FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA RED DE DATOS DE LA COOPERATIVA 29 DE OCTUBRE BAJO EL ESTÁNDAR PCI_DSS

AUTORES

Santiago Andrés Hernández Esparza

Wladimir Alexander Muñoz Jaramillo

AÑO

2017

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA RED DE DATOS DE LA COOPERATIVA 29 DE OCTUBRE BAJO EL ESTÁNDAR PCI_DSS

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

Profesor Guía

Mgt. Milton Neptalí Román Cañizares

Autores

Santiago Andrés Hernández Esparza

Wladimir Alexander Muñoz Jaramillo

Año

2017

DECLARACIÓN 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”

Milton Neptalí Román Cañizares
Magister en Gerencia de Redes y Telecomunicaciones
CI: 050216344-7

DECLARACIÓN PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

William Eduardo Villegas Chiliquinga
Magister en Redes de Comunicaciones
CI: 171533826-3

DECLARACIÓN DE AUTORÍA DE LOS ESTUDIANTES

“Declaramos que este trabajo es original, de nuestra 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.”

Santiago Andrés Hernández Esparza	Wladimir Alexander Muñoz Jaramillo
CI: 172196209-8	CI: 171531465-2

AGRADECIMIENTOS

“A Dios, a mi esposa y a mis padres quienes me han brindado todo su apoyo”

Santiago

DEDICATORIA

“Dedico este logro a mi querido padre Marcial Hernández quien con sus enseñanzas supo encaminar mi vida en todo momento. A mi esposa por ser un ejemplo de amor, trabajo y constancia, y a toda mi familia por su paciencia y comprensión”

Santiago

AGRADECIMIENTOS

“A mi familia por el apoyo brindado a lo largo de este camino por ser mi mejor aliado.”

Wladimir

DEDICATORIA

“Dedico este logro a mi esposa y mi hija que iluminan mi vida con su presencia dándome la fortaleza para terminar esta meta. A toda mi familia por su ayuda incondicional”

Wladimir

RESUMEN

El presente trabajo de titulación, ayuda a identificar y resolver las necesidades de la institución financiera, mediante el alcance se planteará los objetivos a cumplir, métodos que serán utilizados y resultados obtenidos, a continuación, se dará una perspectiva general de lo que se va a tratar en el trabajo de titulación.

Capítulo I – Introducción

En el primer capítulo se trata de la introducción del presente trabajo de titulación.

Capítulo II – Marco teórico

En el segundo capítulo se realizará una revisión documental sobre las redes multiservicios y el estándar PCI-DSS. Esto con el fin de sustentar teóricamente la elaboración del presente trabajo de titulación

Capítulo III – Situación actual

En el tercer capítulo su desarrollo se fundamentará en el Modelo de Referencia OSI y TCP/IP para lo cual se dividirá en dos marcos de estudio: red física y red lógica, esto ayudará a tener una visión más clara del estado actual de la red LAN de la Institución.

Capítulo IV – Diseño de la red

En el cuarto capítulo se propone el diseño de una nueva red, en base a las recomendaciones establecidas por el estándar PCI-DSS y tomando como referencia el estándar de la serie ISO 27000.

Capítulo V – Análisis costo-beneficio

En el quinto capítulo se especificará el análisis costo beneficio que permitirá demostrar la rentabilidad del proyecto, el cual será evaluado desde el punto de vista monetario, también se considerara los beneficios que se obtendrán al contar con una red multiservicios basada en el estándar PCI-DSS.

ABSTRACT

The present titling work, helps to identify and solve the needs of the financial institution, through the scope will be set out the objectives to be met, methods to be used and results obtained, then will give an overview of what will be try on job titling.

Chapter I - Introduction
The first chapter deals with the introduction of the present titling work.

Chapter II - Theoretical framework
In the second chapter, a documentary review will be carried out on multiservice networks and the PCI-DSS standard. This in order to theoretically support the preparation of the present titling work

Chapter III - Current situation
In the third chapter, its development will be based on the Reference Model OSI and TCP / IP, which will be divided into two frameworks: physical network and logical network, this will help to have a clearer view of the current state of the LAN Of the Institution.

Chapter IV - Design of the network
The fourth chapter proposes the design of a new network, based on the recommendations established by the PCI-DSS standard and taking as reference the standard of the ISO 27000 series.

Chapter V - Cost-benefit analysis
The fifth chapter will specify the cost benefit analysis that will demonstrate the profitability of the project, which will be evaluated from the monetary point of view, and will also consider the benefits to be gained by having a multi-service network based on the PCI-DSS standard.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

La cooperativa de ahorro y crédito “29 de octubre” ofrece varios servicios, por lo que busca mediante un rediseño poder ofrecer una red convergente que pueda cumplir con los desafíos de las redes como redundancia, escalabilidad, rendimiento, flexibilidad y seguridad. En la institución la red de voz está basada en varios PBX los cuales están conectados a la PSTN externa o publica, también tiene implementado telefonía IP, mientras tanto la red de datos utiliza enrutadores ayudando a conectar la red LAN y permitiendo el acceso y uso de internet, toda la administración de la red se maneja por medio del firewall, sin embargo nace la necesidad de que por una misma red se pueda utilizar datos, voz, video y cualquier otro de servicio, por lo que se busca mantener disponibilidad y calidad de servicio en la red multiservicios, teniendo en cuenta que se pueden reducir costos por mantenimiento, administración, y un mejor manejo de la información.

Además, la institución desea trabajar con tarjetas de crédito por lo que es necesario obtener la certificación PCI-DSS, estás son normas que ayudan a mantener de forma segura la información de los tarjeta habientes, también se tomara como referencia las normas de la ISO27000, tener una idea clara de lo que la entidad necesita para cumplir este desafío, se evidencia en este documento con las normas necesarias para el cumplimiento y además se indica que normas ya están siendo cumplidas, también teniendo en cuenta que el rediseño ayudara a cumplir con las normas establecidas en el PCI-DSS.

1.1 JUSTIFICACIÓN

El proyecto está enfocado a presentar una solución de red de datos que cumpla con los requerimientos de seguridad que solicita el estándar internacional PCI DSS, el cual permitirá a la Cooperativa de Ahorro y Crédito “29 de octubre” certificarse como PCI DSS y de esta manera que la información de las tarjetas de crédito que se transmiten por red sea segura.

El aporte a la comunidad es un procedimiento técnico de cómo transmitir datos de forma segura dentro de una red empresarial.

Por otro lado, el aporte para la UDLA es ofrecerle una propuesta de diseño de red de datos que sea fácilmente entendible, basada en el conocimiento adquirido ellas materias de especialización cursadas en el transcurso de la carrera.

1.2 OBJETIVOS

Objetivo General

Rediseñar una red multiservicios para la Cooperativa de Ahorro y Crédito “29 de octubre” Sede Central y sus agencias, considerando el estándar PCI DSS y tomando como referencia el estándar de la serie ISO 27000.

Objetivos específicos

- ✓ Realizar un análisis de la red de datos actual.
- ✓ Diseñar la red multiservicios considerando parámetros de redundancia y gestión.
- ✓ Proponer los parámetros de seguridad conforme al estándar PCI DSS.
- ✓ Realizar un análisis costo-beneficio del rediseño propuesto.

1.3 ALCANCE

El alcance de este trabajo de titulación es rediseñar la red de datos de la Cooperativa 29 de Octubre para lo cual se empezará con un análisis de la situación actual de la red (parte lógica y parte física), elaborar una propuesta donde se especifique los requisitos necesarios de red, ya sean lógicos o físicos para que la cooperativa pueda alcanzar la certificación. Posteriormente, se pretende proponer un diseño de red de alta disponibilidad y que considere la seguridad según el estándar PCI–DSS y bajo la referencia del estándar ISO27000.

Para la propuesta de diseño, se recomendará una segmentación de red para una mejor administración de la red de datos. Se propondrá la utilización de VLANs interdepartamentales para la segmentación del tráfico de red. Finalmente se propondrá establecer redundancia a nivel de capa de núcleo para garantizar la continuidad del negocio.

Para la segmentación de red se tendrá en cuenta la estructura organizacional de la institución lo cual ayudará a realizar de mejor manera la configuración de las VLANs del diseño indicado, así se facilitará la administración de tal forma tener controlado el tráfico que circula por la misma. Por último, se va a sugerir una configuración que permita tener alta disponibilidad a nivel de capa de núcleo para de esta manera asegurar la continuidad del negocio frente posibles fallas de hardware que pudieran ocurrir, es decir, el usuario tanto interno como externo no deberá tener ninguna interrupción del servicio.

Para alcanzar el cumplimiento de lo antes mencionado se va a utilizar lo aprendido en las materias de: administración de redes, seguridad de redes, evaluación de redes y certificación de redes.

El costo beneficio que obtendrá la institución al cumplir con las normas que indica el estándar PCI DSS a sugerir para la red multiservicios, podrá ser visto una vez que la Cooperativa aplique a futuro a la Certificación PCI DSS y la apruebe, todo esto con la finalidad de transaccionar con tarjetas de crédito. Sin embargo, se presentará un análisis costo beneficio.

2. MARCO TEÓRICO

2.1 Introducción a las redes informáticas

Una red informática comprende un conjunto de dispositivos que se interconectan entre sí a través de un medio, siendo capaces de transmitir información e intercambiar recursos, ya sea utilizando medios cableados como el par trenzado de cobre o fibra óptica, o a su vez su transmisión sea inalámbrica utilizando ondas electromagnéticas.

Las redes se componen tanto por hardware como por software. El hardware se refiere a la parte tangible de la red como lo son enrutadores, conmutadores y los equipos terminales o hosts, sin dejar a un lado los servidores quienes brindan servicios a los usuarios de red. El software representa la parte intangible de la red, básicamente se refiere a los programas que son utilizados por los usuarios de la red.

“Para que los equipos puedan transmitir y compartir información unos con otros, deben manejar un lenguaje común. Se establece entonces de antemano un conjunto de normas y reglas que permita esta comunicación. A estos grupos de reglas se los denomina protocolos de comunicación y forman parte del software de la red. También se maneja software a nivel de aplicación, es decir para la interacción del usuario con la red”. (Morales, 2016, pág. 1)

2.2 Clasificación de las redes informáticas

Las redes se clasifican considerando diferentes criterios como: alcance o cobertura, método de conexión, relación funcional, topología de red y direccionalidad de los datos.

2.2.1 Por el alcance o cobertura

De bastante utilidad resulta la división de las redes por su rango de cobertura, por ejemplo, cuando se analiza las aplicaciones más comunes o cuando se revisa algunos estándares relacionados a alguna de estas clases.

