



FACULTAD INGENIERIA Y CIENCIAS AGROPECUARIAS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD  
PERIMETRAL PARA LA RED COAC ALIANZA DEL VALLE LTDA.,  
UTILIZANDO TECNOLOGÍA UTM

Trabajo de Titulación presentado en conformidad con los requisitos  
establecidos para optar por el título de Ingeniero en Redes y  
Telecomunicaciones

Profesor guía

Ing. William Eduardo Villegas Chilibingua, MSc

Autor

Geovanny Raúl Villota Loachamin

Año

2016

### **DECLARACIÓN DEL PROFESOR GUÍA**

Declaro haber dirigido este trabajo a través de reuniones periódicas con la Estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

---

William Eduardo Villegas Chilibingua  
Master en Redes de Comunicaciones  
C.I. 171533826-3

### **DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE**

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

---

Geovanny Raúl Villota Loachamin

C.I. 171819737-7

## **AGRADECIMIENTOS**

A mi Santísima Virgen por estar siempre conmigo dándome su ayuda y protección, a mis padres Rosa y Raúl por todo su esfuerzo, dedicación, preocupación y apoyo incondicional a lo largo de mi vida, a Paola y Antonio por brindarme su apoyo en la decisión de alcanzar esta meta, a Ana por estar en mi vida apoyándome incondicionalmente con cariño y amor, agradezco a la COAC Alianza del valle Ltda. por haberme proporcionado toda la información para realizar mi proyecto de titulación, en especial a todas las personas que integran el área de Sistemas.

## **DEDICATORIA**

Dedico de manera especial a mi hermana Paola pues ella fue el principal cimiento para la construcción de mi vida profesional, sentó en mí las bases de responsabilidad y deseos de superación, en ella tengo el espejo en el cual me quiero reflejar pues sus virtudes infinitas y su gran corazón me llevan a admirarla cada día más.

A mis padres Rosa y Raúl por haber formado en mí el deseo de superación y el anhelo de triunfo en la vida.

## RESUMEN

La COAC Alianza del Valle Ltda. es una Institución Financiera de Ahorro y Crédito que presta productos y servicios financieros a sus socios, clientes y la comunidad, enmarcados dentro del ámbito de la responsabilidad social.

La Institución maneja diariamente importante información por lo cual es elemental la instauración de un mecanismo de seguridad que proteja los datos en la red. La implementación de seguridad facultará que no exista la generación de pérdidas en los servicios prestados por la red en la cooperativa.

La implementación de seguridad sobre la red de datos de la COAC Alianza del Valle Ltda. favorecerá a la información constituyéndola exenta de intrusos, por medio de la implementación de políticas en el uso de servicios de red, también la configuración e instalación de la tecnología UTM que permitirá una fácil y perfecta administración, control y monitoreo de la red de la institución.

## ABSTRACT

The COAC Valley Alliance Ltda. Is a financial institution Savings and Credit providing financial products and services to its partners, customers and the community, framed within the field of social responsibility.

The institution manages daily important information which is the establishment of a basic security mechanism that protects the data on the network. Security Implementation empower that there is no generation loss in the services provided by the network in the cooperative.

The implementation of security on the data network of the COAC Valley Alliance Ltda. Favor the information constituting it free from intruders, through the implementation of policies on the use of network services, also the configuration and installation of the UTM technology that allow easy and perfect management, control and monitoring of the network of the institution.

# ÍNDICE

INTRODUCCIÓN.....	1
<b>1. CAPITULO I. MARCO TEÓRICO .....</b>	<b>4</b>
1.1. Fundamentos teóricos de seguridad en redes.....	4
1.2. Seguridad Informática.....	4
1.2.1.Aspectos principales de la seguridad .....	4
1.3. Seguridad Lógica .....	5
1.4. Seguridad Física .....	5
1.5. Gestión de riesgo de la seguridad informática.....	5
1.6. Análisis de riesgo informático.....	6
1.7. Amenazas de la seguridad de la Información .....	7
1.7.1. Ataques Informáticos.....	7
1.8. Mecanismos de monitoreo, control y seguimiento .....	8
1.8.1. Servicios Seguros.....	8
1.8.2. Cortafuegos .....	8
1.8.2.1. Tipos de cortafuegos.....	9
1.8.2.2. Firewall Híbridos .....	9
1.8.2.3. Firewall con zona Desmilitarizada (DMZ).....	9
1.8.2.4. Proxys .....	10
1.8.3. Prácticas enfocadas a la seguridad de la información .....	10
1.9. Mecanismos en la seguridad informática .....	11
1.9.1. ISO 27001 .....	11
1.9.1.1. Política del SGSI .....	11
1.9.2. Recomendaciones NIST serie 800 .....	13
1.9.3. Cooperativas de ahorro y crédito en el Ecuador .....	14
1.9.3.1. Resolución JB-2012-2148 .....	14
1.9.3.1.1. Seguridad en canales electrónicos.....	14
1.9.3.2. Perspectiva de la Norma ISO 27001 en Cooperativas de Ahorro y Crédito.....	15
1.9.3.2.1. Beneficios de una Cooperativa con ISO 27001 .....	15



2. CAPITULO II. SITUACIÓN ACTUAL DE LA RED DE COMUNICACIONES DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE LTDA .....	17
2.1. Antecedentes de la COAC Alianza del Valle Ltda. ....	17
2.1.1. Misión .....	17
2.1.2. Visión.....	18
2.1.3. Organigrama Estructural.....	18
2.2. Estudio de la infraestructura de red de la cooperativa .....	19
2.2.1. Establecer con planificación .....	19
2.2.2. Infraestructura Física .....	19
2.2.3. Análisis de la situación actual de la red de datos.....	21
2.2.4. Infraestructura de la red LAN.....	21
2.2.4.1. Servidores .....	22
2.2.4.2. Información (Base de Datos) .....	23
2.2.5. Estructura de la red WAN de la cooperativa .....	23
2.2.6. Situación actual de la seguridad informática.....	24
2.2.7. Seguridad de las comunicaciones .....	25
2.2.7.1. Antivirus .....	25
2.2.7.2. Ataques de red.....	25
2.2.7.2.1. Contraseñas.....	25
2.2.7.2.2. Seguridad de Base de datos .....	26
2.2.8. Administración del centro de procesamiento de datos .....	27
2.2.8.1. Responsabilidad del departamento de sistemas.....	27
2.2.8.2. Mantenimiento .....	28
2.2.8.3. Respaldos.....	28
2.2.8.4. Documentación .....	28
2.2.9. Amenazas y vulnerabilidades de los servicios de la red.....	28
2.2.9.1. Identificación de Amenazas y Vulnerabilidades .....	29
2.2.9.2. Nivel de Atención de Riegos .....	34

### 3. CAPITULO III. DISEÑO DE LA SEGURIDAD

INFORMATICA.....	40
3.1. Diseño de seguridad en la red de datos .....	40
3.1.1. Alcance y requerimientos de la propuesta.....	40
3.1.2. Esquema de seguridad perimetral.....	40
3.1.3. Mecanismos y Controles de Seguridad .....	40
3.1.4. Definición de políticas de control de acceso.....	46
3.1.4.1. Política de Seguridad de la Información .....	46
3.1.4.1.1. Generalidades .....	46
3.1.4.1.2. Objetivos .....	46
3.1.4.1.3. Alcance.....	46
3.1.5. Seguridad Lógica.....	47
3.1.5.1. Identificación.....	47
3.1.5.1.1. Identificación del dominio .....	48
3.1.5.1.2. Estructura de directorio activo .....	48
3.1.5.1.3. GPO .....	49
3.1.5.1.4. Grupos de Administración de AD .....	50
3.1.5.2. Contraseñas.....	51
3.1.6. Seguridad en las telecomunicaciones .....	52
3.1.6.1. Topología de red .....	52
3.1.6.2. Correo Electrónico .....	52
3.1.6.3. Red de datos.....	52
3.1.6.4. Propiedad de la Información .....	53
3.1.6.5. Uso de los sistemas de comunicación .....	53
3.1.6.6. Conexiones Externas .....	53
3.1.6.7. Configuración lógica de red .....	54
3.1.6.8. Correo .....	54
3.1.6.9. Antivirus .....	55
3.1.6.10. Firewall.....	55
3.1.6.10.1. Tecnología UTM seleccionada.....	55
3.1.6.10.2. Análisis de los Dispositivos UTM.....	56

3.1.6.10.3. Análisis de costos.....	58
3.1.6.11. Ataques de red.....	59
3.1.7. Seguridad de las aplicaciones.....	59
3.1.7.1. Software.....	59
3.1.7.2. Control de aplicaciones en las computadoras.....	60
3.1.7.3. Control de datos en las aplicaciones.....	60
3.1.8. Seguridad Física.....	61
3.1.8.1. Control de acceso físico al Data Center.....	61
3.1.8.2. Control de acceso a equipos.....	61
3.1.8.3. Equipos portátiles.....	62
3.1.8.4. Cableado estructurado.....	62
3.1.9. Administración del centro de cómputo.....	62
3.1.9.1. Dispositivos de soporte.....	62
3.1.9.2. Capacitación.....	63
3.1.9.3. Respaldos.....	63
3.1.9.4. Documentación.....	64
3.1.10. Seguridad física y del entorno.....	64
3.1.10.1. Perímetro de Seguridad.....	64
3.1.10.2. Controles Físicos de Entradas.....	64
3.1.10.3. Seguridad de oficinas, despachos y recursos.....	65
3.1.10.4. Desarrollo de tareas en áreas protegidas.....	65
3.1.10.5. Suministros de energía.....	66
3.1.10.6. Mantenimiento de equipos.....	66
3.1.11. Protección contra software malicioso.....	67
3.1.11.1. Controles contra software malicioso.....	67
3.1.12. Gestión interna de respaldo.....	67
3.1.12.1. Recuperación de la Información.....	67
3.1.13. Gestión de la seguridad de red.....	67
3.1.13.1. Controles de Red.....	67
3.1.13.2. Mensajería electrónica.....	68
3.1.13.3. Uso del Correo Electrónico Corporativo.....	68
3.1.13.4. Restricciones.....	69

3.1.14. Utilización de los servicios de red.....	70
3.1.15. Configuración de acceso por defecto .....	70
3.1.16. Monitoreo de control de acceso.....	70
3.1.17. Restricción del cambio de paquetes de software .....	71
3.1.18. Gestión de continuidad del negocio .....	71
3.1.18.1. Aspectos de la gestión de continuidad del negocio .	71
3.1.18.2. Proceso de gestión de la continuidad del negocio ..	71

## 4. CAPITULO IV. IMPLEMENTACIÓN DE LA

<b>SOLUCIÓN .....</b>	<b>72</b>
4.1. Instalación de equipo UTM .....	72
4.2. Configuración de las interfaces de red.....	75
4.2.1 Interfaz de Acceso principal a Internet mediante Telconet .....	75
4.2.2 Interfaz de Acceso principal a Internet mediante New Access .	76
4.3. Interfaz de Acceso WAN .....	76
4.3.1. AsisteCooper C&W (vlan 50).....	77
4.3.2. Banred Telconet (vlan 40) .....	78
4.3.3. Wan-Claro (vlan 60).....	78
4.3.4. Wan-Cables&Wireless (vlan20).....	79
4.3.5. Wan-Panchonet (vlan10) .....	79
4.3.6. Wan-Telconet (vlan 30) .....	80
4.4. Red Interna .....	80
4.4.1. Configuración de rutas.....	81
4.4.2. Configuración de Policy Routes.....	82
4.4.3. Fail-Over de salida a Internet.....	82
4.4.4. Políticas .....	83
4.4.5. Configuración de Virtual IPs .....	84
4.4.6. Política de conexión entrante por Telconet.....	84
4.4.7. Política de conexión entrante por New-Access.....	85
4.4.8. Configuración de IP POOLS.....	86
4.4.9. Políticas de DoS (Deny of Service).....	86
4.4.10. Configuración de puertos para publicación de servicios	

y accesos entre zonas de firewall .....	86
4.4.11. Objetos de red (direcciones) .....	87
4.4.12. Configuración de VPNs .....	89
4.4.12.1. VPN SSL .....	89
4.4.12.2. VPN IPSec.....	91
4.4.13. Autenticación con Active Directory.....	92
4.4.14. Políticas de conexión entre zonas y la red interna de la Matriz.....	94
4.4.15. Políticas de conexión entre la red interna y las zonas externas fuera de la matriz .....	94
<b>5. CONCLUSIONES Y RECOMENDACIONES.....</b>	<b>96</b>
5.1. Conclusiones.....	96
5.2. Recomendaciones .....	97
<b>REFERENCIAS .....</b>	<b>102</b>
<b>ANEXOS .....</b>	<b>101</b>

## ÍNDICE DE FIGURAS

Figura 1. Gestión de Riesgos.....	6
Figura 2. Firewall.....	9
Figura 3. Firewall con DMZ .....	10
Figura 4. Servidor Proxy.....	10
Figura 5. Análisis de Riesgos NIST 800-30.....	13
Figura 6. Actuación del SGSI sobre el Riesgo Operativo.....	15
Figura 7. Organigrama Estructural de la COAC Alianza del Valle Ltda. ....	18
Figura 8. Edificio Matriz.....	20
Figura 9. Esquema de la red LAN .....	21
Figura 10. Esquema de la red WAN.....	24
Figura 11. Esquema de firewall .....	25
Figura 12. Esquema de seguridad perimetral de la cooperativa .....	45
Figura 13. Estructura de directorio activo .....	49
Figura 14. Grupos de administración del directorio activo.....	50
Figura 15. Esquema de conexión Fortigate 500D .....	74
Figura 16. Configuración interface INTERNET-Telconet.....	75
Figura 17. Configuración interface INTERNET-New Access.....	76
Figura 18. VPN creadas en la interfaz WAN .....	77
Figura 19. Configuración interface AsisteCooper C&W.....	77
Figura 20. Configuración interface Banred Telconet .....	78
Figura 21. Configuración interface Wan-Claro .....	78
Figura 22. Configuración interface Wan-Cables&Wireless.....	79
Figura 23. Configuración interface Wan-Panchonet.....	79
Figura 24. Configuración interface Wan-Telconet .....	80
Figura 25. Configuración interface Red Interna.....	81
Figura 27. Políticas de acceso a los servicios mediante la VPN .....	83
Figura 28. Políticas de acceso a los servicios mediante la VPN .....	83
Figura 29. Política de conexión entrante por Telconet .....	85
Figura 30. Política de conexión entrante por New-Access .....	85
Figura 31. Puerto Uncategorized.....	87

Figura 32. Direcciones de IP Bloqueadas .....	88
Figura 33. Direccionamiento IP de las Agencias .....	88
Figura 34. Grupo de Direcciones.....	89
Figura 35. VPN SSL .....	89
Figura 36. VPN SSLMATRIZG .....	90
Figura 37. VPN SSL .....	90
Figura 38. VPN IPSec .....	91
Figura 39. VPN Amaguaña.....	92
Figura 40. Autenticación con Active Directory .....	93
Figura 41. Autenticación con Active Directory .....	93
Figura 42. Políticas de conexión entre zonas y la red interna de la Matriz.....	94
Figura 43. Políticas de conexión entre la red interna y las zonas externas fuera de la matriz .....	95

## ÍNDICE DE TABLAS

Tabla 1. Amenazas de la seguridad .....	7
Tabla 2. Grados del test .....	8
Tabla 3. Descripción de la infraestructura física.....	19
Tabla 4. Servidores de producción.....	22
Tabla 5. Bases de datos que posee la Cooperativa .....	23
Tabla 6. Análisis de las posibles amenazas que afectarían a las Base de datos que posee Cooperativa en el servidor central y su impacto sobre ella .....	27
Tabla 7. Identificación de vulnerabilidades (Amenaza Usuarios Locales) .....	29
Tabla 8. Identificación de vulnerabilidades (Amenaza Usuarios Externos) .....	31
Tabla 9. Identificación de vulnerabilidades (Desastres Naturales) .....	32
Tabla 10. Identificación de vulnerabilidades (Amenazas Lógicas) .....	33
Tabla 11. Probabilidad de Impacto y Ocurrencia.....	34
Tabla 12. Estudio de controles de seguridad .....	41
Tabla 13. Servicios de Seguridad de los dispositivos.....	56
Tabla 14. Características adicionales de los dispositivos.....	57
Tabla 15. Costos comparativos de las soluciones presentadas. ....	59
Tabla 16. Áreas restringidas.....	65
Tabla 17. Periodo de mantenimiento de equipamiento .....	66
Tabla 18. Vlans .....	72
Tabla 19. Distribución de puertos.....	73
Tabla 20. Descripción de Puertos .....	75



## INTRODUCCIÓN

El proyecto está enfocado en la implementación de seguridad informática en la red de datos de la Cooperativa de Ahorro y Crédito Alianza del Valle Ltda., aplicando políticas de seguridad y utilizando tecnología UTM con la finalidad de reforzar las comunicaciones de la institución.

El primer capítulo describe los conceptos, características, vulnerabilidades y mecanismos relacionados con la Seguridad en Redes; también se presenta la normativa referente a seguridad de información, enfocado el concepto de la Norma ISO 27001.

El segundo capítulo se realiza un análisis de la red COAC Alianza del Valle Ltda. tomando en cuenta aspectos como la infraestructura, los servicios, los protocolos, las aplicaciones que maneja la red y la forma de acceso al Internet, a la Intranet y a la Extranet. Se desarrolla el estudio de la tecnología UTM (Unified Threat Management) realizando un análisis de los módulos que la conforman y exponiendo soluciones de seguridad mediante esta tecnología de tres proveedores: Fortinet, Juniper y Cisco para finalmente realizar una comparación de las mismas para desarrollar el diseño del sistema de seguridad perimetral

En el tercer capítulo se desarrolla el diseño de la seguridad informática en la red, definición de políticas, análisis de las características y costos de las tecnologías UTM.

El cuarto capítulo se basa en la configuración e implementación de los equipos UTM en la red COAC Alianza del Valle Ltda.

Al final de la realización de los capítulos mencionados se desarrollaran las conclusiones y recomendaciones alcanzadas después del desarrollo del proyecto.

## TEMA

Diseño e implementación de un sistema de seguridad perimetral para la red COAC Alianza del Valle Ltda., utilizando tecnología UTM.

## PLANTEAMIENTO DEL PROBLEMA

El sistema de comunicación de la COAC Alianza del Valle Ltda., se encuentra en una fase de desarrollo adaptando nuevas tecnologías que permitirán la transferencia de información en la red.

La red en la actualidad no permite verificar y administrar la transferencia de información que recepta en el exterior de la red LAN, agregando una defectuosa configuración de los dispositivos de red, y un registro de acceso a páginas web no relevantes, que producen la difusión de amenazas de Internet, también la defectuosa administración de servicios como: servidores Web, servidor de producción, servidor de correo electrónico, esto determina que compartir servicios de red entre secciones de la cooperativa no se ejecuten de manera óptima, ocasionando que el tiempo de requerimiento sea alto.

## OBJETIVOS

### OBJETIVO GENERAL

Implementar un sistema de seguridad perimetral en la red COAC Alianza del Valle Ltda., utilizando tecnología UTM.

### OBJETIVOS ESPECÍFICOS

- Analizar las características y ventajas existentes en cada una de las tecnologías UTM de tal manera la seleccionada cubra las necesidades que se presentan en la institución.
- Realizar un análisis costo beneficio de las diferentes tecnologías.
- Diseñar el modelo de seguridad perimetral en la red de datos de la cooperativa tomando en cuenta los estándares establecidos en la ISO 27001 y la resolución JB-2012-2148. Artículo 4.3.11.5. que regula a entidades de la economía popular y solidaria.

- Implementar el diseño de seguridad perimetral en la red de datos con el correcto funcionamiento de cada segmento de red.
- Crear las políticas de seguridad que permitan la continuidad del negocio en la institución para posterior evaluación de las mismas simulando tanto ataques internos como externos.

## 1. CAPITULO I. MARCO TEÓRICO

### 1.1. Fundamentos teóricos de seguridad en redes

Un aspecto esencial en un sistema de red moderna es la seguridad de la información, la cual se considera como un agente que no ayuda directamente en el rendimiento del sistema, debido a esto no se otorga una atención apropiada ni los recursos para ejecutar esta tarea. Los sistemas informáticos en la actualidad se exponen a diferentes peligros por lo cual es necesario implementar métodos que proporcionen el adecuado uso de contenidos y recursos.

### 1.2. Seguridad Informática

Es el grupo de recursos designados a conseguir que los activos de una institución sean reservados, intactos, consistentes y disponibles a sus clientes, autorizados por dispositivos de control de acceso y sometidos a auditoria.

#### 1.2.1. Aspectos principales de la seguridad

La seguridad considera tres aspectos importantes:

- **Confidencialidad.** Se refiere a la protección de información personal a fin de no ser divulgada sin consentimiento.
- **Disponibilidad.** Un sistema seguro debe poseer la cualidad de permitir que la información se encuentre disponible para el usuario, cuando él lo requiera.
- **Integridad.** Condición de seguridad que garantiza que la información solo puede ser modificada por personal autorizado.

### 1.3. Seguridad Lógica

Se fundamenta en la aplicación de procedimientos que protejan el acceso de datos, estableciendo que solo el personal autorizado podrá acceder a ellos.

Existen controles que se logran efectuar en la seguridad lógica:

- **Controles de acceso.** Se refiere a la implementación de controles en varios utilitarios de red permitiendo la integridad de información.
- **Roles.** Se ejecuta mediante el análisis al cargo que desempeña el usuario que necesita dicho acceso.
- **Limitaciones a los servicios.** Se fundamentan en las restricciones del propio aplicativo impuestos por el administrador.
- **Identificación, autenticación.** Identificación es el instante en el cual el usuario se da a conocer en el sistema y autenticación se basa en la verificación que ejecuta el sistema sobre esta identificación.
- **Listas de control de acceso (ACL's).** Su función es depurar el tráfico de la red.

### 1.4. Seguridad Física

La seguridad física no es tomada en cuenta en el diseño de un esquema de red, aunque es sustancial pues acepta la aplicación de barreras físicas y procedimientos de control.

### 1.5. Gestión de riesgo de la seguridad informática

Es un método que determina, analiza, valora y clasifica el riesgo, con la finalidad de implementar mecanismos que controlen el riesgo.

La gestión de riesgo está constituida por cuatro partes como se visualiza en la figura 1.



- **Análisis:** Establece los elementos de un sistema que demanda protección ante vulnerabilidades que lo exponen a un peligro.
- **Clasificación:** Ayuda a instaurar si los riesgos identificados y restantes pueden ser aceptados.
- **Reducción:** Constituye e implementa las acciones de defensa.
- **Control:** establece y ajusta las medidas defectuosas y ratifica la falta de cumplimiento.

Cualquier proceso está establecido en políticas de seguridad, normas y reglas, que establecen el marco operativo del proceso.

### 1.6. Análisis de riesgo informático

La información es el activo más importante de la institución, por ello, deben constar métodos que la protejan.

Esto se consigue mediante los siguientes medios:

- a) Delimitar el acceso a los archivos y programas.
- b) Certificar que los operadores logren trabajar sin modificar los archivos y programas.
- c) Asegurar el uso de archivos y programas idóneos por el medio seleccionado.
- d) Certificar la información entregada y ésta sea la misma recibida por el receptor al cual se ha enviado.
- e) Afirmar que consten sistemas y procedimientos de emergencia alternos de transmisión entre varios puntos.
- f) Organizar a los empleados en base a jerarquía informática, estipulando claves y permisos distintos en cada uno de los sistemas que el empleado podrá acceder.
- g) Reemplazar continuamente las contraseñas de accesos a los sistemas.

### 1.7. Amenazas de la seguridad de la Información

Se pueden mencionar cuatro categorías en la siguiente tabla 1:

Tabla 1. Amenazas de la seguridad

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

Tomado de (Vienites, 2007)

#### 1.7.1. Ataques Informáticos

Es un intento por el cual un usuario podría tomar el control o dañar a un sistema informático o de red.

- *Ataques pasivos.* Se basan en escuchar los datos transmitidos pero no

pueden ser modificados.

- *Ataques activos*. Se basan en modificar la información que ha sido interceptada.

En la tabla 2 se presenta el test de penetración conformado por cuatro grados.

Tabla 2. Grados del test

DESCUBRIMIENTO	•Recopila toda información crítica.
EXPLORACIÓN	•Identificar las posibles víctimas.
EVALUACIÓN	•Búsqueda de vulnerabilidades de los datos encontrados.
INTRUSIÓN	•Realizar ataques a través de las vulnerabilidades.

Tomado de (Monroy, 2010)

## 1.8. Mecanismos de monitoreo, control y seguimiento

Dependiendo de los requerimientos de la institución los mecanismos de monitoreo varían, entre ellos tenemos bitácoras de acceso a sistema, errores de sistema, tráfico de red, entre otros.

### 1.8.1. Servicios Seguros

Estos servicios brindan confianza en sus procesos, entre éstos tenemos la integridad, confidencialidad, no repudio, autenticación, control de acceso y disponibilidad.

### 1.8.2. Cortafuegos

Su tarea es controlar los datos de entrada y salida de la red, estos deben estar ubicados en un sitio en el que puedan interceptar todo el flujo de datos como se observa en la figura 2.



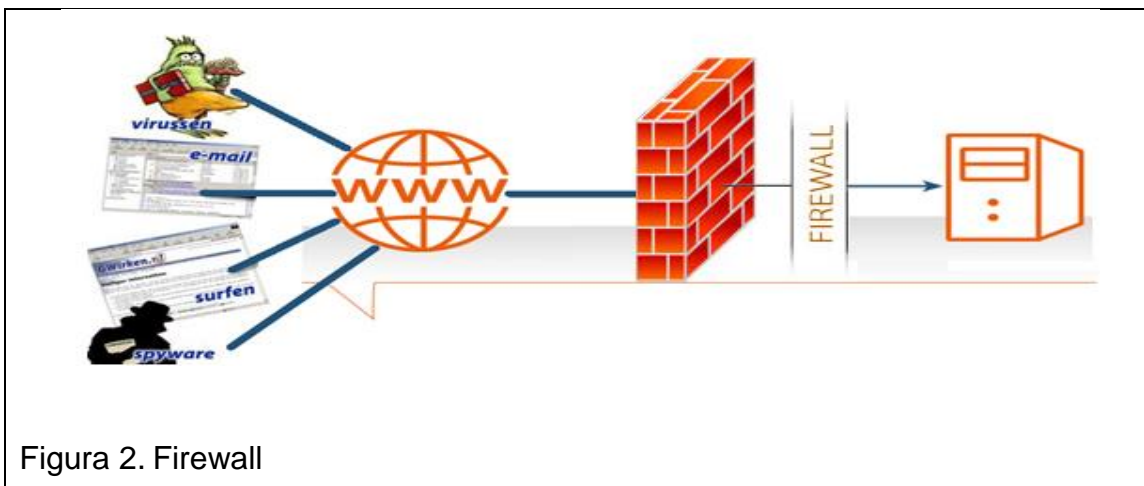


Figura 2. Firewall

### 1.8.2.1. Tipos de cortafuegos

Los cortafuegos se pueden clasificar en:

- Software: Programa instalado en un servidor provisto de al menos dos tarjetas de red.
- Hardware: dispositivos de red especializados que están conformados tanto de hardware y software personalizados.

