UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO.

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

ÁREA: Administrativas Informáticas

LÍNEA DE INVESTIGACIÓN: Administración de Recursos

AUTOR: Ramos Ruiz Kevin Paul

TUTOR: Ing. Franklin Mayorga, Mg.

Ambato - Ecuador

Abril – 2021

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: "AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO", desarrollado bajo la modalidad Proyecto de Investigación por el señor Kevin Paul Ramos Ruiz, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, 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, abril 2021.

Firmado electrónicamente por:
FRANKLIN OSWALDO
MAYORGA MAYORGA

Ing. Franklin Mayorga, Mg
TUTOR

AUTORÍA DEL TRABAJO

El presente proyecto de investigación titulado: "AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO."

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, abril 2021

Kevin Paul Ramos Ruiz

CC:2100628037

AUTOR

DERECHOS DE AUTOR

Autorizo la Universidad técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta 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 parcial dentro de las regulaciones de la institución.

Ambato, abril 2021

Kevin Paul Ramos Ruiz

CC: 2100628037

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Kevin Paul Ramos Ruiz, 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 "AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO", 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, abril 2021.

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

DEDICATORIA

Primeramente, a Dios por darme los conocimientos y la fuerza para alcanzar mis metas.

A mi padre Juan a pesar de las dificultades, nunca me dejo solo para seguir adelante.

A mi madre Elsa por su sacrificio y esfuerzo, por siempre velar por mi educación y mi bienestar a lo largo de mi vida, por ser una persona incondicional y excepcional.

A mi tío Saulo y tía Lola que me dieron un techo para vivir durante toda esta etapa.

A mis hermanos, mis tíos y mis primos por enseñarme que con dedicación todo se puede cumplir. A mis amigos por ofrecerme un apoyo incondicional a lolargo en este periodo educativo.

Ramos Ruiz Kevin Paul

AGRADECIMIENTO

Primeramente agradezco a Dios por darme salud y vida, ya que en estos momentos difíciles de pandemia en que estamos atravesando fue un poco complicado movilizarme para hacer el proyecto de investigación, ya que sin él no podría ser un gran profesional.

A la Universidad Técnica de Ambato especialmente a la Facultad de Ingeniería en Sistemas Electrónica e Industrial por tener excelentes docentes que me permitieron llegar hacer un gran profesional.

A mi tutor Ing. Franklin Mayorga por ser una gran persona y un excelente docente que me compartió sus conocimientos y por regalar un poco de su tiempo para realizar este proyecto de investigación.

Al Ing. Oscar Curichumbi, al gerente de la cooperativa de Ahorro y Crédito Prodvisión el Sr. Jorge Masaquiza y a todos los equipos de trabajo que conforma la cooperativa por brindarme su apoyo en hacer este trabajo de investigación.

Ramos Ruiz Kevin Paul

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El actual trabajo de investigación se efectuó con el propósito de elaborar una Auditoría Informática en la cooperativa de Ahorro y Crédito Prodvisión, entidad no se ha desarrollado dicha auditoría en años anteriores, para analizar las posibles deficiencias y orientar al personal responsable del área informática, sobre los efectos logrados para que obtengan las normas preventivas y disciplinarias previniendo inseguridades de la información.

La inexperiencia institucional que consta con relación a los riesgos para el manejo de la información tomaría resultados desfavorables si no se evita previamente la importancia de las transacciones que se administra externa e internamente en la cooperativa.

Se utilizó la metodología Octave lo cual me permitió organizar prácticas importantes en la cooperativa, con este efecto se logró determinar las vulnerabilidades de cada uno de los departamentos y activos críticos, generando normas de protección y recomendaciones para evitar la inseguridad de la información.

Una de las soluciones que se ha logrado obtener en este Proyecto de Investigación es disponer un estudio de cómo se encuentra la cooperativa hoy en día, y los problemas que se están teniendo para así corregir su trabajo tanto profesional, intelectual y propia; dicha entidad tiene la finalidad de contribuir al crecimiento y desarrollo de las personas.

Palabras clave: Seguridad informática, normas de protección, vulnerabilidades, Octave

ABSTRACT

The current research work was carried out with the purpose of preparing a Computer Audit in the Cooperativa de Ahorro y Crédito Prodvisión, an entity that has not carried out such an audit in previous years, to analyze possible deficiencies and guide the personnel responsible for the computer area, on the effects achieved so that they obtain the preventive and disciplinary norms preventing information insecurities.

The institutional inexperience that appears in relation to the risks for the management of the information would take unfavorable results if the importance of the transactions that is managed externally and internally in the cooperative is not previously avoided.

The Octave methodology was used which allowed me to organize important practices in the cooperative, with this effect it was possible to determine the vulnerabilities of each of the departmentsand critical assets, generating protection standards and recommendations to avoid the effects of the dangers found.

One of the solutions that has been obtained in this Research Project is to have a study of how the cooperative is today, and the problems that they are having in order to correct their professional, intellectual and own work; This entity has the purpose of contributing to the growth and development of people.

Keywords: Computer security, protection standards, vulnerabilities, Octave

INTRODUCCIÓN

La Seguridad Informática es utilizada por la mayoría de las cooperativas, bancos e instituciones financieras ya que es una herramienta muy esencial para proteger la información, es por eso, que cada vez se tiene mayor conocimiento y acuerdo de la importancia de la Seguridad de la Información de datos.

De tal forma que la finalidad principal es determinar inspecciones para protección de la información, recursos, privacidad de los datos y examinarlos diariamente con la finalidad de demostrar su grado de aptitud. Este desarrollo se efectúa mediante de una auditoria de seguridad informática conseguirán organizar las mejores medidas y tomar decisiones adecuadas para dar respuesta a las dificultades que existen.

En consecuencia, proporcionar apropiadamente la protección de los datos no solo permite a la entidad desempeñar a sus cargos y normas, sino que también cause seguridad en sus usuarios, socios y en sus inversionistas, al asegurarles que disponen con instalaciones especializadas y las normas de seguridad adecuadas para cuidar los datos y elaborar adecuadamente las diferentes acciones, financieras, productivas y operacionales de la entidad.

Este proyecto de investigación se distribuye en cuatro capítulos para tener una mejor comprensión: la descripción del proyecto lo cual se solucionará los objetivos propuestos, la metodología adecuada donde se muestra una rápida descripción de los distintas materiales utilizadas, el análisis de riesgos asociados de los datos en la entidad, la evaluación de la realización de la Auditoría y las normas de seguridad de la información, y por último se mostrará a qué conclusiones se ha logrado con el informe elaborado, como asimismo se da unas recomendaciones a la entidad según los resultados conseguidos de la investigación.

CAPITULO I.- MARCO TEÓRICO

1.1 Tema de investigación

AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO.

1.2 Antecedentes Investigativos

Se encontró en la tesis presentado por la Ing. Rosa Alexandra Gálvez Morocho de una Auditoría Informática realizado la Cooperativa De Ahorro y Crédito "Fernando Daquilema" según las observaciones encontradas de dicho proyecto por lo cual se elabora un inventario que se puede tener investigación sobre los equipos, datos importantes que se tiene en cada matriz de una cooperativa tomando muy en cuenta que cada equipo que se consigue es una inversión para la cooperativa, para proteger informaciones muy valiosas y definir en el departamento de sistemas los tipos de riesgos de TI, y así tener una mayor seguridad en los usuarios ya que cada información segura basándose en la ley general de Instituciones del Sistema Financiero porque cumple con los productos y servicios establecidos por la ley, siendo esta investigación de gran ayuda para la creación del sistema de inventarioque en la actualidad se está elaborando en el departamento de sistemas [1].

Se buscó información en la tesis de la Universidad Católica de Colombia del Ing. Daniel Arturo Alejo Blanco y de la Ing. Erika Alejandra García Hernández, por lo cual se informa que a través del detalle de una guía de auditoría permite perfeccionar el método de revisión central en formas financieras y en determinado en áreas afines con la manifestación de informes financieros conducidos de métodos tecnológicos, lacual alcanza todo el argumento de intervención central como progreso para las sistematizaciones de las distribuciones y para cuestión de estudio de las formas financieras, los distantes sujetan lineamientos exactos para valorar el cambio presente

de métodos claves en las distribuciones, afirmando que estos alcancen todo un argumento impuesto para la valoración por parte de la auditoria, prevalece los implicados como corporaciones, individuos o representaciones que valoran la seguridad de las intervenciones admitiendo corregir faltas o desviaciones en métodos característicos en lo que se describe a transacciones de tipo financiero. Como conclusión al ejecutar una valoración de riesgos del área Financiera y del área de Tecnología de un Banco se consigue alcanzar la causa de la comisión de riesgos el cual se alcanza: igualar, analizar, evaluar y conocer los riesgos como fragmento esencial de la auditoria, por consiguiente se consigue establecer el nivel de riesgos efectiva en las áreas de los departamentos a través de la creación de una matriz de inseguridades que sujeta razonamientos de dureza del riesgo y servicios ponderados de resultado y posibilidad que estuvieron designados a criterio de los autores, admitiendo registrar los riesgos más críticos para dar paso a la ejecución de controles determinados a cada acción coherente a los elementos de estudio [2].

En el proyecto de investigación de la universidad de Colombia de la Ing. Marrugo Hernández Claudia Patricia y el Ing. Salgado Tovar Fernando Andrés se establece que la auditoría informática está orientada directamente a los distintos sistemas de información con las que cuenta la entidad bancaria y todos los cambios que puedan ser actualizados, desarrollados o modificados en sus aplicaciones. Lo cual se concluye que es fundamental contar con una enseñanza más organizada que apoyen el desarrollo de auditoría, con el resultado de manifestar un mayor alcance y detalle de cada capítulo a evaluar, además que permitirá hacer un seguimiento más absoluto que contribuya eficiente a la toma de decisiones [3]

Una información del proyecto de investigación de la Ing. Amarilis Carolina Loor Párraga y de la Ing. Verónica Alexandra Espinoza Castillo se establecen en la metodología empleada se acomoda al progreso de la auditoría, y contribuyó a través de cada una de sus etapas, a las movimientos e instrucciones a alcanzar, con el propósito de lograr el objetivo planteado, el artículo y análisis del entorno existente, admitió conocer las insuficiencias efectivas para los diferentes áreas de la carrera, en la que se reconoce ideas manejables, habilidades y técnicas a desempeñar, la presencia de un procedimiento de seguridad para una correcta estimación y revisión de los recursos de TI. Trae como resultados que estos apliquen en situaciones poco

positivos y confidenciales, el estudio de técnicas de auditoría, se refleja de gran utilidad, admitiendo lograr información acerca de los ordenamientos, que se desenvuelven en la carrera, logrando así, representar en representación detallada los hallazgos encontrados durante el cumplimiento de la misma [4].

1.2.1 Contextualización del problema

A nivel mundial, en el campo empresarial, se ha alcanzado a manifestar un gran interés en los diferentes técnicas o métodos para alcanzar a tener un buen control, así como también un excelente manejo de la información adquirida en las distintas instituciones.

La tecnología logra un gran desarrollo, pero muy pocas de las empresas desarrollan medidas de seguridad para proteger la información, por lo cual es importante que se desarrolle medidas de seguridad para así poder evitar algún tipo de fraude o perdida de datos [5]

La mayoría de las veces, la información se almacena en diversos medios físicos y electrónicos, lo cual es motivo de preocupación y trata de mejorar la protección de la información, ya que uno de los mayores problemas en la unidad de información y estadísticas de las empresas que el acceso no autorizado a la información se vuelve más fácil. Debido a la cantidad de métodos nuevos y existentes para obtener información, ha hecho más difícil proteger la información y sus métodos de transmisión si estas comunicaciones son verbales, archivos, documentos, bases de datos, etc [5].

Un hecho que afectó a la empresa Pescanova en el que el informe de auditoría informática concluyo en julio de 2013 las cuentas de la compañía habían sido alteradas durante años para ocultar las pérdidas que sufría. El presidente de honor de la Asociación Española de Auditores, no se podía imaginar lo que estaba ocurriendo en esa empresa sobre todo porque casos como este suelen ocurrir en empresas de menores dimensiones". Por esa razón califica el suceso de "hito raro" y asegura queel 97% de las empresas funcionan correctamente, pero suelen conocerse los casos de las que funcionan mal [6].

En el Ecuador descuidan realizar evaluaciones acerca de su progreso y funcionamiento, sin olvidar que en el área empresarial hoy en día existe gran competencia en cuanto a la calidad de servicio o en lo que afecta al buen funcionamiento interno o externo de la empresa. En la actualidad las cooperativas en la provincia de Tungurahua corren altos riesgos en el tema relacionado a la administración de la información por lo que no se debe olvidar que su manejo está basado en la tecnología que mejora rápidamente y que requiere tomar precaución para evitar pérdidas para las cooperativas. [7]

Los peligros con las tecnologías de información y comunicaciones afectan también a la gestión y administración de las redes, ya que es uno de los medios por los cuales se puede causar serios daños a la información almacenada, compartir archivos redundantes, acceso de los usuarios a información de manera intencionada y no intencionada.

Otro riesgo asociado es el manejo inadecuado de claves de acceso conjuntamente con la asignación de roles de manera incorrecta, esto se convierte en una entrada para diversos ataques.

Algunas personas tratan de dañar el beneficio de empresas, es decir roban información, dinero, en fin, un número peligros que puedan perjudicar a una cooperativa de ahorro y crédito o bancos, por lo que cada gerente tiene el compromiso de proteger la información de sus socios, clientes, manteniendo la confidencialidad, la autenticidad y la integridad de la misma.

Según las investigaciones que se han realizado una de las causas que influyen para que existan altos riesgos en el manejo de la información, es la insuficiente capacitación del personal en las diferentes áreas, por lo que genera información incompleta e inexacta; como también se debe tomar en cuenta que esta información debe estar actualizada de una manera completa, segura y confiable. “La cooperativa debe pensar que al poseer una insuficiente aplicación de la presencia de Normas de

Seguridad Informática puede haber un colapso irremediable, por ejemplo la cooperativa Prodvisión tiene sus sucursales en diferentes provincias del país.

Ya que en raros momentos la red se colapsa, o si el servidor es adecuado para proteger informaciones personales de sus socios y clientes, por lo que el gerente debetener en cuenta, si algún socio, cliente, se ha perjudicado en sus cuentas bancarias, puesto que estas Normas de Seguridad Informática logran alcanzar a ser muy útiles, ventajosos, y rentables para la misma, ya que son el medio de comunicación en elcual se establecen las reglas, normas, controles y procedimientos que normalicen la forma en que la cooperativa prevenga, proteja y maneje los altos riesgos en el manejo de la seguridad de la información.“.[8]

“En una cooperativa o banco uno de los sucesos que permanentemente está atravesando por un mal de manejo de información personales, cuentas bancarias, por lo que hay una insatisfacción de los usuarios, socios, clientes y esto no beneficia en nada a la cooperativa. Considerar, que el manejo de la información es un aspecto de gran jerarquía en todas las organizaciones, cooperativas, bancos e instituciones para mejorar la calidad de servicio que se les facilita a los usuarios o clientes.”.[9]

1.2.2 Fundamentación Teórica

1.2.2.1 Auditoría

Es la revisión independiente de algunos o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones [10].

1.2.2.2 Tipos de auditoría

Los tipos de Auditoría se basan según: La clasificación que se propone está integrada por:

Auditoría por lugar, Área, Especialización, Ambiental, y Especializadas en Sistemas Computacionales.

Como se muestra en la tabla 1. Tipos de Auditoría.

Tabla 1. Tipos de Auditoría [11]

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistema de aplicación, recursos informáticos, planes de contingencia, etc	Operatividad eficientey según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad.
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas.

Es necesario recalcar como análisis de este cuadro que Auditoría de Sistemas no es lo mismo que Auditoría Financiera.

1.2.2.3 Auditoría informática

Es una herramienta muy importante para que nuestro sistema siempre esté en marcha de forma correcta, ayuda a las empresas a verificar la capacidad del sistema que está determinado. Debido a este análisis observaremos si trabaja de manera delicada, manejando los elementos correctos, consideraremos si se ha surgido alguna dificultad en su interior o los obstáculos alcanzados para tener presentes [12].

La auditoría informática es una modalidad que corresponde a la apreciación en fondo de los procesos informáticos y tecnológicos de una organización u empresa [13].

1.2.2.4 Características de la auditoría informática

Los expertos auditores no simplemente deben tener formación para la elaboración de servicios de auditoría, sino que asimismo serie determinada coherente con un argumento especializado o informático. Una delicada auditoría debe servir para manifestar un aspecto inseparable en base al ajuste al medio analógico y especializado de una sociedad [14].

1.2.2.5 Beneficios de la Auditoría Informática

De hecho, el objetivo final que se espera en las empresas con la implementación de una Auditoría Informática se puede circunscribir a dos aspectos concretos como son:

a) Beneficios Tangibles

Con el establecimiento de los sistemas en la empresa se pretende lograr mejorar por parte de quienes utilizan dichos sistemas para dar una mayor emisión de facturas en la empresa, más y mejores registros contables por jornada, mayor emisión de cheques de nómina en menor tiempo, mejor captura y proceso de impuestos vía sistema, entre otros.

b) Beneficios Intangibles

Los beneficios que se espera obtener de los sistemas de cómputo son algunos intangibles, ya que sus resultados no pueden ser contados ni se ven en forma física ni palpable, por ejemplo el teletrabajo que los empleados realizan actividades desde casa" [15]

1.2.2.6 Propósitos de la auditoría informática

El propósito fundamental de la Auditoría Informática es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la institución [16].

1.2.2.7 Metodología para el desarrollo o realización de la Auditoría Informática

Existen varias metodologías de Auditorias Informáticas y que reconocen de lo que se procure examinar o analizar, pero como esquema consideraremos las cuatro etapas primordiales de un proceso de investigación:

a) Estudio preliminar

Incluye delimitar el equipo de trabajo, el método de auditoria, verificar inspecciones al componente informático para saber referencias de esta, realizar un cuestionario para la elaboración de una investigación para valorar previamente la inspección interna, cuidado del procedimiento de movimientos, manuales de manejo, ordenanzas, reglamentos, entrevistas con los primordiales empleados del Departamento de Informática.

b) Revisión y evaluación de controles y seguridades

Radica en la revisión de los flujogramas, elaboración de pruebas de desempeño de las seguridades, estudio de aplicaciones de los espacios críticos, investigación de conocimientos históricos (backups), exploración de documentación y registros, entre diferentes actividades.

c) Examen detallado de áreas críticas

Con las etapas anteriores el auditor establece los espacios críticos que precisará específicamente el equipo de trabajo formará los impulsos, objetivos, importancia y recursos que utilizará, delimitará la sistemática de compromiso, la estabilidad de la auditoría mostrará el método de trabajo y examinará detalladamente cada inconveniente enfrentado con todo lo principalmente detallado.

d) Comunicación de resultados

Se realizará el informe a ser revisado con la directiva de la empresa hasta obtener al informe decisivo, el cual se mostrará esquemáticamente en representación principal, cuadros o composición simple y directa que recalque las dificultades encontradas, los efectos y los resultados de la Auditoria [17].

El manejo de la información es el desarrollo de un plan de acción que conduzca desde la decisión de manejo activo de la información hasta el uso final de los datos manejados. Esto debería ser un punto de partida obvio, pero, con demasiada frecuencia, los que administran la información pasan por alto este elemento clave.

Los planes pueden variar desde muy simples a complejos, formales o informales, pero sin excepción, estos deben incluir siempre una clara definición de los objetivos que deben lograrse a través del manejo de la información [18].

En la actualidad existen diferentes tipos de metodologías de auditoria informática, entre otras:

- R.O.A. (RISK ORIENTED APPROACH)
- MAGERIT
- OCTAVE

1.2.2.8 Metodología MAGERIT

Es una metodología enfocada al análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España cuyo propósito es minimizar los riesgos de implantación y uso de Tecnologías de la Información, principalmente dirigida a las instituciones públicas. Complementa su accionar mediante la aplicación del software PILAR.

a) Objetivos de Magerit

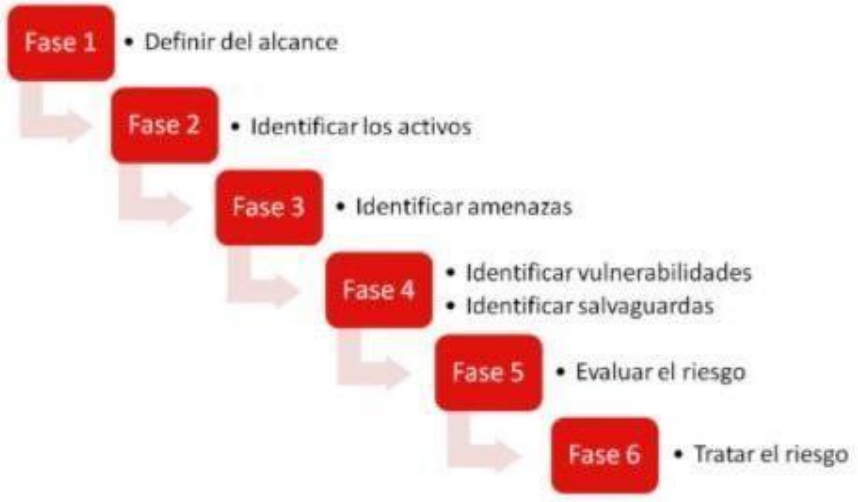
Magerit cumple con los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medias oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación, o acreditación, según corresponda en cada caso.

b) Fases de la metodología Magerit

- Definir del alcance.
- Identificar los activos.
- Identificar amenazas.
- Identificar vulnerabilidades y salvaguardas.
- Evaluar el riesgo
- Tratar el riesgo [19]

Figura 1. Fases de la metodología Magerit [19]



1.2.2.9 Metodología OCTAVE (METODOLOGÍA DE EVALUACIÓN DE RIESGOS DESARROLLADA POR EL SEI (SOFTWARE ENGINEERING INSTITUTE) DE LA CORNEGIE MELLON UNIVERSITY)

Esta Metodología que es Evaluación de Amenazas Operacionalmente Críticas, de Activos y Vulnerabilidades, se implementa con la conformación de un equipo mixto, compuesto de personas de las áreas de negocio y de TI.

Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener.

a) Existen 3 versiones de la metodología OCTAVE

- La versión original OCTAVE
- La versión para pequeñas empresas OCTAVE-S
- La versión simplificada de la herramienta OCTAVE-ALLEGRO

b) Características de la metodología OCTAVE

- Requiere un grupo de 3 a 5 personas que conozcan a planitud el desarrollo de la empresa, para recopilar información sobre los activos informáticos más importantes los requisitos de seguridad, las amenazas y las prácticas de seguridad.
- Solo realiza un barrido de manera superficial a la infraestructura informática [20]

c) Fases de la metodología OCTAVE

El proceso de evaluación contemplado por OCTAVE se divide en tres fases:

1. Construcción de perfiles de amenazas basadas en activos.

"Esta fase realiza una evaluación de los aspectos organizacionales, el equipo de análisis define el criterio de evaluación de impacto que será utilizado más adelante para evaluar los riesgos. También identifica los activos organizacionales importantes y evalúa las prácticas de seguridad actuales de la organización. El equipo completa todas las tareas por sí mismo, recolectando información adicional cuando es necesaria. Entonces se seleccionan de tres a cinco activos críticos para analizar en profundidad, basándose en la importancia relativa de estos para la organización. Finalmente el equipo define requerimientos de seguridad y define un perfil de amenaza para cada activo crítico" [20].

Octave divide los activos en dos tipos que son:

- Sistemas (Hardware. Software y Datos)
- Personas

2. Identificación de vulnerabilidades en la infraestructura.

La segunda fase para la identificación de vulnerabilidades, el equipo de trabajo realizará el siguiente proceso: Examinar la infraestructura computacional en relación con los activos críticos.

En esta fase el equipo de análisis con un enfoque tecnológico conduce una revisión a nivel general de la infraestructura computacional de la organización y la relaciona con los encargados del mantenimiento. Así se evalúa cómo ha sido considerada la seguridad de la infraestructura computacional.

El equipo de análisis primero identifica los sistemas más cercanamente relacionados con el activo crítico considerado principal (sistema de interés), a continuación se identifican los componentes clave de la red que son parte o están relacionados con el sistema de interés. Aquí se determinan puntos de acceso intermedio, es decir, los componentes de red utilizados para transmitir información desde el sistema de interés hacia los diferentes usuarios. Se consideran además desde que componentes de red se puede acceder al sistema de interés.

Se determina la localización del almacenamiento de información y se identifican en que clases de componentes esta almacenada la información con el propósito de respaldo.

Finalmente en esta actividad se identifican que otros sistemas, aplicaciones u otros componentes pueden ser utilizados para acceder al sistema de interés.

Analizar procesos relacionados con la tecnología Se marca el camino para cada componente clave y para cada punto de acceso intermedio, para identificar qué clase de componentes de red están relacionados con uno o más activos críticos. Se relacionan los activos con cada componente y punto de acceso.

Se determina responsables de mantener y asegurar cada componente.

Finalmente se identifica el grado de protección cuando se configura y mantiene cada componente y si se conoce este hecho por medios formales o no [20]

3. Desarrollo de estrategias y planes de seguridad

“Esta fase se desarrolla siempre y cuando las fases uno y dos hayan sido completadas.

En esta fase se deben desarrollar las siguientes actividades: Evaluación de activos tecnológicos, estrategias de protección y desarrollar planes de mitigación del riesgo.

Evaluación de activos tecnológicos

Es muy importante realizar este proceso dentro de la empresa ya que permite identificar los activos, controles de seguridad, ya que se evalúa los activos de la empresa por medio de la probabilidad, impacto y el grado de riesgo. El valor de la probabilidad con la previa evaluación de las amenazas, el impacto es evaluado tomando el valor conforme a su descripción, el grado de riesgo se encuentra acordeen sus valores de probabilidad e impacto, la clasificación de los posibles eventos a materializarse

Estrategias de protección

La estrategia de protección perfila la dirección de la organización con respecto a sus prácticas de seguridad de la información

Plan de mitigación de riesgo

Estos planes están pensados para mitigar los riesgos a los activos críticos por el mejoramiento de prácticas de seguridad seleccionadas” [20]

Figura 2. Fases Octave [20]

1.2.2.10 Metodología ROA

La metodología utilizada es la Evaluación de Riesgo (ROA Risk Oriented Approach) recomendada por ISACA (Information System, Audit and Control Association, Asociacion Internacional de Auditores de Sistemas de Información).

Esta evaluación de Riesgo se desarrolla sobre determinadas áreas de aplicación y bajo técnicas de Checklist (Cuestionarios) adaptados a cada entorno específico; deberá tenerse en cuenta que determinados controles se repetirán en diversas áreas deriesgo. Esto debido a que dichos controles tienen incidencia independiente en cada una.

a) Áreas de riesgos

La auto guía está dividida en varias áreas de riesgo, concretamente seis, que son:

1. Riesgo en la continuidad del proceso.
2. Riesgo en la eficacia del servicio.
3. Riesgo en la eficiencia del servicio.
4. Riesgos económicos directos.
5. Riesgos de la seguridad lógica.
6. Riesgos de la seguridad física.

b) Fases de la autoevaluación

Se explicará superficialmente el significado de cada uno, tomando en cuenta que no existe una separación absoluta entre los mismos, sino que frecuentemente se solapan e incluso determinados riesgos conllevan otros que se han evaluado en diferentes áreas.

c) Riesgo en la continuidad del proceso

Son aquellos riesgos de situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y, por ende, llegar a perjudicar gravemente a la empresa o incluso también a paralizarla. Se deberá hacer especial hincapié en el análisis estricto de estos riesgos puesto que, si bien otros podrían afectar relativamente a la empresa o bien causarle perjuicio de diverso tipo,

éstos podrían ocasionar un verdadero desastre.

a) Riesgo en la eficacia del servicio informático

Se entiende como eficacia del servicio la realización de los trabajos encomendados. Así pues, los riesgos en la eficacia serán aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

b) Riesgo en la eficiencia del servicio informático

Eficiencia del servicio es la mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad de servicio. Hay que matizar en este aspecto que determinados controles podrían resultar una mejora considerable de la eficiencia del servicio pero igualmente podrían resultar económicamente poco rentables sobre todo para pequeñas empresas. La valoración de dichos controles deberá ser analizada por los responsables de la empresa en cuya mano estará la decisión de aplicación de estos.

c) Riesgos económicos directos

En cuanto a estos riesgos se analizará aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse, e incluso aquellos gastos derivados de acciones ilegales con o sin consentimiento de la empresa que pudieran transgredir la normativa de la empresa o las leyes vigentes (LORTAD).

d) Riesgos de la seguridad física

Los riegos en cuanto a la seguridad física comprenderán todos aquellos que actúen sobre el deterioro o apropiación de elementos de información de una forma meramente física.

Dadas estas áreas de riesgo, el usuario podrá valorar cada una independientemente según sus necesidades. [21]

1.2.2.11 Estrategias de los riesgos en el manejo de la información

"Las estrategias de inversión se pueden agrupar según la siguiente clasificación:

a) Estrategias activas

Pretenden obtener una rentabilidad superior a la media del mercado.

b) Estrategias pasivas

Pretenden reproducir el comportamiento del mercado.

c) Estrategias de cartera estructurada

Persiguen garantizar la consecución de un objetivo mínimo, habitualmente un nivel mínimo de rentabilidad".

En síntesis, se puede decir que para gestionar estrategias para los diferentes riesgos existentes en una empresa se debe tomar en cuenta que existen Estrategias activas, pasivas y de cartera estructurada, las mismas que no deben pasar desapercibidas [22].

1.2.2.12 Seguridad de la Información

"El conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio."

La Seguridad de la Información son aquellas medidas protectoras y reactivas del individuo, de las formaciones y de los procedimientos tecnológicos que admitan ocultar y proteger la información buscando conservar la privacidad, la legitimidad e integridad de esta.

La información es poder y a la información se le conoce como:

a) Crítica

Es indispensable para la operación de la empresa.

b) Valiosa

Es un activo de la empresa y muy valioso.

c) Sensitiva

Debe de ser conocida por las personas autorizadas" [23].

1.2.2.13 Importancia de la Información

"La información es la parte fundamental de toda empresa para tener un alto nivel de competitividad y posibilidades de desarrollo.
Se debe conocer que la información:

- Esta almacenada y procesada en computadores.
- Puede ser confidencial para algunas personas o a escala institucional.
- Puede ser mal utilizada o divulgada.
- Puede estar sujeta a robos, sabotaje o fraudes" [24]

La importancia de la información es la parte esencial de toda Organización ya que sin información sería una Organización muerta y no habría ningún desarrollo alguno para la misma. En cualquier actividad productiva en la que estemos inmersos, día a día debemos tomar decisiones que indicarán el rumbo de nuestra empresa, ya sea hacia el éxito o al fracaso.

Pero para tomar una decisión lo más acertada posible es necesario basarnos en información de calidad" [25]

1.2.2.14 Técnicas de Seguridad

Son las acciones, procesos y métodos dirigidos a la detección y análisis de las causas y factores de riesgo. Las técnicas de seguridad se clasifican en:

a) Analíticas

Identificación de riesgos de accidentes, análisis de las causas y medidas correctoras.

b) Operativas

Control de riesgos (técnicas orientadas al control de riesgos de cada uno de los componentes de la condición de trabajo-agentes)"

1.2.2.15 Importancia del respaldo de la información

"Resguardar la información y respaldarla es algo que siempre debemos hacer para tenerla segura para en caso de alguna perdida tener una copia de esta y así recuperarla.

En la actualidad hay varias técnicas de seguridad como:

a) Confidencialidad

Garantiza que la información sea accesible a personas autorizadas.

b) Integridad

Es la seguridad de que una información no sea o haya sido alterada, borrada, copiada, reordenada, entre otras.

c) Disponibilidad

Es la seguridad de que la información sea presentada o recuperada en el momento en que esta se requiera, evitando su pérdida o bloqueo" [26].

1.2.2.16 Riesgos

Es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento.

Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro [27].

1.2.2.17 Análisis de Riesgos

El riesgo es analizado a través de la combinación de estimativos de probabilidad y de las consecuencias en el contexto de las medidas de control existentes. El análisis de riesgos involucra un debido examen de las fuentes de riesgo, sus consecuencias y la probabilidad de que esas consecuencias puedan ocurrir.