2.2.1.1 WAN

Las redes de área extensa (WAN). Son redes capases de cubrir un área geográfica extensa como por ejemplo brindar servicios a un país o continente.

Su composición radica en varios nodos los cuales se encargan de la trasmisión de los mensajes desde un origen al destinatario. El ejemplo más conocido de este tipo de redes es la INTERNET.

Las redes WAN a diferencia de las redes LAN no solo se distinguen por su cobertura. La información atraviesa largas distancias y eso hace que se deban utilizarse técnicas de transmisión, protocolos e interfaces apropiadas para que la comunicación sea efectiva y el uso de los recursos sea eficiente. Además, es muy común que este tipo de redes las administren varios o pertenezcan a más de un dueño.

2.2.1.2 MAN

Una red de área metropolitana (MAN), está constituida gracias a la interconexión de varias redes LAN, este tipo de redes pueden llegar a cubrir geográficamente hasta ciudades enteras sin sobrepasar el ámbito urbano. Se utilizan para enlazar diferentes edificios o campus pudiendo ser estos de la misma organización o diferentes empresas que comparten la misma información, ya que dichas redes pueden ser privadas como públicas. La red MAN tiene una cobertura que no va más allá de los 50 km. Se las puede considerar como una evolución de una red LAN pero en un ámbito mucho más amplio. Por lo cual se trata de una red de alta velocidad cuya cobertura se extiende más allá de una LAN.

2.2.1.3 LAN

Las redes de área local (LAN), se caracterizan por tener una cobertura pequeña, se utilizan para interconectar computadoras y otros dispositivos de red que se encuentran dentro de un mismo campus o edificio con el propósito de permitir la compartición de recursos y el intercambio de información entre ellos. En el caso que hubiere varias redes conectadas entre sí, se mantiene el nombre de red LAN siempre y cuando se encuentren ubicadas dentro del mismo campus o edificio.

Este tipo de redes se caracteriza por tener bastante capacidad, lo cual permite alcanzar grandes velocidades y por ende se puede manejar un tráfico interno

grande. Las redes LAN, se diferencian de las redes de mayor alcance, por pertenecer a una sola empresa o propietario.

2.2.1.4 PAN

Las redes de área personal (PAN), abarcan el rango de una persona. Su cobertura se alcanza a unos cuantos metros. Su uso es común para interconectar dispositivos personales, como, por ejemplo: un terminal o host con sus periféricos. La tecnología más usada es el Bluetooth y ya con muy poco uso el Infrarrojo.

2.2.2 Por el método de conexión

2.2.2.1 Medios guiados

A través de un cable es como conducen las señales desde un extremo al otro. Como características principales de los medios guiados podemos mencionar que son: el tipo de conductor que utilizan, la velocidad máxima de transmisión, las distancias máximas que se puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel enlace.

Los medios guiados se conectan utilizando:

- ✓ Cable trenzado
- ✓ Cable coaxial
- ✓ Cable de fibra óptica

2.2.2.2 Medios no guiados

Son aquellos en los cuales no se utiliza cable, sino que las señales se propagan a través del medio; es decir que no se utiliza ningún medio físico y esta se transmite a través de ondas electromagnéticas:

Los medios no guiados se clasificación en:

- ✓ Radiofrecuencia
- ✓ Microondas
- ✓ Luz (infrarrojo/laser)
- ✓ Bluetooth

2.2.3 Por la relación funcional

2.2.3.1 Cliente-Servidor

Se trata de una red de comunicación en la que los clientes se conectan a un servidor, en dicho servidor es donde se centralizan recursos y las aplicaciones las cuales se ponen disposición de los clientes cada vez que lo requieran.

2.2.3.2 Igual-a-igual

Se habla de una red igual-a-igual cuando la red no tiene clientes ni servidores fijos, esta red se compone de una serie de nodos cuyo comportamiento simultáneo es como clientes y servidores de los demás nodos de la red. Es una red creada con el fin de que sus usuarios pudiesen compartir sus archivos entre sí.

2.2.4 Por topología de red

2.2.4.1 Topología de bus

Es aquella donde el servidor y las estaciones de trabajo se conectan a un único canal de comunicaciones, y por este canal se transmiten todas las señales y los datos permitiendo a las estaciones comunicarse con el resto. La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos.

2.2.4.2 Topología en estrella

La topología en estrella utiliza un dispositivo como un punto de conexión de todos los cables que parten de las estaciones de trabajo. Este dispositivo puede ser un servidor de archivos o un dispositivo especial de conexión. Básicamente las estaciones de trabajo están conectadas directamente a un punto central y todas comunicaciones se han de hacer necesariamente a través de este. Una red formada en estrella tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

2.2.4.3 Topología en anillo

En esta topología las señales viajan por una única dirección a lo largo de un cable en forma de círculo conectando así a las computadoras. Cada estación

tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación. La comunicación en este tipo de red se da gracias al paso de un token, el cual pasa por cada estación recogiendo y entregando paquetes de información evitando pérdidas de información a causa de colisiones.

Con esta topología las redes pueden extenderse a largas distancias, y una avería en algunos de sus cables hará caer el sistema.

2.2.4.4 Topología en malla

Topología en la cual cada nodo está conectado a uno o más de los otros nodos, permitiendo así llevar los mensajes de un nodo a otro por distintas rutas. Si este tipo de red está bien instalada no debe haber ninguna falla en las telecomunicaciones. A diferencia de otras redes, en las redes de malla los nodos o elementos de la red están conectados todos con todos, utilizando cables separados ofreciendo así rutas redundantes por toda la red. En el caso de que un cable falle siempre habrá otro que se haga cargo del tráfico.

2.2.4.5 Topología en árbol

Topología en donde los nodos están colocados en forma de árbol. La conexión en árbol es semejante a una serie de redes en estrella pero no tiene un nodo central sino un nodo de enlace troncal el cual puede ser un hub o switch del cual se ramifican los demás nodos. En el caso de que alguno de estos nodos deja de funcionar la comunicación se interrumpe.

La topología en árbol puede ser vista como una mezcla de varias topologías en estrella.

2.2.5 Direccionalidad de los datos

2.2.5.1 Simplex

Un equipo terminal de datos transmite y otro recibe los mismos.

2.2.5.2 Half-Duplex

Es aquella en la que un solo equipo transmite a la vez. También se la conoce como Semi-Duplex.

2.2.5.3 Full-Duplex

Ambas pueden transmitir y recibir a la vez una misma información, ejemplo: establecimiento de una videoconferencia.

2.3 Red multiservicios

Las redes multiservicios permiten usar una misma red para brindar varios servicios de telecomunicaciones, donde se puede integrar en ella los servicios de voz, video y datos.

El tráfico de datos, voz y video dentro red multiservicios requiere que se realice un trato diferenciado; esto con el propósito de asegurar la calidad del servicio, en base a configuraciones las cuales deben implementar prioridades a estos flujos de tráfico a nivel de todos los elementos de la red, es decir desde el tráfico proveniente de los telefónicos IP hasta el tráfico que pasa por los switches de las diferentes capas de la red.

2.4 Modelo de red jerárquica

Las redes se hacen más predecibles gracias a la jerarquía y sus beneficios. En sí, se definen funciones al interior de cada capa para ayudar a tener un modelo entendible de una red. Una red jerárquica también ayuda a aplicar una configuración de una manera apropiada en redes grandes que pueden ser muy complejas, las cuales incluyen protocolos y tecnologías.

Las buenas prácticas en el diseño de redes recomiendan la utilización de un modelo jerárquico (véase figura 1), el cual consiste en dividir la red en capas independientes: capa de acceso, capa de distribución y capa de núcleo o core. Una red tiene más probabilidades de éxito cuando se utiliza este modelo en la implementación de redes ya que puede expandirse con más facilidad, la administración de la misma es mucho más manejable y por último permite resolver los problemas con rapidez.

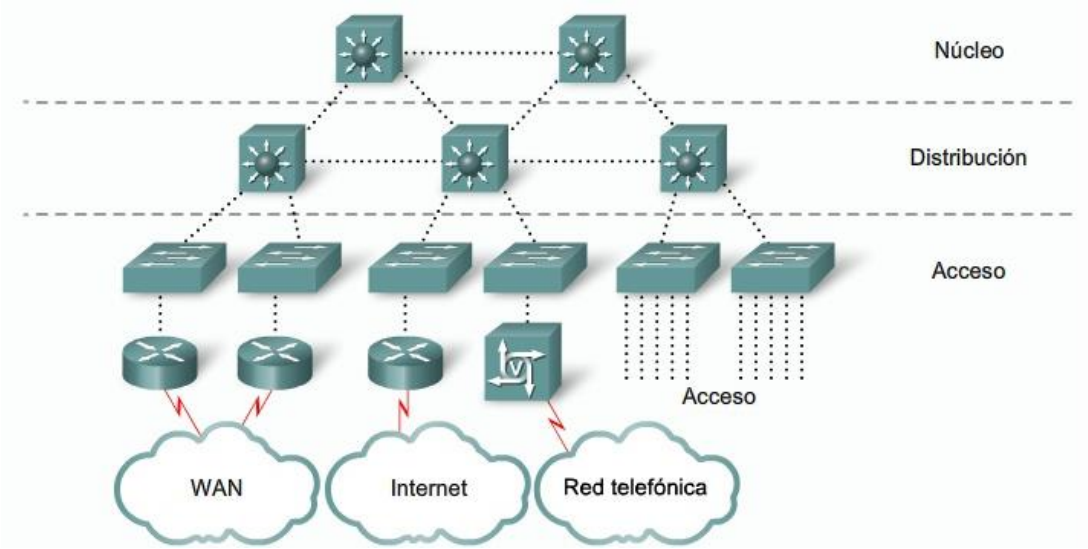


Figura 1. Capas del Modelo Jerárquico

Tomado de: Redes-autoestudio, s.f.

El separar las redes en 3 niveles permite tener ventajas como: diseñar, implementar, mantener y escalar la red más fácilmente, además la red se vuelve más confiable y esto se ve reflejado en la relación costo/beneficio. Funciones específicas se asignan a cada capa de red, se trata de una separación lógica y no física; esto permite disponer distintos dispositivos en una sola capa o un dispositivo podrá hacer las funciones de más de una de las capas.

2.4.1 Capas del modelo jerárquico

Capa de acceso: Esta capa se encarga de interactuar de manera directa con los terminales, host o dispositivos finales. Además, controla el acceso a la red para los grupos de trabajo y los usuarios.

Capa de Distribución: Esta capa intermedia provee comunicación entre la capa de Acceso y la capa de Core, estableciéndose un punto medio entre las dos. La principal función es el enrutamiento, es decir establece la ruta más conveniente a seguir hasta un destino determinado, también otras funciones son: que provee ruteo, acceso a la red WAN y decide que paquetes deben enviarse al Core.