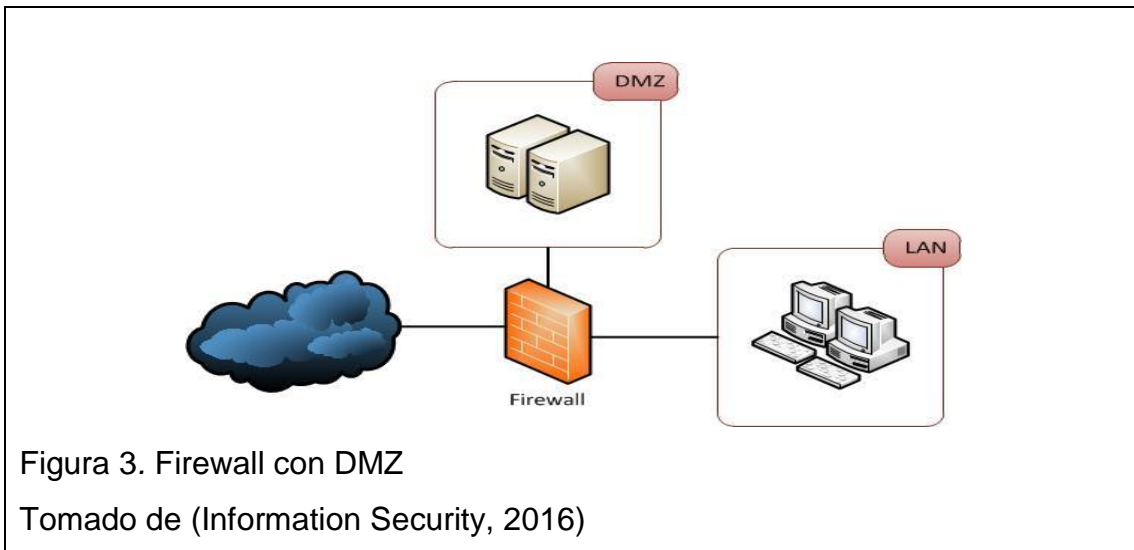
### 1.8.2.2. Firewall Híbridos

Se refiere a una combinación de dos tipos de firewalls.

### 1.8.2.3. Firewall con zona Desmilitarizada (DMZ)

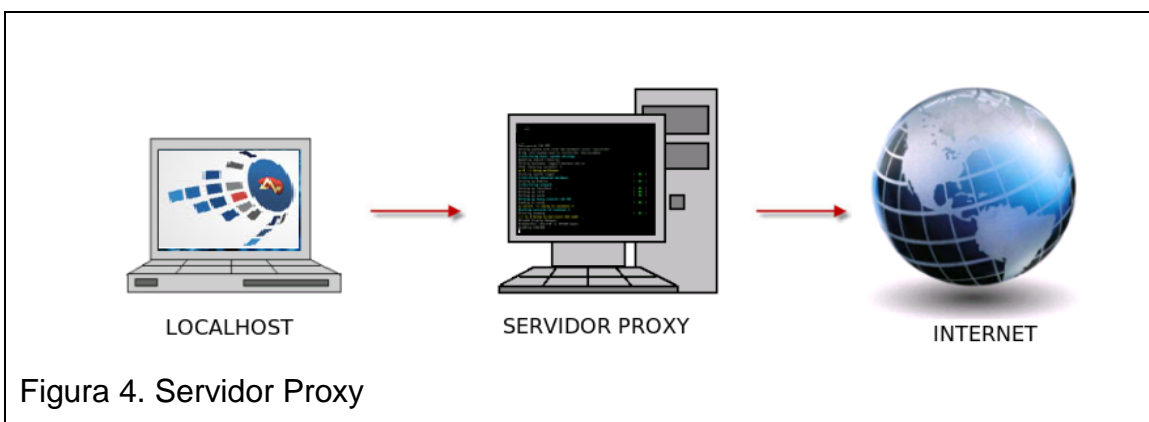
Solución que permite a los clientes conectarse a la red a partir de cualquier medio externo que puede ser Internet o diferente ruta.

Los usuarios externos consiguen asociarse a la sección protegida de la red, pero no logran interactuar con el resto de la red como se puede visualizar en la figura 3.



#### 1.8.2.4. Proxys

Es un programa o dispositivo que tiene como objetivo realizar una tarea de acceso a Internet en lugar de otro computador como se puede visualizar en la figura 4.



#### 1.8.3. Prácticas enfocadas a la seguridad de la información

Las principales prácticas para la seguridad de información son:

- Desarrollo de inventarios de activos.
- Realización de inventarios de activos.
- Aplicación un cuestionario al administrador de la red.
- Utilización un plan de contingencia.

- Realización de políticas de seguridad.
- Implementación niveles de seguridad informática.
- Concientización sobre seguridad de la red LAN.
- Utilización de la Norma ISO 27001.

### **1.9. Mecanismos en la seguridad informática**

Las instituciones financieras para funcionar regularmente deben cumplir con algunos estándares y normas además los métodos tecnológicos están basados en las Normas ISO cumpliendo sus estándares y normas, que corresponde al conjunto de metodologías determinadas para el manejo de otros procesos dentro de las instituciones.

Cada uno de los procedimientos para el diseño, planeación e implementación de la seguridad informática dentro de la red de datos de la cooperativa se realizará por medio de los fundamentos de las Normas ISOS 27000.

#### **1.9.1. ISO 27001**

Es un estándar de referencia desarrollado para el establecimiento, implementación, monitorización, operación, revisión, mantenimiento y mejora de un SGSI para los diferentes tipos de organización.

Esta norma permite diseñar y establecer un SGSI mediante la influencia de las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, la dimensión, la estructura y los sistemas de soporte de la organización.

##### **1.9.1.1. Política del SGSI**

Documento general que se basa en una declaración de intenciones donde se debe tomar en cuenta:

- Incluye el marco general y los objetivos de seguridad de la información de la organización.

- Estimar las necesidades de negocio conjunto a los requerimientos legales referentes a seguridad de información.
- La organización donde se amparará el SGSI se establecerá con el contexto importante de la gestión de riesgos.
- Construye las razones de evaluación de riesgo.
- Acoger por la dirección.

En el enfoque se define la estimación de riesgos por medio de una metodología de valoración del riesgo adecuada para el SGSI. Es preciso especificar una táctica de aprobación de riesgo constituyendo razones de aprobación y los niveles de riesgo admisible.

- **Reconocer los riesgos:**

- Conocer las amenazas notables en los activos reconocidos.
- Conocer los activos de la información que están conformando el alcance del SGSI, los cuales tienen valor para la organización.
- Determinar las vulnerabilidades que son aprovechadas por las amenazas.
- Establecer el impacto por pérdida de confiabilidad, disponibilidad e integridad de los activos.

- **Valorar los riesgos:**

- Calcular el impacto de una interrupción de seguridad de un activo de información en el negocio.
- Apreciar de forma objetiva la posibilidad de ocurrencia de interrupción de seguridad en dependencia a las vulnerabilidades.
- Valorar los niveles de riesgo.

- **Tratamiento de riesgos:**

- Utilizar controles apropiados.
- Admitir el riesgo siempre y cuando se cumplan con criterios para admisión de los riesgos.

- Evadir el riesgo.

### 1.9.2. Recomendaciones NIST serie 800

La finalidad del NIST reside en construir normas y procesos con la finalidad de aumentar la producción, agilizar el comercio, optimizar la calidad de vida. En la figura 5 se presenta los controles necesarios para salvaguardar los sistemas.

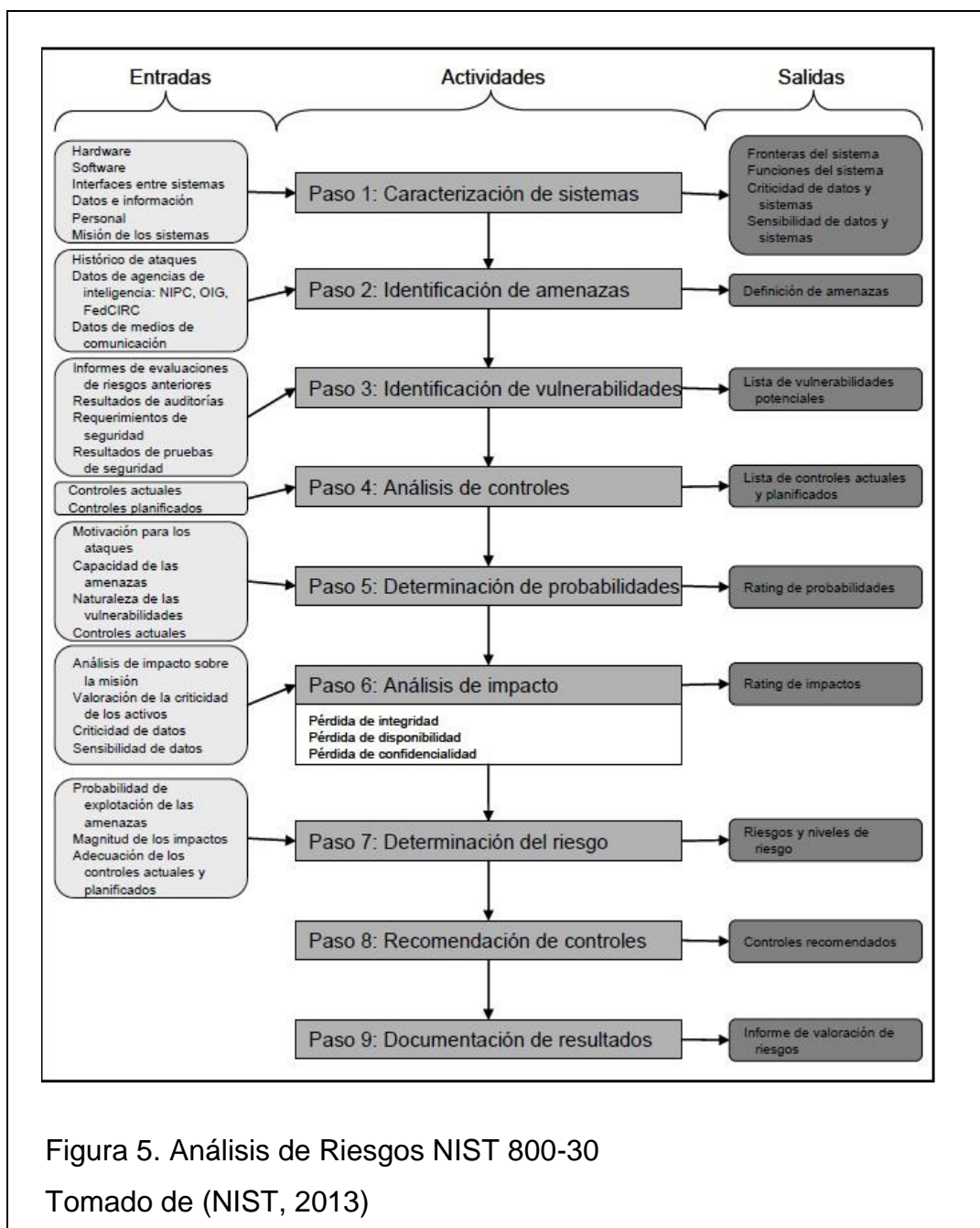


Figura 5. Análisis de Riesgos NIST 800-30

Tomado de (NIST, 2013)

### **1.9.3. Cooperativas de ahorro y crédito en el Ecuador**

En el sistema financiero nacional las cooperativas de ahorro y crédito han logrado la intervención del 10%, por lo cual en el 2013 son vigiladas por la Superintendencia de Economía Popular y Solidaria.

#### **1.9.3.1. Resolución JB-2012-2148**

La Superintendencia de Economía Popular y Solidaria emitió la resolución JB-2012-2148, la cual estipula la gestión y administración de riesgos para las instituciones financieras que ayudan a advertir el cometimiento de fraudes bancarios.

##### **1.9.3.1.1. Seguridad en canales electrónicos**

Con el propósito de asegurar las transacciones realizadas a través de canales electrónicos las cooperativas deben cumplir con lo siguiente:

- Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes.
- El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, ésta deberá estar sometida a técnicas de encriptación internacionales.
- Las instituciones del sistema financiero deberán tener en todos sus canales electrónicos un software antimalware permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código.
- Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, para identificar eventos inusuales, fraudulentos o corregir fallas.
- Ofrecer a los clientes la personalización de las condiciones bajo las

cuales desean realizar sus transacciones a través de los canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. (Junta Bancaria, 2012).

### 1.9.3.2. Perspectiva de la Norma ISO 27001 en Cooperativas de Ahorro y Crédito

En las cooperativas de ahorro y crédito la norma ISO 27001 se debe considerar debido a que estas instituciones están expuestas a diferentes riesgos.

En general, los riesgos toman diferentes naturalezas, no obstante, el sistema de gestión de seguridad de la información determinado por la norma ISO 27001, se ejerce en los riesgos operativos. La figura 6 especifica este concepto.



#### 1.9.3.2.1. Beneficios de una Cooperativa con ISO 27001

El SGI con ISO 27001 en una institución financiera brinda beneficios en la calidad de su organización.

- Admite a la institución financiera ajustarse a los requerimientos de BASILEA II en vinculación a riesgos patrimoniales.
- Establecer un sistema para atenuar el riesgo operativo con advertencias en la realización de los controles.
- La reducción del riesgo operativo permite un alto impacto económico.
- Faculta a la institución la aseguración de continuidad en su funcionamiento gracias a un sistema.



## **2. CAPITULO II. SITUACIÓN ACTUAL DE LA RED DE COMUNICACIONES DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE LTDA**

### **2.1. Antecedentes de la COAC Alianza del Valle Ltda.**

La Cooperativa de Ahorro y Crédito Alianza del Valle Ltda. en el año 1969 moradores del barrio Chaupitena ubicado en el Valle de los Chillos, identificaron la necesidad de crear una Institución que apoye a la comunidad en sus proyectos y tenga una visión solidaria, por ello inicia la idea de realizar una cooperativa de ahorro para captar el dinero, capitalizarlo y brindar crédito a todos y cada uno de sus asociados. COOAC Alianza del Valle Lta. Siempre enfocada hacia la satisfacción de sus asociados, apoyo a la comunidad brindando seguridad, confianza, para convertirse en una verdadera amiga a su servicio. La institución tiene una trayectoria de 46 años en el Ecuador.

Es una institución financiera que brinda servicios de captación de recursos, operaciones crediticias destinados a sus socios, esto ha ayudado que la institución tenga un progreso moderado pero seguro, lo que se irradia en su permanencia en el sector.

La institución en el edificio matriz cuenta con aproximadamente 65 empleados distribuidos en tres plantas y 72 empleados distribuidos en sus nueve agencias entre ellas Chillogallo, Colón, Conocoto, Guamaní, El Inca, Machachi, Sangolquí, Amaguaña y Tumbaco.

#### **2.1.1. Misión**

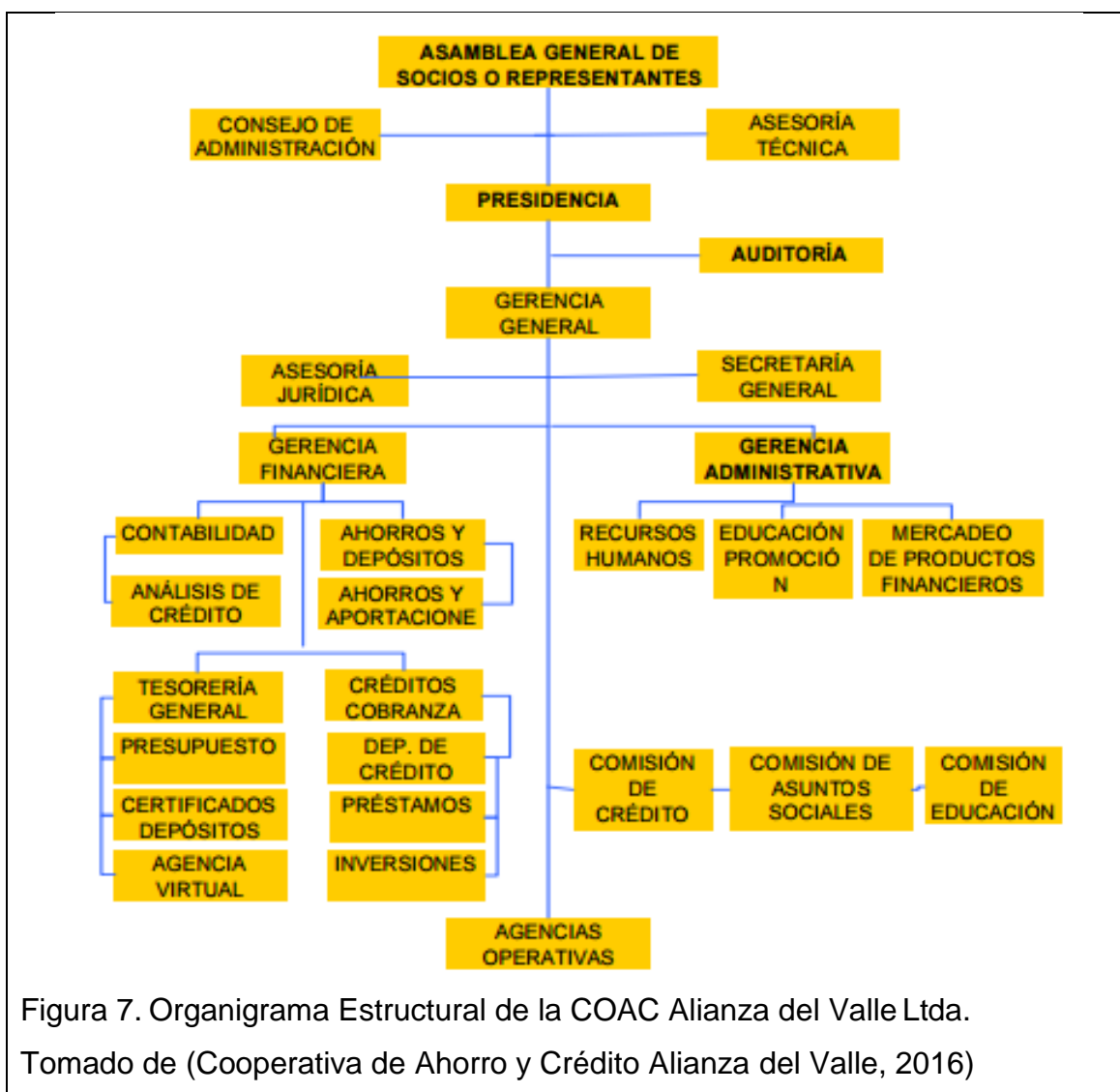
"Somos una institución financiera de ahorro y crédito que brindamos servicios financieros de calidad que contribuyen a satisfacer las necesidades de inversión y financiamiento de nuestros socios, clientes y la comunidad, enmarcados dentro del ámbito de la responsabilidad social". (COAC Alianza del Valle Ltda., 2014).

### 2.1.2. Visión

En el año 2018 “Alianza del Valle Ltda.” se mantendrá dentro de las cinco primeras Cooperativas del Segmento 1, evaluados en términos de productividad y desempeño; ofertando sus productos y servicios financieros dentro de la Provincia de Pichincha. (COAC Alianza del Valle Ltda., 2014).

### 2.1.3. Organigrama Estructural

La estructura de organización de la institución se muestra en la Figura 7:



## 2.2. Estudio de la infraestructura de red de la cooperativa

El presente proyecto se basó en la utilización de la norma ISO 27001, para desarrollar cada uno de los procesos de forma sistemática y correcta, en la actualidad la cooperativa está creciendo y es preciso el cumplimiento de los diferentes parámetros estandarizados para adquirir una acreditación.

### 2.2.1. Establecer con planificación

Para el diseño de un sistema de gestión de seguridad fundamentado en la norma ISO 27001, se debe analizar varios aspectos para alcanzar un correcto diseño e implementación, a continuación se definen varios parámetros que se encuentran conformando la etapa de planificación de la norma.

### 2.2.2. Infraestructura Física

La tabla 3 presenta la descripción de la infraestructura física que posee la cooperativa.

Tabla 3. Descripción de la infraestructura física

COMPONENTE	SITUACIÓN ACTUAL
Infraestructura de la Cooperativa	<ul style="list-style-type: none"> <li>• La matriz de la cooperativa cuenta con un edificio de tres pisos como se puede visualizar en la figura 8.</li> <li>• En la planta baja se encuentra ubicadas las cajas, información, créditos, cobranzas y el área de Procesos.</li> <li>• En el primer piso se ubica el departamento de contabilidad, inversiones y sistemas. En el segundo piso de encuentran las áreas de Recursos Humanos, Legal y la oficina de Gerencia.</li> <li>• Los servidores están ubicados en el Data Center el cual se encuentra en el área de Sistemas.</li> </ul>
Entrada a las instalaciones en la Matriz	<ul style="list-style-type: none"> <li>• Constan dos accesos principales en el edificio las cuales están custodiadas por guardias de seguridad.</li> <li>• Cualquier persona puede ingresar al área de cajas.</li> </ul>

Planos Arquitectónicos	<ul style="list-style-type: none"> <li>• El edificio tiene planos de la edificación completa.</li> </ul>
Instalaciones Eléctricas	<ul style="list-style-type: none"> <li>• Las tomas eléctricas no cumplen con las especificaciones técnicas adecuadas.</li> <li>• Tiene una planta de energía eléctrica defectuosa.</li> <li>• Carece de una red de UPS centralizada para los distintos departamentos.</li> </ul>
Detectores de humo	<ul style="list-style-type: none"> <li>• Carece de sistemas detectores de humo.</li> </ul>
Extintores de incendio	<ul style="list-style-type: none"> <li>• En los diferentes departamentos no se cuentan ubicados los extintores de incendio.</li> </ul>
Cableado estructurado	<ul style="list-style-type: none"> <li>• Tienen un cableado estructurado que no se encuentra certificado, carece de planos de cableado.</li> </ul>
Acceso al Data Center	<ul style="list-style-type: none"> <li>• El acceso no es restringido para el personal de sistemas.</li> <li>• Posee una puerta de vidrio y una cerradura</li> </ul>
Seguridades del Data Center	<ul style="list-style-type: none"> <li>• El Data Center no cuenta con ninguna seguridad contra incidentes.</li> </ul>
Sistema de enfriamiento para el Data Center	<ul style="list-style-type: none"> <li>• Tiene un sistema de aire acondicionado defectuoso sin un controlador de temperatura.</li> </ul>
Central Telefónica	<ul style="list-style-type: none"> <li>• Tiene una central telefónica VoIP.</li> </ul>
Salida de emergencia	<ul style="list-style-type: none"> <li>• El edificio posee una salida de emergencia.</li> </ul>



Figura 8. Edificio Matriz

### 2.2.3. Análisis de la situación actual de la red de datos

Mediante la información proporcionada por el departamento de sistemas, la realización de inventarios y la revisión de las instalaciones se recopiló información necesaria para establecer el análisis actual que presenta la red de datos.

### 2.2.4. Infraestructura de la red LAN

La infraestructura de red que posee la cooperativa está conformada de la siguiente forma:

La red tiene 2 ISP o salidas a internet y 4 enlaces de datos como se puede observar en la figura 9; es decir, que conjuntamente con la LAN y DMZ, se dispone de 8 Zonas de firewall en la Matriz y 3 en cada sucursal (1 ISP, 1 datos y LAN).

Consta de un switch 3COM de 24 puertos /100 MBPS el cual se encarga de controlar los puntos de red, desde el servidor están interconectados en un rack en el data center, la distribución de los puntos de red están realizados mediante cableado UTP categoría 5e, permitiendo una transmisión entre 100 Mbps.

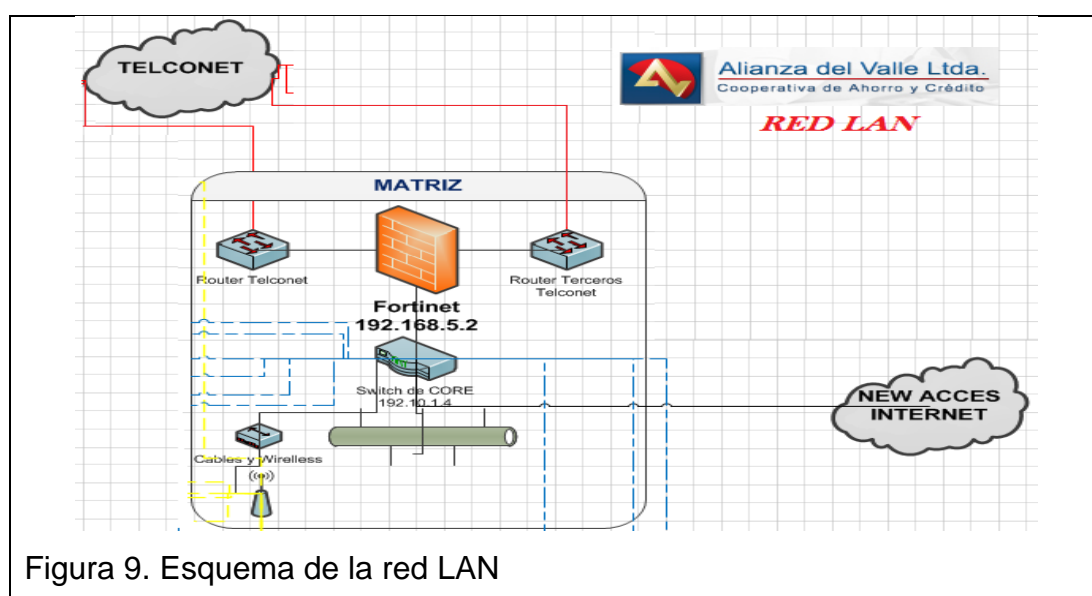


Figura 9. Esquema de la red LAN

### 2.2.4.1. Servidores

La cooperativa dispone de un servidor de producción (Branch), un servidor central y uno de transacciones. El servidor encargado de controlar la información relevante de la cooperativa es el servidor central tanto en matriz como en agencias.

En la tabla 4 se detallan los nombres e IP's de los servidores de producción.

Las agencias cuentan con un servidor Branch cada una, el cual se conecta directamente al servidor central ubicado en matriz, para realizar el intercambio y actualización de información.

En cada agencia los servidores presentan lo siguiente:

- Tiene configurado 4 Appserv (Herramienta OpenSource para Windows)
- Diagrama de seguridad
- Encolamiento por prioridad en las transacciones

Tabla 4. Servidores de producción

<b>SERVIDOR DE PRODUCCIÓN</b>	
<b>Nombre del host</b>	<b>Alianza</b>
Dirección IP	192.10.xx.xx
<b>Servidor de Standby</b>	
<b>Nombre del host</b>	alianza1
<b>Dirección IP</b>	192.168.xxx.xx
<b>Servidor de Replicación</b>	
<b>Nombre del host</b>	<b>Alianza</b>
<b>Dirección IP</b>	192.10.xxx.xx
<b>Servidor de Base de Datos</b>	
<b>Nombre del host</b>	SERVIDOR ASE DE PRODUCCION
<b>Dirección IP</b>	192.10.xx.xx
<b>Nombre del host</b>	SERVIDOR ASE DE STANDBY
<b>Dirección IP</b>	192.168.xxx.xx
<b>Nombre del host</b>	SERVIDOR ASE QUE ADMINISTRA LA RSSD
<b>Dirección IP</b>	192.10.xx.xxx

## Especificación de servidores

- Servidor Central Sun Fire 250 (**PRODUCCIÓN**)
- Servidor Central SUN 250 ENTER PRISE (**DESARROLLO**)
- Servidor Compaq EVO para control de BANRED
- Servidor HP de red LAN de Matriz Alianza de Valle
- Servidor HP Linux Firewall
- Servidor HP cajeros automáticos
- Servidor HP Sitio Web

### 2.2.4.2. Información (Base de Datos)

Cada módulo del sistema COBIS, tiene su particular base de datos las que se encuentran en el motor de base de datos SYSDATABASE. Al final de la jornada de trabajo diario se realizan los respaldos de cada uno de estos módulos.

Las bases de datos que posee la cooperativa se presenta en la tabla 5.