El Análisis de Riesgo no es más que una prueba donde se especifica los orígenes del riesgo y sus consecuencias que podrían estos llegar a proporcionar, para así saber qué consecuencias negativas acarrearía la empresa [28].

a) Probabilidad de Riesgo

La probabilidad de que ocurra una amenaza debe establecerse en qué circunstancias el activo tendrá valor o necesitará protección. Se determinará en función de las estadísticas recopiladas en toda la administración, también se tendrá en cuenta lo siguiente: Lo importante que es el activo para la institución. El nivel de ocurrencia que posee la vulnerabilidad en el activo. La susceptibilidad técnica que la

vulnerabilidad se materialice.

b) Evaluación de Probabilidad de Riesgo

Es el proceso con el que se identifica la frecuencia con la que ocurren las amenazas, los activos afectados y las vulnerabilidades; a su vez los criterios de riesgo establecidos se comparan con los riesgos estimados de esta manera, se determinará el nivel de importancia del riesgo. El riesgo se evalúa contemplando tres elementos básicos:

1. Estimado del valor de los activos de riesgo.

2. Probabilidad de ocurrencia del riesgo.

3. Valoración del riesgo de los activos.[29]

c) Impacto del Riesgo

El impacto es la medida del daño en el activo derivado de la materialización de una amenaza, puede afectar de inmediato a más de un activo en la institución, o puede conducir a la pérdida de información en el futuro, resultando en una pérdida financiera.

Existen varios criterios para evaluar el impacto a causa de los diferentes riesgos. Depende de cada organización definir las consideraciones necesarias para llevar a cabo esta actividad, se tomó a consideración criterios muy importantes para la cooperativa para de esta manera elaborar la tabla de evaluación de impacto entre los cuales tenemos:

El nivel de impacto para la institución en caso de cualquier daño o interrupción de los procesos de gran importancia. La valoración de la importancia de los activos. Las vulnerabilidades que existen tanto a nivel lógico como físico. Los datos y servicios que son de uso tanto interior como exterior en la institución. El valor monetario para la cooperativa en caso de sufrir algún daño, interrupción o falla en sus principales servicios. [29]

d) Determinación del Riesgo

Para determinar el riesgo de un sistema, se lleva a cabo a través del impacto de las amenazas en el valor de cada uno de los activos más relevantes para la cooperativa y la probabilidad de ocurrencia.

La metodología OCTAVE sugiere asignar valores esperados a los impactos teniendo en cuenta los valores contenidos en una matriz como ponderación alta media y baja según corresponda como se muestra en la figura 3 [29]

Figura 3. Matriz de ponderación [29]

		IMPACTO			
PROBABILIDAD	Crítica	A	A	C	C
	Alta	M	M	A	C
	Media	B	M	M	A
	Baja	B	B	M	A
		Baja	Media	Alta	Crítica

- El color rojo nos indica los riesgos críticos.

- El color naranja nos indica que son riesgos altos.

- El color amarillo son riesgos medios.

- El color verde no indica los riesgos bajos.

1.2.2.18 Tipos de Riesgos

"La Superintendencia de Bancos y Seguros ponen énfasis en los riesgos de:

a) Riesgos de Mercado

Es la contingencia de que una Institución del sistema financiero incurra en pérdidas debido a variaciones en el precio de mercado de un activo financiero.

b) Riesgo de Crédito

Es la probabilidad de proporcionar un desgaste financiero procedente del incumplimiento de los compromisos afiliadas por contrato entre las partes que lo firman, por lo cual está profundamente mezclado a las formas financieras, dificultad que se podría desarrollar a cualquier sociedad, mercado, cooperativa, banco u organismo institucional.

c) Riesgo de Liquidez

"Es la contingencia de pérdida que se manifiesta por la incapacidad de la institución del sistema financiero" [30].

1.2.2.19 Riesgos en el manejo de la información

El manejo de riesgos dentro de la seguridad en la información implica:

a) Evitar

No se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo.

b) Reducir

Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción esla más económica y sencilla.

c) Retener, Asumir o Aceptar el riesgo

Aceptar las consecuencias de la ocurrencia del evento, puede ser voluntaria que se caracteriza por el reconocimiento de la existencia del riesgo, puede ser involuntaria se da cuando el riesgo es retenido inconscientemente.

d) Transferir

Es buscar un respaldo y compartir el riego con otros controles o entidades.

1.3 Objetivos

1.3.1 Objetivo General

Realizar una Auditoría Informática para la evaluación de riesgos en la seguridad de la información de la Cooperativa de Ahorro y Crédito Prodvisión, de la provincia de Tungurahua, cantón Pelileo

1.3.2 Objetivos Específicos

- Evaluar la situación actual y la infraestructura tecnológica informática de la Cooperativa de Ahorro y Crédito Prodvisión.
- Aplicar procedimientos de Auditoría Informática orientados a los riesgos en el manejo de la seguridad de la Información.
- Emitir un informe de Auditoría Informática.

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

2.1.1 Institucionales

- Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Cooperativa de ahorro y crédito PRODVISON
- Biblioteca virtual.

2.1.2 Humanos

- Autoridades de la cooperativa
- Docente Tutor.
- Investigador.

2.1.3 Materiales

Suministros de oficina.

- Ordenador.
- Internet.
- Libros.
- Resma de hojas.
- Flash Memory
- Dispositivos de almacenamiento.

2.1.4 Económico

El Proyecto de investigación va a hacer financiado en su totalidad por el investigador.

Tabla 2. Materiales

Nº	DETALLE	UNIDAD	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
1	LAPTOP	C/U	1	900	900
2	INTERNET	H	200	0.9	180
3	RESMAS HOJAS DE PAPEL BOND	C/U	2	4	8
4	ANILLADOS	C/U	3	1.20	3.6
5	CARPETAS	C/U	3	0.8	2.4
6	IMPRESIONES	C/U	120	0.05	6
7	COPIAS	C/U	400	0.02	8
8	MEDIOS DE ALMACENAMIENTO	C/U	3	15	45
9	TRANSPORTE	DIAS	200	0.5	100
10	ESFEROS	C/U	6	0.40	2.4
11	LÁPIZ	C/U	6	0.40	2.4
					Subtotal: 1257.8
					Imprevistos (10%): 125.78
					Total: 1383.58

2.2 Métodos

2.2.1 Modalidad de Investigación

2.2.1.1 Investigación Bibliográfica y Documental

Es una investigación de tipo Bibliográfica y Documental que se constituye en una amplia búsqueda de información en revistas, libros, artículos científicos, papers, proyectos de investigación que proporcionen información adecuada relacionada con el tema de investigación

2.2.1.2 Investigación de Campo.

La investigación utiliza una indagación de Campo para representar de qué modo o porqué causas se origina el problema y poder establecer si es posible o no solucionarse, ya que es necesario trasladarse y realizar la investigación dentro del Departamento de Sistemas de la cooperativa de Ahorro y Crédito Prodvisión donde

se encuentra el problema a solucionarse y más aún tener la relación directa con cada uno de los investigados y poder sacar así una conclusión directa y confiable.

2.2.2 Población y Muestra

2.2.2.1 Población

Tabla 3. Población de la Empresa

Áreas	Número de personas
Gerencia General	**1**
Jefe de Sistemas	**1**
Socios	**20**
Total:	**22**

2.2.2.2 Muestra

Debido a que la población es menor a 100 personas no se requiere sacar una muestra.

2.2.3 Recolección de Información

El proyecto se necesitará información efectuada específica y clara para la recopilación de la información lo cual el departamento de tecnologías de información se puede verificar la ejecución de las normas determinadas en la cooperativa Prodvisión, para verificar las vulnerabilidades de la cooperativa se utilizó la metodología Octave. Por esta razón se logrará saber la situación actual de los departamentos y los activos informáticos que tiene la cooperativa.

Por ello para la recopilación de la información a nivel interno se emplea varios métodos, la entrevista, la observación y la encuesta. Conjuntamente se hará uso de fuentes bibliográficas de revistas, proyectos de investigación, para así poder cumplir los objetivos planeados.

2.2.4 Procesamiento y análisis de datos

En la cooperativa de Ahorro Crédito Prodvisión no se ha realizado una Auditoría Informática, para verificar que problemas tienen en su red, en su base de datos y aun así no han presentado algún ataque informático; además cuenta con el departamento de sistemas que está en constante monitoreo del tráfico de la red, así como de su servidor.

Para hacer transacciones bancarias la cooperativa posee un software llamado minkasoft, y un gestor de Base de Datos Oracle, y cada uno de ellos acceden al software mediante roles.

Para verificar si terceras personas han realizado alguna modificación en las cuentas bancarias, la cooperativa siempre hace un respaldo incremental en la base de datos. Para garantizar la seguridad informática la cooperativa tiene un antivirus llamada ESET NOD32.

El 5% los socios nunca cambian su contraseña, un 55% de los socios encuestados dicen que los usuarios guardan su clave en un papel ya que esto no es recomendable por qué se puede perder o romperse con el tiempo, al momento de que llega unenlace desconocido los socios dicen que se comunica con la cooperativa para no presentar inconvenientes.

CAPITULO III.- RESULTADO Y DISCUSION

3.1 Análisis y discusión de Resultados

3.1.1 Entrevista

Entrevista efectuada para saber la situación actual de la cooperativa que se describe de manera sintetizada para descubrir los problemas.

3.1.1.1 Objetivo de la entrevista

Conocer previamente los procesos de asistencia técnica e información que ofrece la cooperativa de Ahorro y Crédito Prodvisión

Tabla 4. Elaboración de la Entrevista

No.	Pregunta
1	¿Ha realizado alguna vez una auditoría informática dentro de su entidad?
2	¿El trabajador recibe algún curso o instrucción sobre el manejo de la aplicación tecnológica?
3	¿Cree importante la elaboración de una auditoria informática en el departamento de sistemas?
4	¿La cooperativa Prodvision ha sufrido ataque mediante la red?
5	¿Qué sistema operativo maneja la cooperativa?
6	¿Cuál es el proceso que debe cumplir un socio, clientes para notificar algún daño en cuanto a los servicios que la entidad ofrece?
7	¿Cuántos servidores tiene en su entidad?
8	¿Qué sistema operativo maneja su servidor?
9	¿Ha existido alguna vez, problemas sobre algún robo de información en su entidad?
10	¿Encriptas de alguna forma la clave de la base de datos?
11	¿Sus empleados, clientes, socios utilizan una contraseña larga en sus cuentas?
12	¿Para ingresar a la cuenta, sus socios, clientes utilizan un sistema de autenticación de doble factor?
13	¿Qué tipo de software utilizan para las transacciones de los clientes?
14	¿En el software de transacciones que gestión de Base de Datos posee?
15	¿En la base de datos, posee roles y perfiles que les permiten acceder al software?
16	¿En su entidad realizan respaldos de la información?
17	¿Se tienen instalados antivirus en cada departamento?
18	Con que frecuencia pide a sus trabajadores que cambien su contraseña

Elaborado por: Investigador

3.1.2 Resultado de la entrevista

3.1.2.1 Entrevista en la cooperativa de Ahorro y crédito Prodvisión

Fecha: 21/Agosto/2020

a) Lugar de la entrevista

Debido a la emergencia por la cual actualmente atraviesa el país se la realizó implementando la herramienta de videoconferencias Zoom.

ENTREVISTADOR: Kevin Paul Ramos Ruiz

ENTREVISTADO: Sr. Jorge Manuel Masaquiza Masaquiza

CARGO: Gerente

Tabla 5. Entrevista realizada a la cooperativa Prodvisión

No.	Pregunta	Respuesta
1	¿Ha realizado alguna vez una auditoría informática dentro de su entidad?	No
2	¿El trabajador recibe algún curso o instrucción sobre el manejo de la aplicación tecnológica?	Si, los trabajadores reciben una instrucción frecuente.
3	¿Cree importante la elaboración de una auditoria informática en el departamento de sistemas?	Si, una auditoría permite saber los problemas que presenta la cooperativa.
4	¿La cooperativa Prodvision ha sufrido ataque mediante la red?	No
5	¿Qué sistema operativo maneja la cooperativa?	WINDOWS 8.

6	¿Cuál es el proceso que debe cumplir un socio, clientes para notificar algún daño en cuanto a los servicios que la entidadofrece?	El socio y el cliente, informa al personal de cajas que problemas presenta, luego el personal de cajas informa al gerente que inconveniente presenta, si ha sufrido el robo de alguna información el gerente de la cooperativa le informa al personal desistemas para solucionar el problema.
7	¿Cuántos servidores tiene en su entidad?	1
8	¿Qué sistema operativo maneja su servidor?	WINDOWS SERVER 2012 RS
9	¿Ha existido alguna vez, problemas sobre algún robo de información en su entidad?	No
10	¿Encriptas de alguna forma la clave de la base de datos?	No
11	¿Sus empleados, clientes, socios utilizan una contraseña larga en sus cuentas?	Si
12	¿Para ingresar a la cuenta, sus socios, clientes utilizan un sistema de autenticación de doble factor?	No
13	¿Qué tipo de software utilizan para las transacciones de los clientes?	Minkasoft
14	¿En el software de transacciones que gestión de Base de Datos posee?	Oracle
15	¿En la base de datos, posee roles y perfiles que les permiten acceder al software?	Si
16	¿En su entidad realizan respaldos de la información?	Si, los respaldos se realizan diariamente
17	¿Se tienen instalados antivirus en cada departamento?	SI, el antivirus ESET NOD32.
18	Con que frecuencia pide a sus trabajadores que cambien su contraseña	Cada 3 meses pero por lo general no cambian con frecuencia.

Elaborado por: Investigador

b) Conclusiones o interpretación de la entrevista

De acuerdo con la entrevista realizada en la cooperativa de Ahorro y Crédito Prodvisión se encontraron los siguientes resultados:

- La cooperativa de Ahorro y crédito Prodvisión no se ha realizado ninguna auditoría informática, ya que por lo general las autoridades de la cooperativa no pueden saber que riesgos o peligros se pueden presentar.

- La cooperativa de ahorro y crédito Prodvisión pide que cambien la contraseña cada 3 meses ya que por lo general los trabajadores no lo cambian con frecuencia tal como pide la cooperativa.

- La cooperativa tiene un solo servidor, ya que por lo general si este servidor fallara se puede perder la conexión con las demás sucursales.

- La cooperativa no encripta la clave de la base de datos, ya que por lo general las claves se debe encriptar de alguna manera, para que usuarios no autorizados no logre entrar a la información.

- La cooperativa de ahorro y crédito contiene un software muy importante llamado minkasoft lo cual esta enlazado en la base de datos Oracle.

- No contiene una autenticación de doble factor lo cual no le permite informar al trabajador si usuarios no autorizados entraron a su información

3.1.3 Observación

Dentro de la Observación se fijan los detalles a investigarse de los diferentes departamentos en las diferentes capacidades y las observaciones de investigación planteadas.

Tabla 6. Observación de los Departamentos de la cooperativa

Departamento	Detalle	Observación
Departamento de Sistemas	Cables de red desordenados.	Los cables de red de la cooperativa están desordenados sin canaleta, ni identificación.
	Servidor de poca memoria.	La cooperativa tiene una Ram de 8 gb y una memoria de 4 tb ya que con la poca memoria Ram que tiene, las transacciones son un poco lentas.
	Cables de energía eléctrica cerca del hardware.	El hardware de la cooperativa están cerca de extensiones eléctricas ya que para evitar inconvenientes se debe alejarlas y no causar pérdida alguna.
	Clave de la base de datos no encriptada.	Al momento de ingresar usuarios la base de datos de la cooperativa la clave no tiene encriptada para evitar inconvenientes.
	Bios sin clave.	La cooperativa debe tener la bios con una seguridad adecuada para evitar personas no autorizadas entre al sistema operativo para cambiar o eliminar la configuración.
	Puertos abiertos.	Antes de abrir cualquier puerto, se debe de tener la seguridad apropiada para no tener inconvenientes la información.
	Clave de seguridad en la red Wifi fácil de ingresar.	Ya que la cooperativa tiene la clave de red Wifi fácil de ingresar se debe tener una configuración adecuada para que personas no autorizadas no entren a la red y para que así evitar inconvenientes.
Departamento de Cajas	Cables desordenados.	Los cables de red de la cooperativa están desordenados sin canaleta, ni identificación.
	Bios de las computadoras sin clave.	La cooperativa debe tener la bios con una seguridad adecuada para evitar personas no autorizadas entre al sistema operativo para cambiar o eliminar la configuración.

	Acceso a páginas no autorizadas.	Algunos empleados de la cooperativa en tiempos de descanso entran a páginas no autorizadas ya que puede entrar algún virus que pueda dañar el sistema operativo.
	Cables de energía eléctrica cerca del hardware.	El hardware de la cooperativa están cerca de extensiones eléctricas ya que para evitar inconvenientes se debe alejarlas y no causar pérdida alguna.
	Interruptores salidos.	Algunos interruptores en los departamentos no se encuentran bien ajustados ya que se debe ajustar adecuadamente para evitar inconvenientes.
	Transacción Un poco lenta.	Debido al que servidor se va llenando su disco, las transacciones que hacen en la cooperativa se vuelve un poco lenta
Departamento de Crédito	Interruptores salidos.	Algunos interruptores en los departamentos no se encuentran bien ajustados ya que se debe ajustar adecuadamente para evitar inconvenientes.
	Cables de Red desordenados	Los cables de red de la cooperativa están desordenados sin canaleta, ni identificación.
	Acceso a páginas no autorizadas	Algunos empleados de la cooperativa en tiempos de descanso entran a páginas no autorizadas ya que puede entrar algún virus que pueda dañar el sistema operativo.
Departamento de Gerencia	Interruptores salidos.	Algunos interruptores en los departamentos no se encuentran bien ajustados ya que se debe ajustar adecuadamente para evitar inconvenientes.
	Acceso a páginas no autorizadas.	Algunos empleados de la cooperativa en tiempos de descanso entran a páginas no autorizadas ya que puede entrar algún virus que pueda dañar el sistema operativo.
	Cable de Re desordenados. d	Los cables de red de la cooperativa están desordenados sin canaleta, ni identificación.

Elaborado por: Investigador

3.1.4 Encuesta a los socios de la cooperativa de Ahorro y Crédito Prodvisión

Conocer las dificultades que se presentan en el proceso transacciones y asistencia técnica que ofrece la cooperativa.

Analizar y Determinar de qué formas se puede agilitar mejorar y automatizar el proceso de asistencia técnica, transacciones y difusión de la información que tiene la entidad.

a) Grupo de interés que deberían responder el cuestionario

Se aplican preguntas de Seguridad Informática acerca del uso básico de las distintas herramientas y aplicativos tecnológicos a 20 socios que pertenecen la cooperativa.
Fecha: 24/Agosto/2020

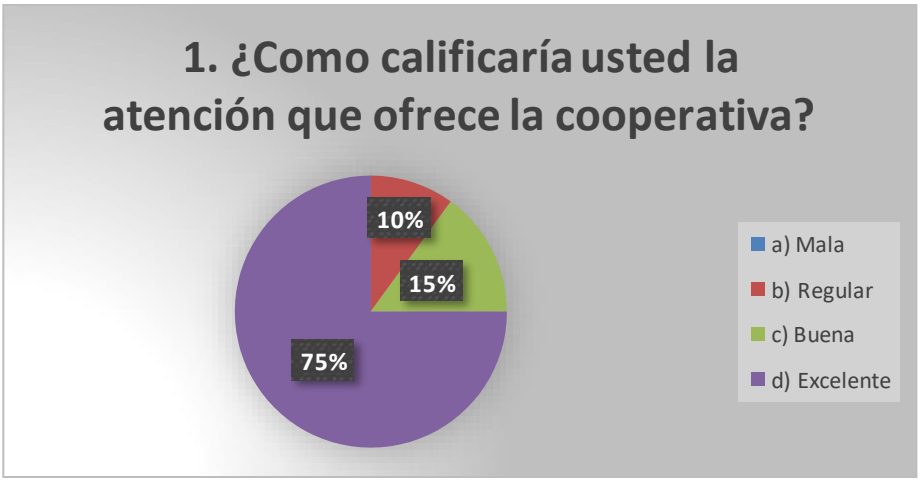
b) Preguntas para el cuestionario

1. ¿Como calificaría usted la atención que ofrece la cooperativa?

Tabla 7. Resultado de la pregunta 1

Ítems	Cantidad	Porcentaje
a) Mala	0	0
b) Regular	2	10
c) Buena	3	15
d) Excelente	15	75
Total	20	100

Figura 4. Resultado de la pregunta 1



Análisis: El 75% de los encuestados califica como excelente la atención que ofrece la cooperativa, el 15% indican que buena y el 10% dicen que la atención es regular.

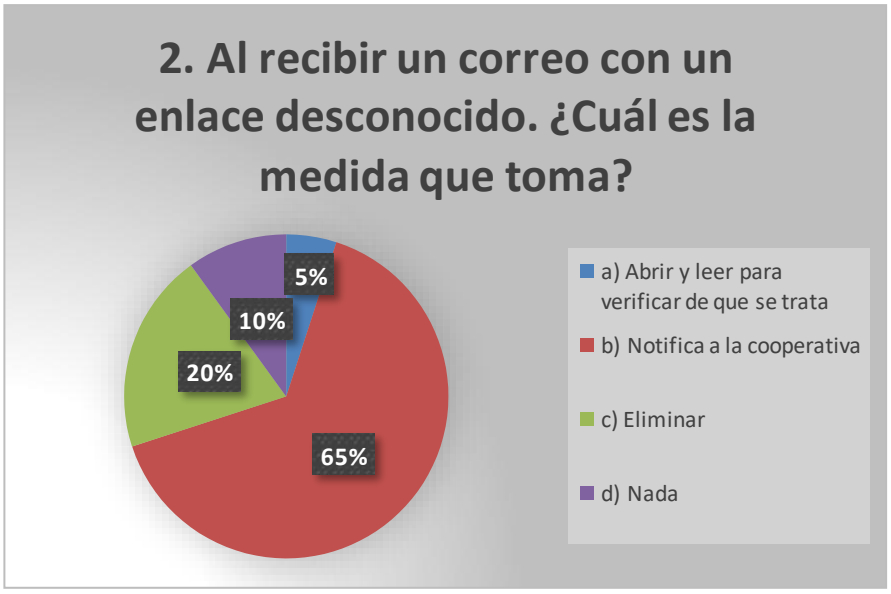
Interpretación: La cooperativa ofrece una determinada atención para el beneficio de los socios, ya que una buena atención permite crecer tanto económicamente y como institución financiera.

2. Al recibir un correo con un enlace desconocido. ¿Cuál es la medida que toma?

Tabla 8. Resultado de la pregunta 2

Ítems	Cantidad	Porcentaje
a) Abrir y leer para verificar de que se trata	1	5
b) Notifica a la cooperativa	13	65
c) Eliminar	4	20
d) Nada	2	10
Total	20	100

Figura 5. Resultado de la pregunta 2



Análisis: El 65% de los encuestados dicen que notifican a la cooperativa paraverificar si no existe algún peligro al momento de abrirlo el enlace, el 20% de los encuestados dice que elimina el correo, el 10% dice que hacen nada, y el 5% de los encuestados abren el enlace para verificar de que se trata.

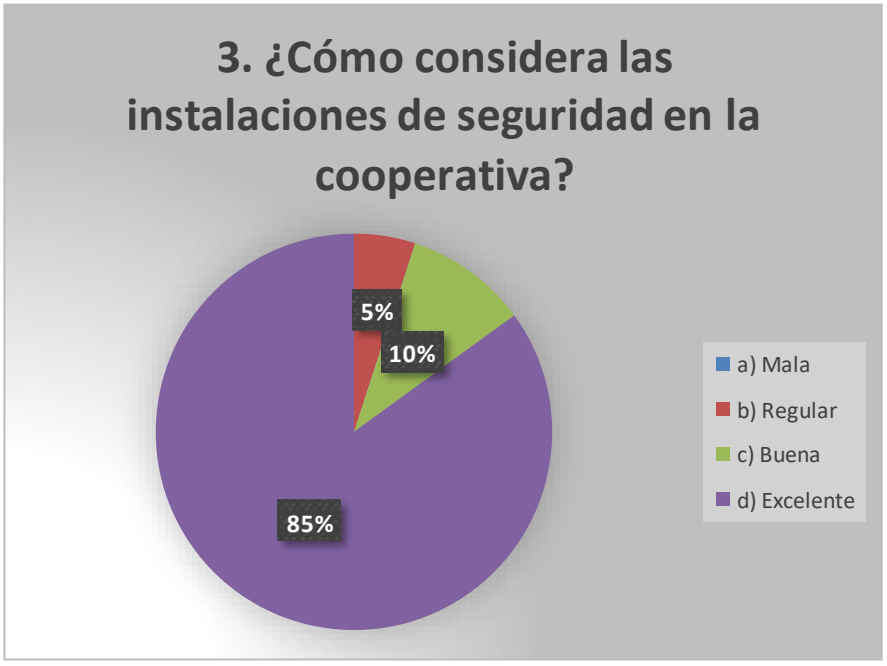
Interpretación: No es recomendable abrir un enlace sospechoso ya que puede sufrir algún ataque informático, para evitar más seguridad en sus cuentas es preferible avisar a las autoridades de la cooperativa sobre el problema ocasionado.

3. ¿Cómo considera las instalaciones de seguridad en la cooperativa?

Tabla 9. Resultado de la pregunta 3

Ítems	Cantidad	Porcentaje
a) Mala	0	0
b) Regular	1	5
c) Buena	2	10
d) Excelente	17	85
Total	20	100

Figura 6 Resultado de la pregunta 3



Análisis: El 85% de los encuestados dicen que la instalación de seguridad de la cooperativa es excelente, el 10% de los encuestados dice que las instalaciones de la cooperativa son buenas y un 5% dicen que las instalaciones son regular

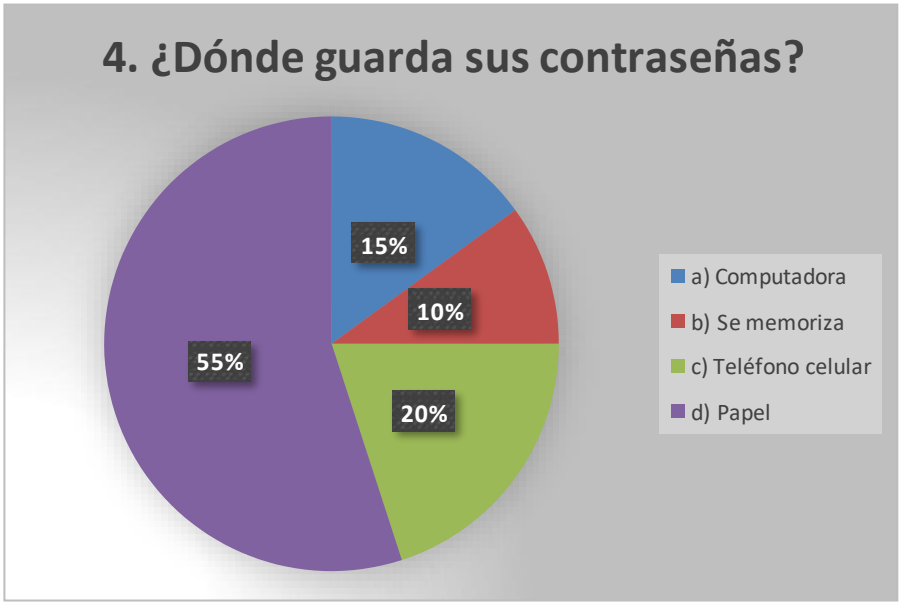
Interpretación: Los peligros y ataques a la seguridad de la cooperativa ya que puede afectar todos los días a varios socios, clientes y usuarios. Para prevenir esos peligros a la seguridad de la información se debe una mayor seguridad tanto física y lógicamente para que los socios estén tranquilos de su información.

4. ¿Dónde guarda sus contraseñas?

Tabla 10. Resultado de la pregunta 4

Ítems	Cantidad	Porcentaje
a) Computadora	3	15
b) Se memoriza	2	10
c) Teléfono celular	4	20
d) Papel	11	55
Total	20	100

Figura 7. Resultado de la pregunta 4



Análisis: El 55% de los encuestados dicen que guarda sus contraseñas en papel, el 20% dicen que guarda en su celular, el 15% dice que guarda la clave en una computadora, y el 10% de los encuestados dicen que se memorizan su clave.

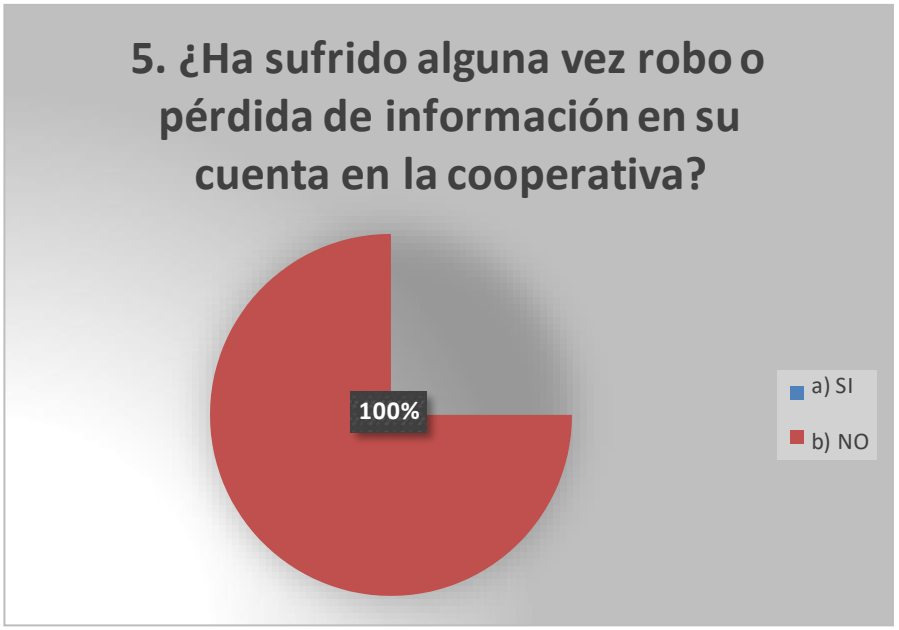
Interpretación: No es recomendable aprenderse la clave ya que en algunos casos la mente es frágil y nos podemos olvidar, lo recomendable sería por medio de un software anotar la clave de seguridad para que no nos olvidemos y para otras personas no se metan a nuestra información.

5. ¿Ha sufrido alguna vez robo o perdida de información en su cuenta en la cooperativa?

Tabla 11. Resultado de la pregunta 5

Ítems	Cantidad	Porcentaje
a) SI	0	0
b) NO	20	100
TOTAL	20	100

Figura 8. Resultado de la pregunta 5



Análisis: Todos los encuestados dicen no ha sufrido algún robo o pérdida de información en su cuenta en la cooperativa.

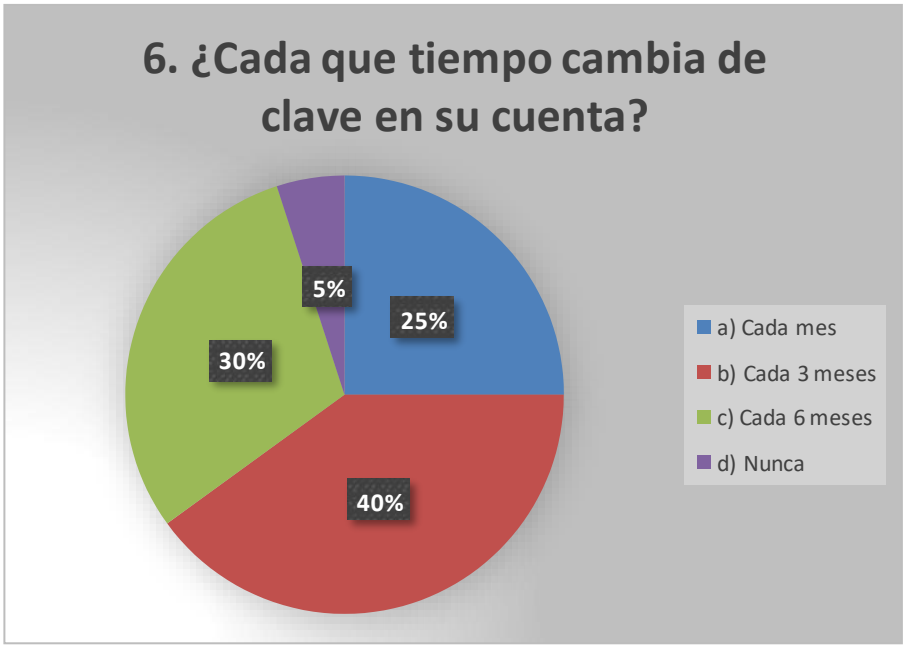
Interpretación: Ya que por no sufrir alguna pérdida de información no significa que la seguridad de la cooperativa es confiable por lo cual se debe estar atento sobre alguna anomalía que se pueda presentarse en la cooperativa.

6. ¿Cada que tiempo cambia de clave en su cuenta?

Tabla 12. Resultado de la pregunta 6

Ítems	Cantidad	Porcentaje
a) Cada mes	5	25
b) Cada 3 meses	8	40
c) Cada 6 meses	6	30
d) Nunca	1	5
Total	20	100

Figura 9. Resultado de la pregunta 6



Análisis: El 40% de los encuestados mencionan que cada 3 meses cambian su clave en su cuenta, el 30% de los encuestados dicen que cambian su clave cada 6 meses, el 25% dicen que cada mes cambian su contraseña y el 5% dicen que nunca lo ha cambiado.