Capa de Core: También conocida como Core Layer o Núcleo de la red se constituye en el backbone de la red, es la encargada de brindar conectividad entre los equipos de la capa de distribución, aquí es donde se realizará el más alto performance ya que debe conmutar grandes cantidades de tráfico en la red de manera rápida pero segura, siendo la velocidad y la latencia factores determinantes en esta capa. Esta capa se convierte en la parte más sensible de la red ya que por su importancia en el caso que existiera alguna falla, los usuarios conectados de la red se verían directamente afectados. Es una capa cuya tolerancia a errores debe ser elevada. Por último, esta capa debe estar en la capacidad de ofrecer redundancia y alta disponibilidad.

2.4.2 Beneficios de una red jerárquica

2.4.2.1 Escalabilidad

Una red que se expande rápidamente con el propósito de permitir nuevos usuarios y aplicaciones no afectando el performance del servicio se denomina red escalable. Este concepto es muy importante a la hora de hacer el planteamiento de una red. Un diseño jerárquico en capas elaborado para la infraestructura resulta ser una base para que la red pueda admitir nuevas interconexiones. El cómo funciona cada capa hace que proveedores y usuarios puedan hacer inserciones de equipos sin causar interrupciones en la red.

2.4.2.2 Redundancia

La disponibilidad toma importancia, a medida que una red va creciendo. Se puede hacer que la disponibilidad de una red aumente mediante la implementación redundante usando redes jerárquicas. Por ejemplo, conectar los switches de la capa de acceso a dos switches diferentes de la capa de distribución con el propósito de asegurar la redundancia de la ruta. En caso de fallar dos switches diferentes de la capa de distribución, el switch de la capa de acceso deberá conectarse automáticamente al otro switch de la capa de distribución. Continuando con el modelo jerárquico de abajo hacia arriba los switches de la capa de distribución se conectan con dos o más switches de la capa núcleo, esta conexión le permite a la red asegurar la disponibilidad de la

ruta si falla un switch del núcleo. (Toro, 2009). Normalmente, si falla un switch de la capa de acceso, quienes perderían conectividad serían los dispositivos conectados a ese switch como tal, el resto de la red funcionaria de forma normal.

2.4.2.3 Seguridad

La red en el caso de estar establecida mediante capas en base al modelo de red jerárquica, resulta fácil el establecer políticas de acceso entre los segmentos de la red, autorizando o implementado restricciones que se basen en protocolos para determinadas áreas, de forma que solo se brinde acceso

Debido a la conceptualización de la red jerárquica y su segmentación resulta fácil establecer políticas de acceso entre los segmentos de la red, de manera que se otorgue solo el acceso a un determinado segmento o segmentos autorizados, implementando restricciones que se basen en protocolos para determinadas áreas.

Con el uso de un modelo jerárquico la seguridad mejora y se hace más fácil su administración. Ejemplo: para proveer un control sobre qué dispositivos se permite conectar a la red a nivel de los switches de la capa de acceso es posible configurar varias opciones de seguridad de puerto. Además, en la capa de distribución es posible utilizar políticas de seguridad más avanzadas. (Toro, 2009)

2.5 VLANs

Una VLAN (LAN virtual), representa un circuito lógico y por medio de ellas se puede agrupar dispositivos o servicios de red, además permite dividir un dominio de broadcast en distintos dominios separados. Su propósito fundamental es disminuir el tráfico broadcast dentro de una red. Para poder realizar esto los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN. En cuanto a la configuración de las VLAN, esta se la efectuará en los switches que están situados dentro de la LAN, las VLANs resultan ser una importante herramienta a la hora de administrar y

asegurar las redes, además de que se puede ofrecer Calidad de Servicio (QoS) estableciendo prioridad del tráfico generado desde las VLANs. (Acurio, 2015)

2.5.1 Ventajas de las VLAN's:

- ✓ **Incrementan el desempeño de la red**

  Reúnen en conjuntos a terminales o host, recursos y servidores según su función, con ello se mejora el poder administrarlos de mejor manera a los mismos, no importa si estos se encuentran en el mismo segmento físico LAN.

- ✓ **Facilidad en la administración**

  En el caso en que se desee adicionar, mover o simplemente cambiar los terminales o host se cuenta con flexibilidad, escalabilidad y facilidad de administración a la hora de realizarlo.

- ✓ **Mejoran la seguridad de la red**

  Solamente los terminales o host que pertenezcan a la misma VLAN se podrán comunicar de forma directa, esto en el caso de trabajar sin enrutamiento.

- ✓ **Facilitan el control de flujo de tráfico**

  Permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un Switch.

  Para configurar o reconfigurar VLAN's se lo realiza por medio de software, por tanto, no es necesario movimientos o conexiones físicas de los terminales de red.

2.5.2 Tipos de VLAN

Existen tres métodos o tipos de VLAN:

- ✓ VLAN por puerto
- ✓ VLAN por dirección MAC
- ✓ VLAN por protocolo

2.5.2.1 VLAN por puerto.

Conocida también como VLAN de nivel 1, es aquella en la cual cada puerto del switch puede asociarse a una VLAN. Cuyas ventajas son:

- ✓ Facilidad de movimientos y cambios.
- ✓ Micro segmentación y reducción de dominio de broadcast.
- ✓ Es multiprotocolo, al no existir limitación en cuanto a los protocolos que pueden ser utilizados, incluso se permite el uso de protocolos dinámicos. (Tipán, 2005).

2.5.2.2 VLAN por dirección MAC

Conocida también como VLAN de nivel 2, su operación consiste en agrupar terminales o host a una VLAN en base a sus direcciones MAC. Se utiliza un servidor de políticas de administración de VLAN'S (VMPS) para realizar la asignación de usuarios a una VLAN con el propósito de que maneje la base de datos de todas las direcciones MAC; es por ello que cuando un usuario se conecta a un puerto de un Switch, éste último, consulta al servidor a que VLAN corresponde este dispositivo, en base a su dirección MAC.

Ventajas

- ✓ **Facilidad de movimientos**. - los terminales o host pueden cambiar o moverse de su ubicación física y estos seguirán perteneciendo a la misma VLAN a menos que se configure lo contrario.
- ✓ **Multiprotocolo**. - no existe ningún inconveniente de compatibilidad con los distintos protocolos y soporta protocolos dinámicos como DHCP.

2.5.2.3 VLAN por protocolo

Su configuración es parecida al método por direcciones MAC, lo único que cambia es que se introducen en el switch las direcciones lógicas de los equipos terminales. No es muy común que se use este tipo de VLAN debido a que en las empresas se implementan servidores DHCP, que son quienes asignan las direcciones IP de forma dinámica a las computadoras.

En base a la información de protocolos de red (por ejemplo, dirección IP o dirección IPX y tipo de encapsulamiento) se realiza la asignación a las VLANs. Finalmente, la pertenencia a la VLAN es realizada en base al uso de filtros aplicados a las tramas. Los filtros se aplican a cada trama que entra por uno de los puertos del switch. (Baxter, 2005).

La ventaja principal al configurar este tipo de VLAN es que el usuario se conectará a la VLAN que le corresponde dependiendo el protocolo que esté usando. (Del valle, 2012).

2.6 Modelo de referencia OSI

La necesidad de tener un estándar el cual permita compatibilidad e interoperabilidad entre equipos de diferentes fabricantes hizo que se creara el modelo de referencia de interconexión de sistemas abiertos.

El modelo de referencia OSI fue desarrollado por la Organización Internacional de Estandarización (ISO).

Se constituye por siete capas y cada capa define sus propias funciones. Véase Figura 2.

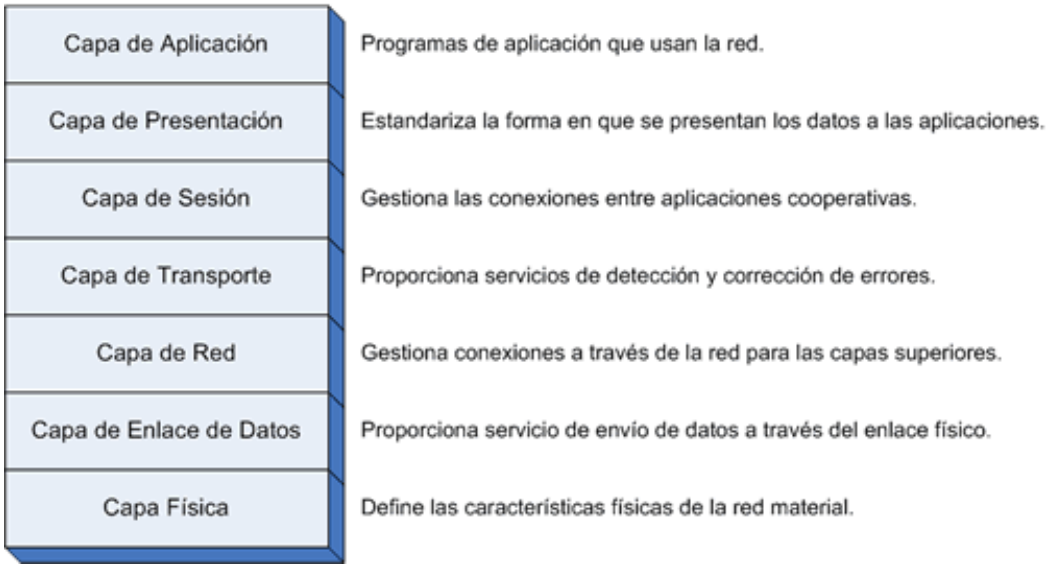


Figura 2. Capas del Modelo OSI

Tomado de: Textoscientificos, s.f.

- ✓ **Capa 1 (Física):** Se ocupa de la transmisión y recepción del flujo de bits a través del medio físico conectado, describe características mecánicas, eléctricas y funcionales. La unidad de información es el bit.
- ✓ **Capa 2 (Enlace de Datos):**
  Es la encargada del acceso al medio de transmisión, se ocupa del direccionamiento físico, control del flujo y de la distribución en forma ordenada de las tramas, proporcionando un enlace seguro de comunicación. La unidad de información es la trama en la que encapsula el paquete recibido desde la capa superior.
- ✓ **Capa 3 (Red):** Esta capa es la encargada de interconectar redes heterogéneas realizando el enrutamiento, conmutación, control de flujo y recuperación de fallas de la capa de enlace. La unidad de información es el paquete.
- ✓ **Capa 4 (Transporte):** Es la encargada de la segmentación de los datos recibidos de la capa de sesión, para ser enviados a la capa red. Esta capa realiza control de flujo entre los dos extremos. Los mecanismos de intercambio de datos extremo a extremo utilizados en este nivel

aseguran que los datos lleguen correctamente a su destino. La unidad de información es el segmento.

