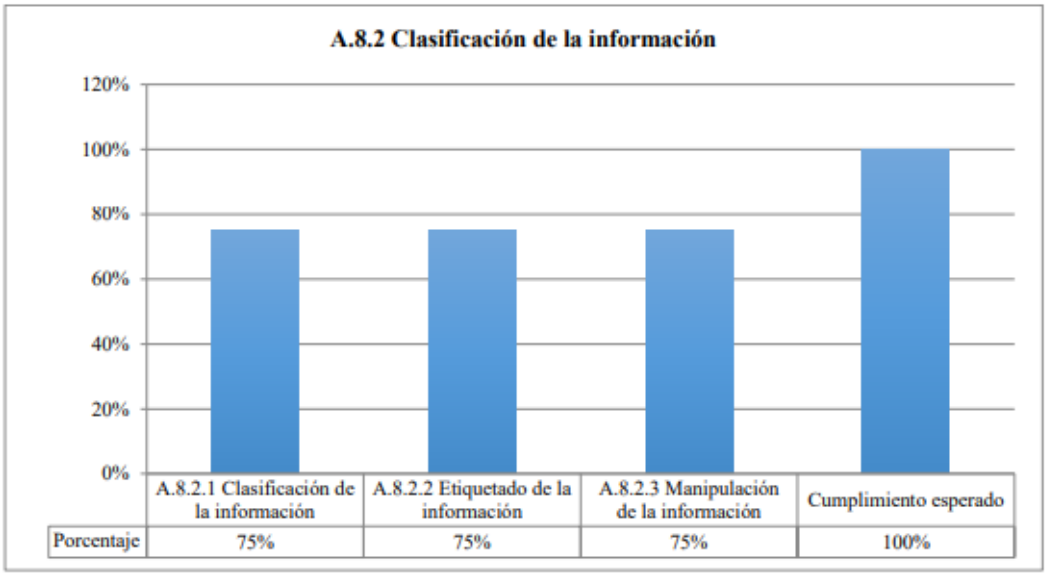


Grafico 18 Análisis porcentual - clasificación de la información

A.9 Control de Acceso

A.9.1 Requisitos de negocio para el control de acceso

- **A.9.1.1 Política de control de acceso**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta con la documentación que detalle políticas para un adecuado control en el acceso de la información, pero, sin embargo, cuenta con varios procesos para asegurar la información, al aplicarse ciertas normas básicas estas no aseguran un total control acceso de la información.

- **A.9.1.2 Acceso a las redes y a los servicios de red**

El Departamento de Tecnologías de la Información, es el que se encarga de proporcionar todos los accesos y que el servicio de la información esté disponible, previo a la autorización de acceso.

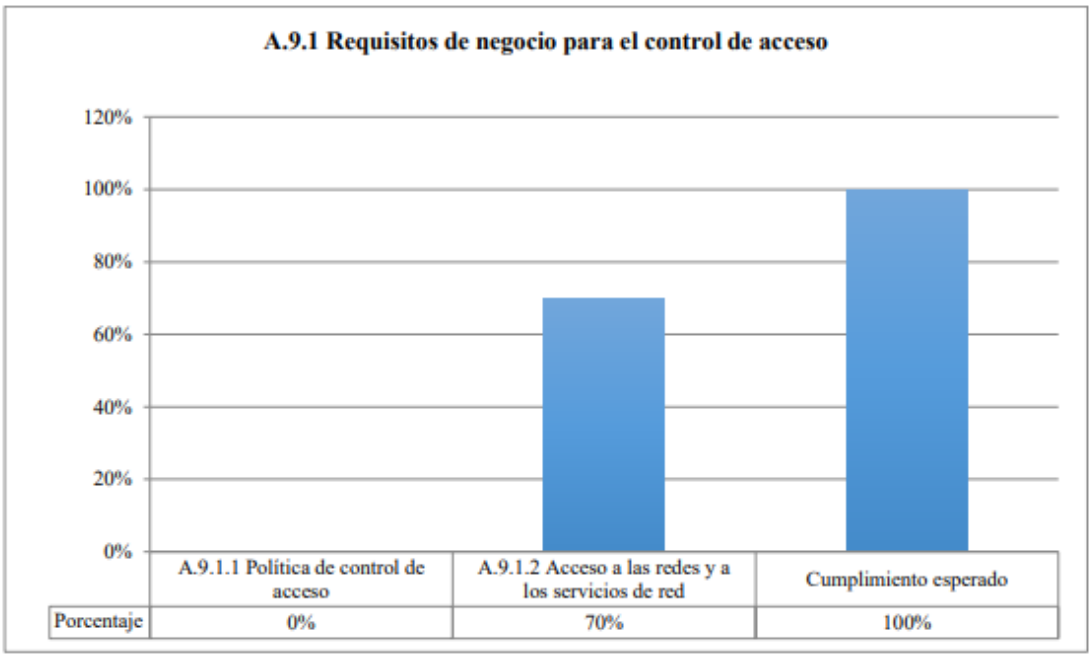


Grafico 19 Análisis porcentual - requisitos de negocio para el control de acceso

A 9.2 Gestión de acceso de usuario

- **A.9.2.1 Registro y baja de usuario**

El Departamento de Tecnologías de la Información, es el que se encarga de administrar todas las adjudicaciones de usuarios tanto para registrarlos como dar de baja los mismos, así genera los permisos a los que cada uno tiene acceso.

- **A.9.2.2 Provisión de acceso de usuario**

El Departamento de Tecnologías de la Información, es el que se encarga de administrar todos los procesos de retiro de accesos de información a cada uno de los usuarios, así se mantiene la seguridad a la información y aplicaciones de la entidad financiera.

- **A.9.2.3 Gestión de privilegios de acceso**

El Departamento de Tecnologías de la Información, es el que se encarga de restringir el control, también de asignar y otorgar privilegios para los usuarios hacia la información de la entidad financiera.

- **A.9.2.4 Gestión de la información secreta de autenticación de los usuarios**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta con una política para una correcta autentificación para la información secreta, esto quiere decir que se debería crear una política para los usuarios tanto como la creación, como la eliminación de los mismos, dando los accesos a los que estos tendrían.

- **A.9.2.5 Revisión de los derechos de acceso de usuario**

El Departamento de Tecnologías de la Información, es el que se encarga de revisar todos los derechos de los usuarios hacia la diferente información de la entidad financiera, esto lo hace periódicamente así cuida la seguridad de cada usuario.

- **A.9.2.6 Retirada o reasignación de los derechos de acceso**

El Departamento de Tecnologías de la Información, es el que se encarga de dar de baja a un usuario o a su vez la reasignación de derechos, dependiendo de cada caso, ya sea este por culminación del contrato laboral o cambio de rol del usuario.