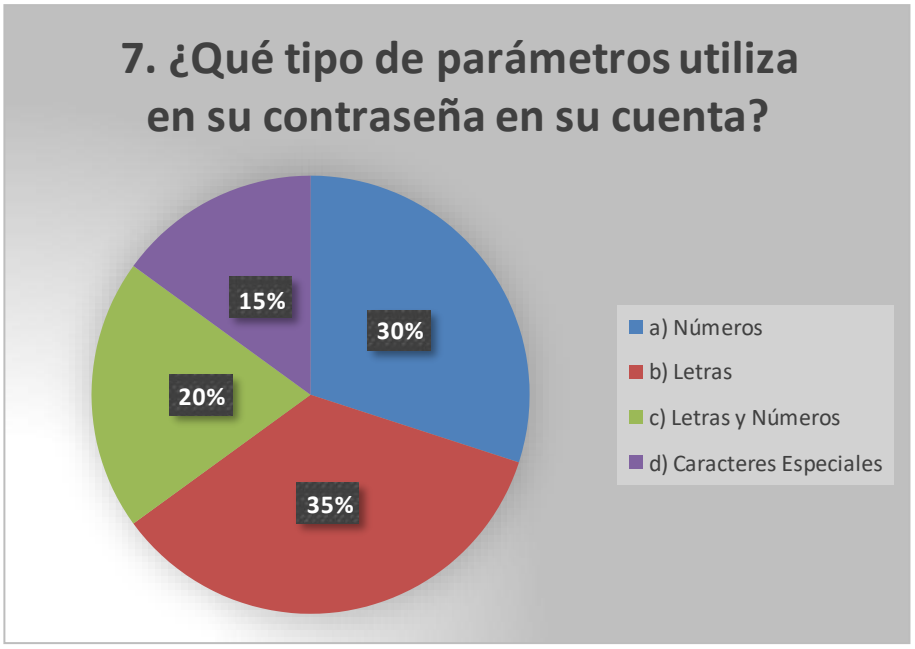
Interpretación: Por lo general ningún sistema informático es seguro es recomendable cambiar la contraseña si quiera cada 3 meses para así evitar robo de la información.

7. ¿Qué tipo de parámetros utiliza en su contraseña en su cuenta?

Tabla 13. Resultado de la pregunta 7

Ítems	Cantidad	Porcentaje
a) Números	6	30
b) Letras	7	35
c) Letras y Números	4	20
d) Caracteres Especiales	3	15
Total	20	100

Figura 10. Resultado de la pregunta 7



Análisis: El 35% de los encuestados dicen que solo utilizan letras en su contraseña, el 30% de los encuestados dicen que solo utilizan números, el 20% de los encuestados dicen que su contraseña utiliza parámetros letras y números y el 15% dicen que utilizan caracteres especiales.

Interpretación: Poner contraseña es muy esencial para que no accedan a nuestra información por lo cual es conveniente que la contraseña sea larga y sea difícil de descifrar.

8. ¿Qué piensa usted sobre la seguridad en el manejo de la información proporcionada que utiliza la cooperativa?

Tabla 14. Resultado de la pregunta 8

Ítems	Cantidad	Porcentaje
a) Riesgosa	1	5
b) Satisfactoria	6	30
c) Excelente	8	40
d) Desconoce	5	25
Total	20	100

Figura 11. Resultado de la pregunta 8

Análisis: El 40% de los encuestados dice que la seguridad que proporciona la cooperativa es excelente, el 25% dice que desconoce qué tan seguro sea su información en la cooperativa, 30% dice que están muy satisfechos en la seguridad de información que proporciona la cooperativa y el 5% dice que es riesgosa

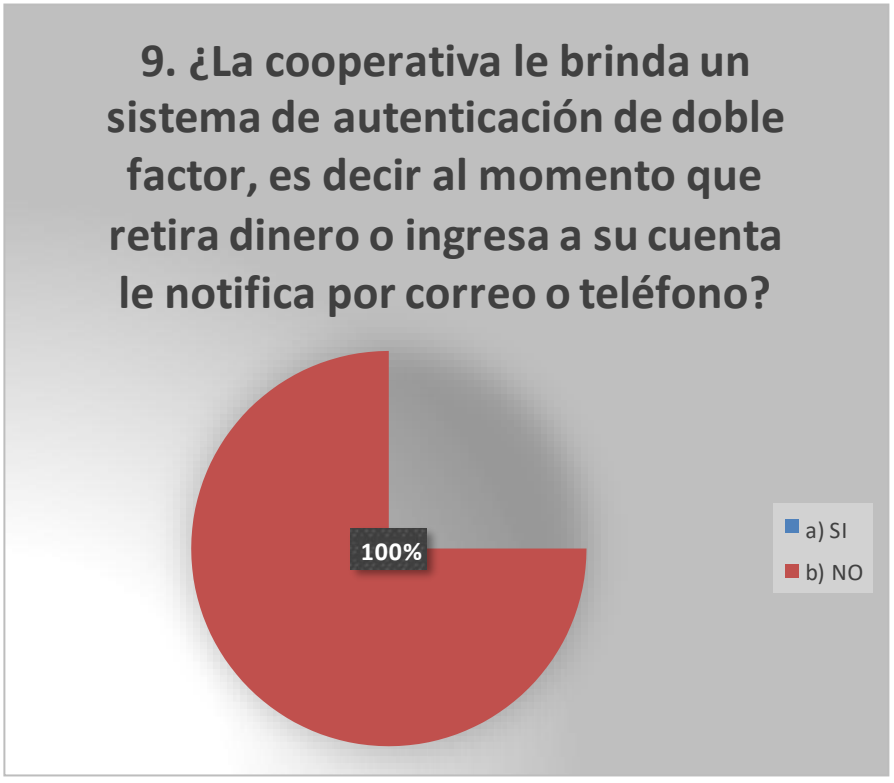
Interpretación: La cooperativa maneja una información riesgosa por lo cual los socios tienen miedo de que su dinero e información se pierda por algún ataque informático, hay algunos peligros que deberíamos considerar para no tener inconvenientes, para el robo de información.

9. ¿La cooperativa le brinda un sistema de autenticación de doble factor, es decir al momento que retira dinero o ingresa a su cuenta le notifica por correo o teléfono?

Tabla 15. Resultado de la pregunta 9

Ítems	Cantidad	Porcentaje
a) SI	0	0
b) NO	20	100
Total	100	100

Figura 12. Resultado de la pregunta 9



Análisis: Todos los encuestados dicen que la cooperativa no brinda un sistema de autenticación de doble factor.

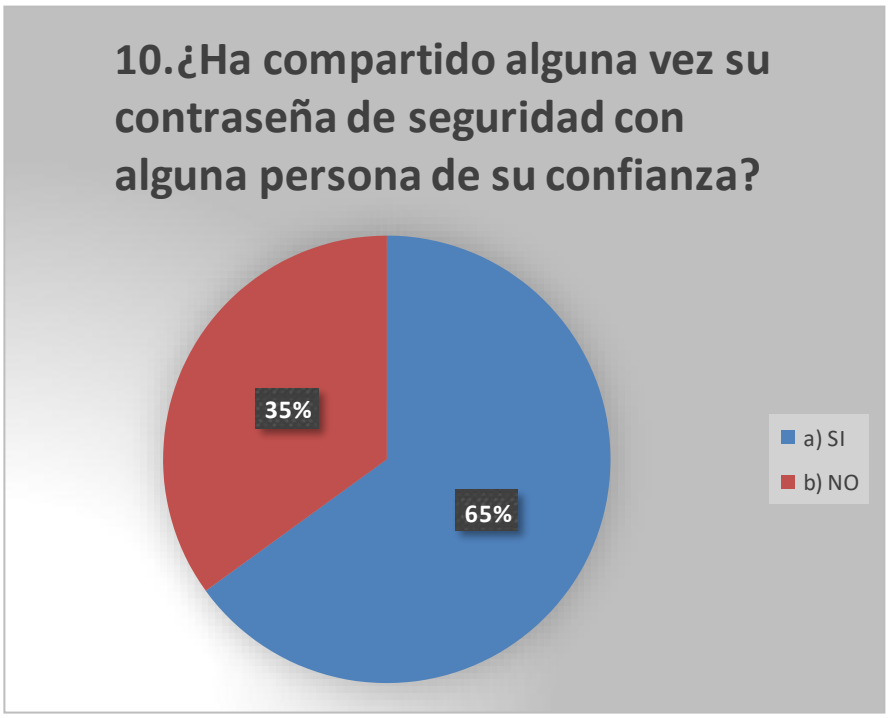
Interpretación: El sistema de autenticación de doble factor es una herramienta muy útil se recomienda que la cooperativa tenga esta herramienta ya que nos permite saber si otras personas accedieron a las cuentas sin autorización.

10. ¿Ha compartido alguna vez su contraseña de seguridad con alguna persona de su confianza?

Tabla 16. Resultado de la pregunta 10

Ítems	Cantidad	Porcentaje
a) SI	13	65
b) NO	7	35
Total	20	100

Figura 13. Resultados de la pregunta 10



Análisis: El 65% de los encuestados dicen que si comparten su contraseña con personas de confianza ya que si les olvida le puede ayudar a recordarla, y el 35% dicen que no comparte su contraseña ya que por tienen temor a que le roben la información en su cuenta.

Interpretación: Por lo general los socios por no olvidarse su clave, dicen su contraseña a una persona de confianza lo cual no es conveniente compartirla ya que sólo una persona tenga su contraseña, para que su información no sea robada.

3.1.5 Cuadro comparativo de las metodologías de auditoría

Tabla 17. Cuadro comparativo de Metodologías

METODOLOGÍA	EN QUE CONSISTE	FASES	VENTAJAS	DESVENTAJAS
OCTAVE	Esta Metodología de evaluación de amenazas operacionalmente críticas, de activos y vulnerabilidades, se implementa con la conformación de un equipo mixto, compuesto de personas de las áreas de negocio y de TI. Por su parte el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener.	- Construcción de perfiles de amenazas basadas en activos. Octave divide los activos en dos tipos que son: a) Sistemas (Hardware. Software y Datos) b) Personas - Identificación de vulnerabilidades en la infraestructura. - Desarrollo de estrategiasy planes de seguridad.	- Es una metodología autodirigida. - Comprende los procesos de análisis y gestión de riesgos. - Involucra a todo el personal de la entidad. - Se considera una de las metodologías más completas.	- No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. - Usa muchos documentos de anexos - Requiere de profundos conocimientos técnicos. - No explica en forma clara la definición y determinación de los activos de información.
ROA	Esta evaluación de riesgo se desarrolla sobre determinadas áreas de aplicación y bajo técnicas de cuestionarios adaptados a cada entorno específico. Se debe tener en cuenta que determinados controles se repetirán en diversas áreas de	- Riesgo en la continuidad del proceso. - Riesgo en la eficacia del servicio. - Riesgo en la eficiencia del servicio. - Riesgos de la seguridad lógica. - Riesgos de la seguridad física.	- Pueden ser utilizadas por personas no expertas - Cuando están bien diseñadas, combinan la experticia amplia en un sistema fácil de usar	- Tienden a abstenerse al conocimiento en la identificación de riesgos. - Tienden a establecer en la observación, omitiendo las dificultades que no se observan con claridad.

	riesgo. Dichos controles tienen incidencia independiente en cada una.			
Magerit	Es una metodología orientada a la observación y s de riesgos de los sistemas de información creada por el Consejo Superior de Administración Electrónica de España cuyo objetivo es reducir los riesgos de implantación y uso de Tecnologías accionar con la ayuda de la aplicación del software.	- Definir del alcance. - Identificar los activos. - Identificar amenazas. - Identificar vulnerabilidades y salvaguardas. - Evaluar el riesgo - Tratar el riesgo	Las dimensiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.	El hecho de tener que traducir en forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

Elaborado por: Investigador

Se ha elegido OCTAVE por las siguientes razones:

- Lo cual esta metodología fue impulsada para empresas entre 1 a 100 trabajadores, lo cual se adapta en la organización de la cooperativa
- Sintetiza la generalidad de las reglas y criterios de la protección de los datos.
- Es autodirigido ya que si se presenta algún tipo de problema se acude al trabajador principal de la cooperativa, quien conoce los inconvenientes que presenta, ya que puede orientar en la investigación en los sitios no seguros con el propósito de no malgastar dinero.
- OCTAVE es un método para evaluar los riesgos que contempla la principal cantidad de elementos que interceden en la protección de la información.
- Esta metodología considera los factores técnicos en la protección, en relación con la cooperativa, y los sitios menos seguros o vulnerables se valoran en contacto con los elementos que vinculen en la protección de la cooperativa.
- Esta metodología proporciona un gran ajuste de los problemas que tiene las empresas a las que se les emplea este método para analizar los peligros. En tal sentido se tiene una gran precaución en el progreso de las técnicas y métodos de disminución de peligros ya que estos se realizan considerando la situación de la cooperativa y sobre todo se usan las destrezas y enfoques de los trabajadores de la empresa para resolver y afrontar los peligros detallados a los activos de las empresas.
- El estudio de esta metodología, similar que nuevas metodologías, puede soportar varias dificultades que fundamentan especialmente en las normas de los dirigentes de la cooperativa, lo cual consigue no considerar legal el desarrollo para el servicio dentro de la cooperativa. Sin embargo, al considerar varios métodos, esto se puede solucionar.

3.1.6 Aplicación de la metodología Octave

Para la evaluación de riesgos del proyecto de investigación se escogió la metodología OCTAVE, ya que esta metodología está dividida en tres fases:

3.1.6.1 Fase 1: Construir perfiles de amenazas de activos de información

"Esta fase forma parte de la visión organizacional o de gestión. Entonces serealizan los procesos de: Identificar la información organizacional, y crear los perfiles de amenazas" [31].

a) Identificar la información organizacional

Durante la visita preliminar se identifica todas las salas donde se encuentra el equipamiento de cómputos y se clasificó en "principales" y "secundarias", entendiéndose por principales aquellas donde se ubican los dispositivos más importantes para la red tales como servidores, hubs, switch, etc.

Es válido resaltar que las salas principales deben contar con un mayor control de seguridad que las secundarias.

a) Activos de Información

La Organización utiliza el software necesario para sus actividades en cada departamento.

Entre el Software que maneja la cooperativa tenemos:

Microsoft SQL Server

Microsoft Visual Studio.

Servicio de Internet:

Puntonet Windows 8

Microsoft Office 2013 TeamViewer

Antivirus ESET NOD32

b) Descripción del Servidor

Tabla 18. Descripción del servidor

Servidor			
Cantidad	**Componente**	**Marca**	**Modelo**
1	Servidor	Intel	Proliant ml150
	Capacidad	4TB	
	Ram	4GB	

Tabla 19. Descripción del software que tiene el servidor

SOFTWARE		
Nombre	**Versión**	**Tipo**
Windows server	2008r2 estándar	Sistema Operativo Servidores
Microsoft Office	2013	Ofimática
SQL SERVER	2012	Base de Datos
ESET NOD32		Antivirus

c) Activos de Base de Datos

Tabla 20. Base de Datos de la cooperativa de Ahorro y Crédito Prodvisión

Variables	Detalle
Cobertura geográfica	Tungurahua, Galápagos
Número de usuarios	25076
Usuarios por género	F: 10322 M: 14754
Usuarios por edad	18-57 años
Recursos humanos	
- Directivos	8
- Empleados	10
- Trabajadores	18
Recursos Tecnológicos	
- Computadores	25
- Impresoras	8
- Servidor	1
Recursos físicos	
- Edificios	1
Recursos materiales	
Vehículos	Ninguno
Sillas	65
Escritorios	10
Archivadores	2
Mesas	2
Recursos Financieros	$ 800523,06 Activos
Otros recursos	Ninguno

d) Activos de software

En la tabla 27 se detallan el tipo de software que es usado en los diferentes departamentos de la cooperativa, la mayoría de software utilizado posee su respectiva licencia, o a su vez aplicaciones desarrolladas por el Departamento de Sistemas tomando en cuenta las necesidades de los socios y clientes.

Tabla 21. Activos de software detallado por departamento

SOFTWARE			
Nombre	**Versión**	**Tipo**	**Departamento**
Windows	7 Home 64-bits	Sistema Operativo	Sistemas
Microsoft Office	2013 64-bits	Ofimática	Sistemas
TeamViewer	11	Acceso Remoto	Sistemas
ESET NOD32		Antivirus	Sistemas
Windows	7 Home 64-bits	Sistema Operativo	Gerencia
Microsoft Office	2013 64-bits	Ofimática	Gerencia
TeamViewer	11	Acceso Remoto	Gerencia
ESET NOD32		Antivirus	Gerencia
Windows	7 Home 64-bits	Sistema Operativo	Contabilidad
Microsoft Office	2013 64-bits	Ofimática	Contabilidad
TeamViewer	11	Acceso Remoto	Contabilidad
ESET NOD32		Antivirus	Contabilidad
Windows	7 Home 64-bits	Sistema Operativo	Información
Microsoft Office	2013 64-bits	Ofimática	Información
TeamViewer	11	Acceso Remoto	Información
ESET NOD32		Antivirus	Información
Windows	7 Home 64-bits	Sistema Operativo	Cajas
Microsoft Office	2013 64-bits	Ofimática	Cajas
TeamViewer	11	Acceso Remoto	Cajas
ESET NOD32		Antivirus	Cajas
Windows	7 Home 64-bits	Sistema Operativo	Asesor de Créditos
Microsoft Office	2013 64-bits	Ofimática	Asesor de Créditos
TeamViewer	11	Acceso Remoto	Asesor de Créditos
ESET NOD32		Antivirus	Asesor de Créditos
Windows	7 Home 64-bits	Sistema Operativo	Jefe de Créditos
Microsoft Office	2013 64-bits	Ofimática	Jefe de Créditos
TeamViewer	11	Acceso Remoto	Jefe de Créditos
ESET NOD32		Antivirus	Jefe de Créditos

Fuente: Cooperativa de Ahorro y Crédito Prodvisión

e) Activos de Hardware

La cooperativa comprende recursos de hardware que se manejan como activos fijos y que son los que se han tomado en cuenta, detallados por departamento.

Tabla 22. Activos del Hardware

HARDWARE				
Cantidad	**Componente**	**Marca**	**Modelo**	**Departamento**
1	Monitor	Acer	al1711 fb(1280x1024)	Sistemas
1	Procesador	Intel	Core 2 Duo E8200	Sistemas
1	RAM	4gb	DDR2	Sistemas
1	Placa base	Biostar	G31-M7 OC	Sistemas
1	Disco Duro ATA Device (465GB)	Samsung	HD502HI	Sistemas
1	Monitor	Acer	al1711 fb(1280x1024)	Administración
1	Procesador	Intel	Core i3 2120	Administración
1	RAM	-	DDR3	Administración
1	Placa base	Intel	DH61HO	Administración
1	Disco Duro SATA (698GB)	Seagate	ST3750640NS	Administración
1	Monitor	Acer	al1711 fb(1280x1024)	Administración
1	Monitor	Acer	al1711 fb(1280x1024)	Administración
1	Monitor	Samsung	732 n plus	Administración
1	Monitor	Acer	al1711 fb(1280x1024)	Administración
1	Monitor	Lg	22ld310 ma	Administración
1	Monitor	Vaio	Touch smart 600 1050	Administración
1	Copiadora	Ricoh	Aficio MP C4502	Administración
1	Impresora	Epson	l565	Administración
1	Impresora	Canon	mp280	Administración
1	Monitor	Acer	W1943 (1280x720)	Contabilidad
1	Procesador	Intel	Pentium Dual-Core CPU E5700	Contabilidad
1	RAM	Kingston	DDR3	Contabilidad
1	Placa base	Biostar	G41D3C	Contabilidad

1	Disco Duro ATA (465GB)	Seagate	ST500DM0021B D142	Contabilidad
1	Monitor	BenQ	G925HDA (1366x768)	Contabilidad
1	Procesador	Intel	Pentium Dual-Core CPU E5800	Contabilidad
1	RAM	Kingston	DDR3	Contabilidad
1	Placa base	Intel	DG41WV	Contabilidad
1	Disco Duro ATA (465GB)	Samsung	HD502HJ	Contabilidad
1	Impresora	EPSON	LX-300+ /II	Contabilidad
1	Monitor	Acer	AL1711 (1280x1024	Facturación
1	Procesador	Intel	Intel Core i3-4160	Facturación
2	RAM	Kingston	DDR3	Facturación
1	Placa base	Gigabyte Technology	H81M-S2PH	Facturación
1	Disco Duro SATA (465GB)	Seagate	ST500DM005 HD502 SCSI	Facturación
1	Impresora	Epson	lx 300II	Facturación
1	Monitor	Lg	L177wsb	Facturación
1	Monitor	LG TV (1280x720)	22ld310 ma	Importaciones
1	Procesador	Intel	Intel Core i3-3220	Importaciones
2	RAM	Kingston	DDR3	Importaciones
1	Placa base	Intel	DH67BL	Importaciones
1	Disco Duro ATA (1397GB)	Seagate	ST1500DL0039V T16L	Importaciones
1	Impresora	Canon	mp280	Importaciones
1	Monitor	Lg	W1943 (1360x768)	Información
1	Procesador	Intel	Intel Core i7 4770	Información
2	RAM	A-Data Technology	DDR3	Información
1	Placa base	Gigabyte Technology	H81M-DS2	Información
1	Disco Duro SATA (931GB)	Westem Digital	WD10EZEX08M 2NA0	Información
1	Monitor	Lg	L177WSB (1440x900)	Recepción
1	Procesador	Intel	Pentium Dual-Core CPU E5700	Recepción

2	RAM	Kingston	DDR3	Recepción
1	Placa base	Biostar	G41D3C	Recepción
1	Disco Duro ATA (500GB)	Samsung	HD502HJ	Recepción
1	Monitor	Lg	W1943 (1360x768)	Bodega
1	Procesador	Intel	Pentium Dual-Core CPU E540	Bodega
1	RAM	Kingston	DDR3	Bodega
1	Placa base	Intel	DG41TY	Bodega
1	Disco Duro ATA (37,3GB)	Maxtor	4K040H2	Bodega

Fuente: Cooperativa de Ahorro y Crédito Prodvisión

f) Personal

La Cooperativa comprende el siguiente personal lo cual se describe en la tabla 23.

Tabla 23. Personal de la Cooperativa

Función	Nombre	Cédula
Gerente General	Jorge Manuel Masaquiza Masaquiza	1806739372
Presidente de consejo administrativo	Andres Geovany Masaquiza	1804760765
Presidente de consejo de vigilancia	Darwin Eugenio Masaquiza	1807272718
Contadora	Maria Teresa Masaquiza	1802352727
Gerente sucursal Galápagos	Jose Andres Masaquiza	1838828828
Jefe de sistemas	Segundo Alfredo Tenelema Tixe	1727832788
Asesor de créditos	Rubén Masaquiza	1809737299

Fuente: Cooperativa de Ahorro y Crédito Prodvisión

g) Descripción de cargos y funciones de la cooperativa

Tabla 24. Funciones del Gerente

Cargo: Gerente

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Ingeniería 7mo Semestre
CONOCIMIENTOS:	Contabilidad, Informática, Administración, Asesorías en créditos, Inversiones, Proyectos
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Habilidad numérica, Toma de decisiones, Pensamiento estratégico, Compromiso y Ética.
EXPERIENCIA:	8 años
RESPONSABILIDAD:	
Dirigir y Tutelar al personal de la cooperativa, administrar inversiones, créditos, contabilidad, proyectos y publicidad.	
AUTORIDAD:	
Dar informes al consejo directivo.	
FUNCIONES:	
Planificar, coordinar, supervisar y evaluar la gestión administrativa y financiera de la cooperativa, según normas técnicas, legales y administrativas vigente. Diagnosticar las condiciones y evaluar el mercado financiero en función de los planes de crecimiento y de la continuidad del negocio. Analizar, sugerir e implementar las estrategias de mercadeo de productos y servicios, recuperación de cartera, captación de recursos e inversiones. Aprobar créditos solicitados según rangos de aprobación establecidos, por el Consejo de Administración en el reglamento de Crédito. Participar del Comité de Crédito para la aprobación de solicitudes según rango establecido, en el Reglamento de Crédito. Informar, ejecutar, coordinar, controlar y evaluar el cumplimiento de las disposiciones de los órganos de control, Públicos en los términos establecidos por sus respectivas Leyes.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 25. Funciones del Contador

Cargo: Contadora General

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Ing./ Lic. Contabilidad y auditoría o a fines
CONOCIMIENTOS:	Tributación, Derecho Laboral, Programas Contables, Inventarios, NIIF.
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Ética, Habilidad Analítica y Numérica.
EXPERIENCIA:	4 años.
RESPONSABILIDAD:	
Manejar documentación contable, elaboración de Balances, Declaraciones mensuales, anexos, nomina.	
AUTORIDAD:	
Informa de sus actividades al Gerente General	
FUNCIONES:	
Ingreso de facturas de compras. Cancelación de Cuentas por pagar.	
Elaboración de quincenas para los trabajadores.	
Elaboración y pago de los roles de pago.	
Revisión de reporte de reloj y cálculo de horas extras.	
Revisión y reposición de caja chica, de las diferentes oficinas.	
Elaboración de formularios para pagos de decimos y utilidades.	
Toma física de inventarios.	
Elaboración de ajustes de entradas y salidas de inventarios.	
Elaboración de formularios para trámites de patentes y 1.5 por mil de la empresa.	
Paso de la información a la súper intendencia de compañías.	
Revisión y manejo de anticipos de los trabajadores.	
Contabilizaciones mensuales.	
Cálculo de comisiones para asesores de crédito.	
Colaboración con el control de inventario anual.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 26. Funciones del Cajero

Cargo: Cajero

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Universitaria
CONOCIMIENTOS:	Conocimiento de los productos de la empresa, conocimiento del mercado, conocimiento de la empresa.
COMPETENCIAS:	Orientación al cliente, Calidad de trabajo, Orientación a los resultados, Pensamiento estratégico, Negociación
EXPERIENCIA:	6 años
RESPONSABILIDAD:	
Manejo de documentos de facturación y entrega de pagos a la organización.	
AUTORIDAD:	
Informa de sus actividades al Jefe de cajas y al Gerente.	
FUNCIONES:	
Entrega de cuentas de la ruta al Jefe de Cajas. Revisión y planificación de cobro de los estados de cuenta de los clientes. Llamado a clientes para comunicar el cobro de las cuentas. Sacar copias de las facturas como respaldo de las cuentas. Elaboración de información de clientes. Retroalimentar a la empresa todo lo que sucede con el cliente: inquietudes, quejas, sugerencias, reclamos, agradecimientos, y otros de relevancia. Informe de devoluciones de pedidos. Atender y resolver las quejas y reclamaciones que presenten los socios. Aplicar eficientemente lo concerniente a transparencia de información y protección de los socios de servicios financieros	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 27. Funciones del Director Gestión de Talento Humano

Cargo: Director de Gestión de Talento Humano

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Psicólogo Organizacional
CONOCIMIENTOS:	Derecho Laboral, Mrl, Seguridad Industrial, Código de Trabajo.
COMPETENCIAS:	Temple, Integridad, Conciencia Organizacional, Orientación al cliente, Liderazgo.
EXPERIENCIA:	3 años.
RESPONSABILIDAD:	
Manejo de documentación personal de los trabajadores.	
AUTORIDAD:	
Informa de sus actividades a la Gerencia General.	
FUNCIONES:	
Realizar el proceso de Contratación de nuevo personal. Realizar Inducción de la empresa al personal. Proyectar y coordinar programas de capacitación y entrenamiento para los empleados. Realización de eventos que ayuden al mejoramiento del clima organizacional. Solución de conflictos entre el personal. Elaboración de certificados de trabajo; Creación de Sistemas de motivación. Revisión mensual del sistema de alimentación Emisión y autorización de permisos en la empresa. Llevar el Registro de vacaciones del personal. Coordinar y controlar el proceso de egreso para la desincorporación del personal, ya sea por despido, retiro voluntario o culminación de contrato. Realizar una evaluación de las capacitaciones impartidas al personal. Llevar un registro de asistencia de las capacitaciones recibidas por el personal. Llevar un control del personal donde cumplan con las normas y procedimientos de seguridad y salud en el trabajo.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 28. Funciones del Jefe de Cajas

Cargo: Jefe de Cajas

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	BACHILLERATO
CONOCIMIENTOS:	Contabilidad, Informática, Administración
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Habilidad numérica, Toma de decisiones, Pensamiento estratégico, Compromiso y Ética.
EXPERIENCIA:	5 años
RESPONSABILIDAD:	
Dirigir y Tutelar al personal de Cajas.	
AUTORIDAD:	
Informa de sus actividades a la Gerencia General	
FUNCIONES:	
Control de calidad de todos los ítems que estén en cada máquina de cada cajero. Control de medidas de los programas de cada una de las máquinas de cada cajero. Coordinación y planificación de los cajeros conjuntamente con gerencia. Revisión de abastecimiento de cajeros para la respectiva atención personalizada de los clientes. Revisión y planificación de abastecimiento de herramientas maquinas físicas que cubran a los respectivos cajeros. Presentar Informes mensuales de acuerdo al formato establecido. Inspección, investigación y muestreo con el fin de controlar los factores que puedan afectar la calidad de servicio que se brinda a los clientes. Aprobar los procedimientos relacionados con las operaciones, incluyendo los controles en proceso y asegurar su estricto cumplimiento. Optimizar el espacio interno, mejorando el flujo de los procesos financieros realizados, eliminando movimientos innecesarios ya sea recursos materiales como recursos humanos.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 29. Funciones del Jefe de Créditos

Cargo: Jefe de créditos

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Bachillerato
CONOCIMIENTOS:	Informática, Administración, Costos
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Habilidad numérica, Toma de decisiones, Pensamiento estratégico, Compromiso y Ética.
EXPERIENCIA:	4 años
RESPONSABILIDAD:	
Verificar la documentación y aprobación de los créditos	
AUTORIDAD:	
Informa de sus actividades a la Gerencia General	
FUNCIONES:	
Atender a los socios y colaboradores de la Institución que requieran créditos. Evaluar solicitudes de crédito según políticas y reglamento de crédito vigentes. Aprobar o negar operaciones dentro de su rango permitido. Participar del comité de crédito para evaluar y recomendar la aprobación o negación de solicitudes de crédito. Coordinar y establecer políticas de recuperación de créditos con los Jefes de Agencias, el control de la morosidad de los deudores, según las leyes vigentes y según normas del Reglamento de Crédito vigente. Coordinar las acciones administrativas de cobro a socios con créditos en mora, con el Abogado de planta de la Cooperativa y abogados externos de Matriz y Agencias. Distribución y calificación de cartera. Notificar a socios morosos visitándolos in situación.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 30. Funciones del Asesor de Créditos

Cargo: Asesor de créditos

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	BACHILLERATO
CONOCIMIENTOS:	Informática, Recopilación de datos, Asesorías crediticias
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Habilidad numérica, Toma de decisiones, Pensamiento estratégico, Compromiso y Ética.
EXPERIENCIA:	3 años
RESPONSABILIDAD:	
Recopila datos de los clientes, realiza informes, verifica y entrega créditos	
AUTORIDAD:	
Informa de sus actividades al Jefe de Créditos	
FUNCIONES:	
Recibir, evaluar, y realizar informes, según las políticas establecidas en el Reglamento de Crédito Vigente. Evaluar solicitudes de crédito según políticas y reglamento de crédito vigentes, dentro de su rango de aprobación. Despachar los créditos aprobados, según las normas internas de crédito Elaborar y presentar diariamente informes de riesgos, morosidad y recuperación de los créditos de socios deudores. Traslado a las distintas provincias del Ecuador, con la finalidad de realizar cobros, ventas y asesoramiento de los productos. Determinación de estándares de calidad. Ingreso de información de los clientes para las revisiones previas acerca del crédito. Notificar a socios morosos visitándolos en sus lugares de vivienda o trabajo.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 31. Funciones de Personal de Información

Cargo: Personal de información

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	BACHILLERATO
CONOCIMIENTOS:	Contabilidad, Informática, Administración, Asesorías en créditos.
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Habilidad numérica, Toma de decisiones, Pensamiento estratégico, Compromiso y Ética.
EXPERIENCIA:	8 años
RESPONSABILIDAD:	
Dirigir y Tutelar al personal de la cooperativa, administrar inversiones, créditos, contabilidad, proyectos y publicidad.	
AUTORIDAD:	
Dar informes al consejo directivo.	
FUNCIONES:	
Brindar asesoramiento a los clientes de los diferentes productos que ofrece la empresa. Atender y resolver las quejas y reclamaciones que presenten los socios. Aplicar eficientemente lo concerniente a transparencia de información y protección de los socios de servicios financieros Establecer una conexión entre cliente y empresa comunicando oportunamente la información importante. Consulta y actualización del histórico de los socios en la base de datos en el sistema. Resumen de las resoluciones adoptadas, con indicación del carácter favorable o desfavorable para el reclamante. Responsable de las aperturas y cierre de cuentas de ahorros de los socios de personas naturales y jurídicas.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

Tabla 32. Funciones de Jefe de Sistemas

Cargo: Jefe de Sistemas

PERFIL BÁSICO

FORMACIÓN:	
EDUCACIÓN:	Ing. En Sistemas
CONOCIMIENTOS:	Computación, Manejo de base de Datos, Programación, Administración.
COMPETENCIAS:	Orientación a la Eficiencia, Calidad de Trabajo, Innovación, Certificación CISCO.
EXPERIENCIA:	5 años.
RESPONSABILIDAD:	
Administración de la Información, Tecnologías de la Información.	
AUTORIDAD:	
Informa de sus actividades al Gerente General.	
FUNCIONES:	
Mantenimiento preventivo y correctivo de las computadoras. Mantenimiento de software y hardware. Mantenimiento del Sistema interno de la empresa. Mantenimiento de la Red. Realizar informes mensuales de actividades. Responsable del manejo del correo electrónico de la empresa.	

