UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIÓN POPULAR LTDA."

Trabajo de Graduación Modalidad: TEMI Trabajo Estructurado de Manera Independiente, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTORA: Silvana Judith Garcés Ulloa

TUTOR: Ing. Jaime Bolívar Ruiz Banda, Mg.

Ambato – Ecuador

Febrero 2015

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el H. Consejo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

CERTIFICO:

Que el Informe de Investigación: "SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIÓN POPULAR LTDA.", presentado por la señorita Silvana Judith Garcés Ulloa estudiante de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del jurado examinador que el H. Consejo de la Facultad ha asignado

Ambato, Febrero 2015.

_____

TUTOR

Ing. Jaime Bolívar Ruiz Banda, Mg.

AUTORÍA DE TESIS

El abajo firmante, en calidad de estudiante de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, declaro que los contenidos de este informe de investigación científica, requisito previo a la obtención del grado de Ingeniero en Sistemas Computacionales e Informáticos, son absolutamente y de exclusiva responsabilidad legal y académica del autor.

Ambato, Febrero de 2015

_____

Garcés Ulloa Silvana Judith

CI: 1804311346

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Galo Mauricio López Sevilla, Mg. e Ing. Carlos Israel Núñez Miranda, Mg., revisó y aprobó el Informe Final del trabajo de graduación titulado "SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIÓN POPULAR LTDA.", presentado por la señorita Silvana Judith Garcés Ulloa de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Febrero 2015

…….……..

Ing. José Vicente Morales Lozada Mg.

PRESIDENTE DEL TRIBUNAL

……..…….. ….. ……..……..……

Ing. Galo Mauricio López Sevilla, Mg.

DOCENTE CALIFICADOR

Ing. Carlos Israel Núñez Miranda, Mg.

DOCENTE CALIFICADOR

DEDICATORIA

A Dios nuestro señor que siempre guía nuestros caminos para que hagamos el bien y contribuyamos en la sociedad.

A mis padres por el apoyo incondicional que siempre me brindaron, ellos que me enseñaron el valor de luchar por mis sueños y que nada es imposible si se lo desea con todo el corazón.

A mis familiares y compañeros quienes siempre me brindaron su apoyo y voluntad.

A mis amigos quienes han estado a mi lado siempre brindándome su amistad sincera y a esa personita especial que siempre se mantuvo a mi lado a pesar de todo.

Silvana Garcés

AGRADECIMIENTO

A mis profesores que me guiaron para llegar a la meta anhelada, la de ser un profesional con título de tercer nivel.

A mis padres quienes me brindaron todo el apoyo necesario durante mi vida de estudiante.

A mi persona favorita quien siempre me brindo su amor, apoyo y empuje para seguir el camino hacia esta meta.

Silvana Garcés

ÍNDICE GENERAL

CONTENIDO **Pág.**

CAPÍTULO I
EL PROBLEMA

CAPÍTULO II
MARCO TEORICO

CAPÍTULO III

METODOLOGIA

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

RESUMEN EJECUTIVO

La Cooperativa de Ahorro y Crédito Unión Popular Ltda. es una entidad financiera que presta servicios de captación de recursos, operaciones crediticias y servicios financieros destinados a microempresarios, brindando confianza, seguridad, y atención personalizada para propiciar el desarrollo social y económico de sus socios.

Dada la importancia de la información que maneja diariamente la cooperativa es fundamental la implementación de mecanismos de seguridad informática que protejan los datos que se transmiten e interactúan en la red de datos. Instaurando recursos de red que permitan que no se violen barreras de acceso que puedan generar pérdidas a la cooperativa y que los servicios prestados por la red se utilicen de la mejor manera y se encuentre disponibles por todos los usuarios.

La ejecución de seguridad en la red de datos de la Cooperativa de Ahorro y Crédito Unión Popular Ltda. permitirá que la información sea mucho más segura y libre de intrusos, mediante el establecimiento de políticas para la correcta utilización de los servicios de red, las que deben ser cumplidas por los empleados de la cooperativa; así como también la instalación de mecanismos de seguridad como un Firewall, servidor Proxy e IDS (Sistema de Detección de Intrusos) que permitirán una correcta administración, control y monitoreo de la red de la cooperativa.

ABSTRACT

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Is a financial institution providing fundraising services, lending and financial services for microentrepreneurs, providing confidence, security, and personal attention to promote social and economic development of its partners.

Given the importance of the information handled by the cooperative daily is essential to implement computer security mechanisms to protect the data transmitted in the network and interact with data. Instituting network resources that allow no barriers that could result in losses to the cooperative are violated and that the services provided by the network are used in the best way and find available for all users.

The implementation of network security data from Cooperativa de Ahorro y Crédito Unión Popular Ltda. People. Allow the information to be much safer and free from intrusion by setting policies for the proper use of the network services, which must be met by employees of the cooperative; well as the installation of safety devices such as a firewall, proxy server and IDS (Intrusion Detection System) to enable proper management, control and monitoring of the cooperative network.

INTRODUCCIÓN

La seguridad informática se ha tornado fundamental, dado la importancia de la información que se genera. Las redes de datos son esenciales para la comunicación ya que estas permiten la transmisión y recepción de información.

Este proyecto está dedicado a la seguridad informática de la red de datos de la Cooperativa de Ahorro y Crédito Unión Popular Ltda., para fortalecer la integridad de las comunicaciones, mediante la aplicación de políticas y mecanismos que brindan seguridad.

El primer capítulo pone en evidencia el problema real que tiene la Cooperativa en lo que se refiere a la seguridad informática, su planteamiento, delimitación, justificación y objetivos con el fin de clarificar el contexto sobre el cual se va a desarrollar este proyecto.

En el segundo capítulo se dan a conocer antecedentes que se han encontrado sobre la presente investigación y fundamentos teóricos sobre los que la investigación se basa para desarrollarse. Aquí se menciona la propuesta de solución del trabajo.

En el tercer capítulo se describen los diferentes tipos de investigación que se utilizaron por parte del investigador y se detalla la población y a la muestra, Además, se plantean los planes de recolección, procesamiento y análisis de datos y se enumeran los pasos del desarrollo del proyecto.

En el capítulo cuatro se desarrolla la propuesta de tal manera que se describe punto por punto lo mencionado en el capítulo tres, con la finalidad de obtener un mejor diseño e implementación de seguridad informática.

En el quinto capítulo se dictan las conclusiones y recomendaciones obtenidas luego del desarrollo del proyecto.

CAPÍTULO I

EL PROBLEMA

1.1 TEMA

"Seguridad Informática para la Red de Datos en la Cooperativa de Ahorro y Crédito Unión Popular Ltda."

1.2 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, con los servicios que brinda la red toda organización que maneje distintas líneas de negocio se ha visto inclinada al uso prioritario de distintos servicios informáticos para tener acceso a su información, trayendo como consecuencia un gran avance tecnológico por la implementación de infraestructuras que permitan la administración, acceso a la información y la comunicación entre los sistemas informáticos y aportando consigo grandes necesidades de seguridad para resguardar cualquier tipo de información de la empresa.

Las redes de computadoras tienen un papel esencial en el manejo, transmisión y recepción de información, por lo que el diseño adecuado de la red y la seguridad de la información se ha tornado en un asunto de primera importancia dado el incremento de incidentes ocasionados por terceros al querer acceder a la información restringida mediante mecanismos de ataques o violaciones a las barreras de acceso a los recursos tecnológicos o al acceder a los diferentes servicios que brinda la red de la mejor manera. En Ecuador poco a poco se ha ido poniendo mayor atención a los avances tecnológicos, permitiendo así que las redes sean un pilar fundamental, con el fin de proteger la

información mediante metodologías de seguridad para su manejo, transmisión y recepción de manera segura y eficiente, así mismo permita que este recurso sea escalable y administrable. [1]

En las diferentes organizaciones esta necesidad se ha tornado fundamental por lo que se ha puesto mayor atención a la seguridad informática para las redes de datos en su infraestructura tecnológica, tanto física como lógica, implementando recursos de red que permitan que no se violen barreras en su acceso que puedan generar pérdidas a la empresa y que los servicios prestados por la red se utilicen de la mejor manera y se encuentre disponibles por todos los usuarios.

En la Cooperativa de Ahorro y Crédito "Unión Popular Ltda.", el sistema de comunicación se encuentra en un proceso de desarrollo adaptándose a las nuevas tecnologías para la transmisión de información mediante la red, la cual en la actualidad permite la comunicación entre los diferentes dispositivos, pero no la correcta administración de sus servicios y tiene falencias en la seguridad.

La cooperativa carece de un Departamento de Sistemas con el suficiente personal, lo que ocasiona que no se permita el desarrollo de mecanismos y nuevos recursos que eviten el incremento de vulnerabilidades dentro de los patrimonios tecnológicos y se ponga mayor atención en los estándares de red que se deben cumplir para un correcto funcionamiento.

La infraestructura de red actual no permite controlar y administrar la transmisión de información que ingresa desde el exterior de su red LAN, añadiendo una deficiente configuración de los equipos de la red, y un deficiente control en el acceso a URL's o páginas web innecesarios, que pueden provocar la propagación de amenazas del Internet, además la deficiente administración de los servicios, tales como: Correo Electrónico, Servidor Web, Servidores de Archivos e Impresoras, lo que genera que el compartir datos y recursos entre sus diferentes departamentos no se realice de la manera más adecuada, provocando que la información no esté disponible en el tiempo requerido.

1.3 DELIMITACIÓN

ÁREA ACADÉMICA: Hardware y Redes
LÍNEA DE INVESTIGACIÓN: Sistemas Administradores de Recursos
SUB-LÍNEA DE INVESTIGACIÓN: Seguridad informática
ESPACIAL: La presente investigación se realizará en la ciudad de Ambato, en la Cooperativa de ahorro y Crédito "Unión Popular Ltda."
TEMPORAL: El presente proyecto de investigación tendrá una duración de 6 meses, a partir de la aprobación por el Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4 JUSTIFICACIÓN

El presente proyecto busca responder las necesidades que tiene toda red de datos empresarial, permitiendo de este modo diseñar la seguridad informática para la red de datos, que permita tener mayor control en la transmisión de información y la adecuada administración de los recursos dentro de la red.

Una infraestructura correcta que permita la administración de los recursos de la red aportará en la preservación de la confidencialidad, integridad y disponibilidad de la información de la red, así mismo proporcionará el uso compartido inteligente de archivos y dispositivos de red; y la utilización de la Internet de forma segura y controlada.

Establecer la seguridad informática aportará integridad y disponibilidad de la información en la red, a través de la utilización de mecanismos, para garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos de red cada vez que lo requiera, manteniendo la exactitud y totalidad de la información.

Los beneficiarios del proyecto serán en primera instancia todos quienes conforman la cooperativa ya que podrán contar con mejores servicios tecnológicos con mayor rapidez en su accesibilidad y teniendo la confianza que la información no ha sido vulnerada y

poder brindar a los socios un servicio de primera, que cumpla con los estándares establecidos por las entidades reguladoras, así mismo se beneficiarían los clientes ya que cuentan con el respaldo que su cooperativa cumple con los estándares para un funcionamiento óptimo.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

"Implementación de seguridad informática para la red de datos en la Cooperativa de Ahorro y Crédito "Unión Popular Ltda."

1.5.2 OBJETIVOS ESPECÍFICOS:

- Conocer los mecanismos, medidas y contramedidas en la seguridad informática.
- Elaborar un estudio de la infraestructura de red con la que cuenta la cooperativa.
- Diseñar la seguridad informática para la red de datos en la Cooperativa.
- Aplicar seguridad informática para mejorar el firewall, proxy e IDS en la Cooperativa.

CAPÍTULO II

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

Al realizar una investigación bibliográfica se encontraron los siguientes temas afines a la propuesta de solución:

El primer tema se encontró en el repositorio digital de la Universidad Técnica de Ambato bajo el título "Implementación de seguridad en la red interna de datos para el manejo adecuado de usuarios y acceso remoto en el Instituto tecnológico Pelileo" presentada por el señor Julio Cesar Pilla Yanzapanta en el año 2013 quien de manera concreta concluye que:

"La implementación de seguridad en la red interna de datos, permitirá que la información institución sea mucho más segura y libre de intrusos, y mediante la autenticación de usuarios podremos restringir accesos a direcciones no aptas.

La seguridad en Internet cobra cada vez mayor importancia, ya que no sólo se deben proteger los servidores de la empresa con Firewalls, sino también la comunicación que se realizan a través de Internet, que es una red pública susceptible de ser interceptada por millones de usuarios" [2]

En el presente proyecto se implementan mecanismos para la autentificación de los usuarios, permitiendo de esta manera tener control en los recursos que pueden ser utilizados y restringidos.

Se encontró en el repositorio digital de la Universidad Nacional Autónoma de México balo el título “Diseño e Implementación de un esquema de seguridad perimetral para redes de datos. Caso Práctico: Dirección General del Colegio de Ciencias y Humanidades” presentada por José Miguel Baltazar Gálvez y Juan Carlos Campuzano Ramírez en el año 2011 quien de concluye que:

“Haber implementado el esquema de seguridad dentro del Colegio de Ciencias y Humanidades, después de haber realizado un análisis de las necesidades del Colegio en cuanto a seguridad de la información. Es importante destacar que gracias a este trabajo fue posible implementar el primer esquema de seguridad de red perimetral para la institución, esperando que las perspectivas de seguridad plasmadas en este documento presente al lector la importancia de la seguridad de la información, procedimientos, buenas prácticas y mecanismos que permitan llevar a cabo un ciclo de mejora continua.”[3]

En el presente proyecto se diseña un esquema de seguridad para una red de datos, en la cual se muestra cada uno de los pasos a seguir para poder implementarla; desde el análisis inicial de la dirección, la identificación de las vulnerabilidades y de acuerdo a estos diseñar una solución óptima de acuerdo a las necesidades de la Dirección General.

2.2 FUNDAMENTACIÓN TEÓRICA

Una red de datos involucra más que solo conectar computadoras entre sí. Una red requiere muchas características a cumplir de manera que el diseño sea escalable y administrable. [3]

2.2.1 Red de Computadores

Una red de computadoras es un sistema formado por múltiples equipos de cómputo que se enlazan por medio de comunicación de datos, como por ejemplo cable coaxial, par trenzado, fibra óptica, señal de radio, satélite, entre otros. [4]

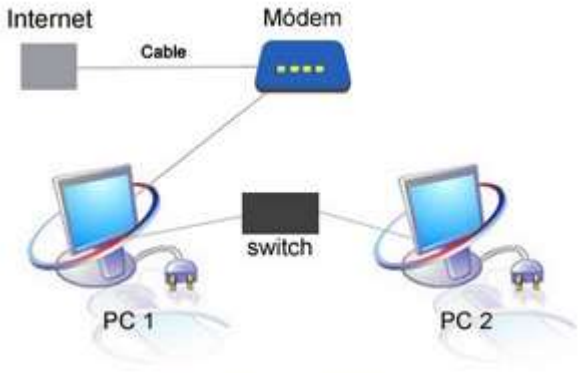

Fig. 1 Red de computadores
Fuente: Nereida GF https://sites.google.com/site/dnereidagfinformatica1/

Por extensión las redes pueden ser:

- Red de Área Local (LAN)
- Red de Área extendida (MAN)
- Red de Área amplia (WAN)
- Red de Área Personal (PAN)

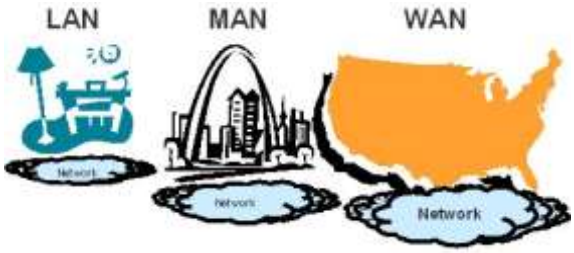

Fig. 2 Tipo de Redes
Fuente: http://zannybeliita16.galeon.com/redes.html

Por su distribución Lógica:

- Cliente/Servidor
- Igual a Igual (P2P)

Fig. 3 Por su Distribución Lógica
Fuente: http://construiryadministrarredcbtis7740ele.blogspot.com/2011/02/red-de-distribucion-logica.html

Por su topología:

- Red de Anillo
- Red de Bus
- Red de Estrella
- Red Mesh

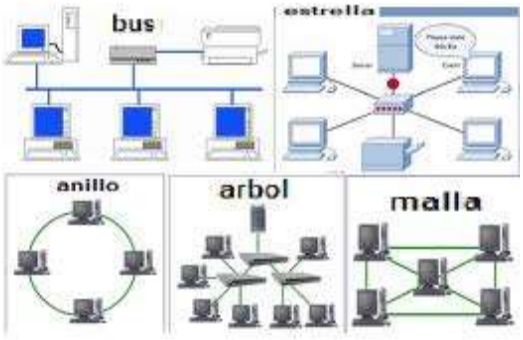

Fig. 4. Topología
Fuente: http://estudiateleco.wordpress.com/2011/02/13/tipos-de-redes-de-computadores-segun-su-topologia/
Requerimientos de Red

2.2.2 Seguridad Informática

Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoria. [7]

Aspectos importantes de la seguridad.

En la seguridad se ha considerado tres aspectos importantes que son:

Confidencialidad. Servicio de seguridad que asegura que la información no pueda estar disponible o ser descubierta por procesos no autorizados.
Disponibilidad. Un sistema seguro debe mantener la información, hardware y software disponible para los usuarios todo el tiempo.
Integridad. Condición de seguridad que garantiza que la información debe ser creada, modificada y borrada sólo por el personal autorizado. [8]

2.2.2.1 Seguridad Lógica

Consiste en la "aplicación de barreras y/o procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo" [8].

Existen muchos controles que se pueden implementar en la seguridad lógica:

Roles. Se lo realiza controlando a través de la función o rol del usuario que requiere dicho acceso.

Controles de acceso. Constituyen en la implementación de controles en cualquier utilitario de red para mantener la integridad de la información y resguardar los datos confidenciales de accesos no autorizados.

Autenticación, identificación. La identificación es el momento en que el usuario se da a conocer al sistema y autenticación se refiere a la verificación que realiza el sistema sobre esta identificación.

Listas de control de acceso ACL's. Su objetivo es filtrar tráfico, permitiendo denegando el tráfico de red de acuerdo a diferentes condiciones establecidas en los equipos de redes.

Limitaciones a los servicios. Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador.

2.2.2.2 Seguridad Física

Este aspecto no es tomado muy en cuenta a la hora del diseño de un esquema de redes, sin embargo, es un punto importantísimo ya que permite "la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial", es decir la implementación de

mecanismos, controles de acceso físico u otros componentes para preservar los sistemas tangibles de la organización.

Las amenazas pueden ser:

- Casos fortuitos o caso mayor (terremotos, inundaciones, tormentas, etc.).
- Intencionados por el hombre (robos, demoliciones, incendios etc.). [9]

2.2.2.3 Estrategias de Seguridad

Definir esquemas de seguridad que contemplen la seguridad física, lógica y de procedimientos, el esquema que se puede definir depende de la empresa.

Las aplicaciones, el almacenamiento de la información, las computadoras, los dispositivos de red y los de seguridad perimetral forman parte de un modelo de seguridad.

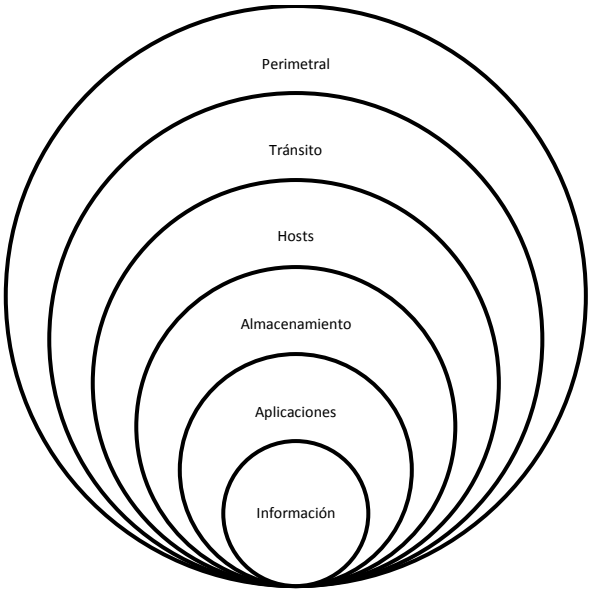

Fig. 5. Modelo de Seguridad
Fuente: http://www.cujae.edu.ec/eventos/cittel/Trabajos/CIT052.pdf

Este tipo de modelos contempla estas capas, las cuales pueden aumentar o disminuir, deben estar asociadas con las diferentes posturas para implementar mecanismos de seguridad de acuerdo a las necesidades de la organización. [10]

Defensa Perimetral.- en este modelo en la seguridad de una red, las organizaciones aseguran o fortalecen los perímetros de sus sistemas y los límites de sus redes, en sí la defensa perimetral es un conjunto de medidas, estrategias, técnicas que permiten defender y establecer un monitoreo de la parte más exterior de la red, los mecanismos más utilizados para establecer perímetros son los firewalls, IDS, VPN, DMZ y NAT. Permite una administración centralizada de la red, ya que se concentran los esfuerzos en algunos pocos puntos de acceso que definen al perímetro.

Seguridad en Profundidad.- es el modelo más robusto de defensa ya que se esfuerza por robustecer y monitorear cada sistema. Se basa en la implementación de diferentes zonas de seguridad resguardadas por diferentes mecanismos, donde cada uno de ellos refuerza a los demás, de esta manera se evita que si uno de los mecanismos falla se deje vulnerable la red completa ya que existen otros mecanismos que vencer. Los mecanismos empleados deben ser cuidadosamente configurados para evitar que las fallas de uno no se propaguen al resto, la defensa en profundidad recomienda que los mecanismos sean de diferentes marcas, debido a que si se logra vulnerar por algún medio uno de ellos, el siguiente no pueda ser vulnerado de la misma forma.

Seguridad basada en Red.- Se centra en controlar el acceso a la red, y no en asegurar los hosts, este modelo se encuentra diseñado para tratar los problemas en el ambiente de seguridad perimetral, aplicando los mecanismos de protección en un lugar común por el cual circula todo el tráfico desde y hacia los hosts. Un enfoque de seguridad en red involucra la construcción de firewalls, mecanismos de autenticación, cifrado para proteger la confidencialidad e integridad de datos y detectores de intrusos principalmente.

Principio de menor privilegio.- control de acceso y autenticación, consiste en conceder a cada objeto (usuario, programa, sistema, entre otros) sólo aquellos permisos o privilegios para que se realicen las tareas que se programaron para ellos.

Cuando se implementa alguna política de seguridad, un comienzo para una buena implementación es brindar derechos a los usuarios en función de su trabajo, una

filosofía conocida como menor privilegio.

Simplicidad.- La simplicidad de los sistemas de seguridad es un factor importante de una sólida defensa de red, particularmente de los sistemas de seguridad de red a nivel de aplicación, no deberá tener funcionalidades desconocidas y deberá mantenerse lo más simple posible.

Punto de Ahogo.- Consiste en depender de un único punto de acceso a la red privada para todas las comunicaciones entre ésta y la red pública, ya que no existe otro camino para el tráfico de entrada y salida, los esfuerzos de control y mecanismos se centran en monitorear un solo sitio de red.

Esta estrategia se considera como una solución centralizada, pero como consecuencia si se logra comprometer la seguridad en esta estrategia, se tendrá acceso a todos los recursos de la red, o en caso contrario, bloquear todos los servicios, esta situación puede ser tratada utilizando mecanismos de protección redundantes y reforzar la seguridad de los puntos de ahogo. [3]

2.2.2.4 Gestión de riesgo de la Seguridad Informática

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Fig. 6 Gestión de Riesgos
Fuente: http://protejete.files.wordpress.com/2009/07/pres_2_gestion_riesgo.jpg

La gestión de Riesgo está formada por cuatro partes:

Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.

Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- ✓ Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- ✓ Orientar el funcionamiento organizativo y funcional.
- ✓ Garantizar comportamiento homogéneo.
- ✓ Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- ✓ Conducir a la coherencia entre lo que pensamos, decimos y hacemos. [10]

2.2.2.5 Normas y Metodologías Internacionales

Tabla 1 Normas ISO

Norma	Descripción
ISO-IRAM-IEC 17799 - Tecnología de la Información – Técnicas de Seguridad - Código de Práctica para la Administración de la Seguridad de la Información.	Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. Secciones: 1. Política de seguridad. 2. Aspectos organizativos para la seguridad. 3. Clasificación y control de activos. 4. Seguridad ligada al personal. 5. Seguridad física y del entorno. 6. Gestión de comunicaciones y operaciones. 7. Control de accesos. 8. Desarrollo y mantenimiento de sistemas. 9. Gestión de incidentes de seguridad de la información. 10. Gestión de continuidad de negocio. 11. Conformidad. [11]
ISO/IEC 27000 - Tecnología de la Información – Técnicas de Seguridad – La Seguridad de la Información de Gestión de Sistemas – Fundamentos y Vocabulario	La serie ISO/IEC 27000 está formado por algunas normas que van desde (27000 a 27019 y de 27030 a 27044) y que indican cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI).

ISO/IEC 27001: Tecnología de la información -Técnicas de seguridad - Especificación de un Sistema de Gestión de Seguridad de la Información	Publicada el 15 de Octubre de 2005, es la certificación que deben obtener las organizaciones. Esta norma específica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
ISO / IEC 27002: Tecnología de la información –Técnicas de seguridad - Código de Práctica para la Gestión de Seguridad de la Información	Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.
ISO / IEC 27003: Tecnología de la información -Técnicas de Seguridad – Guía de implementación del sistema de administración y seguridad de la información	Publicada el 01 de Febrero de 2010. No es certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.
ISO / IEC 27004: Tecnología de la información -Técnicas de Seguridad – Administración de medidas de seguridad de la información.	Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según

	ISO/IEC 27001.
ISO / IEC 27005: Tecnología de la información -Técnicas de Seguridad – Administración de riesgos en la seguridad de la información	Publicada el 4 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
ISO/IEC 27033: Tecnología de la información – Técnicas de Seguridad - Seguridad en Redes	Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 10 de Diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de redes de referencia; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas. [12]

Series NIST

NIST maneja sus propios estándares y recomendaciones, cabe aclarar que no sólo se enfocan al área de las tecnologías de la información.

Los estándares y recomendaciones tienen como objetivo garantizar calidad, donde las instituciones pueden contar con un punto de referencia para identificar las necesidades y problemas de seguridad en las que éstas pueden verse involucradas. El uso de estándares de manera continua permite obtener beneficios para las organizaciones.

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de incrementar la productividad, facilitar el comercio, mejorar la calidad de vida.

La serie 800 del NIST es un conjunto de documentos de interés general sobre Seguridad de la Información; son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad. [13]

Cobit

El significado de COBIT viene del ingles "Control Objectives for Information and related Technology", que significa Objetivos de Control para la información y Tecnologías relacionadas.

Conjunto de buenas prácticas para el manejo de información que ha sido creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés:

Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute).

Los habilitadores de COBIT 5 para la SI.

1. Políticas, principios, y marcos de SI.
2. Procesos, incluyendo actividades y detalles específicos de SI.
3. Estructuras organizacionales específicas a la SI.
4. En términos de cultura, ética y comportamiento, los factores que determinan el éxito del gobierno y la administración de la SI.
5. Los tipos de información específicos a la SI.
6. Las capacidades de servicio requeridas para proveer funciones de SI a una empresa.
7. Gente, habilidades y competencias específicas para la SI.

2.2.2.6 Análisis de Riesgo Informático

El activo más importante que se posee es la información y, por lo que, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

1. Construir un perfil de las amenazas que esté basado en los activos de la organización.
2. Identificación de los activos de la organización.
3. Identificar las amenazas de cada uno de los activos listados.
4. Conocer las prácticas actuales de seguridad.
5. Identificar las vulnerabilidades de la organización.
    - Recursos humanos
    - Recursos técnicos
    - Recursos financieros
6. Identificar los requerimientos de seguridad de la organización.
7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
8. Detección de los componentes claves
9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:
    - Riesgo para los activos críticos
    - Medidas de riesgos
    - Estrategias de protección
    - Planes para reducir los riesgos. [14]

2.2.2.7 Amenazas de la seguridad de la Información

Las amenazas se pueden considerar en 4 categorías presentadas a continuación:

Tabla 2. Categorías de Amenazas *[15]*

Categoría	Descripción
Interrupción	Disponibilidad de una parte o total del sistema
Intercepción	Confidencialidad
Modificación	Ataque contra la integridad
Fabricación	Autenticidad

Ataques Informáticos

- *Ataques pasivos.* Estos ataques se basan en escuchar los datos que son transmitidos pero no en modificarlos.
- *Ataques activos.* Por el contrario de los ataques pasivos estos modifican o alteran la información que ha sido interceptada, con el fin de hacer daño.

A continuación, una lista de algunos ataques informáticos que pueden ser originados por personas internas o externas. [15]

- Actividades de reconocimiento de activos.
- Detección de vulnerabilidades en los sistemas.
- Robo de información.
- Modificación del contenido y secuencia de los mensajes transmitidos.
- Análisis de tráfico.
- Ataques de suplantación de identidad.
- Conexiones no autorizadas.
- Introducción de código malicioso.
- Denegación de servicio.

Los servicios internos como externos comparten riesgos comunes tales como:

- Intercepción de las comunicaciones.
- Suplantación de identidad.
- Interrupción de las actividades de los servicios.
- Robo de información.
- Introducción de código malicioso.
- Alteración de la información.

Para comprometer la seguridad de cualquier sistema el atacante debe tener conocimiento de 4 etapas para realizar un test de penetración [14]

Tabla 3. Etapas de Test de Penetración *[14]*

Descubrimiento	•Recopila toda información crítica.
Exploración	•Identificar los posibles víctimas.
Evaluación	•Búsqueda de vulnerabilidades de los datos encontrados.
Intrusión	•Realizar ataques a traves de las vulnerabilidades.

2.2.2.8 Mecanismos de monitoreo, control y seguimiento

El monitoreo es una de las actividades que permite tener mejor acotada la seguridad de la organización ya que permite observar los comportamientos normales y anormales en los sistemas. Los mecanismos que se emplean para monitorear varían con base en los requerimientos y alcances que planee dar la organización, dentro de éstos se encuentran bitácoras de acceso al sistema, tráfico de red, errores en los sistemas, límites de cuotas, intentos fallidos de sesión, entre otros.

Si se enfoca al monitoreo de la red de una organización los dispositivos que permiten realizar esta tarea son escogidos a partir de la propia arquitectura de red, por medio de puertos mirror, firewall, IDS, sniffer's, appliance, protocolos de monitoreo como SNMP, RMON principalmente, las características de cada uno de éstos es muy específica y la elección depende sólo de los responsables de la seguridad de la organización.

Muchos de los equipos activos en la actualidad permiten su administración y definición de servicios tanto de hardware, como de software, un ejemplo de estos son las diferentes maneras de administración por medio de TELNET, SSH, terminal, y Web, así como el manejo de protocolos como SNMP, RMON, redes virtuales y puertos espejo principalmente. El Puerto monitor o puerto espejo es una más de las prestaciones de algunos equipos, la cual permite transmitir el tráfico de un puerto específico del equipo, en otro puerto del mismo, esto con la finalidad de analizar el tráfico que pasa.

- Propósitos de diagnóstico.
- Análisis de tráfico: Identificar el tipo de aplicaciones que son más utilizadas.
- Flujo: conjunto de paquetes con la misma dirección IP origen y destino, mismo puerto y tipo de aplicación.
- Sniffer de todos los tipos.
- Appliance: Hardware con una funcionalidad dedicada, como los son los analizadores de tráfico, equipos de almacenamiento, servidores web, firewall, etc.
- Detectores de Intruso.
- Creación de bitácoras por hora, día, mes, etc.

Los mecanismos de control y seguimiento son utilizados en parte para determinar la integridad de la información y equipos, comportamiento, generación de estadísticas, tendencias así como registrar todos los eventos que se produzcan.

Servicios Seguros

Los servicios seguros brindan mayor confiabilidad en sus procesos, dentro de éstos se encuentran integridad, confidencialidad, no repudio, autenticación, control de acceso y disponibilidad.

Cifrado.- Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. [15]

Seguridad en Servidores Web.- Un servidor web puede utilizarse como una plataforma de acceso a todo el complejo de computadoras de una agencia o corporación, una vez comprometida la seguridad del servidor web, un atacante podrá obtener acceso a datos y sistemas fuera del propio servidor pero que están conectados a éste en el sitio local.

SSL.- está diseñado de forma que utilice TCP para proporcionar un servicio fiable y seguro extremo a extremo, SSL no es un protocolo simple, ya que está formado por dos niveles de protocolos (SSLRecord Protocol – Protocolo de registro SSL y SSL Handshake Protocol - Protocolo de saludo SSL).

SSL emplea llaves tanto simétricas como asimétricas para configurar la transferencia de datos de una manera segura sobre una red insegura, cuando un cliente establece una conexión SSL entre su navegador y el servidor, genera un canal seguro para HTTP conocido usualmente como HTTPS, de tal forma que impide a un intruso interpretar los datos que son trasmitidos por este canal. [16]

Cortafuegos

Los cortafuegos (firewalls) tienen como misión controlar los datos entran y salen de la red.

La ubicación del firewall es fundamental. Debe estar situado en el lugar donde podrá interceptar todos los datos. Crear zonas presenta la ventaja de circunscribir el riesgo, limitando desgastes de pirateo a una única zona.

La mayoría de las empresas adoptan un esquema clásico de tres zonas:
Zona 1: Internet y el medio externo de alto riesgo.
Zona 2: la DMZ de riesgo moderado.
Zona 3: la red Local – protegida.

Fig. 7. Firewall
Fuente: http://1.bp.blogspot.com/-vKAJy1QL1Wg/UZgEnwStWjI/AAAAAAAAAuQ/3r12F2vIMAI/s1600/firewall.jpg

Tipos de cortafuegos:

Software: Programa que es instalado en un ordenador servidor dotado de al menos dos tarjetas de red. Este computador es solamente dedicada al uso de cortafuegos, es necesario evitar su uso para otras aplicaciones.

Hardware: Serie de cajas de red especializadas que contienen hardware y software personalizados. Si se configuran correctamente, los cortafuegos de hardware constituyen una barrera protectora que mantiene ocultos los equipos de una organización con respecto al mundo exterior.

Firewall con Zona Desmilitarizada (DMZ)

Un firewall que provee protección DMZ es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta. La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y a la frecuencia con la que lo hace. Un firewall con DMZ crea un área de información protegida "desmilitarizada" en la red. Los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información que se quiere que vean, pero previene que obtengan información no autorizada. [17]

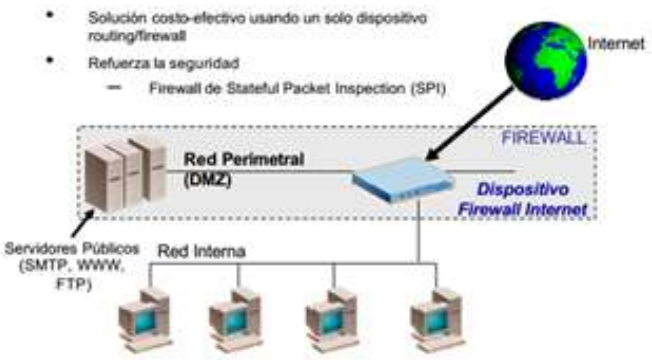

Fig. 8 Firewall con DMZ
Fuente: https://www.frozentux.net/iptables-tutorial/chunkyhtml/images/rc_DMZ_firewall.jpg

Proxys

Consiste en desconectar completamente la red local de la red exterior y luego implementar pasarelas llamadas proxy entre las dos redes para reenviar las solicitudes de la red interna hacia el exterior.

Fig. 9 Servidor Proxy
Fuente: http://diginota.com/wp-content/themes/twentyten/images/stories/marzo10/anonymous-proxy-server.jpg

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud. [18]

A continuación se presentan los requerimientos mínimos generales que debe poseer una red.

Tabla 4. ***Requisitos generales para asegurar la red LAN. [8] [9]***

Necesidades	Beneficios
Conocer al detalle las aplicaciones de la red y capacidad para controlarlas.	• Reducción en las inversiones en ancho de banda. • Mejora del rendimiento de la red. • Ahorre de costos

	• Disminución de problemas.
Firewall de Aplicación	• Definición de políticas de control y bloqueo a nivel de aplicación, usuario, servicio, entre otros.
Sistema Central de Informes	• Contar con historiales para el seguimiento de incidencias. • Poder escalar a los superiores el conocimiento detallado de la red para toma de decisiones.
Control de Flujos no Deseados	• Detección y control de ataques de spam, DoS, troyanos. • Conocer que usuarios generan dichos flujos.
Mejorar el rendimiento	• Controlar el tráfico.
Sistema de alertas	• Saber lo que pasa en la red en el momento oportuno.