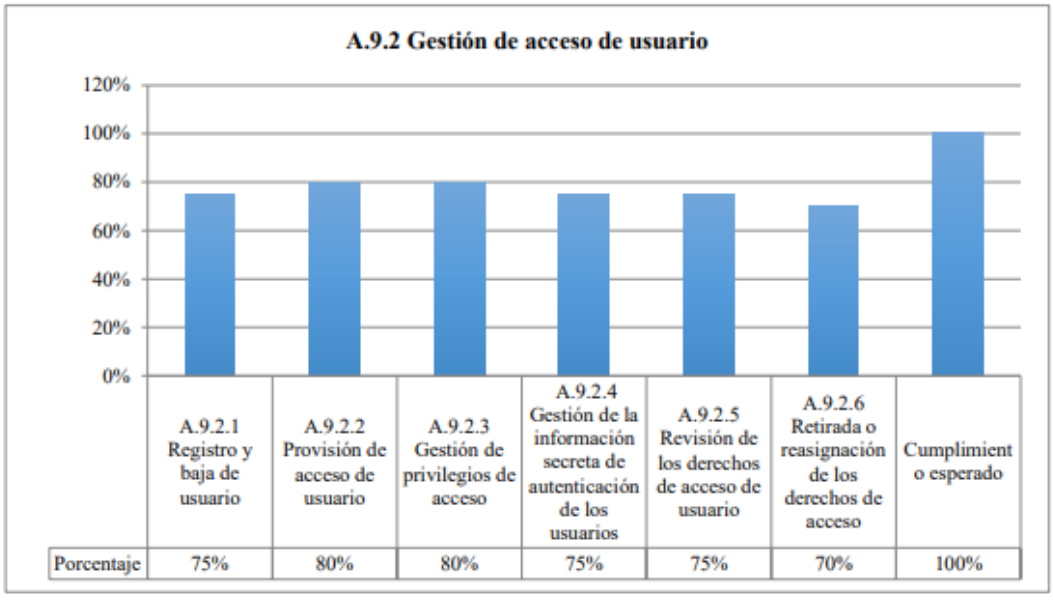


Grafico 20 Análisis porcentual - gestión de acceso de usuario

A.9.3 Responsabilidades del usuario

- **A.9.3.1 Uso de la información secreta de autenticación**

El Departamento de Tecnologías de la Información, maneja el proceso para el control de los usuarios, recomendando mejores prácticas para asegurar la información secreta de la entidad financiera.

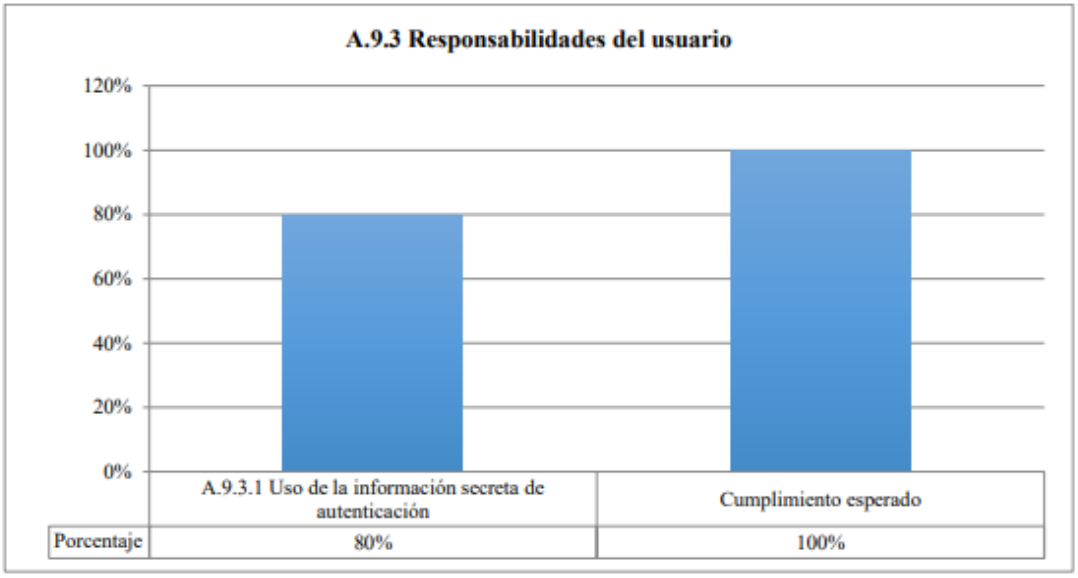


Grafico 21 Análisis porcentual - responsabilidades del usuario

A 9.4 Control de acceso a sistemas y aplicaciones

- **A.9.4.1 Restricción del acceso a la información**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta con un documento de políticas para restringir el acceso de información, pero llevan algunos procesos básicos para restringir la información, pero estas no garantizan la seguridad ni el control total de la información en la entidad financiera.

- **A.9.4.2 Procedimientos seguros de inicio de sesión**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta con un documento de procesos de inicio de sesión para el acceso a la información, pero llevan algunos procesos básicos para restringir la información en el inicio de sesión de la información, pero estas no garantizan la seguridad ni el control total en el inicio de sesión de la entidad financiera.

- **A.9.4.3 Sistema de gestión de contraseñas**

El Departamento de Tecnologías de la Información, tiene un proceso para generar o cambiar contraseñas, de los usuarios siempre manteniendo un nivel de contraseña que no sea fácil de descifrar, para evitar el hurto de las mismas.

- **A.9.4.4 Uso de utilidades con privilegios del sistema**

El Departamento de Tecnologías de la Información, tiene un proceso para que los usuarios obtengan la información que necesitan, esto se lo hace a base de roles para cada uno de ellos, así se evita que tengan acceso a información relevante para la entidad financiera.

- **A.9.4.5 Control de acceso al código fuente de los programas**

El Departamento de Tecnologías de la Información, tiene un proceso para la restricción de los códigos fuente que son desarrollados por la entidad financiera, cabe mencionar que el sistema principal es administrado por la entidad financiera pero desarrollada por una tercera empresa.

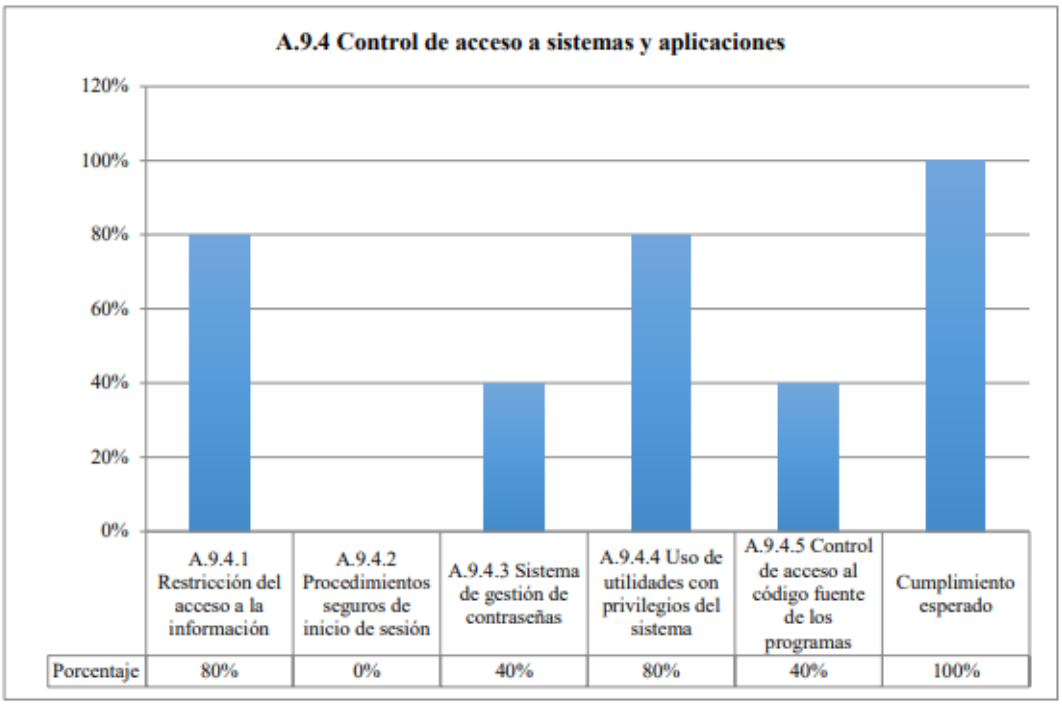


Grafico 22 Análisis porcentual - control de acceso a sistemas y aplicaciones

A.11 Seguridad física y del entorno

A.11.1 Áreas seguras

- **A.11.1.1 Perímetro de seguridad física**

La Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con una seguridad insuficiente para la infraestructura, por lo que esta no asegura que se proteja la información, se recomiendo que se implemente un nivel de seguridad óptimo para la seguridad de la información dentro de la entidad financiera. para precautelar el acceso a las áreas que contienen la información sensible de la empresa.