- ✓ **Capa 5 (Sesión):** Los usuarios para poder comunicarse necesitan establecer sesiones entre diferentes aplicaciones, esta capa es la encargada de crear dichas sesiones. En el caso de producirse una inconsistencia realiza la sincronización de puntos de comparación y recuperación durante una transferencia de archivos.
- ✓ **Capa 6 (Presentación):** Define el formato de los datos que se van a intercambiar entre las aplicaciones, el servicio que proporciona es el de codificación de datos en modo estándar. Además, realiza funciones de compresión y cifrado. No se interesa en el significado de los datos.
- ✓ **Capa 7 (Aplicación):** Esta capa proporciona la interfaz final entre el usuario y la red, da importancia al significado y no al formato de los datos.

2.7 Modelo TCP/IP

Fue desarrollado por un grupo de investigadores de la agencia gubernamental norteamericana ARPA (Advanced Research Projects Agency) bajo petición del Departamento de Defensa Norteamericana con el propósito de que los sistemas de distintos fabricantes pudiesen comunicarse entre sí, de esta manera por primera vez en diciembre del 69 aparece la denominada ARPAnet. (López, 2011)

TCP/IP cuyas siglas significan “Protocolo de control de transmisión/Protocolo de Internet”. Es el resultado de unir dos protocolos como lo son el protocolo TCP y el protocolo IP.

La Internet TCP/IP son una serie de protocolos que posibilitan la comunicación entre los terminales o hosts, dicho de otro modo, permiten la transmisión de datos en las redes de computadoras, convirtiéndose en la base de la red Internet. Este modelo hace posible direccionar los paquetes de datos desde un origen hacia su destino mediante la utilización de direcciones IP en cada equipo.

El Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP) son los dos protocolos más importantes de este modelo, el cual consta de cuatro niveles o capas como lo son: Aplicación, Transporte, Internet y Acceso de Red. Véase figura 3.

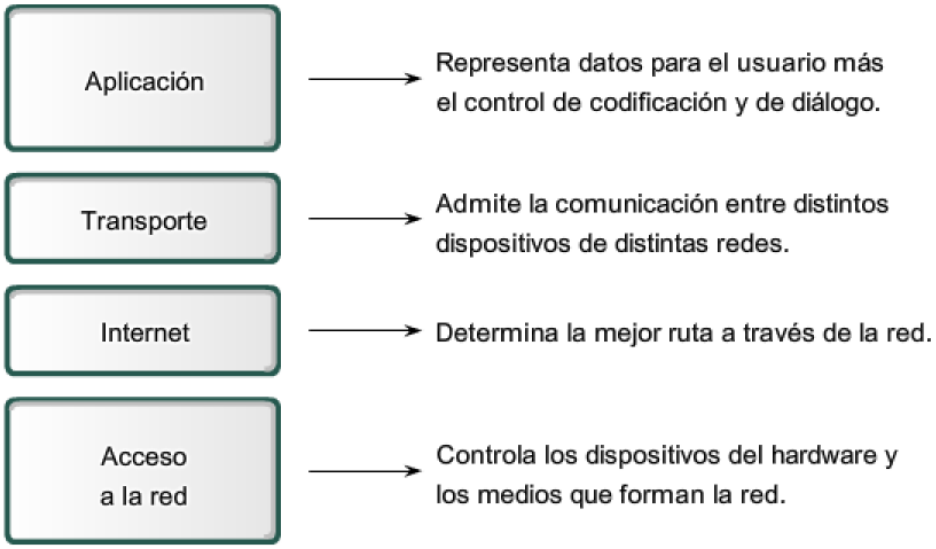


Figura 3. Capas del Modelo TPC/IP
Tomado de: Modelozzy, s.f.

La arquitectura TCP/IP tiene cinco capas:

- ✓ **Aplicación:** Capa que es conformada por un conjunto de protocolos cuya función es proporcionar servicios al usuario, tales como: DNS, SMTP, TELNET, RPC, FTP que permite la transferencia de archivos, y otros como el protocolo HTTP el cual enlaza páginas WWW.
- ✓ **Transporte:** Capa que cumple la tarea de proporcionar la comunicación entre un programa de aplicación y otro, permitiendo que las entidades pares en los nodos origen y destino establezcan una conversación.

  En esta capa se puede brindar un transporte confiable, así como uno no confiable utilizando dos protocolos: TPC y UDP. De los cuales TPC ofrece un servicio orientado a conexión y por lo cual es confiable. El UDP ofrece un servicio sin conexión por lo que se lo denomina no confiable.

- ✓ **Internet:** Su tarea es entregar paquetes de información al destino. Esto implica ruteo de los paquetes y evitar la congestión. En esta capa se accede y encaminan los datos de diferentes redes. Los paquetes viajan de forma independiente dado que es un servicio no orientado a conexión. Este host destino puede estar en la misma red o en una red diferente.
- ✓ **Red:** El funcionamiento de esta capa es similar a las capas físicas y enlace del modelo OSI.

  - o **Acceso a la red**

  También conocida como host de red, se trata de la interfaz de la red real, es la encargada de intercambiar datos entre el sistema final y la red a la cual está conectado.

  - o **Conexión física**

  Es la interfaz física entre el dispositivo que trasmite los datos y el medio de transmisión de red, encargada de especificar características tales como: velocidad de datos, naturaleza de la señal y medio de transmisión.

2.8 Calidad de Servicio (QoS)

La calidad de servicio se la conoce como la capacidad de brindar prioridades de tráfico a cada una de las aplicaciones o servicios con el propósito de otorgar un cierto nivel de rendimiento para las mismas.

Al no aplicarse QoS en una red de datos los datagramas de servicio son enviados por la red de la siguiente forma: El primero en llegar será el primero en ser despachado (*FIFO, First in - First Out*), también conocido como *Best-effort Service*. No se prioriza ningún datagrama y como resultado no se puede diferenciar los datagramas, siendo así propensos a bajar su rendimiento al mezclarse la información que se transporta en la red.

2.8.1 Modelos de Calidad de Servicio

2.8.1.1 Modelo de Servicios Integrados

Se lo conoce también como IntServ, se trata de una arquitectura relacionada estrechamente con el concepto de flujo de información (corriente continua de información creada por un usuario). A nivel de transporte, la dirección y número de puerto identifican un flujo de origen como destino. Dentro de la arquitectura de IntServ se definen los siguientes tipos de servicio:

Servicio garantizado: Existen aplicaciones que demandan de estrictas medidas de calidad por que el servicio garantizado asegura un mínimo desempeño para aplicaciones y servicios de tiempo real.

Servicio de Carga Controlada: Brinda garantías las cuales no son estrictas, por lo cual aquí se pretende alcanzar principalmente un buen tiempo de respuesta.

Servicio Best Effort: No ofrece ningún tipo de garantía.

RSVP: El Protocolo de Reserva de Recursos, es un protocolo de señalización orientado a garantizar la QoS. Pues reserva un ancho de banda en cada uno de los nodos en un determinado flujo. Es utilizado ampliamente en transmisiones multicast. RSVP se utilizada para dos tipos de servicio:

- ✓ **Carga controlada**, aquí la pérdida de paquetes es baja o nula,
- ✓ **Servicio garantizado**, aquí se reserva un mínimo ancho de banda para llevar a cabo el flujo de datos.

2.8.1.2 Modelo de Servicios Diferenciados

Se lo conoce también DiffServ, se caracteriza porque es una tecnología altamente escalable ya que la información de QoS esta descrita en los datagramas, además realiza la reserva de bits para su uso futuro con el objeto de lograr funciones de clasificación y condicionamiento. DiffServ suministra un método que en redes de gran tamaño como Internet intenta garantizar la calidad de servicio. Esta arquitectura es utilizada para brindar calidad de

servicio rápidamente y a diferentes niveles en redes IP y por proveedores de servicio.

2.9 Estándar PCI DSS

2.9.1 Historia

El incremento de transacciones por medio de tarjetas de débito y crédito genero un alto índice de fraudes, obligando a las seis más grandes entidades de tarjetas de pagos (MasterCard, Visa, American Express, Discover y JCB Internacional), que se unieran en el 2004 para crear normas que ayuden a mantener buenas prácticas sobre las transacciones con información dando como resultado la generación de un Consejo de PCI y la creación del estándar PCI DSS.

Pero hoy en día las amenazas han progresado de forma impresionante que mantener actualizado las normas es imperioso, además que debe ser aplicado a todo tipo de entidades que manejen tarjetas de pago como negocios grandes, medianos y pequeños.

2.9.2 Definición

“PCI Data Security Standard (PCI DSS), es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito.” (Auditors, 2007)

2.9.3 Tarjetas de pago

Las tarjetas de uso en el sistema son de débito y crédito y que nos ayudan a realizar consumos mediante transacciones. Llevan información que puede contener almacenamiento permitido y no permitido, a continuación, se ilustra en la siguiente figura:

	Elemento de datos	Almacenamiento permitido
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí
	Nombre del titular de la tarjeta	Sí
	Código de servicio	Sí
	Fecha de vencimiento	Sí
Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No
	CAV2/CVC2/CVV2/CID[4]	No
	PIN/Bloqueo de PIN[5]	No

Figura 4. Almacenamiento tarjeta de pago

Tomado de: Council, s.f.

La información que es de almacenamiento permitido deben ser salvaguardados para que se puedan efectuar fraudes con a nombre del tarjetahabiente.

En la siguiente figura se detallará los componentes de la tarjeta de pago.

Figura 5. Partes de una tarjeta de pago

2.9.4 Para que sirve PCI DSS

Proporciona requisitos técnicos y operativos que una entidad financiera debe cumplir con la finalidad de asegurar, proteger datos de los tarjetahabientes y así fomentar la adopción de este estándar de seguridad a nivel mundial. En la

siguiente figura se puede visualizar de una forma general las normas de seguridad.

Desarrolle y mantenga redes y sistemas seguros.	1.	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.
	2.	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3.	Proteja los datos del titular de la tarjeta que fueron almacenados
	4.	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5.	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
	6.	Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7.	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8.	Identificar y autenticar el acceso a los componentes del sistema.
	9.	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10.	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta
	11.	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12.	Mantener una política que aborde la seguridad de la información para todo el personal

Figura 6. Normas de seguridad de datos de la PCI

Tomado de: Council, s.f.

2.9.5 Campo de aplicación de PCI DSS

PCI DSS se aplica a todas las entidades que almacenan, procesan o transfieren datos del titular de la tarjeta y/o datos confidenciales de autenticación.