Mejores prácticas enfocadas a la seguridad de la información

A continuación se destacan las mejores prácticas de seguridad para la seguridad de la información:

- ✓ Políticas de seguridad.
- ✓ Inventarios de activos.
- ✓ Norma ISO 27001.
- ✓ Aplicar un cuestionario al administrador de la red.
- ✓ Fomentar la concientización sobre seguridad de la red LAN.
- ✓ Implementar niveles de seguridad informática.
- ✓ Utilizar un plan de contingencia.

Análisis para el diseño de seguridad informática

- ✓ Analizar el nivel de riesgo.
- ✓ Analizar el nivel de riesgo que pueda correr la empresa, mediante el uso de estadística, estudio de siniestros informáticos declarados, etc.

Acciones Concretas:

- ✓ Agregar sistemas de seguridad (cortafuegos, antivirus, control de acceso, etc.)
- ✓ Modificación de configuraciones de las aplicaciones y de los sistemas operativos.
- ✓ Contar con software legal.
- ✓ Actualizar frecuentemente las aplicaciones con los "parches de seguridad".
- ✓ Modificaciones eventuales de la arquitectura informática, de los flujos de la información y de la topología de red.
- ✓ Medidas a tomar para sensibilizar al personal.
- ✓ Redacción de procedimientos de seguridad destinados a los administradores del sistema, de la red y a los usuarios. [19]

2.3 PROPUESTA DE SOLUCIÓN

Este proyecto plantea la implementación de la seguridad informática para la red de datos que permitirá controlar y administrar la información y los servicios de red, la cual aportará en la preservación de la confidencialidad, integridad y disponibilidad de la información en la red mediante la instalación y configuración de diferentes mecanismo de administración y seguridad informática.

CAPÍTULO III

METODOLOGIA

3.1 MODALIDAD DE INVESTIGACIÓN

La presente investigación se contextualizará en la modalidad de campo y documental – bibliográfica.

De campo porque los problemas recolectados se hicieron directamente en la Cooperativa de Ahorro y Crédito Unión Popular y documental bibliográfica porque se buscará información en libros, informes, revistas porque se tiene como propósito detectar, profundizar y ampliar diferentes enfoques, teorías, conceptualizaciones y criterios en todo lo relacionado el diseño de redes, su administración y seguridad.

3.2 RECOLECCIÓN DE INFORMACIÓN

Para la recolección de información se utilizarán fuentes bibliográficas como libros, artículos técnicos, etc. relacionado con la temática propuesta con los cuales se pretende tener una idea general sobre las ventajas y desventajas del proyecto planteado.

Se realizará una inspección de la infraestructura de red y una observación de sus operaciones, así mismo se revisará la documentación necesaria acerca de la infraestructura.

Además esta investigación se apoya en la realización de una entrevista estructurada mediante cuestionarios de evaluación elaborados en base a estándares de seguridad

informática, dirigida al personal del departamento de sistemas de la cooperativa, con el fin de complementar la información obtenida por el investigador, puesto que el personal sabe cada uno de los procesos que se realizan a diario y pueden aportar con detalles importantes que el investigador omita en su observación.

3.3 POBLACIÓN Y MUESTRA

Por las características de la investigación, se trabajará con la persona encargada del Departamento de Sistemas de La Cooperativa de Ahorro y Crédito Unión Popular Ltda.

3.4 PROCESAMIENTO DE DATOS

Para el procesamiento de datos se tomara en cuenta las siguientes actividades:

- ✓ Revisión de la documentación obtenida durante la recolección de información presentando una descripción ordenada sobre los ámbitos específicos a estudiarse en el presente proyecto.
- ✓ Análisis de la información lo que permitirá plantear estrategias para la solución del problema.
- ✓ Interpretación de la información que contribuirá a desarrollar la solución para el problema planteado.

3.5 DESARROLLO DEL PROYECTO

Para cumplir el desarrollo de este proyecto de investigación, se realizara en forma secuencial los métodos, procesos y/o actividades.

- Revisión de los mecanismos actuales utilizados para la seguridad informática.
- Conocimiento de las medidas y contramedidas más eficientes de la seguridad informática.
- Obtención de información de los activos y de la infraestructura de la red de datos.

- Identificación de puertos y servicios accesibles dentro de la red.
- Identificación de amenazas y vulnerabilidades de la red de datos.
- Establecimiento de mecanismo de seguridad para la red de datos (Firewalls, IDS, DMZ, Proxy).
- Definición de políticas de control de acceso.
- Determinación de procedimientos de configuración de servidores, servicios y equipos activos.
- Realización de Configuraciones del dominio en el Servidor a utilizar.
- Configuración de un Servidor Proxy.
- Establecimiento de DMZ.
- Configuración del Firewall en base a las políticas de seguridad.
- Documentación del diseño de seguridad informática para la red en la cooperativa.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

Para concretar el desarrollo de la propuesta, se toma como guía los objetivos específicos planteados, es así que por cada objetivo específico se realizan pasos concretos como se detallan a continuación:

4.1 MECANISMOS, MEDIDAS Y CONTRAMEDIDAS EN LA SEGURIDAD INFORMÁTICA

La seguridad informática, en principio, debe estar respaldada por la confianza de que los equipos desde donde se realiza el envío y recepción de información, estos deben estar correctamente asegurados.

Para la implementación de seguridad de la información es necesario basarse en estándares y normas, las cuales guían a una correcta implementación de seguridad de la información.

Toda institución financiera debe regirse en el cumplimiento de ciertas normas y estándares, los cuales regulan su funcionamiento. Los procesos tecnológicos también deben cumplir con normas y estándares, estos están basados en las Normas ISO correspondientes en conjunto con metodologías establecidas para el manejo de diferentes procesos dentro de las instituciones.

Mediante los fundamentos de las Normas ISOS 27000 se realizará cada uno delos procedimientos para la planeación, diseño e implementación de la seguridad informática

dentro de la red de datos de la cooperativa.

4.1.1 Series ISO 27001

Sistema de Gestión de Seguridad de la Información (SGSI)

ISO 27001, estándar cuyo objetivo es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

En este estándar se hace referencia sobre la importancia de:

- Entender los requerimientos de la seguridad de la información de una organización.
- Implementar y operar controles para manejar los riesgos de la seguridad, 133 controles generales de seguridad definidos, 11 áreas referidas a la seguridad física, ambiental y de los recursos humanos.
- Monitorear y revisar el desempeño y la efectividad del SGSI. [16]

El propósito de un sistema de gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- ✓ Plan (planificar): establecer el SGSI.
- ✓ Do (hacer): implementar y utilizar el SGSI.
- ✓ Check (verificar): monitorizar y revisar el SGSI.
- ✓ Act (actuar): mantener y mejorar el SGSI. [16]

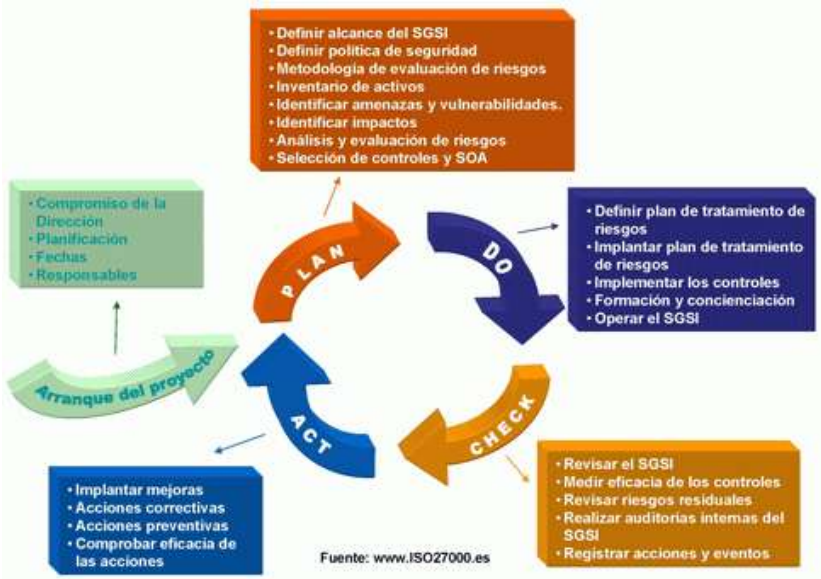

Fig. 10 PDCA
Fuente: http://www.iso27000.es/

4.1.1.1 Plan = Establecer con planificación

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; es recomendable empezar por un alcance limitado. Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc.

La política del SGSI es un documento muy general, una especie de "declaración de intenciones" de la Dirección que debe:

- Incluir el marco general y los objetivos de seguridad de la información de la organización.
- Considerar los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información.
- Alinear con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
- Establecer los criterios con los que se va a evaluar el riesgo.
- Ser aprobada por la dirección.

Definir el enfoque de evaluación de riesgos mediante una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio. Es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. [12]

- *Identificar los riesgos:*
  - Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
  - Identificar las amenazas relevantes asociadas a los activos identificados.
  - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
  - Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo. [12]

- *Analizar y evaluar los riesgos:*
  - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
  - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
  - Estimar los niveles de riesgo.
  - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado. [12]

- *Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:*
  - Aplicar controles adecuados (mitigación).
  - Aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.
  - Evitar el riesgo.
  - Transferir el riesgo total o parcialmente a terceros.

Fig. 11 Gestión de riegos
Fuente: http://www.iso27000.es/

Los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento.

Definir una declaración de aplicabilidad también llamada SOA (Statement of Applicability) que incluya:

- los objetivos de control y controles seleccionados y los motivos para su elección;
- los objetivos de control y controles que actualmente ya están implantados;
- los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias. [12]

4.1.1.2 Implementar y utilizar SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades

y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones. [12]

4.1.1.3 Monitorizar y Revisar

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
- Identificar brechas e incidentes de seguridad.
- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas. Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, entre otros.

Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo las adecuadas y posibles mejoras en el proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI. [12]

4.1.1.4 Mantener y Mejorar

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.

- Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. [12]

4.1.2 Recomendaciones NIST serie 800

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de incrementar la productividad, facilitar el comercio, mejorar la calidad de vida.

La serie 800 del NIST es un conjunto de documentos de interés general sobre Seguridad de la Información. Estas publicaciones comenzaron en 1990 y son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad. La serie 800 incluye una lista de documentos que pueden ser descargados de manera gratuita desde el sitio oficial.

NIST SP800-53 Recommended Security Controls for Federal Information Systems
Son controles de seguridad recomendados para sistemas de información federal, en éste se especifican los controles necesarios para la protección de los sistemas de información entre los que se encuentran:

- Control de acceso.
- Concientización y entrenamiento.
- Responsabilidad y Auditoría.
- Administración de la seguridad.

- Planes de contingencia.
- Identificación y autenticación.
- Respuesta a incidentes.
- Mantenimiento. [13]

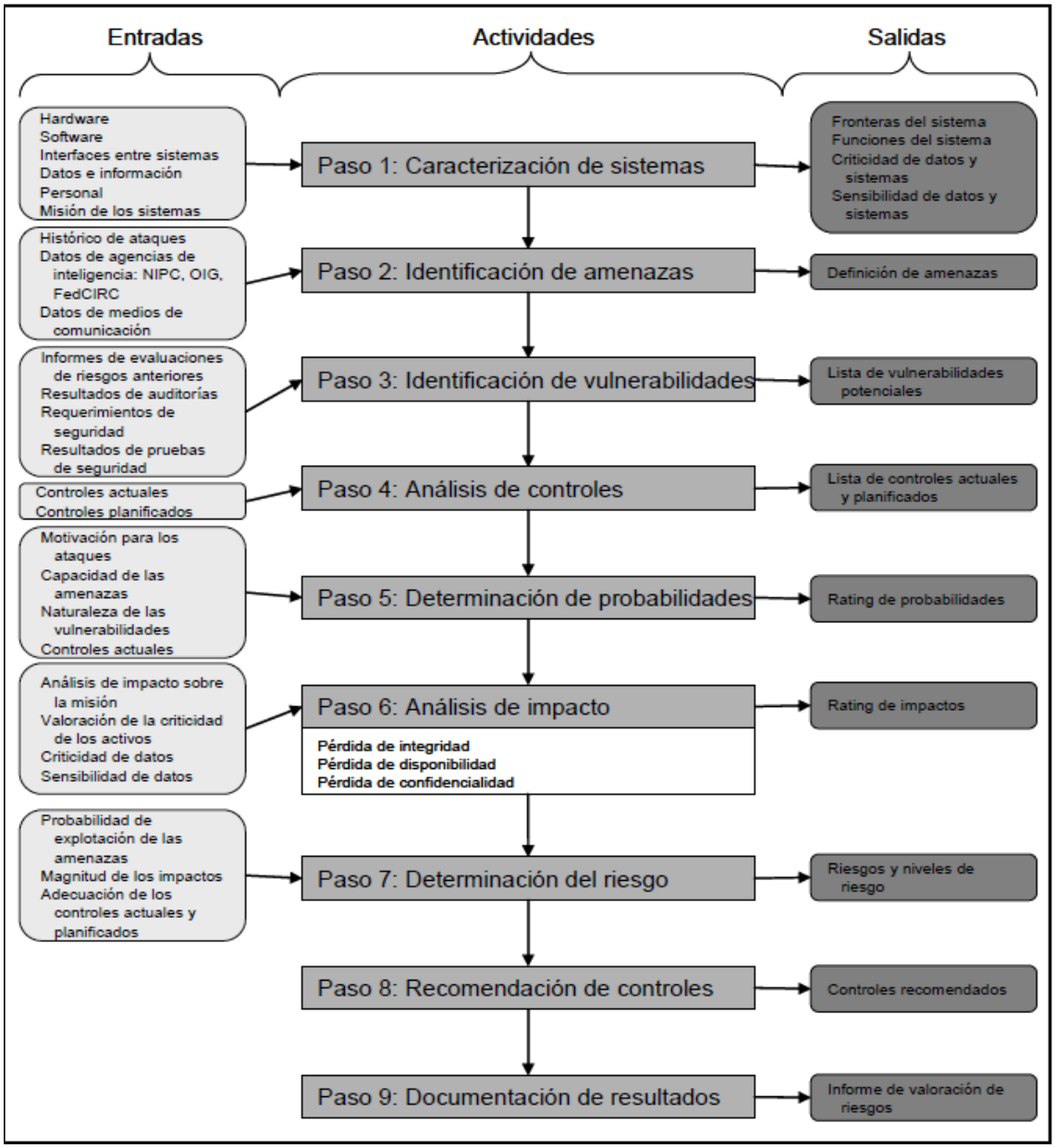

Fig. 12 ***Análisis de Riesgos NIST 800-30*** *[13]*

4.2 ESTUDIO DE LA INFRAESTRUCTURA DE RED DE LA COOPERATIVA

Para obtener la información necesaria para poder realizar el presente proyecto, se basó en la utilización de la norma ISO 27001, para poder realizar cada uno de los procesos de manera sistemática y de forma correcta, dado que la cooperativa en la actualidad está en

constante crecimiento y es necesario el cumplimiento de varios parámetros estandarizados para obtener una mejor acreditación.

4.2.1 Establecer con Planificación

El diseño de un sistema de gestión de seguridad basado en la norma ISO 27001, nos indica que debemos analizar diferentes aspectos para poder llegar a un correcto diseño e implementación de seguridades, a continuación se definirán los diferentes aspectos que se encuentran dentro de la etapa de planificación de la Norma.

LA COOPERATIVA

Antecedentes

La Cooperativa de Ahorro y Crédito Unión Popular Ltda. Nació el 30 de agosto de 1971 en la parroquia la Merced, según acta de constitución de la institución; de la idea de unos amigos de organizar una cooperativa con el fin de apoyarse mutuamente, la mayoría de ellos eran de la parroquia de San Bartolomé de Pinllo, los mismos que con el paso del tiempo serían los socios fundadores de la misma.

El nombre de la institución fue elegido de forma unánime y no ha tenido variación alguna, se eligió la directiva, quienes se encargaron de pulir algunos detalles de gran importancia, descubrieron los beneficios que obtienen al pertenecer a una cooperativa.
La inscripción de la cooperativa en el Registro General de Cooperativas se lo hizo con el número de orden 1210-0 según acuerdo ministerial número 03185-0.

Se encuentra ubicada en la ciudad de Ambato, calles Cuenca 12-55 y Mera.

Es una entidad financiera que presta servicios de captación de recursos, operaciones crediticias y servicios financieros destinados a microempresarios, brindando confianza, seguridad, y atención personalizada para propiciar el desarrollo social y económico de sus socios, esto ha permitido que la institución tenga un crecimiento moderado pero firme, lo que se refleja en su permanencia en el sector.

Infraestructura Física

El edificio cuenta con cuatro pisos, uno de estos en el subsuelo de la edificación, se comunican mediante escaleras.

- La cooperativa cuenta con oficinas desde el subsuelo hasta el tercer piso, en el segundo piso se establece una sala de recepciones.
- En el primer piso se encuentra los Departamentos de Contabilidad, Sistemas y la oficina de Gerencia.
- En la planta baja se encuentran Cajas e Información.
- En el subsuelo funciona el área de Créditos y Cobranzas.

Los servidores están ubicados en el tercer piso del edificio, en un área independiente a los departamentos, se observó que para el acceso a este piso no cuenta con ningún tipo de restricción.

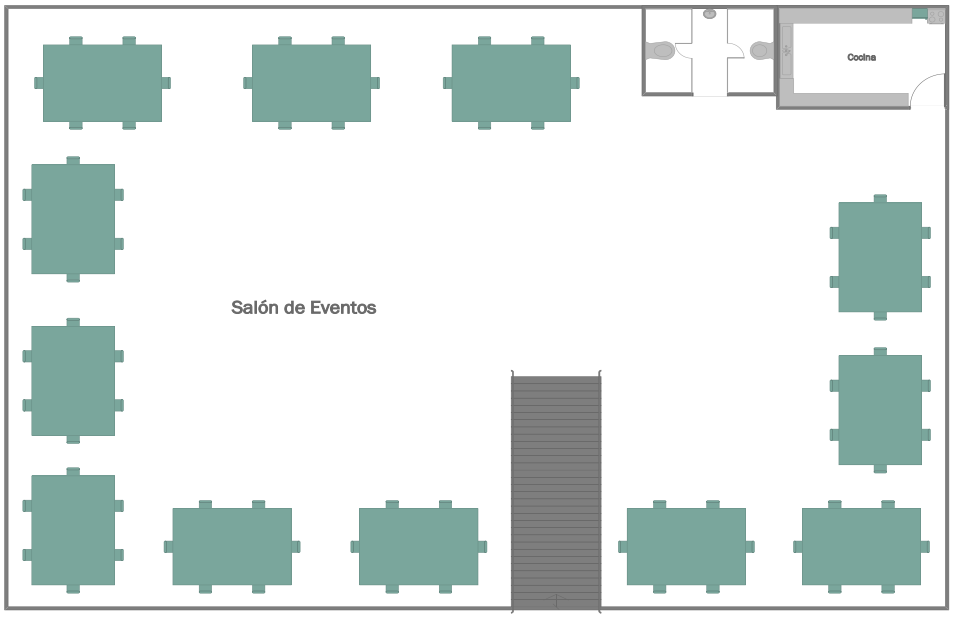

Fig. 13 Segundo Piso
Elaborado por: El Investigador

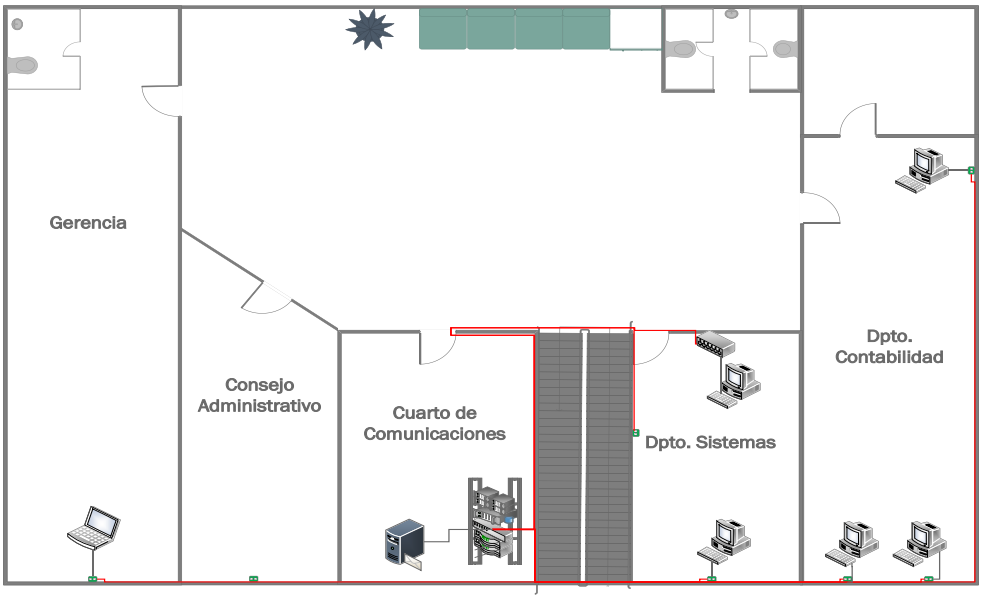

Fig. 14 Primer Piso
Elaborado por: El Investigador

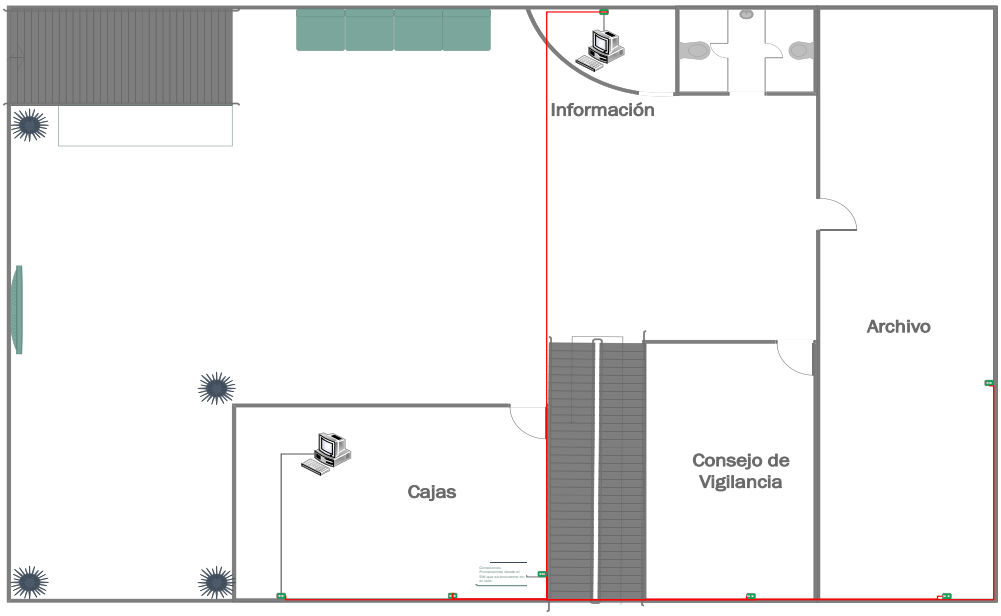

Fig. 15 Planta Baja
Elaborado por: El Investigador

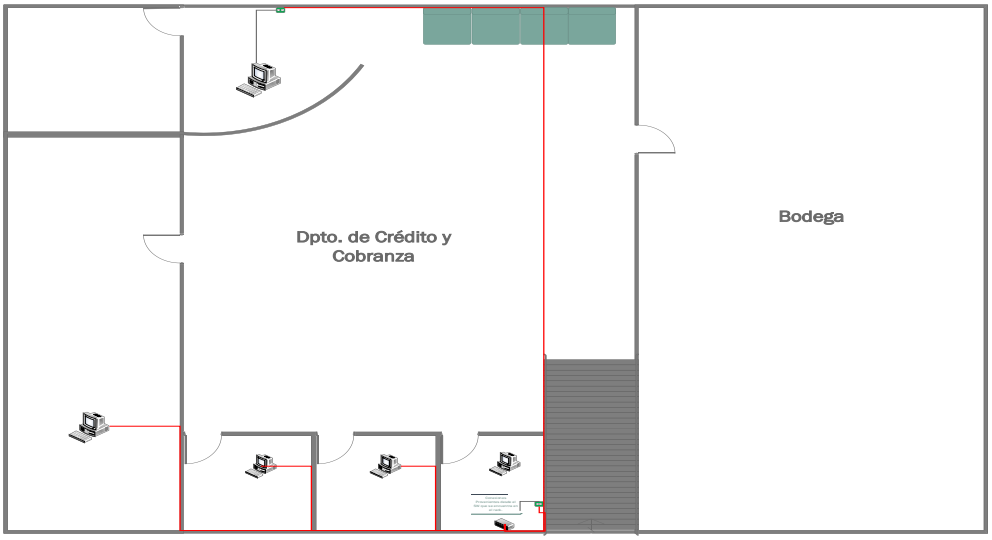

Fig. 16 Subsuelo
Elaborado por: El Investigador

Organigrama Estructural

Realizada la revisión de las funciones requeridas para el desempeño de las actividades de la cooperativa, se ha sintetizado la estructura organizacional de la entidad.

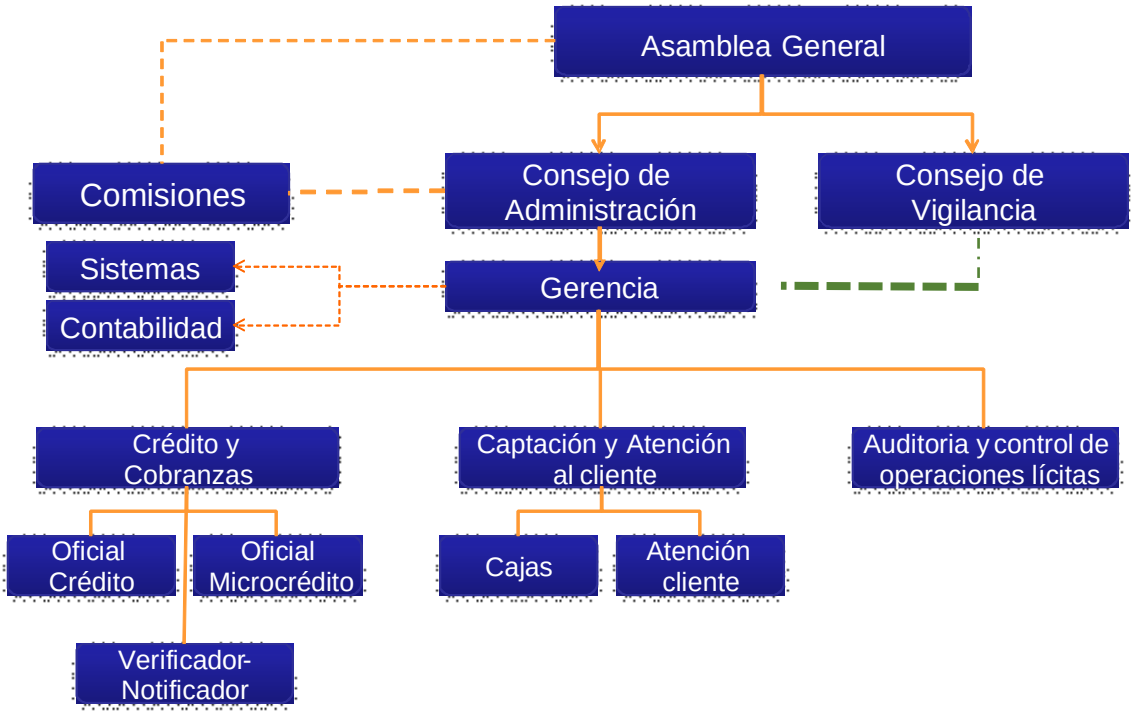

Fig. 17 Estructura Organizacional
Fuente: Gerencia

4.2.2 Alcance

Identificada cada una de las funciones y procesos que se llevan a cabo en la cooperativa [ANEXO A] es necesario establecer el alcance al que se va a aplicar de acuerdo al diseño del sistema de gestión de seguridad de la información, el cual está enfocado a la red de datos de la cooperativa.

Se instaurará políticas para las mejores prácticas de la utilización de la red y todos los dispositivos que interactúan en la misma, así también, se establecerá mecanismos de protección y un nuevo diseño del diagrama de red utilizando los mismos.

4.2.3 Análisis de la situación actual de la red de datos de la cooperativa

Se detalla la infraestructura de red que se utiliza actualmente en la cooperativa, con la información obtenida en colaboración del encargado del Departamento de sistemas quien es el encargado de administrar la red, además se contará con un inventario realizado y la revisión de las instalaciones físicas.

Con todo lo recolectado se podrá realizar un análisis sobre la situación actual que presenta la red de datos concerniente a la seguridad para determinar la mejor manera de implementación de un Sistema de Gestión de seguridad.

4.2.4 Estructura de la red LAN de la cooperativa

La infraestructura de red con la que cuenta la cooperativa está conformada de la siguiente manera:

Tabla 5. Recurso de Red

Activos Informáticos	Tipos	Cantidad
Servidores físicos (Hardware)	Servicio	3
Servidores virtuales (KVM)	Servicio	1
Máquinas Virtuales (Software)	Servicio	4

Dominios	Servicio	0
Nodos de red	Servicio	19
Equipos Windows XP	Servicio	7
Equipos Windows 7	Servicio	8
Equipos de Computo Linux	Servicio	2
Portátiles	Servicio	1
Router	Comunicaciones	4
Switch	Comunicaciones	3
Firewall	Comunicaciones	0
Printserver	Comunicaciones	0
IDS	Comunicaciones	0
Sensores de red	Comunicaciones	0
UPS	Comunicaciones	2
Reguladores	Comunicaciones	8
Rack	Comunicaciones	1
Página web de la institución	Comunicaciones	0
Servidores Web otros	Comunicaciones	0
Servidores de correo	Comunicaciones	1
Antispam en servidor de correo	Comunicaciones	1
Servidores de base de datos	Comunicaciones	2
Servidores hotspot	Comunicaciones	0
Conexiones a internet	Comunicaciones	1
Servidores NAS/SAN	Comunicaciones	3
VPN hacia la red interna	Comunicaciones	0
VPN hacia otras entidades	Comunicaciones	1
Cámaras de Vigilancia	Monitoreo	10
Personal de Seguridad	Vigilancia perimetral	1
Cifrado en medios de almacenamiento	Equipos personales críticos	0
Recursos humanos	Personal	17

Elaborado por: El Investigador

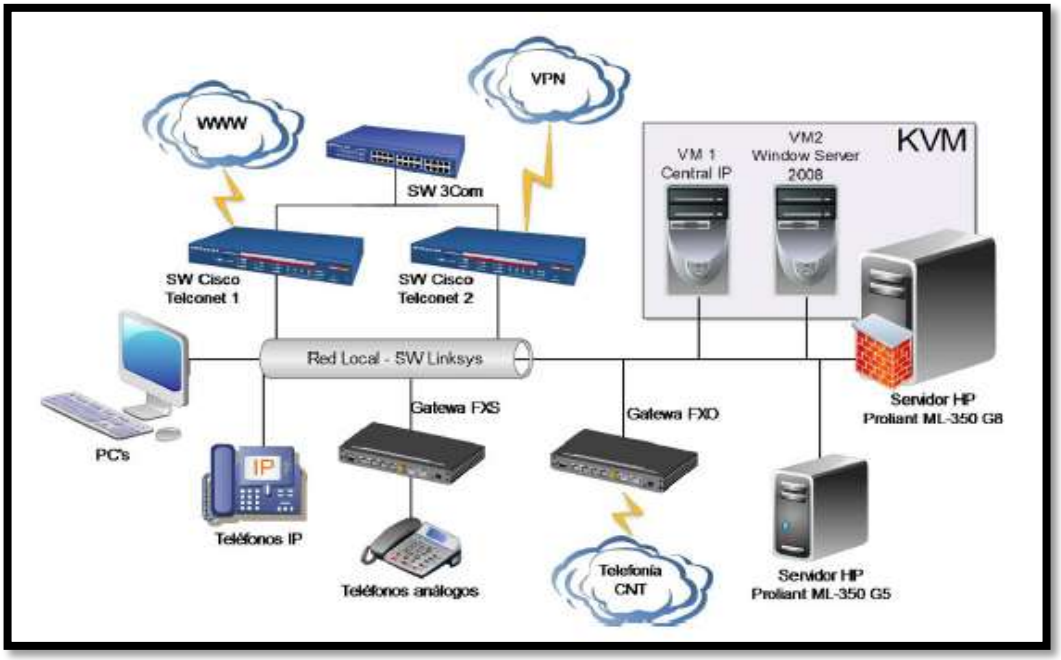

Fig. 18 Red LAN de la cooperativa
Fuente: Telconet

Detalle de Servidores

- Servidor HP ProLiant ML350 G5
  - Procesador Intel Xeon Quad Core 2.50 Ghz
  - Memoria
  - Almacenamiento 5TB
  - Sistema Operativo Windows Server 2003

- Servidor HP ProLiant ML350p Gen8
  - Procesador Intel® Xeon® E5-2600
  - Memoria, máxima 768 GB
  - Almacenamiento 5Tb
  - Sistema Operativo Centos 5
  - Virtualización (Windows Server 2012, Centos 6.4)

- Computador HP ProDesk 400 G1
  - Procesador Intel Core i3-4130 3.4Ghz
  - Memoria 4Gb

- Disco duro 500 Gb
- Sistema Operativo Centos 6.4

Los sistemas operativos y su versión

La cooperativa cuenta con Licencia de los siguientes sistemas operativos:

- Windows Server 2003 Standard
- Windows Server 2012 Standard
- Windows 8 Professional
- Windows 7 Professional
- Windows XP Professional Sp3
- Centos 6.4

Detalle de la estaciones de Trabajo

Las estaciones de trabajo de la cooperativa cuentan con diferentes características, ya que han sido adquiridas en diferentes temporadas. [ANEXO B]

En la actualidad la red LAN no cuenta mecanismos de seguridad informática, que permita el correcto control y administración de la misma, mediante herramientas que permitan el monitoreo, seguridad y administración de la red.

4.2.5 Estructura de la red WAN de la cooperativa

La cooperativa cuenta con dos enlaces, el primero es el que provee de Internet y un segundo que permite la conexión con la agencia y sucursal para la transmisión de los datos del sistema financiero que se utiliza.

Tabla 6. Cuadro de enlaces

DESCRIPCION	BW	UM	CISCO	WAN	LAN
COOPERATIVA DE AHORRO Y CREDITO UNION POPULAR LTDA - MATRIZ INTERNET	2048 Kbps	Fibra Optica	2611	186.3.60.38	186.3.45.97/29
COOPERATIVA DE AHORRO Y CREDITO UNION POPULAR LTDA - MATRIZ	1024 Kbps	Fibra Optica	2611XM	10.23.150.146	192.168.0.199/24
COOPERATIVA DE AHORRO Y CREDITO UNION POPULAR LTDA - AGENCIA MAYORISTA	512 Kbps	Fibra Optica	2611	10.23.150.147	192.168.2.199/24
COOPERATIVA DE AHORRO Y CREDITO UNION POPULAR LTDA - AGENCIA PAYAMINO	512 Kbps	Fibra Optica	2611	10.23.150.148	192.168.1.199/24

Elaborado por: Telconet

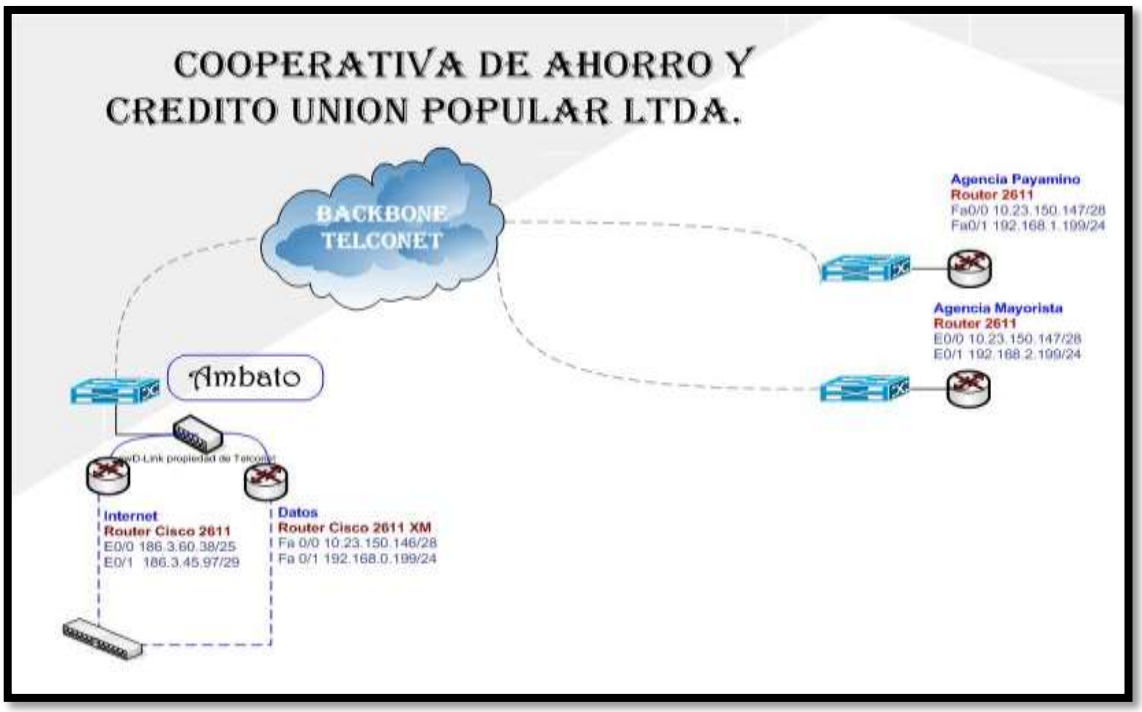

Fig. 19. Diagrama de red WAN de la cooperativa
Elaborado por: Telconet

4.2.6 Situación Actual de la Seguridad Informática

Para tener un mejor conocimiento acerca de toda la infraestructura de la red y las seguridades que se manejan en la actualidad, se ha realizado un análisis para establecer el nivel de seguridad con el que cuenta la cooperativa para proteger su recurso tecnológico, este se ha basado en la entrevista que se realizó al personal encargado del Departamento de Sistemas. [ANEXO C]

4.2.6.1 Seguridad de las comunicaciones

Antivirus

La cooperativa adquirió a principios del presente año 16 licencias corporativas del antivirus NOD32, el cual está instalado en todas las estaciones de trabajo y servidores. Las actualizaciones del antivirus se realizan automáticamente por medio del internet.