- **A.11.1.2 Controles físicos de entrada**

La Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con normas básicas en la infraestructura lo que no asegura la protección de la información, por lo tanto es importante implantar, una adecuada protección a cada uno de los equipos detallando la ubicación de cada uno de ellos para un mejor control y manejo.

- **A.11.1.3 Seguridad de oficinas, despachos y recursos**

La Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con una seguridad para el ingreso a las oficinas con su debido registro, pero esto no es una protección adecuada ya que al cuarto de servidores no existe una autenticación previa ya que cualquier persona podría ingresar, por lo tanto este no asegura un total aseguramiento de la información.

- **A.11.1.4 Protección contra las amenazas externas y ambientales**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente cuenta con un plan para las amenazas externas que pudieran suscitarse dentro de una entidad financiera, pero este no asegura la seguridad de la información, así mismo se debería ingeniar un plan sobre catástrofes ambientales para la protección y evacuación de la información dentro de la entidad financiera.

- **A.11.1.5 El trabajo en áreas seguras**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente tiene todos los procedimientos para que los empleados desempeñen su labor en un área segura para cada uno de los procesos que el empleado deba cumplir dentro de la entidad financiera.

- **A.11.1.6 Áreas de carga y descarga**

La Cooperativa de Ahorro y Crédito Indígena SAC, debido a su ubicación en el centro de la ciudad no cuenta con un área adecuada tanto para el ingreso como

despacho de los diferentes equipos que maneja la entidad financiera.

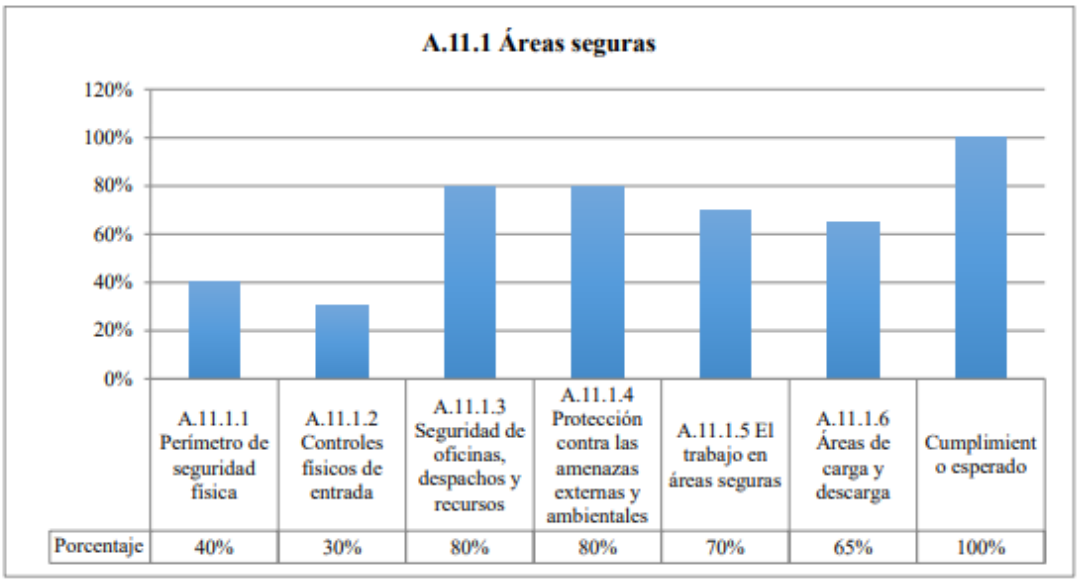


Grafico 23 Análisis porcentual - áreas seguras

A.11.2 Seguridad de los equipos

- **A.11.2.1 Emplazamiento y protección de equipos**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente lleva un registro para saber la ubicación de cada uno de los equipos dentro de la entidad financiera por lo que esto no garantiza una adecuada seguridad para los equipos.

- **A.11.2.2 Instalaciones de suministro**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta con una adecuada protección para algún fallo de energía que pudiera suscitarse, aunque tienen su propio generador, pero este no abastece en un 100% a toda la entidad financiera.

- **A.11.2.3 Seguridad del cableado**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente posee con todas las especificaciones para un buen cableado para las instalaciones eléctricas y telecomunicación, lo cual asegura que no se puedan tener problemas de intercepciones o interferencias dentro de la entidad financiera.

- **A.11.2.4 Mantenimiento de los equipos**

La Cooperativa de Ahorro y Crédito Indígena SAC, para un adecuado funcionamiento de los equipos informáticos que se encuentran dentro de la entidad financiera, realiza mantenimientos preventivos y correctivos periódicamente, este

proceso lo realiza el Departamento de Tecnologías de la Información, así se asegura que los equipos este disponibles y funcionando correctamente para cada uno de los usuarios.

- **A.11.2.5 Retirada de materiales propiedad de la empresa**

El Departamento de Tecnologías de la Información, maneja un procedimiento muy meticuloso en el caso de que alguna información que sea propiedad de la entidad financiera debiera ser retirada por cual motivo.

- **A.11.2.6 Seguridad de los equipos fuera de las instalaciones**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente cuenta con un registro cuando un equipo debiera ser sacado de las instalaciones de entidad financiera por cualquier motivo que este pudiera ser, lo cual asegura su integridad y un custodio para el equipo mientras este regrese a la entidad financiera, lo cual asegura un responsable y seguridad del equipo, si por algún caso ocurriera algún percance con el equipo el responsable deberá comunicarse inmediatamente para las decisiones que el caso lo requiera.

- **A.11.2.7 Reutilización o eliminación segura de equipos**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente cuenta con un procedimiento que respalda la información antes de cualquier reutilización o dada de baja de algún equipo informático, lo cual garantiza un correcto respaldo de la información.

- **A.11.2.8 Equipo de usuario desatendido**

La Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con el plan de mantenimiento de equipos lo cual ayuda a llevar un registro de los equipos que fueron atendidos, y evita que algún equipo pueda ser desentendido o falta de manteamiento, esto evita que el usuario tenga algún problema, y asegura el correcto funcionamiento de los equipos dentro de la entidad financiera.

- **A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta actualmente con algún proceso que indique al usuario de un adecuado uso de los recursos informáticos, para evitar la saturación de memoria o perdida de información por sobrecarga a los mismo, se debe realizar un proceso en el cual se capacite al usuario sobre un uso adecuado de los recursos de los equipos informáticos.