Fuente: Cooperativa de ahorro y crédito Prodvisión

b) Creación de perfiles de amenazas

"Para crear los perfiles de amenazas realizamos a cumplir los siguientes requerimientos: Identificar los requerimientos de seguridad para activos críticos e identificar las amenazas a los activos críticos" [31].

a) Identificar los requerimientos de seguridad para activos críticos

"Entre lo más fundamental dentro de la cooperativa están los activos lo cual se emite el requerimiento adecuado, puesto que esto es trascendental para la seguridad de la información, según los activos nombrados en la tabla 33, estos deben ser evaluados para establecer los más importantes, establecidos en los tres aspectos principales disponibilidad, integridad y confidencialidad de los requerimientos.

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, de tipo software y de tipo físico. Para la evaluación de estos activos se debe obtener el promedio para cada uno de los niveles" [31].

Tabla 33. Identificación de los requerimientos de seguridad para los activos críticos.

DESCRIPCION DE ACTIVO	D	I	C	TOTAL
SERVIDOR	4	4	4	4
COMPUTADORES	4	3	4	3,67
ROUTER	3	3	4	3,33
IMPRESORAS	3	3	4	3,33
CUENTAS DE USUARIOS	4	4	4	4
LAPTOPS	2	3	2	2,33
RED WIRELESS	4	3	3	3,33
RED LOCAL	4	4	4	4
TEAMVIEWER	3	3	3	3
MINKASOFT	4	4	4	4
SOFTWARE	4	3	3	3,33
SQL SERVER	4	4	4	4
CAMARA DE SEGURIDAD	4	4	4	4

Elaborado por: Investigador

b) Identificar las amenazas a los activos críticos.

"Se establece todos los activos críticos con un valor sea mayor o igual a 3 para evaluar el riesgo, lo cual se anota en la columna el nombre del activo a evaluar y se lo establece en la matriz que interseca a un árbol de amenazas. Las ramas representan las amenazas que establecen en el activo

Después de la tasación se establece la probabilidad de incidencia de las amenazas, asumiendo el impacto en el caso de suscitarse. Se asigna la siguiente fórmula para evaluar el riesgo:

Riesgo = Total del activo crítico × Probabilidad de amenaza" [32]

Tabla 34. Identificar las amenazas a los activos críticos.

ACTIVO	AMENAZAS	VULNERABILIDAD	VALORACION TOTAL DEL ACTIVO	PROBABILIDAD DE AMENAZA	RIESGO TOTAL
SERVIDOR	PÉRDIDA DE INFORMACIÓN	MAL MANEJO EN EL SOFTWARE Y DEL HARDWARE	4	3	12
		LAS NORMAS DE SEGURIDAD NO SON ADECUADAS			
		PERDIDA DE DATOS POR ERROR DEL HARDWARE			
		ACTUALIZACIÓN DEL SOFTWARE			
	RASONWARE	BLOQUEO DE DISPOSITIVOS Y DE INFORMACIÓN			
	VIRUS	INSERTAR USB INFECTADAS			
	PERDIDA DE CONEXIÓN	MALA CONFIGURACIÓN EN LA RED			
COMPUTADORES	VIRUS	ENTRAR A ENLACES NO AUTORIZADAS	3,66	4	14,64
		METER USB INFECTADA			
	PERDIDA DE INFORMACIÓN	ACTUALIZACION DEL SOFTWARE Y DEL SISTEMA OPERATIVO			

	PHISING	INGRESO A ENLACES SOSPECHOSOS			
	RASONWARE	BLOQUEO DE DISPOSITIVOS Y DE INFORMACIÓN			
ROUTER	PÉRDIDA DE CONEXIÓN	CONFIGURACIÓN INADECUADA EN LAS IPS	3,33	3	9,99
	DAÑO EN EL HARDWARE	PROBLEMAS AL ENCENDER EL ROUTER			
IMPRESORAS	EL PAPEL SE ATORA	PAPEL MÁS PUESTO	3,33	3	9,99
	DAÑOS EN LOS CABEZALES	FALTA DE MANTENIMIENTO			
	DAÑOS EN LOS CARTUCHOS				
	PERDIDA DE CONEXIÓN	CONFIGURACIÓN INADECUADA DE LA RED			
CUENTAS DE USUARIOS	MODIFICACIÓN DE PERFILES DE USUARIOS	POLÍTICAS DE SEGURIDAD INADECUADAS	4	3	12
	INGRESO DE USUARIOS INACTIVOS Y NO AUTORIZADOS	FALTA DE CONTROL DE ACCESO			
	ACCEDER A INFORMACIÓN NO AUTORIZADA	ABUSO DE PRIVILEGIOS			

RED WIRELESS	MALWARE	ACCESO LIBRE A LA RED	3,33	4	13,32
	CRACKING DE CONTRASEÑAS	CONTRASEÑAS FACILES DE CRACKEAR			
	ESPIONAJE	USO INADECUADO DE LA RED			
	PERDIDA DE INFORMACIÓN	LAS NORMAS SEGURIDAD NO SON APROPIADAS			
	RASONWARE	BLOQUEO DE DISPOSITIVOS Y DE INFORMACIÓN			
RED LOCAL	MALWARE	ACCESO LIBRE A LA RED	4	4	16
	INGENIERÍA SOCIAL	MANIPUCIÓN DE LA INFORMACIÓN			
	SUPLANTACIÓN DE IDENTIDAD	CULPAR A OTROS USUARIOS POR PÉRDIDA DE INFORMACIÓN			
	RASONWARE	BLOQUEO DE DISPOSITIVOS Y DE INFORMACIÓN			
	PERDIDA DE CONEXIÓN	CABLES DETERIORADOS			
		CABLES MAL CONECTADOS			
		MALA CONFIGURACIÓN DE LAS IPS			

TEAMVIEWER	ESPIONAJE	USO INADECUADO DE LA RED	3	4	12
	ROBO DE INFORMACIÓN	CONFIGURACIÓN INADECUADA DEL SOFTWARE			
MINKASOFT	PERDIDA DE INFORMACIÓN	FALTA DE REQUERIMIENTOS EN EL SISTEMA	4	4	16
		ACTUALIZACIÓN DEL SOFTWARE			
	MODIFICACIÓN DE PERFILES DE USUARIOS	POLÍTICAS DE SEGURIDAD INADECUADAS			
	INGRESO DE USUARIOS INACTIVOS Y NO AUTORIZADOS	FALTA DE CONTROL DE ACCESO			
SOFTWARE	PERDIDA DE INFORMACIÓN	LAS NORMAS DE SEGURIDAD NO SON ADECUADAS	3,33	3	9,99
		ACTUALIZACIÓN DEL SOFTWARE			
	VIRUS	DESCARGAR EN PÁGINAS NO SEGURAS.			
		METER USB INFECTADA			
	MALWARE	BLOQUEO DE DISPOSITIVOS Y DE INFORMACIÓN			

SQL SERVER	MANIPULACIÓN DE LA INFORMACIÓN	INYECCION SQL	4	3	12
	PERDIDA DE INFORMACIÓN	LAS NORMAS SEGURIDAD NO SON APROPIADAS			
		ACTUALIZACIÓN DEL SOFTWARE			
CAMARA DE SEGURIDAD	PERDIDA DE CONEXIÓN	CABLES DETERIORADOS	4	4	16
		CABLES MAL CONECTADOS			
		MALA CONFIGURACIÓN DE LAS IPS			
	MALWARE	ACCESO LIBRE A LAS CÁMARAS DE SEGURIDAD			

Elaborado por: Investigador

3.1.6.2 Fase 2. Identificar vulnerabilidades en la estructura

Esta se efectuará de acuerdo con la evaluación de la inseguridad que han sido mostradas en los distintos activos que tiene una evaluación crítica, la posibilidad de casos de cada uno de los activos, por lo cual examinamos distintas medidas:

- Lo valioso que es el activo para la cooperativa

- El grado de amenaza que conoce en el resultado de la vulnerabilidad en el activo.

- La sensibilidad concreta que la inseguridad se realice.

Tabla 35. Identificación de vulnerabilidades

Nº	Amenaza	Área y activos afectados	Vulnerabilidad	Impacto
1	Pandemia/Desastres Naturales/Terremotos	Departamentos	Se puede perder la información porque tiene almacenada en un solo lugar	Alta
2	Incendio		Falla eléctrica	Baja
3	Paralización de servicios		Daños en software y hardware	Media
4	Deterioro Físic o lógico o		Cables de red rotos, limpieza de máquinas	Media
5	Humedad	Servidor	Falta de ventilación	Media
6	Acceso al servidor sin autorización		Movimientos de claves sin autorización	Media
7	Problemas en el servidor		El servidor no responde a las transacciones hechas por el usuario	Alta
7	Ingeniería Social		Hackers	Media
8	Instalar Software Dañinos		Pérdida de Información	Alta
9	Fallas de energía eléctrica		Apagones	Baja
10	Información no guardada		Caída del sistema	Baja
11	Mantenimiento al servidor			Baja

12	Perdida de datos por error del usuario		Saturación de Base de Datos	Media
13	Pérdida de conexión entre las sucursales		Falla del servidor	Baja
14	Electromagnetismo	Red	Fallas en el diseño en la red	Media
15	Modificaciones en los datos		Tráfico en la red insegura	Alta
16	Usuarios ingresan al pc		Puertos abiertos	Alta
17	Manipulación inapropiada en el teamviewer		Transferir información indebida en la cooperativa	Baja
18	Manipulación del sistema Minkasoft		Pérdida de información	Baja
19	Cable de red en el piso		Perdida de conexión si el cable se llega a mover	Media
20	El cableado de la red se encuentra junto al de la red eléctrica		Los cables se pueden quemar	Media
21	Falta de organización del cableado		Perdida de Conexión	Media
22	Partes del cable deteriorado			Media
23	Cableado sin identificadores		Mala configuración en la red	Alta
24	Fallas en la energía de la computadora	Computadores	Daños en el pin de encendido de la pc	Media
25	Fallas del software		El usuario no puede manejar bien el software	Baja
26	Fallas del Hardware		Falta de mantenimiento y vida útil del Hardware	Media
27	Conectores de PC sin atornillar		Falla en el equipo de computo	Media
28	Incumplimiento con los requerimientos de la cooperativa	Estructural organizacional de la empresa	Falta de personal en el área de sistemas	Baja
29	Incumplimiento de autenticación de usuarios inactivos de		Los usuarios inactivos logran ingresar al	Baja

	la cooperativa		sistema.	
30	Extintor alejado al computador		Daños a los equipos por explosión del extintor	Baja
31	Espacio reducido entre el escritorio y el computador		No se puede trabajar adecuadamente	Media
32	Inseguridad en la instalación de los tomacorrientes		Las normas de seguridad no son adecuadas	Media
33	No se restringe el acceso a persona no autorizadas a los dispositivos mayores, ni menores		Se pueden acceder sin autorización ala información	Alta
34	No existen cartelesque prohíban comer y fumar dentro de la cooperativa.		Se puede regar comida y bebidas que pueden perjudicar al hardware	Media
35	Dispositivos sin identificadores		Pérdida de conexión	Alta
			La información se puede pasar al computador equivocado	
36	Dispositivos accesibles a personas no autorizadas		Se pueden acceder sin autorización a la información	Alta
37	Conectores de pared no se encuentran fijos		Falla eléctrica	Media
38	Conectores en el piso			Media
39	Mal funcionamiento en las cámaras de seguridad		Pérdida de conexión	Media
40	Acceder a páginas no autorizadas	Información	Pérdida de datos	Media
41	Dispositivos accesibles a personas no autorizadas		Robo de Información	Media
42	Listado de trabajadores en la cooperativa con el área de desarrollo	Base de Datos	Faltas de normas de seguridad	Baja

43	Estándar de asignación de usuarios y claves			Baja
44	Mala Asignación de Perfil		Permisos insuficientes	Baja
45	Verificación de Logs		Solicitudes fallidas para acceder a algunos de los servicios que se ejecutan.	Baja
46	Fallas de procesos para recuperar la información		La información no se logra recuperar de manera correcta y rápidamente	Alta
47	Fallos en la creación de backups		Fallos en el procedimiento para respaldar la información	Media
48	Mala documentación para verificar de los cambios realizados en la base		Lista de información no realizada en la base de datos.	Alta
49	Mala Estructura de la base de datos		No nos facilita ver la estructura lógica y física de los datos obtenidos	Media
50	Olvidar la creación de la clave primaria		Redundancia de la información en la Base de Datos	Baja
51	Acceso a la base de datos sin autorización		Movimientos de claves sin autorización	Alta
52	Manipulación en el software	Software	Pérdida de Información	Media
53	Virus			Media
54	Accesibles a personas no autorizadas		Robo de Información	Media
55	Estándar de asignación de usuarios y claves		Faltas de normas de seguridad	Media
56	Mala asignación de perfiles		Permisos insuficientes	Baja

Elaborado por: Investigador

3.1.6.3 Fase 3. Desarrollar estrategias y planes de seguridad

"En esta última fase se investiga siempre y cuando las fases uno y dos hayan sido completadas, lo cual se realizan las siguientes labores: evaluación de activos tecnológicos que consiste en evaluar la probabilidad y el impacto, seleccionar enfoques de mitigación que se transfieren los estados de alerta del riesgo del resultado de la probabilidad y del impacto como muestra la figura 3, también se desarrolla las estrategias de protección y desarrollar planes de mitigación delriesgo.

a) Evaluación de activos tecnológicos

La tabla 36 pertenece a la evaluación de los activos tecnológicos, el valor de la probabilidad con la previa evaluación de las amenazas, el impacto es evaluado tomando el valor conforme a su descripción, el grado de riesgo se encuentra acorde en sus valores de probabilidad e impacto, la clasificación de los posibles eventos a materializarse" [31]

Tabla 36. Evaluación de activos tecnológicos

Nº	Amenaza	Probabilidad	Impacto	Riesgo
Activo: Departamentos				
1	Pandemia/Desastres Naturales/Terremotos	Baja	Alta	Media
2	Incendio	Baja	Media	Baja
3	Paralización de Servicios	Baja	Media	Baja
4	Deterioro físico o lógico	Baja	Media	Baja
5	Manipulación del sistema Minkasoft	Alta	Crítica	Crítica
Activo: Servidor				
6	Humedad	Media	Media	Media
7	Problemas en el servidor	Baja	Crítica	Alta
8	Acceso al servidor sin autorización	Baja	Crítica	Alta
9	Ingeniería Social	Media	Crítica	Alta
10	Instalar Software Dañinos	Media	Crítica	Alta

11	Fallas de energía eléctrica	Media	Alta	Media
12	Información no guardada	Media	Crítica	Alta
13	Mantenimiento al servidor	Media	Media	Media
14	Perdida de datos por error del usuario	Baja	Crítica	Alta
15	Código Sospechoso	Baja	Crítica	Alta
16	Pérdida de conexión entre sucursales	Baja	Crítica	Alta
Estructura organizacional de la cooperativa				
17	Incumplimiento con los requerimientos de la empresa	Baja	Alta	Media
18	Incumplimiento de autenticación de los usuarios activos e inactivos de la cooperativa	Baja	Crítica	Alta
19	Extintor alejado al computador	Baja	Media	Baja
20	Espacio reducido entre el escritorio y el computador	Media	Media	Media
21	Inseguridad en la instalación de los tomacorrientes	Baja	Alta	Media
22	No se restringe el acceso a persona no autorizadas.	Alta	Crítica	Crítica
23	No existen carteles que prohíban comer y/o fumar dentro de los cubículos	Media	Alta	Media
24	Dispositivos sin identificadores	Media	Alta	Media
25	Dispositivos accesibles a personas no autorizadas	Media	Crítica	Alta
26	Conectores de pared no se encuentran fijos	Baja	Alta	Media
27	Conectores en el piso	Media	Media	Media
28	Mal funcionamiento en las cámaras de seguridad	Baja	Alta	Media

Activo: Redes				
29	Modificaciones en los datos	Baja	Crítica	Alta
30	Usuarios no autorizados ingresana la pc	Baja	Crítica	Alta
31	Manipulación inapropiada en el teamviewer	Baja	Crítica	Alta
32	Manipulación del sistema Minkasoft	Baja	Crítica	Alta
33	Cable de red en el piso	Media	Alta	Media
34	El cableado de la red se encuentra junto al de la red eléctrica	Alta	Alta	Alta
35	Falta de organización del cableado	Alta	Alta	Alta
36	Partes del cable deteriorado	Media	Alta	Media
37	Cableado sin identificadores	Baja	Alta	Media
Activo: Computadores				
38	Fallas en la energía de la computadora	Media	Alta	Media
39	Fallas del software	Media	Crítica	Alta
40	Fallas del Hardware	Media	Alta	Media
Activo: Información				
41	Acceder a páginas no autorizadas	Media	Crítica	Alta
42	Acceso no autorizado a terceras personas	Baja	Crítica	Alta
Activo: Base de Datos				
43	Listado de trabajadores en la cooperativa con el área de desarrollo	Baja	Alta	Media
44	Verificación de Logs	Media	Alta	Media
45	Estándar de asignación de usuarios y claves	Baja	Alta	Media
46	Mala Asignación de Perfil	Baja	Alta	Media

47	Fallas de procesos para recuperar la información	Baja	Crítica	Alta
48	Procesos de creación de backups	Baja	Alta	Media
49	Mala documentación para verificar de los cambios realizados en la base	Baja	Crítica	Alta
50	Mala Estructura de la base de datos	Baja	Alta	Media
51	Olvidar la creación de la clave primaria	Baja	Alta	Media
52	Acceso a la base de datos sin autorización	Alta	Alta	Alta
Activo: Software				
53	Manipulación en el software	Baja	Alta	Media
54	Virus	Media	Alta	Media
55	Accesibles a personas no autorizadas	Baja	Alta	Media
56	Estándar de asignación de usuarios y claves	Baja	Alta	Media
57	Mala asignación de perfiles	Baja	Media	Baja

Elaborado por: Investigador

b) Estrategias de protección

Cuando se detallaron los riesgos de seguridad en la tabla 36, se establecieron los requerimientos fundamentales paraestablecer la seguridad de los datos de cada uno de los activos. En la tabla 37, se menciona el activo simultáneamente con las estrategias para reparar los requerimientos de seguridad.

Tabla 37. Estrategias de protección

ACTIVO	ESTRATEGIAS DE PROTECCIÓN
Estructura organizacional de la cooperativa	- La Cooperativa Prodvisión debe tener asegurado equipos, datos, ya que si pierden por fuerza mayor no tenga problemas a futuro. - Establecer normas de seguridad para evitar el ingreso de alimentos y a personas no autorizadas. - Realizar documentación que contenga las políticas y procedimientos para la asignación correcta de responsabilidades, con lo cual se pueda tener una organización más adecuada de cargos. - Se debe tener el listado correctamente de todos los trabajadores activos e inactivos para no tener problemas en la autenticación del sofware y hardware. - Tener un mejor ambiente de trabajo. - Verificar si el extintor este en un mejor lugar para que no afecten a los equipos. - Comprobar la conexión de la cámara de seguridad. - Ubicar estratégicamente los cubículos. - Ubicar los tomacorrientes en lugares definidos.
Servidor	- Siempre debe estar disponible para realizar las transacciones adecuadas. - Los datos guardados solo pueden acceder, el personal de sistemas o un personal autorizado - Normas de seguridad para la autenticación de usuarios. - Si el software es actualizado se debe tener respaldo, para no tener

	inconvenientes después de las actualizaciones correspondiente. - No ejecutar programas, ni archivos desconocidos. - Contar con un antivirus. - Se debe tener un segundo servidor en caso de que el primer servidor tenga problemas para realizar las transacciones
Computadores	- Si el software es actualizado se debe tener respaldo, para no tener inconvenientes después de las actualizaciones correspondiente. - No ejecutar programas, ni archivos desconocidos. - No entrar a enlaces desconocidos. - Contar con un antivirus. - Usar claves seguras y cambiarlas habitualmente.
Red	- Siempre debe estar disponible para realizar los trabajos adecuados en la cooperativa. - Verificar la seguridad de la red. - Poner canaletas para evitar pisar los cables de red. - Bloquear a los usuarios no autorizados que ingresaron en la red de Wireless. - Reemplazar los cables deteriorados. - Establecer normas de seguridad para establecer las configuraciones de los puntos de conexión. - Almacenar el cableado faltante en bodega. - El manejo de la red solo puede ser realizado por el personal de sistemas o por un personal autorizado. - Realizar los documentos de las políticas y procedimientos deinventario para poder tener conocimiento de las máquinas, cableado, routers, etc. que tiene la cooperativa dentro de sus instalaciones. - Los dispositivos de comunicación deben encontrarse alejados de terceros.
Base de Datos	- Cambiar las claves por lo menos 1 vez cada 3 meses para evitar robo de información. - Hacer backups todos los días y un backup completo al menos una vez a la semana. - Verificar el proceso de backup, así como el de restauración de

	archivos, al menos una vez al mes. - Guardar una copia completa de seguridad fuera del lugar habitual de trabajo. - Normas de seguridad para la autenticación de usuarios. - Se debe tener una información cifrada
Software	- El personal de sistemas o personas autorizadas pueden acceder al sistema. - Cambiar las claves por lo menos 1 vez cada 3 meses para evitar robo de información. - La información que se guarda mediante el software debe tener credibilidad. - Si el software es actualizado se debe tener respaldo, para no tener inconvenientes después de las actualizaciones correspondiente. - El software debe tener un mayor grado disponibilidad. - Cerrar la sesión al momento de acabar el trabajo.
Información	- Distribuir copias de seguridad en la nube o en lugares que no estén dentro de la cooperativa. - Establecer filtros de Spam para evitar enlaces sospechosos.

Elaborado por: Investigador

c) Desarrollo de plan de mitigación de riesgos

En la tabla 38, se plantean las actividades de mitigación para las áreas de práctica de seguridad, la razón de haber seleccionado, el responsable de llevarlos a cabo y que soporte adicional se necesita para implementarlas.

Tabla 38. Desarrollo de plan de mitigación de riesgos

Área	Actividades	Proceso	Responsables	Factores de Riesgos
En todos los departamentos	Realizar inspección en el sistema Minkasoft	Comprobar si los usuarios se loguen de acuerdo con el perfil que le asignen. Verificar si no hay pérdida de información. Verificar si en el software no se puede hacer una inyección sql.	Jefe de Sistemas, Gerente	Error de conexión con la base de Datos Inyección Sql Perdida de Información
	Control de Seguridad en las laptops	Verificar si no hay virus. Ver si no hay pérdida de Información Verificar si no hay sospecha de malware Conexión adecuada de Wireless y Lan		Virus Malware Pérdida de Información. Pérdida de conexión de la red.

	Inspeccionar las computadoras de escritorio	Comprobar si las computadoras estén bien conectadas en el cortapicos Verificar si no existen virus. Comprobar si usuarios no autorizados no estén conectados al computador Conexión adecuada de la red. Verificar si existe conexión entre las computadoras Verificar si no hay pérdida de información.		Computadores no prende Falla eléctrica Perdida de Información Virus en las máquinas. Pérdida de conexión de la red
	Infraestructura de la cooperativa	Comprobar si los cables no estén deteriorados Verificar si los reguladores de energía estén correctamente conectados Comprobar si el extintor esté en un lugar correcto Verificar si las cámaras de seguridad estén funcionando correctamente. Verificar si los cables de red no estorban al caminar. Verificar si hay letreros de acceso a personas no		Cables deteriorados Extintor no está en un lugar adecuado Falla eléctrica Error de conexión en las cámaras de seguridad. Pérdida de conexión. Ingreso de personas no autorizadas. Ingreso de alimentos que puede perjudicar al hardware. Pérdida de información

		autorizadas. Verificar si hay letreros de prohibir de ingreso de alimentos. Verificar si no hay sospecha de Phising.		
Departamento de Sistemas	Control de Seguridad en el Servidor	Verificar si no existe virus en el servidor. Verificar si las computadoras hacen conexión con el servidor Verificar si el software de las máquinas de la cooperativa hace conexión con el servidor Verificar si no hay sospecha de Malware.	Jefe de Sistemas	Virus Pérdida de conexión. Malware
	Realizar un control de seguridad en la red Wireless	Verificar si la clave de Wireless sea segura. Verificar si hay usuarios no autorizados conectados en la red		Contraseña débil. Usuarios sospechosos en la red. Malware.
	Realizar un control de seguridad en la red Lan.	Comprobar si el cable de red este correctamente conectado. Comprobar si las ips estén asignados correctamente en los computadores. Verificar la seguridad de los puertos.		Cables de red deteriorados. Puertos inseguros. Pérdida de conexión Malware

	Control en la base de Datos	Verificar si los usuarios activos e inactivos permiten ingresar a la base Examinar si los usuarios no autorizados ingresan a la base Verificar si los respaldos hacen correctamente Comprobación de perfiles correctamente. Comprobar si no hubo modificaciones en la información		Usuarios inactivos ingresan a la base de datos. Usuarios no autorizados ingresan a la base Pérdida de información Los respaldos no son sacados correctamente. Mala de asignación de perfiles de los usuarios

Elaborado por: Investigador

3.1.7 Situación Actual de la Cooperativa de Ahorro y Crédito Prodvisión

Prodvision Cooperativa de Ahorro y Crédito es una institución que ofrece servicios financieros a los más altos estándares y tiene por objetivo principal contribuir con el crecimiento de pequeñas y medianas empresas a nivel nacional e internacional. Es un referente en cuanto a instituciones financieras ya que ofrece servicios financieros con una atención de primera y con tecnología de punta para el adecuado servicio, comprometida en luchar contra la pobreza, el desempleo y la migración, fue constituida legalmente con Acuerdo N° 2540 del Consejo de Desarrollo de las Nacionalidades y Pueblos Indígenas CODENPE del 15 de septiembre de 2011 y registrada en la SEPS Superintendencia de Economía Popular y Solidaria, con registro No. SEPS-ROEPS-2013-002581.

Entre las principales características que ofrece Provisión Cooperativa de Ahorro y Crédito tenemos:

1. Atención personalizada cuenta con profesionales calificados para ofrecer asesoría completa a los clientes.

2. Tasa de tarifas de interés competitivos al 21 % a nivel Nacional K.

3. Enfocados en las necesidades de sus clientes: pequeñas y medianas empresas al ofrecerles las más bajas tarifas de interés.

4. Mantienen una tecnología actualizada para brindar una gama amplia de servicios financieros para sus asociados.

5. Efectuar inversiones en el capital social de cajas centrales.

6. Cuenta con sucursales para abastecer la demanda generada por la sociedad [33]

3.1.7.1 Evaluación de las Condiciones Actuales de la Organización

a) Estrategias de Negocios

Prodvisión Cooperativa de Ahorro y Crédito cuenta con un documento de planificación estratégica formal en la que se basan para avanzar en el crecimiento y desarrollo de la Institución referente a la Planeación Estratégica del Área de Tecnologías de la Información.

Prodvisión Cooperativa de Ahorro y Crédito cuenta con las siguientes estrategias

de negocios:

Mantener publicidad dirigida al mercado meta.

Realizar todas las operaciones con transparencia informando todo proceso al socio.

Realizar incentivos a las capacitaciones financieras de socio, depósitos en libretas de ahorro y búsquedas de financiamiento internacional.

Participación en varias actividades comunitarias y sociales mediante donaciones, capacitación, etc.

Difundir en medios de comunicación los resultados obtenidos después de un determinado tiempo o actividad relevante.

Incrementar inversiones a nivel estable desarrollando proyectos de inversión con el Banco de Fomento.

Estas estrategias de negocios son conocidas por todos quienes conforman esta organización, lo que ha permitido establecer la necesidad de un Plan Estratégico conformado formalmente a corto plazo [33].

b) Misión

"Prodvisión Cooperativa De Ahorro y Crédito es una entidad financiera de ahorro y crédito de apoyo social a las microfinanzas y emprendimientos de la región, mediante la innovación de sistemas y procesos de calidad agiles y oportunos para el socio y la comunidad" [33].

c) Visión

"La cooperativa Prodvisión es una institución consolidada y reconocida a nivel nacional, como proveedora de servicios financieros. Solvente y sólida, ofrece servicios ágiles y oportunos a sus socios y clientes, a través de recursos tecnológicos, personal capacitado, comprometido y procesos internos establecidos"[33].

d) Valores y principios

a) Valores

Igualdad

Equidad

Solidaridad

Honestidad

Transparencia.

Responsabilidad social [33].

b) Principios

Se aplicarán los principios universales del cooperativismo

1. Membresía abierta y voluntaria

2. Control democrático de los miembros

3. Participación económica de los miembros

4. Autonomía e independencia

5. Educación, formación e información

6. Cooperación entre cooperativas

7. Compromiso con la comunidad

La cooperativa no concederá privilegios a ninguno de sus socios, ni aún a pretexto de ser directivo, fundador o benefactor, ni los discriminará por razones de género, edad, etnia, religión o de otra naturaleza [33].

3.1.7.2 Antecedentes históricos de la Institución

Prodvision ha proyectado ser líder en mercado financiero. Un día viernes 30 de julio del 2010, nace en la parroquia de Salasaca perteneciente a la Provincia de Tungurahua una institución financiera con el fin de promover el desarrollo económico del pueblo de Salasaca, siendo el promotor Andrés Geovany Masaquiza Masaquiza.

La institución inicia sus actividades el 16 de agosto del año 2010 en la comunidad de Rumiñawi Grande con la idea de ser en el futuro una institución bancaria, con la denominación de banco comunitario centro con un capital inicial de 1000 dólares americanos.

El 15 de septiembre, un nuevo acuerdo ministerial 2450 emitido por el codempe lo denomina corporación de desarrollo financiera Prodvision, una entidadfinanciera popular y solidaria, apoyar el desarrollo del Sumak Kausay de los pueblos y nacionalidades del país, a lo que sigue de inmediato periodo de transición bajo el CODENPE (CONSEJO DE DESARROLLO DE LAS NACIONALIDADES Y PUEBLOS DEL ECUADOR). Por estos días la
corporación de desarrollo financiera Prodvision con 50,000 dólares americanos.

El 12 de septiembre, un grupo de jóvenes, adquiere la calidad de socios fundadores. El Sr Darwin Eugenio Masaquiza Masaquiza, Jorge Manuel Masaquiza Masaquiza, Oscar Eduardo Curichumbi Jerez, Fanny Gloria Caizabanda Masaquiza, Ethan Josué Masaquiza Masaquiza, José Andrés Masaquiza Masaquiza, Mario Rubén Masaquiza Masaquiza,

Desde esta fecha, la nueva administración de la corporación de desarrollo financiera Prodvision, aplica un enfoque moderno de nueva institución financiera, adquiere los equipos de computación más sofisticados del mercado y crea cuatro divisiones básicas para desarrollar sus servicios: ahorros, créditos, remesas internas, inversiones.

Segundo Directorio estaba formado por jóvenes de la parroquia de Salasaka Tecnólogo Andrés Geovany Masaquiza Masaquiza (director Ejecutivo Fundador), Darwin Eugenio Masaquiza Masaquiza (Subdirector Ejecutivo fundador).

Jorge Manuel Masaquiza Masaquiza (coordinador general), Oscar Eduardo Curichumbi Jerez (secretario General), Fanny gloria Caizabanda Masaquiza (Director Financiero Fundador), Ethan Josué Masaquiza Masaquiza (consejo de vigilancia fundador), José Andrés MasaquizaMasaquiza (consejo de vigilancia fundador), Mario Rubén Masaquiza Masaquiza (consejo de vigilancia fundador)

El 2 de diciembre del 2011, gracias el esfuerzo del director ejecutivo se aprueba para la creación de dos sucursales en las provincias de Carchi Cantón Tulcán Provincia Pastaza Cantón Puyo y el 30 de diciembre mismo mes se aprueba para la creación de cinco sucursales mas en las provincias de Napo

cantón Tena, Provincia de Tungurahua cantón Ambato y Pelileo, Provincia de Galápagos San Cristóbal y Santa Cruz. Aprovechando las recientes reformas a la Ley orgánica de la economía popular y solidaria y del sector financiero popular y solidario, el 30 de marzo del surge reconstitución de socios fundadores y recapitulación cumpliendo con el articulo 7 numeral cuarto. Así se transforma a cooperativa de ahorro y crédito Prodvision, con un capital pagado de 280,000 dólares americanos. Estos pasos iniciales formaron a la cooperativa de ahorro y crédito Prodvision de ghoy, y le permitieron alcanzar grandes e importantes metas que lo han convertido en una institución solvente en el ámbito financiero [33].