Se han presentado inconvenientes en algunas estaciones de trabajo por contagio de virus ocasionadas por dispositivos extraíbles y descargas de internet.

No se realizan escaneos habituales en busca de infecciones en los servidores ni estaciones de trabajo, ni se ha establecido un responsable para la realización de este procedimiento, salvo estos presenten problemas y sean notificados al departamentos de sistemas.

Ataques de red

Se ha podido constatar que no existen herramientas para prevenir y combatir los ataques de red, hasta el momento no se han presentado ningún tipo de inconvenientes detectados.

Contraseñas

Actualmente las únicas contraseñas que se manejan en la institución son las que se

utilizan para acceder al sistema financiero que utiliza la cooperativa, estas se almacena en el motor de la base de datos SQL 2008 cuya configuración encripta los datos que se almacenan en ella.

El Administrador del sistema es el único autorizado a acceder a la información de la base de datos.

Cabe destacar que para el acceso a las estaciones de trabajo no se maneja de manera obligatoria el uso de las contraseñas, ya que se observó que no en todas las computadoras se establece su uso mediante el acceso con contraseña.

4.2.6.2 Seguridad de las Aplicaciones

Seguridad de Base de datos

La cooperativa utiliza el motor de base de datos SQL 2008, el cual cuenta con su respectiva licencia, el mismo se utiliza para el almacenamiento y administración de los datos de las transacciones a tiempo real que se realizan a diario al ser una institución financiera. Dado su origen propietario cuenta con las seguridades propias del motor de la base de datos.

La base de datos es utilizada para el manejo del aplicativo financiero elaborado para los diferentes procesos que realiza la cooperativa.

El acceso a esta aplicación, se lo realiza por medio de su módulo de administración, el cual consiste en el registro de los usuarios con sus permisos asignados para la utilización del sistema informático.

El administrador del sistema es el único que tiene acceso a la información de la base de datos y a su infraestructura física, es decir los servidores donde se acentúa la base de datos.

Control de Aplicaciones

En la mayoría de las computadoras se encuentra configurado dos tipos de usuario, el primero administrador el cual tiene la potestad de instalar programas en el computador, y el segundo usuario quien no cuenta con privilegios de instalación de programas.
No existe ningún tipo de documentación acerca de los procesos a seguir para la instalación, configuración y actualización de aplicaciones en los computadores. Las instalaciones que se realizan son básicas y no tienen seguimiento de las aplicaciones que se han instalado.

Aplicaciones instaladas:

- Internet Explorer
- Antivirus (NOD32)
- Microsoft Office 2013 Home and Business Edition
- Adobe Reader
- Open Office
- Winrar

Cabe destacar que se cuenta con 5 licencias de Microsoft Office 2013, las cuales están instaladas en las computadoras de Gerencia, Contabilidad, Sistemas, Información; el resto de computadores funcionan con Open Office.

Con respecto a los servidores no se cuenta con documentación con fecha acerca de aplicaciones instaladas, configuradas y actualizadas, tampoco se tiene copias de seguridad cada vez que se realiza algún cambio.

4.2.6.3 Seguridad Física

Acceso al cuarto de servidores

La cooperativa al momento de establecerse en su edificio matriz, no tomó en consideración la adecuación adecuada del cuarto de servidores ni la protección al acceso

al mismo.

El cuarto de servidores se encuentra ubicado en el tercer piso, en un pequeño cuarto junto al graderío que conecta al cuarto piso, permanece cerrada con llave, la cual tiene el jefe del departamento de sistemas, la puerta no es la adecuada para el cuarto ya que permite observar desde el exterior los servidores. Cabe destacar que no existe ningún otro de seguridad ni control de acceso al cuarto.

Fig. 20 Puerta de Acceso al Cuarto de Servidores

Control de acceso a los equipos

El acceso a los equipos puede realizarse por medio de dispositivos externos como memorias usb, lectores de discos ópticos, ya que estos se encuentran activados y no existe control de los mismos, está habilitada su reproducción automática lo que puede propagar programas maliciosos. Cabe destacar que no se ha presentado robo de datos usando medios externos que se conozca.

No se realiza inspeccione periódicas de los equipos una vez que han sido instalados y puestos en funcionamiento, solo se los revisa ante fallos detectados o reportados por los usuarios.

Estructura del edificio

Al construir el edificio propio de la cooperativa, no se puso atención a los requerimientos que debe tener un cuarto de datos. Podemos mencionar que en base a

estándares a cumplir el cuarto de servidores se encuentra ubicado de manera correcta en el tercer piso del edificio.

La estructura de las paredes del cuanto de servidores es el mismo que todo el edificio, cuenta con una puerta de acceso tipo reja para el acceso.

La edificación cuenta con cableado estructurado 4e en sus instalaciones antiguas y 5e en los nuevos puntos de red establecidos en el último año, la administración física de la red dado el crecimiento de la cooperativa ha incrementado la dificultad en la administración de la misma, además se puede añadir que el cableado eléctrico y el de datos se encuentran unidos.

Dispositivos de Soporte

Los dispositivos de soporte son los activos que ayudan a un correcto funcionamiento de los equipos de cómputo.

La cooperativa cuenta con los siguientes equipos de soporte:

- UPS: En el cuarto de datos se cuenta con dos, los cuales dan media hora ante fallas eléctricas para poder apagar los equipos de manera correcta.
-

Fig. 21 UPS TripLite

Fig. 22 UPS APC

Podemos mencionar que no se cuenta con suficiente reguladores para las estaciones de trabajo, así también inexistencia de un correcto sistema de aire acondicionado para el cuarto de servidores.

Cableado Estructurado

La instalación del cableado fue tercerizada y se implementó un cableado estructurado, se ha podido observar que el cableado comparte su alojamiento en ciertas partes del edificio con las conexiones eléctricas que unen los pisos.

Fig. 23 Instalaciones Eléctricas (Parte posterior del rack)

Fig. 24 Puntos Finales de las instalaciones

El cableado está estructurado por canaletas que se ubican en los contornos de las paredes por donde tienen que pasar los cables. Estas canaletas a la hora de realizar modificaciones en el cableado no son prácticas, debido al aumento de cables que tienen que pasar por ellas y el escaso espacio que ellas ofrecen.

4.2.6.4 Administración del centro de procesamiento de datos

Responsabilidad del Departamento de Sistemas

En la cooperativa existe una sola persona encargada de las TI, quien es encargado de realizar varias tareas correspondientes a la administración de la tecnología, no hay un encargado de la seguridad.

El jefe de sistemas es el que administra el sistema y la infraestructura, es el encargado de reportar al gerente acerca de cada una de las actividades del departamento.

Mantenimiento

- Para la resolución de inconvenientes de los equipos tecnológicos que informan los usuarios, estos se comunica telefónicamente al departamento de sistemas a pedir asesoría o el servicio correspondiente de acuerdo al inconveniente presentado. No se registra ninguna documentación.
- El mantenimiento preventivo a los equipos de cómputo es programado, pero existen ocasiones que no se cumple ya que al existir solo una persona encargada de las TI de la cooperativa, este tiene que resolver problemas de mayor importancia, por lo que el mantenimiento se pospone.
- Actualmente no existe un inventario con su respectivo etiquetado de activos (dispositivos tecnológicos, programas con licencia).

Instaladores

Hasta la fecha se encuentran con licencia los dos servidores con Windows Server 2003

y 2012 y 14 estaciones de trabajo se encuentran con licencia Windows 7, los restantes tres equipos se encuentran con Sistema Operativo Windows XP pero no cuentan con licencia.

Respaldos

- *Respaldos de datos en los servidores:*
  Se guardan respaldos de la información que genera el motor de base de datos que utiliza el sistema financiero en un disco externo estos se los realizan diariamente.
  No se documenta ni se realiza respaldos de configuraciones ejecutadas a los servidores.
- *Respaldos de datos de los computadores.*
  De acuerdo a lo observado cada uno de los usuarios deben realizar sus respaldos, y como la información es de propiedad de la cooperativa se debe almacenar en el propio computador en una partición secundaria del disco duro realizada en el mismo.

Documentación

En la cooperativa no existe ningún tipo de documentación acerca de los recursos ni configuraciones realizadas o a realizar en los equipos, así también se carece de manuales de políticas y procedimientos a cumplir dentro de las actividades del departamento.

Cabe destacar que se pudo constatar que existe documentación acerca de los cambios que se realizan en el sistema informático financiero y en la base de datos.

4.2.7 Análisis de amenazas y vulnerabilidades en los servicios de la red de datos.

Para esta fase contamos con la información recaudada de los activos expuestos e históricos de actividades concluidos en la entrevista realizada [ANEXO C], además que

se realizó escaneo de puertos.

4.2.7.1 Identificación de Amenazas y Vulnerabilidades

Se pudieron determinar las amenazas en base al **Paso 2 "Identificación de amenazas",** con las cuales se pudo llegar a la determinación de las vulnerabilidades definidas en el **Paso 3 "Identificación de vulnerabilidades"** definido en NIST 800-30.

Tabla 7. Identificación de vulnerabilidades (Amenaza Usuarios Locales)

Amenaza	Vulnerabilidad
Humanas (Usuarios Internos)	Inexistencia o falta de :
Malintencionados **Inexpertos** **Negligentes** **Deshonestos**	*Identificación con credencial del personal que ingresa a la entidad*
	Controles de acceso físicos a oficinas.
	Bitácoras para visitantes en los departamentos.
	Controles de acceso a aplicaciones.
	Controles de acceso a servidores y equipos activos.
	Control de acceso a computadoras.
	Control de asignación de direcciones IP's en la entidad.
	Control de tráfico de red.
	Mecanismos de control perimetral de la red.
	Personal que atienda un incidente de seguridad.
	Políticas de confidencialidad.
	Políticas de uso de la red.
	Políticas sobre el manejo de información.
	Políticas de seguridad en sistemas operativos.
	Políticas de seguridad en servidores.
	Políticas de seguridad en dispositivos activos.
	Políticas de contraseñas.
	Conocimientos de empleados en temas de seguridad.
	Actualización de firmware en equipos de red.
	Actualizaciones en los sistemas operativos y aplicaciones.
	Actualización en antivirus.
	Mantenimiento en servidores y equipo de telecomunicación.
	Mantenimiento preventivo en equipos de cómputo.

	Mantenimiento a estaciones eléctricas.
	Corriente eléctrica regulada.
	Cifrado en discos duros.
	Respaldos de información.
	Respaldos de configuración de equipos activos
	UPS con capacidad suficiente.
	Fuente de corriente eléctrica alterna.
	Capacitación.
	Separación de funciones de los empleados.
	Información en temas de seguridad.
	Tableros eléctricos expuestos.
	Fallas eléctricas.
	Fallas en equipos de cómputo.
	Límites de uso de memoria y procesador en servidor.
	Cableado de red expuesto a los usuarios.
	Respaldos en USB sin cifrado.
	Respaldos en mismo disco duro.
	Acceso a todas las terminales de administración.
	Acceso a todos los recursos de red.
	Acceso total a todos los recursos de Internet.
	Tiempo de vida útil de un equipo.
	Uso de la misma contraseña por periodos largos de tiempo.
	Uso de una contraseña única en varios equipos.
	Uso de contraseñas no robustas.
	Uso de protocolos de administración inseguros.
	Descuidos del personal que labora en la institución.
	Confianza en otras personas.
	Uso de IP homologadas para usuarios en general.
	Fallas por parte del proveedor del servicio de internet.
	Fallas por parte del proveedor suministro eléctrico.

Elaborado por: El investigador

Tabla 8. Identificación de vulnerabilidades (Amenaza Usuarios Externos)

Amenaza	Vulnerabilidad
Humanas (Usuarios externos)	Falta de :
Delincuencia Hacker	*Identificación con credencial del personal que ingresa a la entidad.*
	Controles de acceso físicos a oficinas.
Crackers Ex-empleados Otros	*Bitácoras para visitantes en los departamentos.*
	Controles de acceso a aplicaciones.
	Controles de acceso a servidores y equipos activos.
	Control de acceso a computadoras.
	Control de asignación de direcciones IP's en el segmento de la entidad.
	Control de tráfico de red.
	Control de acceso en la red inalámbrica.
	Mecanismos de control perimetral de la red.
	Personal que atienda un incidente de seguridad.
	Políticas de confidencialidad.
	Políticas de uso de la red.
	Políticas sobre el manejo de información.
	Políticas de seguridad en sistemas operativos.
	Políticas de seguridad en servidores.
	Políticas de seguridad en dispositivos activos.
	Políticas de contraseñas.
	Conocimientos de empleados en temas de seguridad.
	Actualización de firmware en equipos de red.
	Actualizaciones en los sistemas operativos y aplicaciones.
	Actualización en antivirus.
	Mantenimiento en servidores y equipo de telecomunicación.
	Mantenimiento preventivo en equipos de cómputo.

	Mantenimiento a estaciones eléctricas.
	Corriente eléctrica regulada.
	Cifrado en discos duros.
	Respaldos de información.
	Respaldos de configuración de equipos activos
	UPS con capacidad suficiente.
	Fuente de corriente eléctrica alterna.
	Capacitación.
	Información en temas de seguridad.
	Separación de funciones de los empleados.
	Tableros eléctricos expuestos.
	Límites de uso de memoria y procesador en servidor.
	Cableado de red expuesto a los usuarios.
	Respaldos en USB sin cifrado.
	Respaldos en mismo disco duro.
	Acceso a todas las terminales de administración.
	Acceso a todos los recursos de red.
	Acceso total a todos los recursos de Internet.
	Uso de la misma contraseña por periodos largos de tiempo.
	Uso de una contraseña única en varios equipos.
	Uso de contraseñas no robustas.
	Uso de protocolos de administración inseguros.
	Descuidos del personal que labora en la institución.
	Confianza en otras personas.
	Uso de IP homologadas para usuarios en general.
	Fallas por parte del proveedor del servicio de internet.
	Fallas por parte del proveedor suministro eléctrico.

Elaborado por: El investigador

Tabla 9. Identificación de vulnerabilidades (Desastres Naturales)

Amenaza	Vulnerabilidad
Desastres Naturales	Falta de:
	Planeación relacionada con la infraestructura de la organización.
	Impermeabilizado.
	Mantenimiento en cableado eléctrico.
	Controles de humedad.
	Controles de temperatura.
	Fallas en diseño construcción del edificio.
	Tableros eléctricos expuestos.
	Instalación de red expuesta.
	Equipos de telecomunicaciones expuestos.

Elaborado por: El investigador

Tabla 10. Identificación de vulnerabilidades (Amenazas Lógicas)

Amenaza	Vulnerabilidad
Amenazas Lógicas	Falta de :
Virus **Gusanos** **Troyanos** **Spyware** **Malware** **Otros**	Dispositivos de seguridad perimetral.
	Actualización en software.
	Actualización en sistemas operativos.
	Actualización en firmware de dispositivos.
	Políticas de confidencialidad.
	Políticas de uso de la red.
	Políticas sobre el manejo de información.
	Políticas de seguridad en sistemas operativos.
	Políticas de seguridad en servidores Windows /Linux.
	Políticas de seguridad en dispositivos activos.
	Políticas de contraseñas.

	Políticas de desarrollo de software seguro.
	URL con software malicioso.
	Descarga de ejecutables desde sitios no confiables.
	Instalación de software pirata.
	Instalación de software crackeado.
	Descarga de software de recursos peer to peer (P2P).
	Configuración por default.
	Auto arranque de dispositivos extraíbles en terminales y servidores.
	Debilidades en los protocolos de comunicación.
	Errores de configuración de los sistemas.
	Mecanismos de administración remota vulnerables.
	Contraseñas basadas en palabras de diccionario.
	Vulnerabilidades de las versiones empleadas en los servidores.
	Ataques conocidos a sistemas operativos.
	Puertos abiertos sin utilización.
	Falta de conocimiento en temas de seguridad.

Elaborado por: El investigador

Con la realización de la identificación de amenazas y vulnerabilidades mediante la metodología NIST se pudo observar lo siguiente:

- Se pudo constatar que las contraseñas utilizadas para el acceso a las estaciones de trabajo no son seguras, ya que no cuentan con el cumplimiento de políticas de seguridad básicos; lo que debilita la seguridad, además de utilizar protocolos de administración inseguros, lo que en conjunto crea un punto crítico de seguridad.
- Se realizó escaneos desde el interior de la institución los cuales mostraron un número considerable de puertos abiertos que no son utilizados, por lo que pueden ser blanco fácil de ataques directamente a los servidores y atentar contra la seguridad de la información. Así mismo se pudo observar que una de las empresas que ha prestado servicios a los servidores ha habilitado un puerto del switch para poder dar servicio de manera remota, siendo esto un punto de alta

criticidad, ya que puede ser utilizado por terceros para acceder a la red de la cooperativa. [ANEXO D]

- Dentro del área de TI de la cooperativa no se cuenta con la documentación necesaria de las configuraciones realizadas y de los activos con los que cuenta.
- Los equipos de telecomunicaciones no han tenido un control ni programa de mantenimiento preventivo, ya que al ya no contar con garantía del proveedor se hace muy necesario para resguardar los mismos ante daños y evitar así cortes de los servicios que estos prestan.
- Actualmente la cooperativa ha ido creciendo, por lo que ha sido necesario el incremento de puntos de red, los cuales se han realizado de manera improvisada, además no se cuenta con la correcta identificación de cada uno de los puntos de red que se tienen, por lo que si se presentan fallos a causa de la red no se conocerá el punto exacto del problema de manera rápida y salvaguardar de esta manera el acceso físico a los medios de transmisión de datos.

Fig. 25 Instalaciones improvisadas de red

- La cooperativa no cuenta con ningún esquema ni equipos de seguridad, así mismo no se realiza monitoreo de la red, por lo que puede permitir a los atacantes tener acceso a los puntos de conexión, tales como los servidores y los activos de TI. Es necesario establecer un esquema de seguridad que permita monitorear el uso de la red con mayor detalle y establecer políticas de acceso sólo a aquellos recursos que deben estar visibles para los usuarios finales.
- En cuanto a las conexiones eléctricas, se pudo observar que las conexiones que se encuentran el cuarto de datos no están en las mejores condiciones por lo que

pueden ocasionar fallos en la electricidad y provocar daños a los equipos; cabe mencionar que la cooperativa cuenta con un UPS el cual resguarda solo a los servidores de dichos fallos.

- La instalación y configuración de los equipos de cómputo de los usuarios finales, se lo realiza cada vez que se presenten daños en su lógica o en su hardware, no se realizan mantenimientos preventivos y no se cuenta con políticas de instalación de software, así también no se lleva el control del personal que tiene acceso a los equipos ni si se utilizan solo para realizar lo pertinente a la cooperativa.

4.2.7.2 Nivel de Atención de Riegos

Para obtener la probabilidad de *ocurrencia y análisis de impacto, paso 5 y 6* de la metodología utilizada, se determina con base a las entrevistas, revisión de instalaciones y decisiones gerenciales la prioridad de atención de los riesgos.

La estimación del impacto se lo realizará de manera cualitativa, se consideró un activo importante con base en el tipo de información que maneja; el hecho de pérdida de disponibilidad, confidencial o integridad del activo afecta considerablemente con el trabajo de la cooperativa.

Tabla 11. Nivel de Atención de Riesgos

		Probabilidad		
		Alto (1.0)	Medio (0.5)	Bajo (0.1)
Impacto	Alto (100)	Alto (100x1)	Medio (100x0.5)	Bajo (100x0.1)
	Medio (50)	Medio (50x1)	Medio (50x0.5)	Bajo (50x0.1)
	Bajo (10)	Medio (10x1)	Bajo (0.16)	Bajo (0.08)

Alto (>50 a 100); Medio (>10 a 50); Bajo (1 a 10)

Elaborado por: Metodología NIST

Alto: se requiere fuertemente la necesidad de tomar acciones correctivas.

Medio: acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un periodo de tiempo.

Bajo: se observó un bajo riesgo y se deberá determinar si se tomarán acciones correctivas o decidir aceptar el riesgo.

Tabla 12 Probabilidad de Impacto y Ocurrencia

Vulnerabilidad	*Probabilidad de ocurrencia*	*Impacto*	*Principio de seguridad infectado*	*Nivel de Atención de Riesgo*
Red inalámbrica abierta.	Alta	Alto	Confidencialidad	Alto
Inexistencia de controles sobre el uso de la red inalámbrica.	Media	Alto	Disponibilidad	Alto
Poco control en la administración de direcciones IP.	Media	Alto	Disponibilidad	Alto
Inexistencia de control en la Información descargada a través de la red de la institución.	Alta	Alto	Integridad	Alto
Falta de cuidado del equipo de cómputo.	Alta	Alto	Disponibilidad	Alto
Limitantes de potencia en UPS.	Alta	Alto	Disponibilidad	Alto
Falta de mecanismos de control perimetral de la red.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto

Uso de protocolos de administración inseguros.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Inexistencia de políticas de uso de red.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Inexistencia de políticas para servidores.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Inexistencia de respaldos en equipos activos.	Alta	Alto	Integridad	Alto
Acceso a todos los recursos de red institucional.	Media	Alto	Confidencialidad Disponibilidad Integridad	Alto
Uso de una misma contraseña por periodos largos de tiempo.	Media	Alto	Confidencialidad Disponibilidad Integridad	Alto
Uso de una contraseña única en varios equipos.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Uso de contraseñas no robustas.	Media	Alto	Confidencialidad Disponibilidad Integridad	Alto
Confianza en otras personas.	Media	Alto	Confidencialidad	Alto
Uso de IP's homologadas para usuarios en general.	Media	Alto	Confidencialidad	Alto
Fallas por parte del proveedor del suministro eléctrico.	Alta	Alto	Disponibilidad	Alto
Puertos abiertos sin uso en estación de	Alta	Alto	Confidencialidad Disponibilidad	Alto

trabajo.			Integridad	
Daños en la configuración de los equipos por poco mantenimiento.	Alta	Alto	Disponibilidad	Alto
Inexistencia de procedimientos de cambios en sistemas.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Inexistencia de cifrado en discos duros.	Alta	Alto	Confidencialidad Disponibilidad Integridad	Alto
Tableros eléctricos expuestos.	Medio	Medio	Disponibilidad	Medio
Controles de acceso físicos, inseguros para administración de servidores.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Vulnerabilidades en el protocolo TCP/IP.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Daño en hardware por fallas eléctricas.	Media	Medio	Disponibilidad	Medio
Inexistencia de control en el tráfico de red generado por la institución.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Fuga de información.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Daño físico a la infraestructura de red.	Media	Medio	Disponibilidad	Medio
Inexistencia de controles de seguridad en	Media	Medio	Confidencialidad	Medio

portátiles.				
Inexistencia de monitoreo de uso de la red.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Inexistencia en sistemas de aire acondicionado.	Media	Medio	Disponibilidad	Medio
Control de acceso débil en aplicaciones.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Personal poco capacitado en temas de seguridad.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Falta de mantenimiento preventivo en servidores y equipos activos.	Media	Medio	Disponibilidad	Medio
Falta de mantenimiento de estaciones Eléctricas.	Alta	Medio	Disponibilidad	Medio
Falta de corriente eléctrica regulada.	Alta	Medio	Disponibilidad	Medio
Inexistencia de fuente de corriente eléctrica alterna.	Alta	Medio	Disponibilidad	Medio
Cableado de red	Media	Medio	Disponibilidad	Medio

expuesto.				
Respaldos en mismo disco duro.	Media	Medio	Disponibilidad	Medio
Parámetros por default en equipos activos.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Acceso a todas las terminales de administración.	Media	Medio	Integridad	Medio
Acceso a todos los recursos de internet.	Bajo	Medio	Confidencialidad Disponibilidad Integridad	Medio
Uso de protocolos de comunicación inseguros.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Falta de mantenimiento en cableado eléctrico.	Alta	Medio	Disponibilidad	Medio
Consultas de sitios con software malicioso.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Descarga de ejecutables de sitios no confiables.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Inexistencia de políticas sobre el uso del equipo de cómputo.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Autoarranque de dispositivos extraíbles.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Inexistencia de controles de integridad en equipos activos.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio

Inexistencia de políticas de uso de software.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Falta de procedimientos de creación de cuentas.	Alta	Medio	Disponibilidad	Medio
Vulnerabilidades inherentes a las aplicaciones.	Alta	Medio	Disponibilidad	Medio
Uso de versiones viejas en aplicaciones.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Vulnerabilidades conocidas en sistemas operativos.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Fallas eléctricas.	Alta	Medio	Disponibilidad	Medio
Inexistencia de cultura de seguridad en usuarios finales.	Alta	Medio	Confidencialidad Disponibilidad Integridad	Medio
Poca separación de funciones críticas.	Media	Medio	Confidencialidad Disponibilidad Integridad	Medio
Fallas por parte del proveedor de servicios de internet.	Media	Medio	Disponibilidad	Medio
Inexistencia de monitoreo de las aplicaciones.	Alta	Medio	Disponibilidad	Medio
Errores de cambios en la configuración de equipos activos y servidores.	Media	Bajo	Integridad	Medio
Desastres naturales en la institución.	Baja	Bajo	Disponibilidad	Bajo

Elaborado por: El Investigador

Una vez realizado el levantamiento de activos, amenazas, vulnerabilidades, probabilidad de ocurrencia e impacto, se realiza una evaluación de los riesgos para priorizar los niveles de atención, las opciones de los riesgos son:

- Mitigación del riesgo; implementando controles que reduzcan la probabilidad de ocurrencia.
- Transferir el riesgo; con base en el análisis de riesgo contemplar la posibilidad de que algunos controles sean realizados por terceros (outsourcing), en algunas veces reduce costos.
- Aceptar el riesgo; tener conocimiento de los riesgos a los que se está expuesto, aceptando la posibilidad de que se presenten.
- Evitar el riesgo; las acciones están orientadas a cambiar las actividades o la manera de desempeñar una actividad en particular
- Riesgo residual; después de implantar los controles necesarios para el tratamiento de los riesgos, por lo general se encuentran remanentes. Lo que se conoce como riesgo residual. [13]

4.3 DISEÑO DE LA SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS DE LA COOPERATIVA

En base a lo analizado en el punto 4.2, se ha podido determinar los puntos débiles de la seguridad informática en la cooperativa, con esta información es posible realizar un adecuado diseño de seguridad.

A continuación se muestra el desarrollo del diseño utilizando la ISO 27001 (Sistema de Gestión de Seguridad de la Información) conjuntamente con la Metodología NIST que se utilizó para el análisis de vulnerabilidades y riegos.

4.3.1Alcance y requerimientos de la propuesta

Para establecer un adecuado diseño de seguridad para la red de datos de la cooperativa se establecerá controles de seguridad que pueden mitigar o eliminar las vulnerabilidades

los mismos que serán señalados para su implementación o planeación, estos ayudarán a reducir los niveles de riesgo de seguridad dentro de la cooperativa.

Se determinó con aprobación del Departamento de Sistemas que vulnerabilidades tratar; se acordó implementar en el presente proyecto los siguientes mecanismos de seguridad siendo estos esenciales para resguardar el flujo de información:

Esquema de seguridad perimetral

- ✓ 1 Firewall Perimetral; Éste delimitará la salida hacia el exterior (Internet) estableciendo reglas de filtrado apegadas a los requerimientos de servicio.
- ✓ 1 IDS Perimetral; A la fecha de entrega del proyecto, se lo configurará en el mismo servidor del firewall, por falta de recursos.
- ✓ 1 Servidor Proxy; El mismo que contendrá reglas de filtrado para el internet de acuerdo a políticas de uso del internet en la cooperativa.
- ✓ 1 Servidor de Directorio Activo, para el control de los usuarios de la cooperativa.

Además se tendrá como resultado controles para la elaboración un Sistema de Gestión de Seguridad de la Información. Cabe destacar que el proyecto presentó restricciones, no todas de carácter técnico que establecen un marco al que debe limitarse, éste contempla decisiones gerenciales y/o mecánicas de trabajo, por ejemplo:

- La cantidad de recursos asignados.
- La forma de planificar el gasto y de ejecutar el presupuesto. En este punto se aprovecharon los recursos con los que cuenta la institución, contemplado gastos mínimos.
- La cultura o forma interna de trabajo puede ser incompatible con ciertos controles.
- Rechazo de controles, por el personal de la institución.

4.3.2 Mecanismos y Controles de Seguridad

A continuación se presenta el siguiente punto de la metodología utilizada: **Paso 4: "Análisis de los controles"**, mostrando una lista de controles con los que se cuenta actualmente y aquellos que se planifican a futuro, para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad.

Tabla 13. Controles de Seguridad

Vulnerabilidad	*Nivel de riesgo*	*Control sugerido*
Red inalámbrica abierta.	Alto	Hotspot.
Inexistencia de controles sobre el uso de la red inalámbrica.	Alto	Hotspot, servidor Radius, cifrado.
Poco control en la administración de direcciones IP.	Alto	Inventario de asignación de direcciones IP.
Inexistencia de control en la Información descargada a través de la red de la institución.	Alto	Firewall, filtrado de contenido (Proxy).
Falta de cuidado del equipo de cómputo.	Alto	Concientización en temas de seguridad.
Limitantes de potencia en UPS.	Alto	Evaluación y adquisición de un UPS.
Falta de mecanismos de control perimetral de la red.	Alto	Firewall, IDS, gestor de uso de red.
Uso de protocolos de administración inseguros.	Alto	Políticas de configuración de equipos activos.
Inexistencia de políticas de uso de red.	Alto	Elaboración de políticas de uso de red.
Inexistencia de políticas para servidores.	Alto	Elaboración de políticas para servidores.

Inexistencia de respaldos en equipos activos.	Alto	Elaboración de políticas de respaldo.
Acceso a todos los recursos de red institucional.	Alto	Firewall perimetral, firewall local de servidores, vlan's, NAT's.
Uso de una misma contraseña por periodos largos de tiempo.	Alto	Políticas de contraseñas.
Uso de una contraseña única en varios equipos.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Uso de contraseñas no robustas.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Confianza en otras personas.	Alto	Concientización en temas de seguridad.
Uso de IP's homologadas para usuarios en general.	Alto	Vlan, NAT.
Fallas por parte del proveedor del suministro eléctrico.	Alto	
Puertos abiertos sin uso en estación de trabajo.	Alto	Políticas de hardening en estaciones de trabajo.
Daños en la configuración de los equipos por poco mantenimiento.	Alto	Mantenimiento preventivo.
Inexistencia de procedimientos de cambios en sistemas.	Alto	Políticas de control de cambios.
Inexistencia de cifrado en discos duros.	Alto	Cifrado.
Tableros eléctricos expuestos.	Medio	Informar de la observación a la Secretaría Administrativa.
Controles de acceso físicos,	Medio	Implementar controles

inseguros para administración de servidores.		biométricos.
Vulnerabilidades en el protocolo TCP/IP.	Medio	Políticas de monitoreo.
Daño en hardware por fallas eléctricas.	Medio	UPS
Inexistencia de control en el tráfico de red generado por la institución.	Medio	Gestor de uso de red.
Fuga de información.	Medio	Políticas de confidencialidad.
Daño físico a la infraestructura de red.	Medio	Medio Cableado estructurado.
Puertos abiertos sin motivo en servidores críticos.	Medio	Políticas de hardening en servidores.
Inexistencia de controles de seguridad en portátiles.	Medio	Candados de seguridad para portátiles.
Inexistencia de monitoreo de uso de la red.	Medio	Políticas de monitoreo.
Inexistencia en sistemas de aire acondicionado.	Medio	Adquisición de sistema de aire acondicionado.
Control de acceso débil en aplicaciones.	Medio	Políticas desarrollo de software seguro.
Personal poco capacitado en temas de seguridad.	Medio	Capacitación del personal.
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red.	Medio	Políticas de hardening en estaciones de trabajo y Políticas de hardening en servidores.
Falta de mantenimiento preventivo en servidores y equipos activos.	Medio	Mantenimiento preventivo en servidores y equipo activo.

Falta de mantenimiento de estaciones Eléctricas.	Medio	Mantenimiento preventivo en estaciones eléctricas.
Falta de corriente eléctrica regulada.	Medio	Implementar reguladores en la mayoría de los equipos.
Inexistencia de fuente de corriente eléctrica alterna.	Medio	Planta eléctrica.
Cableado de red expuesto.	Medio	Cableado estructurado.
Respaldos en mismo disco duro.	Medio	Políticas de respaldo.
Parámetros por default en equipos activos.	Medio	Políticas de configuración de equipos activos.
Acceso a todas las terminales de administración.	Medio	Firewall perimetral, firewall para servidores, listas de control de acceso.
Acceso a todos los recursos de internet.	Medio	Firewall, gestor de contenido (Proxy).
Uso de protocolos de comunicación inseguros.	Medio	Implementación de comunicaciones cifradas.
Falta de mantenimiento en cableado eléctrico.	Medio	Mantenimiento preventivo en la institución.
Inexistencia de controles de humedad.	Medio	Sensor de humedad.
Inexistencia de controles de temperatura.	Medio	Sensor de temperatura.
Consultas de sitios con software malicioso.	Medio	Gestor de contenido, capacitación al usuario.
Descarga de ejecutables de sitios no confiables.	Medio	Gestor de contenido, capacitación al usuario.
Inexistencia de políticas sobre el uso del equipo de cómputo.	Medio	Políticas sobre el uso del equipo de cómputo.
Autoarranque de dispositivos extraíbles.	Medio	Políticas de hardening en estaciones de trabajo.
Inexistencia de controles de	Medio	Memorias técnicas y respaldos

integridad en equipos activos.		de configuración.
Inexistencia de políticas de uso de software.	Medio	Políticas de hardening en estaciones de trabajo.
Falta de procedimientos de creación de cuentas.	Medio	Políticas de contraseñas.
Vulnerabilidades inherentes a las aplicaciones.	Medio	Actualizaciones.
Tiempo de vida útil de los equipos.	Medio	Mantenimiento preventivo, renovación de hardware.
Uso de versiones viejas en aplicaciones.	Medio	Actualizaciones
Vulnerabilidades conocidas en sistemas operativos.	Medio	Actualizaciones.
Fallas eléctricas.	Medio	Mantenimiento general a la red Eléctrica.
Inexistencia de cultura de seguridad en usuarios finales.	Medio	Capacitación del personal.
Poca separación de funciones críticas.	Medio	Definir responsabilidades, separación de funciones.
Fallas por parte del proveedor de servicios de internet.	Medio	Enlaces redundantes, acuerdos de LSA.
Inexistencia de monitoreo de las aplicaciones.	Medio	Políticas de monitoreo, implementación de herramientas de monitoreo.
Errores de cambios en la configuración de equipos activos y servidores.	Bajo	Capacitación del personal.
Desastres naturales en la institución.	Bajo	Prevención.

Elaborado por: El Investigador

A continuación se muestra el esquema de seguridad que se podrá implementar en la cooperativa en base a las necesidades y recursos con los que cuenta la cooperativa.