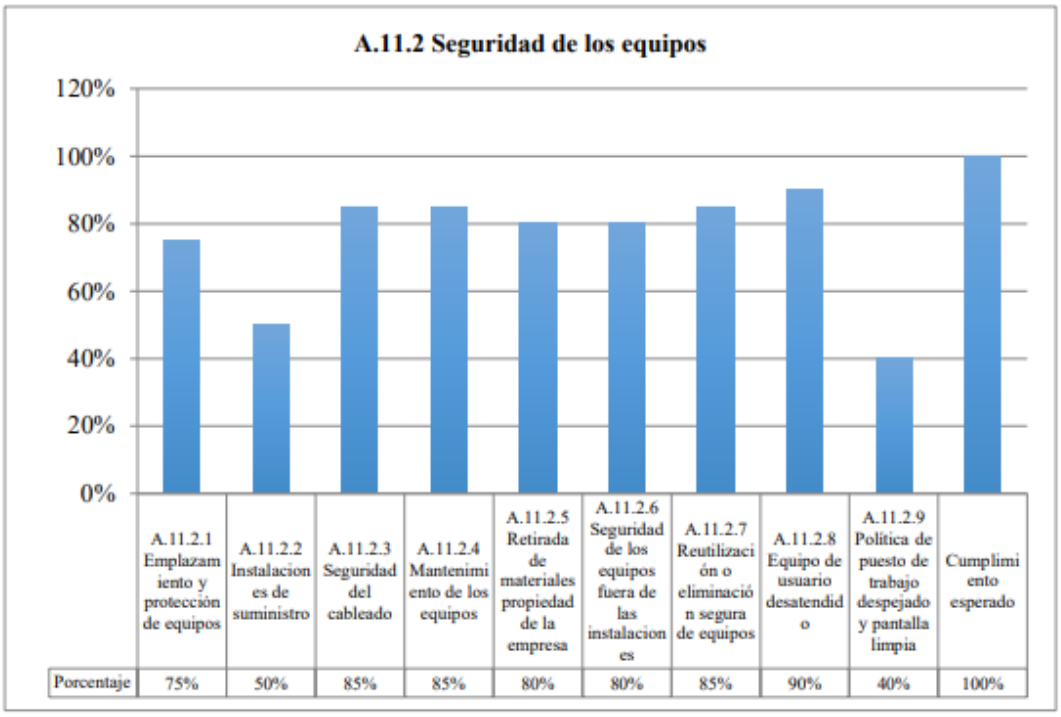


Grafico 24 Análisis porcentual - seguridad de los equipos

A.12 Seguridad de las operaciones

A.12.2 Protección contra el software malicioso (malware)

- **A.12.2.1 Controles contra el código malicioso**

El Departamento de Tecnologías de la Información, tiene un proceso para asegurar de una manera eficiente los equipos informáticos, para que este no se vea afectado por algún software malicioso y así el sistema no se vea afectado, tiene una protección en tiempo real además de los controles necesarios para la prevención, detección contra cualquier software malicioso dentro de la entidad financiera

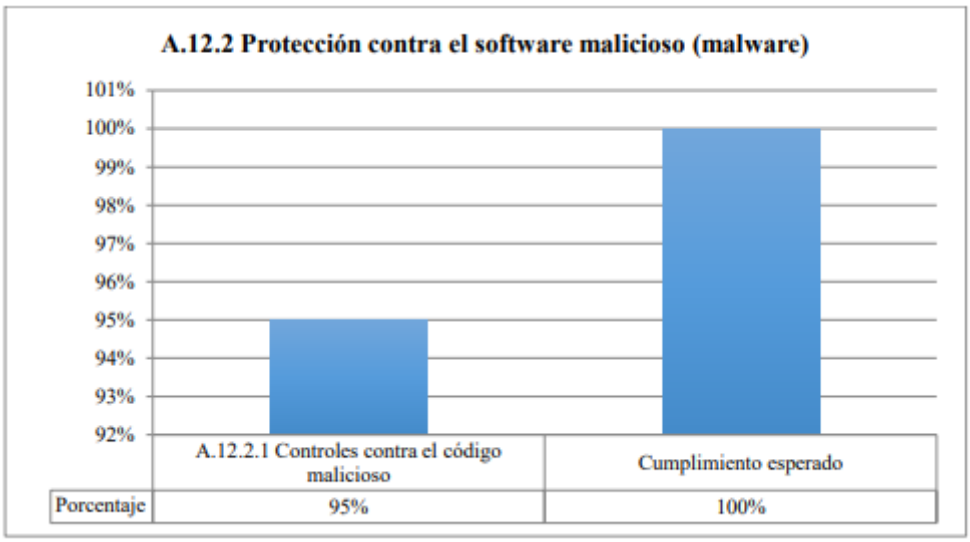
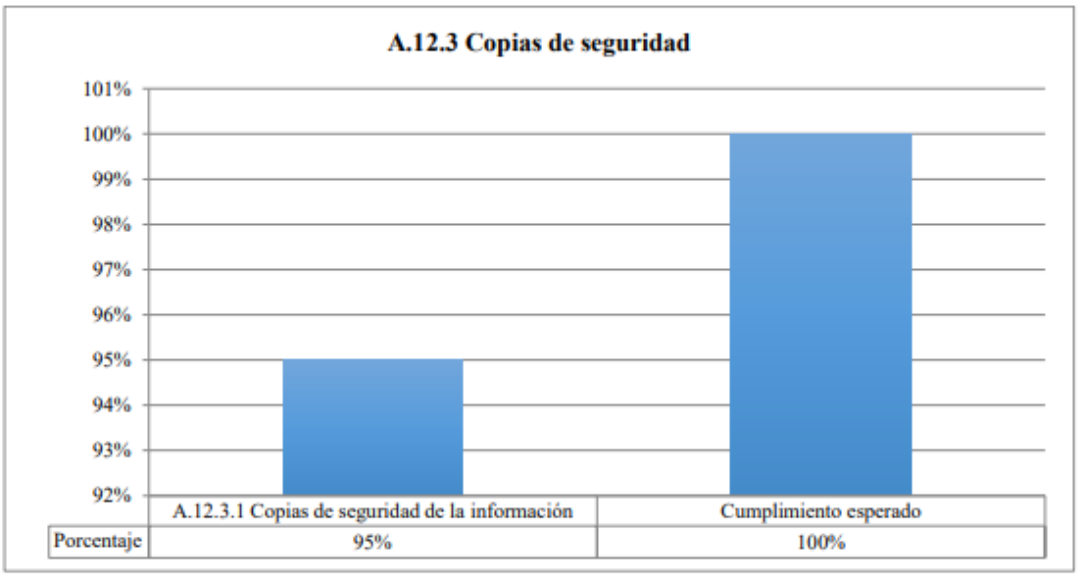


Grafico 25 Análisis porcentual - protección contra el software malicioso (malware)

A.12.3 Copias de seguridad

- **A.12.3.1 Copias de seguridad de la información**



.

Grafico 26 Análisis porcentual - copias de seguridad

A.12.6 Gestión de la vulnerabilidad técnica

- **A.12.6.1 Gestión de las vulnerabilidades técnicas**

El Departamento de Tecnologías de la Información, tiene un proceso para revisar la vulnerabilidad ya que al ser una entidad financiera debe cumplir con ciertos requisitos de seguridad para los clientes y usuarios, pero no existe un protocolo de revisión periódica por lo que se recomienda tener un proceso que ayude a detectar posibles vulnerabilidades cada cierto tiempo.