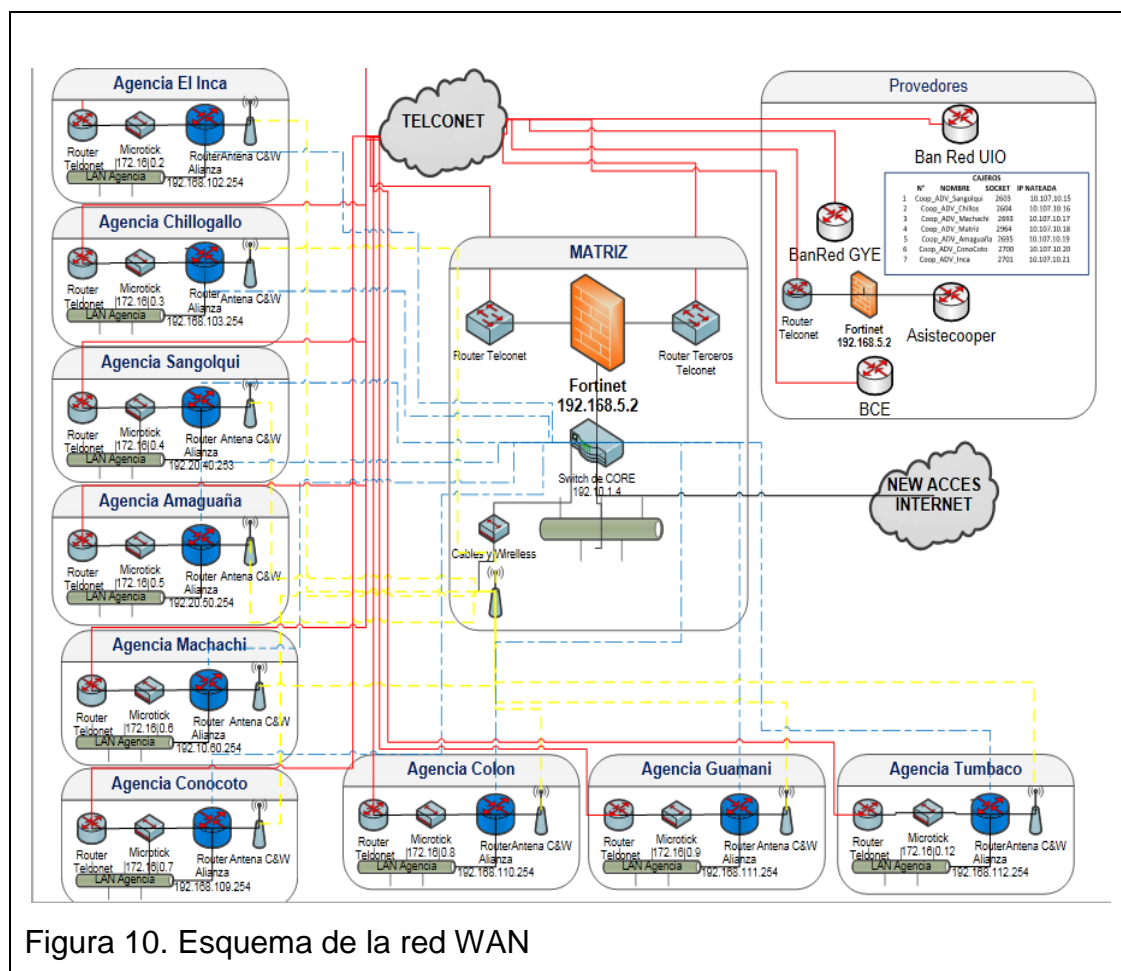
Tabla 5. Bases de datos que posee la Cooperativa

BASE DE DATOS	RESPONSABLE
<b>Seguridades</b>	Administrador BD
<b>Ahorros</b>	Administrador BD
<b>Cartera</b>	Administrador BD
<b>Crédito</b>	Administrador BD
<b>Plazo Fijo</b>	Administrador BD
<b>Contabilidad</b>	Administrador BD
<b>Firmas</b>	Administrador BD
<b>MIS</b>	Administrador BD
<b>Riesgos de Mercado</b>	Administrador BD
<b>Garantías</b>	Administrador BD
<b>Seguridades</b>	Administrador BD
<b>Ahorros</b>	Administrador BD

### 2.2.5. Estructura de la red WAN de la cooperativa

La cooperativa posee dos enlaces que se puede observar en la figura 10, el primer enlace suministra el servicio de internet y el segundo enlace suministra

la conexión entre matriz y las agencias para la transmisión de los datos del sistema financiero.



### 2.2.6. Situación actual de la seguridad informática

Actualmente la cooperativa dispone de un firewall Fortigate 310B con el objetivo de proteger el data center y los usuarios en la matriz que se observa en la figura 11. La cooperativa no dispone de un sistema de seguridad perimetral en las sucursales por lo que no dispone de herramientas de seguridad avanzadas como IPS, App Control y Network Access Control para el aseguramiento de sus datos, previsión de ataques internos y externos y validación y monitoreo de los usuarios de su red interna.



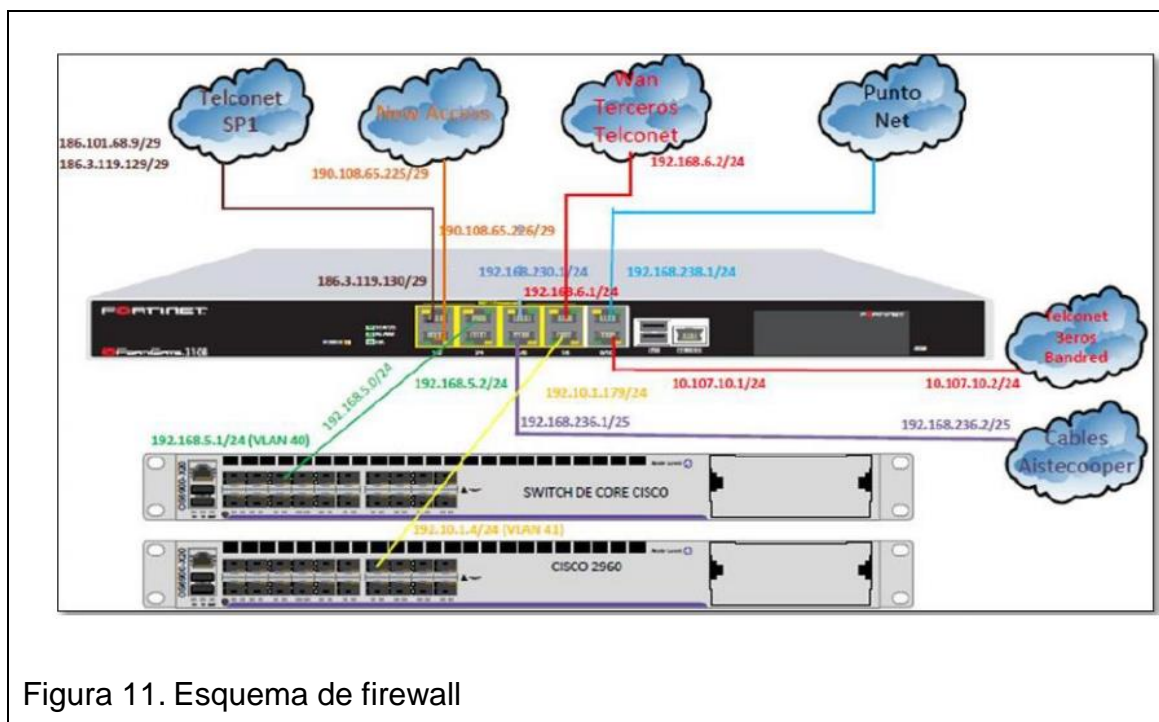


Figura 11. Esquema de firewall

## 2.2.7. Seguridad de las comunicaciones

### 2.2.7.1. Antivirus

La cooperativa cuenta con una licencia corporativa del antivirus ESET Endpoint Security, éste fue instalado en las estaciones de trabajo.

Por medio de dispositivos extraíbles y descargas de internet se han presentado inconvenientes en algunas estaciones de trabajo por contagio de virus.

### 2.2.7.2. Ataques de red

No existen herramientas para advertir y combatir los ataques de red.

#### 2.2.7.2.1. Contraseñas

La Cooperativa Alianza del Valle tiene un directorio activo fundamentado en una organización simple, ésta consta de tres unidades organizacionales que son:

- Asistentes

- Jefaturas
- Operativos

En el directorio activo se registra el ingreso de un nuevo funcionario a la cooperativa según el cargo que va a ejercer, esto admitirá el uso de recursos y aplicaciones de la red en su estación de trabajo. A la información de la base de datos solo puede acceder el Administrador del sistema.

#### **2.2.7.2.2. Seguridad de Base de datos**

La Base de datos son esenciales para el normal funcionamiento de todos los departamentos que forman parte de la cooperativa, éstas se exponen a diferentes tipos de amenazas principalmente a:

- Robo de información
- Acciones hostiles
- Ataques de hackers y Crackers
- Ataques por virus, gusanos, bombas lógicas
- Suspensión del servicio
- Memoria insuficiente del servidor para atender las transacciones solicitadas.

Luego de identificar las principales amenazas a las que se encuentra expuesta la base de datos de la cooperativa, el análisis de dichas amenazas y su impacto en la Cooperativa se detalla en la tabla 6.

Tabla 6. Análisis de las posibles amenazas que afectarían a las Base de datos que posee Cooperativa en el servidor central y su impacto sobre ella

BASE DE DATOS	AMENAZAS	IMPACTO	CALIFICACIÓN
SEGURIDADES	Acciones Hostiles Suspensión del servicio	Catastrófico	<b>Imprescindible</b>
AHORROS	Acciones Hostiles Suspensión del servicio	Catastrófico	<b>Imprescindible</b>
CARTERA	Acciones Hostiles Suspensión del servicio	Catastrófico	<b>Imprescindible</b>
CRÉDITO	Acciones Hostiles Suspensión del servicio	Catastrófico	<b>Imprescindible</b>
PLAZO FIJO	Acciones Hostiles Suspensión del servicio	Crítico	<b>Imprescindible</b>
CONTABILIDAD	Acciones Hostiles Suspensión del servicio	Crítico	<b>Imprescindible</b>
FIRMAS	Acciones Hostiles Suspensión del servicio	Marginal	<b>Prioritario</b>
MIS	Acciones Hostiles Suspensión del servicio	Catastrófico	<b>Imprescindible</b>
RIESGOS DE MERCADO	Acciones Hostiles Suspensión del servicio	Marginal	<b>Prioritario</b>
GARANTÍAS	<b>Acciones Hostiles Suspensión del servicio</b>	<b>Crítico</b>	<b>Imprescindible</b>

## 2.2.8. Administración del centro de procesamiento de datos

### 2.2.8.1. Responsabilidad del departamento de sistemas

El departamento de sistemas tiene una persona encargada de la infraestructura dentro de la cooperativa, quien se encarga de realizar las tareas de administración de la tecnología, no existe un encargado de la seguridad.

El encargado de reportar al gerente cada una de las actividades del departamento es el jefe de sistemas cuyo trabajo es administrar el sistema y la infraestructura.

### **2.2.8.2. Mantenimiento**

- El soporte de inconvenientes en equipos de cómputo de agencias se realiza mediante software de conexión remota, las soluciones dadas a estos inconvenientes no son registradas en bitácoras o documentación del proceso realizado.
- Se programa el mantenimiento preventivo a los equipos de cómputo, existen ocasiones que no se efectúa ya que solo una persona está encargada de las TI de la cooperativa, este resuelve problemas importantes y el mantenimiento se posterga.
- En la actualidad carece de un inventario con su etiquetado de activos.

### **2.2.8.3. Respaldos**

- Respaldos de datos en los servidores.
- En un disco externo se respalda diariamente la información generada en el motor de base de datos.
- Respaldos de datos de los computadores.
- Cada uno de los usuarios efectúa sus respaldos en su computador.

### **2.2.8.4. Documentación**

No disponen de ningún tipo de documentación en base a los recursos ni configuraciones realizadas en los equipos de la cooperativa, de igual forma carece de manuales de políticas y procedimientos a cumplirse en el departamento de sistemas.

### **2.2.9. Amenazas y vulnerabilidades de los servicios de la red**

En esta fase se cuenta con información recopilada de los activos expuestos actividades concluidas en la encuesta realizada [ANEXO A].

### 2.2.9.1. Identificación de Amenazas y Vulnerabilidades

En el **Paso 2 “Identificación de amenazas”**, se puede determinar las amenazas, con las cuales se llegó a la resolución de las vulnerabilidades definidas en el **Paso 3** que consiste en la **“Identificación de vulnerabilidades”** establecido en NIST 800-3, en la tabla 7, tabla 8, tabla 9 y tabla 10 se detallan las principales amenazas y vulnerabilidades.

Tabla 7. Identificación de vulnerabilidades (Amenaza Usuarios Locales)

AMENAZA	VULNERABILIDAD
<b>Humanas (Usuarios Internos)</b> <b>Malintencionados</b> <b>Inexpertos Negligentes</b> <b>Deshonestos</b>	Inexistencia o falta de :
	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.
	Respalos de información.
	Respalos 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.
	Respalos en USB sin cifrado.
	Respalos 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.

Tomado de (Garcés, 2015)

Tabla 8. Identificación de vulnerabilidades (Amenaza Usuarios Externos)

AMENAZA	VULNERABILIDAD
<b>Humanas (Usuarios externos)</b>	Falta de :
<b>Delincuencia Hacker</b>	Identificación con credencial del personal que ingresa a la entidad Controles de acceso físicos a oficinas.
<b>Crackers</b> <b>Ex-empleados Otros</b>	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 de 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.

Tomado de (Garcés, 2015)

Tabla 9. Identificación de vulnerabilidades (Desastres Naturales)



AMENAZA	VULNERABILIDAD
<b>Desastres Naturales</b>	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.

Tomado de (Garcés, 2015)

Tabla 10. Identificación de vulnerabilidades (Amenazas Lógicas)

AMENAZA	VULNERABILIDAD
<b>Amenazas Lógicas</b>	Falta de :
<b>Virus Gusanos Troyanos</b>	Dispositivos de seguridad perimetral.
<b>Spyware Malware Otros</b>	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.

Tomado de (Garcés, 2015)

### 2.2.9.2. Nivel de Atención de Riesgos

Mediante el Paso 5 y 6 “ocurrencia y el análisis de impacto” (ver tabla 11), se lograra obtener la revisión de instalaciones y resoluciones gerenciales sobre la prioridad de interés de riesgos.

La valoración del impacto se lo efectuará de forma cualitativa, se considera un activo sustancial determinando el tipo de información que manipula.

**Alto:** se requiere realizar acciones correctivas inmediatas.

**Medio:** son necesarias acciones correctivas y desarrollar un plan para reunir estas acciones en un intervalo de tiempo.

**Bajo:** se percató de un bajo riesgo y se determina si hay que tomar acciones correctivas o se decide aceptar el riesgo.

Tabla 11. Probabilidad de Impacto y Ocurrencia

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

Limitantes de potencia en UPS.	Alta	Alto	Disponibilidad	<b>Alto</b>
Falta de mecanismos de control perimetral de la red.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Uso de protocolos de administración inseguros.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Inexistencia de políticas de uso de red.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Inexistencia de políticas para servidores.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Inexistencia de respaldos en equipos	Alta	Alto	Integridad	<b>Alto</b>
Acceso a todos los recursos de red institucional.	Media	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Uso de una misma contraseña por periodos largos de tiempo.	Media	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Uso de una contraseña única en varios equipos.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Uso de contraseñas no robustas.	Media	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Confianza en otras personas.	Media	Alto	Confidencialidad	<b>Alto</b>
Uso de IP's homologadas para usuarios en general.	Media	Alto	Confidencialidad	<b>Alto</b>

Fallas por parte del proveedor del suministro eléctrico.	Alta	Alto	Disponibilidad	<b>Alto</b>
Puertos abiertos sin uso en estación de trabajo.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Daños en la configuración de los equipos por poco mantenimiento.	Alta	Alto	Disponibilidad	<b>Alto</b>
Inexistencia de procedimientos de cambios en sistemas.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Inexistencia de cifrado en discos duros.	Alta	Alto	Confidencialidad Disponibilidad Integridad	<b>Alto</b>
Tableros eléctricos expuestos.	Medio	Medio	Disponibilidad	<b>Medio</b>
Controles de acceso físicos, inseguros para administración de servidores.	Alta	Medio	Confidencialidad Disponibilidad Integridad	<b>Medio</b>
Vulnerabilidades en el protocolo TCP/IP.	Media	Medio	Confidencialidad Disponibilidad	<b>Medio</b>
Daño en hardware por fallas eléctricas.	Media	Medio	Disponibilidad	<b>Medio</b>
Inexistencia de control en el tráfico de red generado por la institución.	Media	Medio	Confidencialidad Disponibilidad Integridad	<b>Medio</b>
Fuga de información.	Media	Medio	Confidencialidad Disponibilidad Integridad	<b>Medio</b>
Daño físico a la infraestructura de red.	Media	Medio	Disponibilidad	<b>Medio</b>

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

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

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

Tomado de (Garcés, 2015)

### **3. CAPITULO III. DISEÑO DE LA SEGURIDAD INFORMATICA**

#### **3.1. Diseño de seguridad en la red de datos**

Luego de considerar el punto 2.2, se ha logrado establecer las debilidades de seguridad informática en la cooperativa, a partir de esta información es posible realizar un diseño óptimo de seguridad utilizando la ISO 27001 colectivamente con la Metodología NIST que reconoce el análisis de vulnerabilidades y riesgos.

##### **3.1.1. Alcance y requerimientos de la propuesta**

Para el diseño de seguridad en la red de la cooperativa se implantará controles de seguridad que permitan eliminar vulnerabilidades, facultando la reducción de los niveles de riesgos dentro de la cooperativa.

##### **3.1.2. Esquema de seguridad perimetral**

Se estableció con conformidad del departamento de sistemas las vulnerabilidades; para lo cual se pactó la implementación de mecanismos UTM en el proyecto para proteger el flujo de información.

##### **3.1.3. Mecanismos y Controles de Seguridad**

Se presenta en la siguiente tabla el paso 4 que consiste en el "Análisis de los controles", exponiendo un listado de controles con los que cuenta en la actualidad para restar las vulnerabilidades (ver tabla 12).



Tabla 12. Estudio de controles de seguridad

<i>VULNERABILIDAD</i>	<i>CONTROL SUGERIDO</i>	<i>NIVEL DE RIESGO</i>
Carencia de controles en la red inalámbrica en la Matriz	Implementación de cifrado	<b>Riesgo alto</b>
Administración de direcciones IP	Inventario de asignación de direcciones IP a servidores y usuarios	<b>Riesgo alto</b>
Falta de control en descargas de información a través de la utilización de internet de la red de la cooperativa	Firewall, proxy	<b>Riesgo alto</b>
Carencia de cuidado del equipo de cómputo a cargo de los funcionarios	Sensibilizar en temas de seguridad	<b>Riesgo alto</b>
Restricción de potencia en UPS	Mantenimiento y compra de un UPS	<b>Riesgo alto</b>
Escasez de mecanismos de control perimetral de la red	Gestor de uso de red, Firewall, IDS	<b>Riesgo alto</b>
Carencia de políticas de uso de red	Creación de políticas de uso de red	<b>Riesgo alto</b>
Falta de políticas para la utilización de servidores	Creación de políticas para el funcionamiento de servidores	<b>Riesgo alto</b>
Carencia de respaldos en equipos activos	Creación de políticas de respaldo	<b>Riesgo alto</b>
Utilización de protocolos de administración inseguros	Creación de políticas de configuración de equipos activos	<b>Riesgo alto</b>
Utilización de contraseñas por periodos largos de tiempo	Creación Políticas de contraseñas	<b>Riesgo alto</b>
Utilización de una contraseña única en varios equipos	Sensibilizar en temas de seguridad, políticas de contraseñas	<b>Riesgo alto</b>
Utilización de contraseñas no robustas	Sensibilizar en temas de seguridad, políticas de contraseñas	<b>Riesgo alto</b>
Confianza en otras personas en la utilización de equipos de cómputo personal	Sensibilizar en temas de seguridad.	<b>Riesgo alto</b>
Utilización de IP's homologadas para usuarios en servidores	Vlan, NAT	<b>Riesgo alto</b>

Fallas de suministro eléctrico por falta de transformador	Compra de un transformador	<b>Riesgo alto</b>
Daños de configuración en equipos por poco mantenimiento	Realización de mantenimiento preventivo	<b>Riesgo alto</b>
Puertos abiertos inutilizados en estación de trabajo	Políticas de hardening.	<b>Riesgo alto</b>
Carencia de procedimientos de variaciones en el sistemas	Políticas de control de cambios	<b>Riesgo alto</b>
Carencia de cifrado en discos duros	Implementación Cifrado	<b>Riesgo alto</b>
Tableros eléctricos descubiertos	Informar de la observación al proveedor eléctrico	<b>Riesgo medio</b>
Controles de acceso físicos al Data Center	Poner en funcionamiento controles	<b>Riesgo medio</b>
Deterioro en hardware por fallas eléctricas	Redes eléctricas reguladas	<b>Riesgo medio</b>
Susceptibilidad en el protocolo TCP/IP	Establecer políticas de monitoreo	<b>Riesgo medio</b>
Carencia de registro en el tráfico de red generado por la cooperativa	Establecer gestor de uso de red	<b>Riesgo medio</b>
Fuga de datos	Gestión de fuga de información, políticas de confidencialidad,	<b>Riesgo medio</b>
Desgaste físico en la infraestructura de red	Aplicar cableado estructurado	<b>Riesgo medio</b>
Carencia de controles de seguridad en portátiles	Colocación de candados de seguridad para portátiles.	<b>Riesgo medio</b>
Carencia de monitoreo de uso de la red	Políticas de monitoreo de la red	<b>Riesgo medio</b>
Carencia de un sistemas de aire acondicionado en el Data Center	Adquisición de sistema de aire acondicionado	<b>Riesgo medio</b>
Control de acceso débil en aplicaciones	Políticas desarrollo de software seguro	<b>Riesgo medio</b>
Personal con escasa capacitado en temas de seguridad.	Capacitación del personal de temas de seguridad	<b>Riesgo medio</b>

Carencia de actualizaciones de software en terminales de trabajo, servidores, antivirus y equipos de red	Políticas de hardening en estaciones de trabajo y servidores	<b>Riesgo medio</b>
Carencia de mantenimiento de instalaciones eléctricas	Mantenimiento preventivo en instalaciones eléctricas	<b>Riesgo medio</b>
Carencia de corriente eléctrica regulada	Implementar corriente eléctrica regulada	<b>Riesgo medio</b>
Cableado de red exhibido	Cableado estructurado.	<b>Riesgo medio</b>
Respaldos en la misma unidad de disco duro	Políticas de respaldo	<b>Riesgo medio</b>
Ingreso a todas las terminales de administración	Listas de control de acceso	<b>Riesgo medio</b>
Acceso a todos los recursos de internet sin restricción	Gestor de contenido	<b>Riesgo medio</b>
Falta de controles de humedad	Implementación de sensor de humedad	<b>Riesgo</b>
Inexistencia de controles de temperatura	Sensor de temperatura.	<b>Riesgo medio</b>
Visitas a sitios con software malicioso	Capacitación al usuario	<b>Riesgo medio</b>
Descarga de software ejecutable de sitios no confiables	Capacitación al usuario	<b>Riesgo medio</b>
Carencias de políticas sobre el uso del equipo de cómputo	Creación de políticas sobre el uso del equipo de cómputo	<b>Riesgo medio</b>
Colocación de dispositivos extraíbles en equipos de cómputo sin análisis	Políticas de hardening	<b>Riesgo medio</b>
Falta de políticas de utilización de software	Políticas de hardening	<b>Riesgo medio</b>
Carencia de instrucciones de creación de cuentas	Creación de políticas de contraseñas	<b>Riesgo medio</b>
Tiempo de vida útil de los equipos de cómputo	Renovación de hardware	<b>Riesgo medio</b>

Utilización de versiones viejas en software de aplicaciones	Actualizaciones de software	<b>Riesgo medio</b>
Vulnerabilidades conocidas en sistemas operativos	Actualizaciones de software	<b>Riesgo medio</b>
Falta de cultura de seguridad en usuarios finales	Capacitación para los usuarios	<b>Riesgo medio</b>
Fallas de proveedor de servicios de internet	Establecer enlaces redundantes	<b>Riesgo medio</b>
Carencia de monitoreo de las aplicaciones del Cobis	Implementación de herramientas de monitoreo	<b>Riesgo medio</b>
Fallos de cambios en la configuración de equipos de cómputo y servidores	Capacitación del personal	<b>Riesgo bajo</b>
Desastres naturales en la cooperativa	<b>Prevención de desastres naturales para el personal</b>	<b>Riesgo bajo</b>

A continuación se muestra el esquema de seguridad (ver figura 12) que se podrá implementar en la cooperativa en base a las necesidades y recursos con los que cuenta la cooperativa.

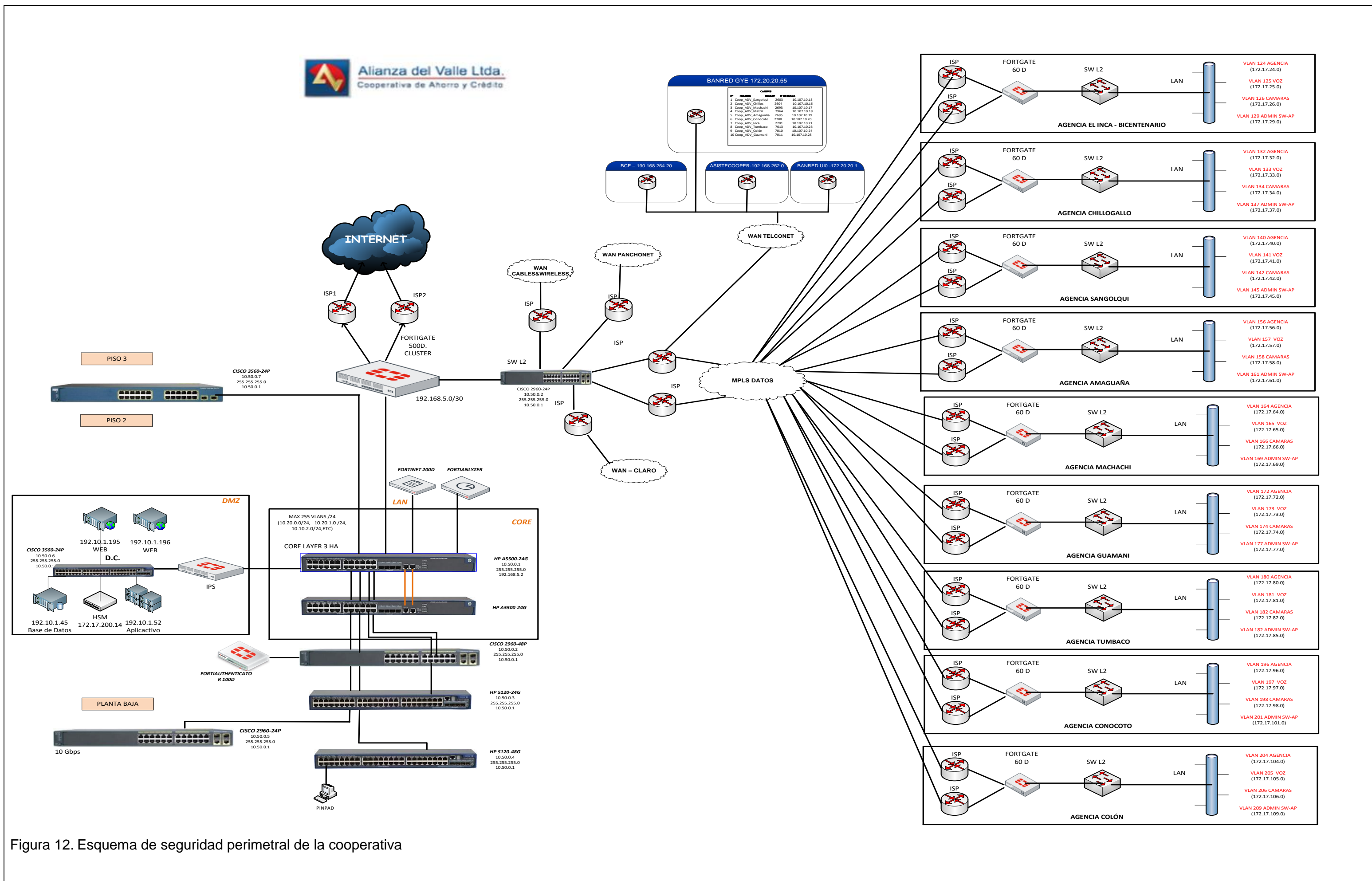


Figura 12. Esquema de seguridad perimetral de la cooperativa

### **3.1.4. Definición de políticas de control de acceso**

Para establecer la definición de políticas de control en la red se necesita utilizar el nivel de implementación y utilización de un SGSI explicados en la norma ISO 27001.