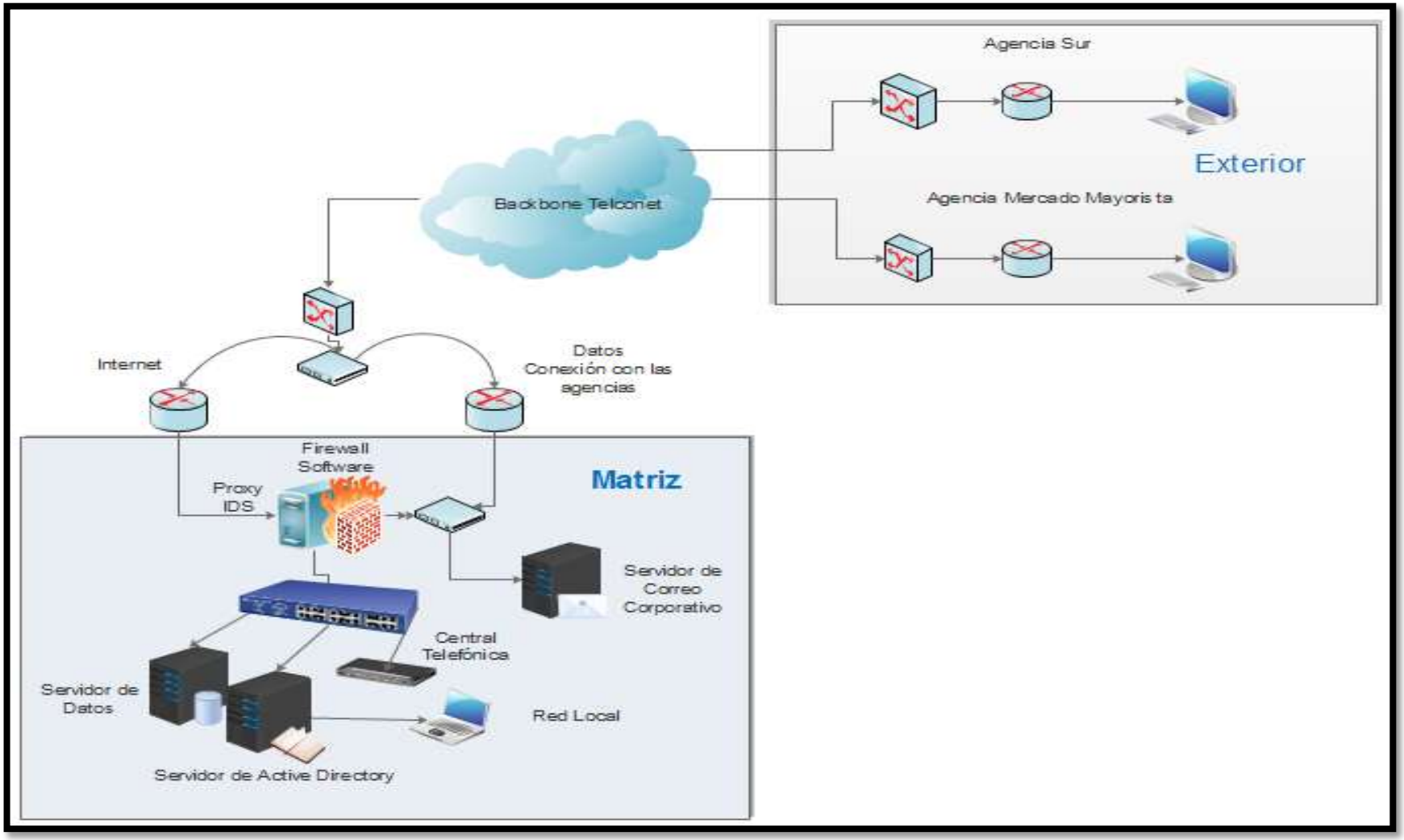

Fig. 26 Esquema de Seguridad de la Red de la cooperativa
Elaborado por: El Investigador

Todas las organizaciones deben planear su seguridad constantemente revisar, observar y aprender del entorno y desarrollar planes para mejóralas. La administración de los sistemas y de los recursos de red es esencial, así también contar con inventarios de todos los activos de TI como computadoras, servidores, impresoras, guías de configuración y conexión de internet son necesarios para una correcta planeación de seguridad.

Para la implantación de seguridad informática en la red de datos se debe contar con un administrador bien definido, con esto podremos realizar una correcta planificación para la seguridad informática, el cual se lo realiza conocimiento del análisis de la situación actual, los recursos económicos, la necesidad y la aprobación de gerencia.

Para la planificación de seguridad informática es recomendable basarse en diferentes metodologías y estándares. En el presente proyecto se basa a lo que establece la norma ISO 27001, se debe conocer los controles de acceso que se deben cumplir, cabe destacar que esta norma cuenta con varios controles establecidos, no es obligatorio cumplirlos todos en el presente proyecto, ya que nos centraremos en aquellos que nos permitan diseñar e implementar Seguridad Informática para la red de datos de la cooperativa.

4.3.3 Controles para la red de datos en base a la norma 27002:2013 (Anexo A 27001:2013) para la red de datos.

En base a las vulnerabilidades detectadas utilizando la metodología NIST, podemos mediante el anexo A de la norma ISO 27001 determinar los mecanismos adecuados para cubrir las vulnerabilidades pertinentes a la red de datos de la cooperativa.

El presente proyecto está orientado a diseñar seguridad en la red de datos de la cooperativa, por lo que se centrará en el establecimiento de los controles de la norma de acuerdo al alcance de SGSI ya establecido.

Tabla 14. Declaración de Factibilidad

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de Políticas para la seguridad de la información	x		Establecer políticas para la correcta administración, configuración y control de la red es primordial.
	5.1.2 Revisión de las políticas para la seguridad de la información	x		
6.1 Organización Interna	6.1.1 Asignación de responsables para la seguridad de la información	x		Es necesario la asignación de roles para el cuidado de la seguridad de la red, y dar conocimiento de estos y los responsables a gerencia.
	6.1.2 Segregación de tareas	x		
	6.1.3 Contacto con las autoridades	x		
8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	x		Se debe tener conocimiento de todos los activos tecnológicos mediante la documentación de los mismos y la asignación de los responsables de los activos.
	8.1.2 Propiedad de los activos	x		
	8.1.3 Uso aceptable de los activos	x		
8.2 Clasificación de la información	8.2.3 Manipulación de activos	x		Se debe definir el uso en concreto que se debe hacer de los equipos de TI.
9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos	x		Es recomendable definir políticas acerca del uso de medios externos, ya que estos pueden ser el origen de inconvenientes.
	9.1.2 Control de accesos a las redes y servicios asociados	x		

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas y bajas en el registro de usuarios	x		Dentro de la cooperativa existen diferentes tipos de usuarios con diferentes privilegios a la información e infraestructura, por lo que es recomendable una correcta administración y control de usuarios.
	9.2.2 Gestión de los derechos de acceso asignados a usuarios	x		
	9.2.3 Gestión de los derechos de acceso con privilegios especiales	x		
	9.2.4 Gestión de información confidencial de autentificación de usuarios	x		
9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autentificación	x		Es necesario exigir a los usuarios que toda su información que permita el acceso a la información sea privada.
9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción de acceso a la información	x		Hoy en día es obligatorio tener políticas adecuadas para el control de contraseñas para acceder a los recursos de TI, para de esta manera evitar que terceras personas accedan a información confidencial de la cooperativa.
	9.4.3 Gestión de contraseñas de usuarios	x		
	9.4.5 Control de acceso al código fuente de los programas y configuraciones	x		

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
2.1 Áreas	11.1.1 Perímetro de seguridad física	x		Una correcta ubicación y recurso para la protección de amenazas tales como incendios, problemas eléctricos y demás son necesarios para el correcto funcionamiento de los equipos de TI.
seguras	11.1.2 Controles físicos de entrada	x		
	11.1.3 Seguridad de oficinas, despachos y recursos	x		
	11.1.4 Protección contra amenazas externas y ambientales	x		
11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos	x		
	11.2.2 Instalación de suministro	x		
	11.2.3 Seguridad del cableado	x		
	11.2.4 Mantenimiento de los equipos	x		
	11.2.9 Política de puesto de trabajo y bloqueo de pantalla	x		
13.1 Gestión de Seguridad en las redes	13.1.1 Controles de red	x		Es imprescindible definir correctos mecanismos que nos permitan brindar la seguridad necesaria para las comunicaciones a través de la red. Los mismos que se hacen óptimos al separar por segmentos a la red de acuerdo a los requerimientos de la infraestructura tecnológica y de las políticas de funcionamiento que tiene la cooperativa.
	13.1.2 Mecanismos de seguridad asociados al servicio de la red	x		
	13.1.3 Segregación de redes	x		
	13.2.3 Mensajería electrónica	x		Dentro de la cooperativa solo se permitirá el uso del correo corporativo para el envió de información.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
14.1 Requisitos de seguridad de los sistemas de información	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	x		Mediante mecanismos se resguardará las comunicaciones hacia el internet y la vpn de la cooperativa.
	14.1.3 Protección de las transacciones por redes telemáticas	x		
15.1 Seguridad de la información en las relaciones con suministradores	15.1.1 Política de seguridad de la información para suministradores	x		Es recomendable establecer políticas para la adquisición de servicios a terceros, para definir acuerdos de los riesgos que se puedan presentar por los servicios que se adquieren.
	15.1.2 Tratamiento de riesgo dentro de los acuerdos de suministradores	x		
15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros	x		Es recomendable que siempre se supervise los servicios prestados por terceros para tener conocimiento de su correcto o mal funcionamiento.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
16.1 Gestión de	16.1.1 Responsabilidades y procedimientos	x		Es necesario establecer responsables de los diferentes procedimientos que se generan en la cooperativa, para que se pueda implementar seguridades que permitan identificar los puntos débiles y notificar cada uno de los inconvenientes que se presenten; de esta manera sobrellevar de la mejor manera las inseguridades que se vayan presentando y tomar las mejores decisiones teniendo un total conocimiento de los problemas.
incidentes	16.1.2 Notificación de los eventos de seguridad de la información	x		
de seguridad	16.1.3 Notificación de puntos débiles de la seguridad	x		
de la información	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	x		
y mejoras	16.1.5 Respuestas a los incidentes	x		
	16.1.6 Aprendizaje de los incidentes de seguridad de la información	x		
	16.1.7 Recopilación de evidencias	x		
17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información	x		Es necesario que todo lo establecido para resguardar la seguridad tenga constante desarrollo.
18.2 Revisión de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información	x		Es imperativo estar en constante control de las seguridades implementadas, además del cumplimiento de las políticas que se establecen para el resguardo de la seguridad de la información dentro de la red.
	18.2.2 Cumplimiento de las políticas y normas de seguridad	x		

Elaborado por: El Investigador

4.3.4 Definición De Políticas De Control De Acceso

Para la definición de las políticas de control de acceso para la red de datos de la cooperativa se utiliza el siguiente nivel que se explica en la norma ISO 27001 (Implementación y utilización de un SGSI). Estas políticas de basan en los controles en la **Tabla 14. Declaración de Factibilidad,** por considerar que el cumplimiento de estos robustece la seguridad de la información en la red de datos.

4.3.4.1 Política de Seguridad de la Información

Generalidades

Uno de los recursos más importantes dentro de cualquier organización es la información, por lo que resguardar su seguridad es primordial para el correcto desarrollo de cualquier actividad.

Las Políticas de Seguridad de la Información son un mecanismo de protección para la información, estas garantizan la continuidad operacional de los sistemas informáticos para cumplir con los objetivos de la cooperativa y minimizar el riesgo a daño de cualquier tipo. Las Políticas deben formar parte de la cultura general de la cooperativa.

Se debe establecer un compromiso manifestó de las autoridades de la cooperativa para la difusión, consolidación y cumplimiento de la presente Política.

Objetivos

- Salvaguardar la información que genera la cooperativa y la los recursos físicos de TI que se utilizan para su procesamiento, frente a amenazas de cualquier tipo, para de esta manera asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
- Aseverar la implementación de los mecanismos de seguridad detalladas en esta Política; la misma que debe mantenerse actualizada para asegurar la mejor

protección a todos los recursos de TI.

- Instaurar las directrices, procedimientos y requisitos necesarios para asegurar la protección oportuna y correcta de los recursos de TI de la Cooperativa de Ahorro y Crédito Unión Popular.

Alcance

El documento está dirigido al personal de la Cooperativa de Ahorro y Crédito Unión Popular Ltda., ya que ellos deben cumplir con las políticas sus normas y procedimientos que se presentan, y de esta manera resguardar la información que se genera en la cooperativa, protegiendo la confidencialidad, disponibilidad y seguridad de la información de los servicios tecnológicos que se utilizan. El no cumplir con dichas políticas tendrá como resultado medidas disciplinarias.

Las políticas que se establecerán se centrarán en la de resguardar la seguridad de los computadores y las comunicaciones a través de la red. Se establecerán los procedimientos y requisitos necesarios para brindar protección de manera adecuada de los equipos tecnológicos y sistemas de comunicaciones de la cooperativa; así también el uso de los servicios de correo electrónico corporativo y el uso del internet.

SEGURIDAD LÓGICA

Identificación

Para que un usuario pueda tener acceso al sistema de información debe establecerse un procedimiento formal y por escrito que normalice y exija el ingreso de los siguientes datos:

- ✓ ID de usuario, valor alfanumérico único.
- ✓ Contraseña, la cual debe ser personal del usuario en intransferible.
- ✓ Nombres y Apellidos completos.
- ✓ Grupo de usuario al que pertenece.

- ✓ Tiempo de expiración de la contraseña.
- ✓ Contador de intentos fallidos.
- ✓ Autorización de ingreso al área de usuarios.

Los permisos asignados deben ser mínimos y necesarios para que el usuario realice de manera correcta su labor diaria dentro de la cooperativa.

El acceso al sistema y la utilización de recursos de la cooperativa deben tener horarios para su utilización, tomando en cuenta lo siguiente:

- ✓ No se debe poder acceder a las cuentas de usuario en horarios no laborales, salvo previa autorización.
- ✓ Durante las vacaciones o licencias de los propietarios de las cuentas deben desactivarse.

La contraseña asociada al Id de usuario para el acceso a un computador es la primera verificación de su identidad, lo que permitirá en primera instancia al computador y a la información. Para resguardo de los recursos de la cooperativa la contraseña debe ser secreta e intransferible a ninguna persona.

El administrador del sistema deberá realizar una inspección mensual de los usuarios del sistema, para verificar que solo los usuarios necesarios tengan acceso y permisos correctos.

El área encargada de las contrataciones y cambios de personal deberá comunicar los mismos; luego de esta notificación el administrador del sistema debe revocar los permisos de la cuenta o su desactivación.

El sistema informático debe expirar la sesión cuando el equipo desde el cual se está ejecutando no tenga ningún tipo de uso en un periodo de cinco minutos, pasado este tiempo la sesión en el sistema debe cerrarse.

Los computadores deben tener configurado en su sistema operativo que después de cinco minutos de inactividad estas deben cerrar sesión de los usuarios, cabe recalcar que cada empleado contará con su ID y contraseña para acceso a las computadoras.

Se debe imposibilitar en los sistemas operativos de las computadores los usuarios genéricos. Se prohíbe el uso de cuentas invitado; todos los usuarios deben acceder a las computadoras y al sistema mediante sus cuentas ya asignadas; así mismo si se cuenta con sistemas operativos Linux no se debe entrar directamente como root (administrador en linux) sino con una cuenta con su ID y password asignado y mediante este acceder al modo de administrador de ser necesario.

Se deberá minimizar la generación y el uso de perfiles de usuario con máximos privilegios. Estos privilegios, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

Para la asignación de nuevas cuentas de usuarios, estas deben hacerse por escrito, el cual debe ser firmado por el usuario a quien se le entrega la ID, con el fin de que declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

Para solicitar una nueva cuenta o el cambio de privilegios estos deben ser aprobados por escrito y encomendados de esta manera al administrador del sistema.

No se debe conceder una cuenta a personas que no sean empleados de la cooperativa a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Contraseñas

Existen requerimientos y estándares internacionales a los cuales las contraseñas deben cumplir.

La contraseña de verificación de identidad no debe ser común o fácil de adivinar, esta debe cumplir con:

- ✓ Ser de al menos 8 caracteres de longitud.
- ✓ Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
- ✓ No contener su user ID como parte la contraseña.
- ✓ Sistemas y aplicaciones de la cooperativa que contengan información crítica requieren cambio de contraseña al menos cada tres meses (90 días). Si existen casos en los cuales las aplicaciones o sistemas no lo realicen automáticamente es obligación del responsable hacer que se cumpla dicho cambio.
- ✓ La nueva contraseña debe ser distinta a por lo menos los últimos tres utilizados.
- ✓ Bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas.
- ✓ El usuario debe poder modificar su contraseña las veces que sean consideradas necesarias.
- ✓ La contraseñada asignada por primera vez a un usuario solo debe ser válida para el primer inicio de sesión, en ese momento el usuario debe cambiar su contraseña cumpliendo con los requisitos establecidos.
- ✓ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
- ✓ Las contraseñas predefinidas que traen los equipos de TI nuevos como routers, switches, etc., deben ser cambiados inmediatamente antes de ponerlos en producción.

"Si existen sospechas que una contraseña ha sido vulnerada, debe ser cambiada inmediatamente."

SEGURIDAD EN LAS TELECOMUNICACIONES

Topología de red

- ✓ Deberá existir documentación detallada sobre los diagramas topológicos de la red.
- ✓ Deberán existir medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.

Correo Electrónico

Dentro de la cooperativa solo se autoriza el uso del correo electrónico corporativo, en cuyo servidor debe almacenar lo siguiente:

- Correo entrante y saliente.
- Hora de envío.
- Contenido del mensaje.
- Asunto del mensaje.
- Archivos adjuntos.
- Reporte de virus de cada parte del mensaje.
- Direcciones de máquina que emite y recepta.
- Tamaño del mensaje.

Red de datos

La red de datos es esencial para la comunicación por lo que debe recopilar información acerca de:

- Ancho de banda utilizado.
- Tráfico generado por las aplicaciones.
- Recursos de los servidores que utilizan las aplicaciones.
- El estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta).

- Intentos de intrusión.
- Uso de los protocolos.
- Solicitudes de impresión de datos de la empresa.

Los cambios y nuevas instalaciones de software que se realicen en los servidores, central telefónica, equipos de vigilancia y equipos de red de la cooperativa, así también el cambio de direcciones IP, reconfiguraciones de Switches, deben ser documentados y aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Propiedad de la Información

Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la cooperativa y no propiedad de los usuarios de los servicios de comunicación que brinda la cooperativa.

Uso de los sistemas de comunicación

Los recursos de los sistemas de comunicación de la cooperativa sólo deben utilizarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando se consuma una cantidad mínima de tiempo y recursos, y estos no interfiera con la productividad del empleado ni con las actividades de la cooperativa.

Conexiones Externas

- ✓ El servicio de Internet de la cooperativa será únicamente para propósitos relacionados con el negocio y mediante autorización de la Gerencia.
- ✓ Se debe asegurar el tráfico entrante y saliente de la red interna, debe ser filtrado y controlado por un firewall prohibiendo el pasaje de todo el tráfico que

no se encuentre expresamente autorizado.

- ✓ Cada vez que se necesite establecer conexión con terceros, los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.
- ✓ El uso de Internet debe ser monitoreado periódicamente; si se cree que la seguridad está siendo vulnerada, la cooperativa puede revisar el contenido de las comunicaciones de Internet.

Configuración lógica de red

Cuando sea necesario conectar a la red algún equipo de terceros o que no pertenezcan a la cooperativa, se debe considerar lo siguiente:

1. No identificarse como un usuario establecido de la red.
2. No ejecutar programas de monitoreo de tráfico (Ej. "sniffer" o similares) sin la debida autorización explícita de la gerencia y la aprobación del administrador de la red.
3. No agregar cualquier dispositivo que amplíe la infraestructura de la red de la cooperativa sin previa autorización.
4. Asegurar que la dirección IP de la empresa sea un número variable y confidencial.

Correo

Para la administración y uso del correo corporativo se debe tomar en cuenta los siguientes puntos:

- Debe existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el servidor correspondiente de la cooperativa.
- El correo electrónico no debe ser utilizado para enviar cadenas de mensajes, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la cooperativa.
- Los datos que se consideren “confidenciales” o “críticos” deben ser encriptados.

- Debe asignarse una capacidad de almacenamiento fija para cada una de las cuentas de correo electrónico de los empleados.

Antivirus

En todos los equipos de la cooperativa se debe instalar y ejecutar un antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción intentada por un software malicioso en tiempo real.
- Ejecutar periódicamente un escaneo de todas las unidades de almacenamiento para revisar y detectar software malicioso almacenado en la estación de trabajo.
- Actualizar su base de datos de virus diariamente.
- Debe ser un producto totalmente legal (con licencia o Software libre).

Los dispositivos externos no deben ser utilizados en las computadoras de la cooperativa, a menos que sea absolutamente necesario y hayan sido previamente escaneados y estén libres de virus u otros agentes dañinos.

Firewall

El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios.

El encargado de mantenimiento debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.

Ataques de red

- ✓ Toda la información que se transmita por la red deberá encriptarse o viajar en

formato no legible.

- ✓ La red debe estar monitoreada con alguna herramienta para evitar el ataque de denegación de servicio (DoS).
- ✓ La red deberá estar segmentada física o lógicamente para disminuir el riego de sniffing.
- ✓ Para poder disminuir la posibilidad de spoofing el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.
- ✓ Los archivos de contraseñas y datos deberán estar encriptados utilizando encriptación en un solo sentido ("one way"), con estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.

SEGURIDAD DE LAS APLICACIONES

Software

No se debe utilizar aplicaciones descargadas de internet, ya que estas pueden ser bajadas de fuentes no confiables, a menos que dicho software sea aprobado por el Departamento de Sistemas una vez que ellos lo hayan comprobado de manera rigurosa.

La cooperativa debe contar con software legal, es decir que cuenten con licencia adquirida para el uso de las labores diarias dentro de la institución para prevenir sanciones por parte de las instituciones que la regulan o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado.

El uso se software libre debe ser previamente analizado por el Departamento de Sistemas de la cooperativa antes de su instalación en los equipos.

Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema.

Deberá existir un responsable en cada área de la empresa, que responda por la información que se maneja en dicho sector. Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

Control de aplicaciones en las computadoras

- ✓ Se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.
- ✓ Antes de hacer un cambio en la configuración de los servidores se deberá hacer un respaldo de la configuración existente.
- ✓ Los cambios satisfactorios realizados en los servidores deberán almacenarse.
- ✓ Se deberán documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen.
- ✓ En el momento en que un nuevo usuario ingrese a la empresa, se lo deberá notificar y deberá aceptar que tiene prohibida la instalación de cualquier producto de software en los equipos.

Control de datos en las aplicaciones

Se deberán proteger con controles de acceso las carpetas que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.

Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá entregar a la cooperativa:

- o Aplicación ejecutable.
- o Código fuente de la aplicación.
- o Documentación del desarrollo.
- o Manuales de uso.

SEGURIDAD FÍSICA

Los recursos de TI tanto físicos como lógicos de la cooperativa sólo deben usarse en un ambiente seguro.

- ✓ Un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Sistemas.
- ✓ Es prohibido comer o fumar en las estaciones de trabajo.
- ✓ Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- ✓ No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.
- ✓ La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Cualquier inconveniente en las computadoras o en la red debe reportarse rápidamente para evitar problemas serios como pérdida de la información o indisponibilidad de los servicios.

Control de acceso físico al centro de cómputos

- ✓ Se deberá asegurar que todos los individuos que ingresen a áreas restringidas se identifiquen, sean autenticados y autorizados para ingresar.
- ✓ Cualquier persona ajena a la empresa que necesite ingresar al centro de cómputos deberá ser escoltado por un personal de sistemas quien debe acompañarlo durante el transcurso de su tarea, hasta que éste concluya.
- ✓ El área del cuarto de datos donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso a los administradores.
- ✓ Los servidores de red y los equipos de comunicación deben estar ubicados

en sitios apropiados, protegidos contra daños y robo. Debe restringirse estrictamente el acceso a estos sitios y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

Control de acceso a equipos

Los siguientes controles de seguridad deben ser activados en todas las estaciones de trabajo (workstation) con el fin de protegerlas contra el robo de la información:

1. Activar la contraseña de disco duro en la BIOS.
2. Configurar el uso de contraseña para proteger el teclado y la pantalla, esto se debe activar automáticamente luego de un período de inactividad. El intervalo de inactividad no debe ser mayor a 15 minutos.
3. Si se necesita conectar una estación de trabajo a una red fuera de la cooperativa, entonces toda la información clasificada Confidencial debe ser criptografiada.

El administrador deberá realizar chequeos periódicos para comprobar:

- La correcta instalación de los dispositivos de los equipos.
- Su buen funcionamiento.
- Sus números de series corresponden con los datos registrados por el administrador al momento de la instalación.

Equipos portátiles

Los equipos portátiles de la cooperativa deben ser aseguradas físicamente, dentro de un cajón bajo llave, si no se tiene esta disponibilidad es indispensable el uso de un cable de seguridad o anclaje físico.

Mantener el equipo en su poder todo el tiempo que sea posible, cuando esté fuera de las instalaciones de la cooperativa.

Dispositivos de soporte

En la cooperativa deben existir los siguientes dispositivos de soporte:

- Aire acondicionado en el cuarto de datos para que se mantenga a una temperatura oscilada entre 19º C y 20º C.
- Extintor de incendios: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación. En el cuarto de datos debe existir uno exclusivamente.
- Alarmas contra intrusos: estas deberán ser activadas en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.
- UPS: (Uninterruptible power supply) deberá existir al menos un UPS en el cuarto de datos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.
- Luz de emergencia: deberá existir una luz de emergencia que se active automáticamente ante una contingencia.

Todos estos dispositivos deberán ser evaluados periódicamente por personal de mantenimiento.

Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

Cableado estructurado

- Se deberá documentar en planos los canales de tendidos de cables y las bocas de red existentes.
- Deberá medirse periódicamente nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones

correctivas necesarias.

- Ante un corte del suministro de energía eléctrica deberán apagarse los equipos del centro de cómputos de forma segura, como medida de prevención.

ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO

El equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, generando una cultura de la seguridad, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debe ser renovado y transmitido a los usuarios en forma anual.

Los usuarios solicitarán asesoramiento o servicios al Departamento de Sistemas por medio de mails, de manera que se genere un registro de los trabajos efectuados y las solicitudes emitidas por los empleados.

Deberá existir un procedimiento para realizar la publicidad de políticas, planes o normas de la empresa y sus modificaciones.

Los administradores deberán informar en tiempo de suspensiones en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.

Deberá generarse un inventario detallado donde se describan los sistemas de información y de los equipos de cómputos utilizados en la organización. Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.

Capacitación

Se debe obtener un compromiso firmado por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de

las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

Asegurar que los empleados reciban capacitación continua para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

Respaldos

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

- ✓ Los archivos de backup deben tener un control de acceso lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.
- ✓ Deben generarse copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones.
- ✓ Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores.
- ✓ Se deberá generar una copia de respaldo de toda la documentación del centro de datos, incluyendo el hardware, el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

Documentación

- ✓ Deberá generarse un soporte de documentación, con información correcta,

consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputos.

- ✓ Deberá existir un registro de los eventos, errores y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.
- ✓ Deberán existir documentación y un registro de las actividades del centro de cómputos (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.

SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física necesita proteger todos los recursos de la organización, incluyendo personas y hardware. La seguridad debe fortalecer la productividad ya que provee un ambiente seguro. Esto permite a los empleados enfocarse en sus tareas, en lo posible no permitir que la seguridad física se transforme en un hueco de seguridad.

Las vulnerabilidades con respecto a la seguridad física tienen relación con destrucción física, intrusos, problemas del ambiente y los empleados que han perdido sus privilegios causen daños inesperados de datos o sistemas.

Instalaciones

Los materiales de construcción y la composición de la estructura han sido evaluados por las características de protección. La construcción de la cooperativa asegura que el edificio no colapse.

Como se indicó anteriormente la puerta del cuarto de servidores permite que los equipos sean vistos por los empleados y las personas que visiten la oficina de gerencia, cabe destacar que solo el Jefe del Departamento de Sistemas cuenta con la llave para abrir la cerradura, se recomienda un cambio de puerta para que cumpla con las siguientes características de seguridad:

- Material resistente, como: madera, aluminio
- Resistente a ingreso forzado
- Cerradura resistente
- En la puerta del cuarto de servidores se colocará un rótulo de zona de acceso restringido para evitar acceso no autorizado.

Es necesario procedimientos de seguridad para ayudar a proteger la cooperativa de actividades que la pongan en riesgo. Muchas veces estos procedimientos de protección usan componentes de seguridad que son parte del ambiente y por consiguiente no necesitan gastos extras. Los procedimientos que se han considera incluyen copias de respaldo de los datos críticos, componentes de seguridad que ya son parte de los sistemas operativos, y la solicitud de mayor colaboración por parte del guardia actual de la cooperativa para que permanezca en una sola área atento a cualquier fallo de seguridad.

- ✓ La seguridad física debería ser complementada con la seguridad contra fuego. Hay estándares nacionales y locales para prevenir, detectar y suprimir el fuego.
- ✓ En la cooperativa se utilizará detectores de fuego activados por el humo, ya que son dispositivos que dan señales de alerta tempranamente.
- ✓ Se colocarán detectores de fuego en el cuarto de servidores, otra en el Departamento de Créditos y otros censores cerca de la Recepción y Cajas, de tal manera que se trate de cubrir todas las instalaciones de la Corporación.

Perímetro de Seguridad

La primera línea de defensa trata el control del perímetro para prevenir acceso no autorizado a la cooperativa. Actualmente la cooperativa trabaja de la siguiente forma: En el momento de cierre de la cooperativa e cierra la única puerta que se tiene para acceder a la misma, en la puerta se tiene un mecanismo de monitoreo para alertar de actividades sospechosas. Cuando la cooperativa está en operación, la seguridad es más complicada porque se debe distinguir el acceso de personas autorizadas de las personas

no autorizadas.

Es importante destacar la seguridad del perímetro ya que la red de datos está desplegada en todo el edificio por lo que es importante su resguardo para que las comunicaciones no se vean afectadas por daños de personas malintencionadas.

Las cerraduras y llaves son los mecanismos de control de acceso más barato pero de gran importancia para prevenir cualquier acceso no autorizado a cualquier sitio de la cooperativa.

Controles Físicos de Entradas

Es importante contar con controles de acceso físico para resguardar todos los activos de la cooperativa, estos deben:

- Supervisar a los visitantes de la cooperativa y registrar la fecha y horario de su ingreso y egreso cuando estos tienen que acceder a áreas protegidas (Cajas, Contabilidad, Sistemas). Sólo se permitirá el acceso mediando propósitos específicos y autorizados.
- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

Seguridad de Oficinas, Despachos y Recursos

Se definen sitios como áreas protegidas de la cooperativa, para lo cual se consideró el tipo de información manejada por cada área.

Tabla 15 Áreas protegidas

Áreas Protegidas
Departamento de Contabilidad
Departamento de Sistemas
Cajas

Elaborado por: El Investigador

Se establecen las siguientes medidas de protección para áreas protegidas:

a. Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b. Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, copiadoras, máquinas de fax, adecuadamente dentro del área no protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
c. Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
d. Almacenar la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal: en la caja de seguridad que tiene la Corporación con el Banco.

Desarrollo de Tareas en Áreas Protegidas

Para complementar la seguridad en la las áreas protegidas, se establecen los siguientes controles:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión, como por ejemplo: trabajos de limpieza.
c) Bloquear físicamente las áreas protegidas desocupadas.
d) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Actualmente no se cuenta con un suministro de energía ininterrumpible, por lo que es necesario la adquisición de un generador de energía que se acople a los requerimientos de la cooperativa.
b) Dar un mantenimiento preventivo a las instalaciones eléctricas e la cooperativa para evitar incidentes.

Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- El responsable del Departamento de Sistemas de la cooperativa, debe realizar un cronograma de mantenimiento de los equipos de TI y llevar un registro de la frecuencia del mantenimiento preventivo y el detalle de los equipos.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

A continuación se indica el período aconsejable para realizar los mantenimientos en los equipos de la red.

Tabla 16 Cuadro de Mantenimiento de Equipos

Equipo	Frecuencia de mantenimiento	Personal autorizado
Servidores	4 meses	**Administrado**
Estaciones de Trabajo	6 meses	**Administrado**
impresoras	6 meses	**Administrado**
Central telefónica	**12 meses**	**Administrado**

Elaborado por: El Investigador

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Controles contra software malicioso

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado.
b) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, para esto se implementará el software de anti-virus Nod32. [ANEXO E]
c) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.
d) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la cooperativa, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas (políticas de control de acceso).
e) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
f) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
g) Concientizar al personal acerca del problema de los virus y sus posibles consecuencias.

GESTIÓN INTERNA DE RESPALDO

Recuperación de la Información

El Responsable de la Seguridad de Información dispondrá y controlará la realización de dichas copias. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la cooperativa. Para los procedimientos del resguardo de información, se considerarán los siguientes puntos:

a) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.
b) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
c) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

GESTIÓN DE LA SEGURIDAD DE RED.

Controles de Red

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Para establecer controles especiales para salvaguardar la confidencialidad e

integridad del procesamiento de los datos. **(Literal 4.3.2)**

b) Implementación de controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

Gestión De Medios Removibles

Se deberán considerar las siguientes acciones para la administración de los medios informáticos removibles:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Corporación.
b) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Intercambio de información. Mensajería electrónica

Se debe documentar normas claras con respecto al uso de correo electrónico:

- Todo empleado de la Corporación puede solicitar y disponer de una cuenta de correo electrónica activa.
- El Área de Sistemas hará la configuración de la cuenta de correo en la computadora asignada al funcionario solicitante.
- La activación de las cuentas de correo Corporativo es centralizada, encargándose de esta el responsable de Sistemas previa autorización del Jefe Administrativo. La activación sigue las políticas dadas por el presente documento.
- Para activar el correo electrónico, se deberá enviar dicha solicitud por escrito y debe ser debidamente aprobada.

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse cuentas de correo electrónico a personas que no sean empleados de la Corporación a menos que estén debidamente autorizados, en cuyo caso la activación durará el tiempo que duré la permanencia de la(s) personas en la Institución, para lo cual se requerirá la notificación respectiva del área administrativa.
- Cuando un empleado es despedido o renuncia a la Corporación, debe desactivarse la cuenta de correo correspondiente, para lo cual se requerirá la notificación respectiva por parte del área administrativa.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismos debe informar claramente a sus empleados: a) cuál es el uso que el organismo espera que los empleados hagan del correo electrónico provisto por el organismo; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

Uso del Correo Electrónico Corporativo

- Es responsabilidad del usuario del correo electrónico hacer buen uso de su cuenta entendiéndose por buen uso:
    - El uso de su cuenta para actividades institucionales administrativas de la Corporación Metropolitana de Salud.
    - Leer diariamente su correo y borrar aquellos mensajes obsoletos para liberar espacio en su buzón de correo
    - El uso de un lenguaje apropiado en sus comunicaciones

    - No permitir que segundas personas hagan uso de su cuenta de correo
- Cada usuario es responsable de respaldar sus correos en su equipo personal.

Restricciones

El usuario que tenga acceso a una cuenta de correo electrónico de la Cooperativa de Ahorro y Crédito Unión Popular se compromete a NO usar este servicio para:

- Fines comerciales, políticos, particulares o cualquier otro que no sea el laboral o de investigación para la Institución.
- Enviar SPAMS de información (correo basura) o enviar anexos (archivos adjuntos) que pudiera contener información nociva para otro usuario como virus o pornografía.
- Enviar o recibir contenido ilegal, peligroso, amenazador, abusivo, tortuoso, difamatorio, vulgar, obsceno, calumnioso, que atente contra el derecho a la intimidad, racial, étnico o de cualquier otra forma ofensiva.
- Enviar o recibir cualquier anuncio no solicitado o no autorizado, materiales promociónales, correo de solicitación ("junkmail", "spam"), cartas en cadena ("chain letters), esquemas de pirámides ("pyramid schemes") o cualquier otra forma de solicitud.
- Diseminar virus, caballos de troya, gusanos y otros tipos de programas dañinos para sistemas de proceso de la información de la CMS.
- Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso de la Institución.
- Falsificar encabezados o cualquier otra forma de manipulación de identificadores para desviar el origen de algún contenido transmitido por medio del Servicio.
- Enviar o recibir por correo electrónico algún contenido que no tiene derecho a transmitir por ley o por relación contractual o fiduciaria (tal como información interna, de propiedad y confidencial adquirida o

entregada como parte de las relaciones de empleo o bajo Reglamentos de confidencialidad).

- Acechar o de cualquier otra forma hostigar a usuarios de correo electrónico.

UTILIZACIÓN DE LOS SERVICIOS DE RED

Las conexiones no seguras a los servicios de red pueden afectar la seguridad de toda la cooperativa, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El administrador de la red es el responsable de otorgar los permisos tanto a servicios como recursos de la red, únicamente de acuerdo al pedido formal del responsable de cada unidad.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la cooperativa.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

Para este control se implementó la asignación el procedimiento de asignación de privilegios.