3.1.7.3 Localización de la Entidad y zona de influencia

La Cooperativa de Ahorro y Crédito "PRODVISION". Ltda, tiene su matriz ubicada en Salasaka Centro – Vía Baños, Tungurahua.

Agencia Galápagos (Santa Cruz) Av. Dulcan y Calle Petrel.

Agencia Galápagos. (Santa Cristobal) Av. Alsacio Northia e Isabel.

Sucursales en las provincias de:

- Carchi Cantón Tulcán
- Pastaza Cantón Puyo
- Napo cantón Tena
- Próximamente en Pelileo

3.1.7.4 Aspectos legales de la Entidad

Las instituciones del servicio financiero, están ubicadas en ciudades, sectores semiurbanos y rurales, captan ahorros y conceden pequeños créditos para la producción y el comercio a sus clientes y si bien es difícil cuantificar la existencia a escala nacional, según la Súper Intendencia de Economía Popular y Solidaria SEPS, este número podría bordear las 400. A estas se suman las 39 instituciones que integran la Asociación de Cooperativas normadas por la Superintendencia de Bancos. Son organizaciones gestionadas democráticamente por los socios, los cuales participan activamente en la fijación de sus políticas y en la toma de

decisiones, las personas elegidas para representar y gestionar son responsables ante los socios.

Los mismos que tienen iguales derechos de voto, están organizadas de forma democrática las cooperativas en un análisis presentan evidentes debilidades en la toma de decisiones, sin que los organismos de control tanto estatales como los de la propia institución hayan efectuada las actividades necesarias para solucionarlos [34].

a) Constitución política de la Republica del Ecuador:

Arts. 138, 246, 267.

Art. 104.- Las cooperativas de Ahorro y Crédito gozarán, además beneficios especiales:

Ley de la economía popular y solidaria primera parte de las formas de organización de la economía popular y solidaria título primero normas generales capítulo primero marco conceptual y clasificación economía popular y solidaria.

Art.- Art.- 2.- Son formas de organización económica sujetas a la presente ley las siguientes:

a) Las organizaciones cooperativas de todas las clases y actividades económicas, que constituyen el sector cooperativista.

b) Los organismos de integración que agrupan las formas de organización económica detalladas en el presente artículo.

c) Las fundaciones y corporaciones civiles que tengan como objeto social principal, la promoción, asesoramiento, capacitación, asistencia técnica o financiera de las organizaciones económicas populares y de los sectores comunitario, asociativo y cooperativista.

Las cooperativas de ahorro y crédito, los bancos comunales, las cajas de ahorro, las cajas solidarias y otras entidades asociativas formadas para la captación de ahorros, la concesión de préstamos y la prestación de otros servicios financieros en común, constituyen el Sector Financiero Popular y Solidario, el mismo que se regulará por lo dispuesto en la Segunda Parte de la presente ley.

Se excluyen de la economía popular y solidaria, las formas asociativas gremiales, profesionales, laborales, culturales, deportivas, religiosas, entre otras, cuyo objeto social principal, no sea la realización de actividades económicas de producción de bienes y servicios o no cumplan con los valores, principios y características que sustentan la economía popular y solidaria.

Del sector financiero popular y solidario título primero cooperativas de ahorro crédito.

DEFINICIÓN Art.- 85.- Son cooperativas de ahorro y crédito las formadas por personas naturales o jurídicas con el vínculo común determinado en su estatuto, que tienen como objeto la realización de las operaciones financieras, debidamente autorizadas por la Superintendencia, exclusivamente con sus socios.

NORMAS APLICABLES Art.- 86.- Las cooperativas de ahorro y crédito se regularán por lo previsto en el título V de la presente ley, por las normas del presente título y las del Reglamento Especial que será dictado por el Ejecutivo, y que contendrá las normas operacionales, administrativas y otros aspectos propiosde su particular naturaleza funcional y operativa [34].

b) Reglamento general a la ley de cooperativas

Art. 66.- Cooperativas de ahorro y crédito son las que reciben ahorros y depósitos, hacen descuentos y préstamos a sus socios y verifican pagos y cobros por cuenta de ellas [34].

c) Personería jurídica

Acuerdo ministerial 2450 emitido por el CODENPE (Actualmente conocida como CONSEJO DE PUEBLOS Y NACIONALIDADES POSESIONÓ A SUS NUEVAS AUTORIDADES) [34]

d) Características de operación y funcionamiento

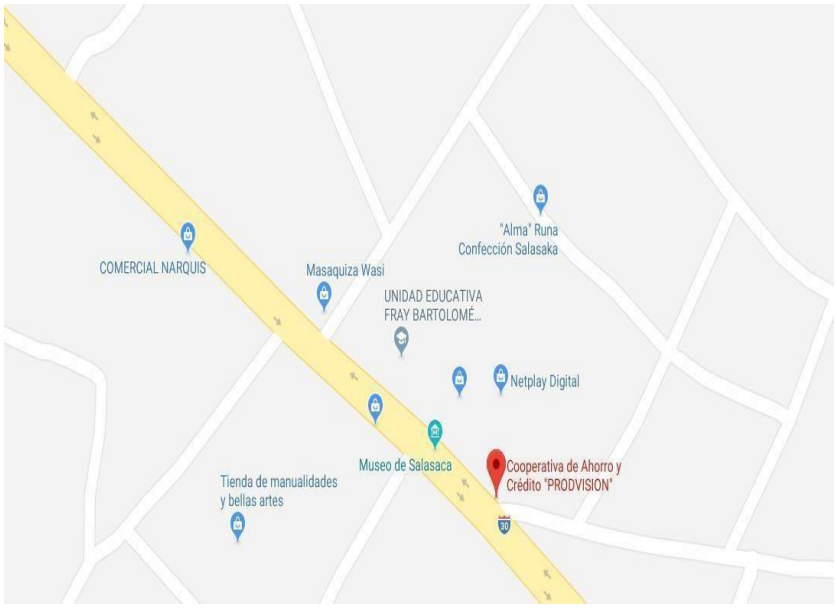
La cooperativa de ahorro y crédito PRODVISION es una sociedad se encuentra registra en la superintendencia de economía popular y solidaria (SEPS) desde el 11 de septiembre del 2013 con el número de oficio N° SEPS- ROEPS-2013-002581 Su estatuto prevé el funcionamiento de la junta general de representantes, el directorio está conformado por los presidentes, gerente general y sus organismos administrativos basándose en el

estatuto de la cooperativa cumpliendo sus atribuciones y funciones de cada una de los administradores [33]

e) Infraestructura

Actualmente la "Cooperativa de Ahorro y Crédito "PRODVISION". Ltda. "se encuentra funcionado un edificio propio de 2 pisos donde se tiene distribuido cada uno de los departamentos.

Figura 14. Localización de la Entidad y zona de influencia



Fuente: Google Maps

Figura 15. Estructura de la entidad financiera

3.1.7.5 Procesos Operativos de la Entidad

a) Proceso de Crédito

Garantizar el desembolso de créditos, revisando respectivamente los documentos de cada cliente que solicite el crédito.

Responsables

Consejo Directivo

Jefe de Crédito

Asesor de Créditos [33]

b) Políticas

La información debe ser verídica, si un aspecto se determina falsedad se niega el crédito solicitado.

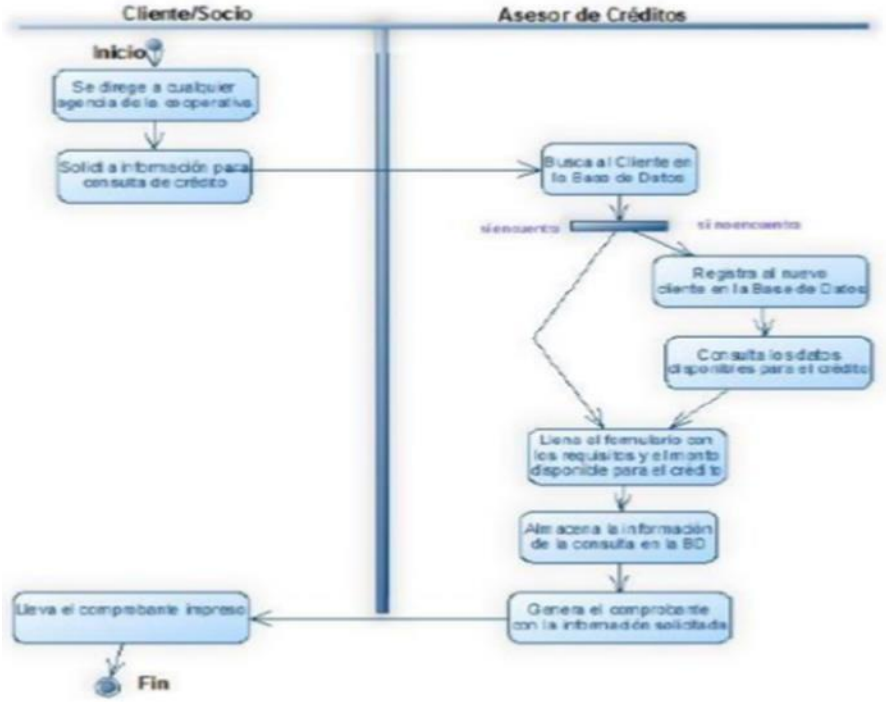
Desembolso en créditos desde $ 100 hasta $ 5000 y más entre los días lunes a viernes, sábados el desembolso es de $ 100 a $ 500.

Para realizar el desembolso a los clientes deben tener los respectivos documentos: cedula de identidad y la libreta correspondiente.

El pago del crédito desembolsado debe regirse a la tabla de Amortización caso contrario se cobra mora de 2.5 % del monto.

Si el pago del crédito sobrepasa de 30 de mora se retiene un objeto mueble o inmueble con el fin de cubrir el monto e interese del crédito desembolsado [33]

Figura 16. Proceso

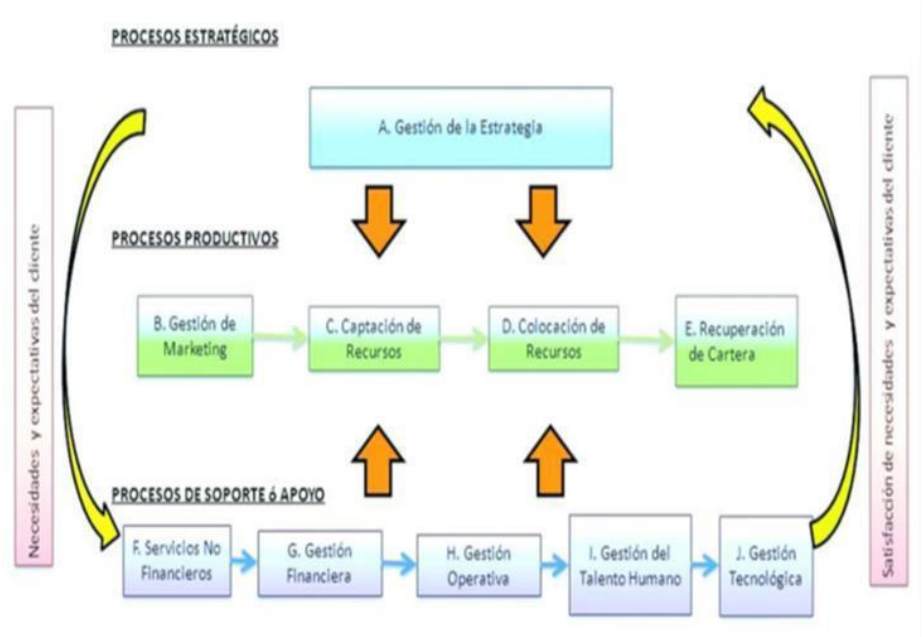


c) Modelo Operativo

Evaluación la Situación Actual de las áreas funcionales de la organización.

Las principales áreas funcionales se detallan en los procesos de la empresa definidos en un mapa de procesos establecido por la cooperativa.

Figura 17. Procesos y actividades



d) Procesos estratégicos

Satisfacen las necesidades financieras y sociales de las micro finanzas de sus socios internos y externos, en forma oportuna, en procura de elevar su calidad de vida.

a) Gestión estratégica

Analiza oportunamente las necesidades financieras de ahorro y crédito del socio.

b) Procesos productivos

Determinan el rendimiento de los trabajadores, en la consecución de una meta o en la ejecución de una tarea o transacción asignada en una unidad de tiempo.

c) Gestión de marketing

Concentración en ventas, precios, participación en el mercado, organización de ventas, calidad del servicio, comunicación integrada, investigación de mercados, análisis de beneficios y costes.

d) Capacitación de recursos

Capacitación a sus socios, empleados y directivos acorde a las necesidades de contexto.

Buena atención al socio en todas las oficinas de la COAC con servicios de calidad y calidez.

e) Recuperación de cartera

El área de cartera de crédito es sumamente sensible dado que la recuperación de los créditos depende de una eficiente gestión.

f) Procesos de soporte o apoyo

El soporte a los procesos de la cooperativa está definido por las funciones del Jefe de Sistemas, además interviene en la mayoría de ellos, como se pudo evidenciar en las responsabilidades de los trabajadores dándole una gran importancia al departamento de sistemas en esta organización; así mismo se consideran los servicios que la entidad recibe externamente.

g) Servicio no financiero

Funciones de preparación, soporte técnico e indicación, para fortificar los métodos beneficiosos.

h) Gestión Financiera

Las personas que ejercen en todas las tareas de responsabilidad de la cooperativa deben interactuar con el personal y los procedimientos financieros para efectuar sus actividades.

i) Gestión Operativa

El área de Gestión Operativa de la cooperativa de ahorro y crédito Prodvisión está comprendida por las secciones de cajas y Balcón de servicios que son las áreas responsables de gestionar operativamente las diferentes actividades con el propósito de garantizar un adecuado servicio a los socios y clientes

j) Gestión del Talento Humano

Coordina y controla el proceso de egreso para la desincorporación del personal, ya sea por despido, retiro voluntario o culminación de contrato.

Realiza una evaluación de las capacitaciones impartidas al personal.

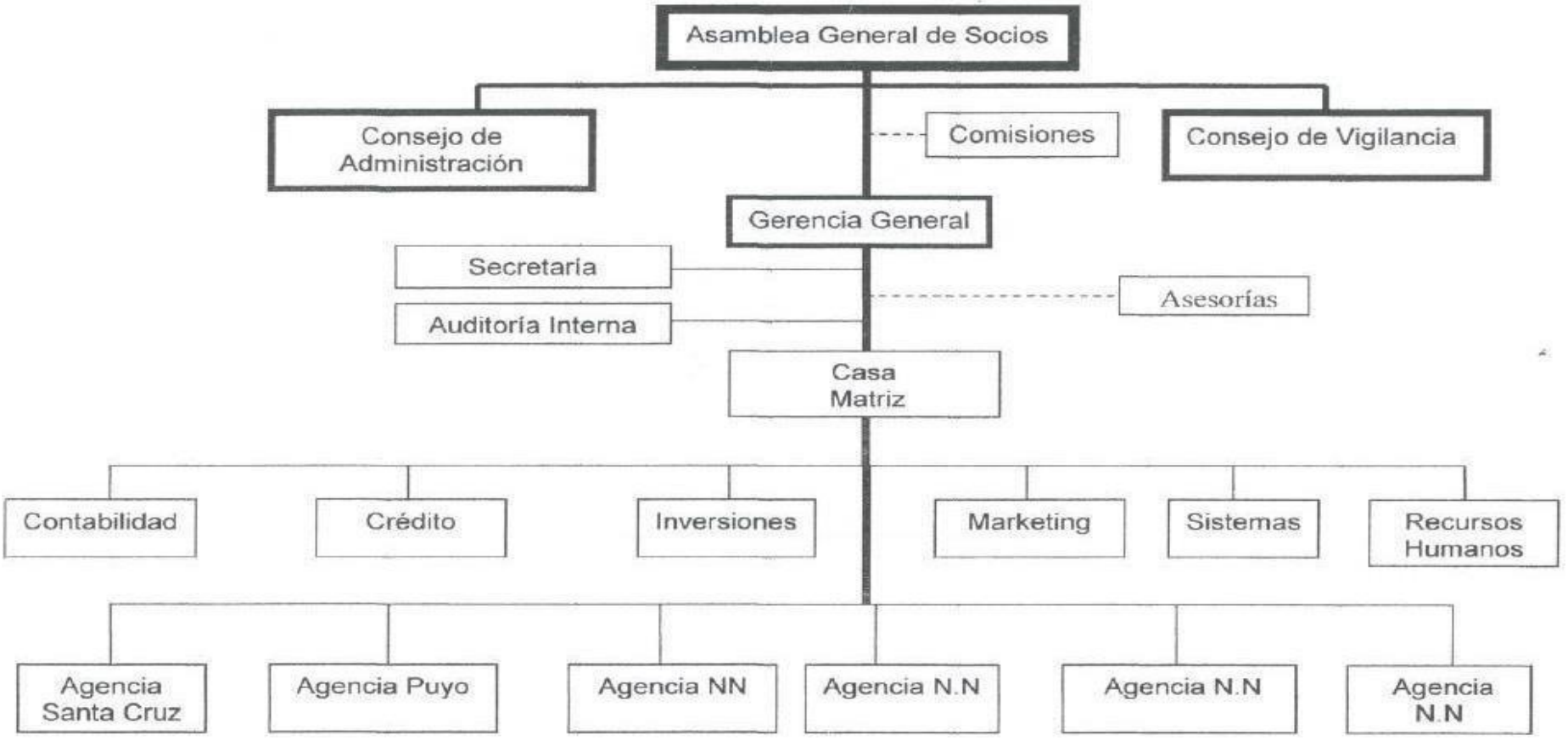
Lleva un registro de asistencia de las capacitaciones recibidas por el personal.

Lleva un control del personal donde cumplan con las normas y procedimientos de seguridad y salud en el trabajo

k) Gestión Tecnológica

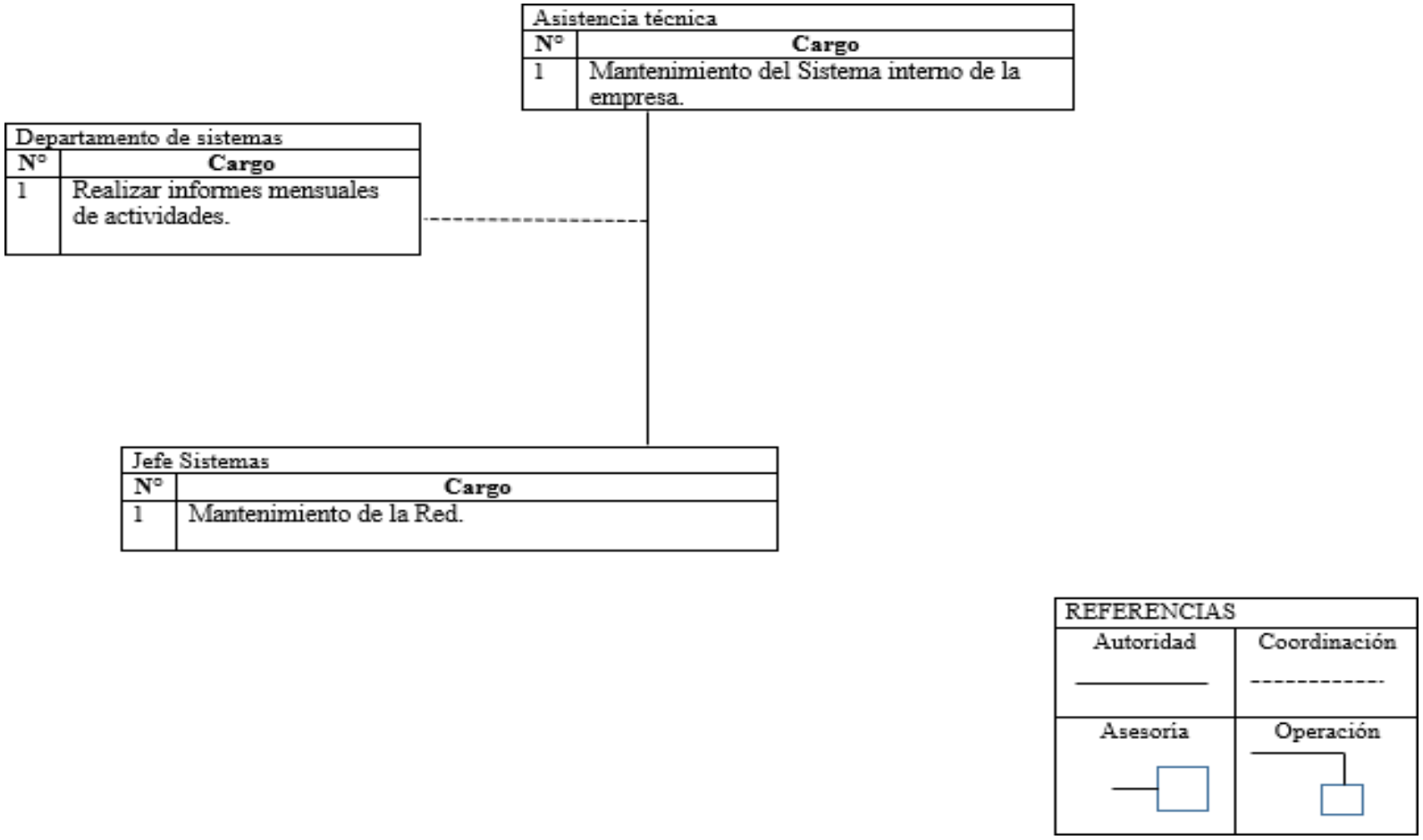
Está conformado por los trabajadores del área tecnológica y reduce el tiempo, los riesgos y costos en los procesos administrativos y operativos, para proteger los recursos de los socios [33].

Figura 18. Estructura Organizacional de la cooperativa de Ahorro y crédito Provisión



Fuente: Cooperativa de Ahorro y Crédito Prodvisión

3.1.7.6 Organigrama Funcional de la Unidad Informática



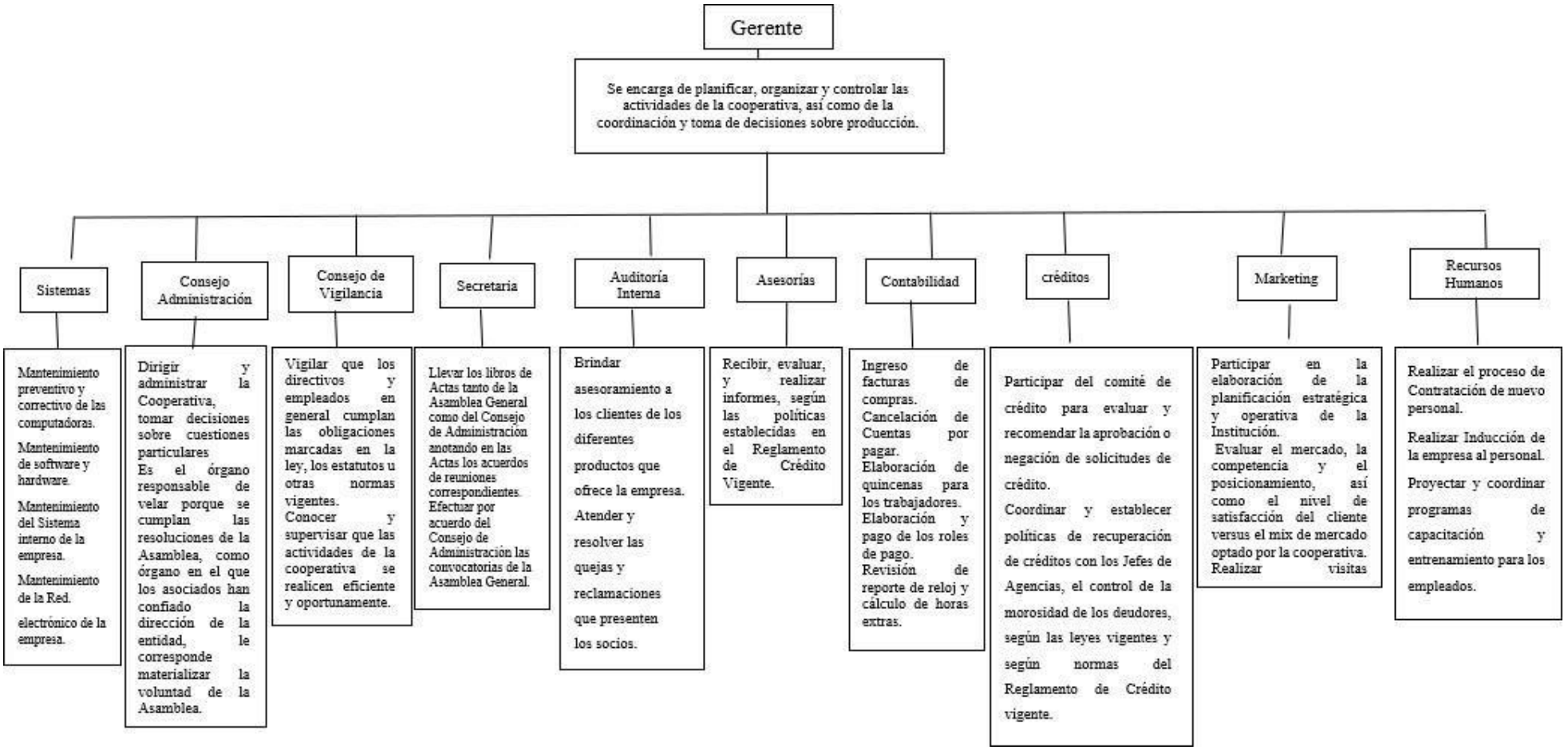
Fuente: Cooperativa de ahorro y crédito Prodvisión

3.1.7.7 Estructura Organizacional del Área Informática.

Figura 19. Organigrama Estructural vigente de la Unidad Informática.

Fuente: Cooperativa de ahorro y crédito Prodvisión

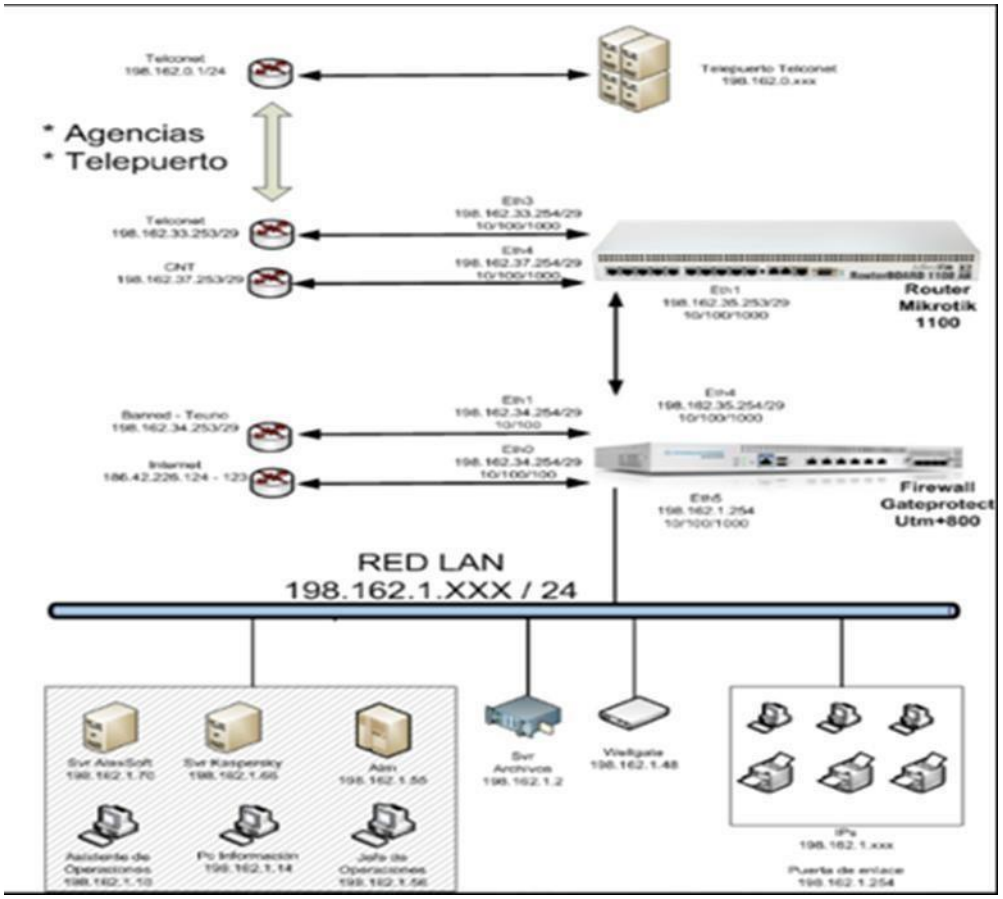
Figura 20. Organigrama funcional de la cooperativa de Ahorro y Crédito Prodvisión



Investigador de la información obtenida de la tabla 24, tabla 25, tabla 26, tabla 27, tabla 28, tabla 29, tabla 30, tabla 31, tabla 32

3.1.7.8 Estructura de Red

Figura 21. Estructura de la red de la cooperativa de Ahorro y Crédito Prodvisión



Se identifica todas las salas donde se encuentra el equipamiento de cómputos y se clasificó en "principales" y "secundarias", entendiéndose por principales aquellas donde se ubican los dispositivos más importantes para la red

La Tabla 39 y la Tabla 40 describen los aspectos típicos a implementar para el control físico de la red en el cubículo principal y cubículos secundarias.

Para obtener una visión general de la ubicación de todos los dispositivos de red, nos contactamos con el personal encargado del mantenimiento, cuidado y control tanto de los dispositivos físicos y lógicos de red. Posteriormente visitamos cadauna de estas salas para evaluar, los controles sobre la seguridad física, las condiciones ambientales y controles sobre las copias de seguridad e inventarios. Para esto nos entrevistamos con el personal de cada una de estas salas.

Tabla 39. Cubículos Secundarios

Para los cubículos Secundarios
▪ Escritura de estándares para la administración de seguridad de los recursos de la red. ▪ Bloqueo de salas permitiendo solo el ingreso a personas autorizadas. ▪ Monitoreo y registro de los accesos a las salas. ▪ Detección de fuego, humo y agua. ▪ Extintores de fuego adecuados y habilitados.

Tabla 40. Cubículos Principal

Para el cubículo Principal (Además de los aspectos necesarios para las salas secundarias)
▪ Escritura de políticas y procedimientos para la elaboración y recuperación de copias de seguridad. ▪ Ubicación de las salas en el interior del edificio y en lo posible sin ventanas ni puertas al exterior o patios internos. ▪ Dispositivos alejados del piso. ▪ UPSs para asegurar la continuidad de las operaciones. ▪ Copias de seguridad ubicadas fuera de la sala y adecuadamente Protegidas

3.1.7.9 Hallazgos

Actualmente no existen políticas ni procedimientos escritos para la gestión de la seguridad física de la red. Sino que, es el encargado de cada sala quien lleva adelante estas tareas a criterio propio y por lo tanto de manera heterogénea.

Tabla 41. Hallazgos

HALLAZGO	DESCRIPCIÓN	RECOMENDACIONES
No existen políticas ni procedimientos para Mantenimiento.	Debido a la ausencia de estos, el mantenimiento, lo realiza el encargado de turno basándose en su experiencia. Además, tampoco se cuenta con procedimientos para el monitoreo de las conexiones de la red por lo que es difícil determinar el estado de los equipos.	Realizar los documentos respectivos que tenga las políticas para el mantenimiento y los procedimientos a seguir para realizar un buen trabajo. Son muy importantes estos documentos porque son la guía para seguir un buen proceso en el mantenimiento de la red de la cooperativa.
No existen políticas ni procedimientos para inventarios.	Por lo que no se conoce la disponibilidad de equipos, su ubicación, estado ni procedencia.	Realizar los documentos de las políticas y procedimientos de inventario para poder tener conocimiento de las máquinas,

		cableado, routers, etc. que tiene la cooperativa dentro de sus instalaciones.
No existen políticas ni procedimientos para registros de errores y soluciones.	No está disponible información referente a errores comunes y sus soluciones encontradas. Por lo que el encargado debe, a cada error, encontrarle una nueva solución, aunque se trate de problemas recurrentes. Tampoco es posible realizar un seguimiento de las fallas y sus causas, con el objeto de implementar medidas correctivas. Esto genera la necesidad de la presencia permanente del encargado. No se cuenta con una metodología para el diagnóstico de fallas.	Realizar el respectivo documento que contenga las políticas y los procedimientos para el registro de errores con sus respectivas soluciones, con lo cual se podrá corregir de inmediato cualquier error o problema que surja en las instalaciones de la cooperativa.
No existen políticas ni procedimientos para la asignación de responsabilidades.	No están claramente definidas las responsabilidades del personal, lo que ocasiona confusión acerca de las tareas que debe realizar cada persona.	Realizar los respectivos documentos que contenga las políticas y procedimientos para la asignación correcta de responsabilidades, con lo cual se pueda tener una organización más adecuada de cargos.