#### **3.1.4.1. Política de Seguridad de la Información**

##### **3.1.4.1.1. Generalidades**

Un mecanismo de protección para la red son la políticas de seguridad, las cuales aprueban la continuación operacional de sistemas informáticos reconociendo cumplir con los objetivos de reducir el riesgo.

##### **3.1.4.1.2. Objetivos**

- Confirmar la ejecución de mecanismos de seguridad, los cuales deben permanecer actualizados para establecer una protección adecuada de todos los recursos de tecnología de la información.
- Proteger la información y recursos físicos de la cooperativa ante las amenazas de cualquier índole.
- Establecer los lineamientos de procedimientos necesarios para establecer la protección y correcto funcionamiento de recursos de información.

##### **3.1.4.1.3. Alcance**

Las políticas se enmarcaran en proteger la seguridad de las comunicaciones y de los equipos de cómputo. Se establecerá una memoria técnica la cual está encaminada al personal de la cooperativa para que cumplan los procedimientos, políticas y normas que permiten resguardar la información. El no cumplimiento de dichas políticas por el personal ocasionará medidas disciplinarias.

### 3.1.5. Seguridad Lógica

#### 3.1.5.1. Identificación

Un usuario para efectuar el acceso al sistema tiene que realizar un procedimiento formal y por escrito donde tienen que constar los siguientes datos:

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:

- Colocar ID de usuario.
- Colocar una contraseña, que tendrá caracteres alfanuméricos.
- Registrar nombres y apellidos completos.
- Especificar el grupo al cual pertenece el usuario.
- Especificar el tiempo de expiración de contraseñas.
- Credenciales de ingreso al área de usuarios

Para los usuarios se estipula la asignación de permisos mínimos necesarios para que realicen su labor diaria, tomando en cuenta lo siguiente:

- En horas no laborables el usuario no puede acceder a sus cuentas de la institución.
- En vacaciones o licencias de maternidad las cuentas de dichos usuarios deben ser desactivadas.
- Las contraseñas de los usuarios deben ser secretas e intransferibles.
- Se necesita establecer un control mensual del ingreso de usuarios solo a las aplicaciones especificadas del sistema según su cargo laboral.
- El área de recursos humanos debe notificar al administrador de sistemas el ingreso o cambio de cargo de los usuarios para emitir los permisos necesarios.

- Los sistemas informáticos deben estar configurados con un tiempo de espera en un periodo de cinco minutos, luego de este tiempo sin utilización el sistema del equipo se cerrara.
- Se impide el uso de cuentas invitadas, los usuarios deberán ingresar con sus respectivas credenciales.
- La generación de usuarios con perfiles de usuarios con máximos privilegios deben ser mínimos.
- La entrega de credenciales de utilización del dominio de la cooperativa a usuarios nuevos debe realizarse por escrito y sumilla de recepción tanto del administrador del sistema como del usuario.
- Los cambios de roles o reseteo de credenciales se debe realizar por escrito al administrador.

#### **3.1.5.1.1. Identificación del dominio**

La infraestructura montada en la Cooperativa Alianza del Valle está compuesta por un total de dos servidores controladores de dominio.

Nombre del dominio FQDN: **alianzadelvalle.fin.ec**

Nombre del dominio NetBios: **alianzadelvalle**

#### **3.1.5.1.2. Estructura de directorio activo**

La estructura de la Cooperativa Alianza del Valle está basado en una organización simple, basada en tres OU llamada:

- Asistentes
- Jefaturas
- Operativo

La estructura está conceptualizada en base a la estructura funcional de la empresa, pero las OU están creadas a nivel de la raíz (Ver figura 13).





Figura 13. Estructura de directorio activo

Las computadoras están alojadas en el contenedor por defecto Computers.

### 3.1.5.1.3. GPO

El directorio activo está compuesto por 15 políticas de grupo.

La lista de políticas es la siguiente:

- Bloqueo Inactividad
- Configuración Internet
- Contraseñas
- Default Domain Controllers Policy
- Default Domain Policy
- Ejecución Office
- Escritorio
- Hora
- Hora Única

- Instalar programas
- Internet
- Manu Inicio
- No Escritura Discos Extraibles
- Prueba GPO Unica
- Pruebacopi

#### 3.1.5.1.4. Grupos de Administración de AD

Los grupos de administración del directorio activo Administrators y Domain Admins poseen varios usuarios, los mismos que deben ser evaluados. (Ver figura 14).

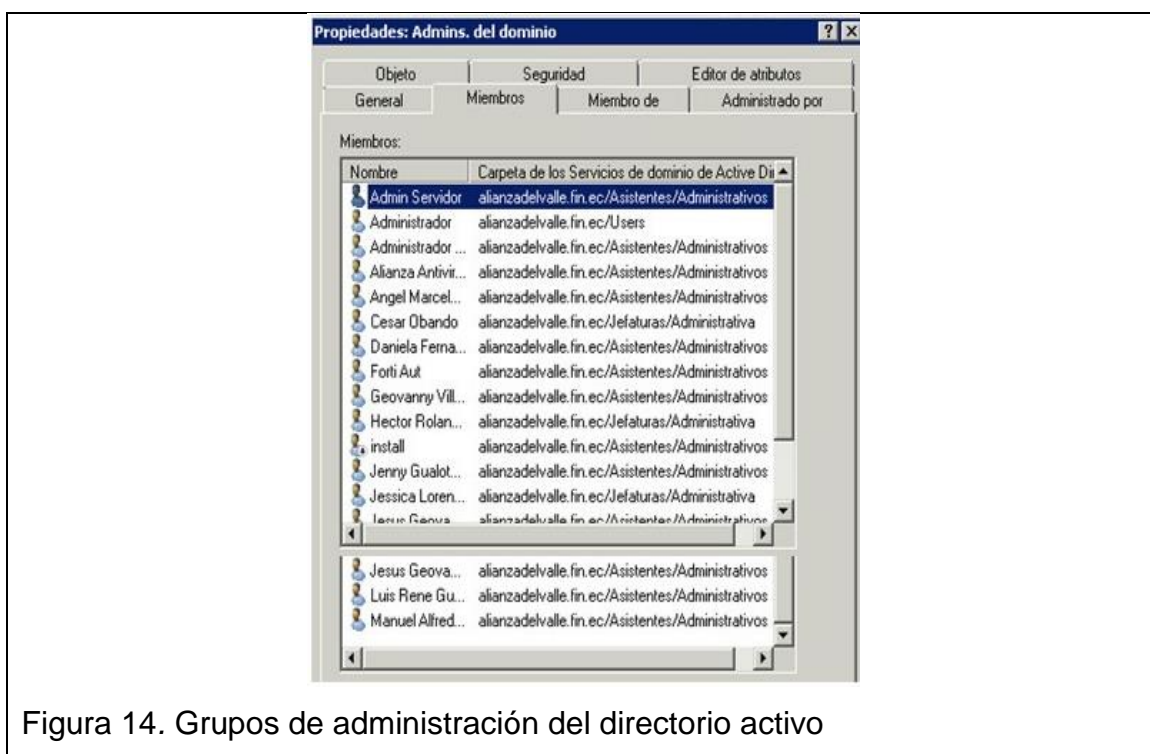


Figura 14. Grupos de administración del directorio activo

Los miembros de este grupo tienen control total sobre los servidores controladores de dominio.

### 3.1.5.2. Contraseñas

Éstas deben cumplir con requerimientos y estándares internacionales.

No debe ser común o fácil de adivinar la contraseña de verificación de identidad, además deben seguir con lo siguiente:

- Como mínimo tener de longitud al menos 8 caracteres.
- Se debe incluir una combinación de caracteres no alfabéticos y alfabéticos (signos de puntuación, números o caracteres especiales) o una combinación mínima dos tipos de caracteres no alfabéticos.
- Como parte la contraseña no debe contener su user ID.
- La información crítica de sistemas y aplicaciones de la cooperativa requiere al menos un cambio de contraseña cada tres meses (90 días). Si los sistemas o aplicaciones no lo realizan automáticamente es obligación del responsable hacer que se cumpla el mencionado cambio.
- La contraseña nueva debe contener al menos los últimos tres utilizados.
- Bloquear a los usuarios que haya intentado acceder al sistema fallando más de cinco veces consecutivas.
- El usuario puede modificar su contraseña las veces necesarias.
- Para el primer inicio de sesión es válida la primera contraseñada asignada al usuario, el usuario debe modificar su contraseña efectuando los requisitos establecidos
- La contraseña de un usuario no debe guardar su en una forma legible en archivos, disco, y mucho menos escrita en papel y dejarla en sitios que pueda ser encontrada.
- Antes de poner en producción los nuevos equipos de TI como routers, switches, etc se debe cambiar inmediatamente las contraseñas predefinidas.

### **3.1.6. Seguridad en las telecomunicaciones**

#### **3.1.6.1. Topología de red**

- Para los diagramas de la infraestructura de red debe existir documentación detallada.
- En el caso de que alguna contingencia afecte al medio primario de comunicación debe existir medios alternativos de transmisión.

#### **3.1.6.2. Correo Electrónico**

Es autorizado exclusivamente el uso del correo electrónico corporativo, para lo cual solo se debe almacenar en servidor lo siguiente:

- Correos de entrada y salida de los usuarios.
- La hora específica de envío.
- El asunto del mensaje
- El contenido de uso de la institución
- Archivos o carpetas adjuntos.
- Novedad de virus de cada parte del mensaje.
- IP de máquina que emite y recepta.
- El tamaño de contenido del mensaje.

#### **3.1.6.3. Red de datos**

Para la comunicación es esencial la red de datos cuya información se debe recopilar acerca de:

- Ancho de banda usada.
- El tráfico formado por aplicaciones.
- Detalle de recursos de servidores que usan los aplicativos.
- 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.

En servidores, central telefónica, equipos de vigilancia y equipos de red de la cooperativa que se realicen los cambios y nuevas instalaciones de software, igualmente reconfiguraciones de Switches y el cambio de direcciones IP deben ser aprobados y documentados, con excepción de una situación de emergencia. Esto se realiza para evadir dificultades por cambios que causen limitación en la comunicación, rechazo de servicio, caída de la red.

#### **3.1.6.4. Propiedad de la Información**

Se considera como propiedad de la cooperativa y no como propiedad de los usuarios de los servicios de comunicación que brinda la cooperativa a los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo.

#### **3.1.6.5. Uso de los sistemas de comunicación**

Solo para actividades de trabajo deben manipularse los recursos de los sistemas de comunicación de la cooperativa. El uso personal es permisible si el consumo mínimo de recursos y tiempo, y estos no dificulte la productividad del empleado ni las actividades de la institución.

#### **3.1.6.6. Conexiones Externas**

- Para propósitos de negocios y mediante autorización de la Gerencia será únicamente habilitado el servicio de Internet de la cooperativa.
- Se debe certificar el tráfico de entrada y salida de la red interna, deben ser filtrados y controlados por un firewall impidiendo todo tráfico que no sea autorizado.
- Deberán establecer por escrito los mecanismos de transmisión y las responsabilidades de las partes, cada vez que se precise instaurar

conexión con terceros.

- La cooperativa puede revisar el contenido de las comunicaciones de Internet si cree que la seguridad está siendo vulnerada, el uso de Internet debe ser monitoreado periódicamente.

### **3.1.6.7. Configuración lógica de red**

Se debe considerar lo siguiente cuando necesite conectar a la red algún equipo de terceros o que no formen parte a la cooperativa:

- En la red no identificarse como un usuario determinado.
- Sin la debida autorización explícita de la gerencia y la aprobación del administrador de la red no ejecutar programas de monitoreo de tráfico (Ej. similares o "sniffer").
- Sin previa autorización no agregar dispositivos que amplíe la infraestructura de la red de la cooperativa.
- Sea un número variable y confidencial la dirección IP de la empresa se la asegura.

### **3.1.6.8. Correo**

Se debe considerar los siguientes puntos para la administración y uso del correo corporativo:

- En el servidor de la cooperativa debe existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico.
- El correo electrónico no debe ser utilizado para mensajes no relacionados con los propósitos de la cooperativa, para enviar cadenas de mensajes, no se debe relacionar con actividades ilegales y no éticas.
- Deben ser encriptados los datos que se consideren "confidenciales" o "críticos".
- Para cada una de las cuentas de correo electrónico de los empleados se debe asignar una capacidad de almacenamiento fija.

### **3.1.6.9. Antivirus**

Se debe instalar y ejecutar un antivirus actualizado en todos los equipos de la cooperativa, cumpliendo con:

1. Controlar y detectar acciones de intento de un software malicioso en tiempo real.
2. Elaborar habitualmente un escaneo de las unidades de almacenamiento para la revisión y detección de software malicioso almacenado en la estación de trabajo.
3. Diariamente se actualiza la base de datos de virus.
4. Debe ser un producto totalmente legal (con licencia o Software libre).

A menos que sea necesario y hayan sido anticipadamente escaneados y estén libres de virus u otros agentes dañinos los dispositivos externos no deben ser usados en las computadoras de la cooperativa.

### **3.1.6.10. Firewall**

La cooperativa debe presentar un firewall configurado de modo que se encuentren habilitados solo los protocolos y servicios requeridos.

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

El personal encargado del mantenimiento periódico del firewall debe verificar la configuración de los servicios de red y desarrollar un informe técnico de las verificaciones desarrolladas.

#### **3.1.6.10.1. Tecnología UTM seleccionada**

Las soluciones de seguridad perimetral han evolucionado en los últimos tiempos debido al progreso de peligrosas amenazas, por lo cual en la

actualidad tenemos sistemas de protección de red en tiempo real. Para la realización del diseño del presente proyecto se analizó tres proveedores de tecnologías UTM como son Juniper, Cisco y Fortinet.

### 3.1.6.10.2. Análisis de los Dispositivos UTM

En la siguiente tabla 13 se presenta las características de servicios de seguridad de los dispositivos UTM:

Tabla 13. Servicios de Seguridad de los dispositivos

Servicios de Seguridad			Fortinet	Juniper	Cisco
<i>VPN</i>					
<b>Túneles IPSec VPN</b>			3.000	1.000	<b>5.000</b>
<i>Firewall</i>					
<b>Paquetes / Segundo</b>			No Especifica	600.000	
<i>Antivirus</i>					
<b>Análisis IM</b>			No Especifica	si	
<b>Firmas de virus</b>				200.000+	
<b>Capacidad de análisis</b>			<ul style="list-style-type: none"> <li>- AntiSpyware</li> <li>- Prevención de Gusanos</li> <li>- Túneles VPN</li> <li>- HTTP/SMTP/POP3/IMAP/FTP/IM</li> </ul>	<ul style="list-style-type: none"> <li>- Anti-spyware</li> <li>- Anti-adware</li> <li>- Anti-keylogger</li> <li>- POP3/HTTP/SMTP/IMAP/FTP/IM</li> </ul>	<ul style="list-style-type: none"> <li>- Antivirus</li> <li>- AntiSpyware</li> <li>- File Blocking</li> <li>- AntiPhising</li> <li>- HTTP/SMTP/FTP/POP3/HTML/ICMP/DNS/RPC/NETBIOS/GRE</li> </ul>
<i>Filtrado web</i>					
<b>Bloqueo</b>			<ul style="list-style-type: none"> <li>- URL</li> <li>- palabra clave</li> <li>- frase</li> <li>- Java Applet</li> <li>- Cookies</li> <li>- Active X</li> </ul>	Filtrado web integrado en Anti-Spam	<ul style="list-style-type: none"> <li>- URL</li> <li>- Active X</li> <li>- Java Applet</li> <li>- VBScript</li> </ul>
<i>IDS / IPS</i>					
<b>Amenazas</b>			3.000+		
<b>Soporte protocolo</b>	anomalía	de	Si	si	<b>Si</b>
<b>Soporte patrón de firma</b>			Si	si	<b>No Especifica</b>
<b>Soporte aplicaciones</b>	anomalía	de	No Especifica	No Especifica	<b>Si</b>
<i>AntiSpam</i>					



Capacidad	<ul style="list-style-type: none"> <li>- Lista Negra en tiempo real</li> <li>- Lista Negra de IP</li> <li>- Análisis cabecera MIME</li> <li>- Filtra frases/palabras</li> </ul>	Filtra URLs	Detecta spam mediante tecnología heurística
-----------	---	-------------	---

Tomado de (Alulema, 2008)

Características adicionales que posee cada dispositivo (Ver tabla 14).

Tabla 14. Características adicionales de los dispositivos

Características Adicionales	Fortinet	Juniper	Cisco
<i>Hardware y Rendimiento</i>			
<b>Slots PIM</b>	-----	6	-----
<b>Interfaz WAN (PIMS)</b>	-----	serial, E1, T1, DS3, E3, ADSL, ADSL2, G.SHDSL	-----
<b>Interfaz LAN (PIMS)</b>	-----	10/100,10/100/1000, SPF	-----
<b>Flash Externo</b>	-----	USB1.1	-----
<b>Nuevas sesiones/Segundo</b>	10.000	15.000	<b>28.000</b>
<b>Políticas</b>	20.000	4.000	<b>100.000</b>
<i>Funciones</i>	Modelado de tráfico	Administración del tráfico (QoS)	<b>Optimizador del ancho de banda: PacketShaper 7500</b>
	Networking/Routing	Routing	<b>Routing</b>
	Administración	Administración	<b>Administración</b>
	Monitoreo/Registro	Monitoreo/Registro	<b>Monitoreo/Registro</b>
	Autenticación de usuarios	Autenticación de usuario y Control de Acceso	-----
	Dominios Virtuales	Virtualización	
	Alta Disponibilidad	Alta Disponibilidad	<b>HA: activo/activo; activo/pasivo</b>

	Control P2P e IM	-----	-----
	-----	Seguridad VoIP	H.323, SIP
	-----	Encapsulación: FR/HDLC	Encapsulación: FR/HDLC/PPP/L2TP/A T M
	IPv6	IPv6	IPv6

Tomado de (Alulema, 2008)

Después de lo mostrado sobre las características que ofrece cada una de las soluciones de seguridad, se puede seleccionar la tecnología **Fortinet** como la más apropiada al momento de referirnos a UTM.

La tecnología Fortinet permite frustrar ataques combinados, gracias a una variedad de funcionalidades y aplicaciones de seguridad, que permiten que sea un sistema de hardware de alto rendimiento.

La tecnología Juniper no están enfocados en sistemas UTM sino en productos aislados para seguridad en redes, por esta razón fueron tomados en cuenta para este proyecto.

Cisco es una tecnología más enfocada a conectividad que una opción de seguridad, pero para cubrir temas de seguridad esta tecnología incorpora en sus equipos servicios enfocados a la seguridad de redes.

De acuerdo al liderazgo de mercado y desarrollo de tecnología en el ámbito de UTM la International Data Corporation ubica en posición estelar a la tecnología Fortinet seguida de Juniper y finalmente Cisco.

### 3.1.6.10.3. Análisis de costos

A continuación se presenta la tabla 15 el análisis de costos de los sistemas UTM tanto en el ámbito de hardware, software, licencias, redundancias, capacitación.

La información de costos se obtuvo de los sitios web de cada proveedor, por lo cual los costos detallados a continuación no constan con costos adicionales de envío e impuestos de aduana.

Tabla 15. Costos comparativos de las soluciones presentadas.

SOLUCION DE SEGURIDAD			
ELEMENTO	<i>FORTINET</i>	<i>JUNIPER</i>	<i>CISCO</i>
Hardware y Software	\$11,996	\$10,600	\$37,456
Servicio y Soporte	\$3,350	\$12,350	\$6,789
Redundancia	\$11,998	\$10,555	\$37,457
Capacitación	\$4,414	\$3,025	\$3,897
<b>TOTAL</b>	<b>\$32,111</b>	<b>\$36,400</b>	<b>\$84,987</b>
<b>TOTAL CRÍTICO</b>	<b>\$19,987</b>	<b>\$25,980</b>	<b>\$47,798</b>

### 3.1.6.11. Ataques de red

- La información transmitida en la red deberá encontrarse encriptada.
- La red requiere de una herramienta de monitoreo para evita ataques.
- Para disminuir riesgos de sniffing se deberá presentar una red segmentada.
- Para disminuir ataques en archivos de contraseñas y datos se requiere encriptar en un solo sentido "one way".

### 3.1.7. Seguridad de las aplicaciones

#### 3.1.7.1. Software

- Cualquier software de aplicación que sea instalado en la cooperativa debe tener su licencia para evitar sanciones por las instituciones de control.
- En los equipos de cómputo si el usuario necesita instalar software libre debe comunicar previamente al departamento de sistema este proceso.
- Cada área de la cooperativa tendrá un responsables del manejo de

información en dicha área.

### **3.1.7.2. Control de aplicaciones en las computadoras**

- Se desarrollará un manual de instalación y configuración de aplicaciones según el perfil del usuario que requiera el aplicativo.
- Para realizar cambios de configuración en los servidores se necesita un respaldo de configuración existente.
- El proceso de mantenimiento de equipos deberá ser documentado para conocer lo que se realizó en dicho proceso.
- En el momento que se entreguen las credenciales de uso de servicios de red por usuarios nuevos, se debe comunicar que está prohibido la instalación de software libre sin previa autorización.

### **3.1.7.3. Control de datos en las aplicaciones**

Solo el administrador del sistema tendrá acceso al software de aplicación para su instalación, dichos archivos se encontraran en una carpeta de almacenamiento con sus respectivos controles de acceso.

El software de aplicaciones realizado por terceros deberá ser entregado a la cooperativa tomando en cuenta la entrega de:

- El ejecutable de la aplicación.
- Traspaso del código fuente del software de aplicación.
- Entrega de documentación tanto del desarrollo como el uso de la aplicación.

### **3.1.8. Seguridad Física**

Los equipos físicos como lógicos que conforman la infraestructura tecnológica de la cooperativa deben ejecutar su funcionamiento en ambiente seguro.

- La configuración tanto de hardware como de software debe realizarse según las configuraciones establecidas por el departamento de sistemas.
- En las estaciones de trabajo es prohibidos el consumo de alimentos y bebidas.
- Los equipos deben ser protegidos contra riesgos establecidos por medioambiente.
- El traslado o reubicación de equipos se lo realizará mediante autorización del encargado del área de sistemas.
- La pérdida de equipos de infraestructura deberá comunicarse inmediatamente después de haber ocurrido dicha pérdida.
- Los inconvenientes en la red deberán comunicarse inmediatamente después de haber ocurrido dicha pérdida.

#### **3.1.8.1. Control de acceso físico al Data Center**

- El acceso al Data Center donde se encuentra equipamiento crítico solo debe tener acceso los administradores.
- Para configuraciones de equipos en el Data Center por personal ajeno a la cooperativa, se designara un escolta que acompañe durante todo el cambio realizado en los equipos hasta su culminación.
- Debe registrarse el ingreso al Data Center mediante una bitácora.

#### **3.1.8.2. Control de acceso a equipos**

El administrador debe realizar mantenimientos periódicos en las estaciones de trabajo para comprobar:

- La ubicación correcta de los equipos.

- Comprobar el correcto funcionamiento del equipo asignado.
- Los números de serie deberán ser los mismos del equipo al momento de su entrega.

#### **3.1.8.3. Equipos portátiles**

- Los equipos portátiles dentro de la cooperativa deben disponer de un cable de seguridad para su anclaje al sitio de trabajo.
- Los equipos portátiles fuera de la cooperativa requieren de todo el tiempo de custodio por parte de su encargado.

#### **3.1.8.4. Cableado estructurado**

- Se requiere los planos de tendido de cable de red.
- Se controlara el ancho de banda de la red periódicamente.
- Los equipos del Data Center cuando existan cortes de energía eléctrica pasaran a trabajar con energía regulada.

#### **3.1.9. Administración del centro de cómputo**

- El departamento de sistemas debe realizar una concientización a nivel de usuarios de las medidas de seguridad.
- La solicitud de soporte técnico por medio de usuarios al departamento de sistemas se realizará mediante mails.
- Se establecerá el procedimiento de políticas y normas de seguridad.
- Si existen suspensiones en el servicio por mantenimiento el administrador de sistema tiene que notificar a los encargados de cada área.
- Deberá existir un inventario de los equipos de cómputo que utiliza la cooperativa.

##### **3.1.9.1. Dispositivos de soporte**

El Data Center de la cooperativa deberá tener equipos de soporte:

- La temperatura óptima en el Data Center es de 19°C a 23°C, para mantener esta temperatura se requiere de aire acondicionado.
- Deberá existir extintores contra incendios con características especiales para equipos electrónicos de computación.
- Alarma contra intrusos, la cual estará constituida por un sistema electrónico que emitirá mensajes vía mails sobre el ingreso de usuarios al Data Center.
- Deberá existir UPS que permitan proporcionar el tiempo suficiente de funcionamiento para que entre a funcionar el generador.
- Deberá existir una luz de emergencia la cual se activara automáticamente en contingencias

#### **3.1.9.2. Capacitación**

La cooperativa debe asegurar que sus empleados reciban capacitación continua para desarrollar una conciencia de seguridad informática que optimice el desempeño eficaz.

#### **3.1.9.3. Respaldos**

Para realizar copias de respaldo de información se requiere procedimientos aprobados.

- Los backup deben poseer control de acceso lógico dependiendo del contenido de sus datos
- Previa la configuración de servidores debe existir respaldos de la configuración.
- Deberá existir un procedimiento para reversar el proceso fallido en configuraciones de servidores.
- Deberá existir una copia de respaldo de los equipos que conforman el Data Center.

#### **3.1.9.4. Documentación**

- Deberán existir documentación de procesos en el Data Center que se desarrollan diariamente.
- Deberán existir documentación sobre políticas, normas y procedimientos de procesos en el Data Center.
- Se asignará un responsable de la gestión de documentación del Data Center.

#### **3.1.10. Seguridad física y del entorno**

La seguridad física protege los recursos de la cooperativa, conteniendo personal y hardware. La productividad se fortalecerá gracias al ambiente seguro permitiendo al empleado enfocarse a sus tareas.

##### **3.1.10.1. Perímetro de Seguridad**

La seguridad perimetral está desplegada en la red de datos que se encuentra en todo el edificio por esta razón es de suma importancia el resguardo de la misma contra personas malintencionadas que ocasionarían daños en las comunicaciones.

##### **3.1.10.2. Controles Físicos de Entradas**

Se requiere poseer controles de acceso físico en la cooperativa para proteger los activos, estos deben:

- En una bitácora se debe registrar las visitas de personas ajenas a la institución en áreas protegidas.
- Se requiere señalización visible de acceso restringido para áreas protegidas.