PROTECCIÓN DE LOS PUERTOS (PORTS) DE DIAGNÓSTICO REMOTO

Para poder determinar cuáles realmente requieren estar abiertos y cuales deben estar cerrados, en este caso vamos a trabajar con una herramienta que nos permita determinar cuáles puertos se encuentran abiertos. Para nuestro caso proponemos pasos tanto para los servidores en LINUX así como los equipos en Windows, con la ayuda de una herramienta que realice este chequeo además de la administración de la red. [ANEXO F]

CONFIGURACION DE ACCESO POR DEFECTO

Para asegurar que no exista alguna equivocación por parte del administrador del sistema, por defecto se configuran a los usuarios como usuario estándar, es decir sin privilegios de instalación de programas, modificación de archivos de red, desinstalación de programas y sin acceso a los sistemas y aplicaciones.

Al igual debe suceder con los módems y switch se configuran listas de control de acceso que por defecto bloqueen todo y solo permitan el paso de lo que se configura.

MONITOREO DE CONTROL DE ACCESO

Para tener un control más adecuado de la red, identificación de vulnerabilidades en la misma, que puedan conllevar a problemas de control de acceso **(Literal 4.4.3)** se muestra la configuración que realizamos para la implementación de un firewall que nos permitirá utilizar las ventajas del sistema operativo Linux de un servidor para un mayor control de acceso.

RESTRICCIÓN DEL CAMBIO DE PAQUETES DE SOFTWARE

Para evitar que los usuarios puedan modificar, sin autorización previa cualquier tipo de software, las cuentas de los empleados en el dominio no tienen permisos para realizar ninguna de estas actividades, así como tampoco pueden instalar ningún tipo de software

ni remover sin previa solicitud al administrador de red y sin autorización del responsable de cada área. Para lograr este objetivo se configura un servidor de dominio **(Literal 4.4.1).**

GESTION DE CONTINUIDAD DEL NEGOCIO

Aspectos De La Gestión De Continuidad Del Negocio

Al desarrollar el plan de la continuidad del negocio para la cooperativa, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres.

Proceso De Gestión De La Continuidad Del Negocio

Los responsables de cada área, deben determinar las aplicaciones críticas de las mismas y desarrollar procedimientos regulares para mantener respaldos continuos de los procesos críticos de cada área. El plan de contingencia de cada proceso debe considerar como mínimo:

- La administración de los recursos críticos, en caso de ser necesaria la implementación del plan de contingencia.
- Identificar los riesgos. Cada riesgo debe identificarse con qué pasos sería necesario detenerlo, pues es más barato evitar la crisis que repararla; por lo cual todos los planes deben tener un enfoque de prevención.
- Documentar el impacto de una pérdida extendida a los funcionamientos y funciones de negocio.
- Debe ser un plan entendible, fácil usar, y fácil para mantener por todos los miembros de la organización.

REVISIONES DE LA POLÍTICA DE SEGURIDAD Y DE LA CONFORMIDAD TÉCNICA

Conformidad con la Política de Seguridad

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, este período como mínimo debe ser cada 6 meses.

4.4 CONFIGURACIÓN DE MECANISMOS DE SEGURIDAD PERIMETRAL

A continuación se muestran las distintas configuraciones de los mecanismos definidos en el alcance del proyecto.

4.4.1 Configuración Servidor de Dominio y Active Directory

La cooperativa cuenta con un servidor encargado de virtualizar varios servicios tales como la central telefónica; en este se realizará la instalación y configuración del servidor de dominio bajo el Sistema Operativo Windows Server 2012, cuya licencia ha sido adquirido por la cooperativa.

EL servidor en el cual se va a instalar es el siguiente:

Servidor HP ProLiant ML350p Gen8

- Procesador Intel® Xeon® E5-2600
- Memoria, máxima 768 GB
- Almacenamiento 5Tb
- Sistema Operativo Centos 5
- Virtualización (Windows Server 2012, Centos 6.4)

El software de virtualización utilizado es KVM.
Dentro de la cooperativa se debe controlar que los usuarios cumplan con las políticas

anteriores, se acordó la instalación de un servidor de Servicio Activo o Active Directory.

A continuación de muestran los pasos para la instalación y configuración necesaria para el servidor de servicio activo:

Una vez instalado el Sistema Operativo Windows Server 2012 se modifica el nombre del servidor ***srvActiveDirectory*** y la dirección IP asignada, en este proyecto ***192.168.0.4.***

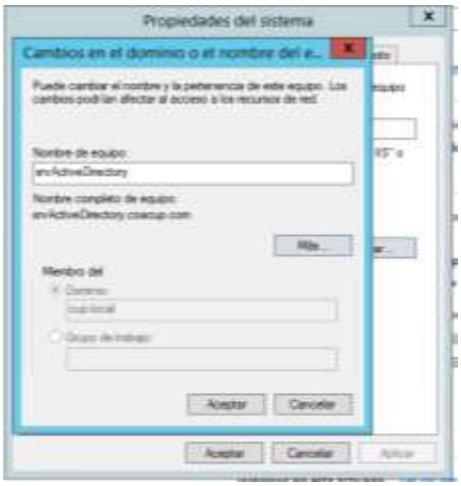

Fig. 27 Nombre del Servidor

Fig. 28 Nombre del Servidor

El servidor debe ser controlador de dominio, esto se realiza automáticamente al instalar *Servicios de Dominio de Active Directory*, este lo encontramos en el Administrador de Servidores de Windows Server 2012.

Seleccionamos la opción "Agregar roles y características"

Fig. 29 Administrador de Servidores

Siguiente

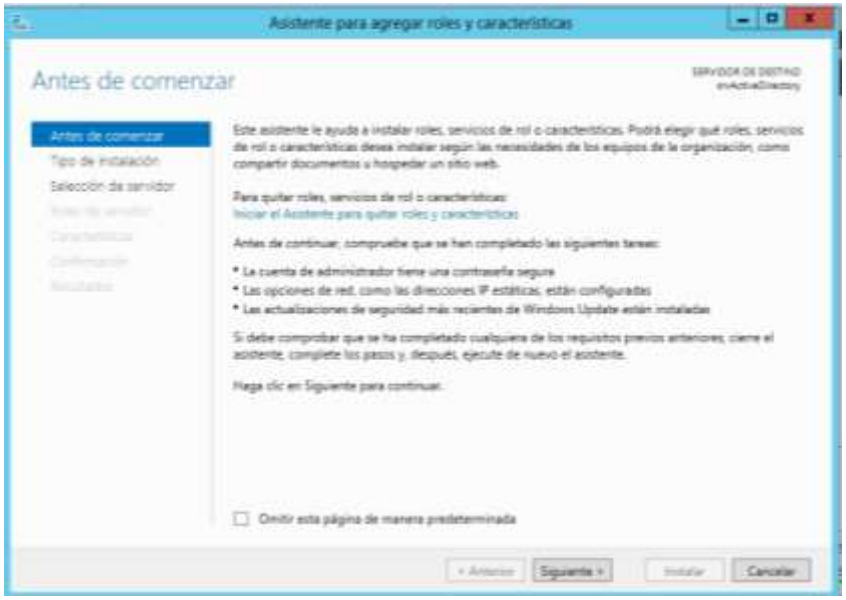

Fig. 30 Asistente para agregar roles y características

Instalación en roles.

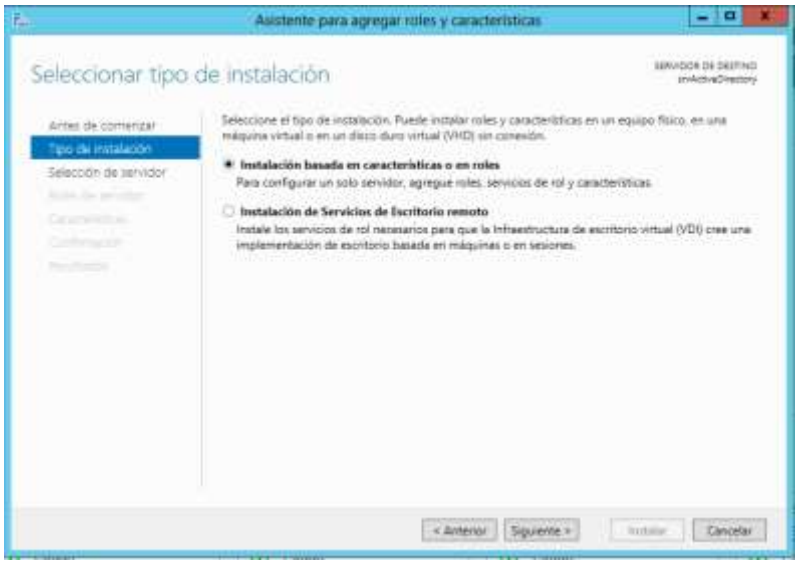

Fig. 31 Asistente para agregar roles y características

Seleccionar el servidor: "srvActiveDirectory"

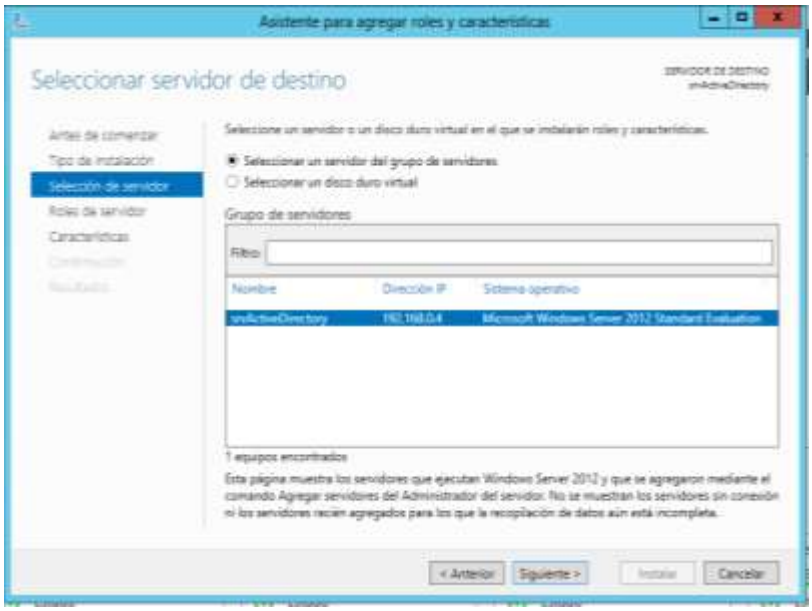

Fig. 32 Asistente para agregar roles y características

Instalar "Servicios de dominio de Active Directory"

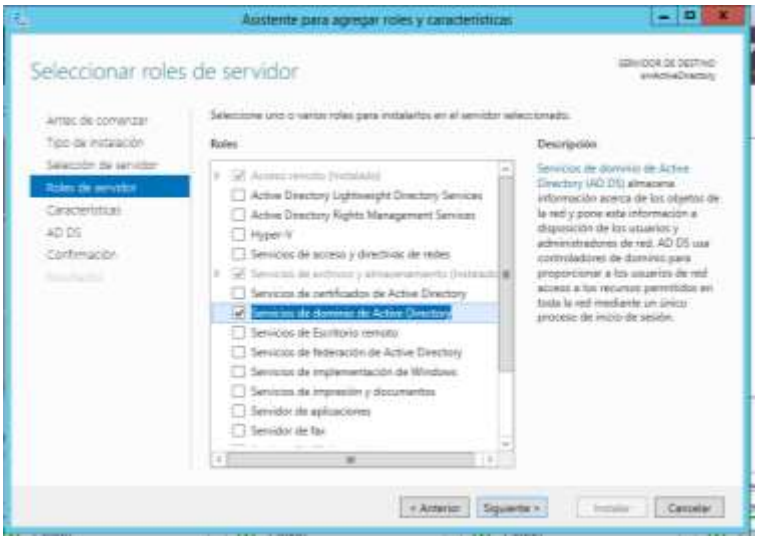

Fig. 33 Asistente para agregar roles y características

Características que necesita instalar para promoverlo a DC

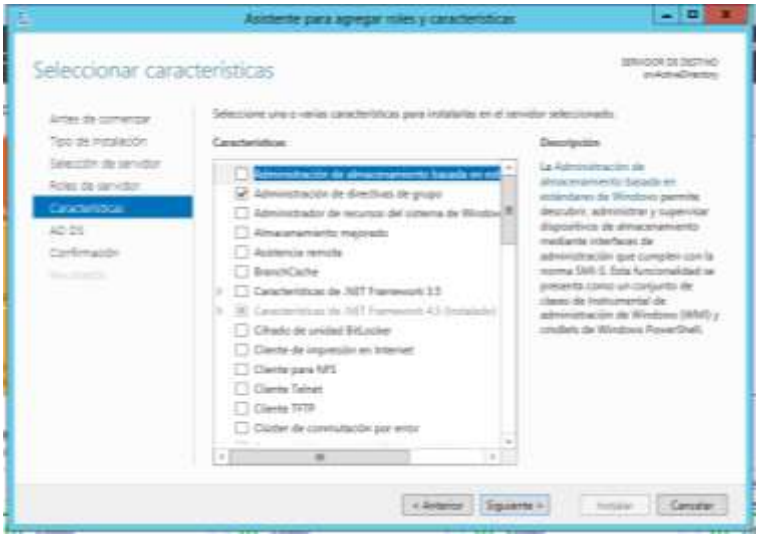

Fig. 34 Asistente para agregar roles y características

Mensaje de información

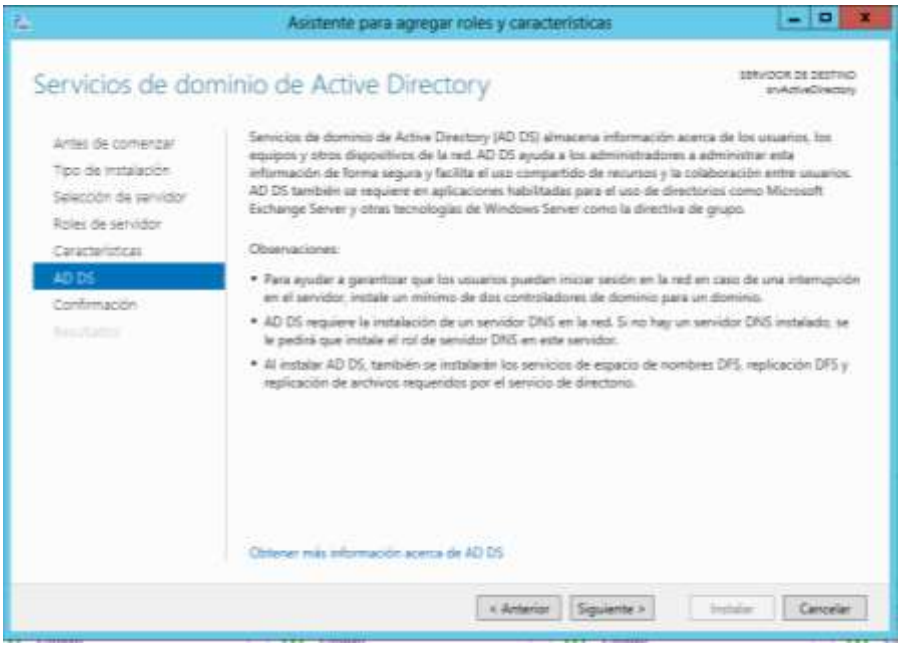

Fig. 35 Asistente para agregar roles y características

Resumen de lo que se instalara

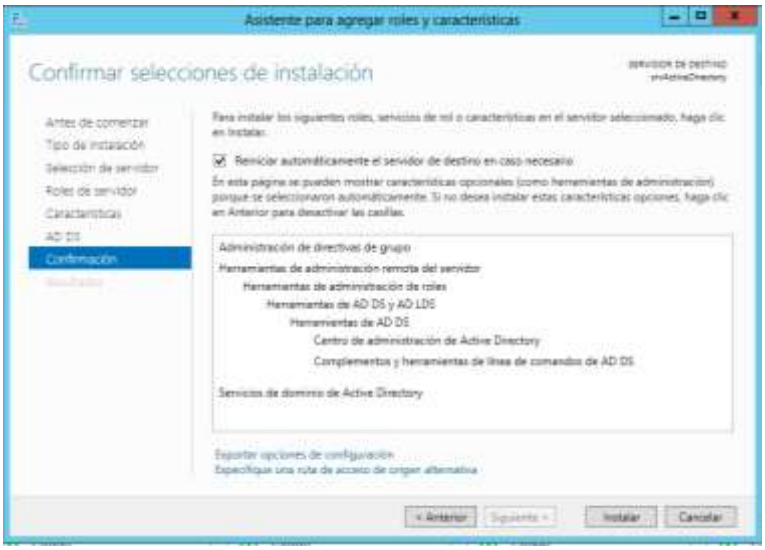

Fig. 36 Asistente para agregar roles y características

Aquí vemos como empieza la instalación

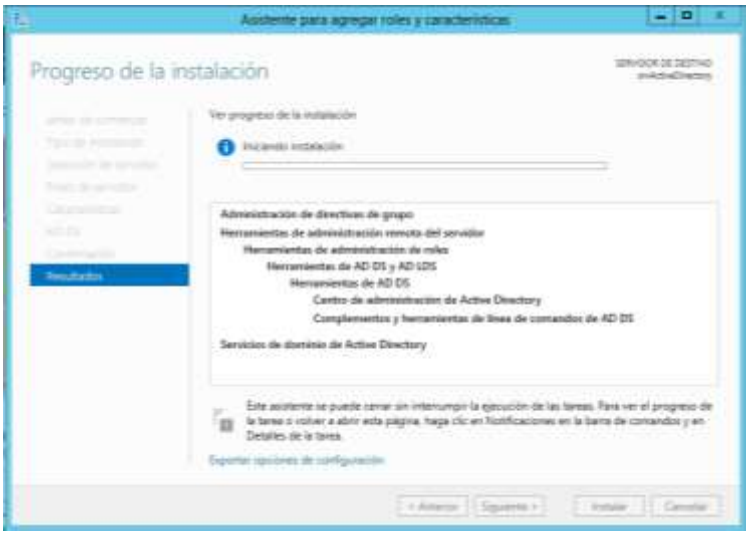

Fig. 37 Asistente para agregar roles y características

Una vez ha terminado de realizar las gestiones, nos deja "promover este servidor a controlador de dominio". Pues a eso vamos.

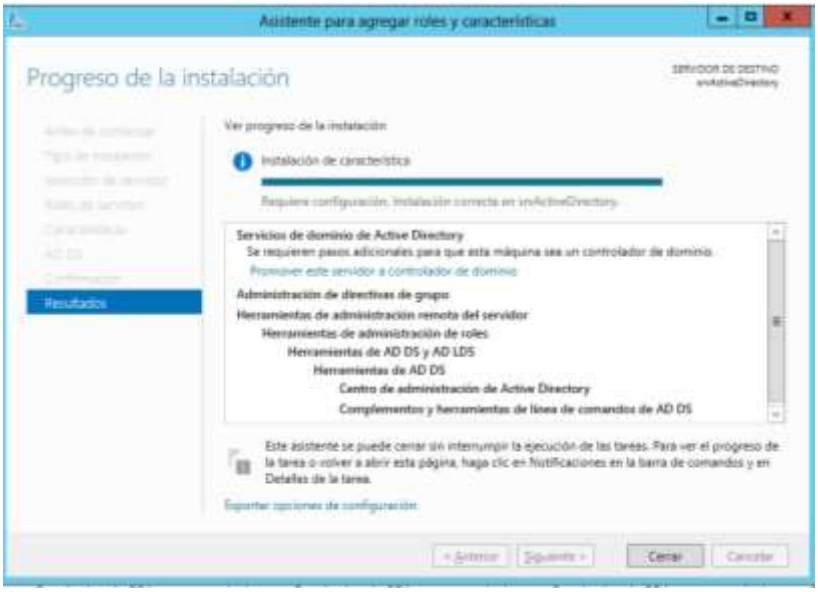

Fig. 38 Asistente para agregar roles y características

Una vez instalado el servicio activo se necesita configurar aspectos adicionales:

Agregamos un nuevo bosque

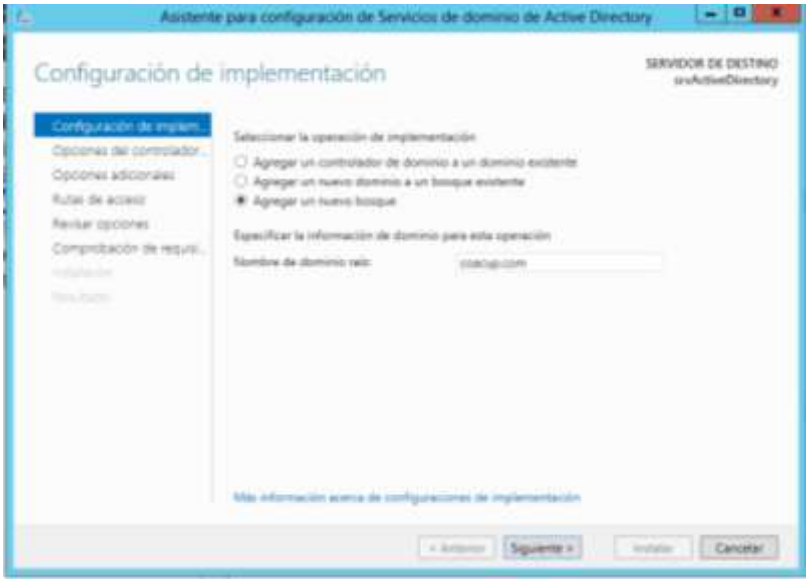

Fig. 39 Asistente para configuración de Servicios de dominio

Niveles funcionales desde 2003 en adelante

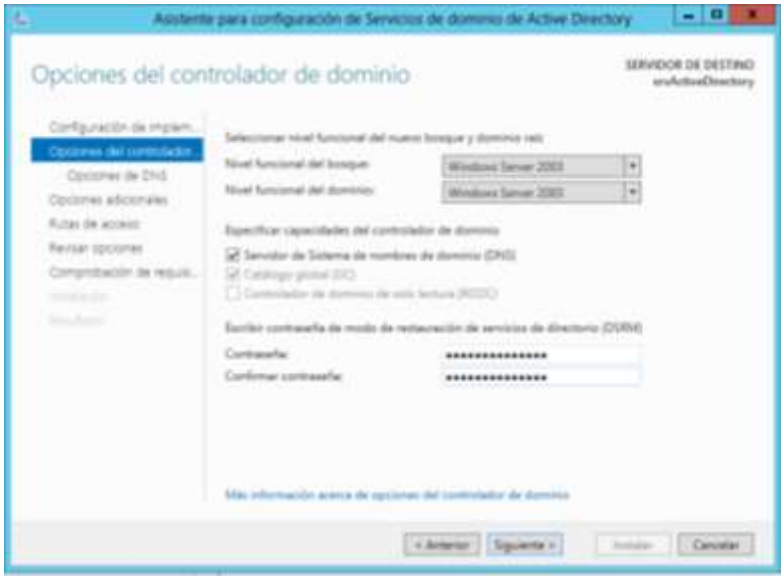

Fig. 40 Asistente para configuración de Servicios de dominio

Crear una zona DNS

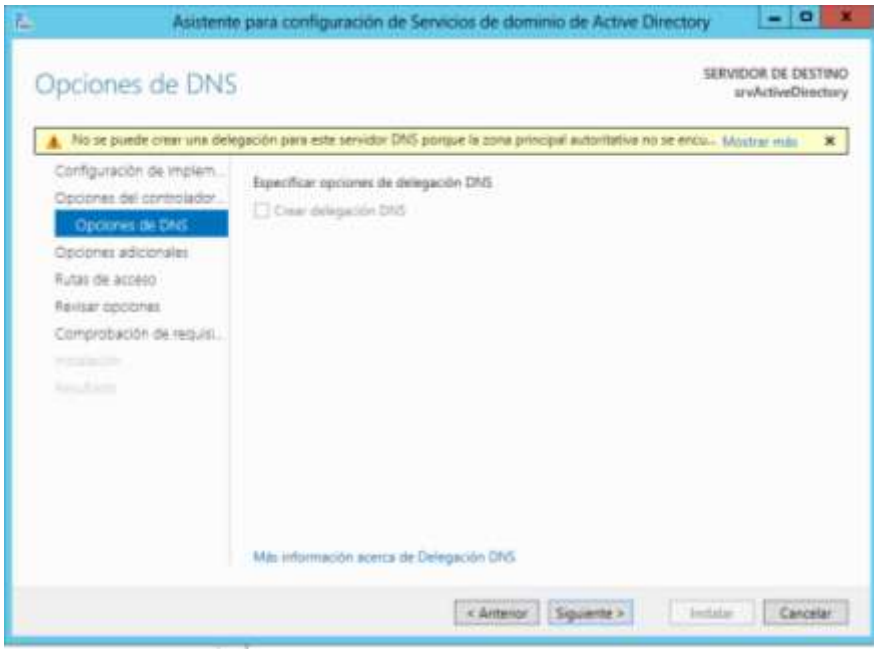

Fig. 41 Asistente para configuración de Servicios de dominio

Nombre Netbios

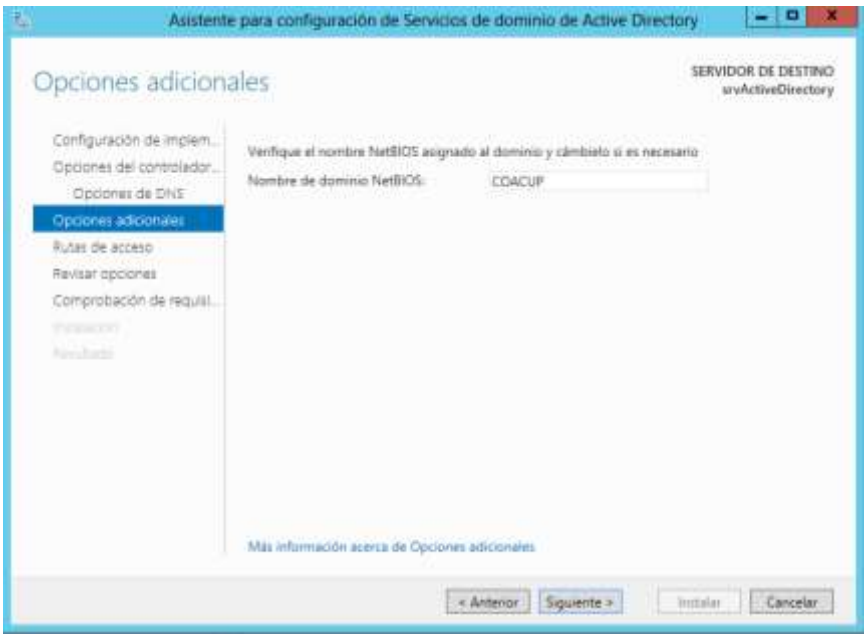

Fig. 42 Asistente para configuración de Servicios de dominio

Carpetas de las bases de datos etc

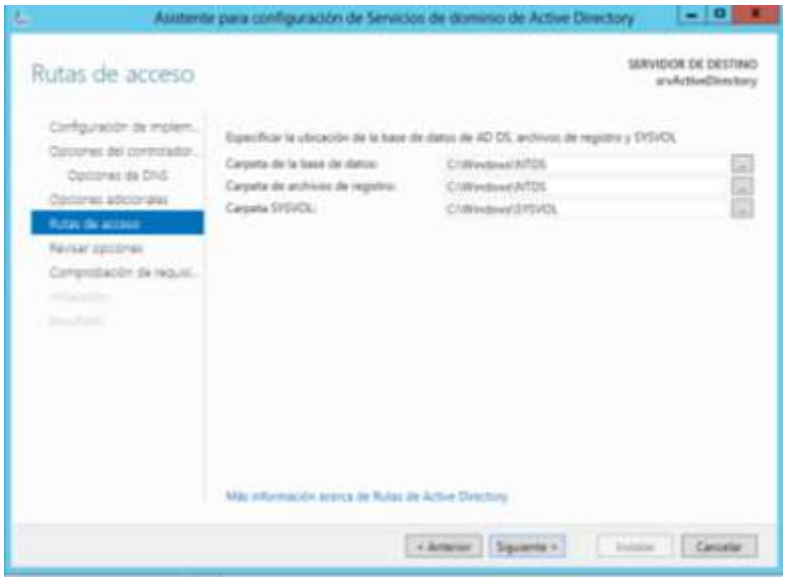

Fig. 43 Asistente para configuración de Servicios de dominio

Resumen de las opciones

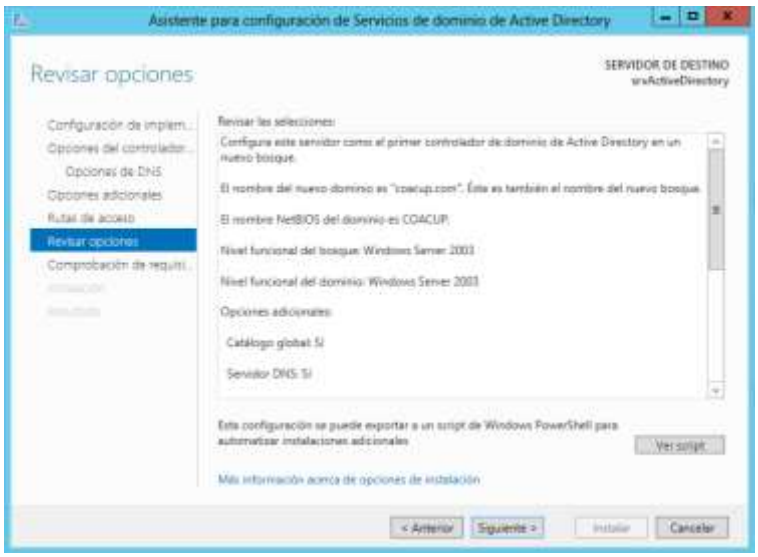

Fig. 44 Asistente para configuración de Servicios de dominio

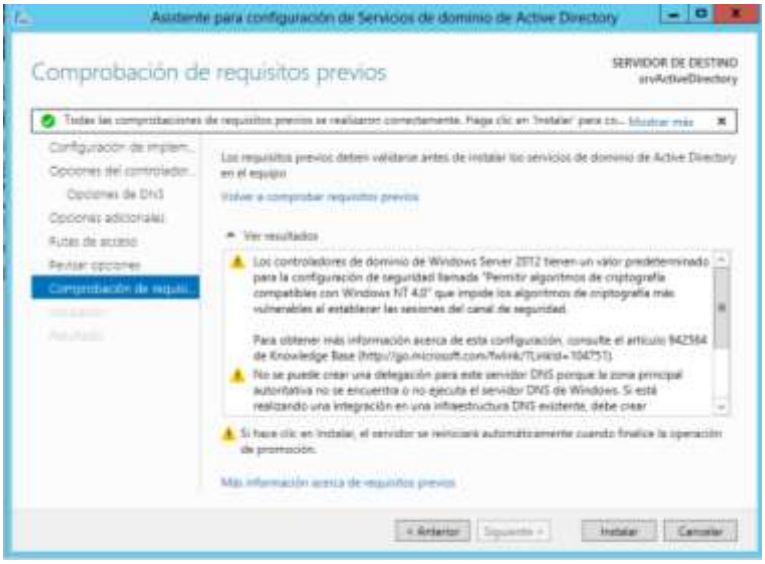

Fig. 45 Asistente para configuración de Servicios de dominio

Se cierra sesión, una vez el proceso ya casi ha terminado.

Ya está instalado el servidor cuenta con las opciones:

Fig. 46 Servicios de Active Directory

Creación de Unidades Organizativas

Cada departamento de la cooperativa será agregado a la estructura lógica del Active Directory a través de unidades organizativas. Cada unidad organizativa anidara unidades organizativas que permitirán tener control sobre los recursos de la red (Usuarios, Impresoras, Carpetas Compartidas y Equipos).

Las unidades organizativas se crean a través del servicio *Usuarios y equipos de Active Directory*. Se observa el nombre del servidor de dominio *coacup.com* en el cual se crean las unidades organizativas.

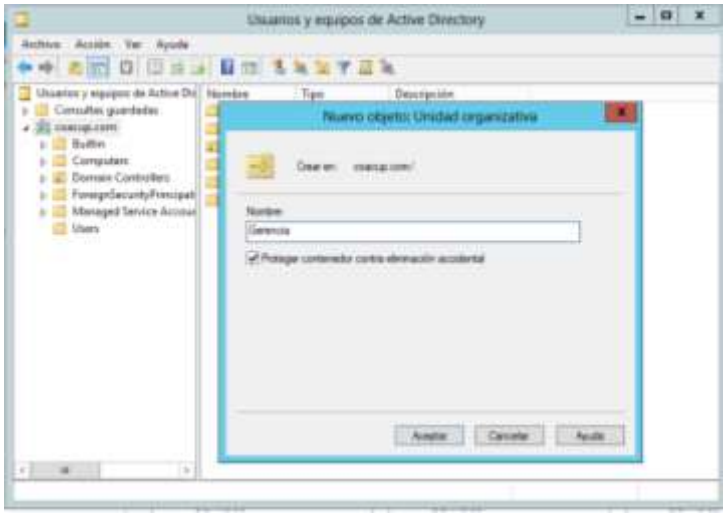

Fig. 47 Creación de Unidad Organizativa

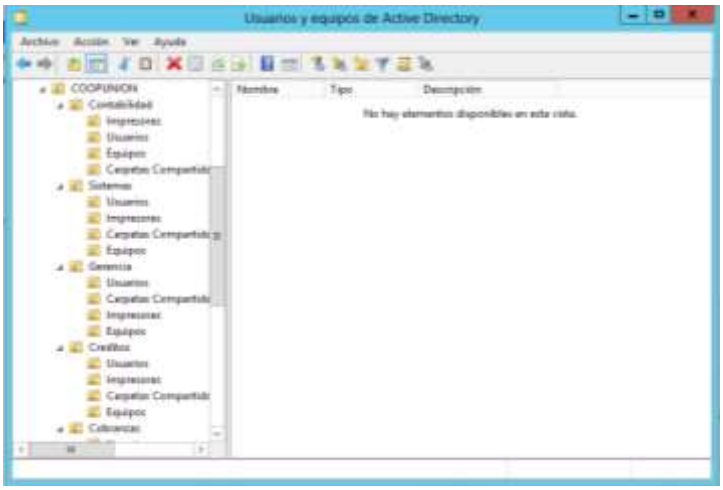

Fig. 48 Unidades Organizativas creadas

Creación de Usuarios de Active Directory

La información de cada usuario de Active Directory debe ser bien detallada.