Tabla 42. Hallazgos referentes al cubículo principal y secundarias

HALLAZGO **Referentes al cubículo principal y secundarias. (No existe distinción entre estas.)**		**RECOMENDACIONES**
AMBIENTAL Ver referencia de figura 22, figura 23, figura 24, figura 25	▪ Cableado con deficientes terminaciones. ▪ Falta de organización del cableado. ▪ Extintor alejado. ▪ Partes del cable deteriorado. ▪ Espacio reducido entre máquina. ▪ Inseguridad en la instalación de los tomacorrientes. ▪ Cable en el piso. ▪ El cableado de la red se encuentra junto al de la red	● Reemplazar las terminaciones ● Utilizar la norma ANSI/EIA/TIA 569 ● Ubicar el extintor en un lugar intermedio ● Reemplazar los cables deteriorados. ● Ubicar estratégicamente los cubículos. ● Ubicar los tomacorrientes en

	eléctrica. ▪ No se restringe el acceso a persona no autorizadas a los dispositivos mayores ni menores (debido a que estos dispositivos coexisten en el mismo cubículo). ▪ No existen carteles que prohíban comer y/o fumar dentro de los cubículos.	lugares definidos. ● Almacenar el cableado faltante en bodega. ● El cableado de la red y el eléctrico deben ir en distintas vías o canaletas. ● Los dispositivos de comunicación deben encontrarse alejados de terceros. ● Crear y situar éstos carteles en áreas visibles

Figura 22. Conectores de computador desordenado

Figura 23. Cortapico conectado cerca de la máquina

Figura 24. Espacio reducido de escritorios

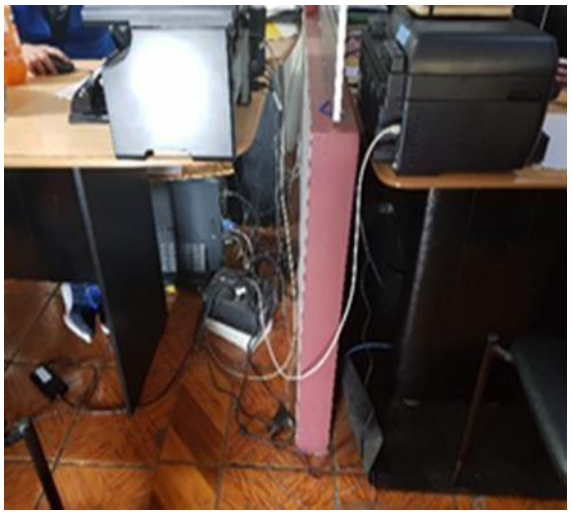
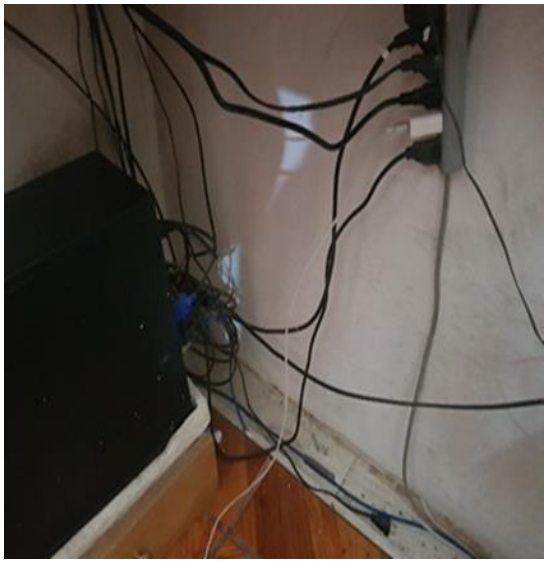


Figura 25. Cortapico alejado del computador área de sistemas



3.1.7.10 ANÁLISIS

Los hallazgos identificados, se han agrupado en categorías. Para permitir una visión más global de los problemas. Esto se refleja en las siguientes tablas:

Tabla 43. Porcentaje de Hallazgos Ambientales

Hallazgos Ambientales	Porcentaje
Cableado con deficientes terminaciones	40,00%
Falta de organización del cableado	50,00%
Extintor alejado	30,00%
Partes del cable deteriorado	40,00%
Espacio reducido entre máquina	30,00%
Inseguridad en la instalación de los tomacorrientes	10,00%
Cable en el piso	10,00%
El cableado de la red se encuentra junto al de la red eléctrica	90,00%
No se restringe el acceso a persona no autorizadas a los dispositivos mayores, ni menores (debido a que estos dispositivos coexisten en el mismo cubículo)	80,00%
No existen carteles que prohíban comer y/o fumar dentro de los cubículos	40,00%

Figura 26. Hallazgos Ambientales

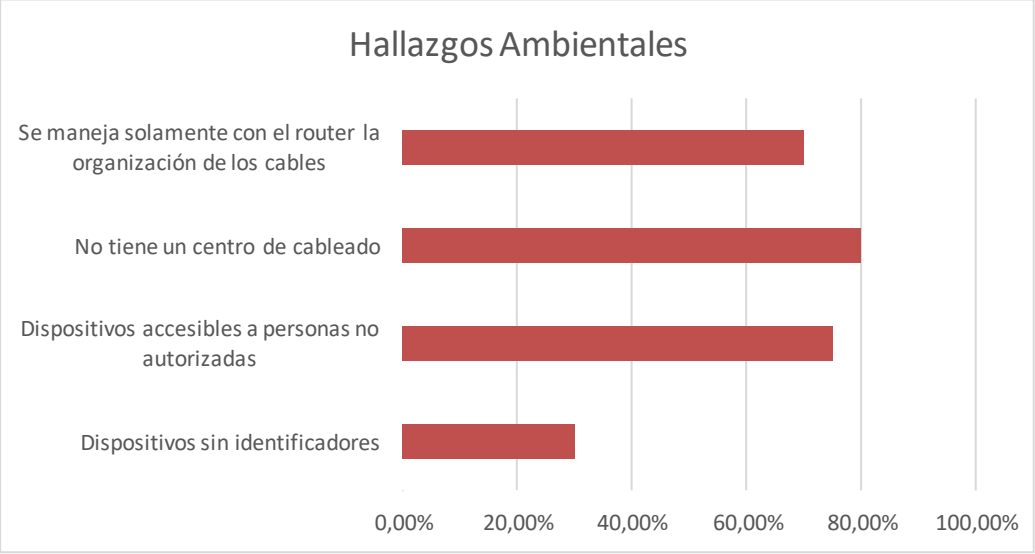


Tabla 44. Porcentaje de Hallazgos en el Cableado de la red Horizontal

Hallazgos de Cableado	Porcentaje
Conectores de pared no se encuentran fijos	60,00%
Conectores sin capuchones	20,00%
Conectores al descubierto	50,00%
Conectores en el piso	30,00%
Conectores de PC sin atornillar	20,00%
Cableado sin identificadores	20,00%
Cableado suelto	60,00%
Cableado sin protección	60,00%
Ausencia de abrazaderas de plástico	20,00%

Figura 27. Hallazgos en el cableado

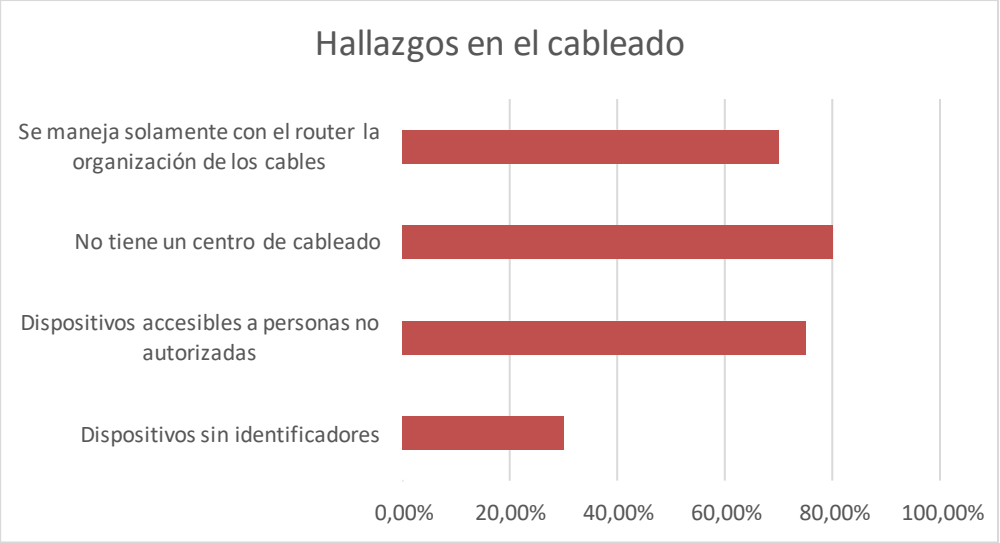
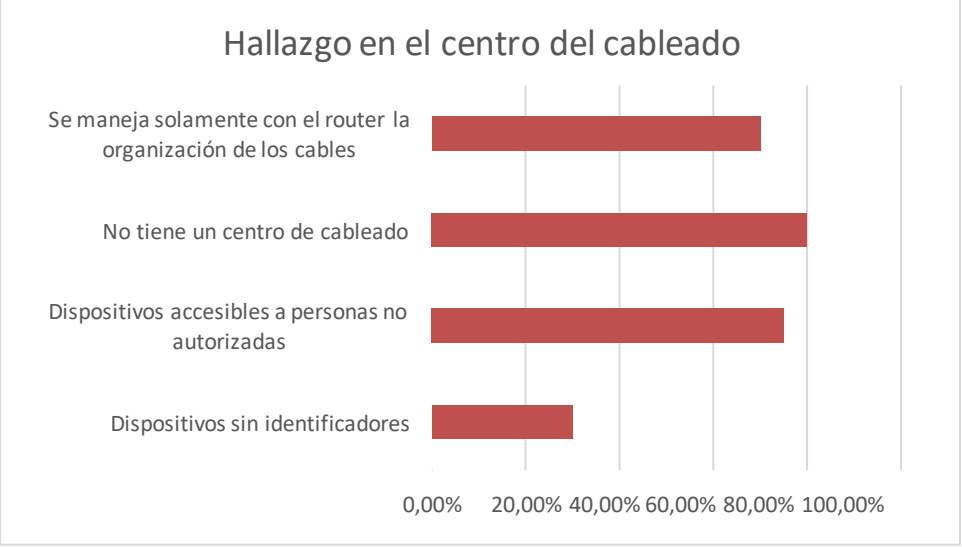


Tabla 45. Porcentaje de Hallazgos en el centro del cableado

Hallazgo en el centro de Cableado	Porcentaje
Dispositivos sin identificadores	30,00%
Dispositivos accesibles a personas no autorizadas	75,00%
No tiene un centro de cableado	80,00%
Se maneja solamente con el router la organización de los cables	70,00%

Figura 28. Hallazgos en el centro de cableado



Las imágenes que corresponde a nuestro respectivo auditoria de la cooperativa se encuentran en los anexos que adjuntamos en este archivo.

3.1.7.11 Análisis con Nmap y Wireshark e Ip-Tools

a) Nmap

Con el respectivo análisis de Nmap se pudo obtener la siguiente información como se muestra en la figura 29, figura 30, figura 31, figura 32.

Se puede observar que únicamente tiene tres puertos abiertos (80, 443 y 49152) en el servidor y en las máquinas de la empresa tienen abiertos los mismos puertos.

Figura 29. Análisis de puertos

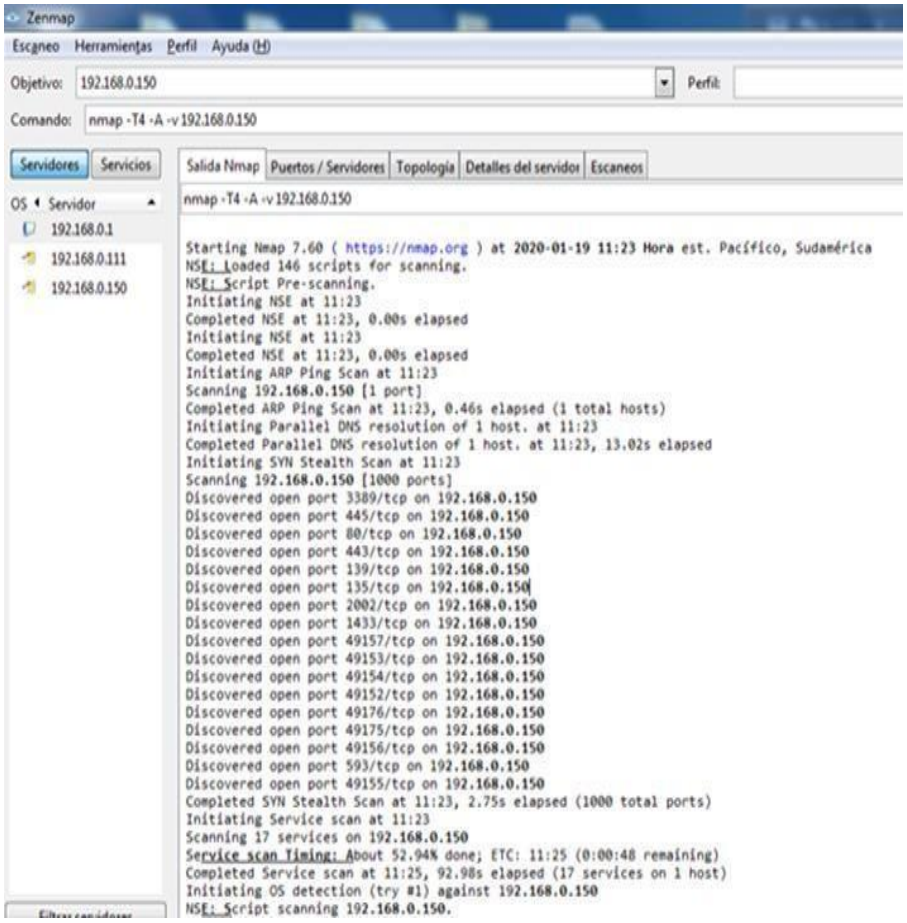


Figura 30. Salida Nmap

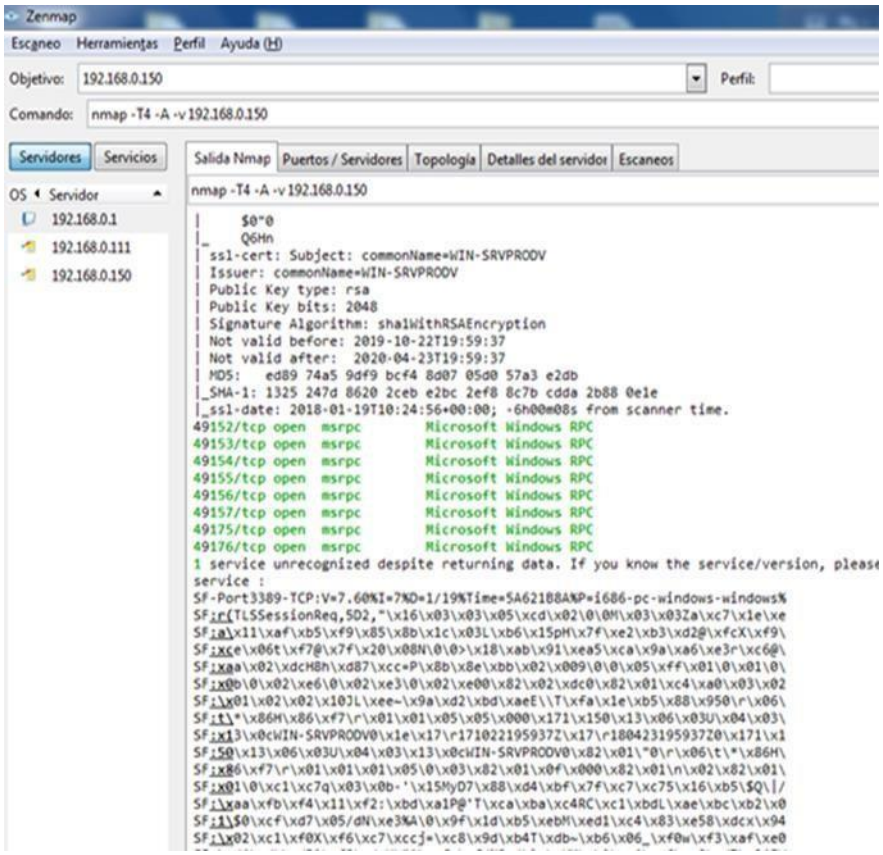


Figura 31. Puertos / Servidores

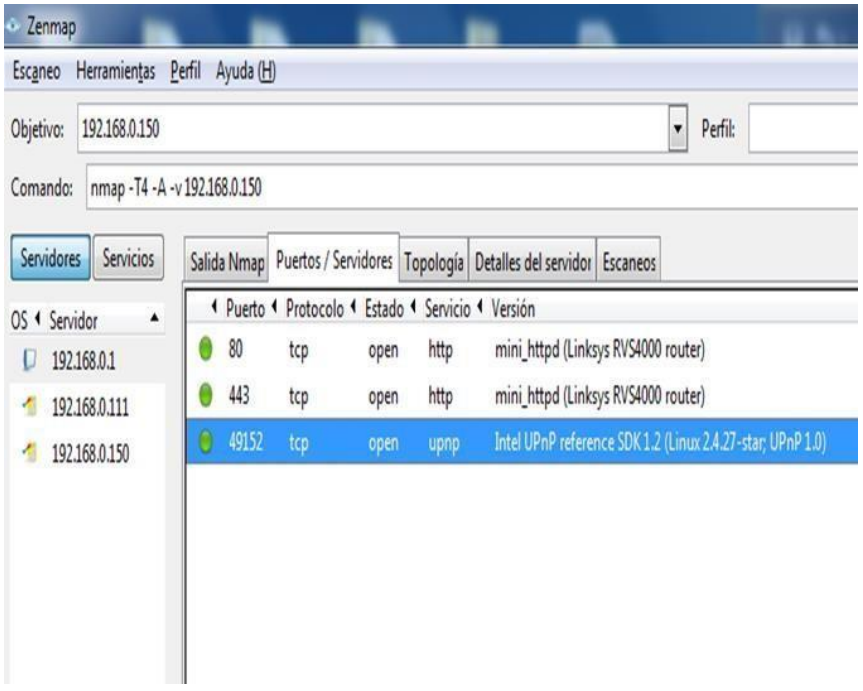
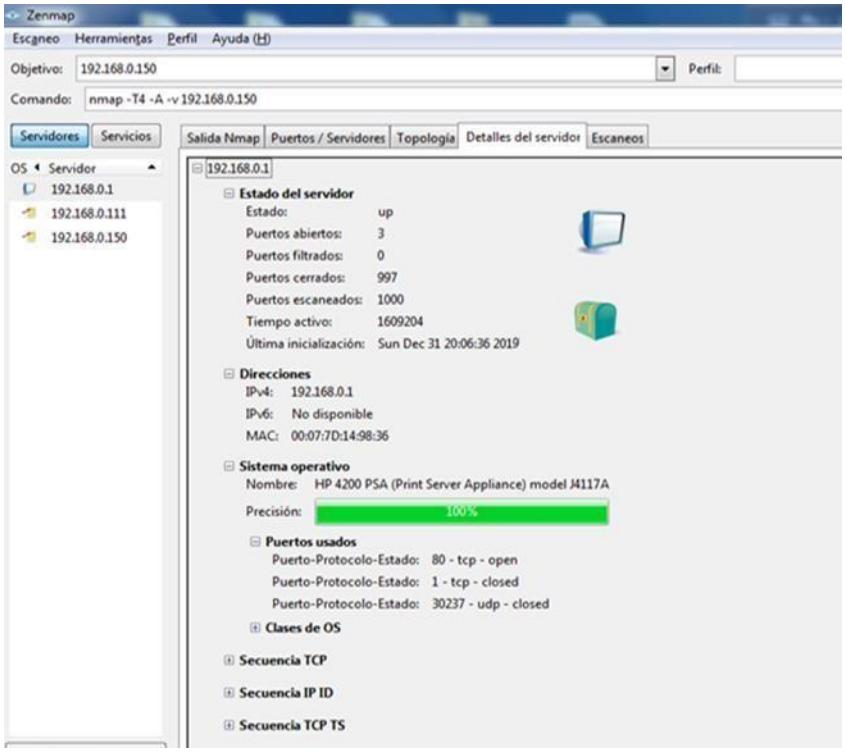


Figura 32. Detalles del servidor



b) Wireshark

"Tener la información detallada que nos facilita este programa nos permite poder analizar el tráfico que pasa por nuestra red y así poder solucionar o incluso prevenir los posibles problemas que puedan surgir. Por ejemplo, imaginamos que está muy lenta la conexión a Internet y no sabes porque, con este sniffer puedes observar si en el equipo se está generando tráfico no deseado (ejemplo. está infectado por un troyano)" [35].

"Una vez iniciada la captura es posible filtrar los paquetes capturados de acuerdo con la necesidad de analizar si hay algún malware en la máquina. Es posible reconocer a qué servidores se conectó a través de las peticiones DNS. Para observar con más comodidad es posible aplicar un filtro. Específicamente, si se escribe DNS en el campo de los filtros y se lo aplica, serán visibles todas las resoluciones de nombres en direcciones IP. En el caso del malware, permite reconocer con que servidores se conecta" A continuación, puede observarse una captura del respectivo análisis y se puede verificar que no hay malware alguno en la red [36].

Figura 33. Análisis de red

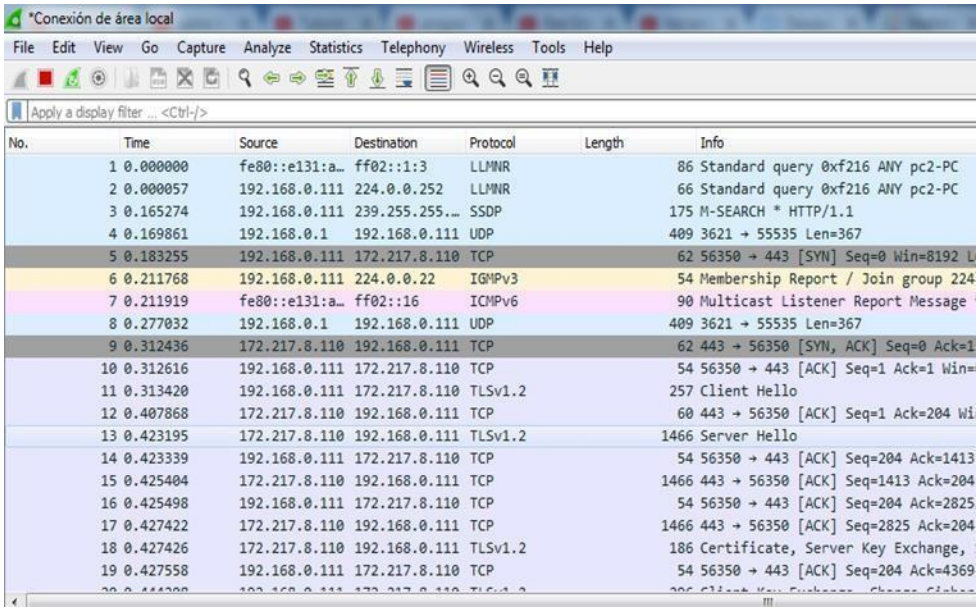
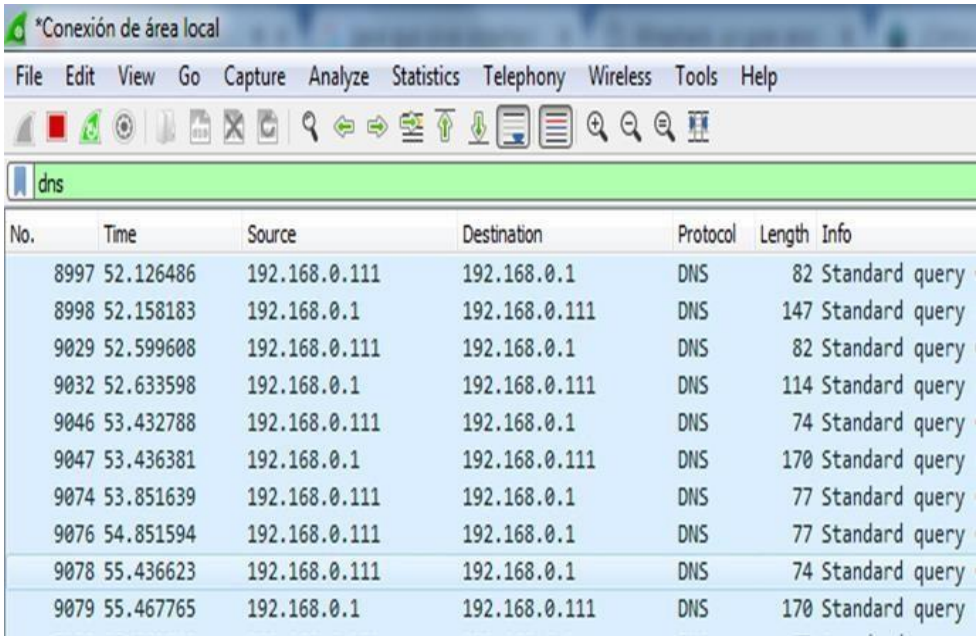
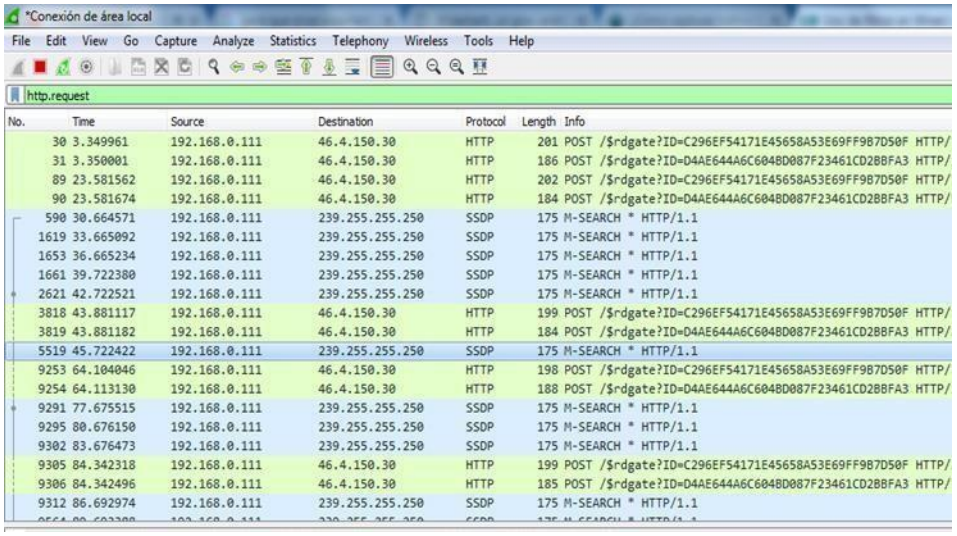


Figura 34. Análisis de DNS



Un aspecto a tener en cuenta son las peticiones realizadas. “Aplicando el filtro “http.request” es posible obtener todos los GET y POST que fueron realizados durante el periodo de captura. Este tipo de peticiones es muy utilizado por los códigos maliciosos, incluso para enviar información sobre el sistema infectado. A continuación, se puede observarse en la figura 35, que no hay malware que obtiene datos y archivos desde un servidor remoto:” [36].

Figura 35. Análisis de Malware



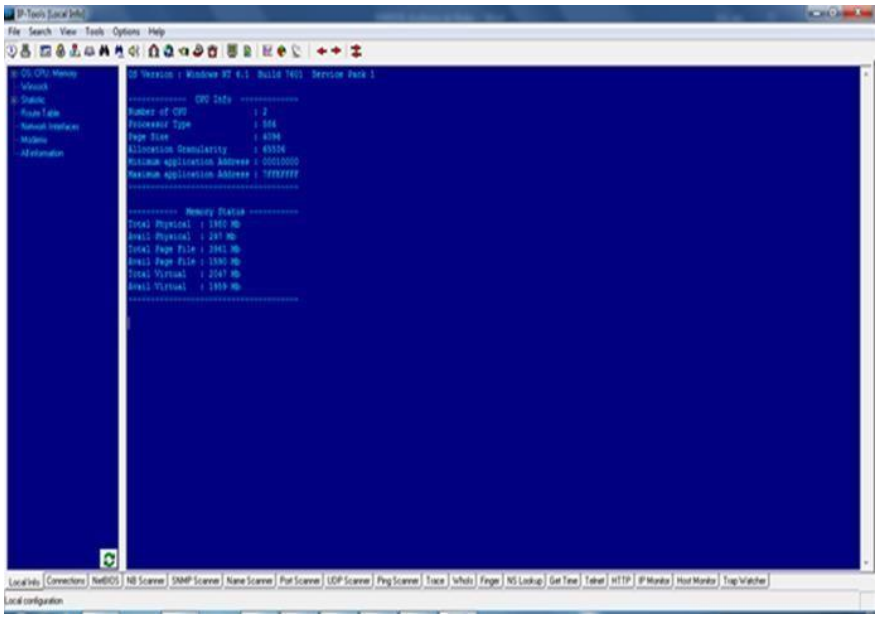
3.1.7.12 Ip-Tools

"IP-Tools ofrece muchas utilidades TCP / IP en un programa. Este galardonado programa puede funcionar en Windows 2000 / XP / Vista, Windows 7/8/10, Windows Server 2003/2008/2012 y es indispensable para cualquiera que use Internet o Intranet" [37].

a) Local Info

"Examina al host local y muestra información del procesador, memoria, datos del Winsock, etc" [37]

Figura 36. Información del procesador de la cooperativa



En la Figura 36 muestra información local de la computadora de la cooperativa.

b) Connection Monitor

Despliega información de las actuales conexiones de red TCP,UDP [37]

Figura 37. Información de la conexión de red

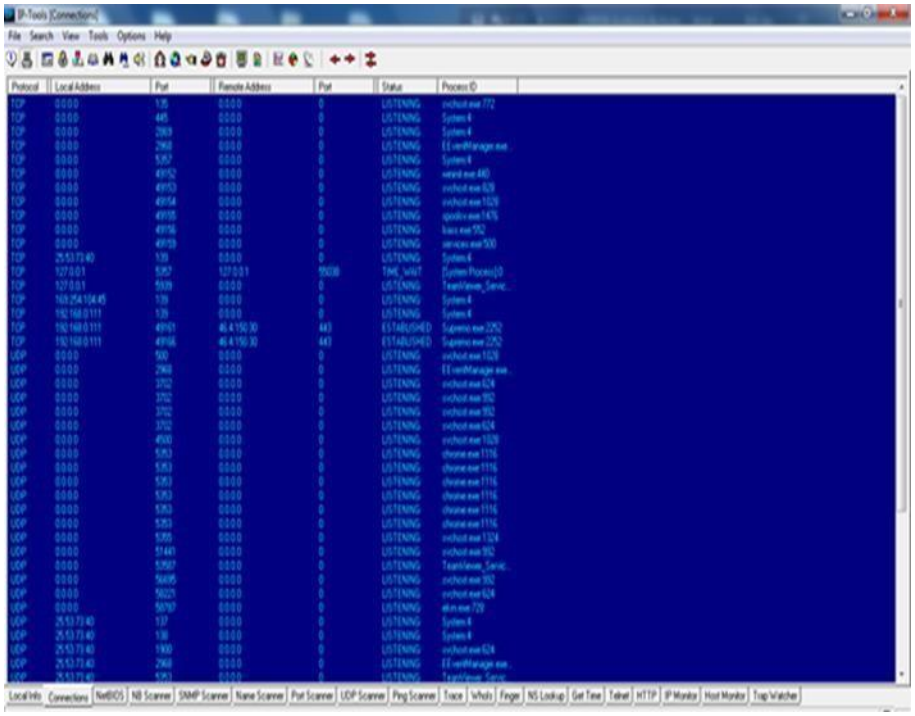
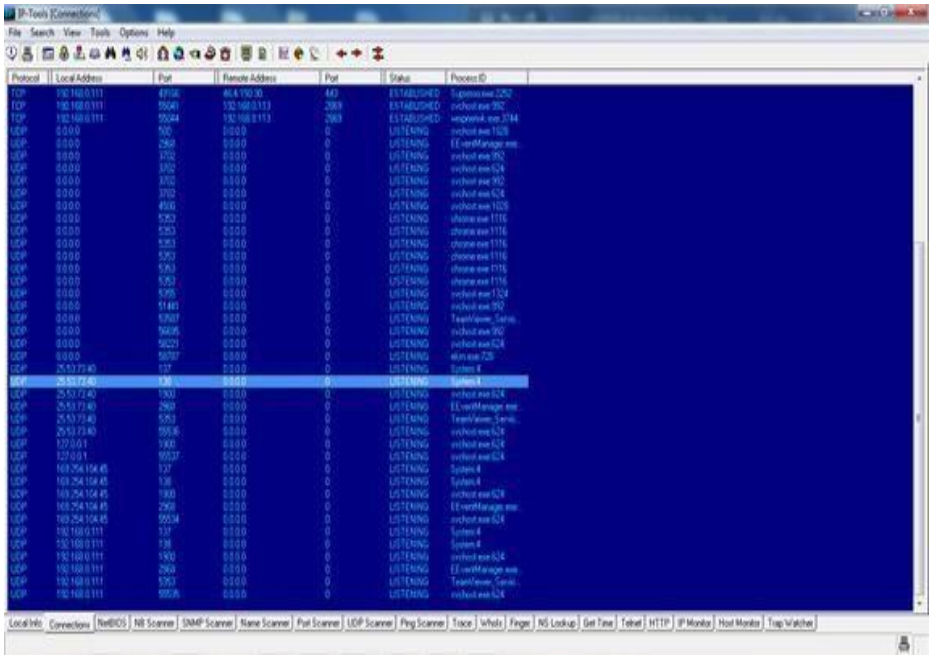


Figura 38. Local Address



c) SNMP Scanner

El Protocolo simple de administración de red es el protocolo estándar de Internet para intercambiar información de administración entre las aplicaciones de la consola de administración y las entidades administradas [37].