### 3.1.10.3. Seguridad de oficinas, despachos y recursos

En la tabla 16 se especifican las áreas restringidas de la cooperativa, debido a la información que manipulan dichas áreas.

Tabla 16. Áreas restringidas

ÁREAS PROTEGIDAS
Departamento de Contabilidad
Departamento de Sistemas
Cajas

Para las áreas protegidas se delimitan las siguientes medidas de protección:

- a. Se requiere localizar las instalaciones críticas en sitios en los cuales no pueda ingresar personal no autorizado.
- b. Ubicar el equipo de escritorio como impresoras, scanner en áreas no protegidas
- c. Cuando no exista vigilancia las ventanas y puertas de la cooperativa deben estar cerradas.
- d. Almacenar los Back up en sitios seguros tomando en cuenta que no sea en el sitio de procesamiento.

### 3.1.10.4. Desarrollo de tareas en áreas protegidas

En áreas protegidas también se debe tomar en cuenta los siguientes controles:

- a. Se requiere la difusión al personal de la existencia de áreas protegidas, solo si necesita para el desarrollo de sus actividades laborales.
- b. Obviar el cumplimiento de trabajos de terceros sin supervisión del personal a cargo del área restringida como para la ejecución de trabajos de limpieza.
- c. Dentro de las instalaciones del procesamiento de información es prohibido el consumo de alimentos o bebidas.

### 3.1.10.5. Suministros de energía

Los equipos estarán protegidos de acuerdo a las especificaciones del fabricante en el ámbito de suministro de energía eléctrica. Para certificar la continuidad del suministro de energía, se cumplirá las siguientes medidas de control:

- a. Se requiere tener un generador de energía en casos de cortes eléctricos para no interrumpir las actividades.
- b. Es fundamental el mantenimiento preventivo tanto de las instalaciones eléctricas como del generador para impedir incidentes.

### 3.1.10.6. Mantenimiento de equipos

Para asegurar la disponibilidad del funcionamiento del equipamiento de debe considerar:

- Se debe realizar un cronograma de mantenimientos de los equipos de TI por parte del responsable del departamento de sistemas.
- Solo personal autorizado deberá realizar el mantenimiento o reparación del equipamiento.
- Documentar los mantenimientos preventivos y correctivos realizados en el equipamiento.

En la tabla 17 se indica el período aconsejable para la realización de mantenimientos en los equipos que interactúan en la red.

Tabla 17. Periodo de mantenimiento de equipamiento

<b>EQUIPO</b>	<b>FRECUENCIA DE MANTENIMIENTO</b>	<b>PERSONAL AUTORIZADO</b>
<b>Servidores</b>	4 meses	Administrador
<b>Estaciones de Trabajo</b>	6 meses	Administrador
<b>Impresoras</b>	6 meses	Administrador
<b>Central telefónica</b>	12 meses	Administrador

### **3.1.11. Protección contra software malicioso**

#### **3.1.11.1. Controles contra software malicioso**

Deberán ser consideradas las siguientes acciones:

- a. Impedir el uso de software no autorizado por el departamento de sistemas.
- b. Instalar actualizaciones de software ESET contra detección de virus para la cooperativa.
- c. Establecer las últimas actualizaciones de seguridad en el sistema.
- d. En los equipos de procesamiento de procesos críticos de debe revisar periódicamente el software que permite la ejecución de dichos procesos.
- e. Realizar la verificación de la presencia de virus en archivos electrónicos antes de su utilización.

### **3.1.12. Gestión interna de respaldo**

#### **3.1.12.1. Recuperación de la Información**

Los módulos que conforman el sistema de información COBIS, se encuentran proporcionados por su propia base de datos las cuales se encuentran en un motor de bases denominado SYSBASE. Al final de la jornada laboral se realiza el respaldo de dichas bases.

### **3.1.13. Gestión de la seguridad de red**

#### **3.1.13.1. Controles de Red**

Para garantizar la seguridad de los datos contra acceso de personal no autorizado el responsable de la seguridad informática ejecutara las siguientes acciones:

- a. Ejecución de controles específicos con el fin de mantener la disponibilidad de los servicios de red y equipos conectados a ella.
- b. Revisión de la infraestructura de procesamiento de información.

### **3.1.13.2. Mensajería electrónica**

Para la utilización del correo electrónico en el dominio de la cooperativa se debe seguir las siguientes normativas:

- Para cada empleado de la cooperativa se asociara un correo electrónico.
- La configuración de las cuentas de correo electrónico en el computador del usuario que lo requiera estarán a cargo del departamento de sistemas.
- Se envía una solicitud por medio del departamento de talento humano haciendo el pedido y la activación del correo solicitado por el usuario.
- El encargado del departamento de sistema deberá entregar un acta de entrega y recepción de correo electrónico asignado, de igual forma tendrá que constar en el acta la aceptación de responsabilidad del uso del mismo.
- En caso de renuncias o despido de empleados se debe desactivar el correo con comunicado del departamento de talento humano.

### **3.1.13.3. Uso del Correo Electrónico Corporativo**

El buen uso del correo electrónico es responsabilidad del usuario asignado:

- El usuario deberá leer diariamente su correo y borrar los mensajes obsoletos.
- Deberá mantener el buzón de entrada de su correo con espacio suficiente.
- Para relacionarse con los usuarios del dominio de correo deberá mantener un cordial lenguaje.
- Cada usuario tiene la responsabilidad de no permitir el uso de su correo

por segundas personas.

- El usuario es responsable de realizar respaldos de su correo en su equipo de trabajo.

#### **3.1.13.4. Restricciones**

El usuario con una cuenta de correo electrónico de la Institución se compromete a NO usar este servicio:

- Con fines políticos, particulares, comerciales laboral o de investigación para la Institución, o cualquier otro.
- Para enviar correo basura (SPAMS) o enviar anexos (archivos adjuntos) que pudiera contener información perjudicial para otro usuario.
- Para enviar o recibir contenido no legal, amenazas, abusos, tortuoso, vulgar, difamatorio, calumnioso, obsceno, que violente contra el derecho a la intimidad, étnico, racial o de cualquier otra forma ofensiva.
- Para enviar o recibir anuncios no requeridos o no autorizados promociones, correo de solicitud ("junkmail", "spam"), cartas en cadena ("chain letters), esquemas de pirámides ("pyramid schemes") o cualquier otra solicitud.
- Para esparcir virus, gusanos, caballos de troya y otros programas que puedan dañar los sistemas de proceso de la información de la CMS.
- Para congestionar sistemas informáticos o enlaces de comunicaciones por medio de la transferencia o ejecución de programas o archivos que no forman parte de la Institución.
- Para cualquier forma de manipulación o falsificación de encabezados de identificadores para desviar algún contenido transmitido por medio del Servicio.
- Para enviar o recibir por correo electrónico contenidos que no pueden transmitir por ley o por relación fiduciaria o contractual (como información interna, de propiedad privada adquirida o entregada como parte de las relaciones de empleo o bajo Reglamentos de confidencialidad).

### **3.1.14. Utilización de los servicios de red**

Se controlará el acceso a los servicios de red tanto internos como externos pues las conexiones pueden afectar a la seguridad de la cooperativa. Esto es preciso para garantizar el acceso del usuario a sus servicios y a las redes, y no expongan la seguridad de los mismos.

El administrador de la red otorga permisos a servicios como recursos de la red, solamente de acuerdo al pedido formal del responsable de cada unidad.

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

Por lo tanto se desarrollarán métodos para la activación y desactivación de derechos de acceso a las redes, los cuales deben comprender:

- a. Identificación de redes y servicios de red a los cuales se permite el acceso.
- b. Realización de normas y procedimientos de autorización, determinación de personas, redes y servicios de red de acceso.

Se implementó para este control el procedimiento de asignación de privilegios.

### **3.1.15. Configuración de acceso por defecto**

Todos los usuarios por defecto se configuraran sin privilegios de instalación de programas para asegurar que el administrador pueda asignar los privilegios según el perfil del usuario.

### **3.1.16. Monitoreo de control de acceso**

Para realizar un control de la red se instalara un firewall, el cual se encontrará a cargo de la administradora del centro de cómputo Ing. Daniela Sánchez, el

dispositivo permitirá identificar vulnerabilidades en la red.

### **3.1.17. Restricción del cambio de paquetes de software**

Para evitar que los usuarios realicen cambios en los paquetes de software, sus cuentas en el dominio se encuentran deshabilitados para realizar estas actividades.

### **3.1.18. Gestión de continuidad del negocio**

#### **3.1.18.1. Aspectos de la gestión de continuidad del negocio**

El plan de continuidad del negocio de la cooperativa se desarrolla considerando los parámetros sobre los cuales se va a desarrollar el mismo, para poder evitar desastres.

#### **3.1.18.2. Proceso de gestión de la continuidad del negocio**

Los responsables de cada área deben mantener respaldos continuos de procesos críticos en su área. Se debe considerar como mínimo:

- Se requiere implementar un plan de contingencia, el cual será fácil de entender por los miembros del área.
- Se requiere identificar los riesgos que afectaran al área.
- Documentar el impacto de pérdidas del funcionamiento.

## 4. CAPITULO IV. IMPLEMENTACIÓN DE LA SOLUCIÓN

### 4.1 Instalación de equipo UTM

Se instaló un equipo FortiGate 500D en Matriz que funciona en modo NAT (Ver figura 18) y proporciona un sistema de gestión unificado de amenazas con las siguientes funcionalidades: Firewall, VPN, Prevención de intrusos (IPS), Antivirus, Antimalware, Control de Aplicación y Filtrado de contenidos web para identificar numerosos tipos de amenazas en un único dispositivo. Se agregó un sistema de administración FortiManager 200D encargado de proporcionar una administración centralizada de los firewall y de brindar los reportes de la navegación y seguridad de manera automatizada. En las agencias 60D en las agencias.

El direccionamiento de la red presentado en este capítulo no corresponde al original por reserva de la cooperativa.

El switch de WAN se ha virtualizado en 6 vlans distintas (Ver tabla 18):

Tabla 18. Vlans

<b>VLAN</b>	<b>PROVEEDOR</b>
<b>10</b>	WAN_Panchonet
<b>20</b>	WAN_Cables&Wire
<b>30</b>	WAN_Telconet
<b>40</b>	Banred_Telconet
<b>50</b>	AsistCooper-C&W
<b>60</b>	WAN-Claro



La distribución de los puertos es como sigue tabla 19:

Tabla 19. Distribución de puertos

<b>PUERTOS</b>	<b>VLANS</b>
<b>Puerto 1</b>	Vlan 10
<b>Puerto 2</b>	Vlan 10
<b>Puerto 3</b>	Vlan 20
<b>Puerto 4</b>	Vlan 20
<b>Puerto 5</b>	Vlan 30
<b>Puerto 6</b>	Vlan 30
<b>Puerto 7</b>	Vlan 40
<b>Puerto 8</b>	Vlan 40
<b>Puerto 9</b>	Vlan 50
<b>Puerto 10</b>	Vlan 50
<b>Puerto 11</b>	Troncal al FortiGate
<b>Puerto 12</b>	Troncal al FortiGate
<b>Puerto 13</b>	Vlan 60
<b>Puerto 14</b>	Vlan 60

En la siguiente figura 15 se presenta la conexión física del Fortigate 500D en el rack de Telecomunicaciones con el switch de core y los diferentes equipos de proveedores que permiten el funcionamiento de la red.

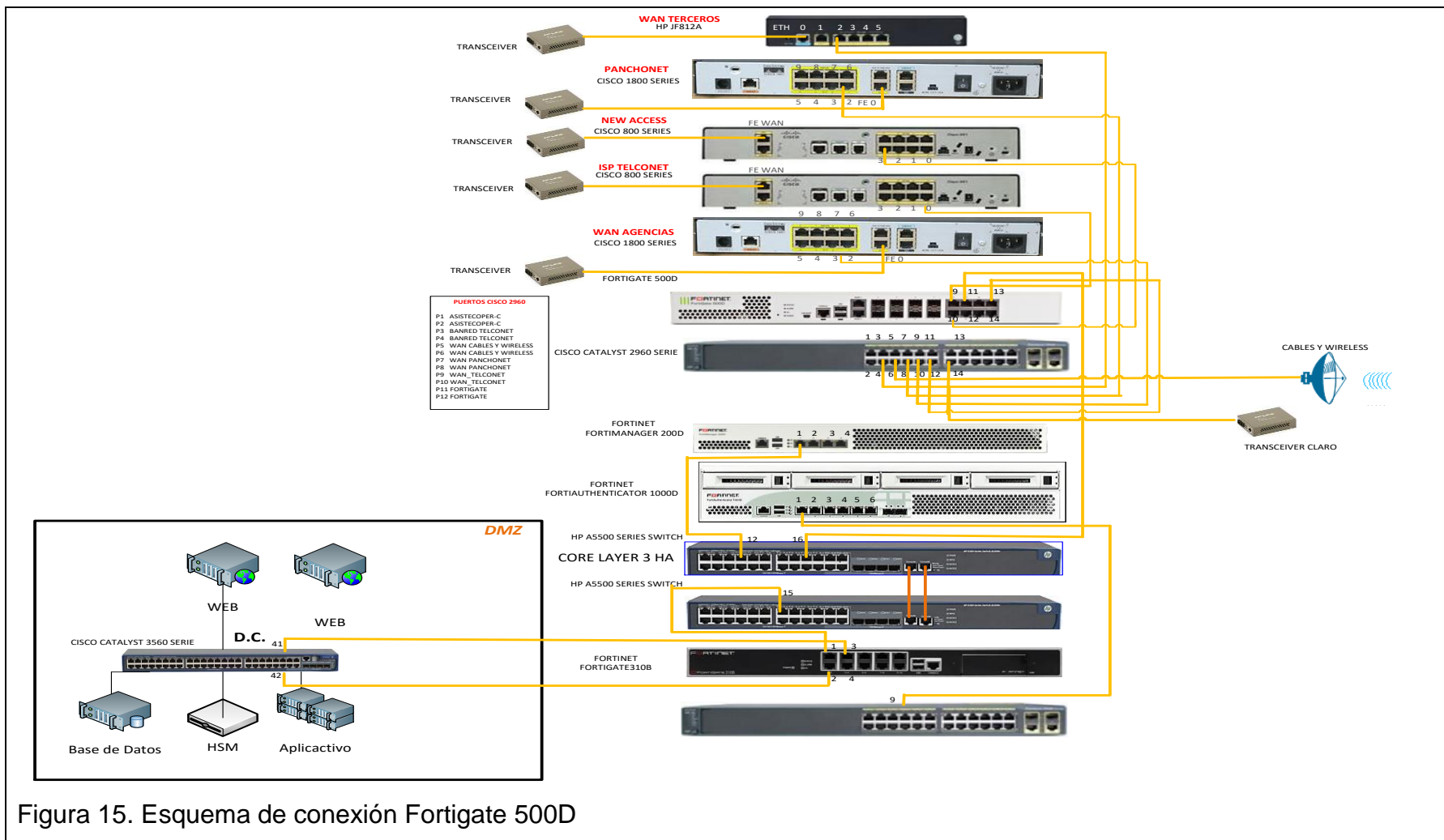


Figura 15. Esquema de conexión Fortigate 500D

## 4.2 Configuración de las interfaces de red

El equipo FortiGate 500D consta de 16 puertos de los cuales actualmente se encuentra conectados 4 puertos (P09, P10, P11 y P13), como se describe en la tabla 20.

Tabla 20. Descripción de Puertos

PUERTO	DESCRIPCIÓN DEL ACCESO
<b>Puerto 09</b>	<b>Internet Telconet - Principal</b>
<b>Puerto 10</b>	<b>Internet New Access – Back-up</b>
<b>Puerto 11</b>	<b>Red Interna</b>
<b>Puerto 13</b>	<b>Red WAN</b>

### 4.2.1 Interfaz de Acceso principal a Internet mediante Telconet

En la figura 16 se visualiza la configuración del puerto 09 correspondiente al acceso a INTERNET mediante el proveedor Telconet, donde se configura la IP pública con su respectiva máscara de red asignada por el proveedor (186.3.119.130/29), adicional la interfaz permite la administración de acceso al equipo mediante varios medios, en este caso se ha seleccionado HTTPS, PING. EL enlace de Telconet es el enlace principal para el acceso al internet para la Matriz así como para también para las Agencias.

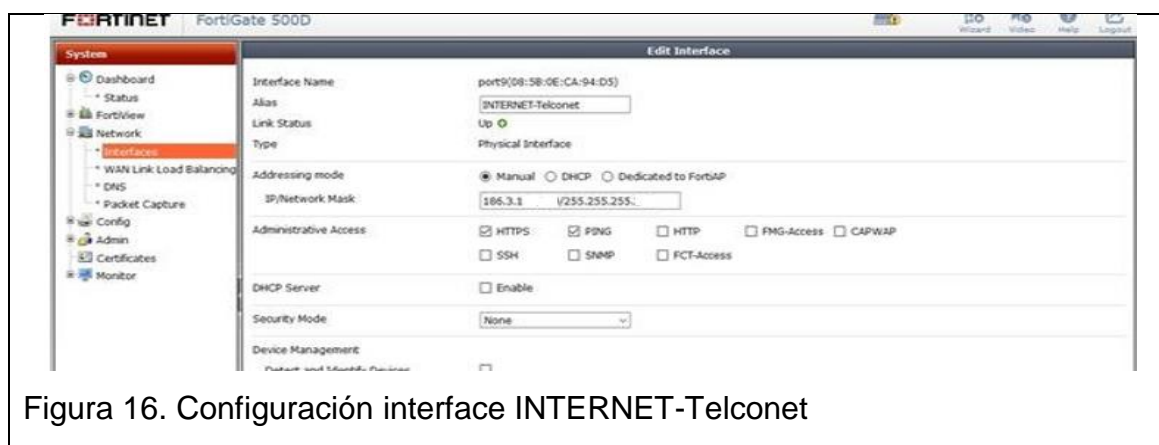


Figura 16. Configuración interface INTERNET-Telconet

## 4.2.2 Interfaz de Acceso principal a Internet mediante New Access

En la figura 17 se visualiza la configuración del puerto 10 correspondiente al enlace de back-up, donde se asigna una IP pública con la respectiva máscara de red (190.108.68.2/16) asignada por proveedor de internet New Access, también se configura los accesos para la administración del equipo FortiGate mediante HTTPS y PING.

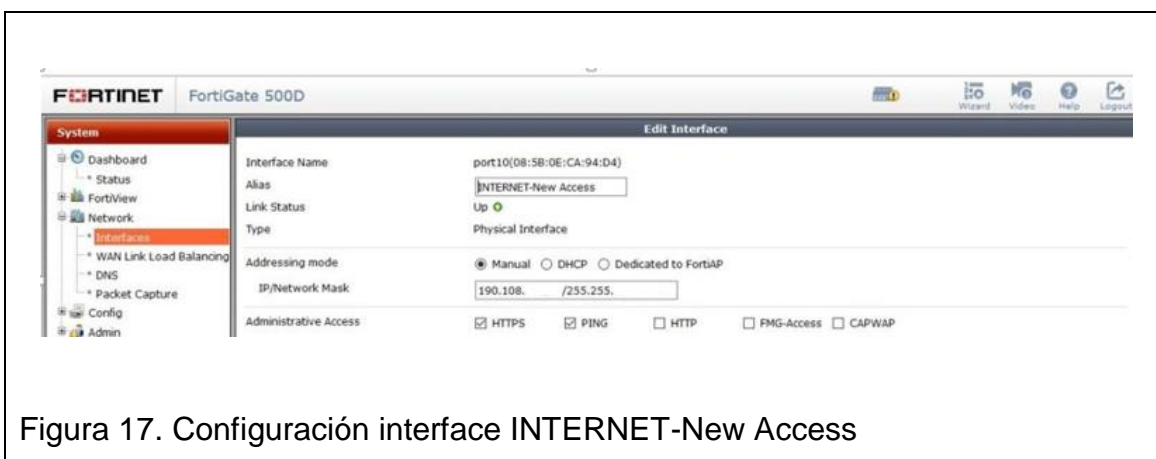


Figura 17. Configuración interface INTERNET-New Access

## 4.3. Interfaz de Acceso WAN

La configuración del interfaz de acceso Wan se lo realizo en el puerto 13, en esta interfaz se encuentran configuradas VLANs para los diferentes acceso de servicios de la cooperativa, mismo que se conecta al switch de capa 2, entre los accesos se tiene el acceso de AsistCoopper por el enlace del proveedor de C&W, acceso a Banred mediante Telconet, Acceso a los servicios mediante en proveedor CLARO y los accesos de datos mediante Cables & Wireless (C&W). El acceso WAN de datos de Cables y Wireless es un enlace de back-up donde se crean accesos de VPN hacia las 9 agencias (Tumbaco, Sangolqui, Machachi, Inca, Guamani, Conocoto, Colon, Chillogallo y Amaguaña) el cual permite tener el acceso al internet y a los diferentes servicios de la cooperativa.

Entre otros servicios que se configura en la interfaz se encuentra los servicios del proveedor Panchonet, también se configura la VLAN para el acceso de

datos mediante el proveedor Telconet, que es el enlace principal para todas las agencias, en el cual se crean VPN para el acceso al internet y el acceso hacia los servicios de la cooperativa, como se muestra en la figura 18. La administración de las VLAN se configura solamente la opción de ping.



Figura 18. VPN creadas en la interfaz WAN

#### 4.3.1. AsisteCooper C&W (vlan 50)

Se configura la interface AsisteCooper C&W asociada a la vlan 50 por el port13 (Ver figura 19), el mismo que se conecta hacia el puerto 1 del switch cisco 2960 y permite el acceso del proveedor AsisteCooper la realización de pruebas en producción.

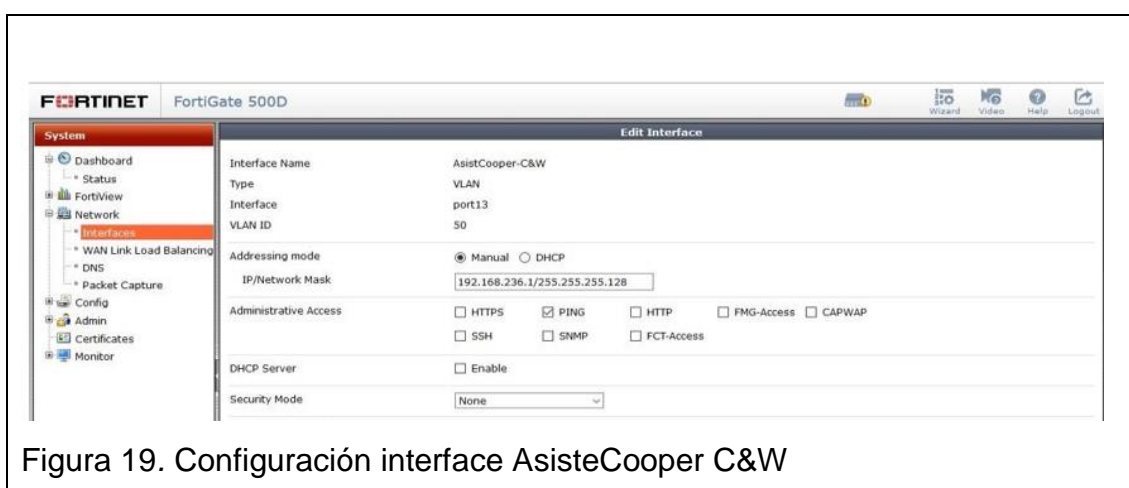


Figura 19. Configuración interface AsisteCooper C&W

### 4.3.2. Banred Telconet (vlan 40)

Se configura la interface Banred\_Telconet asociada a la vlan 40 por el port13 (Ver figura 20), el mismo que se conecta hacia el puerto 12 del switch cisco 2960 y permite el acceso hacia los cajeros de banred de cada una de las agencias. Para la administración a la red de la VLAN se ha configurado solo la opción de ping.

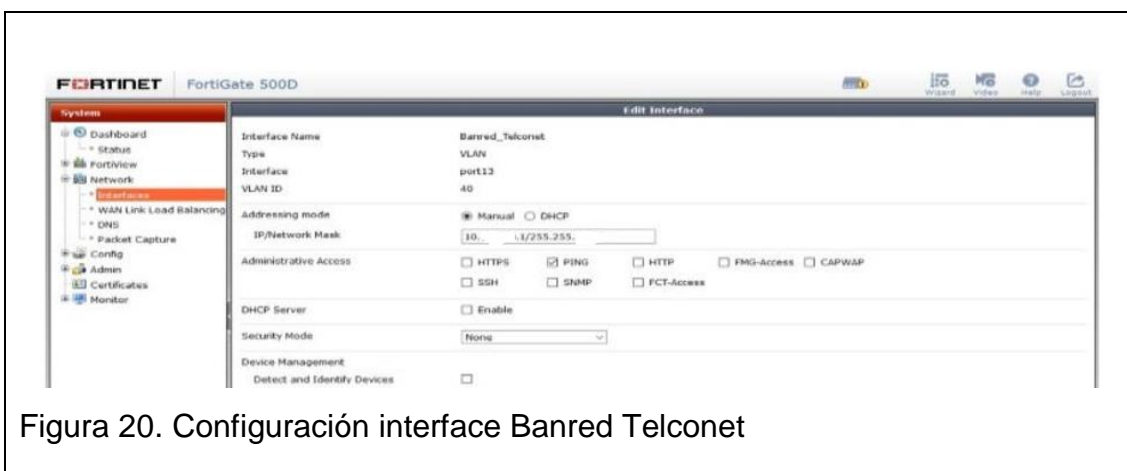


Figura 20. Configuración interface Banred Telconet

### 4.3.3. Wan-Claro (vlan 60)

Se configura la interface Wan-Claro asociada a la vlan 60 por el port13 (Ver figura 21), esta interfaz es un acceso para el funcionamiento del servidor M2M (machine to machine) el cual se utiliza en equipos tablet.



Figura 21. Configuración interface Wan-Claro

#### 4.3.4. Wan-Cables&Wireless (vlan20)

Se configura la interface Wan-Cables&Wireless asociada a la vlan 20 por el port13 (Ver figura 22), esta interfaz es un acceso hacia el enlace back-up de datos del proveedor Cables & Wireless en el cual se crean VPN desde la matriz hacia todas las agencias para el acceso al internet y hacia los diferentes servicios de la cooperativa. Para el acceso de la administración de la red de la Vlan 20 se configura la opción de ping.

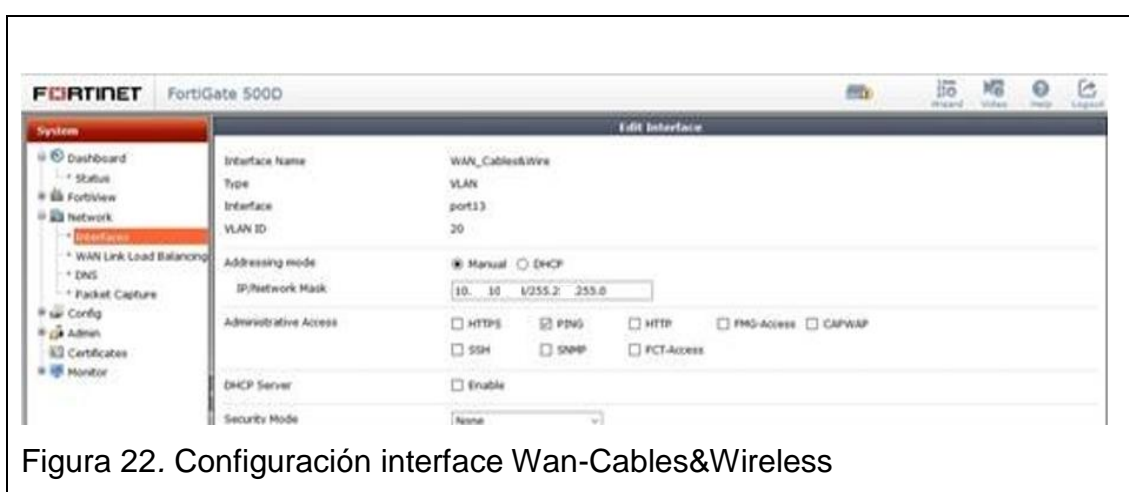


Figura 22. Configuración interface Wan-Cables&Wireless

#### 4.3.5 Wan-Panchonet (vlan10)

Se configura la interface Wan-Panchonet asociada a la vlan 10 por el port13 (Ver figura 23), esta interfaz es un acceso hacia el data center de Panchonet para respaldar datos.