- **A.12.6.2 Restricción en la instalación de software**

El Departamento de Tecnologías de la Información, actualmente no cuenta con un proceso seguro para que los usuarios no puedan instalar algún software no permitido en la entidad financiera, aunque cuentan con ciertos parámetros básicos para evitar esto no es un control que asegure la seguridad de la información.

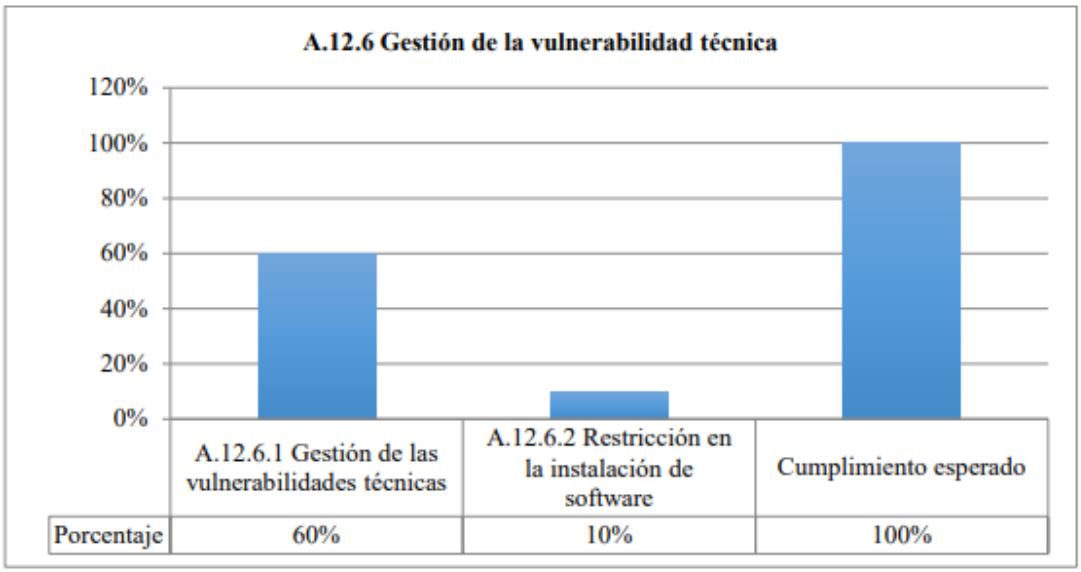


Grafico 27 Análisis porcentual - gestión de la vulnerabilidad técnica

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

- **A.13.1.1 Controles de red**

La Cooperativa de Ahorro y Crédito Indígena SAC, a través del Departamento de Tecnologías de la Información, es el encargado de controlar el flujo de la red dentro de la entidad financiera, por ende, tiene el control, pero esto no garantiza la seguridad de la información, ni el robo de ella por medio de la red o ataques a los equipos informáticos.

- **A.13.1.2 Seguridad de los servicios de red**

La Cooperativa de Ahorro y Crédito Indígena SAC, a través del Departamento de Tecnologías de la Información, es el que se encarga de administrar la red y que los servicios por medio de ellas estén totalmente funcionando, al ser una entidad financiera es de suma importancia que la red siempre este activa para evitar inconvenientes con clientes como con otras entidades

- **A.13.1.3 Segregación en redes**

La Cooperativa de Ahorro y Crédito Indígena SAC, al momento cuenta con sucursales en otras ciudades del país por lo que la red se encuentra segmentada, para que cada sucursal tenga su propia red, esto es importante y ayuda a mantener un control sobre cada una de ellas y mejorar la seguridad en los servidores, pero es importante tener un control con cada uno de los usuarios y sus roles para evitar complicaciones o robo de la información.

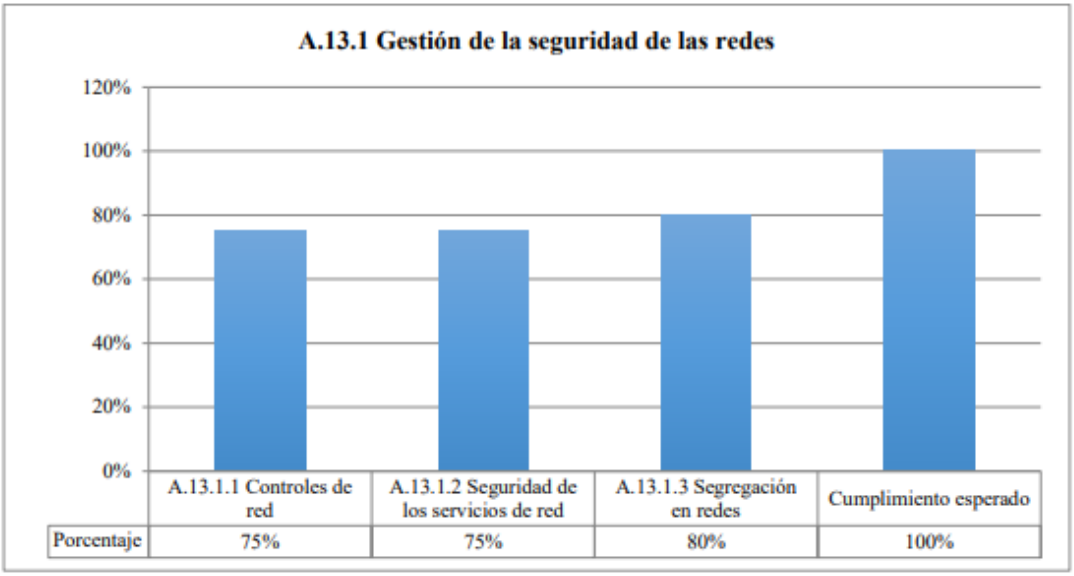


Grafico 28 Análisis porcentual - gestión de la seguridad de las redes

A.13.2 Intercambio de información

- **A.13.2.1 Políticas y procedimientos de intercambio de información**

La Cooperativa de Ahorro y Crédito Indígena SAC, no cuenta al momento con un documento con políticas que ayuda al proceso de cambio de información, es fundamental para la entidad financiera el tener un documento y este sea compartido con todo el personal para mayor seguridad del intercambio de información.

- **A.13.2.2 Acuerdos de intercambio de información**

La Cooperativa de Ahorro y Crédito Indígena SAC, a su vez cuenta con múltiples acuerdos para el cambio de información, con otras entidades financieras, las cuales deben estar estrictamente protegidas, sin embargo, no se intercambia información que pueda ser sensible para la entidad financiera, por lo que la información se trata en el servidor de la Cooperativa.

- **A.13.2.3 Mensajería electrónica**

La Cooperativa de Ahorro y Crédito Indígena SAC, cuenta con el servicio de mensajería propio con todos los estándares de seguridad para el mismo, pero se debe tomar en cuenta que al ser un servicio web este puede ser vulnerado y no es completamente seguro lo que puede ocasionar el robo de información para la entidad financiera.

- **A.13.2.4 Acuerdos de confidencialidad o no revelación**

La Cooperativa de Ahorro y Crédito Indígena SAC, actualmente no tiene una política de confidencial o de no revelación, tiene una especificación al momento del contrato con parámetros que no pueden ser divulgados, pero este no cuenta como revelación de información, por lo que es necesario un documento para la entidad financiera para evitar la salida de información.