Escáner de red para dispositivos SNMP habilitados tal como se muestra en la figura 39 y 40.

Figura 39. Escaneo de la red

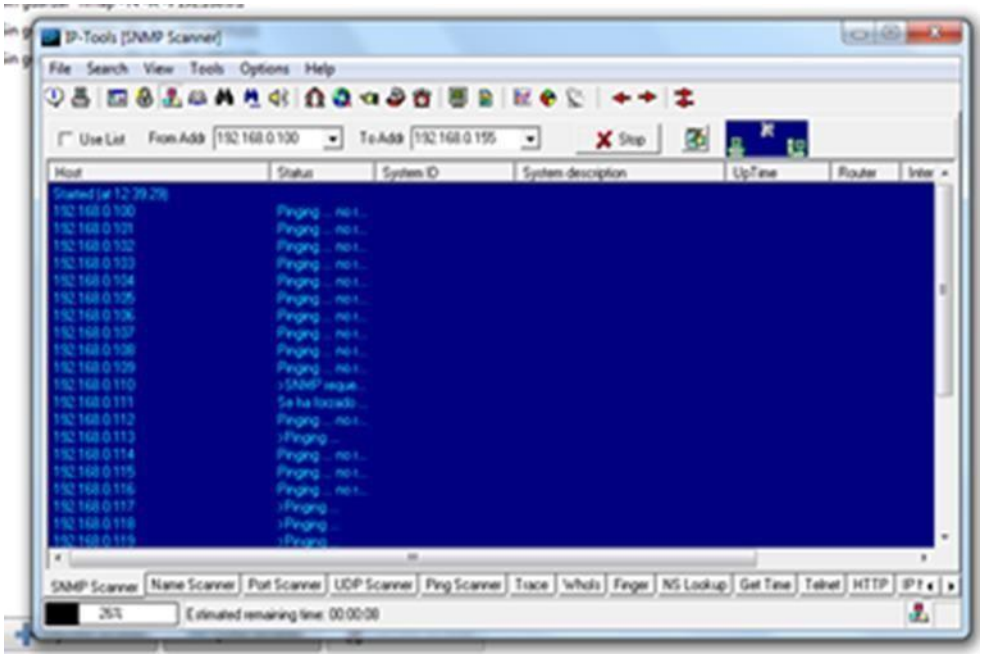
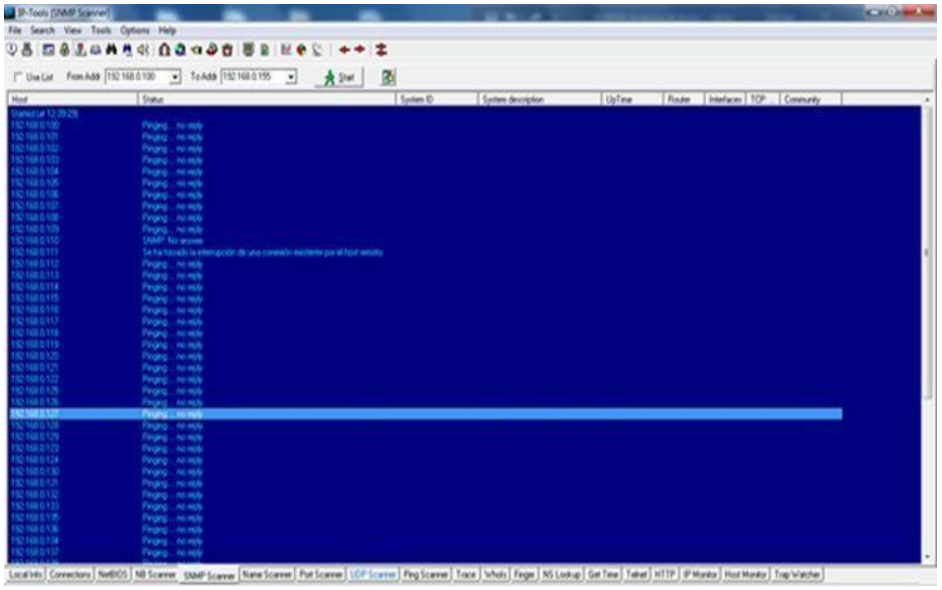


Figura 40. Escaneo de puertos



d) Name Server

Explora los nombres de los hosts bajo el rango de las direcciones IP [37].

Figura 41. Rango de las direcciones IP

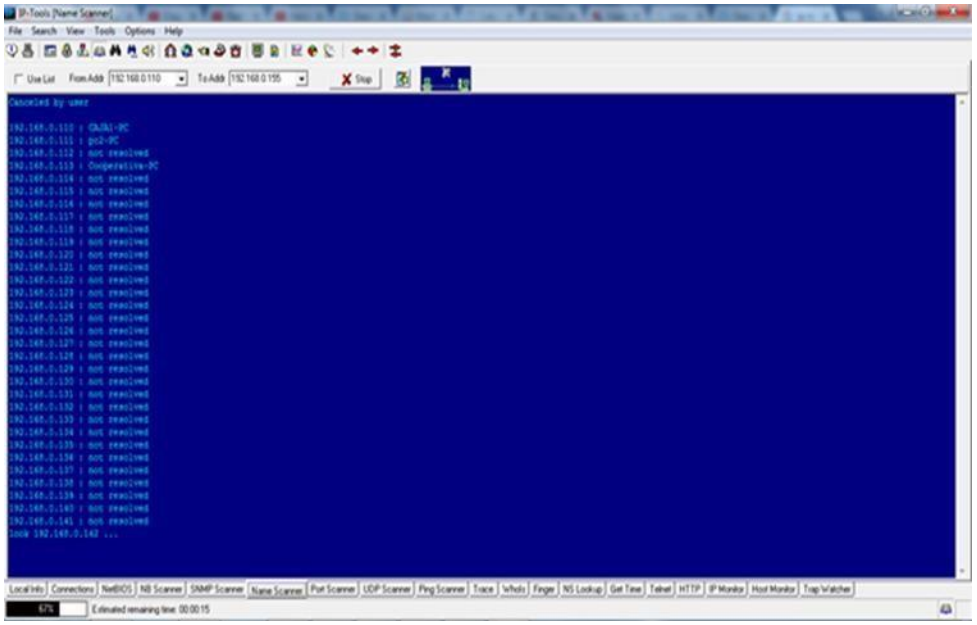
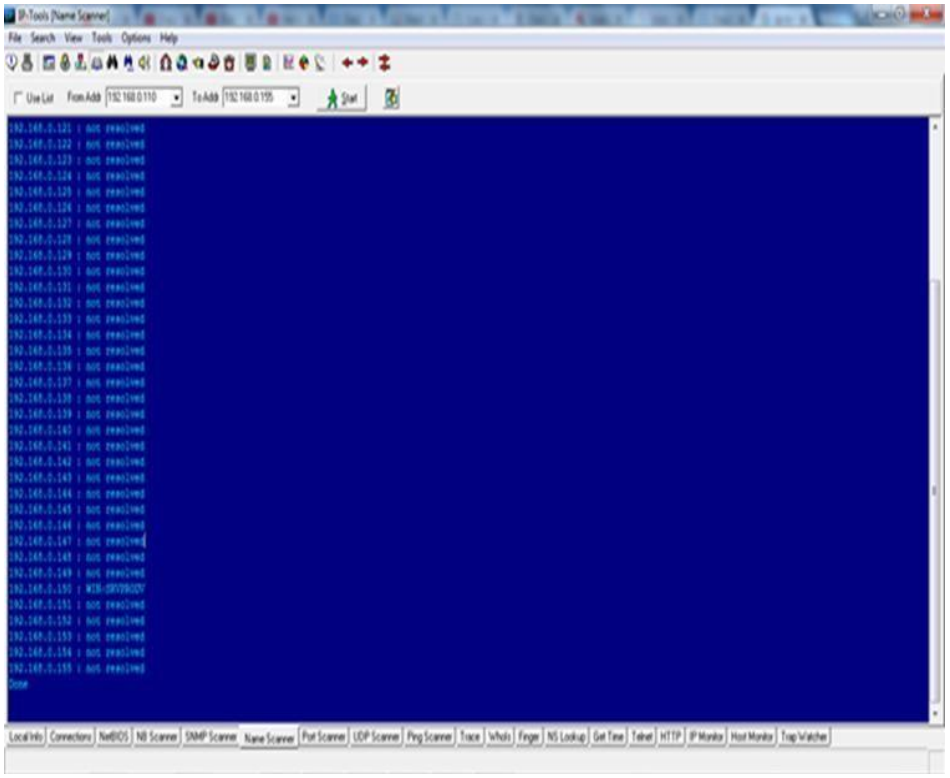


Figura 42. Rango de las direcciones IP terminada



e) UDP Scanner

La utilidad UDP Scanner brinda la capacidad de escanear servicios basados en UDP en un rango en un rango o listas de direcciones ip tal como muestra la Figura 43 y 44 [37].

Figura 43. Servicios activos

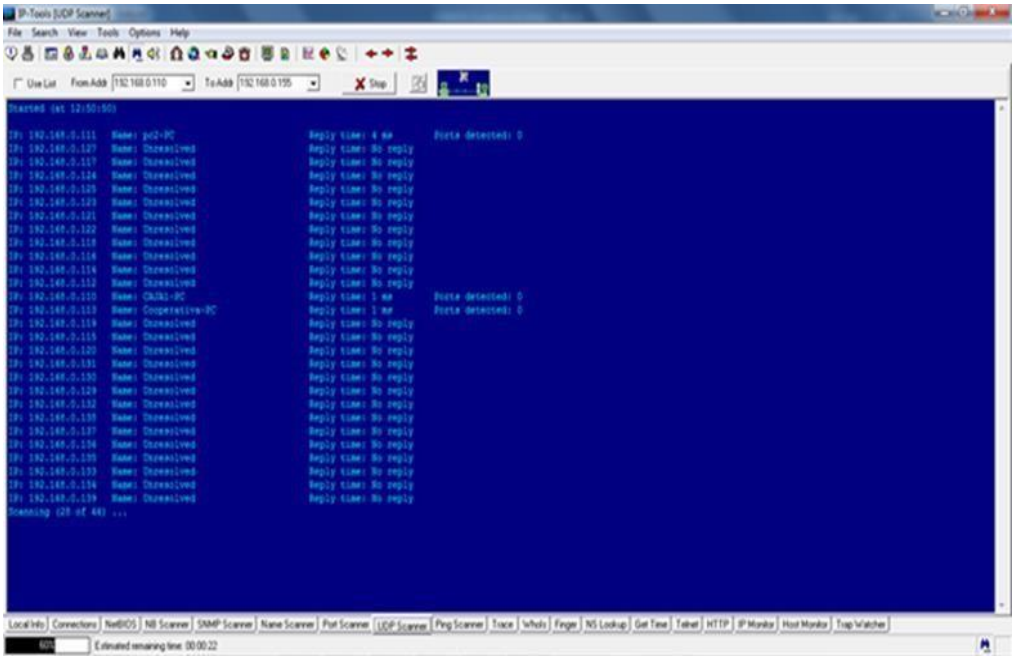
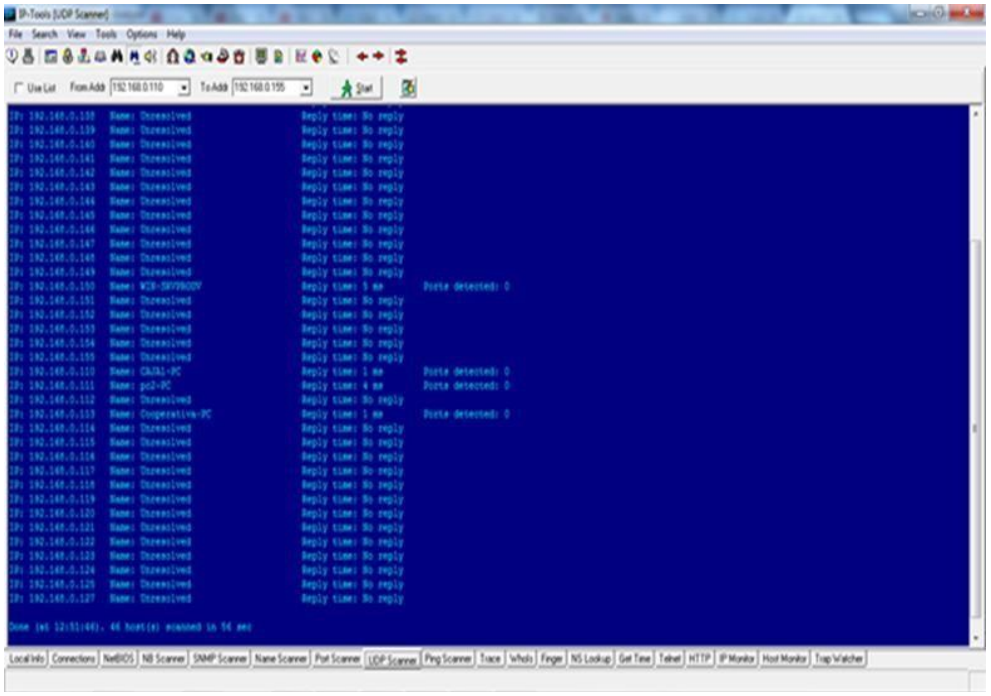


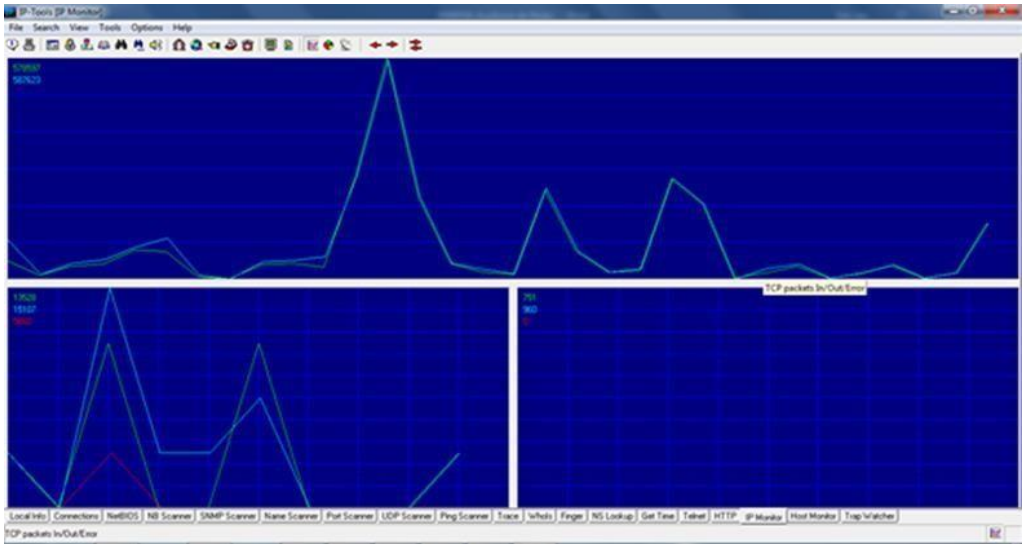
Figura 44. Escaneo de servicios activos



f) IP-Monitor

Muestra gráficas en tiempo real para TCP,UDP,ICMP In,Out,Error packets [38]

Figura 45. TCP packets In Out Error



g) NB Scanner

Permite ver todas las conexiones abiertas en la cooperativa en el que se está ejecutando. Para cada conexión, "IP-Tools muestra el protocolo, la dirección IP local, el puerto local, la dirección IP remota, el puerto remoto y su estatus" tal como muestra en la Figura 46 y Figura 47 [38].

Escáner de recursos compartidos.

Figura 46. Escaneo de recursos compartidos

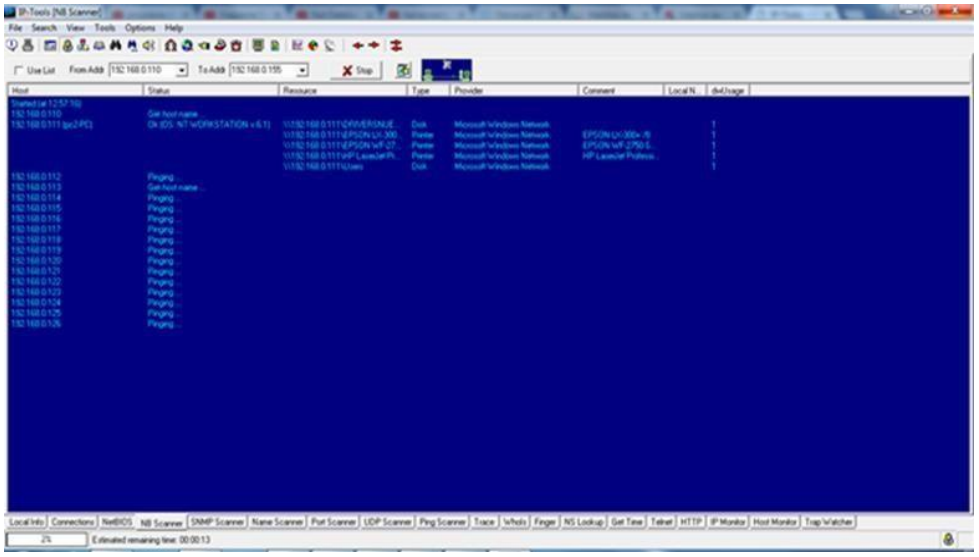
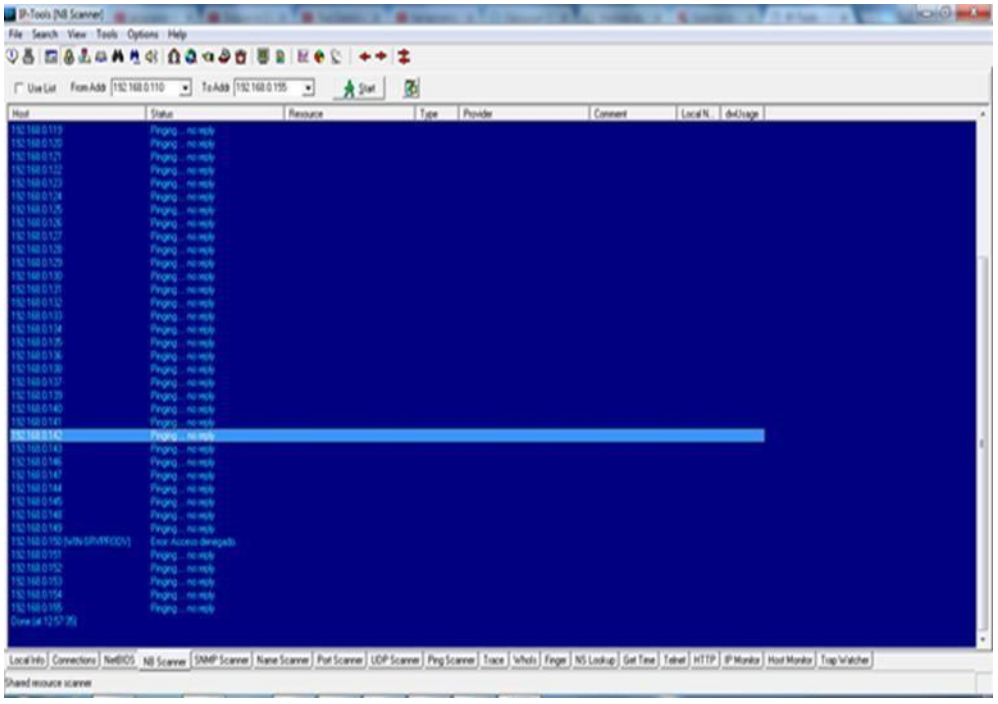


Figura 47. Escaneo de recursos compartidos finalizada



h) Probando las conexiones de red

Antes de ver cómo se realiza un test de velocidad es importante conocer algunos de los términos que comúnmente se utilizan en estas apps y servicios tal como se muestra en la figura 48. El usuario medio conoce lo que es la velocidad dedescarga y la velocidad de subida.

"Velocidad de descarga: La velocidad que tiene la conexión a internet para obtener datos de un servidor.

Es el tiempo que tarda un paquete de archivos en ser descargado desde un punto externo al dispositivo que se está utilizando. Se mide generalmente en megas por segundo. Es decir, en los megas que consigue descargar en un segundo.

Velocidad de subida: En este caso hablamos del tiempo que tarda un archivo en ser subido a un servidor externo. Al contrario que la velocidad de descarga, aquí se mide la cantidad de megas que la conexión a Internet puede subir en un segundo al servidor" [39].

Figura 48. Velocidad de internet cableada

i) Analizador de claves

Ahora se procederá a evaluar la robustez de las contraseñas en los dispositivos y equipos terminales de la infraestructura de la red.

Para esta evaluación se necesitará el sistema operativo Windows se usó WS-PIN Y QSS for Wireless. donde evalúa la solidez de una contraseña.

Esta aplicación proporciona un medio al usuario para mejorar la robustez de las contraseñas y mantener un buen hábito para no crear contraseñas incorrectas.

En este momento se procederá a escribir la contraseña para el modem, tal como se muestra en la figura 49 que la contraseña es muy débil y que fácilmente un hacker podrá acceder al equipo.

Figura 49. Analizador de claves

j) Verificación de Wireless de la cooperativa

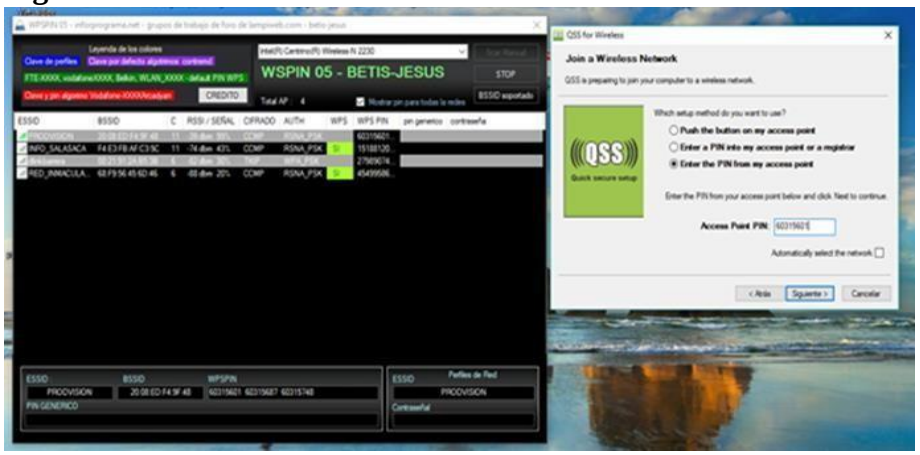
La seguridad de las redes inalámbricas ha evolucionado y mejorado mucho desde la implantación del cifrado WPA, y sobre todo, WPA2.

Configurando nuestra red para que utilice el cifrado WPA2 sabemos que nuestra red utiliza un método de cifrado seguro.

Para la evaluación del wireless se utilizó el software WPSPIN que se lo puede descargar desde esta dirección web; el mismo que sirve para detectar las redes que se encuentran disponibles y ver las características específicas de cada conexión [40]

Como se muestra en la figura 50, hay diferentes redes que se encuentran por la zona donde está instalado el router.

Figura 50. Vulnerabilidad de clave.



Como se puede ver la lista de redes habilitadas, e ingresamos a la Red de PRODVISION que sería la red de la cooperativa, verificamos si se puede ingresar a la red, tal como se muestra en la Figura 51 y Figura 52.

Figura 51. Listado de redes habilitadas

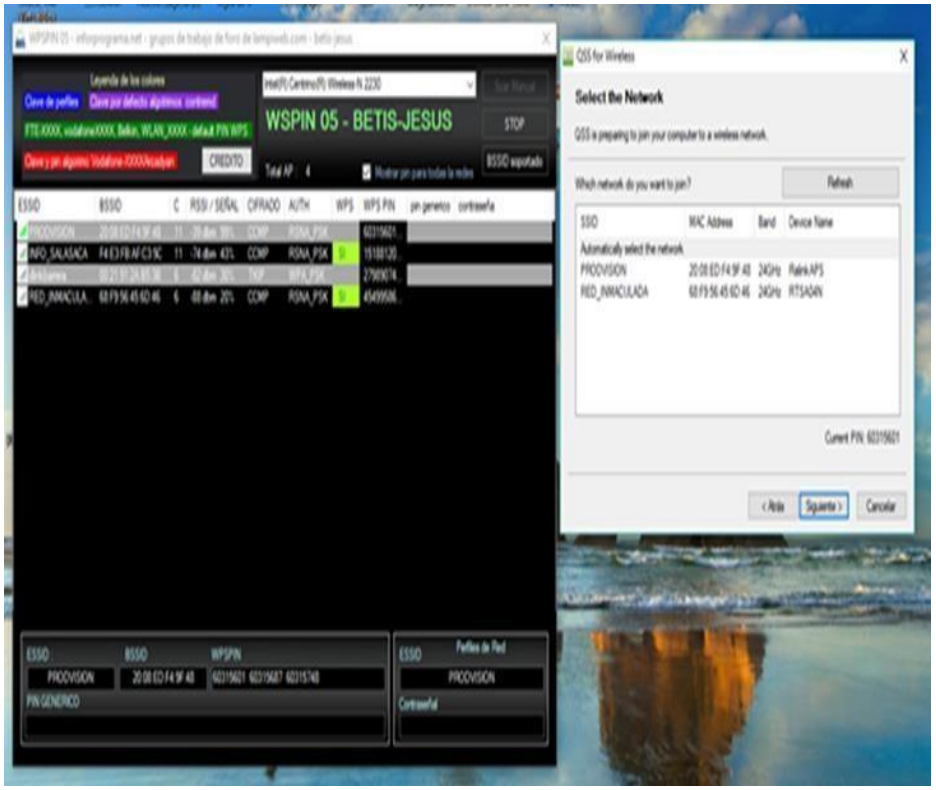


Figura 52. Intento de entrar a la red

Figura 53. Intento de entrar a la red fallida

Le dimos los permisos adecuados para que terceras personas no entren a la red de la cooperativa.

k) Conexión entre sucursales

La cooperativa de Ahorro y crédito tiene un software llamado LogMeInHamachi por lo cual tiene instalado en su servidor tal como muestra la Figura 69, por ello permite conectarse con la sucursal de Galápagos-Ambato, ya que si se va la energía el servidor dura 15 minutos en apagarse y puede guardar dicha información.

l) Servidor de correo.

La cooperativa no tiene un servidor de correo adecuado por lo general se comunican con los usuarios a través de su correo electrónico.

3.1.8 Informe de la Auditoría

3.1.8.1 Identificación del Informe

Auditoría informática para verificar los riesgos altos y críticos de la cooperativa de Ahorro y crédito Prodvisión

3.1.8.2 Identificación de los activos auditada

Estructura Organizacional de la cooperativa y Departamentos

Redes

Servidor

Información

Base de datos

Computadores

3.1.8.3 Identificación de la sociedad auditada

Cooperativa de Ahorro y Crédito Prodvision

3.1.8.4 Antecedentes

La cooperativa Prodvision colectivamente con el alumno Kevin Paul Ramos Ruiz de la Universidad Técnica de Ambato y con la autorización del sr. Jorge Manuel Masaquiza Masaquiza Gerente General de la cooperativa y la organización con el Ing. Franklin Mayorga tutor y el Ing. Segundo Alfredo Tenelema Tixe Jefe de Sistemas de la cooperativa, lo cual se requirió la elaboración de la Auditoría Informática misma que se cumplió desde el 12 de mayo al 24 de diciembre del 2020

La metodología de referencia que se utilizó fue Octave de acuerdo con las fases que nos facilita, se efectuó inspecciones en la cooperativa y los activos que se investigó, donde se utilizaron entrevistas y encuestas que forman parte del proyecto de investigación Auditoría Informática para la evaluación de riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito Prodvisión, de

la provincia de Tungurahua, Cantón Pelileo, simultáneamente se efectuó una evaluación de riesgos en los activos como son: estructura organizacional de la cooperativa y departamentos, redes, servidor, información, base de datos, computadores.

Cabe recalcar que durante la auditoría y la evaluación de riesgos en los activos de la cooperativa se detectaron algunos riesgos altos y críticos y se pusieron en conocimiento al jefe de sistema de la cooperativa y al gerente general para que de ese modo tomen una mayor seguridad dentro de la cooperativa.

3.1.8.5 Alcance de la auditoría

En la auditoría efectuada se conoció la situación actual de la cooperativa, seconoció cada uno de los activos, las vulnerabilidades, se investigó los riesgosbajos, medios, altos y críticos que presenta la cooperativa.

Por esa razón con la auditoría elaborada se pudo deducir que el Departamento de Sistemas es el responsable de la seguridad de los datos y se trata de confirmar las normativas y procesos informáticos basándonos en la metodología aplicada para minimizar los riesgos y ayudar a determinar de decisiones en la cooperativa.

3.1.8.6 Objetivos de la Auditoría

Establecer los riesgos altos y críticos de los activos de la cooperativa de Ahorro y Crédito Prodvisión

Solucionar los principales riesgos que presenta la cooperativa.

3.1.8.7 Grupo de trabajo

Ing. Franklin Oswaldo Mayorga Mayorga (tutor)

Sr. Kevin Paul Ramos Ruiz (investigador)

3.1.8.8 Periodo de ejecución

La auditoría Informática interpreta el periodo 1 abril del 2020 al 29 de enero del 2021, lo cual se efectuó una evaluación a los activos de la cooperativa de Ahorro y Crédito Prodvisión.

3.1.8.9 Metodología de referencia

METODOLOGÍA DE INVESTIGACIÓN APLICADO PARA LA AUDITORÍA INFORMÁTICA

"OCTAVE es una metodología de análisis de riesgos, estudia los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad.

La metodología OCTAVE cuenta con 3 fases durante el proceso de desarrollo de la metodología:

La primera fase contempla la evaluación de la organización, se construyen los perfiles activo-amenaza, recogiendo los principales activos, así como las amenazas y requisitos como imperativos legales que puede afectar a los activos, las medidas de seguridad implantadas en los activos y las debilidades organizativas.

En la segunda fase se identifican las vulnerabilidades a nivel de infraestructura de TI.

En la última fase de desarrolla un plan y una estrategia de seguridad, siendo analizados los riesgos en esta fase en base al impacto que puede tener en la misión de la organización.

Además se desarrollan planes para mitigar los riesgos prioritarios y una estrategia de protección para la organización" [21]

3.1.8.10 Riesgos altos y críticos encontrados en la cooperativa

De acuerdo con la evaluación de riesgos realizado en la cooperativa se encontraron riesgos altos y críticos en los siguientes activos:

Estructura Organizacional de la cooperativa y Departamentos

Manipulación del sistema Minkasoft

Incumplimiento de autenticación de los usuarios activos e inactivos de la cooperativa.

No se restringe el acceso a personas no autorizadas.

Dispositivos accesibles a personas no autorizadas

Redes

Modificaciones en los datos

Usuarios no autorizados ingresan al pc

Manipulación inapropiada en el teamviewer

Manipulación del sistema Minkasoft

El cable de red se encuentra junto al de la red eléctrica

Falta de organización del cableado

Servidor

Acceso al servidor sin autorización

Ingeniería Social

Instalar softwares dañinos

Fallas de energía eléctrica

Información no guardada

Pérdida de datos por error del usuario.