En la unidad organizativa Usuarios de cada Departamento se crean los usuarios correspondientes:

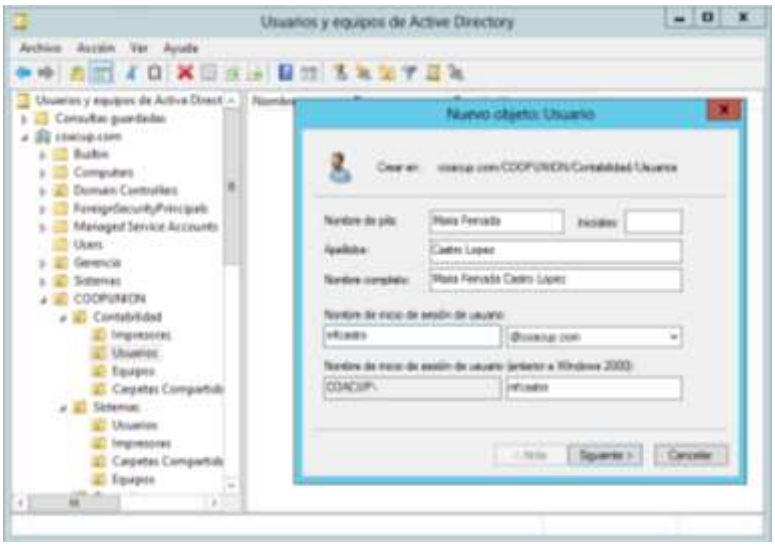

Fig. 49 Creación de Usuarios

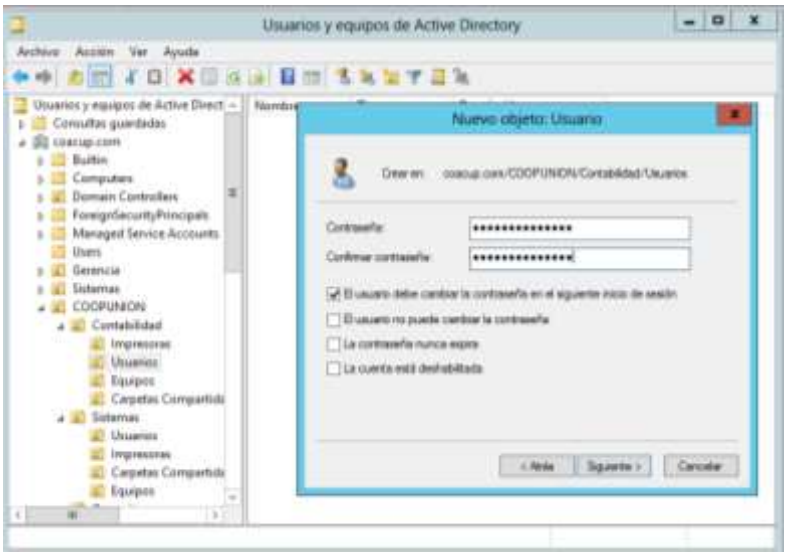

Fig. 50 Creación de Usuarios

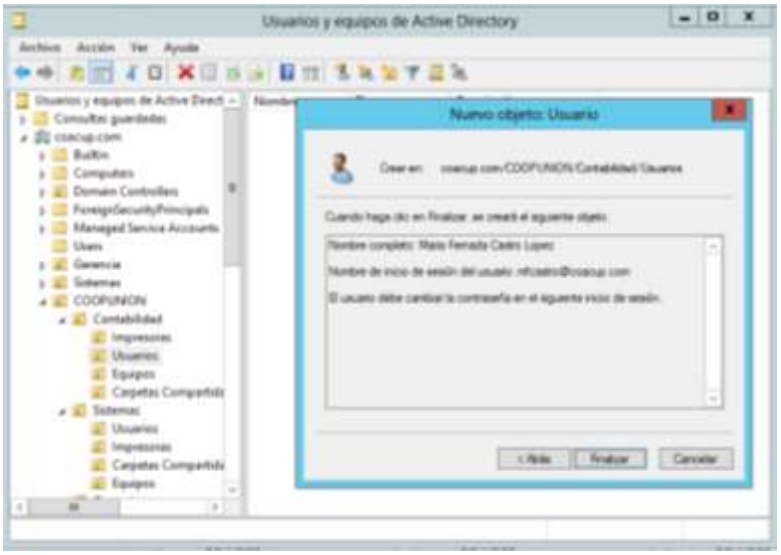

Fig. 51 Creación de Usuarios

Configuración de Políticas de Active Directory

Las políticas se configuran de acuerdo a lo establecido anteriormente. **(Literal 4.4)**

Las configuraciones se las realizan en "Administración de directivas de grupo"

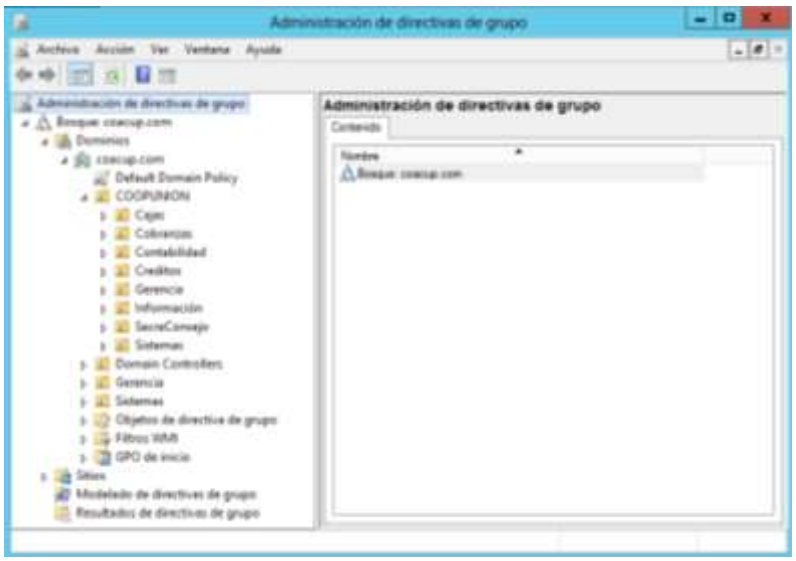

Fig. 52 Administración de directivas de grupo

Creación de Directivas de Grupo:

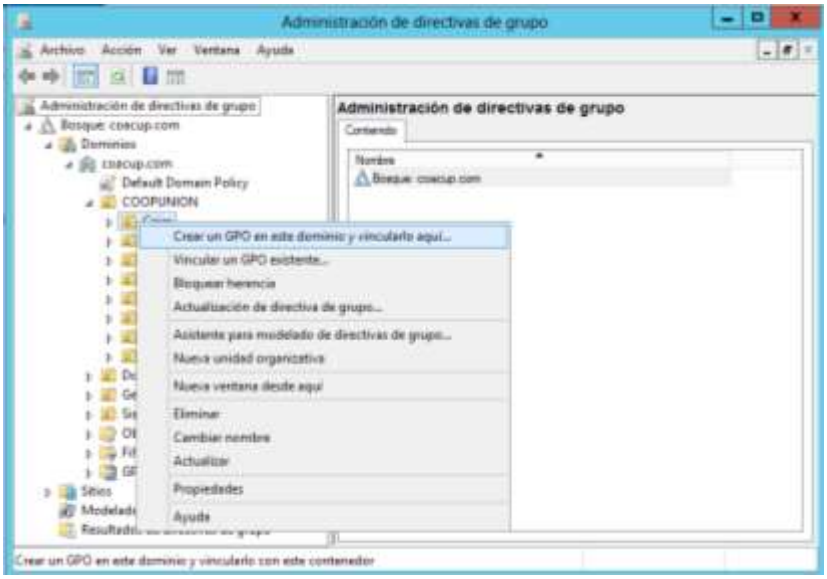

Fig. 53 Creación de Directiva de Grupo

Dar nombre a la GPO y Aceptamos.

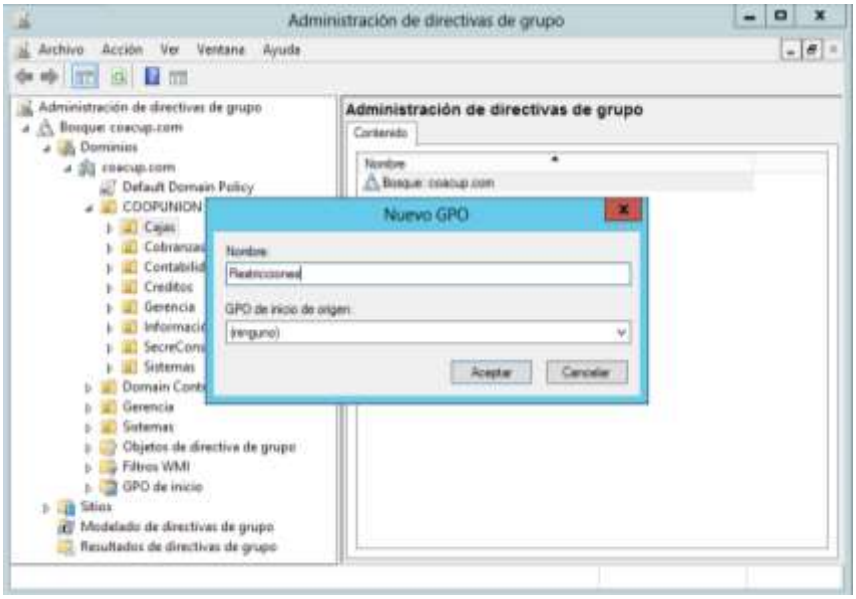

Fig. 54 Creación de Directiva de Grupo

A continuación de presentan algunas configuraciones dentro del Servidor de Active Directory:

Dar click derecho sobre la nueva GPO y damos click en editar.

Dirigirse a Inicio>Editor de administración de directivas de grupo, dentro de configuración de seguridad encontraremos Directiva de contraseñas.

Dar click derecho en Vigencia máxima de la contraseña y en propiedades.
Definir la configuración de directiva para que las contraseñas expiren después de 30 días damos clic en aplicar y luego Aceptar.
Dar click derecho en la opción Almacenar contraseñas con cifrado reversible y vamos a sus propiedades. Habilitamos y damos ok.
Volver a dar click derecho pero sobre la opción Exigir historial de contraseñas.
Habilitar la configuración de directivas y especificamos el número de contraseñas a recordar, aplicamos los cambios y luego aceptar.

A todos los usuarios, exceptuando los administradores del dominio y los usuarios del departamento de Sistemas, tendrán restringido el acceso a los siguientes componentes:

- Menú Ejecutar
- Panel de control
- REGEDIT
- Unidad C: (Visualizar la unidad)
- Reproducción automática de medios extraíbles
- El administrador será el único con la contraseña de supervisor para el Asesor de Contenidos.
- Desbloquear la barra de tareas (Siempre permanecerá bloqueada)
- Acceso del Lecto-escritura a cualquier medio de almacenamiento extraíble.

Crear un nueva GPO para las restricciones.

Nombrar la GPO y Aceptar.

Ahora Inicio>Editor de administración de directivas de grupo dentro de él dirigir a configuración de usuario>directivas>plantillas administrativas>menú de inicio y Barras de tareas. Buscamos la opción

Quitar el menú ejecutar del menú de inicio y damos click derecho en editar.

Habilitar y damos ok.

Ahora en panel de control, buscamos la opción que dice prohibir acceso a panel de control y damos en editar.

Habilitar y dar ok.

Para ocultar la unidad C: / para esto nos dirigimos a Configuración de usuario> directivas>plantillas administrativas>componentes de windows>explorador de Windows. Buscamos la opción Ocultar estas unidades específicas en mi pc, click derecho en editar.

Se debe crear una contraseña para el administrador de contenidos y damos aceptar.

Para bloquear la barra de tareas nos dirigimos a Configuración de usuario>directivas>plantillas administrativas>escritorio>menú inicio y barra de tareas.
Buscar la opción Bloquear la barra de tareas, damos click derecho y editar.
Habilitar y dar ok.

Para restringir Lecto-Escritura a cualquier medio de almacenamiento extraíble para ello vamos a configuración de usuario>directivas>plantillas administrativas>sistema>acceso de almacenamiento extraíble.

Buscar la opción llamada Todas las clases de almacenamiento extraíble. Dar click en editar.

Habilitar y ok.

Crear una GPO con el nombre de Restricciones usuarios.

Ahora ocultar todos los elementos de escritorio nos dirigimos a Configuración de usuario >directivas>plantillas administrativas>escritorio

Buscar el directorio Escritorio y dentro de él la opción Ocultar y deshabilitar todos los elementos del escritorio.

Dar click derecho y editar. Habilitamos y damos ok.

Quitar el administrador de tareas para esto vamos a Configuración de usuario >directivas>plantillas administrativas>sistema>Opciones de Ctrl+Alt+Del

Vamos a la opción quitar administrador de tarea, click derecho y propiedades.

4.4.2 Configuración de un Servidor Proxy

Dentro de la cooperativa es necesario realizar el control de los contenidos de internet a los que pueden o no acceder los usuarios. Para la realización de este control se utilizará un servidor Centos 7, en el cual se instalará y configurará un servidor proxy squid.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes.

Instalación de Squid:

Bajo permisos de administrador en el terminal ejecutamos lo siguiente:

 # yum -y install squid

Para SELinux permita a Squid operar en modo transparente se ejecuta:

 # setsebool -P squid_use_tproxy 1

Squid utiliza el archivo de configuración localizado en /etc/squid/squid.conf, el cual se puede modificar mediante:

 # nano /etc/squid/squid.conf

A continuación se presenta la configuración de squid.conf:

 # Recommended minimum configuration:

#

 # Example rule allowing access from your local networks.

 # Adapt to list your (internal) IP networks from where browsing

 # should be allowed

acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

acl localnet src fc00::/7 # RFC 4193 local private network range

acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

#Mis acls

acl redlocal src "/etc/squid/listas/local.txt"

acl gerencia src "/etc/squid/listas/gerencia.txt"

acl presidencia src "/etc/squid/listas/presidencia.txt"

acl sistemas src "/etc/squid/listas/sistemas.txt"

acl permitidas dstdomain "/etc/squid/listas/webs.html"

acl denegado dstdomain "/etc/squid/listas/denegado.html"

acl palabras url_regex "/etc/squid/listas/porno.txt"

acl extensiones urlpath_regex "/etc/squid/listas/extensiones.txt"

acl blacklist-web dstdomain -i "/etc/squid/listas/blacklist-web"

acl SSL_ports port 443

acl Safe_ports port 80 # http

acl Safe_ports port 21 # ftp

acl Safe_ports port 443 # https

acl Safe_ports port 70 # gopher

acl Safe_ports port 210 # wais

acl Safe_ports port 1025-65535 # unregistered ports

acl Safe_ports port 280 # http-mgmt

acl Safe_ports port 488 # gss-http

acl Safe_ports port 591 # filemaker

acl Safe_ports port 777 # multiling http

acl CONNECT method CONNECT

#

 # Recommended minimum Access Permission configuration:

#

 # Deny requests to certain unsafe ports

http_access deny !Safe_ports

 # Deny CONNECT to other than secure SSL ports

http_access deny CONNECT !SSL_ports

 # Only allow cachemgr access from localhost

http_access allow localhost manager

http_access deny manager

 # We strongly recommend the following be uncommented to protect innocent

 # web applications running on the proxy server who think the only

 # one who can access services on "localhost" is a local user

#http_access deny to_localhost

#

 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

#

 # Example rule allowing access from your local networks.

 # Adapt localnet in the ACL section to list your (internal) IP networks

 # from where browsing should be allowed

#http_access allow localnet

http_access allow localhost

#http_access allow gerencia presidencia sistemas

http_access allow redlocal !extensiones !denegado !blacklist-web

 # And finally deny all other access to this proxy

http_access deny all

 # Squid normally listens to port 3128

http_port 192.168.0.200:3128 intercept

http_port 172.16.1.2:3128 intercept

http_port 3129 intercept

 # Uncomment and adjust the following to add a disk cache directory.

cache_dir ufs /var/spool/squid 1000 16 256

 # Leave coredumps in the first cache dir

coredump_dir /var/spool/squid

#

 # Add any of your own refresh_pattern entries above these.

#

refresh_pattern ^ftp: 1440 20% 10080

refresh_pattern ^gopher: 1440 0% 1440

refresh_pattern -i (/cgi-bin/|\?) 0 0% 0

refresh_pattern . 0 20% 4320

En la declaración de ACLs se muestran ***"/etc/squid/listas/"*** que es el directorio en el cual se almacenan archivos con el direccionamiento ip, páginas web bloquedas entre otros, que nos permiten un mayor control de contenidos del servidor proxy.

Finalmente es necesario:

Activar Servicio Squid

 # systemctl mask squid

Iniciar Servicio Squid

 # systemctl stop squid

4.4.3 Configuración del Firewall en base a las políticas de seguridad

Este servicio se instalará y configurará en el equipo Centos 7 que aloja el servidor Proxy.

Cabe destacar que Centos 7 utiliza diferentes comandos, a los utilizados en versiones anteriores de este sistema operativo.

Centos 7 incorpora el servicio Firewalld en lugar de Iptables. La configuración del servidor Firewall para la cooperativa se lo realizará en base a Iptables considerando que el Jefe de Sistemas cuenta con conocimiento del mismo, para lo cual es necesario realizar lo siguiente:

Desactivar Servicio Firewalld.

 # systemctl mask firewalld

Detener Servicio Firewalld.

 # systemctl stop firewalld

Es necesario instalar con permisos de Administrador lo siguiente:

 # yum –y install iptables

Centos permité la ejecución de scripts, para la configuración de nuestro Firewall se ha desarrollado un Script con todas las reglas necesarias para cumplir con las políticas anteriormente expuestas:

```
#! /bin/bash
echo Iniciando Firewall....
sysadmin="70:5A:B6:93:CB:4F"
internet=enp3s0
publica=186.3.45.99
puertolan=enp4s0
lanip=192.168.0.200
local=192.168.0.0/24
srvdnslocal=192.168.0.4/24
#####################################
puertovpn=enp4s1
lanvpn=172.16.1.0/30,192.168.2.0/24,192.168.1.0/24
vpnip=172.16.1.2
route=/usr/acl
```

```
UNIVERSO=0.0.0.0/0
# alias
alias sed="sed '/#.*/d'"
# Optional modules
iptables=/sbin/iptables
sysctl=/sbin/sysctl
modprobe=/sbin/modprobe
rmmod=/sbin/rmmod
arp=/usr/sbin/arp
## FLUSH de reglas
echo Aplicando Reglas
$iptables -F
$iptables -X
$iptables -Z
$iptables -t nat -F
$iptables -t filter -F
# Cargar modulos requeridos del kernel
$modprobe ip_conntrack_ftp
$modprobe ip_conntrack_irc
$modprobe nf_nat_pptp
$modprobe nf_conntrack_pptp
#POLITICAS POR DEFECTO
$iptables -P INPUT ACCEPT
$iptables -P OUTPUT ACCEPT
$iptables -P FORWARD ACCEPT
#El localhost se deja acceso total
$iptables -A INPUT -i lo -j ACCEPT
$iptables -A OUTPUT -o lo -j ACCEPT
$iptables -A INPUT -i $internet -j ACCEPT
$iptables -A OUTPUT -o $internet -j ACCEPT
```

```
# Acceso a Internet a través del Firewall
# Source NAT de la red local y la VPN
```

$iptables -t nat -A POSTROUTING -o $internet -s $local -j SNAT --to $publica

$iptables -t nat -A POSTROUTING -o $internet -s $lanvpn -j SNAT --to $publica

$iptables -t nat -A POSTROUTING -o $puertovpn -s $local -j SNAT --to $vpnip

$iptables -t nat -A POSTROUTING -o $puertolan -s $lanvpn -j SNAT --to $lanip

###VPN

#Sesion de Netbios a la VPN

$iptables -A FORWARD -s $local -i $puertolan -o $puertovpn -d $lanvpn -p tcp -m multiport --dports 138,139 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -i $puertovpn -o $puertolan -d $local -p tcp -m multiport --sports 138,139 -j ACCEPT

$iptables -A FORWARD -s $local -i $puertolan -o $puertovpn -d $lanvpn -p udp -m multiport --dports 138,139 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -i $puertovpn -o $puertolan -d $local -p udp -m multiport --sports 138,139 -j ACCEPT

#Conexión mediante VNC a la VPN

$iptables -A FORWARD -s $local -i $puertolan -o $puertovpn -d $lanvpn -p tcp --dport 5900 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -i $puertovpn -o $puertolan -d $local -p tcp --sport 5900 -j ACCEPT

$iptables -A FORWARD -s $local -i $puertolan -o $puertovpn -d $lanvpn -p udp --dport 5900 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -i $puertovpn -o $puertolan -d $local -p udp --sport 5900 -j ACCEPT

#Transmision de SQL a la VPN

$iptables -A FORWARD -s $local -i $puertolan -o $puertovpn -d $lanvpn -p tcp -m multiport --dports 1433,1434 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -i $puertovpn -o $puertolan -d $local -p tcp -m multiport --sports 1433,1434 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -d 192.168.0.1 -p tcp --dport 1433 -j ACCEPT

$iptables -A FORWARD -s 192.168.0.1 -d $lanvpn -p tcp --sport 1433 -j

ACCEPT

$iptables -A FORWARD -s $lanvpn -d 192.168.0.1 -p udp --dport 1433 -j ACCEPT

$iptables -A FORWARD -s 192.168.0.1 -d $lanvpn -p udp --sport 1433 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -d 192.168.0.1 -p tcp --dport 1434 -j ACCEPT

$iptables -A FORWARD -s 192.168.0.1 -d $lanvpn -p tcp --sport 1434 -j ACCEPT

$iptables -A FORWARD -s $lanvpn -d 192.168.0.1 -p udp --dport 1434 -j ACCEPT

$iptables -A FORWARD -s 192.168.0.1 -d $lanvpn -p udp --sport 1434 -j ACCEPT

#Bloquear IPs Indebidas, siempre antes de dar acceso a la web

 # BLOCK FACEBOOK

for i in $(/usr/bin/whois -h whois.radb.net '!gAS32934' | tr ' ' '\n' | sort -n -k1,1 -k2,2 -k3,3 -k4,4 |grep /)

do $iptables -A FORWARD -d $i -j DROP

done

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 31.13.73.0/24 --dport 443 -j DROP

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 31.13.65.0/24 --dport 443 -j DROP

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 173.252.64.0/18 --dport 443 -j DROP

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 199.16.156.0/22 --dport 443 -j DROP

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 201.218.32/19 --dport 443 -j DROP

$iptables -A FORWARD -i $puertolan -o $internet -p tcp -d 181.198.79.192/26 --dport 443 -j DROP

###

#Navegación de Internet

 # Aceptamos las peticiones a los servidores web (http) de $internet y las respuetas:

$iptables -A FORWARD -i $puertolan -s $local -o $internet -p tcp --dport 80 -j ACCEPT

$iptables -A FORWARD -o $puertolan -d $local -i $internet -p tcp --sport 80 -j ACCEPT

$iptables -A FORWARD -i $puertovpn -s $lanvpn -o $internet -p tcp --dport 80 -j ACCEPT

$iptables -A FORWARD -o $puertovpn -d $lanvpn -i $internet -p tcp --sport 80 -j ACCEPT

 # Proxy Transparente: peticiones al puerto 80 redirigir al SQUID(3128)

$iptables -A INPUT -s $local -p tcp --dport 3128 -j ACCEPT

$iptables -A OUTPUT -d $local -p tcp --sport 3128 -j ACCEPT

$iptables -A INPUT -s $lanvpn -p tcp --dport 3128 -j ACCEPT

$iptables -A OUTPUT -d $lanvpn -p tcp --sport 3128 -j ACCEPT

$iptables -t nat -A PREROUTING -i $puertolan -p tcp --dport 80 -j DNAT --to $lanip:3128

$iptables -t nat -A PREROUTING -i $puertolan -p tcp --dport 80 -j REDIRECT --to-port 3128

$iptables -t nat -A PREROUTING -i $puertovpn -p tcp --dport 80 -j DNAT --to $vpnip:3128

$iptables -t nat -A PREROUTING -i $puertovpn -p tcp --dport 80 -j REDIRECT --to-port 3128

 # Aceptamos las peticiones a los servidores web (https) de $internet y las respuetas:

$iptables -A FORWARD -i $puertolan -s $local -o $internet -p tcp --dport 443 -j ACCEPT

$iptables -A FORWARD -o $puertolan -d $local -i $internet -p tcp --sport 443 -j ACCEPT

$iptables -A FORWARD -i $puertovpn -s $lanvpn -o $internet -p tcp --dport 443 -j ACCEPT

$iptables -A FORWARD -o $puertovpn -d $lanvpn -i $internet -p tcp --sport 443 -j ACCEPT

 # Aceptamos las peticiones DNS del equipo $srvdnslocal:

$iptables -A FORWARD -i $puertolan -s $srvdnslocal -o $internet -p udp --dport 53 -j ACCEPT

$iptables -A FORWARD -o $puertolan -d $srvdnslocal -i $internet -p udp --sport 53 -j ACCEPT

$iptables -A FORWARD -i $puertolan -s $srvdnslocal -o $internet -p tcp --dport 53 -j ACCEPT

$iptables -A FORWARD -o $puertolan -d $srvdnslocal -i $internet -p tcp --sport 53 -j ACCEPT

 # Se permiten consultas DNS al servidor de la red local:

$iptables -A OUTPUT -o $puertolan -s $lanip -d $srvdnslocal -p udp --dport 53 -j ACCEPT

$iptables -A INPUT -i $puertolan -d $lanip -s $srvdnslocal -p udp --sport 53 -j ACCEPT

$iptables -A OUTPUT -o $puertolan -s $lanip -d $srvdnslocal -p tcp --dport 53 -j ACCEPT

$iptables -A INPUT -i $puertolan -d $lanip -s $srvdnslocal -p tcp --sport 53 –j ACCEPT

Se Permite entrar por ssh desde la red local:

$iptables -A INPUT -i $puertolan -s $local -d $lanip -p tcp --dport 22 -j ACCEPT

$iptables -A OUTPUT -o $puertolan -d $local -s $lanip -p tcp --sport 22 -j ACCEPT

 # Se permite ping desde la red local y la VPN:

$iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

$iptables -A INPUT -i $puertolan -p icmp --icmp-type echo-request -j ACCEPT

$iptables -A OUTPUT -o $puertolan -p icmp --icmp-type echo-reply -j ACCEPT

$iptables -A INPUT -i $puertovpn -p icmp --icmp-type echo-request -j ACCEPT

$iptables -A OUTPUT -o $puertovpn -p icmp --icmp-type echo-reply -j ACCEPT

Cerrarlos puertos bien conocidos

iptables −A INPUT −s 0.0.0.0/0 −p tcp −dport 1:1024 −j DROP

iptables −A INPUT −s 0.0.0.0/0 −p udp −dport 1:1024 −j DROP

exit

Al ejecutar el Script obtendremos los siguientes resultados:

Fig. 55 Ejecución de Script

#Bloquear IPs Indebidas, siempre antes de dar acceso a la web

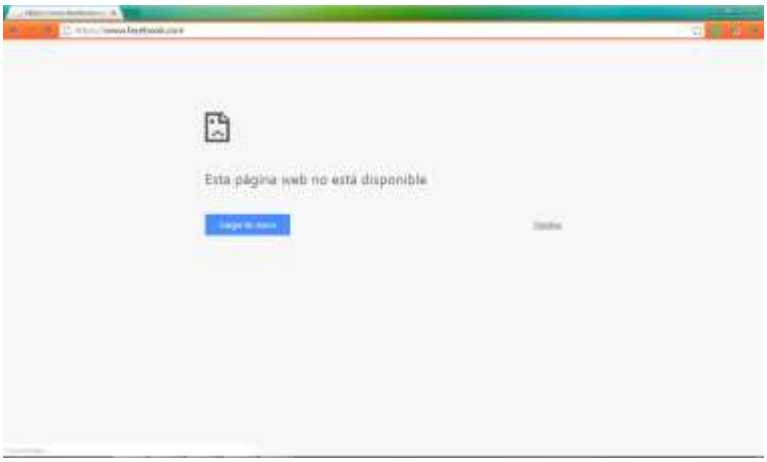

Fig. 56 Acceso Denegado a Facebook Puerto 443

Fig. 57 Acceso Denegado a Facebook Puerto 80

Navegación de Internet

 # Aceptamos las peticiones a los servidores web (http) de $internet y las respuetas:

 # Proxy Transparente: peticiones al puerto 80 redirigir al SQUID(3128)

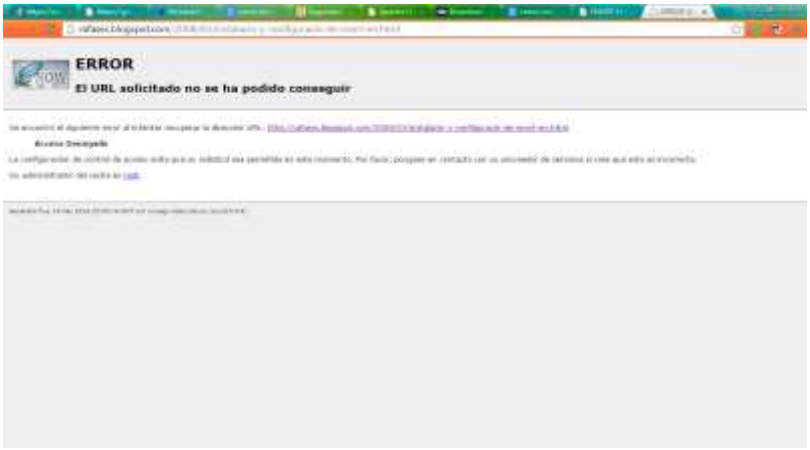

Fig. 58 Acceso Denegado a Blogspot Proxy transparente

 # Aceptamos las peticiones a los servidores web (https) de $internet y las respuetas:

Fig. 59 Acceso a Internet

Se Permite acceder por ssh desde la red local y solo por el Computador del Administrador de la Red cuya MAC se especifica en el Script.:

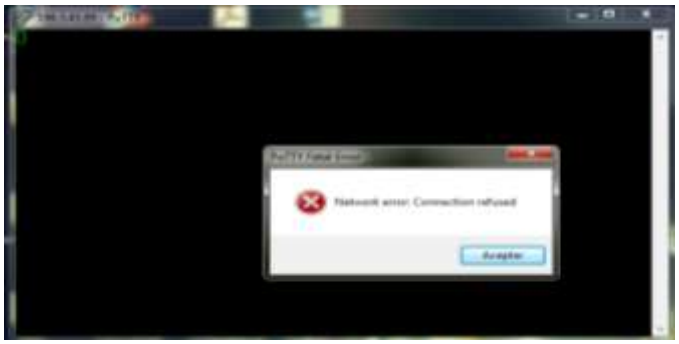

Fig. 60 Acceso Denegado por la interfaz publica

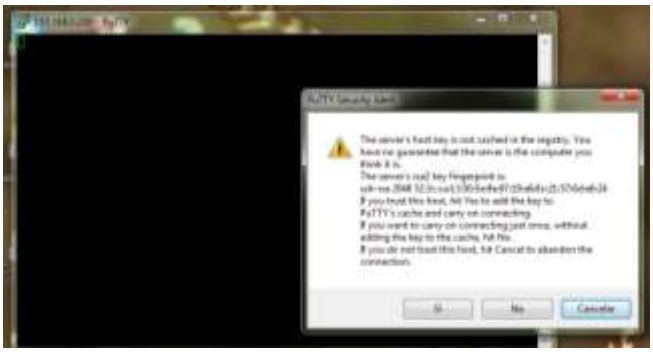

Fig. 61 Acceso a través de la interfaz LAN

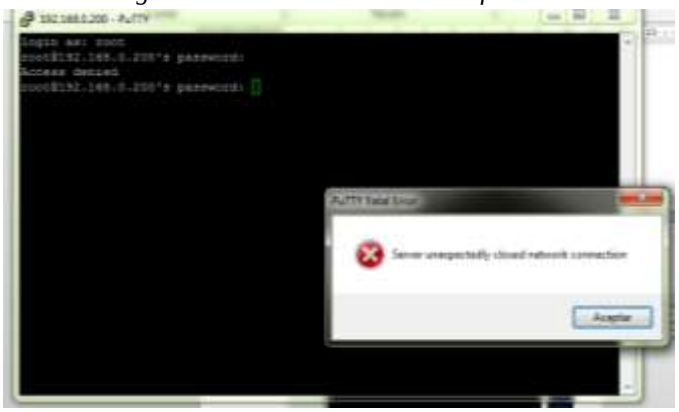

Fig. 62 Acceso Denegado usuario ROOT

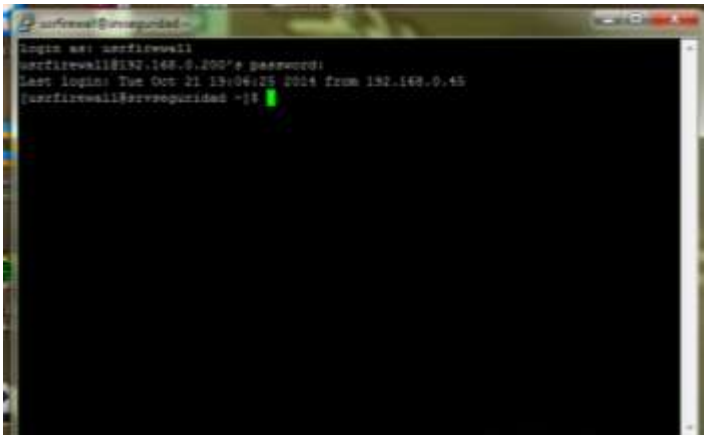

Fig. 63 Acceso por medio del Usuario usrfirewall

4.4.4 Configuración del Servidor IDS

Un Sistema de Detección de Intrusos se encuentra a la entrada de la red, pudiendo observar todo el tráfico de red.

Se instalará y configurará Snort servicio que se puede integrar en Centos 7; el mismo que no cuenta con entorno gráfico propio.

4.4.4.1 Configuraciones Preliminares

Actualizar el sistema y reiniciarlo:

#yum update -y

#reboot

Instalar repositorio EPEL:

#wget http://dl.fedoraproject.org/pub/epel/7/epel-release-7.noarch.rpm

#wget http://ftp.riken.jp/Linux/fedora/epel/RPM-GPG-KEY-EPEL-7

#rpm --import RPM-GPG-KEY-EPEL-7

#rpm -ivh epel-release-7.noarch.rpm

Instalar PCRE, libdnet y otros paquetes necesarios:

#yum install libdnet libdnet-devel pcre pcre-devel gcc make flex byacc bison kernel-devel libxml2-devel wget -y

Crear un directorio de Snort para ir guardando el código de los diferentes módulos:

#mkdir /usr/local/src/snort

#cd /usr/local/src/snort

Descargar e instalar libpcap:

#wget http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz -O libpcap.tar.gz

#tar zxvf libpcap.tar.gz

*#cd libpcap-**

#./configure && make && make install

#echo "/usr/local/lib" >> /etc/ld.so.conf

#ldconfig -v

Descargar e instalamos DAQ:

#cd /usr/local/src/snort

#wget http://www.snort.org/dl/snort-current/daq-2.0.0.tar.gz -O daq.tar.gz

#tar zxvf daq.tar.gz

*#cd daq-**

#./configure && make && make install

#ldconfig -v

Creamos un usuario y un grupo para Snort:

#groupadd snort

#useradd -g snort snort

4.4.4.2 Instalación de Snort

Descargar e instalar Snort:

#cd /usr/local/src/snort

#wget http://www.snort.org/dl/snort-current/snort-2.9.4.6.tar.gz -O snort.tar.gz

#tar zxvf snort.tar.gz

*#cd snort-2**

#./configure --prefix /usr/local/snort --enable-sourcefire && make && make install

Crear links para los ficheros de Snort:

#ln -s /usr/local/snort/bin/snort /usr/sbin/snort

#ln -s /usr/local/snort/etc /etc/snort

Configuramos Snort para que se inicie con el inicio del sistema (Como servicio):

#cp rpm/snortd /etc/init.d/

#chmod +x /etc/init.d/snortd

#cp rpm/snort.sysconfig /etc/sysconfig/snort

#chkconfig --add snortd

Descargar las reglas de Snort desde http://www.snort.org/snort-rules para lo cual es necesario registrarse, las descargamos en /usr/local/src/snort.