Los datos del titular de la tarjeta y los datos de autenticación confidenciales se definen de la siguiente manera:

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

Figura 7. Datos de Cuentas

Tomado de: Council, s.f.

El número de cuenta principal (PAN) define los datos que llevara el titular de la tarjeta de pago, todos los datos de la tarjeta se envían en el PAN, pero siempre deben cumplir los requisitos de seguridad del estándar PCI DSS.

El estándar también se aplica a entidades que tercia rizan el servicio de pago por medio de tarjetas o que manejen el entorno de los datos del titular (CDE), estas instituciones deben asegurarse de proteger los datos.

2.9.6 Alcance de los requisitos de la PCI DSS

Los términos para la seguridad del estándar PCI DSS se utilizan en todos los elementos del sistema incluso en el entorno de datos del titular de la tarjeta.
El CDE (entorno de datos del titular de la tarjeta) se compone de individuos, técnicas y tecnologías que guardan, procesan o envían datos de titulares de tarjetas o datos secretos de autenticación. El término “elementos del sistema” incluye dispositivos de red, servidores, dispositivos informáticos y aplicaciones. Los componentes del sistema incluyen, por ejemplo:

- Sistemas que dan servicios de seguridad, sistemas que facilitan la segmentación o sistemas que pueden afectar la seguridad del entorno de datos del titular de la tarjeta
- Componentes de virtualización e hipervisores.
- Los componentes de red.
- Los tipos de servidores.

Lo primero que se debe realizar para una evaluación del estándar es determinar con precisión el alcance de la revisión. Cada año la entidad a ser evaluada debe poder identificar los flujos y las ubicaciones de los datos del titular de la tarjeta. Además, definir a que sistemas se conectan, si existe riesgo y en que podría afectar los datos del tarjetahabiente.

Para tener claro el CDE (entorno de los datos del tarjeta habiente), se realizara lo siguiente:

- La institución que será evaluada identifica, evidencia, documenta las ubicaciones y existencia de todos los datos del titular de la tarjeta, con el objeto de constatar que no haya datos del titular de la tarjeta fuera del CDE determinado.
- Identificado las ubicaciones de los datos de los titulares de tarjetas, la institución se ayuda de los resultados para comprobar que el alcance de las normas PCI DSS a aplicar sea el apropiado.
- Si la institución encuentra que no todos los datos del titular de la tarjeta están dentro del alcance de la evaluación de las normas PCI DSS y no forman parte del CDE, deberán eliminarse de forma segura y migrar al CDE actualmente especificado para que estos datos estén incluidos. (Council, 2013)

2.9.6.1 Firewall

Para mantener los sistemas y redes seguros en una entidad financiera u organización se debe instalar un firewall con el fin de ayudar a proteger los datos del titular de la tarjeta.

El firewall es un elemento que ayuda a controlar el flujo del tráfico en las redes internas y externas, también maneja el tráfico de áreas donde se guardan información confidencial como por ejemplo el entono de datos de los titulares de tarjetas. El firewall contiene políticas, las cuales se usan para poder bloquear la entrada y salida del tráfico que no cumplen con los criterios de las políticas.

Todos los sistemas que utilizan tráfico de datos deben estar protegidos para que no puedan acceder a la red, manteniendo así una red confiable. Se debe tener en cuenta los ingresos a través del internet como correo electrónico, también del ingreso a través de los computadores de los usuarios finales o empleados, de conexiones dedicadas que pueden ser mediante redes inalámbricas u otras fuentes.

2.9.6.2 Contraseñas y parámetros de seguridad

No se debe usar los valores predeterminados que el proveedor tenga como contraseñas y algunos otros parámetros de seguridad.

Los valores predeterminados que los proveedores utilizan en las contraseñas no son aconsejables debido a que pueden verse afectados los servicios que están en la red que se está administrando, además son valores de uso común en la comunidad de hackers y se han vuelto de información pública.

2.9.6.3 Protección de datos almacenados

Para proteger los datos del titular de la tarjeta y que se almacenan se puede utilizar varios métodos como por ejemplo cifrado, truncamiento, ocultamiento o la función hash. Se utiliza esta protección para que no se pueda visualizar de forma clara, dejando obsoletos el uso de los datos del titular. Siempre es obligatorio usar métodos eficaces que tenga credibilidad para resguardar los datos al momento de almacenar información. La recomendación que se presenta para los datos almacenados del titular es no guardar a menos que sea necesario y al momento del envió no transmitir toda la data sino solo lo que sea de interés.

2.9.6.4 Enmascarar información en las redes.

También se debe cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas. Porque a menudo se ha podido identificar que se realizan malas configuraciones en redes inalámbricas y protocolos de autenticación siendo una inseguridad para que se pueda acceder al entorno de los datos del titular. Él envió o la transmisión de la información de uso privado o confidencial por medio de las redes está sujeta a ataques de delincuentes que pueden acceder a la información, por lo que es indispensable cifrar toda la información.

Un programa de administración de vulnerabilidad protege todos los sistemas contra malware y facilita actualizar los programas o software antivirus regularmente. (Council, 2013)

2.9.6.5 Malware y antivirus

El software que ingresa en la red con un fin malicioso se llama malware o virus, como por ejemplo los troyanos, los gusanos, estos se benefician de la actividad de la red para ingresar mediante correo electrónico o internet y se aprovechan de las vulnerabilidades del sistema. Por este motivo existen antivirus los cuales ayudan a proteger de todo tipo de virus y malware. El antivirus es un software que deberá ser utilizado en los sistemas que estén conectados a la red y así contrarrestar las amenazas a las que se exponen, por lo que también deben ser actualizados debido a que se desarrollan nuevos virus y malware.

2.9.6.6 Aplicaciones y sistemas

El poder desarrollar y mantener sistemas y aplicaciones seguros es sumamente complicado porque existen vulnerabilidades en la seguridad con las que se puede obtener privilegios de acceso a los sistemas. La mayoría de estas debilidades se pueden corregir mediante parches de seguridad que proporciona el proveedor, las instituciones deben instalar los parches indicados para evitar estas vulnerabilidades. Esto evitara que personas mal intencionadas puedan realizar un acceso a los sistemas de los cuales se dispone, donde se puede poner en riesgo los datos del titular de la tarjeta. También se deben verificar que los parches sean certificados por el proveedor y que no creen algún conflicto en las configuraciones de seguridad existentes. (Council, 2013)

2.9.6.7 Control de acceso

Otro tipo de medidas a implementar son las de control de acceso, puesto que restringe el acceso a los datos del titular de la tarjeta tal como lo requiera la empresa, buscando mantener seguro los accesos a los datos de titular de la tarjeta es necesario implementar sistemas que limiten estos accesos mediante privilegios y conforme a la responsabilidad del cargo.

2.9.6.8 Identificación, autenticación y accesos físicos

Asignar una identificación de acceso única a cada persona garantiza que cada uno se hará responsable por lo que suceda con esa identificación. Esto ayudará a que los datos y sistemas críticos estén a cargo de personas

autorizadas, también se hará seguimiento de lo realizado por esta identificación de acceso.

Además, si el sistema permite determinar una contraseña será de mucho más beneficio porque la institución se podrá bazar en los métodos para proteger las contraseñas de usuarios.

“Estos requisitos se aplican a todas las cuentas, incluidas las cuentas de puntos de venta, con capacidades administrativas y todas las cuentas utilizadas para ver o acceder a datos de titulares de tarjetas o para acceder a sistemas con datos de titulares de tarjetas.” (Council, 2013, pág. 74)

Se recomienda restringir los accesos físicos a datos o a sistemas donde se encuentren los datos del titular de la tarjeta para que no se puedan sustraer, cambiar o eliminar dicha información.

2.9.6.9 Inspección y valoración de las redes.

El poder supervisar y evaluar las redes con regularidad es necesario debido a que ayuda a gestionar de mejor forma los recursos de la red, además la existencia de poder rastrear y supervisar las operaciones de los usuarios es complicado, pero ayuda a prevenir, detectar y minimizar las acciones sobre los datos. Existen los registros que son de ayuda en el rastreo y supervisión mediante alertas y análisis las cuales informan si existe un riesgo en los datos del titular de la tarjeta, sin los registros de la actividad del sistema sería muy difícil identificar las acciones de los usuarios.

Otro requisito que presenta la norma es probar regularmente los procesos de seguridad y sistemas sus sistemas.

Probar con frecuencia los sistemas y la seguridad, ayuda a certificar que los controles que se han implementado no han sido vulnerados y que se cuenta con un ambiente seguro, todo esto debido a que personas malintencionadas están constantemente buscando mediante virus o malware ingresar a cualquier sistema o la red, siempre y cuando se mantenga una política de seguridad de información.

2.9.6.10 Políticas de seguridad

Tener una política de seguridad ayuda a que el personal que está a cargo de los datos del titular de la tarjeta tenga la responsabilidad de proteger y mantener la confidencialidad de la información. Así también se usa políticas para empleadores temporales, proveedores, contratistas, consultores que estén en la institución y que tengan acceso a los datos del titular de la tarjeta.

En este apartado se revisa los requisitos de la norma PCI-DSS (https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf).

2.10 ISO-27000

La ISO 27000 es un conjunto de estándares internacionales que proporcionan una gestión de la seguridad de la información (SGSI) que puede ser utilizada por cualquier tipo de entidad privada o pública.

Manejar información es esencial en la actualidad para cualquier organización por lo que mantener segura esta información es el primer objetivo, además hay que manejar una gestión adecuada en la seguridad de esta información, por lo que es necesario implementar métodos que ayuden a minimizar los riesgos que se pueda presentar con el manejo de datos.

2.10.1 Objetivo del estándar ISO 27000

El principal objetivo es definir los requisitos que se deben utilizar para un sistema de gestión de la seguridad de la información (SGSI) y poder certificar los controles de seguridad necesarios manteniendo la protección de la información.

2.10.2 Normas de la ISO 27000

La ISO 27000 contiene las mejores prácticas que se recomiendan para la seguridad de los datos e información y así poder implementar las especificaciones de la norma.

La siguiente tabla muestra las normas en resumen de ISO27000.

Tabla 1.

Normas ISO 27000

Normas ISO 27000	
ISO 27001	Especificaciones para un SGSI.
ISO 27002	Buenas practicas
ISO 27003	Guía de implementación del SGSI
ISO 27004	Sistema de métricas e indicadores
ISO 27005	Análisis y gestión de riesgos
ISO 27006	Especificaciones para organismos certificadores
ISO 27007	Guía para realizar la auditoria
ISO 27011	Gestión del sistema de gestión de la seguridad información (SGSI) en las telecomunicaciones.
ISO 27031	Guía de continuidad del negocio en las tecnologías de la información y comunicaciones.
ISO 27032	Guía de la ciberseguridad.
ISO 27033	“Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNS y diseño e implementación de seguridad en redes” (ISO 27000, 2012)

Tomado de: Logisman, s.f.