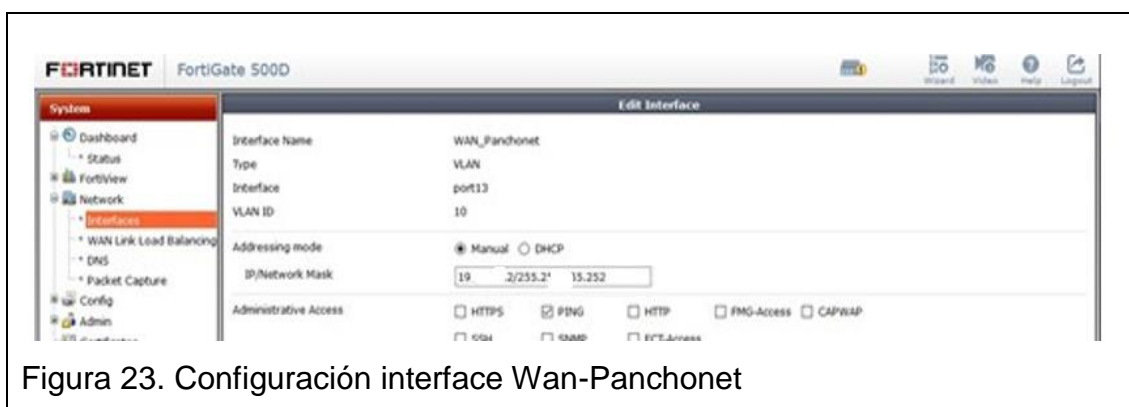


Figura 23. Configuración interface Wan-Panchonet

### 4.3.6 Wan-Telconet (vlan 30)

Se configura la interface Wan-Telconet asociada a la vlan 30 por el port13 (Ver figura 24), esta interfaz es el acceso principal de datos desde la matriz hacia las agencias donde de la misma manera que el acceso por el back –up (C&W) se crea VPN para brindar el acceso al internet así como a los diferentes servicios.

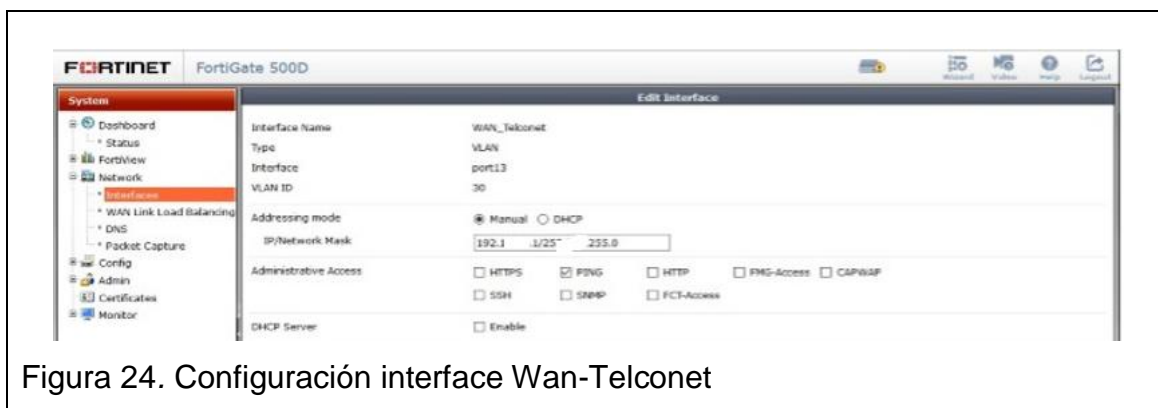


Figura 24. Configuración interface Wan-Telconet

### 4.4. Red Interna

En la figura 25 se visualiza la configuración de la Interface RED-INTERNA asignando una dirección IP privada la misma que se conecta al puerto 16 del switch core de capa 3 (HP A5500 SERIES SWITCH), dentro de esta red se encuentra toda red interna de la matriz de la cooperativa así como también la red DMZ (red de servidores) de los diferentes servicios y aplicaciones de la cooperativa. Para la administración de la interfaz se habilitado los accesos mediante HTTPS, PING y HTTP, el cual también permite la administración del equipo FortiGate.



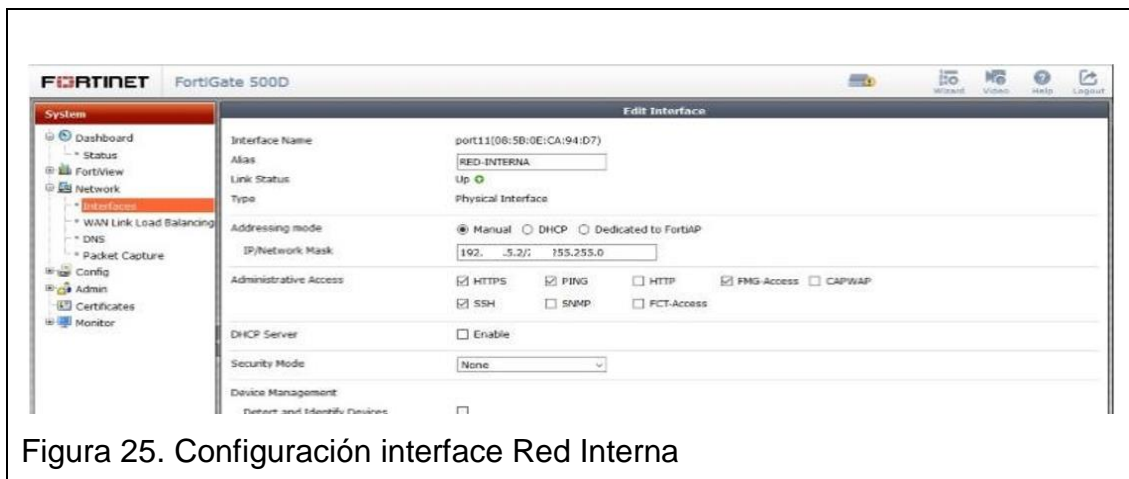


Figura 25. Configuración interface Red Interna

#### 4.4.1. Configuración de rutas

Entre las cuales se encuentra las ruta de acceso al internet mediante el enlace principal Telconet, la ruta de acceso al internet mediante el enlace backup New Access, rutas para el acceso hacia el servicio de banred, ruta de acceso hacia de la wan de telconet hacia cada una de las agencias y rutas de acceso hacia la WAN de Panchonet.

En la figura 26 se muestra las rutas de acceso hacia la VPN de cada una de las agencias (Conocoto, Guamani, Colon, Inca, Amaguaña, Chillogallo, Tumbaco, Machachi y Sangolqui) tanto para el enlace principal (Telconet) como para el enlace back up (C&W) con sus respectivas distancias administrativas de 10 y 20 respectivamente y con prioridades de 0.

IP/Netmask	Gateway	Device	Comment	Distance	Priority
10.50.0.0 255.255.255.0	192.168.5.1	port11	Admin WiFi	10	0
172.17.96.0 255.255.248.0		Conocoto-CBW	VPN Conocoto CBW	20	0
172.17.96.0 255.255.248.0		Conocoto-Telco	VPN Conocoto Telconet	10	0
172.18.1.0 255.255.255.0	192.11.1.1	WAN_Ranchonet		10	0
172.17.72.0 255.255.248.0		Guamani-CBW	VPN Guamani CBW	20	0
172.17.72.0 255.255.248.0		Guamani-Telco	VPN Guamani Telco	10	0
172.17.32.0 255.255.248.0		Chiligall-CBW	VPN Chiligallo CBW	20	0
172.17.32.0 255.255.248.0		Chiligall-Telco	VPN Chiligallo Telco	10	0
172.17.56.0 255.255.248.0		Amaguana-CBW	VPN Amaguana CBW	20	0
172.17.56.0 255.255.248.0		Amaguana-Telco	VPN Amaguana Telco	10	0
172.17.24.0 255.255.248.0		Inca-CBW	VPN Inca CBW	20	0
172.17.24.0 255.255.248.0		Inca-Telco	VPN Inca Telco	10	0
172.17.40.0 255.255.248.0		Sangolqui-CBW	VPN-Sangolqui-CBW	20	0
172.17.40.0 255.255.248.0		Sangolqui-Telco	VPN-Sangolqui-Telco	10	0
172.17.64.0 255.255.248.0		Machachi-CBW	VPN Machachi CBW	20	0
172.17.64.0 255.255.248.0		Machachi-Telco	VPN Machachi Telco	10	0
172.17.80.0 255.255.248.0		Tumbaco-CBW	VPN Tumbaco CBW	20	0
172.17.80.0 255.255.248.0		Tumbaco-Telco	VPN Tumbaco Telco	10	0
172.17.104.0 255.255.255.0		Colon-Telco	VPN Colon-Telco-Datos	10	0
172.17.105.0 255.255.255.0		Colon-Telco	VPN Colon-Telco-Voz	10	0
172.17.106.0 255.255.255.0		Colon-Telco	VPN Colon-Telco-Camaras	20	0
172.17.109.0 255.255.255.0		Colon-Telco	VPN Colon-Telco-Administracion	10	0
172.17.104.0 255.255.255.0		Colon-CBW	VPN Colon-CBW-Datos	20	0
172.17.105.0 255.255.255.0		Colon-CBW	VPN Colon-CBW-Voz	20	0
172.17.106.0 255.255.255.0		Colon-CBW	VPN Colon-CBW-Camaras	10	0
172.17.109.0 255.255.255.0		Colon-CBW	VPN Colon-CBW-Administracion	20	0

Figura 26. Rutas de acceso a las VPN de las agencias

#### 4.4.2. Configuración de Policy Routes

Considerando que la Cooperativa tiene un sistema de grabaciones de las cámaras de video vigilancia de las sucursales en la matriz, se configura políticas de ruteo para que el acceso a las cámaras de cada una de las agencias se lo realice mediante el enlace de datos back-up correspondiente al proveedor de Cables & Wireless, debido al ancho de banda que disponen para garantizar el servicio, ya que el enlace principal está destinado para el acceso al internet y los demás servicios.

#### 4.4.3. Fail-Over de salida a Internet

La cooperativa dispone de 2 salidas a internet, por lo cual, se vuelve necesario que ante una falla del enlace principal (Telconet), el enlace de backup inmediatamente suba el servicio a la cooperativa (New-Access). Esto se logra configurando los Link-Help-Monitor (IP-SLA) en el firewall de la matriz.

#### 4.4.4. Políticas

En el firewall se ha creado 182 políticas, donde para cada una de las agencias se crearon políticas para el acceso al puerto de Banred, para el puerto de acceso al internet New Access (enlace back-up), acceso a la red interna, acceso Telconet (enlace principal), acceso a puerto WAN a donde se conectan los enlaces de datos (Telconet y C&W) y los servicios de Claro, Banred y Asistecoper. Las políticas se crearon para los enlaces de datos principales (Telconet) y back-up (Cables y Wireless) respectivamente como se muestra en la figura 27 y 28.

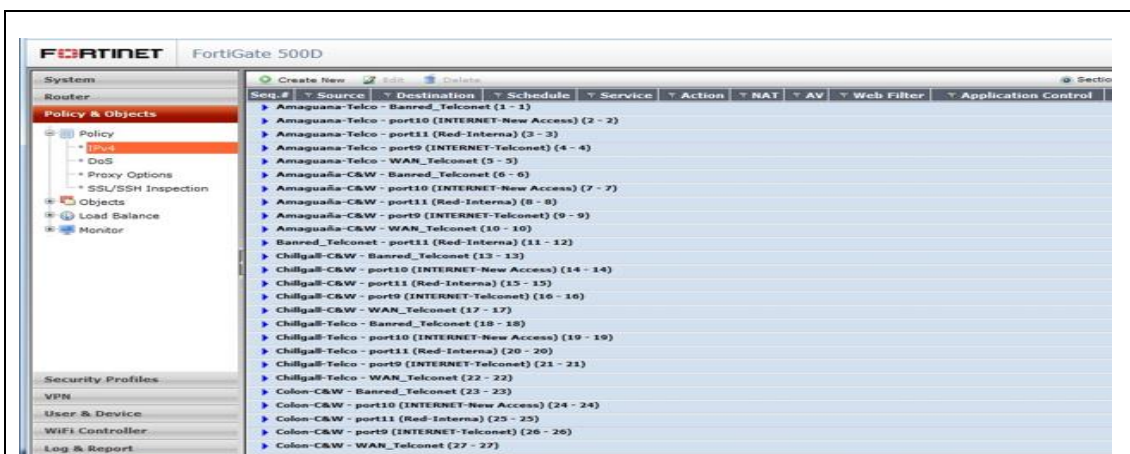


Figura 27. Políticas de acceso a los servicios mediante la VPN



Figura 28. Políticas de acceso a los servicios mediante la VPN

Se ha configurado políticas de acceso desde la red interna hacia la red cada una de las agencias, a los servicios de Banred, AsistCooper y Panchonet. También se crea políticas desde la red interna hacia el acceso al internet por el proveedor principal Telconet y back-up (News Access).

Entre otras políticas configuradas se tiene el acceso de internet Telconet hacia cada una de las agencias y hacia la red interna de la matriz. Adicional se crea la política desde la VPN-SSL hacia la red interna.

Finalmente se crearon políticas del enlace WAN de datos de cables y wireless (C&W), WAN de Panchonet, WAN Telconet y WAN Claro hacia la red interna.

#### **4.4.5. Configuración de Virtual IPs**

Se han configurado Virtual IPs, también conocidas con NAT tanto para las IP públicas de New-Access como para las IP públicas de Telconet, el cual permite tener acceso hacia los servidores (WEB, Mail, Banred ATM, Producción, Transac, Consultas y DNS) desde la red interna por la IP privada y desde una red externa por la IP pública y mediante puertos específicos asignados a cada uno de los servicios.

#### **4.4.6 Política de conexión entrante por Telconet**

Para el acceso hacia los servidores sea desde la red externa se crea políticas dependiendo por la interfaz de salida, en este caso se han creado políticas de acceso desde la red de Internet de Telconet (Port9) hacia la red Interna (Port11). En cada política se han activado los perfiles de antivirus e IPS para proporcionar protección contra intrusiones a estos servicios publicados, adicional se activa el tipo de service (puertos de acceso) hacia los servidores (Ver figura 29):



Figura 29. Política de conexión entrante por Telconet

#### 4.4.7. Política de conexión entrante por New-Access

Con los mismos parámetros configurados para el acceso por el enlace principal se crea las políticas para el acceso por el enlace de back-up (New-Access) (Ver figura 30):



Figura 30. Política de conexión entrante por New-Access

#### **4.4.8. Configuración de IP POOLS**

La configuración de los IP Pools se ha realizado con objeto de proporcionar una conexión con Banred entre los cajeros de la cooperativa y red de Banred para todas las agencias. Esta conexión esta direccionada para siempre salir con una IP proporcionada por el ISP Telconet en conexión con Banred. De esta manera, las conexiones entre los cajeros de cada agencia se hacen siempre con la IP Nateada de salida y sin importar el direccionamiento privado de la cooperativa.

#### **4.4.9. Políticas de DoS (Deny of Service)**

Las políticas de DoS se configuran para prevenir ataques de denegación de servicio sobre el firewall en sí y sobre todas las peticiones de entrada que llegan por la interfaces de acceso a Internet (Telconet y New-Access).

#### **4.4.10. Configuración de puertos para publicación de servicios y accesos entre zonas de firewall**

Los puertos vienen por default creados en los equipos y han sido configurados con el propósito de restringir los accesos en base a puertos, los mismos que son aplicados en las respectivas políticas y de acuerdo restricciones de seguridad requeridas. Entre las categorías de servicios se tiene de web Access, network service, Remoto Access, Email, File Access, General, tunneling Authentication y Uncategorized.

Los puertos específicos a utilizar para el acceso de ciertos servicios se crean en el grupo Uncategorized como se muestra en la siguiente figura 31.

Service Name	Category	Protocol	Port	Ref.
Internet Locator Service	Uncategorized	TCP	399	0
MSCP	Uncategorized	UDP	2427	0
MMS	Uncategorized	TCP	1755	0
NNTP	Uncategorized	UDP	1024-5000	0
NONE	Uncategorized	TCP	0	0
NetMeeting	Uncategorized	TCP	1720	0
QLAKE	Uncategorized	UDP	26000	0
RADIUS-OLD	Uncategorized	UDP	1545	0
RADIO	Uncategorized	UDP	1646	0
REXEC	Uncategorized	TCP	512	0
RLOGIN	Uncategorized	TCP	513	0
RSH	Uncategorized	TCP	514	0
TALK	Uncategorized	UDP	517-518	0
TCP-354	Uncategorized	TCP	354	9
TCP-8000	Uncategorized	TCP	8000	9
TCP_4100-5100-6100-6102	Uncategorized	TCP	4100	2
TCP_4946-4947	Uncategorized	TCP	4946-4947	1
TCP_999	Uncategorized	TCP	999	0
TIMESTAMP	Uncategorized	ICMP	13:ANY	0
UUCP	Uncategorized	TCP	540	0
VDOLIVE	Uncategorized	TCP	7000-7010	0
WAIS	Uncategorized	TCP	210	0
WINFRAME	Uncategorized	TCP	1494	0

Figura 31. Puerto Uncategorized

El uso de estos puertos será desplegado a lo largo del informe en las secciones de políticas de acceso.

#### 4.4.11 Objetos de red (direcciones)

Los siguientes objetos de red se han creado para definir las IPs o subredes a ser filtradas por el firewall en la sección de políticas. Se han configurado en base a las necesidades de la cooperativa, donde se ha creado las IPs correspondientes a los ATMs, servidor biométrico y páginas web. En la figura 32, se muestra las direcciones de IP bloqueadas que corresponde a páginas que se requieren denegar el acceso.

Name	Type	Details	Interface	Visibility	Ref.
FG	Subnet	192.168.5.0/24	Any	✓	0
File-Server	Subnet	192.10.1.7/32	Any	✓	2
GDSystem	FQDN	*gdssystem.com	Any	✓	1
IP Bloqueada 1	Subnet	114.42.0.0/16	Any	✓	1
IP Bloqueada 2	Subnet	183.12.0.0/16	Any	✓	1
IP Bloqueada 3	Subnet	89.174.7.156/32	Any	✓	1
IP Bloqueada 4	Subnet	66.25.67.211/32	Any	✓	1
IP Bloqueada 5	Subnet	91.142.220.51/32	Any	✓	1
IP Bloqueada 6	Subnet	186.71.69.170/32	Any	✓	1
IP Bloqueada 7	Subnet	207.240.10.33/32	Any	✓	1
IP Bloqueada 8	Subnet	64.39.103.191/32	Any	✓	1
IP Bloqueada 9	Subnet	222.74.212.77/32	Any	✓	1
IP Bloqueada 10	Subnet	66.199.253.90/32	Any	✓	1
IP Bloqueada 11	Subnet	222.74.212.77/32	Any	✓	1
IP Bloqueada 12	Subnet	69.174.245.163/32	Any	✓	1
IP Bloqueada 13	Subnet	85.25.140.170/32	Any	✓	1
IP Bloqueada 14	Subnet	80.241.245.194/32	Any	✓	1
IP Bloqueada 15	Subnet	90.21.73.167/32	Any	✓	1
IP Bloqueada 16	Subnet	91.142.209.68/32	Any	✓	1
IP Bloqueada 17	Subnet	82.165.11.172/32	Any	✓	1
IP Bloqueada 18	Subnet	85.17.170.129/32	Any	✓	1
IP Bloqueada 19	Subnet	190.98.1.20/32	Any	✓	1
IP Bloqueada 20	Subnet	198.134.63.131/32	Any	✓	1
IP Bloqueada 21	Subnet	200.29.3.6/32	Any	✓	1
IP Bloqueada 22	Subnet	61.147.103.173/32	Any	✓	1
IP Bloqueada 23	Subnet	209.236.133.201/32	Any	✓	1
IP Bloqueada 24	Subnet	65.10.34.111/32	Any	✓	1
IP Bloqueada 25	Subnet	62.218.224.221/32	Any	✓	1
IP Bloqueada 26	Subnet	65.181.122.102/32	Any	✓	1
IP Bloqueada 27	Subnet	186.3.117.140/32	Any	✓	1

Figura 32. Direcciones de IP Bloqueadas

Entre los objetos también se crearon los respectivos direccionamientos de cada una de las agencias, como se muestra en la figura 33.

Name	Type	Details	Interface	Visibility	Ref.
IP Bloqueada 27	Subnet	186.3.117.140/32	Any	✓	1
IP Bloqueada 28	Subnet	32.78.16.172/32	Any	✓	1
IP Bloqueada 29	Subnet	67.228.95.186/32	Any	✓	1
IPs Bloqueo China	Geography	China	Any	✓	1
IPs Bloqueo Taiwan	Geography	Taiwan	Any	✓	1
IPs-Ecuador	Geography	Ecuador	Any	✓	10
IPs-Rusia	Geography	Russian Federation	Any	✓	1
IPs-Afghanistan	Geography	Afghanistan	Any	✓	1
IPs-India	Geography	India	Any	✓	1
LAN-Amaguana-Actual	Subnet	192.20.50.0/24	Any	✓	1
LAN-Amaguana-Nueva	Subnet	172.17.36.0/21	Any	✓	1
LAN-COLON-VIDEO	Subnet	172.17.106.0/24	Any	✓	1
LAN-Chilloallo-Actual	Subnet	192.168.103.0/24	Any	✓	1
LAN-Chilloallo-Nueva	Subnet	172.17.32.0/21	Any	✓	1
LAN-Colon-Actual	Subnet	192.168.110.0/24	Any	✓	1
LAN-Colon-Nueva	Subnet	172.17.104.0/21	Any	✓	1
LAN-Conocoto-Actual	Subnet	192.168.109.0/24	Any	✓	1
LAN-Conocoto-Nueva	Subnet	172.17.96.0/21	Any	✓	1
LAN-Guamani-Actual	Subnet	192.168.111.0/24	Any	✓	1
LAN-Guamani-Nueva	Subnet	172.17.72.0/21	Any	✓	1
LAN-Inca-Actual	Subnet	192.168.102.0/24	Any	✓	1
LAN-Inca-Nueva	Subnet	172.17.24.0/21	Any	✓	1
LAN-Machachi-Actual	Subnet	192.10.60.0/24	Any	✓	1
LAN-Machachi-Nueva	Subnet	172.17.64.0/21	Any	✓	1
LAN-Matriz-Actual	Subnet	192.10.1.0/24	Any	✓	1
LAN-Sangolqui-Actual	Subnet	192.20.40.0/24	Any	✓	1
LAN-Sangolqui-Nueva	Subnet	172.17.40.0/21	Any	✓	1
LAN-Tumbaco-Actual	Subnet	192.168.112.0/24	Any	✓	1
LAN-Tumbaco-Nueva	Subnet	172.17.80.0/21	Any	✓	1
NTP-INOCAR	FQDN	inocar.ntp.ec	Any	✓	2

Figura 33. Direccionamiento IP de las Agencias

También se ha configurado grupo de direcciones, para este caso se han 13 grupos como son Biometrica, IP Bloqueadas y el grupo LAN para cada uno de las agencias como se muestra en la siguiente figura 34.



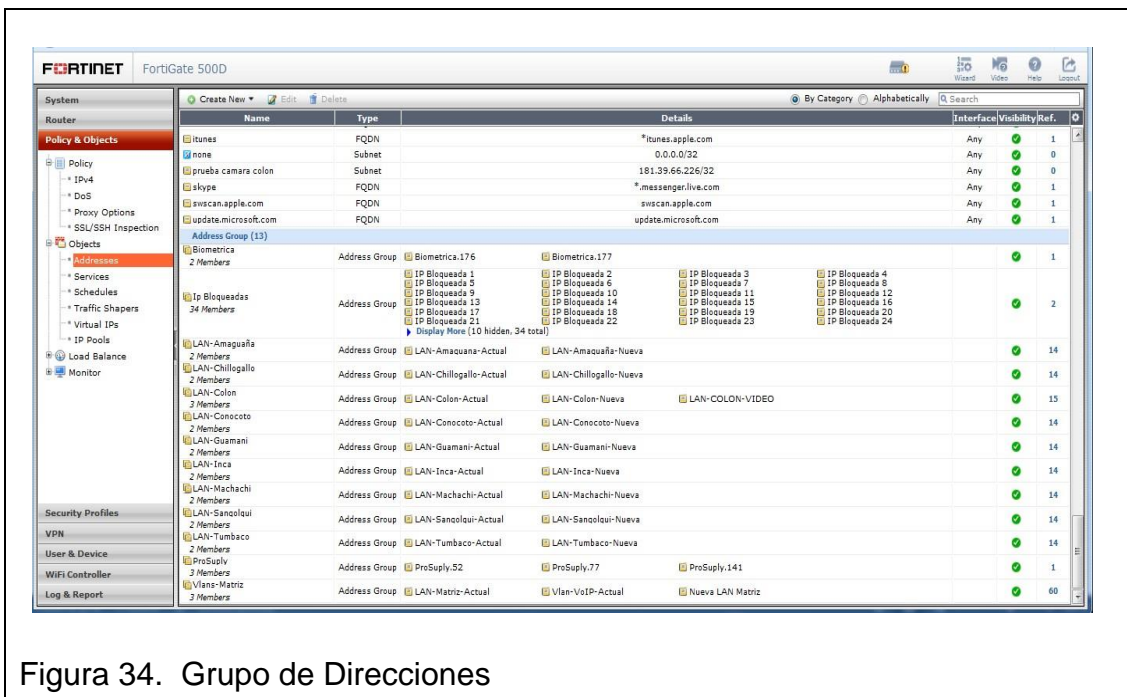


Figura 34. Grupo de Direcciones

## 4.4.12. Configuración de VPNs

### 4.4.12.1. VPN SSL

Se ha configurado la VPN para que se pueda acceder a las Vlans de la matriz (Red interna de la cooperativa) mediante un pool de direcciones ip (SSLVPN\_TUNEL\_ADDR1) entregadas a los usuarios que se conectan a la VPN desde una PC desde cualquier lado del mundo (Ver figura 35).