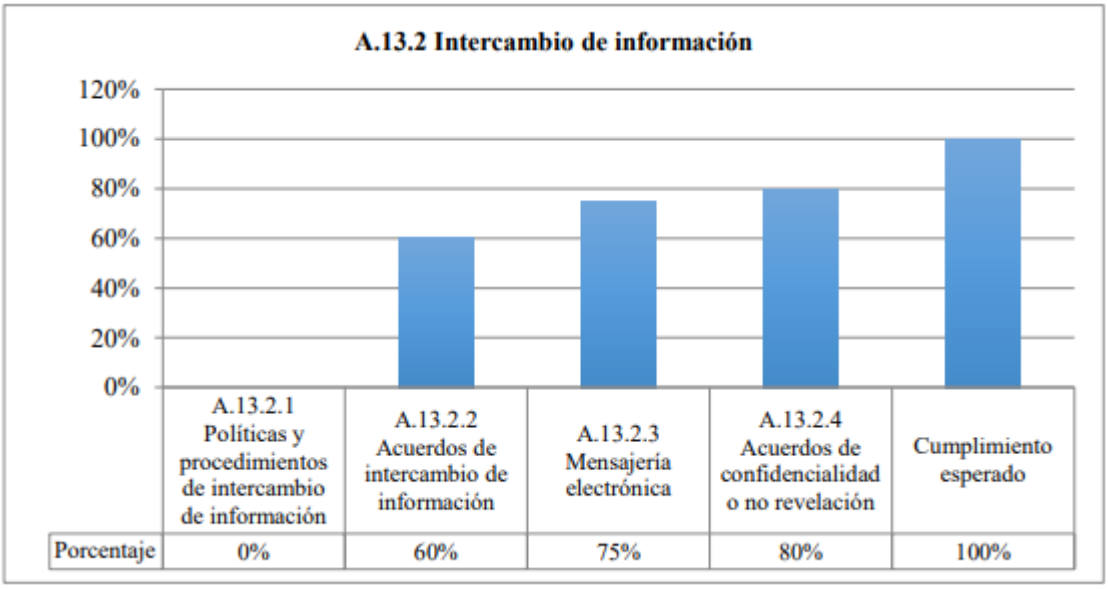


Grafico 29 Análisis porcentual - intercambio de información

3.1.2.20 Políticas y controles establecidos para la seguridad de la información para la Cooperativa de Ahorro y Crédito Indígena SAC

Habiendo acabado de analizar cada uno de los controles que son aplicables dentro de la norma ISO 27001, en cada escenario posible dentro de la Cooperativa de Ahorro y Crédito Indígena SAC, en los que se realizan cada una de las actividades diarias, se pudo llegar a determinar que existen probabilidades muy altas de que la entidad financiera sufra algún percance de seguridad de la información.
Por esta razón, se debe crear las políticas de seguridad para la información, las mismas que serán elaboradas de manera eficiente, con todos los requisitos que la institución financiera lo necesita, estas políticas serán la guía para una correcta gestión de la seguridad para la información.

Lo siguiente, será definir las políticas que satisfacen cada una de las necesidades que requiere la institución financiera, tanto física, organizacional y dentro de lo legal para un mejor y adecuado manejo en la seguridad para la información.

- **Seguridad Organizacional**

Para esto desarrollaremos un cuadro que será administrado por la institución financiera, estos además incluirán los activos, espacios físicos, y también las actividades complementarias. Este documento debe estar enfocado a salvaguardar la seguridad de la información de la Cooperativa de Ahorro y Crédito Indígena SAC

- **Seguridad Lógica**

Emplearemos las normativas que se aplican para gestionar los controles de acceso por parte de los usuarios, como empleados y clientes de la institución financiera, así mismo se aplicaran las normativas necesarias para un mejor control de vulnerabilidades por causa de algún software mal intencionado.

- **Seguridad Física**

Emplearemos las normativas que se aplican para gestionar los controles tanto en mantenimiento, como en soporte de cada uno de los equipos, adicionalmente se deberá precisar los límites para la seguridad de la entidad financiera.

- **Seguridad Legal**

Emplearemos las normativas que nos ayudaran a estructurar todas las políticas de seguridad, como las normas siempre respetando el reglamento de la entidad financiera, este con el fin de respetar y garantizar que se cumpla con el mismo, adicionalmente serán agregadas las penalidades que cada caso lo requiera a cada usuario que no cumpla con dichas políticos y normas, poniendo en riesgo la seguridad de la información de la Cooperativa de Ahorro y Crédito Indígena SAC.

A.5 Políticas de seguridad de la información

A.5.1 Directrices de gestión de la seguridad de la información

Objetivo:

“Proporcionar orientación y apoyo a la gestión de la seguridad de la información de la Cooperativa de Ahorro y Crédito Indígena SAC de acuerdo con los requisitos de la empresa, las leyes y normativa pertinentes”.

- Creación de un manual para las políticas de seguridad de la información, con el que el personal de la Cooperativa de Ahorro y Crédito Indígena SAC deberá ser capacitado para su debido conocimiento.

- El manual para las políticas de seguridad, deberá ser documentado por el departamento de TI de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Creación de un documento con las políticas para la seguridad de la información, este deberá ser revisado y aprobado por el consejo de la Cooperativa de Ahorro y Crédito Indígena SAC.

- El documento deberá ser revisado en un lapso de tiempo no muy amplio, para que este sea aprobado, modificado o desaprobado.

A.8 Gestión de activos

A.8.2 Clasificación de la información

Objetivo:

“Asegurar que la información de Cooperativa de Ahorro y Crédito Indígena SAC reciba un nivel adecuado de protección de acuerdo con su importancia para la organización”.

- Toda la información dentro de la entidad financiera deberá ser clasificada, de acuerdo a la importancia en los ámbitos de valor, como requisitos legales, y niveles críticos para una aprobación o modificación que no sea autorizada por parte del consejo de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Para el manejo de la información, se llevará una semaforización de acuerdo a los procesos que maneja la Cooperativa de Ahorro y Crédito Indígena SAC.

A.9 Control de Acceso

A.9.1 Requisitos de negocio para el control de acceso

Objetivo:

"Limitar el acceso a los recursos de tratamiento de la información y a la información de Cooperativa de Ahorro y Crédito Indígena SAC".

- Para esto se implementará el manual para la política con el control de acceso a la información en la entidad financiera, el personal deberá ser capacitado, además se deberá documentar las políticas por el departamento de TI de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Los usuarios dentro de la entidad financiera, tendrán habilitados los permisos en la red, únicamente para los procesos necesarios de cada uno dentro de sus labores diarios dentro de la Cooperativa de Ahorro y Crédito Indígena SAC.

A.9.2 Gestión de acceso de usuario

Objetivo:

"Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de Cooperativa de Ahorro y Crédito Indígena SAC".

- Se llevará un control para registrar el ingreso, como la retirada de usuarios que ingresen o abandonen la entidad financiera, esto con el fin de que solo usuarios habilitados o que permanezcan aun a la Cooperativa de Ahorro y Crédito Indígena SAC, puedan acceder a la información.

- Se creará un control en la asignación para registrar el ingreso, como la retirada de usuarios, para la gestión de cada uno de los permisos que cada usuario requiera.

- Se llevará un control para los derechos en el acceso, de cada uno de los empleados o como de terceros que necesiten información de la Cooperativa de Ahorro y Crédito Indígena SAC, por los diferentes motivos que pueden

suscitarse dentro de la entidad financiera.

A.9.3 Responsabilidades del usuario

Objetivo:

"Para que los usuarios se hagan responsables de salvaguardar la información de autenticación en Cooperativa de Ahorro y Crédito Indígena SAC".