Código Sospechoso

Pérdida de conexión entre las sucursales

Información

Acceder a páginas no autorizadas

Acceso no autorizado a terceras personas

Base de datos

Fallas en procesos para recuperar la información

Mala documentación para verificar de los cambios realizados en la base

Acceso a la base de datos sin autorización

Computadores

Fallas del software

3.1.8.11 Solución de los riesgos altos y críticos encontrados en la cooperativa

Estructura Organizacional de la cooperativa y Departamentos

Riesgo: Manipulación del sistema Minkasoft

Solución: Si la manipulación del software sucede porque un puerto esta abierto lo cual detallar un conjunto de direcciones MAC correctas en el puerto, admitir que sólo una dirección MAC otorgue al puerto.

Otra posible manipulación del software es que personas no autorizadas sepan la clave de acceso al sistema, lo cual el usuario debe proteger con una contraseña robusta, la contraseña debe estar encriptada para que personas no autorizadas no sepan la clave de seguridad y para que los usuarios no autorizados ingresan al software se debe tener una tabla de auditoría en la base de datos para averiguar qué usuarios ingresaron y que transacciones se realizó al software.

Riesgo: Incumplimiento de autenticación de los usuarios activos e inactivos de la cooperativa.

Solución: Se debe establecer un manejo de clave de seguridad, bloquear, desbloquear y restablecer la clave de seguridad. Loguearse es primordial dentro de las normas de seguridad. Ya que el jefe de sistemas impide que personas inactivas ingresen a los datos personales o a la configuración del software.

Se debe restringir loguearse de forma no válida de acuerdo con el número de intentos y determinar durante cuánto tiempo la cuenta no debe estar activa, también se debe detallar el estado de la cuenta como Activo, Inactivo o Bloquear.

Riesgo: Dispositivos accesibles a personas no autorizadas

Solución: Para evitar el acceso no permitido es la de restringir los sitios en los cuales se recolecta los datos. En las prácticas de la computadora, es conveniente proteger todos los datos, fundamentalmente la información más importante, en servidores y no en la unidad del disco rígido del ordenador. Esto significa quealgún extraño que ingresen a los datos tiene que superar varios límites de acceso, eldel ordenador personal y el del servidor de la red. Habitualmente es más complicado acceder a los datos de un servidor que al de un ordenador

Redes

Riesgo: Modificaciones en los datos

Solución: Un historial de los archivos se pueden utilizar para anotar las actividades de las personas que ingresan a la información estos historiales pueden descubrir qué usuarios ingresaron a la información, qué cambios realizaron y cuándo. SoftPerfect File Access Monitor es una aplicación para este trabajo y tiene como finalidad monitorear el ingreso a toda la información, lo cual la aplicación funcionará en segundo plano dando un historial preciso.

Riesgo: Usuarios no autorizados ingresan al pc

Solución: Por medio del Control de cuentas de usuario que mejora la seguridad del del sistema operativos para impedir modificaciones no otorgadas

Riesgo: Manipulación inapropiada en el teamviewer

Solución: Teamviewer posee una autenticación de segunda fase lo cual es una tarea posible de activar y que ya le pone más complicada el acceso a los hackers, para proteger el acceso a la cuenta son las llamadas usuarios permitidos y usuarios no permitidos. Lo cual se puede contener los usuarios que ingresan al ordenador, también se puede denegar el ingreso a los usuarios no autorizados.

Riesgo: El cable de red se encuentra junto al de la red eléctrica

Solución: Lo recomendable sería desconectar los cables de red y que este a una longitud de 15 centímetros de las extensiones eléctricas ya que si se produce algún inconveniente eléctrico no tenga problemas en el hardware.

Riesgo: Falta de organización del cableado

Solución: La cooperativa de ahorro y crédito Prodvisión en el departamento de sistemas no tiene puesto canaletas para la organización del cable de red y no tiene identificadores para saber que IP está conectado o desconectado ya que si no hay conectividad la cooperativa debe de desconectar todos los cables para que vuelva la conexión.

Servidor

Riesgo: Acceso al servidor sin autorización

Solución: La protección del servidor distribuye distintos tipos de grupos añadidos y diferentes ámbitos de grupo en el servidor para fortificar el sistema operativo, para bloquear a los usuarios no autorizados y corregir la seguridad del servidor, las aplicaciones y los datos, también se requiere tener copias de seguridad correcta que proporcionan establecer la reparación de un archivo borrado o modificado.

Riesgo: Problemas en el servidor

Solución: La cooperativa de ahorro y crédito Prodvisión tiene un solo servidor ya que si este fallara tendría problemas al realizar su trabajo lo recomendable sería tener un segundo servidor en el caso si el servidor principal fallara.

Riesgo: Ingeniería Social

Solución: Una manera de impedir la ingeniería social es no dejarse engañar. Si los usuarios hayan sido víctima de ingeniería social, la gran elección es usar una aplicación antivirus para eliminar todos los archivos maliciosos y cambiar todas las claves de seguridad usando un software de claves para establecer y almacenar claves difíciles de recordar para que así otros usuarios no accedan a la información.

Riesgo: Instalar softwares dañinos

Solución: Para instalar un software debemos de bajar de páginas oficiales de manera protegida, también se debe disponer con un antivirus, que nos conlleve a tener una mejor seguridad. Así lograremos vencer las dificultades al instalar un software.

Riesgo: Fallas de energía eléctrica

Solución: Para prevenir los peligros de perder los datos de los ordenadores, lo cual la cooperativa requiere lograr un método de seguridad en la electricidad, como las UPS apropiadas para los principales problemas de conexión. No obstante, determinar con un sistema eléctrico esencial ya que es tan transcendental y elemental en el hardware.

Riesgo: Información no guardada

Solución: Uno de los problemas que se puede tener al momento que se va la energía eléctrica ya que los ordenadores se apagan y los trabajadores de la cooperativa no guardan la información lo que se debe de hacer si se va la energía eléctrica la cooperativa debe tener un límite de 30 minutos que se apaguen los ordenadores después que se vaya la energía, para que así los trabajadores tengan el tiempo suficiente para hacer su trabajo. Otros principales problemas de no guardar la información que los archivos fueron cerrados por equivocación ya que se debe tener un guardado automático en cualquier software.

Riesgo: Pérdida de datos por error del usuario.

Solución: Se debe tener respaldado toda la información del ordenador en la nube o fuera de la cooperativa ya que si se produce una pérdida de la información se pueda recuperar dicha información fácilmente.

Riesgo: Código Sospechoso

Solución: Se debe proteger los usuarios usando por medio de la autenticación de segunda fase para ofrecer una mayor protección ya que para iniciar la sesión en el usuario tiene que ingresar un código enviado desde el celular o en el correo.

Riesgo: Pérdida de conexión entre las sucursales

Solución: Cuando el servidor pierde un vínculo de los usuarios de modo espontánea, se comunica a los usuarios sobre el hecho y se espera a que inicien sus comprobaciones. Todo esto hace respaldado a los túneles Hamachi frente a dificultades de red momentáneos en el acceso entre el servidor y los usuarios.

También, usar un prefijo de red crea un único dominio de difusión entre todos los clientes. Esto hace posible el uso de etiquetas que acatan la comunicación de la IP para manifestar e informar medios sobre el sistema de Hamachi.

Información

Riesgo: Acceder a páginas no autorizadas

Solución: La técnica adecuada para impedir cualquier tipo de navegación a través de Internet es utilizar un servidor proxy, mediante el cual puede otorgar la dirección a la red intranet y ethernet evitando la salida al exterior, o a ciertos sitios, o bloquear la utilización del protocolo HTTP a través un firewall.

Evidentemente, la cooperativa no usa un servidor proxy para controlar los accesos y los usuarios que tendrán permisos de conexión. Ya que la conexión proxy no deben estar definidos a los trabajadores que no sean el departamento de sistema.

Riesgo: Acceso no autorizado a terceras personas

Solución: Para restringir la dirección desde un computador no permitido de la IP, lo cual se debe determinar el rango de las IP que logran ingresar al hardware. También, se debe definir los protocolos no usados para disminuir los riesgos.

Base de datos

Riesgo: Fallas en procesos para recuperar la información

Solución: La Recuperación de un error en la información obliga, subir nuevamente la base de datos a partir de un respaldo por medio de backups y posteriormente manejar la bitácora, o system log, para realizar de nuevo todas las transacciones terminadas desde que se hizo esa copia para respaldo.

No hay necesidad de anular todas las transacciones inconclusas en el momento de la falla, porque por definición esas transacciones ya se eliminaron de todas maneras.

Riesgo: Acceso a la base de datos sin autorización

Solución: Restringir el ingreso a la base de datos tanto para beneficiarios como para operaciones. Es decir, solo se autoriza a ciertos trabajadores para poderrealizar búsquedas o transacciones relacionadas con datos personales

Computadores

Riesgo: Fallas del software

Solución: En caso de un virus, debemos colocar un antivirus para evitar peligros. Estos antivirus trabajan tanto de modo protectora notificando el acceso de los virus, y los eliminan si entran en el ordenador.

“Mantener el sistema operativo y los programas actualizado. Tanto las reajuste automáticas como las de controladores y drivers de cada uno de los dispositivos en nuestro sistema mejorarán el rendimiento de nuestro equipo e impedirán la aparición de errores potenciales.

Reinstalar Windows soluciona de golpe cualquier fallo en el software. Para ello, se recomienda realizar previamente una copia de seguridad para no perder los datos importantes que queramos mantener" [41]

3.1.8.12 Conclusiones

Como consecuencia del informe y con la investigación que se detalló, lo cual se proporcionó las principales riesgos altos y críticos con el propósito de ayudar con los requerimientos productivos sobre los riesgos hallados.

La cooperativa solo cuenta con un solo servidor ya que si este fallara no pueda realizar sus transacciones.

La cooperativa no tiene un firewall que imposibilite el uso perjudicial y para la ejecución de los procedimientos.

3.1.8.13 Recomendaciones

Es primordial que el personal de sistemas implemente distintas instrucciones para la seguridad de los datos, en los instrumentos que brinda Windows.

El servidor de la cooperativa es la parte principal para realizar las transacciones ya que si este fallara no podría hacer sus respectivas transacciones, por lo general la cooperativa, deberá tener un servidor secundario lo que permitirá en caso de fallo del primer servidor para el proceso de las transacciones de la cooperativa.

Se pide a la cooperativa tener un firewall para la protección de la información.

Se pide al gerente de la cooperativa que solicite al jefe de sistemas dar una información clara sobre los problemas que pueda presentar el software y hardware en el rendimiento y su funcionamiento.

CAPITULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se evaluó la situación actual de la cooperativa de Ahorro y Crédito Prodvisión mediante entrevistas y cuestionarios.

En la cooperativa de Ahorro y crédito no se ha realizado ninguna auditoría informática lo cual el gerente de la cooperativa no sabía que riesgos existen.

Los activos que usan en la actualidad en la cooperativa muestran poca seguridad ya que puede presentar robo de información lo cual puede perjudicar gravemente en la cooperativa.

Mediante la metodología aplicada se determinó en cada uno de los activos los riesgos bajo, medio, alto y crítico que existen en la cooperativa de Ahorro y Crédito PRODIVISION.

El hardware de la cooperativa están cerca de las extensiones eléctricas ya que si se produce un corto circuito se podría quemar el hardware por lo cual se perdería la información y los cables de red se encuentran en el piso de forma desordenada en algunos departamentos sin su respectiva identificación de dirección IP.

.

4.2 Recomendaciones

Se recomienda mejorar las normas de seguridad que conlleven a perfeccionar la seguridad en los datos y el trabajo del departamento de Sistemas.

Se recomienda realizar auditorías cada año las cuales ayuden a minimizar los riesgos en los activos de la cooperativa.

Utilizar metodologías apropiadas para minimizar los riesgos y para un correcto funcionamiento de los activos de la cooperativa.

Es primordial capacitar a todo el equipo de trabajadores de la cooperativa con el propósito de minimizar los riesgos.

Se recomienda poner canaletas y poner identificaciones de dirección IP para evitar que haya pérdida de conexión y se debe evitar poner el hardware junto a las instalaciones eléctricas ya que si se produce un cortocircuito no tenga pérdida alguna.

.

Referencias Bibliográficas

[1] Rosa Alexandra Gálvez Morocho, "Auditoría Informática de la Cooperativa de Ahorro y Crédito "Fernando Daquilema, Aplicando el Marco de Trabajo COBIT", http://dspace.unach.edu.ec/, Ene, 2016. [online], Disponible en http://dspace.unach.edu.ec/bitstream/51000/3295/1/UNACH-EC-ING-SIS-COM-2016-0025.pdf, [Accedido: Abr. 19, 2020].

[2] Daniel Arturo Alejo Blanco, Erika Alejandra García Hernández, "Modelo De Auditoria Para El Mejoramiento Del Sistema De Control Interno De Instituciones Financieras En Colombia Basado En Lineamientos De La Ley Sarbanes Oxley Sección 404.", https://repository.ucatolica.edu.co/, Nov, 2017. [online], Disponible en https://repository.ucatolica.edu.co/ bitstream/10983/15330/1/TRABAJO%20DE%20GRADO%20FINAL%202017.pdf, [Accedido: Abr. 19, 2020].

[3] CLAUDIA PATRICIA MARRUGO HERNÁNDEZ, FERNANDO ANDRÉS SALGADO TOVAR, "EVALUACIÓN A LA GUÍA DE AUDITORÍA ELABORADA PARA EL DESARROLLO DE APLICACIONES Y CONTROL DE CAMBIOS DE LOS SISTEMAS DE INFORMACIÓN EN PRODUCCIÓN EN LA EMPRESA BANCAMÍA S.A.", https://repository.ucatolica.edu.co/, Nov, 2015. [online], Disponible en https://repository.ucatolica.edu.co/bitstream/10983/2462/1/Proyecto%20de%20Grado%20FINAL.pdf [Accedido: Feb. 22, 2021].

[4] Amarilis Carolina Loor Párraga, Verónica Alexandra Espinoza Castillo, "Auditoría de Seguridad Física y Lógica a los Recursos de Tecnología de Información en la Carrera Informática de La ESPAM MFL", http://repositorio.espam.edu.ec, Mar, 2014. [online], Disponible en http://repositorio.espam.edu.ec/bitstream/42000/72/1/TESIS%20AMARILIS%20C-AROLINA%20LOOR%20P%C3%81RRAGA%20-%VER%C3%93NICA%20ALEXANDRA-%20ESPINOZA%20CASTILLO.pdf, [Accedido: Abr. 19, 2020].

[5] GAVINO Alan Raul, "AUDITORIA EN SEGURIDAD INFORMÁTICA Y GESTION DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO, 2018. [online], Disponible en http://repositorio.unjfsc.edu.pe/bitstream/handle/UNJFSC/2924/raul-gavino.pdf?sequence=1&isAllowed=y [Accedido: Feb. 22, 2021]

[6] Muguerza A, "Empresas y Fraudes que se han hecho en la historia", 2014. [online], Disponible en https://www.eleconomista.es/empresas-finanzas/noticias/6023247/08/14/Fraudes-empresariales-que-han-hecho-historia-en-Espana-y-fuera-de-sus-fronteras.html [Accedido: Feb. 22, 2021]

[7] MUÑOZ RAZO Carlos, "Auditoría en Sistemas Computacionales", Pearson Educación, 2002, [Accedido: Jun.12, 2019].

[8] PIATTINI Mario, "Auditoría Informática: Un Enfoque Práctico", Madrid, España: RAMA, 2001, [Accedido: Jun.12, 2019].

[9] YAGUA B, "Auditoría Informática y su incidencia en los Riesgos para el manejo de la Información en la cooperativa de Ahorro y Crédito Educadores de Tungurahua", 2014. [online], Disponible en https://repositorio.uta.edu.ec/bitstream/123456789/8099/1/Tesis_t917si.pdf [Accedido: Feb. 22, 2021]

[10] NARANJO Alice, "Auditoría de Sistemas: Tipos de Auditoría", www.anaranjo.galeon.com, Abr, 2011. [online], Disponible en http://anaranjo.galeon.com/tipos_audi.htm, [Accedido: Jun.12, 2019].

[11] DHARMA Ingeniería, "Auditoría Informática – Dharma", www.dharma.es, Ene, 2005. [online], Disponible en http://www.dharma.es/index.php/auditoriainformatica/auditoriainformatica, [Accedido: Jun.12, 2019].

[12] Business School, "¿Qué es una auditoría informática y qué debes saber sobre ella?", Barcelona, 2020, [Accedido: Jun.12, 2020].

[13] Economipedia, "Auditoría Informática", www.economipedia.com, Feb, 2020. [online], Disponible en https://economipedia.com/definiciones/auditoria-informatica.html, [Accedido: Abr. 20, 2020].

[14] SERAFIN Simón, "Auditoría Informática: Apuntes de la Asignatura", www.scaridad.com, Nov, 2012. [online], Disponible en http://www.scaridad.com/files/Apuntes%20AI%20Tema%201.pdf, [Accedido: Jun.12, 2019].

[15] CRISTINA, "Análisis y Gestión de Riesgos Informáticos para proteger los Sistemas de Información", www.mentesinquietas.net, Ene, 2012. [online], Disponible en http://www.mentesinquietas.net/blog/archives/378, [Accedido: Abr.19, 2020].

[16] CUN, "Auditoría Informática", https://sites.google.com/site/, Mar, 2019. [online],Disponible en https://sites.google.com/site/auditoriaeninformaticacun/planeacion, [Accedido: Abr. 20, 2020].

[17] ITURRICASTILLO PLAZAOLA Iván, "Medición y Gestión de riesgos en las entidades financieras a través de la inmunización", Servicio Editorial de la Universidad del París Vasco, 2007, [Accedido: Abr. 20, 2020].

[18] TIPANTUÑA NARVAEZ Mireya, "Evaluación y Prevención de riesgos financieros en la Fundación de ayuda microempresarial FUNDAMIC", Departamento de Ciencias Económicas, Administrativas y de Comercio, 2013, [Accedido: Abr. 20, 2020].

[19] Administración Electrónica, "Magerit", 2012, [Accedido: Sep. 22, 2020].

[20] HUERTA Antonio, “Introducción al análisis de riesgos metodologías”, 2012, [Accedido: Sep. 22, 2020].

[21] MENDOZA María, “Auditoría de Seguridad Informática interna y perimetral para la empresa confecciones Pazmiño Castillo CIA.LTDA”, 2012, [Accedido: Ago. 20, 2020].

[22] MIRANDA Alex, “Principales riesgos en el manejo de la información: Seguridad de la información”, www.alex-mir.blogspot.com, Mar, 2011. [online], Disponible en http://alex-mir.com/2011/03/principales-riesgos-en-el-manejo-dela.html, [Accedido: Abr. 20, 2020].

[23] HERNÁNDEZ Rocío, “Auditoría Informática: Un Enfoque Metodológico y Practico”, México: Continental, 2009, [Accedido: Abr. 19, 2020]

[24] VELAZQUEZ Dalia, “Auditoría: sistemas de gestión de calidad”, www.emagister.com, Jul, 2011. [online], Disponible en http://www.emagister.com/curso-auditoria-auditor/proceso-auditoria-criteriosobjetivos-beneficios-tipos-auditoria, [Accedido: Feb.12, 2021].

[25] GUTIÉRREZ Ana, “La Auditoría en la Informática”, México: Continental, 2011, [Accedido: Feb. 11, 2021].

[26] HERRERA Cristian, “Hacia una correcta hermeneutica penal: Delitos Informáticos vs. Delitos Electrónicos”, dspace.ucuenca.edu.ec, Mar, 2010. [online], Disponible en https://dspace.ucuenca.edu.ec/bitstream/123456789/2673/1/tm4391.pdf [Accedido: Abr. 20, 2020].

[27] BERGER Simón, “Notas de trabajo para manejo de la información en la acción contra las minas: Planificación para el manejo de la Información”, www.gichd.org, Dic, 2012. [online], Disponible en http://www.gichd.org/fileadmin/pdf/other_languages/spanish/Material_Information_Mgmt_in_MA_sp.pdf, [Accedido: Abr.19, 2020].

[28] Comunidad, Madrid, “Análisis de riesgo”, http://www.madrid.org/, Dic, 2012. [online], Disponible en http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf, [Accedido: Abr. 20, 2020].

[29] BURGOS, Andrés, “Plan de Contingencia Informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la fundación cultural yeducativa Ambato - Unidad Educativa Atenas”, 2020, [Accedido: Sep. 22, 2020].

[30] REPÚBLICA DEL ECUADOR SUPERINTENDENCIA DE BANCOS Y SEGUROS, “Normas generales para las instituciones del sistema financiero”, Ene, 2004. [online], Disponible en: https://www.superbancos.gob.ec/bancos/wpcontent/uploads/downloads/2017/06/L1_X_cap_I.pdf [Accedido: Jun. 02, 2020]

[31] REYES Donald, “EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO”, 2014. [online], Disponible en https://repositorio.uta.edu.ec/bitstream/123456789/6987/1/Tesis_t871mif.pdf [Accedido: Feb. 22, 2021]

[32] MUÑOZ Oscar, “SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTODE TECNOLOGÍAS DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC”, 2020. [online], Disponible en https://repositorio.uta.edu.ec/bitstream/123456789/31305/1/t1709si.pdf [Accedido: Feb. 22, 2021]

[33] COAC Prodvisón, “COAC PRODVISIÓN”, 2018, [Accedido: Jun.12, 2020].

[34] MIES, "LEY DE LA ECONOMÍA POPULAR Y SOLIDARIA", 2018. [online], Disponible en https://www.inclusion.gob.ec/wp-content/uploads/downloads/2012/07/ley_economia_popular_solidaria.pdf [Accedido: Feb. 22, 2021]

[35] RELANCIO Alberto, "Wireshark, un gran analizador de protocolos", 2013. [online], Disponible en https://www.seas.es/blog/informatica/wireshark- un-gran-analizador-de-protocolos/ [Accedido: Feb. 22, 2021]

[36] CATOIRA Fernando, "Uso de filtros en Wireshark para detectar actividad maliciosa", 2013. [online], Disponible en https://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/ [Accedido: Feb. 22, 2021]

[37] NETWORK Software, "20 utilitarios TCP/IP en un solo programa", 2016. [online], Disponible en https://ks-soft.net/ip-tools.esp/index.htm [Accedido: Feb. 22, 2021]

[38] BOSCO, "Redes y transmisión de datos", 2016. [online], Disponible en http://www.ing.unp.edu.ar/asignaturas/rytd/Anexos/RyTD_Anexo_TP6_Escaneo-Puertos_IPTools.pdf [Accedido: Feb. 22, 2021]

[39] RUS Cristian, "Cómo funciona exactamente un test de velocidad y cómo de fiables son", 2019. [online], Disponible en https://www.xataka.com/servicios/como-funciona-exactamente-test-velocidad-como-fiables [Accedido: Feb. 22, 2021]

[40] Oficina de Seguridad del Internauta, "Qué es WPS Pin y por qué debes desactivarlo", 2014. [online], Disponible en https://www.osi.es/es/actualidad/blog/2014/11/07/que-es-wps-pin-y-por-que-debes-desactivarlo?page=12 [Accedido: Feb. 22, 2021]

[41] COROSO, Ramón, "Fallos de software. Síntomas, causas y soluciones", 2020, [Accedido: Sep. 22, 2020].

Anexos

Anexo A. Encuesta

Universidad Técnica de Ambato

Facultad de Ingeniería en Sistemas Electrónica e Industrial

Carrera de Ingeniería en Sistemas Computacionales e Informáticos

Encuesta a los socios de la cooperativa de Ahorro y Crédito Prodvisión

1. ¿Como calificaría usted la atención que ofrece la cooperativa?

a) Mala ○
b) Regular ○
c) Buena ○
d) Excelente ○

2. Al recibir un correo con un enlace desconocido. ¿Cuál es la medida que toma?

a) Abrir y leer para verificar de que se trata ○
b) Notifica a la cooperativa ○
c) Eliminar ○
d) Nada ○

3. ¿Cómo considera las instalaciones de seguridad en la cooperativa?

a) Mala ○
b) Regular ○
c) Buena ○
d) Excelente ○

4. ¿Dónde guarda sus contraseñas?

a) Computadora ○
b) Se memoriza ○
c) Teléfono celular ○
d) Papel ○

5. ¿Ha sufrido alguna vez robo o perdida de información en su cuenta en la cooperativa?

a) SI ○
b) NO ○

6. ¿Cada que tiempo cambia de clave en su cuenta?

a) Cada mes ○
b) Cada 3 meses ○
c) Cada 6 meses ○
d) Nunca ○

7. ¿Qué tipo de parámetros utiliza en su contraseña en su cuenta?

a) Números ○
b) Letras ○
c) Letras y Números ○
d) Caracteres Especiales ○

8. Qué piensa usted sobre la seguridad en el manejo de la información proporcionada en la que utiliza la cooperativa?

a) Riesgosa ○
b) Satisfactoria ○
c) Excelente ○
d) Desconoce ○

9. ¿La cooperativa le brinda un sistema de autenticación de doble factor, es decir al momento que retira dinero o ingresa a su cuenta le notifica por correo o teléfono?

a) SI ○
b) NO ○

10. ¿Ha compartido alguna vez su contraseña de seguridad con alguna persona de su confianza?

a) SI ○
b) NO ○

Anexo B.

Figura 54. Switch de la empresa

Figura 55. Hardware junto a las instalaciones eléctricas

Figura 56. Switch arriba del cpu

Figura 57. Canaletas puesto en la cooperativa

Figura 58. Canaletas puesto en el departamento de cajas

Figura 59. Organización en el departamento de gerencia

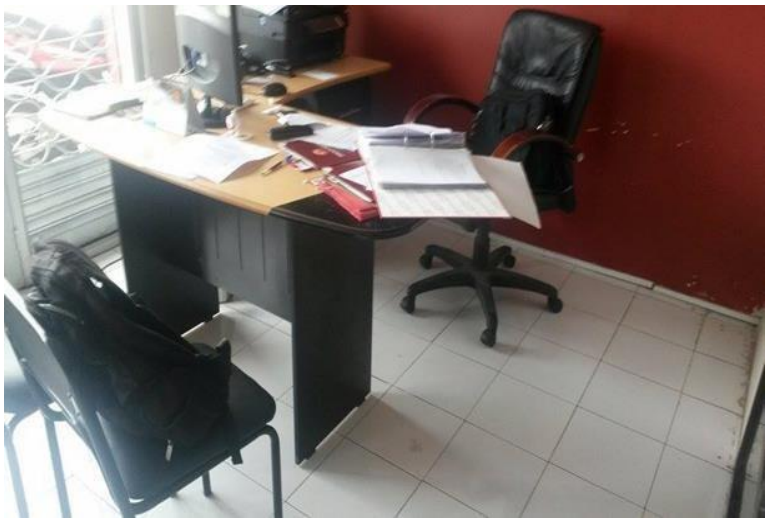


Figura 60. Organización del departamento de talento humano

Figura 61. Cables Desordenados

Figura 62. Cables sin su respectivo canaletas en el área de Sistemas

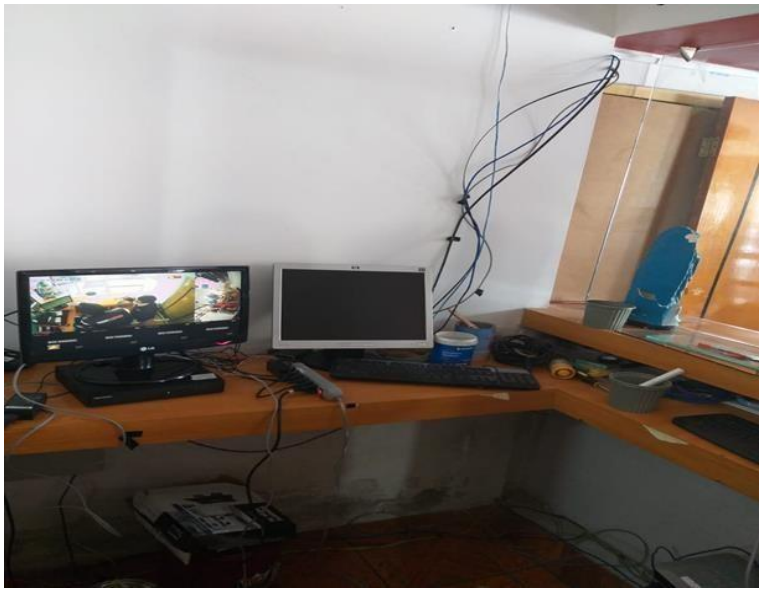


Figura 63. Funcionamiento de las cámaras de seguridad

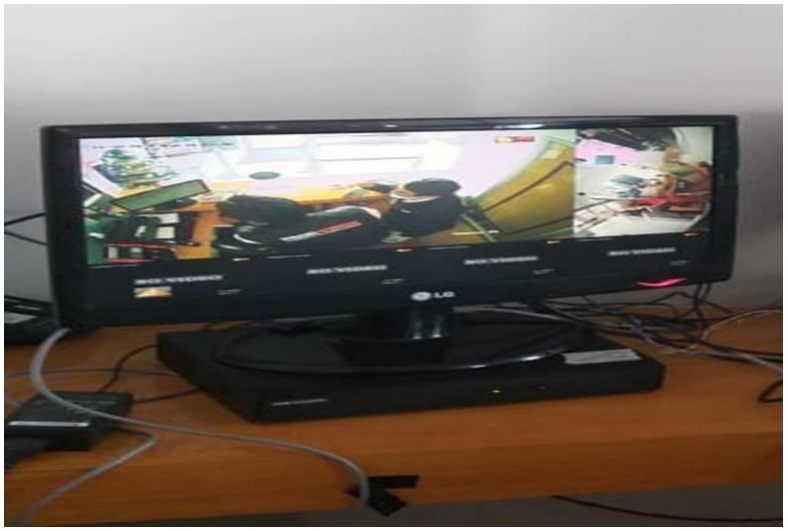


Figura 64. Cámara de seguridad en el área de sistemas

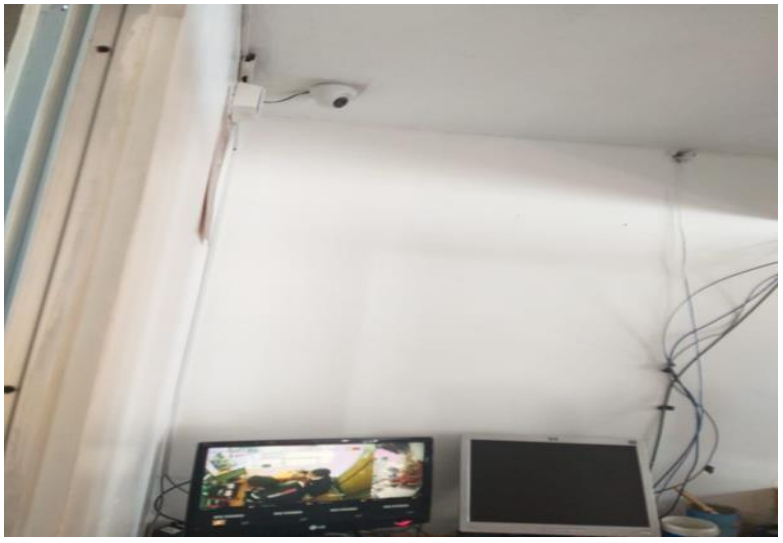


Figura 65. Interruptor en mal estado.

Figura 66. Conexión de cable de red

Figura 67. Cámara de seguridad en el departamento de cajas

Figura 68. Extintor alejado del hardware

Figura 69. Software de conexión entre sucursales

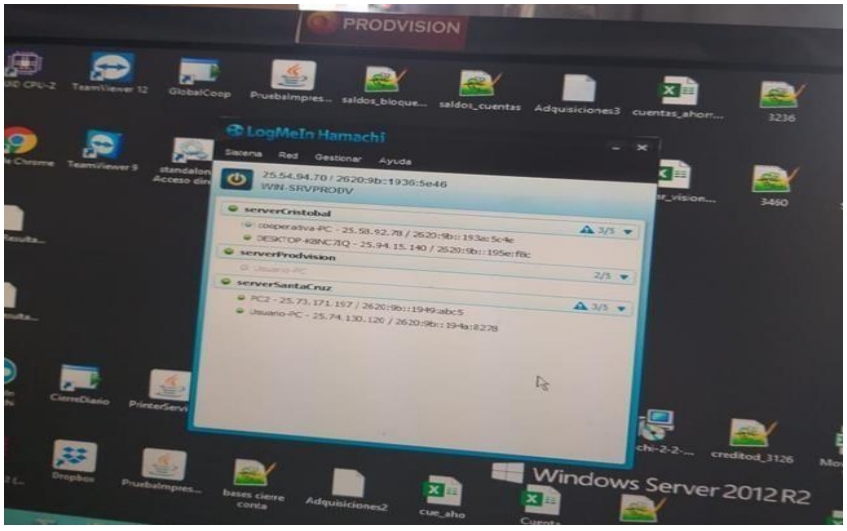


Figura 70. Reunión con el gerente de la cooperativa

Figura 71. Reunión con el personal de sistemas de la cooperativa