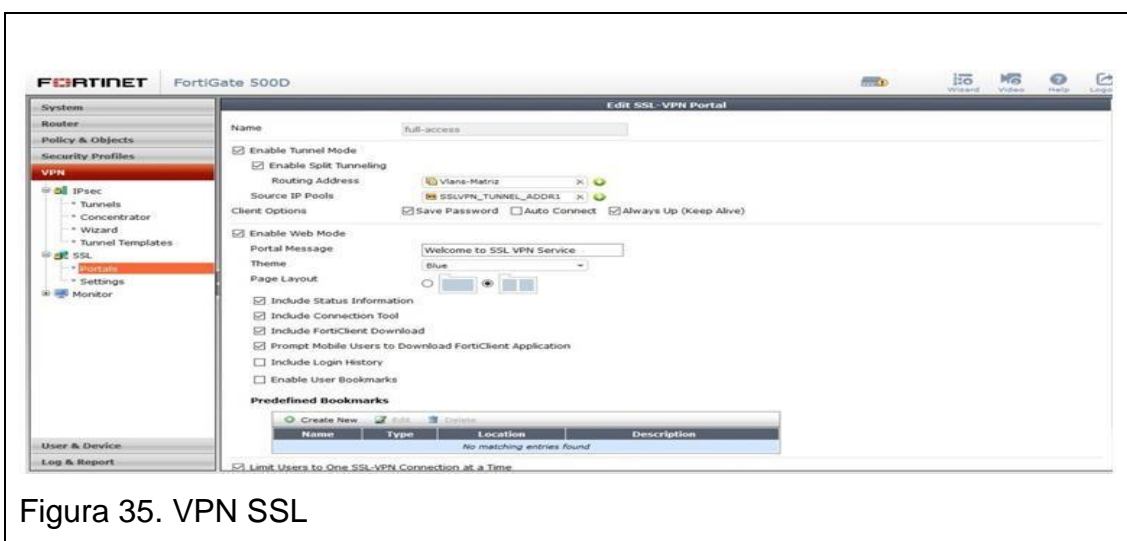


Figura 35. VPN SSL

La conexión a esta VPN se logra mediante la URL: <https://186.4.120.130:10443> y a la misma pueden acceder únicamente los usuarios: biométrica, crativod, ProSupply y VPN-Users de la matriz (Ver figura 36).

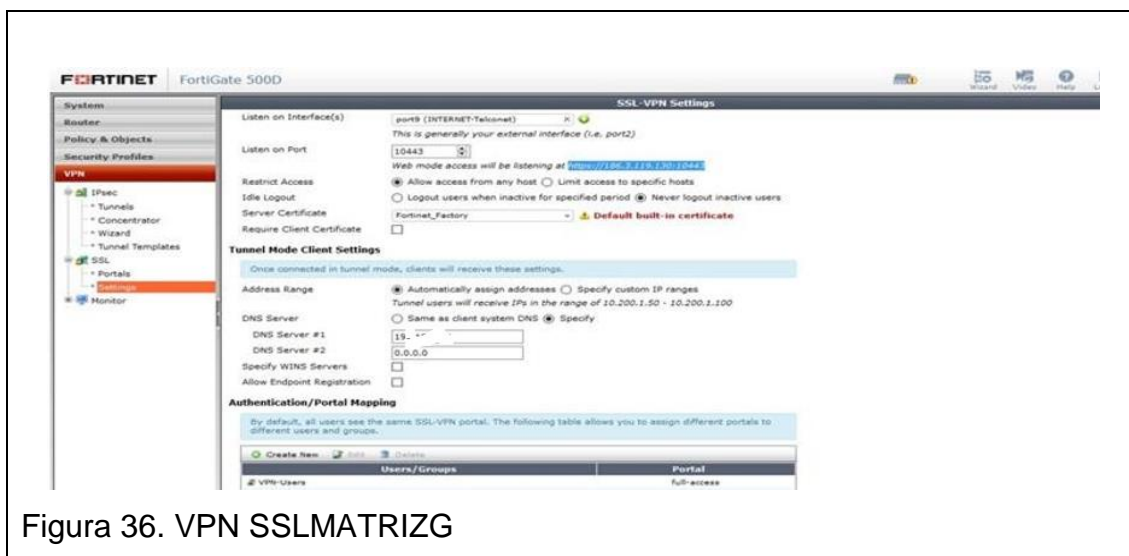


Figura 36. VPN SSLMATRIZG

En función del usuario con que se loguen los usuarios en el VPN, únicamente pueden acceder a los siguientes recursos delimitados en la sección de políticas desde la interfaz ssl.root (SSL VPN Interface) hacia el port11 (Rred-interna) (Ver figura 37):

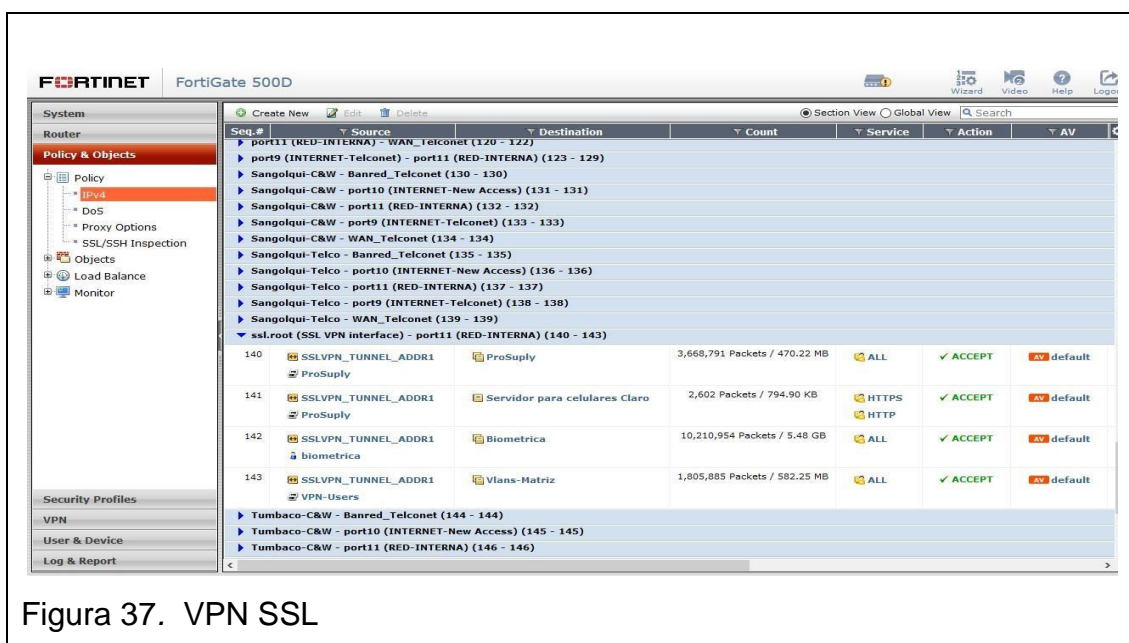
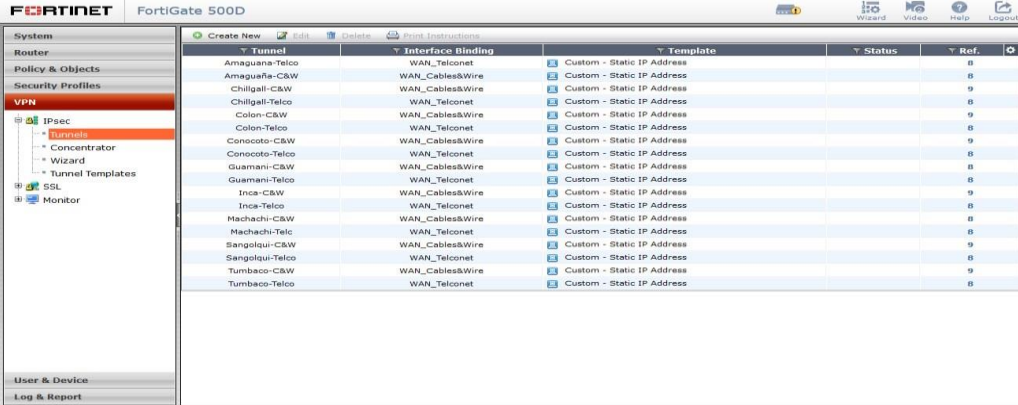


Figura 37. VPN SSL

La definición de cada objeto de red se puede encontrar en la subsección de objetos de red descrita anteriormente.

#### 4.4.12.2. VPN IPsec

Las VPN IPsec es el core de la presente implementación, pues con objeto de lograr un alto nivel de seguridad en los datos compartidos entre las agencias y la sucursal, se ha establecido un túnel ipsec encriptado en cada enlace ya sea del proveedor de datos telconet o mediante el proveedor de cables y Wireless para cada agencia. Es así que en la matriz se han generado los siguientes túneles IPsec. Adicional nos permite el acceso al internet (Ver figura 38):



The screenshot shows the FortiGate 500D configuration interface for VPN IPsec tunnels. The left sidebar shows the navigation menu with 'VPN' selected. The main area displays a table of configured tunnels.

Tunnel	Interface Binding	Template	Status	Ref.
Amaguana-Telco	WAN_Telconet	Custom - Static IP Address		8
Amaguana-C&W	WAN_Cables&Wire	Custom - Static IP Address		8
Chilgali-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Chilgali-Telco	WAN_Telconet	Custom - Static IP Address		8
Colon-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Colon-Telco	WAN_Telconet	Custom - Static IP Address		8
Conocoto-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Conocoto-Telco	WAN_Telconet	Custom - Static IP Address		8
Guamani-C&W	WAN_Cables&Wire	Custom - Static IP Address		8
Guamani-Telco	WAN_Telconet	Custom - Static IP Address		8
Inca-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Inca-Telco	WAN_Telconet	Custom - Static IP Address		8
Machachi-C&W	WAN_Cables&Wire	Custom - Static IP Address		8
Machachi-Telc	WAN_Telconet	Custom - Static IP Address		8
Sangolqui-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Sangolqui-Telco	WAN_Telconet	Custom - Static IP Address		8
Tumbaco-C&W	WAN_Cables&Wire	Custom - Static IP Address		9
Tumbaco-Telco	WAN_Telconet	Custom - Static IP Address		8

Figura 38. VPN IPsec

Cada túnel creado habilita una interfaz virtual que se usa para definir las políticas de acceso; de esta manera, las políticas de acceso definidas para los túneles por telconet son las mismas que para las de cables y wireles con objeto de brindar redundancia a la comunicación. Estos accesos están definidos del siguiente modo:



Figura 39. VPN Amaguaña

#### 4.4.13. Autenticación con Active Directory

La conexión con el Active Directory se realiza para control de navegación de usuarios, se ha instalado el agente colector de datos sobre el servidor de A.D. FSSO; mismo que tiene por objeto llamar los logs del server e identificar los usuarios logeados con sus respectivas IP pertenecientes a determinado grupo. Esto permite realizar un control sobre los usuarios que navegan a través del Fortinet sin depender de una dirección IP estática. La colección de grupos de usuarios se realiza para los siguientes (Ver figura 40):



Figura 40. Autenticación con Active Directory

Por lo que los usuarios a controlar en la navegación serán los que estén dentro de los siguientes grupos (Ver figura 41):



Figura 41. Autenticación con Active Directory

Esto implica que el filtrado de navegación se debe realizar en base a los grupos de usuarios y que cada grupo de usuarios creado debe tener su par en el perfil de navegación web y de control de aplicaciones, esto acorde a lo descrito en la sección zonas para navegación detalladas en secciones anteriores.

#### 4.4.14 Políticas de conexión entre zonas y la red interna de la Matriz

Con objeto de permitir la conectividad entrante desde las redes que se conectan a través de: WAN\_Cables&Wireless, WAN\_Telconet y WAN\_Claro; se han creado políticas de acceso que permiten la entrada de las comunicaciones desde ciertos host a ciertas redes, de tal manera que la configuración es como se detalla para estos 3 proveedores:

Todas estas políticas de acceso se han configurado con un perfil de antivirus que inspecciona los paquetes de entrada y con un perfil de IPS que verifica si las conexiones entrantes no son ataques dirigidos a las redes de destino permitidas (Ver figura 42).

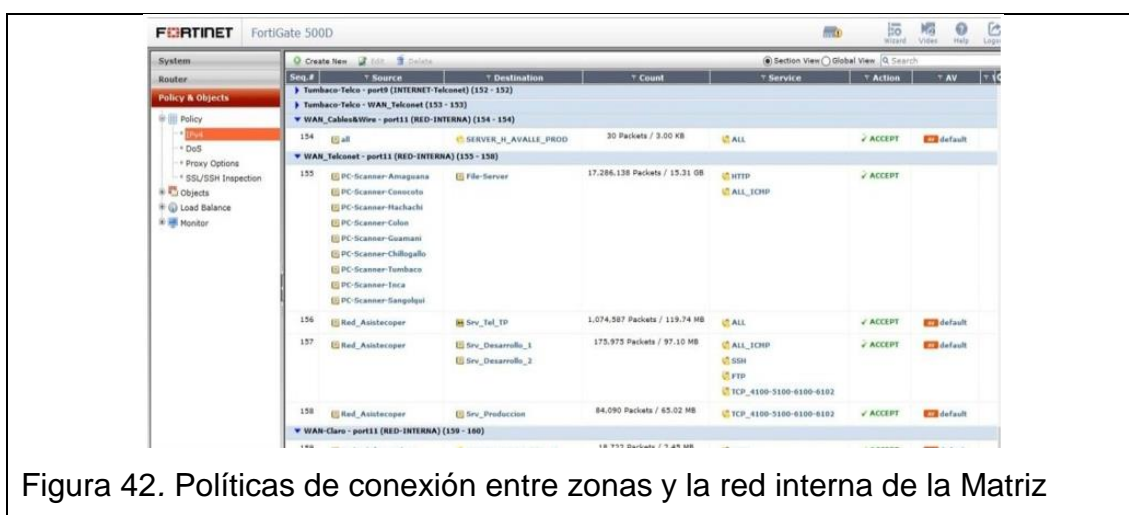


Figura 42. Políticas de conexión entre zonas y la red interna de la Matriz

#### 4.4.15 Políticas de conexión entre la red interna y las zonas externas fuera de la matriz

Se detalla a continuación todas las reglas creadas que permiten la conexión entre las redes de la matriz y las redes externas ya sea de los proveedores o de las sucursales (Ver figura 43):

Figure 43 shows the Firewall Policy configuration in FortiGate 500D. The table below summarizes the data visible in the screenshot:

Seq. #	Source	Destination	Count	Service	Action	Web Filter	Application Control
113	Vlans-Matriz	LAN-Sangolqui-Actual	14,754,971 Packets / 10.22 GB	ALL	ACCEPT		
114	Vlans-Matriz	LAN-Sangolqui-Actual	1,385,815,084 Packets / 883.90 GB	ALL	ACCEPT		
115	Vlans-Matriz	LAN-Tumbaco-Actual	713,679 Packets / 208.87 MB	ALL	ACCEPT		
116	Vlans-Matriz	LAN-Tumbaco-Actual	47,601,621 Packets / 15.82 GB	ALL	ACCEPT		
117	Vlans-Matriz	all	15,148,535 Packets / 988.15 MB	ALL	ACCEPT		RESTRICTED
118	Vlans-Matriz	Srv_NAS_Panchonet	797,120,320 Packets / 599.66 GB	ALL	ACCEPT		
119	Vlans-Matriz	Biometrico_Telco	49,438 Packets / 3.52 MB	ALL	ACCEPT		
120	Vlans-Matriz	Banco_Central	1,260,622 Packets / 412.93 MB	ALL	ACCEPT		RESTRICTED
121	Vlans-Matriz	192.100.100.0/24	52,773 Packets / 3.20 MB	ALL	ACCEPT		RESTRICTED

Additional policies listed in the screenshot include:

- port9 (INTERNET-Telconet) - port11 (RED-INTERNA) (122 - 120)
- Sangolqui-C&W - Banred\_Telconet (129 - 120)
- Sangolqui-C&W - port10 (INTERNET-New Access) (130 - 130)
- Sangolqui-C&W - port11 (RED-INTERNA) (131 - 131)
- Sangolqui-C&W - port9 (INTERNET-Telconet) (132 - 132)
- Sangolqui-C&W - WAN\_Telconet (133 - 133)
- Sangolqui-Telco - Banred\_Telconet (134 - 134)
- Sangolqui-Telco - port10 (INTERNET-New Access) (135 - 135)
- Sangolqui-Telco - port11 (RED-INTERNA) (136 - 136)

Figura 43. Políticas de conexión entre la red interna y las zonas externas fuera de la matriz

## 5. CONCLUSIONES Y RECOMENDACIONES

### 5.1. Conclusiones

De acuerdo al análisis y las comparaciones técnicas realizadas entre las soluciones de tecnologías UTM, se concluye que la solución Fortinet se ajusta a los objetivos planteados para la ejecución de este proyecto; debido a que esta solución está basada en tecnología UTM y abarca los requerimientos necesarios para esta entidad financiera que requiere de un sistema fácil de administrar, en tanto que las soluciones presentadas por Juniper y Cisco demandan de equipos complementarios para revestir las perspectivas de protección completa, distanciándose así de la percepción de un solo dispositivo que resguarde por completo a la red.

En cuanto a costos de hardware la solución Cisco presenta un costo más elevado por el requerimiento de varios dispositivos asociados para su funcionamiento, detrás de esta solución se encuentran Fortinet y Juniper con costos parejos.

El costo de las soluciones expuestas en relación de suscripción a los servicios de seguridad y soporte que ofrecen cada una de ellas determina que la solución de Fortinet brinda la protección requerida a menor costo, con una disimilitud con Juniper relativamente significativa; asimismo se debe considerar que los costos no son simplemente iniciales sino también anuales, debido a esto la solución de Juniper significa la elección más cara.

En función de brindar una solución de comunicaciones seguras y eficientes a todas las sucursales y a la matriz de la cooperativa, se instaló un FortiGate 500D que funciona en modo NAT que proporciona un sistema de gestión unificado de amenazas con las siguientes funcionalidades: Firewall, VPN, Prevención de intrusos (IPS), Antivirus, Antimalware, Control de Aplicación y Filtrado de contenidos web para identificar numerosos tipos de amenazas en un único dispositivo.



Para realizar políticas de acuerdo al SGSI se debe tomar en cuenta las cuatro reglas del proceso de mejora continua antes mencionada, al igual que la gestión eficiente de la información, la cual nos permita siempre asegurar la integridad, confidencialidad y disponibilidad de información.

La implementación del diseño de seguridad perimetral en la red de datos ha dado como resultado:

- Mejora en la seguridad de la red, esto se logró con las políticas, perfiles, grupos y objetos de firewall.
- Mejorar el rendimiento de ancho de banda, con la filtración de contenidos y control de aplicaciones evitamos que una parte de los usuarios accedan a sitios de elevado gasto de ancho de banda.
- Alta disponibilidad, con los dos enlaces brindamos la alta disponibilidad evitando así pérdida de Internet; en consecuencia tiempo y dinero para las agencias.
- Crear las políticas de seguridad que permitan la continuidad del negocio en la institución para posterior evaluación de las mismas simulando tanto ataques internos como externos.

## **5.2. Recomendaciones**

Realizar análisis periódicos de los riesgos y monitorear continuamente la situación de la infraestructura de seguridad.

Estipular un registro de activos y su grado de protección a la vez especificar como se debe manipular los activos de manera que se permita un funcionamiento óptimo.

Se recomienda documentar los procedimientos desarrollados al momento de realizar soporte remoto a los equipos de cómputo, detallando el requerimiento y su posible solución.

En el departamento de sistemas se aconseja el incremento de personal de administración de seguridad debido a que una sola persona realiza el soporte y al momento que se tenga alguna notificación de riesgo se volverá complicado trabajar en dos caos distintos a la vez.

Es recomendable que la ejecución de seguridad perimetral en instituciones financieras se la realice en base a las normas vigentes por las entidades que las controlan.

Se debe tomar en cuenta que la implementación de seguridad perimetral en la red de la institución no es un proceso estático sino un proceso de mejoramiento constante dependiendo de los cambios que presente la institución en el transcurso del tiempo.

## REFERENCIAS

- Alulema, D. (2008). "Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, utilizando tecnología UTM (Unified Threat Management)". Recuperado el 21 de septiembre del 2015 de: <http://bibdigital.epn.edu.ec/handle/15000/618>.
- Arcert, (s.f.). "Manual de Seguridad en Redes". Recuperado el 24 de septiembre del 2015 de: [http://www.arcert.gov.ar/webs/manual/manual\\_de\\_seguridad](http://www.arcert.gov.ar/webs/manual/manual_de_seguridad).
- Baltazar, J. (2011). "Diseño e implementación de un esquema de seguridad perimetral para redes de datos". Recuperado el 21 de septiembre del 2015 de: <http://docplayer.es/2565194-T-e-s-i-ingeniero-en-computacion-universidad-nacional-autonoma-de-mexico-facultad-de-ingenieria.html>.
- Calvo, A. (2016). "Normas y Estándares CERT" ISO 2 , cert.org, 2". Recuperado el 20 de febrero del 2016 de: <http://www.cert.org/octave/>.
- COAC Alianza del Valle Ltda, (s.f.). "Misión". Recuperado el 20 de febrero del 2016 de: <http://www.alianzadelvalle.fin.ec/>
- García, R. (2011). "Canal Cifrado para comunicación Cliente/Servidor", Recuperado el 22 de septiembre del 2015 de: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/.../Tesis.pdf>
- Garcés, S. (2015). "Seguridad informática para la red de datos en la cooperativa de ahorro y crédito". Recuperado el 26 de septiembre del 2015 de: [http://repositorio.uta.edu.ec/bitstream/123456789/8654/1/Tesis\\_t975si.pdf](http://repositorio.uta.edu.ec/bitstream/123456789/8654/1/Tesis_t975si.pdf).
- Information Security. (s.f.). "Public DMZ network architecture". Recuperado el 20 de febrero del 2016 de: <http://security.stackexchange.com/questions/13556/public-dmz-network-architecture>
- Junta Bancaria. (s.f.). "Resolución JB-2012-2148". Recuperado el 20 de febrero

del 2016 de:  
[http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol\\_JB-2012-2148.pdf](http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf)

Monroy, D. (2010). "Análisis inicial de la anatomía de un ataque a un sistema informático". Recuperado el 24 de septiembre del 2015 de:  
<http://www.seguinfo.com.ar/tests/>.

NIST, (s.f.). "Special Publications (8 Series)". Recuperado el 26 de septiembre del 2015 de: <http://csrc.nist.gov/publications/PubsSPs.html>.

Venegas, M. (2011). "Estudio de la importancia de las TICs en Ecuador", utpl.edu.ec. Recuperado el 21 de septiembre del 2015 de:  
<http://dspace.utpl.edu.ec/jspui/bitstream/238/2/VENEGAS2BARRAGAN2MARIANA2DEL2CARMEN2Y2YYEPE2ROSA2MARLENE.pdf>.

Vieites, Á. (2007). "Enciclopedia de la Seguridad Informática". México: Alfaomega. Recuperado el 24 de septiembre del 2015.

VIEITES, Á. (2007). "Enciclopedia de la Seguridad Informática". Recuperado el 26 de septiembre del 2015 de:  
<http://networkingsignora.pbworks.com/f/Unidad%201%20-%20Introduccion%20Seguridad%20Redes.pdf>

## **ANEXOS**

## ANEXO A

### UNIVERSIDAD DE LAS AMÉRICAS

#### FACULTAD INGENIERIA Y CIENCIAS AGROPECUARIAS

**Entrevista dirigida para la persona encargada del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle 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				
<b>Fecha:</b>				
<b>Responsable:</b>				
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? <ul style="list-style-type: none"><li>• Cintas Magnéticas</li><li>• Tarjetas FLASH</li><li>• Unidad ZIP</li><li>• Discos Duros</li><li>• Discos Flexibles</li><li>• Medios Ópticos</li><li>• JUMP Drive</li><li>• Back Ups</li></ul>				
¿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?				

	ISO 15408 clase			
¿Qué lugares utiliza para almacenar estos medios? <ul style="list-style-type: none"> <li>• Cajas Fuertes</li> <li>• Bóvedas Bancarias</li> <li>• Archivos</li> <li>• Otros (especificar)</li> </ul>	ISO 17799 sec 2.			
Este almacenamiento está situado: <ul style="list-style-type: none"> <li>• En la misma empresa</li> <li>• En el departamento de informática</li> <li>• Fuera de la empresa (especifique)</li> </ul>	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 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				
¿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				
<b>Fecha:</b>				
<b>Responsable:</b>				
Verificación	Ref.	SI	NO	Observaciones
¿Poseen en el departamento de informática un manual formal sobre la diagramación de la red de la	ISO 17799			

¿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				
¿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?				
¿Qué tipo de topología se maneja en la red? - Topología de anillo - Topología de estrella - Topología de bus				
¿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 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?				
¿Se realizan mantenimientos en los equipos de la red? (Solicitar plan de mantenimiento)				
¿Qué tipo de mantenimiento se realiza? - Preventivo	ISO 9001 4.14.2			
- Ambos - Proyectivo - Ninguno				
¿Se lleva a cabo el programa de mantenimiento?				
¿Cuáles son los problemas más comunes que se han detectado en la red?				
Cuándo un cable se daña cuál de los dos procedimientos se utilizan: - Reparación				
¿Cuándo una estación de trabajo falla que se hace? <ul style="list-style-type: none"> <li>• Un formateo con preinstalación de software.</li> <li>• Una clonación de un equipo que si funciona.</li> </ul>				
¿Se lleva una bitácora o control de las fallas o problemas detectados en el equipo de la red?				
<b>Medidas de Seguridad Física</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿Poseen seguros el activo informático de la empresa?				
¿Con que compañía? (Solicitar pólizas, tipos de seguro y montos)				

<p>El activo informático de la empresa se encuentra situado a salvo de:</p> <ul style="list-style-type: none"> <li>- Inundaciones</li> <li>- Terremotos</li> <li>- Fuego</li> </ul>	ISO			
<p>Existen alarmas para:</p> <ul style="list-style-type: none"> <li>- Detectar humo o fuego</li> <li>- Fugas de aguas</li> <li>- Fallos en el sistema eléctricos</li> <li>- Otros</li> </ul>	ISO 17799 área 1			
¿Las alarmas son perfectamente audibles o visibles?				
¿Existen extintores de fuego?				
<p>¿Los extintores de fuego funcionan a base de?</p> <ul style="list-style-type: none"> <li>- Agua</li> <li>- Gas</li> </ul>				
¿Se le dan mantenimiento a los extintores? (especifique cada cuanto tiempo)				
<p>Se han tomado medidas para minimizar la posibilidad de fuego.</p> <ul style="list-style-type: none"> <li>• Evitando artículos inflamables.</li> <li>• Prohibiendo fumar en el interior del centro de cómputo.</li> <li>• Vigilando y manteniendo el sistema eléctrico.</li> </ul>	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	ISO 17799			
¿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				
¿Existe el número de tomas corrientes polarizados suficientes para los dispositivos				
¿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?				

<b>Evaluación de la Seguridad Lógica</b>				
<b>Restricciones de acceso a archivos y programas.</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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?				
---	--	--	--	--

<b>Análisis de Amenazas y Vulnerabilidades</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿Si el administración o encargado de la red falta, hay otra persona que pueda realizar sus funciones?				
¿Se tiene procedimientos de seguridad, recuperación y respaldos para asegurar la disponibilidad continua				
¿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				

<p>Tiene la red algún tipo de protección para Internet tales como:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• Software Antivirus</li> <li>• Sistemas de detección de intrusos</li> <li>• Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.</li> <li>• Creación de un disco de rescate o de emergencia</li> <li>• Procedimientos para cuando ocurra una</li> </ul>			
¿Qué marca de firewalls poseen?			
<p>¿En qué máquina (servidor) se encuentra el Firewall?</p> <p>- En una máquina dedicada</p> <p>- En el servidor web</p>			
¿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			

¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí?				
¿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	ISO 17799			
¿Con que frecuencia se hace un escaneo total de virus en los servidores?				
¿Se registra cada violación a los procedimientos a fin de llevar estadísticas y frenar tendencias	ISO 15408			

<b>Identificación, Autenticación de usuarios y Contraseñas</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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	ISO 17799			
¿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?			
<p>¿Qué datos se muestran cuando alguien intenta acceder a la red?</p> <ul style="list-style-type: none"> <li>- Nombre de usuario</li> <li>- Password</li> <li>- Grupo o entorno de red</li> <li>- Estación de trabajo</li> </ul>			
¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?			
<p>¿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?</p>	ISO 17799 área 7		
¿Qué datos hay en el perfil del usuario cuando se hace un alta?			
<p>¿Se guardan los siguientes datos?</p> <ul style="list-style-type: none"> <li>- ID de usuario</li> <li>- Nombre y apellido completo</li> <li>- Puesto de trabajo y departamento de la empresa</li> <li>- Jefe inmediato</li> <li>- Descripción de tareas</li> <li>- Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de "buen uso" del sistema</li> <li>- Explicaciones breves y claras de cómo elegir su password</li> <li>- Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.)</li> <li>- Fecha de expiración de la cuenta</li> <li>- Datos de los permisos de acceso y excepciones</li> </ul>			
¿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			

¿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				
¿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	ISO 17799			
¿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.	ISO			
<b>Proceso de logon/logoff</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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			
<b>Acceso remoto</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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?				
<b>Back Up y RAID's</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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, pueda volverse a su estado anterior?	ISO 15408 área 11			

Evaluación de la Confidencialidad				
Verificación	Ref.	SI	NO	Observaciones
¿Existe una normativa que evalúe 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 transmisión 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?				