- Se creará un control para dar seguimiento a cada uno de los usuarios dentro de la Cooperativa de Ahorro y Crédito Indígena SAC, para verificar que se haga un correcto uso a la información reservada de la entidad financiera.

A.9.4 Control de acceso a sistemas y aplicaciones

Objetivo:

"Prevenir el acceso no autorizado a los sistemas y aplicaciones de Cooperativa de Ahorro y Crédito Indígena SAC".

- Se creará un manual para un correcto y seguro inicio de sesión, en el Core Financiero, el personal deberá ser capacitado, y el manual deberá ser documentado por el Departamento de TI de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Se creará un proceso para asegurar el correcto uso de las contraseñas, para que cumplan con los requisitos de seguridad, esto ayudara a proteger la información de la Cooperativa de Ahorro y Crédito Indígena SAC.

A.11 Seguridad física y del entorno

Objetivo:

"Prevenir el acceso físico no autorizado, los daños e interferencias a la información de Cooperativa de Ahorro y Crédito Indígena SAC y a los recursos de tratamiento de la información".

A.11.1 Áreas seguras

- Para un mejor control en lo que es el acceso físico a los sitios donde se alojan los servidores, que son el mayor punto donde se guarda la información, se deberá implementar un control para personas que no estén autorizadas a ingresar al mismo.

- Para un mejor control, en lo que es el acceso de personas a las diferentes oficinas en la entidad financiera, se creara un sistema de ingreso, así mismo se trabajara en un manual para cualquier desastre natural que pudiera suscitarse y poner en riesgo a las personas como a los recursos físicos de la Cooperativa de Ahorro y Crédito Indígena SAC.

A.11.2 Seguridad de los equipos

Objetivo:

"Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de Cooperativa de Ahorro y Crédito Indígena SAC".

- Se creará políticas para el mantenimiento de los equipos físicos de la entidad financiera, con el fin de mejorar el rendimiento y alargar la vida útil de los mismos.

- Se creará un manual para el mantenimiento de los equipos informáticos, estos serán realizados por el departamento de TI, de manera trimestral, de tal manera se asegura que el equipo cumpla con su función, y ayudara a tener un mejor control y precautelar la información.

- El departamento de TI, tendrá que ser el encargado de asegurar que los equipos informáticos se mantengan seguros, en caso de que se produzca cualquier eventualidad imprevista, para esto será necesario que se cree un documento en el que se detallen como manejar cada una de ellas.

- Se creará un plan para mejorar continuamente, en lo que es el manejo de la información para llevar una mejor pantalla limpia, esto ayudara a salvaguardar la información crítica de la Cooperativa de Ahorro y Crédito Indígena SAC.

A.12 Seguridad de las operaciones

A.12.2 Protección contra el software malicioso (malware)

Objetivo:

"Asegurar que los recursos de tratamiento de información y la información de Cooperativa de Ahorro y Crédito Indígena SAC están protegidos contra malware".

- Actualmente la entidad financiera ya cuenta con un antivirus, pero este debería

también funcionar en los servidores que es el punto más crítico y en donde se almacena la mayor cantidad de información de la Cooperativa de Ahorro y Crédito Indígena SAC.

- Se creará una política para que los usuarios tenga acceso a través de la red únicamente habilitando el tráfico en la red, para cada uno de los servicios que cada uno de ellos requieran utilizar.
- El testeo de la red de una manera seguida está a cargo del Departamento de TI, estos ayudarán a encontrar problemas y deficiencias, que deberán ser controladas por el departamento.
- Los respaldos de la información, deberán ser óptimos con el fin de asegurar que no haya perdida de información, ni estas contenga algún daño que no pueda ser reparado.

A.12.6 Gestión de la vulnerabilidad técnica

Objetivo:

"Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de Cooperativa de Ahorro y Crédito Indígena SAC".

- Se creara un proceso que ayude a gestionar de mejor manera la instalación de software en los quipos de cada uno de los usuarios de acuerdo a sus necesidades para su desempeño en la entidad financiera.

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

Objetivo:

"Asegurar la protección de la información en las redes y los recursos de tratamiento de la información de Cooperativa de Ahorro y Crédito Indígena SAC".

- Se debe gestionar un mejor control para la seguridad de la información, estos se lograrán con un control periódico por parte del Departamento de TI, de la misma manera se debe capacitar a los usuarios de la entidad financiera.

- Se creará una manual con cada incidencia que pueda suscitarse en la entidad financiera, con el fin de tener una repuesta inmediata a cualquier problema que pueda suscitarse en la Cooperativa de Ahorro y Crédito Indígena SAC.

A.13.2 Intercambio de información

Objetivo:

"Mantener la seguridad de la información que se transfiere dentro de Cooperativa de Ahorro y Crédito Indígena SAC con cualquier entidad externa".

- Se debería implementar un manual con las restricciones necesarias en el caso de que se necesite enviar información confidencial para la entidad financiera y que esta sea utilizada solo por la tercera parte involucrada.
- Una política para la confidencialidad con terceras partes y los usuarios de la entidad financiera, será muy importante que sea creado para asegurar la información de la Cooperativa de Ahorro y Crédito Indígena SAC.

3.1.2.21 Cumplimiento

El Departamento de Tecnologías de la Información de la entidad financiera la Cooperativa de Ahorro y Crédito Indígena SAC, será la encargada de revisar cada uno de los controles, así como las mejoras planteadas anteriormente, con el fin de crear el documento, con las diferentes políticas y normas ya definidas por el consejo de la Cooperativa de Ahorro y Crédito Indígena SAC, para que estos cumplan con el reglamento interno de la entidad financiera, este documento deberá ser actualizado con frecuencia para cada uno de los sistemas que contengan información dentro la entidad financiera.

El Departamento de TI, para poder garantizar la seguridad de la información, tendrá que realizar los procesos de monitoreo constante en cada una de las áreas, asegurando el cumplimiento de cada uno de los controles y políticas para la mantener una adecuada seguridad de la información.

La Cooperativa de Ahorro y Crédito Indígena SAC, como el Departamento de TI, tienen la obligación de que las políticas y normas de seguridad, una vez sean creadas y aprobadas, sean cumplidas por cada uno de los usuarios dentro de la entidad financiera, esto ayudará a tener un mejor control tanto en el ámbito de la organización, como en la seguridad de la información, si alguna política o norma no fuera cumplida se deberá sancionar de acuerdo al reglamento de la entidad financiera.

3.1.2.22 Interpretación de Resultados

De esta manera, como resultado del análisis se encontró frente a los requerimientos de la norma ISO/IEC 27001, en la Cooperativa de Ahorro y Crédito Indígena SAC, podemos obtener los siguientes resultados que ayudaron a manejar y diseñar de una mejor manera el Sistema de Gestión de la Seguridad de la Información.

La entidad financiera analizada (La Cooperativa de Ahorro y Crédito Indígena SAC) obtuvo una calificación promedio de 2, lo que se interpreta que se encuentra en un nivel de madurez repetible, es decir, que se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no se han formalizado y por tanto sus procedimientos ejecutorios dependen de cada persona.

Es así que la entidad financiera La Cooperativa de Ahorro y Crédito Indígena SAC, al no disponer de un documento formal de políticas de seguridad de la información, no salvaguarda en su totalidad la información, exponiendo a factores de vulnerabilidad la misma.