2.10.3 Alcance de la norma ISO 27000

Propone una gestión para la seguridad de la información de tal manera que se fomente el cumplimiento de la norma.

La norma no solo se concentra en proteger sistemas informáticos, sino protege cualquier tipo de información sea digital, escrita, etc.

2.10.4 Características de la norma

- ✓ Confidencialidad: característica que tiene la información al momento de ser expuesta a personas no autorizadas.
- ✓ Seguridad de la información: cuidar la confidencialidad, disponibilidad de la información.
- ✓ Sistema de gestión de la seguridad de la información (SGSI): sistema que ayuda implantar, cumplir, monitorear, examinar, conservar y mejorar la seguridad de la información

2.10.5 Introducción al SGSI

2.10.5.1 SGSI (Sistema de gestión de la seguridad de la información)

Es el conjunto de datos que guardan un orden y que son de interés para la organización, indiferentemente del método que se utilice para guardar o transmitir los datos.

En el sistema de gestión de la seguridad de la información, tiene como objetivo preservar la confidencialidad, integridad y disponibilidad, pues es la base para generar la seguridad sobre los datos o información.

2.10.5.2 Para qué sirve un SGSI

Establece procedimientos y políticas en base a los objetivos que se ha planteado la organización, además mantiene un riesgo de nivel bajo. Como la información siempre está bajo riesgo se debe mantener control por medio de definiciones y documentaciones que sean conocidos por todos, para mejorar continuamente.

2.10.5.3 Que contiene el sistema de gestión de la seguridad de la información.

Se ha focalizado la gestión de la seguridad de la información en cuatro niveles de la siguiente forma:

- ✓ **Nivel 1 Manual de seguridad:** Documento que contiene políticas, criterios y lineamientos.
- ✓ **Nivel 2 Procedimientos:** Documentos que contienen un nivel operativo y que certifican que se realicen de forma eficaz los procesos.

- ✓ **Nivel 3 Instrucciones, formularios y checklists:** Documentos que enlista las tareas realizadas y relacionadas con los procedimientos.
- ✓ **Nivel 4 Registros:** Documentos que contienen evidencia física de los eventos realizados y que están enlazados a los otros tres niveles, donde se identifica si se ha cumplido con las normas de seguridad.

2.10.5.4 Implementación del sistema de gestión de la seguridad de la información.

Para realizar la implementación del sistema de gestión de la seguridad de la información se utiliza un ciclo denominado PCA (Plan Do Check Act).

Plan (Como establece el SGSI)

- ✓ Se define el alcance y las políticas de seguridad.
- ✓ Se especifica qué tipo de metodología se utilizará para la evaluación, además de los niveles de riesgo.
- ✓ Se identifica y analiza los riesgos para evaluar su tratamiento.
- ✓ "Seleccionar los objetivos de control y los controles de la norma ISO27000 para el tratamiento de riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo" (Alvarez, 2007).

Do (Implementar y utilizar el SGSI)

- ✓ Definir e implementar el plan de tratamiento de riesgos.
- ✓ Implementar los controles.
- ✓ Sistema que ayude a obtener resultados para evaluar la eficacia de los controles.
- ✓ Oficiar que recursos se utilizaran para el mantenimiento de implementación del SGSI.
- ✓ Realizar controles y procedimientos para una rápida detección y respuesta de los incidentes de seguridad. (Alvarez, 2007).

Check (Monitorizar y revisar el SGSI)

- ✓ Mantener revisado y monitorizado la efectividad del SGSI.

- ✓ Medir la efectividad del cumplimiento de los controles en la seguridad.
- ✓ Tener renovados periódicamente los planes de seguridad.
- ✓ Tener registrado los sucesos y trabajos. (Alvarez, 2007)

Act (Mantener y Mejorar el SGSI)

- ✓ Tener en cuenta que hay que realizar acciones correctivas y preventivas.
- ✓ Mantener una comunicación con todas las partes interesadas de tal forma que se puede tener un buen avance de la implementación.
- ✓ Asegurar que los objetivos mencionados para la implementación lleguen a cumplirse de forma efectiva.

2.10.5.5 Elementos y fases para realizar la implementación del SGSI

La gestión que propone el sistema de gestión de la seguridad de la información sobre la implementación se resume por fases que se detallaran de mejor forma en la siguiente figura.

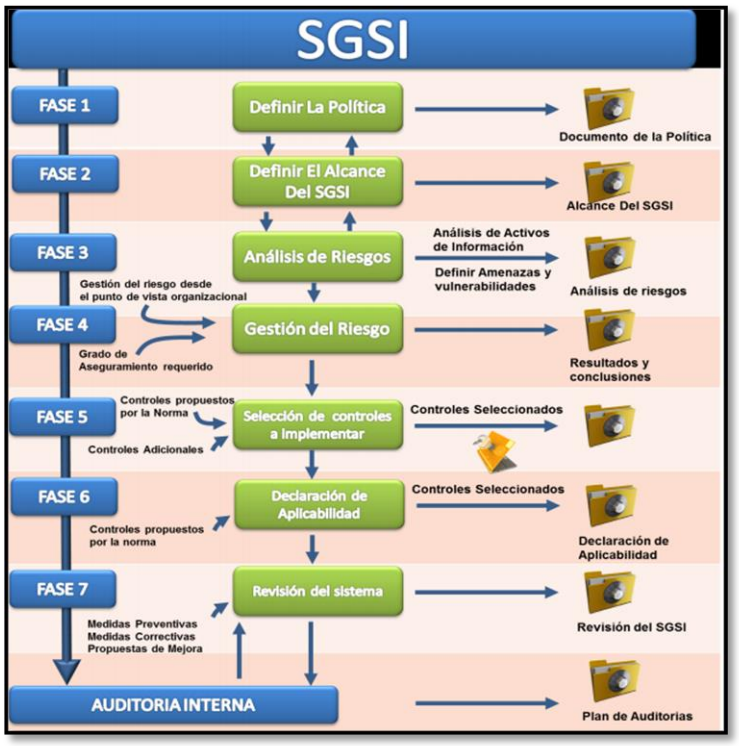


Figura 8. Implementación SGSI

Tomado de: Normas ISO, s.f.

3. SITUACIÓN ACTUAL

3.1 Antecedentes

La Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., con matriz en la ciudad de Quito con ubicación en las calles - Av. Mariscal Sucre S9-543 y Cañarís (La Magdalena) y con presencia a nivel nacional con 34 agencias, es una de las entidades cooperativas más importantes del Ecuador. Enlaza sus agencias mediante una red de datos MPLS con la empresa TEUNO y dispone también de una red de datos interna (LAN) manejada por el departamento de infraestructura y comunicaciones de la institución financiera. Actualmente la institución financiera utiliza la red de datos para brindar a sus socios varios servicios adicionales fuera de los ya tradicionales (depósitos, retiros, inversiones, préstamos), servicios como: el cobro de servicios básicos o el servicio de tarjeta de débito.

3.1.1 Misión

Su misión es: “Ser una Cooperativa de ahorro y crédito que contribuye al desarrollo del país, con productos y servicios financieros oportunos para nuestros socios y clientes con transparencia, responsabilidad y seguridad.”(Coop. 29 de Octubre, 2016)

3.1.2 Visión

Su visión es: “Ser la Cooperativa de ahorro y crédito con mayor cobertura nacional, consolidados entre las tres más grandes del país, promoviendo productos y servicios financieros de calidad con tecnología de punta y responsabilidad social.” (Coop. 29 de Octubre, 2016)

3.1.3 Historia

La Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., se constituyó en la ciudad de Quito, Provincia de Pichincha mediante Acuerdo Ministerial No. 0457 el 15 de mayo de 1972 y fue inscrita en el Registro General de Cooperativas con el número 1330 el 17 de mayo de 1972. Fue autorizada para operar como institución financiera por la Superintendencia de Bancos y Seguros mediante Resolución SB-INCOOP- 99 - 0178 del 29 de septiembre de 1999, resolución debidamente inscrita en el Registro Mercantil, bajo el No. 2855, tomo 130, el 29

de noviembre de 1.999, por tanto, puede realizar actividades de intermediación financiera con el público en general. (Coop. 29 de Octubre, 2016).