<b>Análisis actual de la seguridad informática</b>				
<b>Verificación</b>	<b>Ref.</b>	<b>SI</b>	<b>NO</b>	<b>Observaciones</b>
¿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? <ul style="list-style-type: none"> <li>• Manuales del sistema operativo.</li> <li>• Manuales de procedimientos.</li> <li>• Manuales de usuario.</li> <li>• Manuales de funciones.</li> </ul>	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 B GERENTE GENERAL

### ELEMENTOS DE COMPETENCIA

2	Planificar, coordinar, supervisar y evaluar la gestión administrativa y financiera de la cooperativa, según normas técnicas, legales y administrativas vigentes.	<ul style="list-style-type: none"> <li>▪ Planificación estratégica,</li> <li>▪ Presupuestos,</li> <li>▪ Administración de</li> <li>▪ Característica del mercado financiero</li> <li>▪ Análisis financiero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Negociar y establecer acuerdos.</li> <li>▪ Tomar decisiones.</li> <li>▪ Manejar hoja electrónica.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Tolerancia</li> <li>▪ Flexibilidad</li> <li>▪ Atención distribuida</li> <li>▪ Objetividad</li> <li>▪ Imparcialidad</li> </ul>
3	Diagnosticar las condiciones y evaluar el mercado financiero en función de los planes de crecimiento y de la gestión de la cooperativa.	<ul style="list-style-type: none"> <li>▪ Mercadeo de productos y servicios financieros</li> </ul>	<ul style="list-style-type: none"> <li>▪ Interpretar resultados.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Capacidad predictiva</li> </ul>
4	Analizar, sugerir e implementar las estrategias de mercadeo de productos y servicios.	<ul style="list-style-type: none"> <li>▪ Políticas de crédito</li> <li>▪ Reglamento de crédito</li> </ul>	<ul style="list-style-type: none"> <li>▪ Determinar capacidad endeudamiento</li> </ul>	<ul style="list-style-type: none"> <li>▪ Objetividad</li> <li>▪ Imparcialidad</li> </ul>
5	Aprobar créditos solicitados según rangos de aprobación establecidos.	<ul style="list-style-type: none"> <li>▪ Normas relacionadas</li> <li>▪ Políticas de crédito</li> <li>▪ Reglamento de crédito</li> <li>▪ Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>▪ Determinar capacidad endeudamiento</li> </ul>	<ul style="list-style-type: none"> <li>▪ Objetividad</li> <li>▪ Imparcialidad</li> <li>▪ Independencia</li> <li>▪ Objetividad</li> <li>▪ Prudencia</li> </ul>
6	Participar del comité de crédito para la aprobación de solicitudes según rango establecido, como representante técnico	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>▪ Orientar toma de</li> <li>▪ Ejercer liderazgo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Respeto a las normas</li> </ul>
7	Informar, ejecutar, coordinar, controlar y evaluar el cumplimiento de las disposiciones de los órganos de control, en los términos establecidos.	<ul style="list-style-type: none"> <li>▪ Resultados de gestión</li> </ul>	<ul style="list-style-type: none"> <li>▪ Delegar</li> <li>▪ Supervisar</li> <li>▪ Elaborar presentaciones</li> <li>▪ Comunicar oralmente</li> </ul>	<ul style="list-style-type: none"> <li>▪ Transparencia</li> <li>▪ Aptitud verbal</li> <li>▪ Respeto a las normas</li> </ul>
8	Informar periódicamente sobre la gestión técnica y administrativa de la cooperativa a los organismos directivos, verbal y documentalmente.	<ul style="list-style-type: none"> <li>▪ Reglamento de adquisiciones</li> <li>▪ Mercado de bienes y servicios</li> <li>▪ Gestión de recursos humanos</li> <li>▪ Técnicas de negociación</li> </ul>	<ul style="list-style-type: none"> <li>▪ Negociar y establecer acuerdos</li> <li>▪ Tomar decisiones</li> <li>▪ Ejercer liderazgo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Transparencia</li> <li>▪ Imparcialidad</li> <li>▪ Objetividad</li> </ul>
9	Informar periódicamente sobre la gestión técnica y administrativa de la cooperativa a los organismos directivos, verbal y documentalmente.	<ul style="list-style-type: none"> <li>▪ Resultados de la gestión</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Tomar decisiones</li> </ul>	<ul style="list-style-type: none"> <li>▪ Justicia</li> <li>▪ Equidad</li> <li>▪ Imparcialidad</li> <li>▪ Transparencia</li> <li>▪ Objetividad</li> <li>▪ Objetividad</li> </ul>
10	Aprobar la adquisición de bienes y servicios requeridos, según monto establecido, para la gestión de la cooperativa	<ul style="list-style-type: none"> <li>▪ Mercado de cada</li> <li>▪ Mercado financiero</li> <li>▪ Normas de prudencia financiera</li> <li>▪ Técnicas de</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Tomar decisiones</li> <li>▪ Negociar y establecer acuerdos</li> <li>▪ Tomar de</li> </ul>	<ul style="list-style-type: none"> <li>▪ Equidad</li> <li>▪ Imparcialidad</li> <li>▪ Objetividad</li> <li>▪ Prudencia</li> </ul>
11				



## CONTADOR GENERAL

1	Revisar y validar la información contable, por varios conceptos según normas y procedimientos establecidos.	<ul style="list-style-type: none"> <li>▪ Contabilidad de Costos</li> <li>▪ Contabilidad</li> <li>▪ Normativa Vigente</li> <li>▪ Sistema de Control</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Formar efectivos equipos de trabajo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
2	Visitar, revisar y validar el cuadro diario de las cuentas correspondiente, consolidando información de matriz y	<ul style="list-style-type: none"> <li>▪ Contabilidad de Costos</li> <li>▪ Contabilidad</li> <li>▪ Normativa Vigente</li> <li>▪ Sistema de Control</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Formar efectivos equipos de trabajo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
3	agencias	<ul style="list-style-type: none"> <li>▪ Contabilidad de Costos</li> <li>▪ Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Formar efectivos equipos de trabajo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
4	Revisar y aprobar las conciliaciones bancarias de las cuentas de la cooperativa, según prácticas contables corrientes.	<ul style="list-style-type: none"> <li>▪ Normativa Vigente</li> <li>▪ Sistema de Control</li> <li>▪ Normativa Tributaria vigente</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ejercer liderazgo</li> <li>▪ Formar efectivos equipos de trabajo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
5	Elaborar los formularios para cumplir las obligaciones tributarias	<ul style="list-style-type: none"> <li>▪ Indicadores Contables</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar informes y presentaciones</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
6	Elaborar y presentar informes sobre indicadores contables, según requerimientos superiores y normas y procedimientos establecidos.	<ul style="list-style-type: none"> <li>▪ Indicadores Contables</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar informes y presentaciones</li> <li>▪ Interpretar resultados.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
7	Elaborar listados financieros consolidados, según las normas vigentes de contabilidad.	<ul style="list-style-type: none"> <li>▪ Indicadores Contables</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar informes financieros</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Aptitud numérica</li> </ul>
8	Elaborar mensualmente los roles de pago, planillas del IESS y liquidaciones de personal	<ul style="list-style-type: none"> <li>▪ Código de Trabajo</li> <li>▪ Reformas salariales</li> <li>▪ Seguridad social</li> <li>▪ Hojas de cálculo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar planillas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Honestidad</li> <li>▪ Equidad</li> </ul>
9	Realizar arqueos del inventario de los activos fijos, pagarés, hipotecas, garantías y depósitos a plazo fijo	<ul style="list-style-type: none"> <li>▪ Elaboración de inventarios</li> <li>▪ Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar informes</li> <li>▪ Detectar fallos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Honestidad</li> </ul>
	Dar inicio y fin del día a través			

## ASISTENTE DE CONTABILIDAD

1	Revisar la validez y pertinencia de documentos de pago y elaborar comprobantes de egresos, ingresos y diarios de matriz y agencias.	<ul style="list-style-type: none"> <li>▪ Normativa vigente</li> <li>▪ Normativa interna</li> <li>▪ Obligaciones de pago</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar comprobantes de egreso</li> </ul>	<ul style="list-style-type: none"> <li>□ Oportunidad</li> <li>□ Precisión</li> </ul>
2	Registrar en el libro bancos, los depósitos, pagos diarios realizados según procedimientos establecidos.	<ul style="list-style-type: none"> <li>▪ Contabilidad</li> <li>▪ Computación</li> </ul>	<ul style="list-style-type: none"> <li>▪ Operar sistema, del módulo de Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Precisión</li> <li>▪ Agilidad manual</li> </ul>
3	Realizar la conciliación bancaria de las cuentas de la cooperativa			<ul style="list-style-type: none"> <li>▪ Precisión</li> </ul>
4	Imprimir mayores, auxiliares, balances de comprobación y balances generales y de resultados, y archivar para mantener un archivo físico para la Cooperativa	<ul style="list-style-type: none"> <li>▪ Sistema de cuentas</li> <li>▪ Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Módulo del sistema</li> <li>▪ Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Agilidad manual</li> </ul>
5	Custodiar títulos valores, pólizas, chequeras, efectivo, hipotecas y pagarés según normas y procedimientos vigentes.	<ul style="list-style-type: none"> <li>▪ Reglamento de crédito</li> <li>▪ Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>▪ Operar el sistema informático, en el módulo de Contabilidad.</li> </ul>	<ul style="list-style-type: none"> <li>□ Honradez</li> <li>□ Transparencia</li> </ul>
6	Realizar y mantener actualizado el inventario contable de activos fijos	<ul style="list-style-type: none"> <li>▪ Contabilidad</li> <li>▪ Sistema de inventarios</li> </ul>	<ul style="list-style-type: none"> <li>▪ Operar el sistema informático</li> </ul>	<ul style="list-style-type: none"> <li>□ Agilidad mental</li> <li>□ Honestidad</li> </ul>
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.	<ul style="list-style-type: none"> <li>▪ Normativa tributaria</li> <li>▪ Liquidación de nomina</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar formatos varios</li> </ul>	<ul style="list-style-type: none"> <li>□ Exactitud</li> <li>□ Aptitud numérica</li> </ul>
8	Elaborar y cuadrar formatos de pago de retenciones en la fuente, a contabilidad, para su consolidación.			<ul style="list-style-type: none"> <li>▪ Aptitud numérica</li> <li>▪ Oportunidad</li> <li>▪ Transparencia</li> </ul>
9	Cuadrar el cobro de planillas telefónicas de los socios a través de débito a las cuentas	<ul style="list-style-type: none"> <li>▪ Normativa tributaria</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar formatos varios</li> </ul>	<ul style="list-style-type: none"> <li>▪ Facilidad de comunicación</li> </ul>
10	Identificar las necesidades materiales y equipos de oficina, adquirirlos y controlar su custodia, mantenimiento y consumo.	<ul style="list-style-type: none"> <li>▪ Normativa vigente</li> </ul>	<ul style="list-style-type: none"> <li>▪ Operar el módulo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Honestidad</li> <li>▪ Pro actividad</li> </ul>
11	Elaborar cheques y realizar los pagos a proveedores	<ul style="list-style-type: none"> <li>▪ Contabilidad</li> <li>▪ Tributación</li> <li>▪ Tributación</li> <li>▪ Ley de cheques</li> <li>▪ Contabilidad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Planificar y organizar</li> <li>▪ Habilidad numérica</li> </ul>	<ul style="list-style-type: none"> <li>□ Honestidad</li> <li>▪ Oportunidad</li> </ul>

## RECIBIDOR PAGADOR

1	Recibir y verificar la cantidad, autenticidad del "fondo de cambio" <sup>1</sup> , de acuerdo a procedimientos establecidos y formatos aprobados	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Reconocimiento del dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar, autenticidad cantidad de dinero</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Honestidad y</li> <li><input type="checkbox"/> Precisión</li> <li>▪ Aptitud numérica</li> </ul>
2	Cancelar retiros de fondos a socios de otras agencias para atender los requerimientos de socios y clientes , según procedimientos aprobados	<ul style="list-style-type: none"> <li>▪ Sistema de cuentas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Detectar errores contables</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Oportunidad</li> </ul>
3	Recibir y pagar dinero por varios conceptos, según requerimientos de socios y clientes, verificando montos, autenticidad de papeletas, identidad y más aspectos.	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Calidad en el servicio</li> <li>▪ Relaciones humanas</li> <li>▪ Técnicas de negociación</li> <li>▪ Reconocimiento del dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar autenticidad y de dinero</li> <li>▪ Gestionar el sistema, módulo de caja.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Paciencia cantidad</li> <li><input type="checkbox"/> Aptitud numérica</li> <li><input type="checkbox"/> Honestidad del</li> </ul>
4	Acreditar y debitar, dinero en las cuentas correspondientes de socios y clientes según procedimientos establecidos	<ul style="list-style-type: none"> <li>▪ Gestión de caja</li> </ul>	<ul style="list-style-type: none"> <li>▪ Manejar módulo de Precisión</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Oportunidad caja</li> <li><input type="checkbox"/></li> <li>▪ Aptitud numérica</li> </ul>
5	Realizar cuadro diario de caja, verificando el efectivo y cheques, y los reportes del sistema	<ul style="list-style-type: none"> <li>▪ Gestión de caja</li> </ul>	<ul style="list-style-type: none"> <li>▪ Manejar módulo de Precisión</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Oportunidad caja</li> <li><input type="checkbox"/></li> <li>▪ Aptitud numérica</li> </ul>
6	Custodiar la caja y la recaudación diaria en efectivo	<ul style="list-style-type: none"> <li>▪ Clave de acceso</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar, autenticidad cantidad de dinero</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Honradez y</li> <li><input type="checkbox"/> Precisión</li> <li>▪ Aptitud numérica</li> </ul>
7	Aperturar cuentas de ahorros <sup>2</sup>	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>▪ Manejar módulos del sistema.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Oportunidad</li> <li><input type="checkbox"/> Precisión</li> <li>▪ Aptitud numérica</li> </ul>
8	Recaudar los depósitos de acuerdos con otras	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Reconocimiento de</li> </ul>	<ul style="list-style-type: none"> <li>▪ Manejar módulo de (convenios)</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Precisión caja</li> <li><input type="checkbox"/> Honradez</li> </ul>
9	Realizar diariamente reportes de libretas de: ahorros, aportaciones y préstamos	<ul style="list-style-type: none"> <li>▪ Utilización de utilitarios (Excel)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaboración y presentación de reportes</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Precisión</li> </ul>
10				

## CRÉDITO Y COBRANZAS

1	Atender a los socios / clientes que requieran créditos	<ul style="list-style-type: none"> <li>Reglamento de crédito</li> </ul>	<ul style="list-style-type: none"> <li>Negociar</li> <li>Comunicar</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Transparencia</li> </ul>
2	Evaluar solicitudes de crédito según políticas y reglamento de crédito vigentes,  Aprobar o negar operaciones dentro de su	<ul style="list-style-type: none"> <li>Reglamento de crédito</li> <li>Historial crediticio de clientes</li> <li>Análisis de riesgo crediticio</li> </ul>	<ul style="list-style-type: none"> <li>Detectar inconsistencias de información y documentos de respaldo</li> </ul>	<ul style="list-style-type: none"> <li>Perspicacia</li> <li>Objetividad</li> <li>Imparcialidad</li> </ul>
3	Participar del Comité de crédito para evaluar y recomendar la aprobación o negación de solicitudes de crédito	<ul style="list-style-type: none"> <li>Reglamento de crédito</li> <li>Historial crediticio de clientes</li> <li>Análisis de riesgo crediticio</li> </ul>	<ul style="list-style-type: none"> <li>Detectar inconsistencias de información y documentos de respaldo</li> </ul>	<ul style="list-style-type: none"> <li>Perspicacia</li> <li>Objetividad</li> <li>Imparcialidad</li> </ul>
4	Coordinar con los Jefes de Agencias, el control de la morosidad de los deudores, según las Leyes vigentes	<ul style="list-style-type: none"> <li>Tablas de amortización</li> <li>Análisis de morosidad</li> </ul>	<ul style="list-style-type: none"> <li>Negociar y lograr acuerdos</li> <li>Elaborar informes de morosidad</li> </ul>	<ul style="list-style-type: none"> <li>Pro actividad</li> <li>Eficiencia</li> <li>Imparcialidad</li> </ul>
5	Elaborar y presentar informes de crédito, para gerencia, consejos y las unidades de control externo.	<ul style="list-style-type: none"> <li>Indicadores de gestión de crédito</li> <li>Sistema módulos de cartera cobranzas</li> </ul>	<ul style="list-style-type: none"> <li>Elaborar informes</li> </ul>	<ul style="list-style-type: none"> <li>Objetividad</li> <li>Precisión</li> </ul>
6	Supervisar las operaciones de crédito	<ul style="list-style-type: none"> <li>Indicadores de gestión de crédito</li> <li>Reglamento interno de crédito</li> </ul>	<ul style="list-style-type: none"> <li>Detectar errores u omisiones.</li> <li>Capacidad de comunicación</li> </ul>	<ul style="list-style-type: none"> <li>Objetividad</li> <li>Imparcialidad</li> </ul>
7	Coordinar las acciones administrativas de cobro a socios con créditos en mora, con los abogados de la Cooperativa	<ul style="list-style-type: none"> <li>Tabla de morosidad</li> <li>Procesos judiciales de cobro</li> </ul>	<ul style="list-style-type: none"> <li>Identificar cobros por vía administrativa y judicial</li> </ul>	<ul style="list-style-type: none"> <li>Responsable</li> <li>Honestidad</li> <li>Ética profesional</li> </ul>
8	Elaborar y presentar informes sobre créditos vinculados para presentar a las entidades de control	<ul style="list-style-type: none"> <li>Indicadores de crédito vinculados</li> <li>Normativa vigente</li> </ul>	<ul style="list-style-type: none"> <li>Elaborar informes y presentaciones</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Precisión</li> <li>Objetividad</li> <li>Imparcialidad</li> </ul>
9	Distribución y calificación de cartera	<ul style="list-style-type: none"> <li>Normativa vigente</li> </ul>	<ul style="list-style-type: none"> <li>Elaborar informes</li> </ul>	<ul style="list-style-type: none"> <li>Objetividad</li> <li>Imparcialidad</li> </ul>

## JEFE DE CAPTACIONES

N°	ELEMENTOS DE COMPETENCIA	CONOCIMIENTOS REQUERIDOS	HABILIDADES Y DESTREZAS	ACTITUDES VALORES Y
1	Controlar y monitorear el cumplimiento de dinero en permanencia en las cajas, y dinero en bóveda conforme a	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Gestión de cajas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Manejar el módulo de caja</li> <li>▪ Ejercer liderazgo</li> </ul>	<ul style="list-style-type: none"> <li>▪ Aptitud numérica</li> <li>▪ Transparencia</li> <li>▪ Honestidad</li> </ul>
2	Proveer y prever el "fondo de cambio" diario a cada cajero según montos de efectivo de socios y procedimientos	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Identificación de dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar autenticidad y cantidad de dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Aptitud numérica</li> <li>▪ Transparencia</li> <li>▪ Honestidad</li> <li>▪ Coordinación manual</li> </ul>
3	Controlar el "cuadre diario de caja" de cada cajero según condiciones y procedimientos	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar autenticidad y cantidad de dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Aptitud numérica</li> <li>▪ Transparencia</li> <li>▪ Honestidad</li> </ul>
4	Recibir las recaudaciones diarias de efectivo y cheques de cada cajero, verificando montos y autenticidad del dinero con sus respectivos	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Dinero autentico</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar autenticidad y cantidad de dinero</li> </ul>	<ul style="list-style-type: none"> <li>▪ Aptitud numérica</li> <li>▪ Transparencia</li> <li>▪ Honestidad</li> <li>▪ Coordinación manual</li> </ul>
5	Coordinar el depósito diario de las recaudaciones realizadas por las diferentes cajas, según procedimientos establecidos.	<ul style="list-style-type: none"> <li>▪ Ídem</li> </ul>	<ul style="list-style-type: none"> <li>▪ Llenar formatos de depósito varios</li> <li>▪ Ídem</li> </ul>	<ul style="list-style-type: none"> <li>□</li> </ul>
6	Atender los requerimientos de socios y clientes, de agencias y ventanillas compartidas según procedimientos	<ul style="list-style-type: none"> <li>▪ Sistema de cuentas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ídem</li> </ul>	<ul style="list-style-type: none"> <li>▪ Atención distribuida</li> <li>▪ Oportunidad</li> </ul>
7	Diseñar, proponer y ejecutar estrategias genéricas y específicas para incrementar las captaciones por ahorro, inversiones, remesas y otros,	<ul style="list-style-type: none"> <li>▪ Mercado financiero local y nacional</li> <li>▪ Necesidades de los clientes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Percepción de oportunidades de negocios</li> <li>▪ Percibir las expectativas de los</li> </ul>	<ul style="list-style-type: none"> <li>▪ Proactividad</li> <li>▪ Iniciativa</li> <li>▪ Creatividad</li> </ul>
8	Atender las operaciones de remesas (giros y envíos)	<ul style="list-style-type: none"> <li>▪ Normativa relacionada</li> <li>▪ Gestión de cajas</li> <li>▪ Necesidades de los</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar autenticidad de información</li> <li>□</li> </ul>	<ul style="list-style-type: none"> <li>▪ Proactividad</li> <li>▪ Iniciativa</li> <li>▪ Transparencia</li> </ul>
9	Cuidar las operaciones para el Ingreso de socios	<ul style="list-style-type: none"> <li>Normativa relacionada</li> </ul>	<ul style="list-style-type: none"> <li>Verificar autenticidad de información</li> <li>Percepción de</li> </ul>	<ul style="list-style-type: none"> <li>Proactividad</li> <li>Iniciativa</li> <li>Sentido de oportunidad</li> <li>Objetividad</li> </ul>
10	Verificar y suscribir certificados de aportación, inversión y otros, según normas y procedimientos establecidos.	<ul style="list-style-type: none"> <li>▪ Sistema de captaciones</li> <li>▪ Ley de instituciones financieras</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verificar corrección de procedimientos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Sentido de oportunidad</li> <li>▪ Objetividad</li> </ul>
11	Coordinar la elaboración y presentación de reportes periódicos sobre depósitos a plazo, según estipulaciones de	<ul style="list-style-type: none"> <li>▪ Depósitos a plazo recibidos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Elaborar formatos específicos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Objetividad</li> <li>▪ Oportunidad</li> <li>▪ Transparencia</li> </ul>

12	Llevar el control y presentar reportes consolidados periódicos a diferentes usuarios sobre altas y bajas de socios, según formato	<ul style="list-style-type: none"> <li>Altas y bajas de socios y clientes</li> </ul>	<ul style="list-style-type: none"> <li>Elaborar formatos específicos</li> </ul>	<ul style="list-style-type: none"> <li>Objetividad</li> <li>Oportunidad</li> <li>Transparencia</li> </ul>
----	---	--	---	---

### 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	<ul style="list-style-type: none"> <li>Operación del sistema automático de gestión de la Cooperativa</li> </ul>	<ul style="list-style-type: none"> <li>Supervisar acciones técnicas del arranque del sistema</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Precisión</li> </ul>
2	Supervisar la operatividad de los diferentes equipos, programas y sistema, necesarios para gestionar los servicios	<ul style="list-style-type: none"> <li>Operación del sistema automático de gestión de la cooperativa</li> <li>Demandas operativas de diferentes áreas</li> </ul>	<ul style="list-style-type: none"> <li>Supervisar acciones técnicas de operación del sistema</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Pro actividad</li> <li>Aptitud abstracta y numérica</li> </ul>
3	Corregir los comandos erróneos realizados por los usuarios del sistema, según procedimientos técnicos establecidos	<ul style="list-style-type: none"> <li>Normas y claves de reversión</li> </ul>	<ul style="list-style-type: none"> <li>Detectar causas de fallos</li> <li>Corregir errores</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Precisión</li> <li>Aptitud numérica</li> </ul>
4	Realizar mantenimiento preventivo y correctivo de programas necesarios para mantener operativo el sistema	<ul style="list-style-type: none"> <li>Funcionamiento y programación de programas utilitarios</li> </ul>	<ul style="list-style-type: none"> <li>Detectar fallos</li> <li>Corregir errores</li> </ul>	<ul style="list-style-type: none"> <li>Aptitud abstracta</li> <li>Aptitud numérica</li> <li>Coordinación manual</li> </ul>
5	Crear, registrar, controlar y permitir o denegar accesos de usuarios a los diferentes módulos del sistema	<ul style="list-style-type: none"> <li>Sistema automático de gestión</li> <li>Área de gestión de cada funcionario</li> </ul>	<ul style="list-style-type: none"> <li>Identificar ingresos al sistema según sistema de códigos.</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Precisión</li> <li>Coordinación manual</li> </ul>
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	<ul style="list-style-type: none"> <li>Operación del sistema automático de gestión de la Cooperativa</li> </ul>	<ul style="list-style-type: none"> <li>Operar comandos de impresión y respaldos</li> </ul>	<ul style="list-style-type: none"> <li>Oportunidad</li> <li>Precisión</li> <li>Coordinación manual</li> </ul>

7	Apoyar y asesorar a la gerencia en toma de decisiones para mejorar la tecnología de la	<ul style="list-style-type: none"> <li>▪ Nueva tecnología en el mercado</li> <li>▪ Necesidades de la Cooperativa</li> </ul>	<ul style="list-style-type: none"> <li>▪ Negociar con proveedores</li> <li>▪ Comunicar</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> </ul>
8	Ser parte del Comité Informático (Secretario)	<ul style="list-style-type: none"> <li>▪ Riesgo operativo</li> <li>▪ Planes de</li> </ul>	<ul style="list-style-type: none"> <li>▪ Detectar riesgos y dar soluciones</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Objetividad</li> </ul>
9	Supervisar el proceso de cierre del día, según procedimientos técnicos	<ul style="list-style-type: none"> <li>▪ Operación del sistema automático de gestión de la Cooperativa</li> </ul>	<ul style="list-style-type: none"> <li>▪ Operar computador</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oportunidad</li> <li>▪ Precisión</li> <li>▪ Coordinación manual</li> </ul>

## GLOSARIO

- **Debuggers:** es un programa usado para probar y depurar de otros programas.
- **ACL (*Lista de Control de Acceso*):** es un concepto de seguridad informática usado para fomentar la separación de privilegios.
- **IDS (*Sistema de detección de intrusiones*):** hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.
- **VPN (*red privada virtual*):** es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet.
- **DMZ (*zona desmilitarizada*):** es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red.
- **NAT (*Network Address Translation*):** es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.
- **SNMP (*Simple Network Management Protocol*):** es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- **RMON:** protocolo para la monitorización remota de redes. Es un estándar que define objetos actuales e históricos de control, permitiendo que usted capture la información en tiempo real a través de la red entera.