Extraer las reglas en el nuevo directorio:

#cd /usr/local/snort

*#tar zxvf /usr/local/src/snort/snortrules-snapshot-2**

Crear el directorio para el login de Snort:

#mkdir -p /usr/local/snort/var/log

#chown snort:snort /usr/local/snort/var/log

#ln -s /usr/local/snort/var/log /var/log/snort

Creamos los links para las reglas dinámicas y para los directorios:

#ln –s

/usr/local/snort/lib/snort_dynamicpreprocessor/usr/local/lib/snort_dynamicpreprocessor

#ln -s

/usr/local/snort/lib/snort_dynamicengine/usr/local/lib/snort_dynamicengine

#ln -s /usr/local/snort/lib/snort_dynamicrules /usr/local/lib/snort_dynamicrules

Permisos a Snort:

#chown -R snort:snort /usr/local/snort

Creamos el directorio para las reglas dinámicas:

#mkdir /usr/local/snort/lib/snort_dynamicrules

Copiar las reglas dinámicas:

#cp /usr/local/snort/so_rules/precompiled/RHEL-7-0/x86-64/2.9/*so*

/usr/local/snort/lib/snort_dynamicrules/

Realizar el dump de las reglas:

#snort -c /usr/local/snort/etc/snort.conf --dump-dynamic-rules=/usr/local/snort/so_rules

Habilitar todas las reglas dinámicas:

#nano /usr/local/snort/etc/snort.conf

```
# dynamic library rules
include $SO_RULE_PATH/bad-traffic.rules
include $SO_RULE_PATH/chat.rules
include $SO_RULE_PATH/dos.rules
include $SO_RULE_PATH/exploit.rules
include $SO_RULE_PATH/icmp.rules
include $SO_RULE_PATH/imap.rules
include $SO_RULE_PATH/misc.rules
include $SO_RULE_PATH/multimedia.rules
include $SO_RULE_PATH/netbios.rules
include $SO_RULE_PATH/nntp.rules
include $SO_RULE_PATH/p2p.rules
include $SO_RULE_PATH/smtp.rules
include $SO_RULE_PATH/snmp.rules
include $SO_RULE_PATH/specific-threats.rules
include $SO_RULE_PATH/web-activex.rules
include $SO_RULE_PATH/web-client.rules
include $SO_RULE_PATH/web-iis.rules
include $SO_RULE_PATH/web-misc.rules
```

Comprobar que Snort funciona de forma correcta:

#snort -c /usr/local/snort/etc/snort.conf -T

Probar y testear un poco con el podríamos realizar el siguiente comando:

#snort -c /usr/local/snort/etc/snort.conf -A console

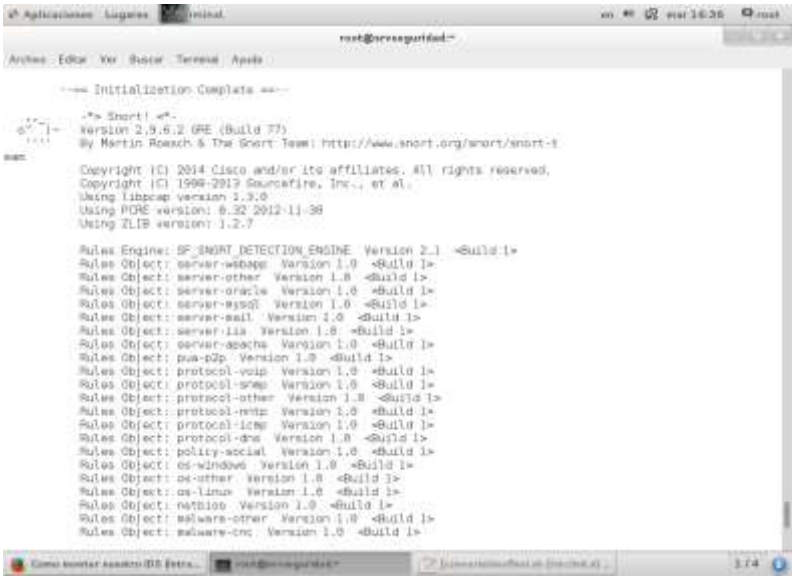

Fig. 64 Testeo con Snort

4.4.4.3 Resultados de Snort IDS

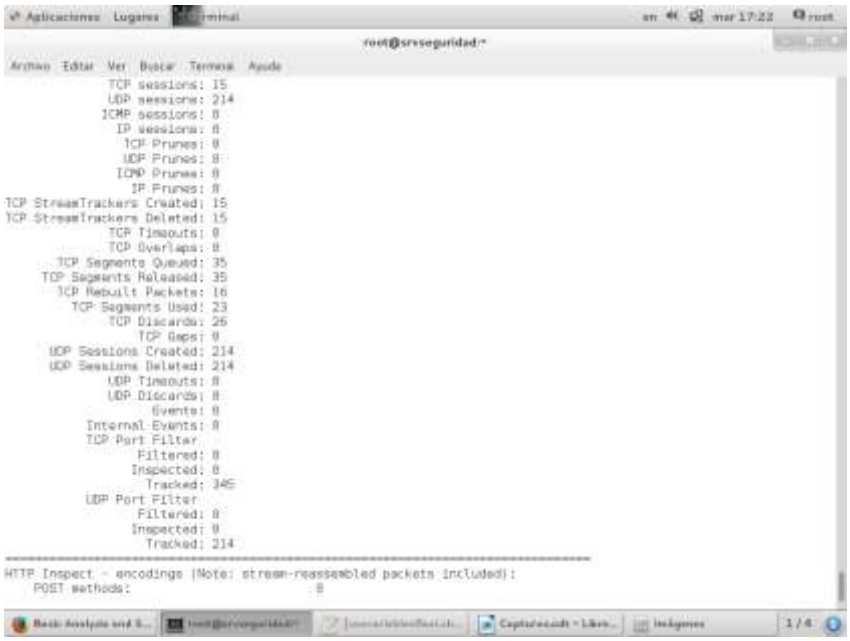

Fig. 65 Resultados del Testeo con Snort

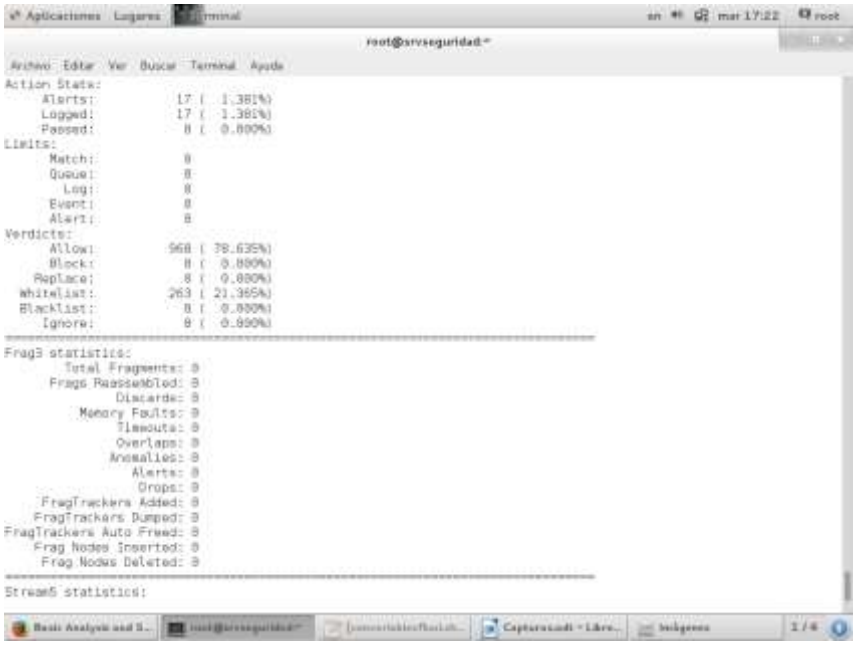

Fig. 66 Resultados del Testeo con Snort

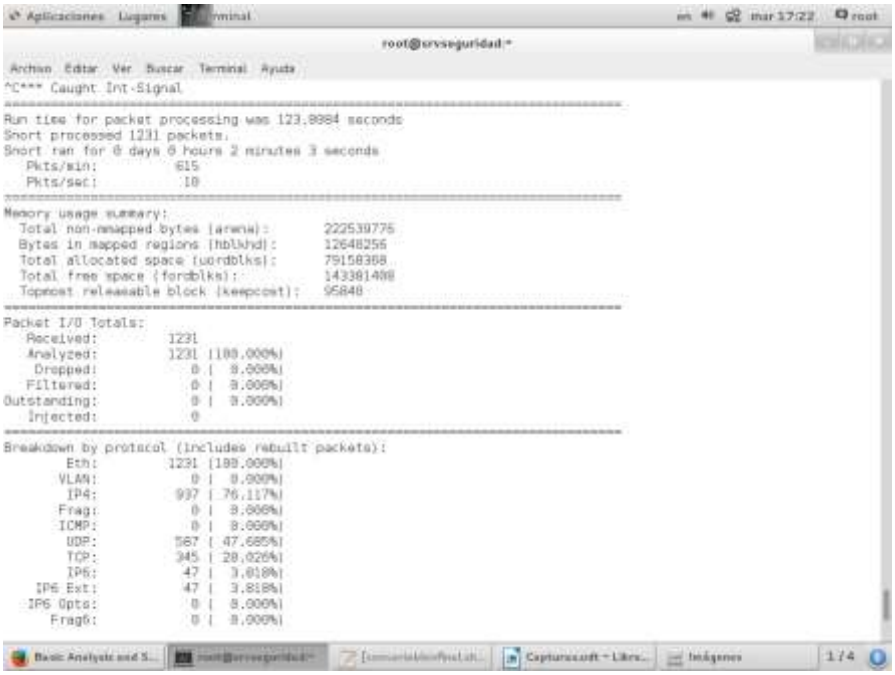

Fig. 67 Resultados del Testeo con Snort

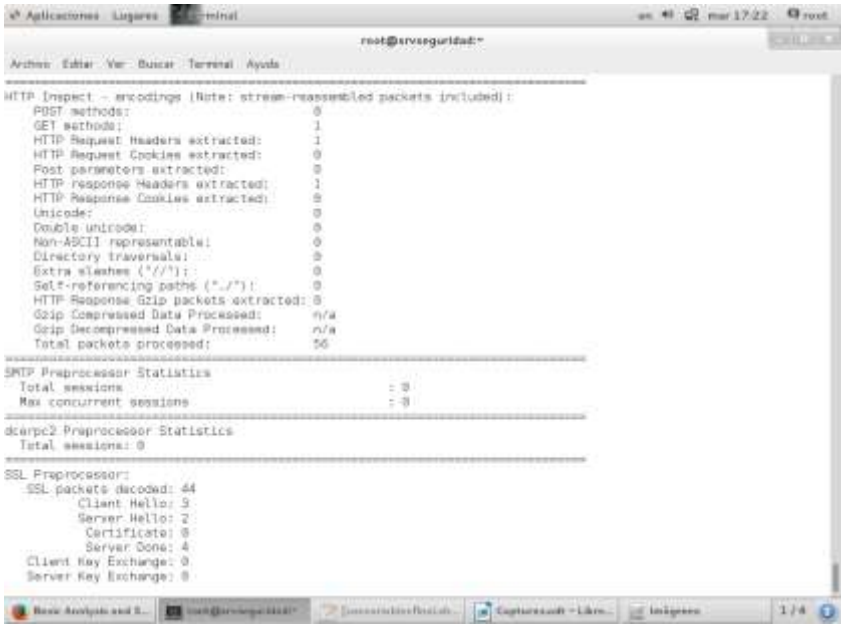

Fig. 68 Resultados del Testeo con Snort

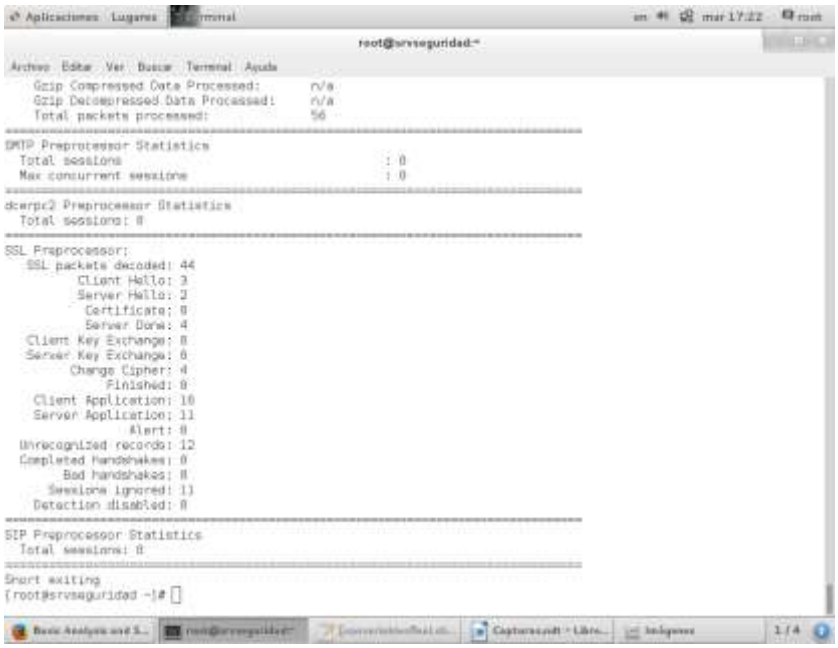

Fig. 69 Resultados del Testeo con Snort

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Tener conocimientos acerca de metodologías y mecanismos de seguridad informática es necesario ya que la tecnología de las comunicaciones avanza y la información que se transmite por los diferentes canales de comunicación son de gran importancia para sus propietarios por lo que es necesario resguardarla adecuadamente.
- La instalación de recursos de seguridad informática sean estos hardware o software son de vital importancia para cualquier tipo de organización, ya que estos son barreras de protección para su recurso informático.
- Una adecuada planificación para recolectar información acerca de los activos, se la realiza en base a metodologías que ayudarán en reconocer la importancia de cada uno de los activos para la comunicación.
- Existen varias herramientas que nos permiten monitorear los eventos que se producen dentro de una red, estos nos presentan información relevante para conocer que puertos son utilizados, además conocer los hosts interconectados y reconocer a posibles intrusos.
- El análisis de riesgos y vulnerabilidades con base a NIST 800-30, en el cual se definieron los activos, amenazas y vulnerabilidades son un punto inicial para la implementación de una adecuada seguridad informática para la red de datos.
- Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información y comunicación para cada usuario o grupo de usuarios en una declaración de política de accesos.

- Es muy útil implementar un servidor de dominio que tenga la función además de active directory ya que este permite un control adecuado de todos los usuarios de una organización permitiendo de esta manera restringir y otorgar permisos necesarios de acuerdo a las funciones de los usuarios.
- Una correcta configuración de mecanismos software como servidores proxy, firewall e IDs son fundamentales para brindar seguridad básica a una organización, ya que estos brindan control de contenido, denegación de puertos innecesarios y además nos permiten el monitoreo de paquetes dentro de la red.
- Una de las bases fundamentales es el apoyo de la alta gerencia, ya que se requiere un cambio de cultura y concientización hace necesario el impulso constante de la Dirección.
- La seguridad de la información no se debe considerar como un aspecto solo tecnológico sino de tipo organizacional y de gestión, es decir organizar la seguridad de la información e implementar la seguridad en base a los requerimientos de la empresa.

5.2 RECOMENDACIONES

- Identificar de forma clara cuales son los activos y asignarles un grado de protección según su criticidad, indicando como debe ser tratado y protegido; para de esta forma mantener una adecuada protección de los activos.
- Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar es permanente para lo cual es necesario de un proceso continuo, más no de acciones puntuales
- Documentar los procedimientos operativos, cualquiera que sea su tipo, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes.
- Es aconsejable que se aumente el personal que administra el departamento de IT, pues al implementar Seguridad Informática se incrementan las responsabilidades y al recaer en una sola persona se vuelve complicada la ejecución de las diferentes tareas.

- Es recomendable que el desarrollo de seguridad informática respete las normas y leyes vigentes del país en base a los documentos que las instituciones reguladoras proporcionan.
- Se recomienda la implementación de la norma 27001 porque a más de proteger la empresa, permite mejorar la imagen al exterior.
- La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no un estado estático, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.

Bibliografía

[1] VENEGAS, Mariana "Estudio de la importancia de las TICs en Ecuador", utpl.edu.ec, Marzo, 2011 [Online]. Disponible en: http://dspace.utpl.edu.ec/jspui/bitstream/123456789/2690/1/VENEGAS%20BARRAGAN%20MARIANA%20DEL%20CARMEN%20Y%20YEPEZ%20MONTENEGRO%20ROSA%20MARLENE.pdf [Accedido: Marzo. 10, 2014].

[2] PILLA, Julio "Implementación de seguridad en la red interna de datos para el manejo adecuado de usuarios y acceso remoto en el Instituto tecnológico Pelileo", uta.edu.ec, Mayo, 2013 [Online]. Disponible en: http://repo.uta.edu.ec/handle/123456789/4936 [Accedido: Marzo. 10, 2014].

[3] BALTAZAR, José "Diseño e Implementación de un esquema de seguridad perimetral para redes de datos. Caso práctico: Dirección General del Colegio de Ciencias y Humanidades", ptolomeo.unam.mx, 2011 [Online]. Disponible en: https://www.google.com.ec/search?q=implementacion+de+un+esquema+de+seguridad&rlz=1C1AVNC_enEC584EC584&oq=implementacion+de+unn+esquema+de+seguri&aqs=chrome.1.69i57j0.9516j0j7&sourceid=chrome&es_sm=93&ie=UTF-8# [Accedido: Marzo. 10, 2014].

[4] VILET, Gerardo "La tecnología y los sistemas de información", books.google.com.ec, Mayo, 1999. [Online]. Disponible en: https://www.google.com.ec/search?tbo=p&tbm=bks&q=isbn:9687674571 [Accedido: Marzo. 10, 2014].

[5] NEREIDA GF "Informática 1", sites.google.com, [Online]. Disponible en: https://sites.google.com/site/dnereidagfinformatica1/ [Accedido: Marzo. 10, 2014].

[6] RUIZ, P. "Concepto de Sistema Operativo de Red", somebooks.es, Agosto, 2013 [Online]. Disponible en: http://somebooks.es/?p=3358 [Accedido: Marzo. 10, 2014].

[7] GARCIA, Rubi RIOS, Edgar "Canal Cifrado para comunicación Cliente/Servidor", Ptolomeo.unam.mx, Abril, 2011 [Online]. Disponible en: www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/.../Tesis.pdf? [Accedido: Marzo. 10, 2014].

[8] CALVO, A. "Normas y Estándares CERT" ISO 27001, cert.org, 2006 [Online]. Disponible en: http://www.cert.org/octave/ [Accedido: Junio. 23, 2014].

[9] ArCERT. (s.f.). “Manual de Seguridad en Redes”. [Online]. Disponible en http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf [Accedido: Junio. 23, 2014].

[10] ERB, M. "Gestión de Riesgo en la Seguridad Informática", 2006 [Online]. Disponible en: http://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/ [Accedido: Junio. 23, 2014].

[11] "NORMA IRAM-ISO IEC 17799 Tecnología de la información", espol.edu.ec [Online]. Disponible en: www.icm.espol.edu.ec/materias/.../files/Políticas%20de%20Seguridad.ppt [Accedido: Junio. 23, 2014].

[12] LÓPEZ, A. RUIZ, J. "ISO 27000", iso27000.es [Online]. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf [Accedido: Junio. 23, 2014].

[13] NIST, “Special Publications (800 Series)”, nist.gov, 2013, [Online]. Disponible en: http://csrc.nist.gov/publications/PubsSPs.html [Accedido: Junio. 28, 2014].

[14] MONROY, D “Análisis inicial de la anatomía de un ataque a un sistema informático” Junio 2009. [Online]. Disponible en: http://www.seguinfo.com.ar/tests/ [Accedido: Junio. 23, 2014].

[15] VIEITES, Á. G. (2007). “Enciclopedia de la Seguridad Informática”. México: Alfaomega. [Accedido: Junio. 23, 2014].

[16] FIRTMAN, Sebastián “Seguridad Informática”, book.google.com.ec, Septiembre 2005 [Online]. Disponible en: books.google.com.ec/books?isbn=9871857292 [Accedido: Marzo. 10, 2014].

[17] MICROSOFT “Firewall”, Microsoft.com, 2014 [Online]. Disponible en: http://windows.microsoft.com/es-419/windows/what-is-firewall#1TC=windows-7 [Accedido: Marzo. 10, 2014].

[18] ROYER, Jean-Marc “Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones”, book.google.com.ec, 2004, [Online]. Disponible en: http://books.google.com.ec/books?id=K8XdRni4t94C&pg=PA9&dq=seguridad+inform%C3%A1tica&hl=es-419&sa=X&ei=hFqfU6_sGaezsQSk3YCwDw&ved=0CD8Q6AEwAw#v=onepage&q&f=false [Accedido: Junio. 28, 2014].

[19] LACAYO, Aaron “Análisis e Implementación de un esquema de seguridad en

Redes para las Instituciones de Educación Superior”, cujae.edu.ec, Septiembre 2005 [Online]. Disponible en: http://www.cujae.edu.ec/eventos/cittel/Trabajos/CIT052.pdf [Accedido: Julio. 7, 2014].

[20] “Nod32”, eset-la.com, [Online]. Disponible en: http://www.eset-la.com/empresas [Accedido: Noviembre. 1, 2014].

[21] “Nmap”, nmap.org, [Online]. Disponible en: http://nmap.org/man/es/ [Accedido: Noviembre. 1, 2014].

ANEXOS

ANEXO A

GERENTE GENERAL

ELEMENTOS DE COMPETENCIA

N°	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES, VALORES Y OTROS
1	Planificar, coordinar, supervisar y evaluar la gestión administrativa y financiera de la cooperativa, según normas técnicas, legales y administrativas vigentes.	▪ Planificación estratégica, ▪ Presupuestos, ▪ Administración de empresas ▪ Técnicas negociación	▪ Negociar y establecer acuerdos. ▪ Tomar decisiones. ▪ Ejercer liderazgo.	▪ Tolerancia ▪ Flexibilidad ▪ Atención distribuida
2	Diagnosticar las condiciones y evaluar el mercado financiero en función de los planes de crecimiento y de la gestión de la cooperativa.	▪ Característica del mercado financiero ▪ Análisis financiero	▪ Manejar hoja electrónica.	▪ Objetividad ▪ Imparcialidad
3	Analizar, sugerir e implementar las estrategias de mercadeo de productos y servicios.	▪ Mercadeo de productos y servicios financieros	▪ Interpretar resultados.	▪ Capacidad predictiva ▪ Objetividad ▪ Prudencia
4	Aprobar créditos solicitados según rangos de aprobación establecidos.	▪ Políticas de crédito ▪ Reglamento de crédito ▪ Normas relacionadas	▪ Determinar capacidad endeudamiento	▪ Imparcialidad ▪ Independencia ▪ Objetividad ▪ Prudencia
5	Participar del comité de crédito para la aprobación de solicitudes según rango establecido, como representante técnico	▪ Políticas de crédito ▪ Reglamento de crédito ▪ Normativa relacionada	▪ Determinar capacidad endeudamiento ▪ Orientar toma de decisiones	▪ Imparcialidad ▪ Independencia ▪ Objetividad ▪ Prudencia
6	Informar, ejecutar, coordinar, controlar y evaluar el cumplimiento de las disposiciones de los órganos de control, en los términos establecidos.	▪ Normativa relacionada	▪ Ejercer liderazgo ▪ Delegar ▪ Supervisar	▪ Respeto a las normas
7	Informar periódicamente sobre la gestión técnica y administrativa de la cooperativa a los organismos directivos, verbal y documentalmente.	▪ Resultados de gestión	▪ Elaborar presentaciones ▪ Comunicar oralmente ▪ Elaborar informes escritos	▪ Transparencia ▪ Aptitud verbal ▪ Respeto a las normas
8	Aprobar la adquisición de bienes y servicios requeridos, según monto establecido, para la gestión de la cooperativa	▪ Reglamento de adquisiciones ▪ Mercado de bienes y servicios ▪ Negociación	▪ Negociar y establecer acuerdos ▪ Tomar decisiones	▪ Transparencia ▪ Imparcialidad ▪ Objetividad
9	Analizar y aprobar las acciones de selección, contratación, capacitación, valoración y evaluación de desempeño para la gestión técnica del talento humano	▪ Gestión de recursos humanos ▪ Técnicas de negociación	▪ Negociación ▪ Tomar decisiones ▪ Ejercer liderazgo	▪ Justicia ▪ Equidad ▪ Imparcialidad ▪ Transparencia ▪ Objetividad
10	Coordinar la gestión financiera y administrativa de las agencias de la cooperativa.	▪ Resultados de la gestión ▪ Mercado de cada agencia ▪ Sistemas de control	▪ Ejercer liderazgo ▪ Tomar decisiones	▪ Objetividad ▪ Equidad ▪ Imparcialidad
11	Suscribir convenios de préstamo con entidades financieras según políticas de endeudamiento aprobadas.	▪ Mercado financiero ▪ Normas de prudencia financiera ▪ Técnicas de negociación	▪ Negociar y establecer acuerdos ▪ Toma de decisiones	▪ Objetividad ▪ Prudencia

CONTADOR GENERAL

Nº	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES, VALORES Y OTROS
1	Revisar y validar la información contable, por varios conceptos según normas y procedimientos establecidos.	▪ Contabilidad de Costos ▪ Contabilidad ▪ Normativa Vigente ▪ Sistema de Control	▪ Ejercer liderazgo ▪ Formar efectivos equipos de trabajo	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
2	Visitar, revisar y validar el cuadre diario de las cuentas correspondiente, consolidando información de matriz y agencias	▪ Contabilidad de Costos ▪ Contabilidad ▪ Normativa Vigente ▪ Sistema de Control	▪ Ejercer liderazgo ▪ Formar efectivos equipos de trabajo	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
3	Revisar y aprobar las conciliaciones bancarias de las cuentas de la cooperativa, según prácticas contables corrientes.	▪ Contabilidad de Costos ▪ Contabilidad ▪ Normativa Vigente ▪ Sistema de Control	▪ Ejercer liderazgo ▪ Formar efectivos equipos de trabajo	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
4	Elaborar los formularios para cumplir las obligaciones tributarias	▪ Normativa Tributaria vigente	▪ Elaborar informes y presentaciones	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
5	Elaborar y presentar informes sobre indicadores contables, según requerimientos superiores y normas y procedimientos establecidos.	▪ Indicadores Contables	▪ Elaborar informes y presentaciones ▪ Interpretar resultados.	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
6	Elaborar listados financieros consolidados, según las normas vigentes de contabilidad.	▪ Indicadores Contables	▪ Elaborar informes financieros	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
7	Elaborar mensualmente los roles de pago, planillas del IESS y liquidaciones de personal	▪ Código de Trabajo ▪ Reformas salariales ▪ Seguridad social ▪ Hojas de cálculo	▪ Elaborar planillas	▪ Honestidad ▪ Equidad
8	Realizar arqueos del inventario de los activos fijos, pagarés, hipotecas, garantías y depósitos a plazo fijo	▪ Elaboración de inventarios ▪ Contabilidad	▪ Elaborar informes ▪ Detectar fallos	▪ Honestidad
9	Dar inicio y fin del día a través del sistema; realizar el proceso de fin de mes en el sistema; arreglar el sistema en la matriz y agencias.	▪ Funcionamiento y programación del sistema	▪ Detectar fallos ▪ Corregir errores	▪ Aptitud abstracta ▪ Aptitud numérica ▪ Coordinación manual

ASISTENTE DE CONTABILIDAD

Nº	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES, VALORES Y OTROS
1	Revisar la validez y pertinencia de documentos de pago y elaborar comprobantes de egresos, ingresos y diarios de matriz y agencias.	▪ Normativa vigente ▪ Normativa interna ▪ Obligaciones de pago	▪ Elaborar comprobantes de egreso	▪ Oportunidad ▪ Precisión
2	Registrar en el libro bancos, los depósitos, pagos diarios realizados según procedimientos establecidos.	▪ Contabilidad ▪ Computación	▪ Operar sistema, del módulo de Contabilidad	▪ Precisión ▪ Agilidad manual
3	Realizar la conciliación bancaria de las cuentas de la cooperativa	▪ Sistema de cuentas ▪ Contabilidad	▪ Módulo del sistema ▪ Contabilidad	▪ Precisión
4	Imprimir mayores, auxiliares, balances de comprobación y balances generales y de resultados, y archivar para mantener un archivo físico para la Cooperativa	▪ Sistema de cuentas	▪ Operar el sistema informático, en el módulo de Contabilidad.	▪ Agilidad manual
5	Custodiar títulos valores, pólizas, chequeras, efectivo, hipotecas y pagarés según normas y procedimientos vigentes.	▪ Reglamento de crédito ▪ Normativa relacionada	▪ Manejar documentos valorados	▪ Honradez ▪ Transparencia
6	Realizar y mantener actualizado el inventario contable de activos fijos	▪ Contabilidad ▪ Sistema de inventarios	▪ Operar el sistema informático	▪ Agilidad mental ▪ Honestidad
7	Elaborar los comprobantes de retención en la fuente, del IVA y planilla de aportes al IESS, aplicando las normas tributarias y de seguro social obligatorio vigentes.	▪ Normativa tributaria ▪ Liquidación de nomina	▪ Elaborar formatos varios	▪ Exactitud ▪ Aptitud numérica
8	Elaborar y cuadrar formatos de pago de retenciones en la fuente, a contabilidad, para su consolidación.	▪ Normativa tributaria	▪ Elaborar formatos varios	▪ Aptitud numérica ▪ Oportunidad ▪ Transparencia
9	Cuadrar el cobro de planillas telefónicas de los socios a través de débito a las cuentas	▪ Normativa vigente	▪ Operar el módulo	▪ Facilidad de comunicación
10	Identificar las necesidades materiales y equipos de oficina, adquirirlos y controlar su custodia, mantenimiento y consumo.	▪ Contabilidad ▪ Tributación	▪ Planificar y organizar ▪ Habilidad numérica	▪ Oportunidad ▪ Honestidad ▪ Pro actividad
11	Elaborar cheques y realizar los pagos a proveedores	▪ Tributación ▪ Ley de cheques ▪ Contabilidad	▪ Habilidad numérica	▪ Honestidad ▪ Oportunidad

RECIBIDOR PAGADOR

Nº	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES, VALORES Y OTROS
1	Recibir y verificar la cantidad, autenticidad del "fondo de cambio"[1], de acuerdo a procedimientos establecidos y formatos aprobados	▪ Normativa relacionada ▪ Reconocimiento del dinero	▪ Verificar, autenticidad y cantidad de dinero	▪ Honestidad ▪ Precisión ▪ Aptitud numérica
2	Cancelar retiros de fondos a socios de otras agencias para atender los requerimientos de socios y clientes , según procedimientos aprobados	▪ Sistema de cuentas	▪ Detectar errores contables	▪ Oportunidad
3	Recibir y pagar dinero por varios conceptos, según requerimientos de socios y clientes, verificando montos, autenticidad de papeletas, identidad y más aspectos.	▪ Normativa relacionada ▪ Calidad en el servicio ▪ Relaciones humanas ▪ Técnicas de negociación ▪ Reconocimiento del dinero	▪ Verificar autenticidad y cantidad de dinero ▪ Gestionar el sistema, del módulo de caja.	▪ Paciencia ▪ Aptitud numérica ▪ Honestidad
4	Acreditar y debitar, dinero en las cuentas correspondientes de socios y clientes según procedimientos establecidos	▪ Gestión de caja	▪ Manejar módulo de caja	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
5	Realizar cuadre diario de caja, verificando el efectivo y cheques, y los reportes del sistema	▪ Gestión de caja	▪ Manejar módulo de caja	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
6	Custodiar la caja y la recaudación diaria en efectivo	▪ Clave de acceso	▪ Verificar, autenticidad y cantidad de dinero	▪ Honradez ▪ Precisión ▪ Aptitud numérica
7	Aperturar cuentas de ahorros[2]	▪ Normativa relacionada	▪ Manejar módulos del sistema.	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
8	Recaudar los depósitos de acuerdos con otras instituciones	▪ Normativa relacionada ▪ Reconocimiento de dinero	▪ Manejar módulo de caja (convenios)	▪ Precisión ▪ Honradez
9	Entregar papeletas y más documentos de soporte a las unidades correspondientes, mediante procedimiento establecido	▪ Gestión de caja	▪ Elaborar y presentar reportes	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
10	Realizar diariamente reportes de libretas de: ahorros, aportaciones y préstamos	▪ Utilización de utilitarios (Excel)	▪ Elaboración y presentación de reportes	▪ Precisión

[1] *Cantidad de dinero entregado en efectivo para operar la caja diariamente*

[2] *En aquellas oficinas que el flujo de atención es mínimo, el cajero puede realizar esta función paralelamente*

CRÉDITO Y COBRANZAS

Nº	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTUTUDES, VALORES Y OTROS
1	Atender a los socios / clientes que requieran créditos	▪ Reglamento de crédito	▪ Negociar ▪ Comunicar	▪ Oportunidad ▪ Transparencia
2	Evaluar solicitudes de crédito según políticas y reglamento de crédito vigentes, Aprobar o negar operaciones dentro de su rango de aprobación.	▪ Reglamento de crédito ▪ Historial crediticio de clientes ▪ Análisis de riesgo crediticio	▪ Detectar inconsistencias de información y documentos de respaldo	▪ Perspicacia ▪ Objetividad ▪ Imparcialidad
3	Participar del Comité de crédito para evaluar y recomendar la aprobación o negación de solicitudes de crédito	▪ Reglamento de crédito ▪ Historial crediticio de clientes ▪ Análisis de riesgo crediticio	▪ Detectar inconsistencias de información y documentos de respaldo	▪ Perspicacia ▪ Objetividad ▪ Imparcialidad
4	Coordinar con los Jefes de Agencias, el control de la morosidad de los deudores, según las Leyes vigentes	▪ Tablas de amortización ▪ Análisis de morosidad	▪ Negociar y lograr acuerdos ▪ Elaborar informes de morosidad	▪ Pro actividad ▪ Eficiencia ▪ Imparcialidad
5	Elaborar y presentar informes de crédito, para gerencia, consejos y las unidades de control externo.	▪ Indicadores de gestión de crédito ▪ Sistema módulos de cartera cobranzas	▪ Elaborar informes	▪ Objetividad ▪ Precisión
6	Supervisar las operaciones de crédito	▪ Indicadores de gestión de crédito ▪ Reglamento interno de crédito	▪ Detectar errores u omisiones. ▪ Capacidad de comunicación	▪ Objetividad ▪ Imparcialidad
7	Coordinar las acciones administrativas de cobro a socios con créditos en mora, con los abogados de la Cooperativa	▪ Tabla de morosidad ▪ Procesos judiciales de cobro	▪ Identificar cobros por vía administrativa y judicial	▪ Responsable ▪ Honestidad ▪ Ética profesional
8	Elaborar y presentar informes sobre créditos vinculados para presentar a las entidades de control	▪ Indicadores de crédito vinculados ▪ Normativa vigente	▪ Elaborar informes y presentaciones	▪ Oportunidad ▪ Precisión ▪ Objetividad ▪ Imparcialidad
9	Distribución y calificación de cartera	▪ Normativa vigente	▪ Elaborar informes	▪ Objetividad ▪ Imparcialidad

JEFE DE CAPTACIONES

N°	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES VALORES Y OTROS
1	Controlar y monitorear el cumplimiento de dinero en permanencia en las cajas, y dinero en bóveda conforme a las coberturas establecidas.	▪ Normativa relacionada ▪ Gestión de cajas	▪ Manejar el módulo de caja ▪ Ejercer liderazgo	▪ Aptitud numérica ▪ Transparencia ▪ Honestidad
2	Proveer y prever el "fondo de cambio" diario a cada cajero según montos de efectivo de socios y procedimientos establecidos.	▪ Normativa relacionada ▪ Identificación de dinero	▪ Verificar autenticidad y cantidad de dinero	▪ Aptitud numérica ▪ Transparencia ▪ Honestidad ▪ Coordinación manual
3	Controlar el "cuadre diario de caja" de cada cajero según condiciones y procedimientos establecidos.	▪ Normativa relacionada	▪ Verificar autenticidad y cantidad de dinero	▪ Aptitud numérica ▪ Transparencia ▪ Honestidad ▪ Coordinación manual
4	Recibir las recaudaciones diarias de efectivo y cheques de cada cajero, verificando montos y autenticidad del dinero con sus respectivos documentos de soporte.	▪ Normativa relacionada ▪ Dinero autentico	▪ Verificar autenticidad y cantidad de dinero	▪ Aptitud numérica ▪ Transparencia ▪ Honestidad ▪ Coordinación manual
5	Coordinar el depósito diario de las recaudaciones realizadas por las diferentes cajas, según procedimientos establecidos.	▪ Ídem	▪ Llenar formatos de depósito varios ▪ Ídem	▪
6	Atender los requerimientos de socios y clientes, de agencias y ventanillas compartidas según procedimientos establecidos.	▪ Sistema de cuentas	▪ Ídem	▪ Atención distribuida ▪ Oportunidad
7	Diseñar, proponer y ejecutar estrategias genéricas y específicas para incrementar las captaciones por ahorro, inversiones, remesas y otros, de parte de socios y clientes.	▪ Mercado financiero local y nacional ▪ Necesidades de los clientes	▪ Percepción de oportunidades de negocios ▪ Percibir las expectativas de los clientes	▪ Proactividad ▪ Iniciativa ▪ Creatividad
8	Atender las operaciones de remesas (giros y envíos)	▪ Normativa relacionada ▪ Gestión de cajas ▪ Necesidades de los clientes	▪ Verificar autenticidad de información ▪	▪ Proactividad ▪ Iniciativa ▪ Transparencia ▪ Honestidad
9	Cuidar las operaciones para el Ingreso de socios	Normativa relacionada	Verificar autenticidad de información Percepción de oportunidad de negocio	Proactividad Iniciativa Sentido de oportunidad Objetividad
10	Verificar y suscribir certificados de aportación, inversión y otros, según normas y procedimientos establecidos.	▪ Sistema de captaciones ▪ Ley de instituciones financieras	▪ Verificar corrección de procedimientos	▪ Sentido de oportunidad ▪ Objetividad
11	Coordinar la elaboración y presentación de reportes periódicos sobre depósitos a plazo, según estipulaciones de los organismos de control.	▪ Depósitos a plazo recibidos	▪ Elaborar formatos específicos	▪ Objetividad ▪ Oportunidad ▪ Transparencia
12	Llevar el control y presentar reportes consolidados periódicos a diferentes usuarios sobre altas y bajas de socios, según formato establecido.	▪ Altas y bajas de socios y clientes	▪ Elaborar formatos específicos	▪ Objetividad ▪ Oportunidad ▪ Transparencia