3.1.4 Estructura Organizacional

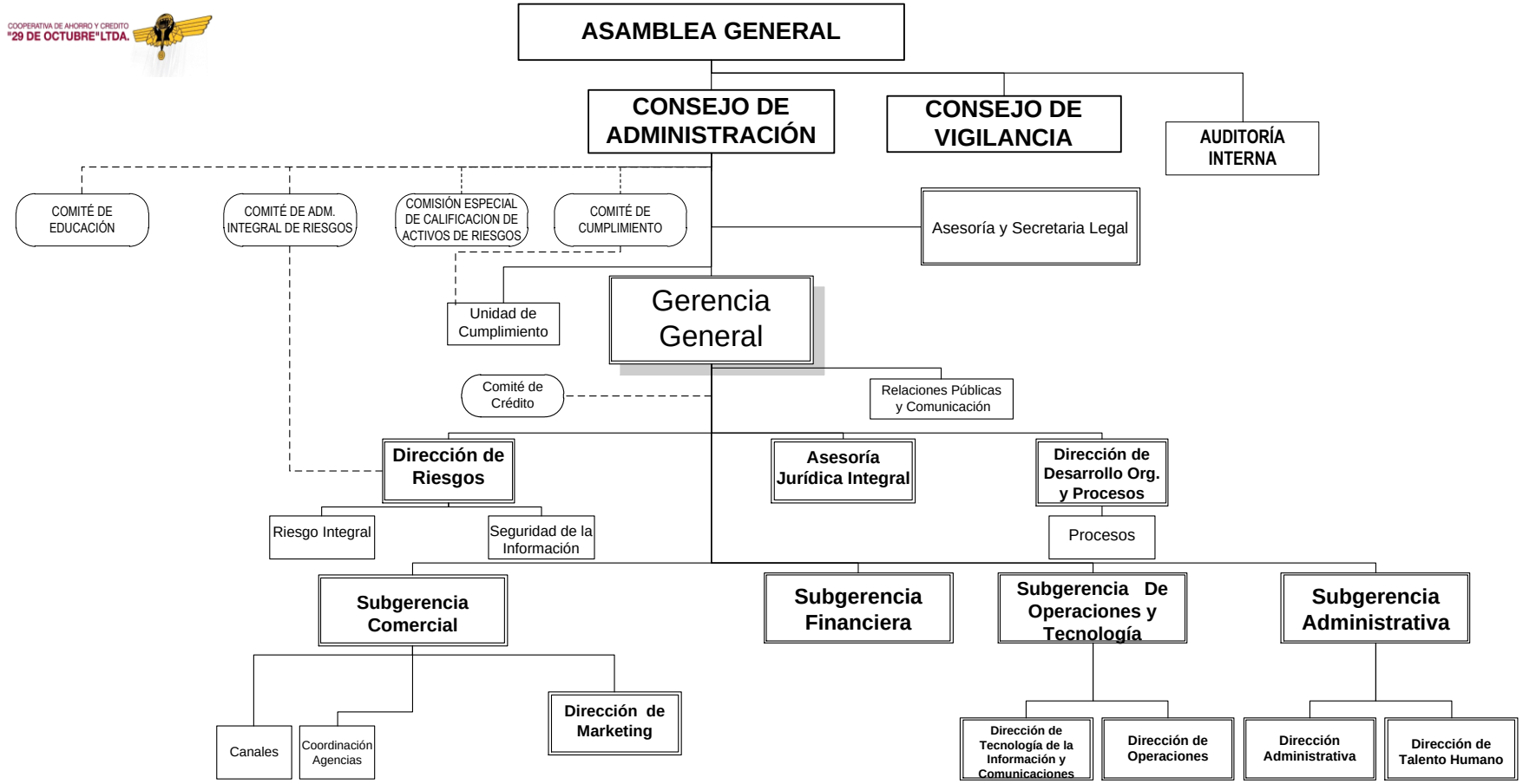


Figura 9. Estructura Organizacional

Tomado de: Cooperativa 29 de Octubre, s.f.

3.1.5 Ubicación Geográfica

3.1.5.1 Edificio Matriz

Actualmente la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., está ubicada en la ciudad de Quito entre las calles Cañarís Oe6-140 y Av. Mariscal Sucre (sector La Magdalena) tal como se puede apreciar en la siguiente figura.

Figura 10. Edificio Matriz

Es un edificio cuya infraestructura consta de cinco plantas y 3 bloques. Con respecto al edificio, la planta baja corresponde al área de Talento Humano y Seguridad, en el (Piso 2) funcionan las oficinas del área Financiera y Administrativa, En el (Piso 3) se encuentran las oficinas de las áreas de Operaciones y Sistemas, seguido se tiene el (Piso 4) donde se encuentran ubicadas las oficinas de Gerencia, Presidencia y el Departamento Legal, en el (Piso 4) se encuentra el salón de eventos. Los planos de planta de la oficina matriz se muestran en el Anexo 1.

Adjunto a la oficina matriz se encuentra el (Bloque B) en cuyas instalaciones desempeñan sus labores el área Comercial y los departamentos de Riesgos, Marketing y Desarrollo Organizacional. Encima del (Bloque B) se ubica el (Bloque A) donde se encuentra el área de Callcenter y Aula Virtual. Finalmente, al fondo de las instalaciones se ubica el (Bloque C) donde se desempeñan las áreas de Custodio, Centro Médico, Auditoría Interna y el departamento de Proceso Industrial de Crédito. Los planos de los bloques de la oficina matriz se muestran en el Anexo 2.

3.1.5.2 Agencias

Existen a nivel nacional 34 agencias distribuidas a nivel del territorio nacional ecuatoriano, a manera de ejemplo se detalla a continuación la ubicación de una de sus agencias. (Véase figura 11).

Agencia San Rafael

Esta agencia se encuentra en el sector de San Rafael, Av. General Enríquez 3113, junto al Colegio San Rafael.

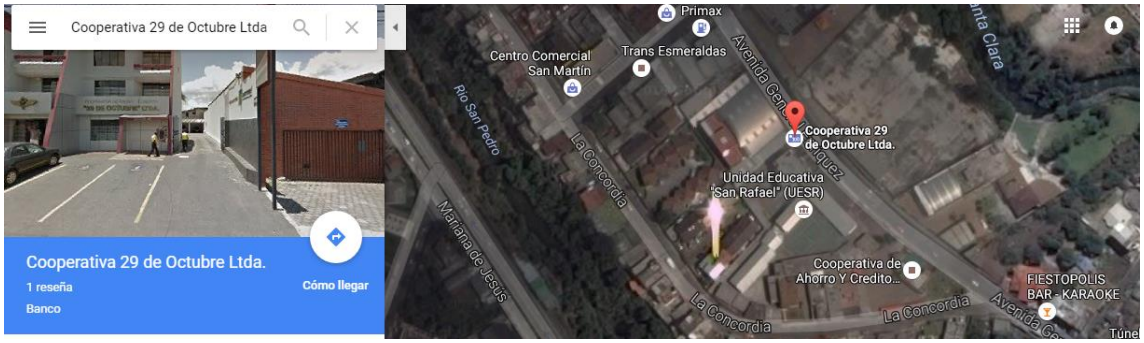


Figura 11. Agencia San Rafael

Al lado izquierdo de la figura anterior se evidencia una infraestructura que consta de dos plantas. En estas instalaciones funciona la atención al público para el sector de San Rafael y el valle de los chillos.

3.2 Red de datos actual de la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda.

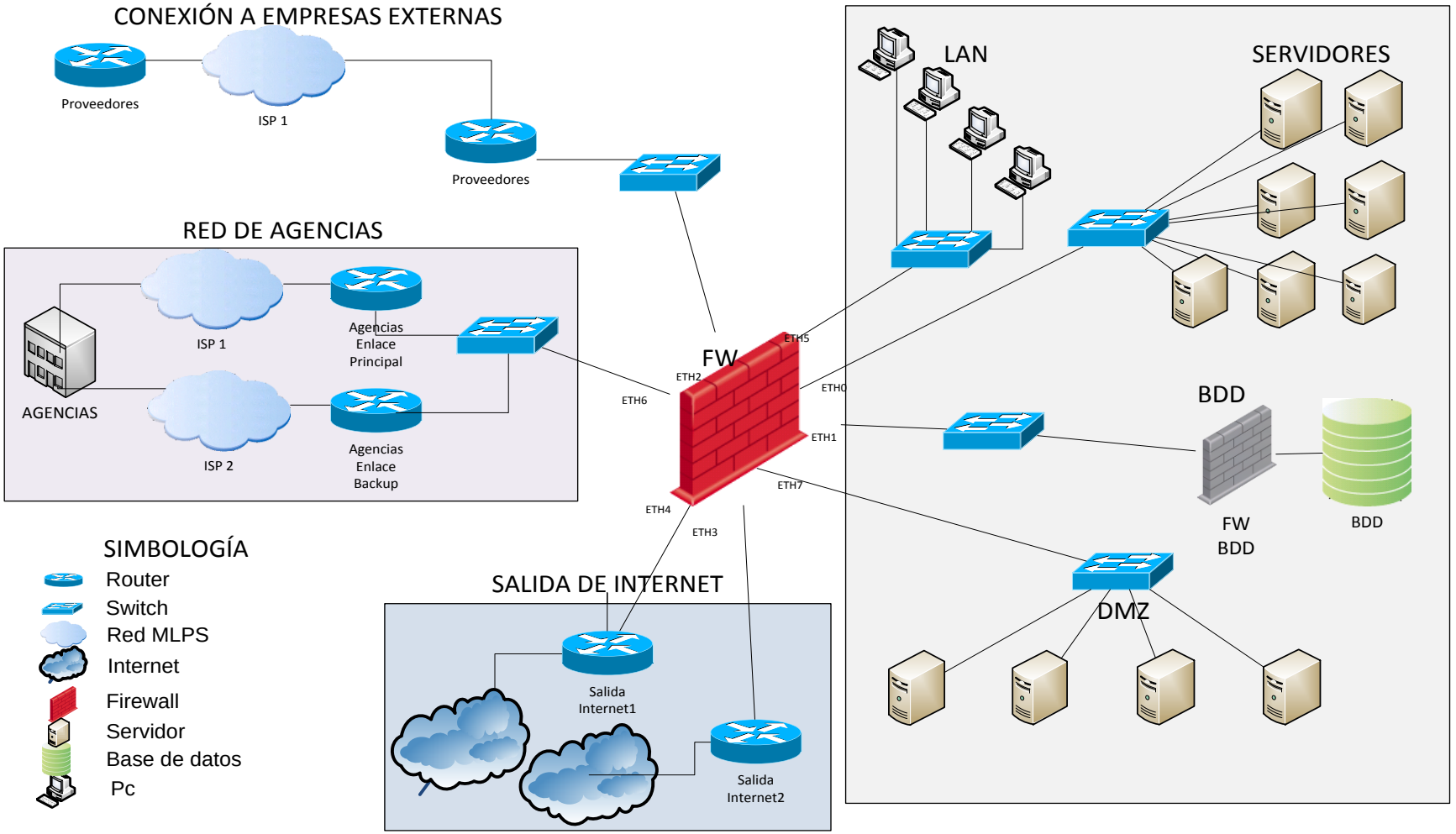


Figura 12. Diagrama de red y comunicaciones

3.2.1 Direccionamiento IP (GLOBAL)

La información en cuanto a las direcciones de red que se mencionan en este documento no son exactas debido a que se trata de tan solo una aproximación para preservar la confidencialidad de la información (véase tabla 2).

Tabla 2.

Direccionamiento IP actual (GLOBAL)

EDIFICIO MATRIZ	
Dirección de red	**Prefijo**
118.16.0.0	/24
Servidores	
192.168.80.0	/24
Impresoras	
192.168.90.0	/24
Cámaras IP	
192.168.100.0	/24
Teléfonos IP	
192.168.110.0	/24
Agencia San Rafael	
118.17.0.0	/24

3.3 Diagramas de la topología física y lógica

El estudio de la red actual de la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., se lo va a realizar tanto para Edificio Matriz, así como para una de sus agencias, se menciona solo una de sus dependencias debido a que la infraestructura y equipos de cómputo en las demás agencias se enlazan de la misma forma con la matriz.

3.3.1 Oficina Matriz

La red local de la oficina matriz trabaja sobre una topología de tipo estrella (véase Figura 12), el cableado instalado es de categoría 6A el cual alcanza

velocidades máximas de 10 Gbps. El cableado es de par trenzado y está implementado tanto para el subsistema horizontal como para el backbone, recorre las instalaciones por canaletas plásticas desde el cuarto de equipos hasta cada uno de sus nodos. La red de datos de la institución cuenta con switches en cada piso y bloques. Los switches se albergan en los gabinetes de telecomunicaciones (véase Figura 13).