CAPITULO IV

4.1 Conclusiones

- Se evidencia falencias en los procesos informáticos que se manejan dentro de la entidad financiera, lo que genera que los equipos informáticos estén expuestos a múltiples amenazas y/o vulnerabilidades, lo que hace que esto no asegure una seguridad confiable dentro de la misma.

- Los equipos informáticos que forman parte de los activos, como los servidores que fueron auditados, muestran falencias al salvaguardar la información de la Cooperativa de Ahorro y Crédito Indígena SAC, por lo que al aplicar las normas y los estándares de la norma ISO 27001, mejorara la protección de la misma.

- En este momento la Cooperativa de Ahorro y Crédito Indígena SAC, no posee políticas, que aseguren la información, que se maneja en la entidad financiera, los proceso con los que cuentan y son realizados no están basadas en una política que esta sea capaz de asegurar la disponibilidad y garantizar la confidencialidad de la información.

- Dentro de la entidad financiera y luego de los análisis necesarios, se diseñó un Sistema de Gestión de la Seguridad de la Información aplicando los estándares que se indica en la norma ISO 27001, cumpliendo así las necesidades dentro de la institución financiera, esto permitirá tener una mejor seguridad en cuanto a la disponibilidad y una seguridad de la información más confiable.

- La aplicación del Sistema de Gestión de la Seguridad de la información que fue diseñado, ayudará a un mejor control en el manejo de la seguridad de la información como de los activos este será exclusivamente del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito indígena SAC quien será el encargado de hacer cumplir cada una de las normas que indica la norma ISO 270001.

4.2 Recomendaciones

- Se debe manejar los procedimientos marcados en las políticas que se definieron, cumpliendo con cada una de las especificaciones, para así garantizar la seguridad de la información dentro de la entidad financiera.

- Es sumamente importante mejorar las normas de seguridad dentro de la entidad financiera, con el fin de asegurar la seguridad de la información.

- Es importante mantener a todo el equipo del Departamento de Tecnologías de la Información, capacitado para cualquier eventualidad que pudiera suscitarse, con el fin de asegurar que la información, se encuentre disponible cuando así se lo requiera.

- Reuniones periódicas con el fin de evaluar el sistema de gestión de la seguridad informática (SGSI), para cumplir con lo establecido en la misma, y mejorar lo que se requiera.

REFERENCIAS BIBLIOGRAFICAS

[1] Guía Comercial de Quito, “Seguridad Informática.” 2015. [en línea]. Disponible en: www.guiaccq.com/product/index/403/.

[2] Ernst & Young, “Seguridad de la información en un mundo sin fronteras.” 2011.[enlínea].Disponible en: www.ey.com/Publication/vwluassets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf/.

[3] Terán Valen Referencias Bibliográficas

[4] F. A. R. Echeverry, «Inicio y Evolución de la Seguridad Informática en el Mundo,» [En

[5] línea]. Available: http://polux.unipiloto.edu.co:8080/00001532.pdf. [Último acceso: 2019].

[6] M. d. T. y. d. l. S. d. l. Información, «Ministerio de Telecomunicaciones y de la Sociedad de la Información,» 2017. [En línea]. Available: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region- segun-indice-de-ciberseguridad/. [Último acceso: 2019].

[7] R. A. Guevara, «Sistema de Gestion de la Seguridad de la Información basado en la Norma ISO/IEC 27001 para el departamento de Tecnologias de la información y comunicación del Distrito 18D01 de Educación,» Noviembre 2017. [En línea]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339si.pdf.

[8] T. V. G. Aucapiña, «NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA,» 2012. [En línea]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf. [Último acceso: 2019].

[9] M. E. R. Quintero, «IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO,» 2016. [En línea]. Available: http://dspace.espoch.edu.ec/bitstream/123456789/5453/1/98T00101.pdf. [Último acceso: 2019].

[10] C. R. Criollo, «IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA INFORMACION, BAJO LA NORMA ISO/IEC 27001, EN UNA EMPRESA DE SERVICIOS,» Noviembre 2015. [En línea]. Available: http://bibdigital.epn.edu.ec/handle/15000/11957. [Último acceso: 2019].

[11] A. E. p. l. Calidad, «Seguridad de la Información,» 2019. [En línea]. Available: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion. [Último acceso: 2019].

[12] Firma-E, «Pilares de la Seguridad de la Información: Confidencialidad, integridad y disponibilidad,» Octubre 2014. [En línea]. Available: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-

[13] [9] C. E. F. Diaz, «ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE UN

[14] APLICATIVO DE GESTIÓN DOCUMENTAL LIDER EN EL MERCADO COLOMBIANO,»

[15] Junio 2017. [En línea]. Available: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y. [Último acceso: 2019].

[16] G. Q. Guerrero, «Normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de las empresas de desarrollo de software, basada en la Norma Internacional ISO 27001,» 2018. [En línea]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/27119/1/Tesis_%20t1355mbd.p

df. [Último acceso: 2019].

[17] A. y. f. e. s. d. gestión, «NORMAS ISO,» [En línea]. Available: https://www.normas- iso.com/. [Último acceso: 2019].

[18] C. ISO, «CERTIFICACIONES,» 2018. [En línea]. Available: https://www.certificadoiso9001.com/certificaciones/. [Último acceso: 2019].

[19] I. I. D. Advisors, «ISO 27000 y el conjunto de estándares de Seguridad de la Información,» [En línea]. Available: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html. [Último acceso: 2019].

[20] I. Tools, «ISO 27001,» Julio 2017. [En línea]. Available: https://www.pmg-ssi.com/2017/07/iso-27001-contexto-alcance-y-politica/. [Último acceso: 2019].

[21] zuela, K. M. (2018). Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador (Master's thesis, Universidad de las Fuerzas Armadas ESPE. Maestría en Gerencia de Sistemas.)

[22] Casadiegos santana, a. L., Quintero Jiménez, m. A. R. C. E. L. A., & toro rueda, m. I. L. E. I. D. Y. (2014). sistema de gestión de seguridad de la información (SGSI) para el área de contabilidad de la ese hospital local de rio de oro cesar (doctoral dissertation).

[23] Vallejo Cáceres, A. A. (2018). Propuesta de Sistema de Gestión de Seguridad de la Información para el centro de datos de la empresa Leterago del Ecuador SA (Bachelor's thesis, Quito).

[24] León León L. A. (2018) Planificación de un SGSI basado en la norma ISO 27001: 2013 en la empresa Mafelesa (Doctoral dissertation Universidad de Guayaquil, Facultad de Ingeniería Industrial, Carrera de Ingeniería en Teleinformática).

[25] Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información tecnológica, 26(2), 129-134.

[26] Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI-Revista Ibérica de Sistemas e Tecnologías de Información, (22), 73-88.

[27] Iso27001, (2017). International Organization for Standardization. Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[28] Delgado, M. F. (2017). Taller de Implementación de la norma ISO 27001. Recuperado de https://www.gobiernodigital.gob.pe/docs/ISO_27001_v011.pdf.

[29] Montaño, V. (2015). Sistema de Gestión de la Seguridad de la Información.

[30] Solarte, F., Enriquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.

[31] Escuela Europea, 2019. Cómo evaluar las consecuencias y la probabilidad en el análisis de riesgos ISO 27001. Recuperado de: https://www.escuelaeuropeaexcelencia.com/2019/03/como-evaluar-las-consecuencias-y-la-probabilidad-en-el-analisis-de-riesgos-iso-27001/