ADMINISTRADOR DE SISTEMAS

Nº	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES REQUERIDAS	ACTITUDES, VALORES Y OTROS
1	Supervisar el inicio del sistema automático de gestión de la cooperativa, según los procedimientos técnicos.	▪ Operación del sistema automático de gestión de la Cooperativa	▪ Supervisar acciones técnicas del arranque del sistema	▪ Oportunidad ▪ Precisión
2	Supervisar la operatividad de los diferentes equipos, programas y sistema, necesarios para gestionar los servicios.	▪ Operación del sistema automático de gestión de la cooperativa ▪ Demandas operativas de diferentes áreas de gestión	▪ Supervisar acciones técnicas de operación del sistema	▪ Oportunidad ▪ Pro actividad ▪ Aptitud abstracta y numérica
3	Corregir los comandos erróneos realizados por los usuarios del sistema, según procedimientos técnicos establecidos.	▪ Normas y claves de reversión	▪ Detectar causas de fallos ▪ Corregir errores	▪ Oportunidad ▪ Precisión ▪ Aptitud numérica
4	Realizar mantenimiento preventivo y correctivo de programas necesarios para mantener operativo el sistema	▪ Funcionamiento y programación de programas utilitarios	▪ Detectar fallos ▪ Corregir errores	▪ Aptitud abstracta ▪ Aptitud numérica ▪ Coordinación manual
5	Crear, registrar, controlar y permitir o denegar accesos de usuarios a los diferentes módulos del sistema.	▪ Sistema automático de gestión ▪ Área de gestión de cada funcionario	▪ Identificar ingresos al sistema según sistema de códigos.	▪ Oportunidad ▪ Precisión ▪ Coordinación manual
6	Elaborar respaldos diarios de la base de datos del servidor principal y de la gestión de cada uno de los módulos, según normas y procedimientos técnicos y administrativos establecidos.	▪ Operación del sistema automático de gestión de la Cooperativa	▪ Operar comandos de impresión y respaldos	▪ Oportunidad ▪ Precisión ▪ Coordinación manual
7	Apoyar y asesorar a la gerencia en toma de decisiones para mejorar la tecnología de la cooperativa.	▪ Nueva tecnología en el mercado ▪ Necesidades de la Cooperativa	▪ Negociar con proveedores ▪ Comunicar	▪ Oportunidad ▪ Precisión
8	Ser parte del Comité Informático (Secretario)	▪ Riesgo operativo ▪ Planes de contingencia	▪ Detectar riesgos y dar soluciones	▪ Oportunidad ▪ Objetividad ▪ Facilidad de comunicación
9	Supervisar el proceso de cierre del día, según procedimientos técnicos establecidos	▪ Operación del sistema automático de gestión de la Cooperativa	▪ Operar computador	▪ Oportunidad ▪ Precisión ▪ Coordinación manual

ANEXO B

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Presidencia
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		PRESIDENCIA
	Nombre Usuario		
CPU	Velocidad (GHZ)		
	Marca		
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		
	Dirección IP		192.168.0.14
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	
		Nombre	
		N° Licencia	
	Otros (1)	Fabricante	Microsoft
		Nombre	Office 2013
		N° Licencia	
	Otros (2)	Fabricante	Eset
		Nombre	Eset Nod 32
		N° Licencia	
	Otros (3)	Fabricante	
		Nombre	Financial
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		
	2		
	3		
	4		
	5		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Gerencia
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		GERENCIA
	Nombre Usuario		Angélica Gordón
CPU	Velocidad (GHZ)		3,2
	Marca		Intel Core i5
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		4GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.14
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		--------
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	Microsoft
		Nombre	Widows 7 profesional x 64bits
		N° Licencia	
	Otros (1)	Fabricante	Microsoft
		Nombre	Office 2013
		N° Licencia	Si
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	Fibra optica
		Contingente	
Aplicaciones o servicios	1		VNC
	2		Ablee3extraction
	3		
	4		
	5		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Sistemas
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		Disco Duro Portatil Samsung
	Nombre PC		SISTEMAS
	Nombre Usuario		Ángel Chicaiza
CPU	Velocidad (GHZ)		3,3
	Marca		Intel Core i3
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		DDR3 4G
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		930
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.35
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		LG
	N° Serie		
	Teclado (Marca)		HP
	Mouse (Marca)		HP
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7 Ultimate 32bits
		N° Licencia	----------
	Otros (1)	Fabricante	OpenOffice
		Nombre	Apache OpenOffice
		N° Licencia	----------
	Otros (2)	Fabricante	Microsoft
		Nombre	Office 2013
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		Iomega Encription
	3		Anviz Sistema de Administración
	4		IVMS-4000
	5		
Código del Activo	CPU		
	MONITOR		
	TECLADO		
	MOUSE		
	MAC ADDRESS		4C-72-B9-66-7F-AA
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Contabilidad
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		----------
	Drive 3 1/2		----------
	CD ROM		----------
	CD ReWritable		----------
	CD DVD/ReWritable		----------
	Accesorios		----------
	Nombre PC		CONTABILIDAD
	Nombre Usuario		Juliana Guerrero
CPU	Velocidad (GHZ)		3
	Marca		Core i5
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		4GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.67
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		Epson Nx530
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7 Profesional x64
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft
		Nombre	Office 2013
		N° Licencia	Si
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32, Avast
		Nombre	Eset Nod 32, Avast
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		SRI DIMM
	3		
	4		
	5		
Código del Activo	MAC ADDRESS		EC-A8-6B-F8-E6-0F
	MONITOR		
	TECLADO		----------
	MOUSE		----------
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Auxiliar de Contabilidad
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		AUXCONTABILIDAD
	Nombre Usuario		Andrea Carrera
CPU	Velocidad (GHZ)		3
	Marca		Intel Pentium 4
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		1GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.18
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		----------
	N° Serie		----------
	Teclado (Marca)		----------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows XP Profesional
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft, Apache
		Nombre	Office 2010, OpenOffice
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32, Avast
		Nombre	Eset Nod 32, Avast
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios		1	VNC
		2	SRI DIMM
		3	
		4	
Código del Activo		CPU	----------
		MAC ADRESS	00-11-95-B7-74-0D
		TECLADO	----------
		MOUSE	----------
		IMPRESORA	----------

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de CRÉDITO1
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		----------
	Drive 3 1/2		
	CD ROM		----------
	CD ReWritable		
	CD DVD/ReWritable		----------
	Accesorios		----------
	Nombre PC		NEGOCIOS-PC
	Nombre Usuario		Ramiro Santos
CPU	Velocidad (GHZ)		3
	Marca		Intel Pentium 4
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		512 MB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.22
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7 64 BITS
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft, Apache
		Nombre	Office 2010, OpenOffice
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	CPU		
	MONITOR		
	TECLADO		
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Negocios 2
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		----------
	N° Serie (Mainboard)		----------
	Drive 3 1/2		----------
	CD ROM		----------
	CD ReWritable		
	CD DVD/ReWritable		----------
	Accesorios		----------
	Nombre PC		NEGOCIOS2
	Nombre Usuario		
CPU	Velocidad (GHZ)		1,8
	Marca		Intel Pentium 4
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		1GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.37
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		----------
	N° Serie		----------
	Teclado (Marca)		----------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7
		N° Licencia	
	Otros (1)	Fabricante	Apache OpenOffice
		Nombre	OpenOffice
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	MAC ADRESS		00-19-D1-F8-A6-73
	MONITOR		----------
	MAC ADRESS WIFI		----------
	MOUSE		----------
	IMPRESORA		----------

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de CRÉDITO1
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		CREDITO
	Nombre Usuario		Gustavo Urvina
CPU	Velocidad (MHZ)		3,2
	Marca		Core i5
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		4GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		
	Velocidad (mbps)		
	Dirección IP		192.168.0.15
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7 Ultimate x32
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft
		Nombre	Office 2010
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	
		Nombre	
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	MAC ADDRESS		70-71-BC-42-80-F6
	MONITOR		
	TECLADO		
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Información (Secretaría)
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		----------
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		----------
	CD DVD/ReWritable		----------
	Accesorios		----------
	Nombre PC		SECRETARIA
	Nombre Usuario		Mónica Becerra
CPU	Velocidad (GHZ)		3,2
	Marca		Intel Pentium D
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		960 MB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.33
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		CANON MP250
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows XP Profesional
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft
		Nombre	Office 2010
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	MAC ADDRESS		00-19-21-05-E4-C6
	MONITOR		
	TECLADO		
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Caja
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		Caja
	Nombre Usuario		Cecilia Prado
CPU	Velocidad (GHZ)		3,2
	Marca		Intel Pentium D
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		448MB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.41
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		
	N° Serie		
	Teclado (Marca)		
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows XP Profesional
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft
		Nombre	Office 2007
		N° Licencia	
	Otros (2)	Fabricante	Apache OpenOffice
		Nombre	OpenOffice
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		SRI DIMM
	3		MINKARED
	4		PUNTOMATICO
	5		
Código del Activo	CPU		
	MONITOR		
	MAC ADRESS		
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
Departamento de Inversiones
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		INVERSIONES-PC
	Nombre Usuario		Margarita Ortiz
CPU	Velocidad (GHZ)		3,2
	Marca		Intel Core 2 duo
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		2GB
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		Ethernet Incorporada
	Velocidad (mbps)		100/10
	Dirección IP		192.168.0.8
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		--------
	N° Serie		--------
	Teclado (Marca)		--------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	MicroSoft
		Nombre	Windows 7
		N° Licencia	
	Otros (1)	Fabricante	MicroSoft
		Nombre	Office 2010
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	Eset Nod 32
		Nombre	Eset Nod 32
		N° Licencia	
Ubicación	Oficina		Matriz
	Ciudad		Ambato
Acceso	Local		Red LAN
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	CPU		
	MONITOR		
	MAC ADRESS		00-1C-C0-7B-4C-61
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
SERVIDOR 1
Detalle de Hardware y Software

Características y componentes			
General	Marca		HP
	Modelo		ProLiant ML350 G5 E5420 2.50GHz Quad Core
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		SERVIDOR
	Nombre Usuario		
CPU	Velocidad (GHZ)		2.50GHz Quad Core
	Marca		
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		1GbE NC373i Multifunction 2 Ports
	Velocidad (mbps)		
	Dirección IP		192.168.0.1
	Compuerta de Enlace		192.168.0.200
Perifericos	Monitor (Marca)		--------
	N° Serie		--------
	Teclado (Marca)		--------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	Microsoft
		Nombre	Windows Server 2003
		N° Licencia	Si
	Otros (1)	Fabricante	
		Nombre	Sql Server 2008
		N° Licencia	Si
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	
		Nombre	
		N° Licencia	
Ubicación	Oficina		
	Ciudad		
Acceso	Local		
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	CPU		
	MONITOR		
	MAC ADRESS		00-23-7D-A9-9B-04
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
SERVIDOR 2
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		Servidor HP ProLiant ML350p Gen8
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		CENTOS
	Nombre Usuario		SRVWIN2003/SERVSOLVERFIN
CPU	Velocidad (GHZ)		
	Marca		
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		
	Velocidad (mbps)		
	Dirección IP		192.168.0.9/192.168.0.10
	Compuerta de Enlace		
Perifericos	Monitor (Marca)		--------
	N° Serie		--------
	Teclado (Marca)		--------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	Microsoft
		Nombre	Windows Server 2008
		N° Licencia	Si
	Otros (1)	Fabricante	Microsoft
		Nombre	Windows Server 2012
		N° Licencia	Si
	Otros (2)	Fabricante	
		Nombre	Sql Server 2008
		N° Licencia	Si
	Otros (3)	Fabricante	
		Nombre	Sql Server 2012
		N° Licencia	Si
Ubicación	Oficina		
	Ciudad		
Acceso	Local		
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		KVR (Herramienta para virtualizar servidores)
	3		
	4		
	5		
Código del Activo	CPU		
	MONITOR		
	MAC ADRESS		52-54-00-B5-01-37
	MOUSE		
	IMPRESORA		

Cooperativa de Ahorro y Crédito Unión Popular Ltda. Matriz
SERVIDOR 3
Detalle de Hardware y Software

Características y componentes			
General	Marca		
	Modelo		
	Mainboard		
	N° Serie (Mainboard)		
	Drive 3 1/2		
	CD ROM		
	CD ReWritable		
	CD DVD/ReWritable		
	Accesorios		
	Nombre PC		SERVSOLVERFIN
	Nombre Usuario		
CPU	Velocidad (GHZ)		
	Marca		
Memoria RAM	Tipo y Cap.Instalada (MB) (socket 1)		
	Marca		
	N° Serie		
	Tipo y Cap.Instalada (MB) (socket 2)		
	Marca		
	N° Serie		
Almacenamiento interno	Cap.Instalada (GB)		
	Marca		
Comunicaciones	Tipo Tarjeta		
	Velocidad (mbps)		
	Dirección IP		192.168.0.10
	Compuerta de Enlace		
Perifericos	Monitor (Marca)		--------
	N° Serie		--------
	Teclado (Marca)		--------
	Mouse (Marca)		
	Impresora (Marca)		
	N° Serie		
Software de propósito general	Sistema Operativo	Fabricante	
		Nombre	
		N° Licencia	
	Otros (1)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (2)	Fabricante	
		Nombre	
		N° Licencia	
	Otros (3)	Fabricante	
		Nombre	
		N° Licencia	
Ubicación	Oficina		
	Ciudad		
Acceso	Local		
	Remoto	Modalidad	
		Contingente	
Aplicaciones o servicios	1		VNC
	2		
	3		
	4		
	5		
Código del Activo	CPU		
	MONITOR		
	MAC ADRESS		52-54-00-B5-01-37
	MOUSE		
	IMPRESORA		

ANEXO C

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL (FISEI)

Entrevista dirigida para la persona encargada del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito Unión Popular Ltda.

OBJETIVO: Recolectar información sobre la situación actual en que se va desarrollando las operaciones diarias dentro de la red de datos de la cooperativa.

Almacenamiento de los tipos y medios de almacenamiento

Evaluación de los tipos y medios de almacenamiento de la información				
Fecha:				
Responsable:				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Posee algún medio de almacenamiento de la información que maneje la empresa en la red?	ISO 17799 sec 2.			
¿Qué dispositivos utiliza para almacenar la información? • Cintas Magnéticas • Tarjetas FLASH • Unidad ZIP • Discos Duros • Discos Flexibles • Medios Ópticos • JUMP Drive • Back Ups • RAID's				
¿Posee lugares estratégicos para almacenar los dispositivos utilizados para guardar la información?				
¿Se tiene clasificados los archivos con información confidencial?				
¿Posee alguna metodología para la clasificación de la información (explique)				
¿Poseen estos archivos claves de acceso?				

¿Utilizan algún método de encriptación? (explique)	ISO 15408 clase 4			
¿Qué lugares utiliza para almacenar estos medios? • Cajas Fuertes • Bóvedas Bancarias • Archivos • Otros (especificar)	ISO 17799 sec 2.			
Este almacenamiento está situado: • En la misma empresa • En el departamento de informática • Fuera de la empresa (especifique)	ISO 17799 sec 2.			
¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?				
¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento?	ISO 15408 clase 7			
¿Se tiene control del personal autorizado para firmar la salida de archivos confidenciales?	ISO 15408 clase 7			
¿Se posee un registro para los archivos que se prestan y la fecha en que se devolverán?				
En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperación de archivos?				
¿Estos conocimientos los acceden los operadores?				
¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?	ISO 17799			
¿Se lleva a cabo dicho programa?				

Documentación de la Red				
Fecha:				
Responsable:				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Poseen en el departamento de informática un manual formal sobre la diagramación de la red de la empresa?	ISO 17799 área 5			
¿Existe algún plano donde se especifica la instalación de la red?	ISO 17799 área 5			
¿Está segmentada la red?				
¿Cuántos segmentos posee la red?				
Cuántas estaciones de trabajo hay: - En cada segmento de la red - En la red.				
¿Cuántos servidores están en la distribución de la red?				
¿Se maneja algún tipo de control para manejar el número de equipos, su localización y las características de los equipos instalados en la red? (especifique)				
¿Qué tipo de topología se maneja en la red? - Topología de anillo - Topología de estrella - Topología de bus - Otras (especifique)				
¿Por qué cree conveniente el uso de este tipo de topología?				
De acuerdo al tipo de topología que se utiliza: ¿Cuál es el tipo de cableado empleado en la red?				
Si el tipo de cable que se está utilizando es el estructurado, ¿Qué estándares utilizan? - Estándar ANSI/TIA/EIA-568-A/B - Estándar ANSI/TIA/EIA-569 - Estándar ANSI/TIA/EIA-606 - Otros (especifique)	ISO 17799 área 5			
¿Considera usted adecuado el tipo de cableado utilizado en la red? (explique)				
¿El cableado se encuentra protegido de la intemperie? (explique)				
¿Cuál es la longitud del cableado en la red?				
¿De cuántos metros está estimada el área de cobertura de la red?				
¿Es adecuada la longitud utilizada en				

el cableado?				
¿En algún punto de la red existen dispositivos inalámbricos?				
¿Qué tipo de conectores utilizan en la red?				
¿Tiene conocimiento sobre los estándares de seguridad en la red?				
¿Tiene conocimiento sobre los estándares de seguridad en la red?				
¿Qué tipo de estándares manejan en la red?				
¿Considera usted que el estándar utilizado en la red es el adecuado?				
¿Qué tipos de arquitectura de red utilizan? - Ethernet - Token Ring - Apple Talk ARCnet - Otros (especifique)	ISO 17799 área 5			
¿Considera el tipo de arquitectura el adecuado para la red?				
¿Qué tipo de protocolo utiliza en la red? - TCP/IP - NetWare - NetBIOS - Otros (especifique)	ISO 17799 área 5			
¿Utilizan tarjetas de interfaz de red?				
¿Qué tipo de tarjeta de red poseen para la interconectividad?				
¿Posee las estaciones de trabajo sus respectivos UPS?				
¿Cuántas impresoras se utilizan dentro de la red?				
¿Las impresoras están compartidas en la red?				
¿Poseen conexión a Internet?				
¿Qué tipo de conexión?				
¿Este servicio es para una estación específica o todos tienen acceso?				
¿Posee la red algún tipo de protección de Internet como Firewall físico u otros? (especifique)				
¿Se realizan mantenimientos en los equipos de la red? (Solicitar plan de mantenimiento)				
¿Qué tipo de mantenimiento se realiza? - Preventivo - Correctivo	ISO 9001 4.14.2 4.14.3			

- Ambos - Proyectivo - Ninguno				
¿Se lleva a cabo el programa de mantenimiento?				
¿Cuáles son los problemas más comunes que se han detectado en la red actualmente? (explique)				
Cuándo un cable se daña cuál de los dos procedimientos se utilizan: - Reparación - Cambio				
¿Cuándo una estación de trabajo falla que se hace? • Un formateo con preinstalación de software. • Una clonación de un equipo que si funciona.				
¿Se lleva una bitácora o control de las fallas o problemas detectados en el equipo de la red? (Solicite bitácora)				
¿Se tienen proyectos de expansión de la red y están documentados?				
¿Se tienen proyectos de expansión del centro de cómputo y están documentados?				

Medidas de Seguridad Física				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Poseen seguros el activo informático de la empresa?				
¿Con que compañía? (Solicitar pólizas, tipos de seguro y montos)				
El activo informático de la empresa se encuentra situado a salvo de: - Inundaciones - Terremotos - Fuego - Sabotajes - Otros (especifique)	ISO 17799 área 1			
Existen alarmas para: - Detectar humo o fuego - Fugas de aguas - Fallos en el sistema eléctricos - Otros	ISO 17799 área 1			
¿Las alarmas son perfectamente audibles o visibles?				
¿Existen extintores de fuego?				
¿Los extintores de fuego funcionan a base de? - Agua - Gas - Otros (especifique)				
¿Se le dan mantenimiento a los extintores? (especifique cada cuanto tiempo)				
Se han tomado medidas para minimizar la posibilidad de fuego. • Evitando artículos inflamables. • Prohibiendo fumar en el interior del centro de cómputo. • Vigilando y manteniendo el sistema eléctrico. • No se ha previsto.	ISO 17799 área 1			
¿Pasan cañerías de agua a través o encima del centro de cómputo?				
¿La humedad del centro de cómputo u oficinas es la adecuada?				
¿Existe humedad en donde están ubicados los dispositivos que componen la red?				
¿Poseen un sistema de aire acondiciona capaz de mantener la temperatura adecuada?				
¿El interruptor de encendido/apagado de la luz esta inmediatamente dentro del centro de cómputo o en un punto accesible aun cuando no hubiere suministro eléctrico?	ISO 17799 área 1			

¿La iluminación en el centro de cómputo es de tipo fluorescente?				
¿Es apropiada la iluminación dentro de las instalaciones, y a cuantas candelas o luces asciende?				
¿Existe el número de tomas corrientes polarizados suficientes para los dispositivos utilizados en el centro de cómputo?				
¿Existe un panel de control eléctrico dedicado al centro de cómputo?				
¿Existen redes de tierra?				
¿La ubicación de los conductos de alimentación eléctrica de alto voltaje está debidamente identificada?				
¿Se hace limpieza periódicamente dentro del departamento de informática?				
¿Existen señalizaciones adecuadas dentro del departamento de informática?				
¿Está restringido el acceso al área de informática?	ISO 17799 área 7			
¿Existen medidas de seguridad en cuanto al acceso de personal no autorizado en la red?	ISO 17799 área 7			
¿Se posee control de accesos a los equipos de la red?				
¿Existen claves y contraseñas para permitir el acceso a los equipos?				
¿Se utiliza algún tipo de monitorización del estado de la red?				
¿Se controla al personal que posee acceso físico a los servidores y estaciones de trabajo?				
¿Existen procesos para identificación de desastres en los equipos que conforman la red?				
¿Se realiza periódicamente una verificación física de uso de terminales y de servidores?				
¿Se monitorea frecuentemente el uso que se les está dando a las terminales?				
¿Se permite a algún usuario el uso de cables para conectar otros dispositivos como laptops?	ISO 17799 área 7			
¿Se restringe el acceso de alimentos o líquidos dentro del área informática?				

Evaluación de la Seguridad Lógica				
Restricciones de acceso a archivos y programas.				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Se tienen definidos directorios de equipos y usuarios?	ISO 17799 área 6			
¿Se restringe el acceso a los programas y archivos de la empresa?				
¿Cuántas personas están autorizadas a realizar cambios en la configuración y/o equipos de la red?				
¿Poseen mecanismos de control de acceso al sistema?				
¿Poseen normativas de restricción a archivos con permisos especiales?				
¿Se permite la instalación de software no autorizado?				
¿Se restringen a los operadores modificar los archivos o programas que no correspondan?				
¿Tienen claro los operadores su área de trabajo dentro de la red?				

Análisis de Amenazas y Vulnerabilidades				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Si el administración o encargado de la red falta, hay otra persona que pueda realizar sus funciones? (explique)				
¿Se tiene procedimientos de seguridad, recuperación y respaldos para asegurar la disponibilidad continua de los sistemas de la red?				
¿Existen control o políticas sobre el uso de Internet en la red?	ISO 17799 área 1			
¿Es permitida la instalación de software obtenido de Internet por cualquier usuario?				
¿El sistema operativo de los servidores de la red es la misma que se utiliza en las terminales?				
¿Se controla el uso de programas de mensajería y correo electrónico a los usuarios?	ISO 17799 área 7			
¿Se permite el uso de programas P2P, como Kazaa u otros para que los usuarios de la red, bajen música, películas u otros contenidos?				
Tiene la red algún tipo de protección para Internet tales como: • Firewalls • Software Antivirus • Sistemas de detección de intrusos • Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos. • Creación de un disco de rescate o de emergencia • Procedimientos para cuando ocurra una infección con virus. • Hardware de seguridad de red dedicado • Back up de datos • RAID's • Otros (especifique)	ISO 15408 área 10			

¿Qué marca de firewalls poseen?				
¿En qué máquina (servidor) se encuentra el Firewall? - En una máquina dedicada - En el servidor web - Otros (especifique)				
¿Está habilitada alguna herramienta antivirus?	ISO 15408 área 10			
¿Están seguros que detecta los virus, los elimina correctamente y como lo documenta?				
¿El antivirus que compra posee actualizaciones periódicas?				
¿El antivirus utilizado es individual o corporativo?				
¿El firewall interactúa con el análisis de los virus, o solo se encarga de los servicios de la red?				
¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí? (especifique)				
¿Se actualiza en forma periódica este software?				
¿Existen control para evitar el uso de disquetes, CD u otros dispositivos de almacenamiento?				
¿Se han detectado mensajes, documentos y archivos infectados y como están documentado estos hallazgos?	ISO 17799 TL9000			
¿Con que frecuencia se hace un escaneo total de virus en los servidores?				
¿Se registra cada violación a los procedimientos a fin de llevas estadísticas y frenar tendencias mayores?	ISO 15408 área 6			

Identificación, Autenticación de usuarios y Contraseñas				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Existe un formato donde se define a cada usuario sus derechos y privilegios dentro de la red?	ISO 17799 área 7			
¿Existen grupos de usuarios, y están documentados?				
¿Cómo se forman los grupos? - Según el departamento de la empresa donde trabajen - Según el rol que desempeñen - Otros (especifique)	ISO 17799 área 7			
¿El acceso puede controlarse con el tipo de trabajo o la función (rol) de quien lo solicite?				
¿No se permite el acceso por default en el sistema operativo? (Cuentas Guest, por ejemplo)				
¿Hay tipos de perfil de administrador?				
¿Cuántas personas hay asignadas a la tarea de administrador?				
¿Puede acceder un administrador desde cualquier terminal?				
Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?				
¿Qué datos se muestran cuando alguien intenta acceder a la red? - Nombre de usuario - Password - Grupo o entorno de red - Estación de trabajo - IP - Fecha y hora				
¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?				
¿Un usuario puede tener solo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias? ¿Depende de la cantidad de grupos a los que pertenezca?	ISO 17799 área 7			
¿Qué datos hay en el perfil del usuario cuando se hace un alta?				

¿Se guardan los siguientes datos? - ID de usuario - Nombre y apellido completo - Puesto de trabajo y departamento de la empresa - Jefe inmediato - Descripción de tareas - Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de "buen uso" del sistema - Explicaciones breves y claras de cómo elegir su password - Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.) - Fecha de expiración de la cuenta - Datos de los permisos de acceso y excepciones - Restricciones horarias para el uso de recursos	ISO 17799 área 7			
¿El ID de usuario puede repetirse?				
¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo? (explique)				
¿Se guardan los archivos y datos de las cuentas eliminadas? ¿Por cuánto tiempo?				
¿Se documentan las modificaciones que se hacen en las cuentas?				
¿Los usuarios son actualizados por el nivel jerárquico adecuado?				
¿Se actualizan los privilegios de acceso de acuerdo a los cambios que se dan en la empresa?				
¿Se tiene un control preciso efectivo y documentado de los servicios autorizados y funciones de los usuarios?				
¿Se verifican que no se queden sesiones activas de usuarios, abiertas por descuido?				
¿Existen políticas para asegurar, prevenir o detectar la suplantación de identidades en el sistema?				
¿El personal de seguridad del sistema informa sobre accesos indebidos, a través de un formulario y oralmente?				
¿Se generan reportes de inconsistencias por accesos indebidos al sistema y donde quedan registrados?				

¿Se han establecido cambios periódicos de passwords y cómo se maneja la confidencialidad?				
¿Los ID y contraseñas se vencen por no usarlos recurrentemente en el sistema?				
¿Si se tiene acceso a internet se tiene control sobre el tráfico que se genera para evitar la fuga de información confidencial y como se respalda dicho registro?	ISO 17799 área 7			
¿Existen horarios de conexión establecidos en las redes ajustadas a los horarios de trabajo?				
¿Los password de los empleados son generados por alguien diferente al administrador de la red?				
¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios?				
¿Dos cuentas pueden tener las mismas passwords?				
¿Existe una normativa que establezca el procedimiento para el cambio de los passwords de los usuarios?				
¿Se puede cambiar en cualquier momento?				
¿Quién puede hacer los cambios? - El administrador - Los usuarios a través de una opción en el menú - Otros (especifique)	ISO 17799 área 7			
¿Se entrena a los usuarios en la administración del password? Se les enseña a: - no usar passwords fáciles de descifrar - no divulgarlas - no guardarlas en lugares donde se puedan encontrar. - entender que la administración de passwords es el principal método de seguridad del sistema.	ISO 17799 área 2			

Proceso de logon/logoff				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Se bloquea el usuario después de varios intentos fallidos de autenticación o se inhabilita la cuenta o la terminal?				
¿Después de cuantos intentos?				
Antes de terminar con la sesión, ¿se avisa al usuario que se lo desconectará? Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?	ISO 17799 área 7			
¿Después de qué período de inactividad (de cuantos días) se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado?				
¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?				
¿Existe la normativa del modelo o mecanismo estándar de control de acceso?				
¿Se usa una aplicación para el control de acceso?	ISO 15408 área 7			
Esta aplicación es: - Propia del sistema operativo - De aplicación y programas propios o comprados - Con paquetes de seguridad agregados al sistema operativo	ISO 17799 área 7			

Acceso remoto				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Existe una normativa para permitir el acceso remoto?	ISO 17799 área 7			
¿Existe acceso externo a los datos, desde Internet o desde el módem?				
¿Quién tiene ese acceso?				
¿Qué procedimientos se tienen en cuenta para mantener la integridad y la confiabilidad de los datos?				
Back Up y RAID's				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Se generan disco de rescate con el antivirus?	ISO 15408 área 10			
¿Para todas las máquinas o solo para los servidores?				
¿Se hacen y son efectivos los backups y los mecanismos de seguridad?				
¿Se realizan Back ups y/o RAID's de los datos?				
¿Con que medios?				
¿Con qué frecuencia hacen los backups?				
¿Hay imágenes Ghost de las máquinas?				
¿Se hacen backups de la configuración de red?				
¿Con qué aplicación se hacen?				
¿Utilizan archivos de tipo específicos o archivos .zip, por ejemplo?				
¿Hay herramientas de back up automáticas, que a través de una agenda hacen las copias?				

¿Existe la función operativo responsable de generar los respaldos?				
¿Contratan a terceros para que proporcione los insumos necesarios en caso de emergencia?				
¿Tienen formalizados los procedimientos de back up?				
¿Existen procedimientos escritos para recuperar archivos backupeados, o un Plan de backup?				
¿Hacen pruebas periódicas de recuperación de backups?				
¿Los backups se almacenan dentro y fuera del edificio?				
¿Estos lugares son seguros?				
¿Hay información afuera de la red interna de la empresa que sea valiosa?				
¿Se hacen backups de estos datos?				
¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior?	ISO 15408 área 11			

Evaluación de la Confidencialidad				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Existe una normativa que evalué la información disponible para terceros?	ISO 17799			
¿Existe la normativa para la creación de certificados digitales (criptografía) para los activos informáticos?	ISO 15408 área 4			
¿Existe un procedimiento de evaluación del desempeño del personal a cargo de la actividad de encriptación?	ISO 15408 área 4			
¿Qué tipo de criptografía utilizan para la confidencialidad? - Criptografía de clave pública (Asimétrica). - Criptografía de clave privada (Simétrica)	ISO 15408 área 4			
¿Existe un método seguro de almacenamiento y procesamiento para la trasmisión de datos confidenciales? ¿Está documentado?				
¿Poseen un sistema de administración de cookies? ¿Está documentado?				
¿Se ha capacitado a los Administradores para el empleo adecuado del sistema de cookies?				
¿Quién realiza la revisión de las historias en los terminales de los usuarios?				

Análisis actual de la seguridad informática				
Verificación	**Ref.**	**SI**	**NO**	**Observaciones**
¿Se cuenta con Políticas y estándares de los procesos relacionados con el sistema?				
¿Se tienen políticas de seguridad en la empresa?				
¿Con que tipo de manuales cuenta la empresa? • Manuales del sistema operativo. • Manuales de procedimientos. • Manuales de usuario. • Manuales de funciones.	ISO 17799 área 9			
¿Se cuenta con procedimientos para efectuar cambios, modificaciones y revisiones a los manuales?	ISO 17799 área 9			
¿Se cuenta con documentación de la instalación y configuración inicial de la red?				
¿Poseen un plan de contingencia contra desastres que proteja los activos informáticos? ¿Está documentado?	ISO 17799 área 9			
¿Posee un plan contra desastres? ¿Está documentado?				

ANEXO D

La siguiente lista se obtuvo mediante la realización de escaneos a la red de la cooperativa, donde se pudo evidenciar los servicios que se utilizan.

Puerto	Protocolo	Estado	Servicio	Versión
21	TCP	Abierto	ftp	Vsftpd 2.0.8
22	TCP	Abierto	ssh	OpenSSH5.3(protocol 2.0)
23	TCP	Abierto	telnet	
80	TCP	Abierto	http	Microsoft IIS httpd 6.0
135	TCP	Abierto	msrpc	Microsoft Windows RPC
139	TCP	Abierto	netbios-ssn	
443	TCP	Abierto	https	
445	TCP	Abierto	Microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
515	TCP	Abierto	printer	
554	TCP	Abierto	rtsp	
631	TCP	Abierto	tcpwrapped	
1025	TCP	Abierto	msrpc	Microsoft Windows RPC
1433	TCP	Abierto	ms-sql-s	Microsoft SQL Server 2008 10.00.1600 00; RTM
2383	TCP	Abierto	ms-sql-olap4	
2869	TCP	Abierto	http	Microsoft HTTPAPI httpd 2.0
3389	TCP	Abierto	ms-wbt-server	Microsoft Terminal Service
4567	TCP	Abierto	tram	
4915	TCP	Abierto	msrpc	Microsoft Windows RPC
5000	TCP	Abierto	msrpc	Microsoft Windows RPC
5001	TCP	Abierto	msrpc	Microsoft Windows RPC
5002	TCP	Abierto	msrpc	Microsoft Windows RPC
5003	TCP	Abierto	msrpc	Microsoft Windows RPC
5004	TCP	Abierto	msrpc	Microsoft Windows RPC
5800	TCP	Abierto	vnc-http	VNC Server Entrepise Edition
5900	TCP	Abierto	vnc	RealVNC Personal (protocolo 4.0)
8000	TCP	Abierto	tcpwrapped	
9100	TCP	Abierto	jetdirect	
123	UDP	Abierto	ntp	
137	UDP	Abierto	netbios-ns	
138	UDP	Abierto	netbios-dgm	
445	UDP	Abierto	microsoft-ds	
500	UDP	Abierto	isakmp	
1026	UDP	Abierto	Win-rpc	
4500	UDP	Abierto	nat-t-ike	

Para obtener esta información se utilizó el software de escaneo de puertos NMAP.

ANEXO E

Descripción de Antivirus utilizado en la cooperativa
ESET Endpoint Antivirus

ESET Endpoint Antivirus es una solución de seguridad integral que nació tras un gran esfuerzo por combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar proactivamente la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques que albergan en Internet sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

ESET Endpoint Antivirus está diseñado principalmente para su uso en estaciones de trabajo en empresas grandes o pequeñas. Se puede utilizar con ESET Remote Administrator, de forma que puede administrar fácilmente cualquier número de estaciones de trabajo cliente, aplicar políticas y reglas, controlar detecciones y configurar de manera remota cualquier ordenador en red.

Requisitos del sistema

Para un funcionamiento óptimo de ESET Endpoint Antivirus, el sistema debería cumplir con los siguientes requisitos de hardware y software:

- Microsoft® Windows® 2000, XP, NT4 (SP6) y Server 2003
- 400 MHz 32 bits (x86)/64 bits (x64)
- 128 MB RAM de memoria del sistema
- 320 MB de espacio disponible
- Super VGA (800 x 600)
- Microsoft® Windows® 7, Vista, Home Servery Server 2008
- 1 GHz 32 bits (x86)/64 bits (x64)
- 512 MB RAM de memoria del sistema
- 320 MB de espacio disponible
- Super VGA (800 x 600) [20]

ANEXO F

Escaneo de puertos

Durante este proceso se permiten identificar los puertos TCP/IP disponibles, las herramientas utilizadas para el escaneo de puertos como NMAP permite conocer los puertos abiertos y el tipo de servicios asociados a ellos), herramientas como HPING permiten realizar escaneo, alteración de paquetes e incluso se pude indicar un rango de puertos a escanear.

El escaneo implica una metodología a seguir según Certified Ethical Hacker, incluye los siguientes pasos.

- ✓ Verificar sistemas activos.
- ✓ Verificar puertos abiertos.
- ✓ Identificar servicios.
- ✓ Determinar el sistema operativo utilizado.
- ✓ Escanear vulnerabilidades.
- ✓ Realizar diagrama de red y las vulnerabilidades de los equipos.
- ✓ Atacar.

La aplicación por excelencia para realizar exploración de puertos es Nmap (Network Mapper), esta herramienta implementa la gran mayoría de las técnicas conocidas para la exploración de puertos y permite descubrir información de los servicios y sistemas encontrados. Nmap también implementa un gran número de técnicas de reconocimiento. Mediante Nmap pueden realizarse, por ejemplo, las siguientes acciones de exploración:

- Descubrimiento de direcciones IP activas mediante una exploración de la red
  .nmap -sP IP ADDRESS/NETMASK
- Exploración de puertos TCP activos.
  .nmap -sT IP ADDRESS/NETMASK
- Exploración de puertos UDP activos.
  .nmap -sU IP ADDRESS/NETMASK
- Exploración del tipo de sistema operativo de un equipo en red.
  .nmap -O IP ADDRESS/NETMASK [21]