,

Figura 13. Gabinete de comunicaciones

3.3.1.1 Cuarto de comunicaciones

El cuarto de telecomunicaciones o Data Center se encuentra ubicado en el segundo piso de la oficina matriz, que consta de cinco racks de 36 UR (Unidades de Rack); un sistema de enfriamiento y condiciones climáticas favorables que están entre los 18 y 24 grados centígrados, garantizando el buen desempeño de los equipos como servidores y equipos activos, además apegándose a la normativa ANSI/TIA/EIA-569.

Desde este cuarto de telecomunicaciones se realiza la distribución hacia todos los nodos de la oficina matriz y otros bloques, en la Figura 14 se puede visualizar la distribución de los bloques y donde se encuentra ubicado el Data Center.

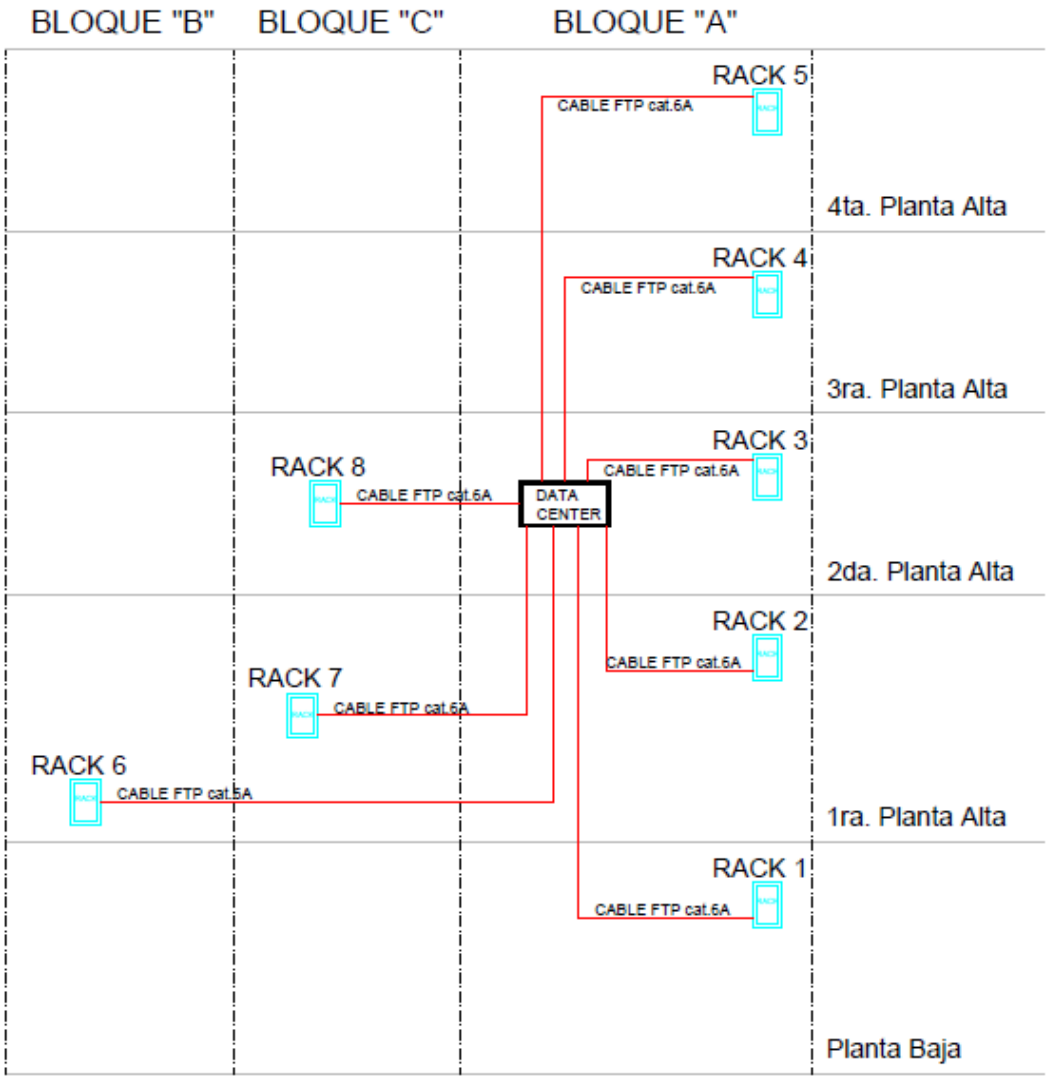


Figura 14. Diagrama unifilar Edificio Matriz y bloques A, B y C.

Tomado de: Cooperativa 29 de Octubre, s.f.

3.3.1.2 Backbone de Datos

Los switches ubicados en los gabinetes de telecomunicaciones de la planta baja hasta el quinto piso, se interconectan en topología tipo estrella con el switch de core del segundo piso ubicado en el cuarto de equipos, enlazándose mediante fibra óptica. Además, se utiliza canaletas metálicas para el transporte de los cables entre las salas de comunicaciones y punto de demarcación del cuarto de telecomunicaciones (véase Figura 15).

Figura 15. Canaletas metálicas para el transporte de los cables

3.3.1.3 Acometida de Servicios

El punto de demarcación de servicio telefónico está situado en la segunda planta, mismo que es provisionado por la CNT (Corporación Nacional de Telecomunicaciones) (véase Figura 16).

La cooperativa a nivel de enlaces de datos e Internet su servicio es redundante, debido a que contrata sus enlaces principales de la oficina matriz y agencia con la empresa de telecomunicaciones TE UNO, mientras que sus enlaces backup los ha contratado con la empresa PUNTO NET, siendo su punto de demarcación de ambas empresas ubicado en el segundo piso de la oficina matriz.

La institución tiene contratado un servicio corporativo de Internet cuya capacidad es de (30 Mbps), mismo que es para uso del correo en la nube (Office 365) y otras aplicaciones de segundo orden como: Youtube, Hotmail, Yahoo, etc. Mientras que la capacidad del enlace de datos contratado que prioriza el tráfico del Core Bancario es de 120 Mbps desde la oficina matriz hacia el ISP.

En cuanto a los enlaces de datos hacia las agencias, el servicio que se tiene contratado es de (2Mbps) por agencia.

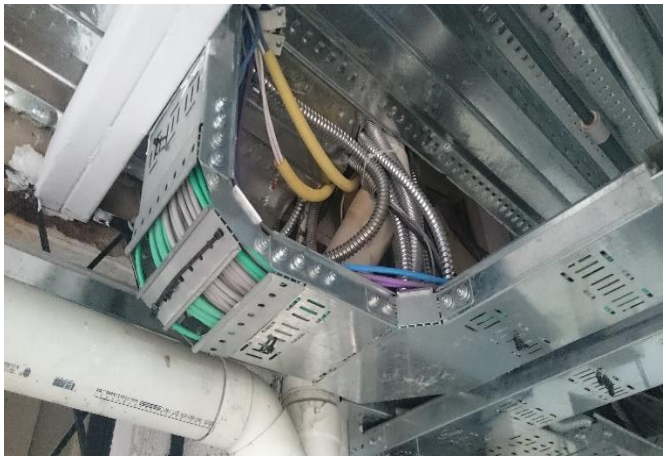


Figura 16. Acometida de servicios

3.3.1.4 Tráfico de datos

El monitoreo del tráfico de red se lo realizó mediante la utilización de dos programas cuya licencia es software libre.

El primer software utilizado es Zenoss, el cual se instaló y se lo puso en funcionamiento conectándolo para red de la oficina matriz, se lo instaló en una máquina virtual utilizando Vmware Player, esto con el propósito de monitorear el tráfico a nivel LAN en las interfaces del switch de core.

Figura 17. Software Zenoss

Tomado de: Zenoss, s.f.

La cooperativa a nivel del switch de core tiene dividido el tráfico a través de 2 VLANs, la primera corresponde a la red LAN del edificio matriz y la otra administra los servidores de la institución. Se ha sumado el trafico agrupando

las interfaces del switch y el resultado del monitoreo se muestra a continuación. Por seguridad de la información los nombres reales no se dan a conocer y se utilizan 2 nombres genéricos.

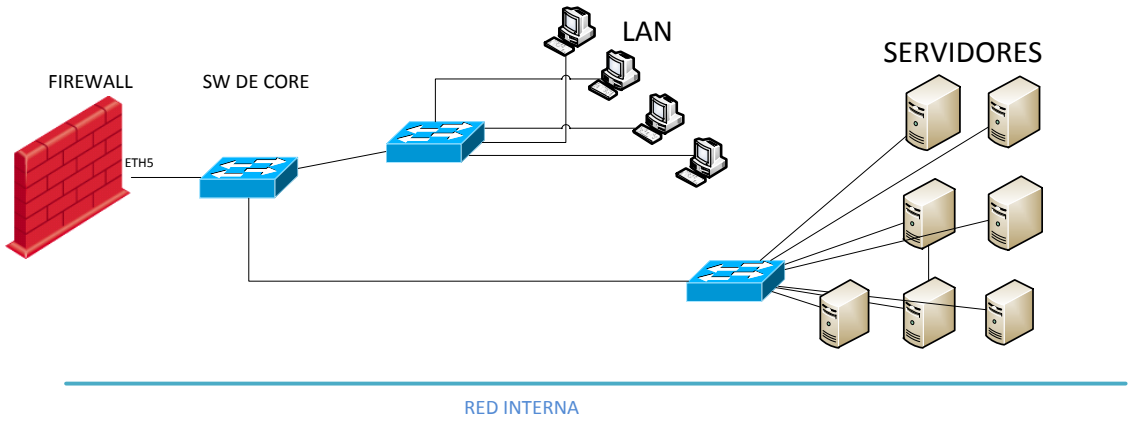


Figura 18. Tramo de red monitoreado por el software Zenoss

Tabla 3.

Carga de utilización promedio del switch de core por VLANs.

VLAN	DESCRIPCIÓN	CONSUMO PROMEDIO EN LA INTERFAZ DE ENTRADA (Kbps)	CONSUMO PROMEDIO EN LA INTERFAZ DE SALIDA (Kbps)
VLAN 1	Servidores	36305.86	55697.58
VLAN 2	Red de oficina matriz	89436.75	70767.94
	TOTAL DE TRÁFICO	125742.61	126465.52

La tabla anterior muestra el tráfico promedio en el switch de core, calculado durante un monitoreo realizado por 72 horas, se monitoreó las interfaces del switch que están asociadas a las VLANs tanto de servidores como de la red de la oficina matriz.

El segundo software es Jperf en su versión 2.0.2, con este software se realizó la medición de ancho de banda que la red de la oficina matriz soporta a nivel de la red LAN (véase Figura 19), la principal ventaja de este software es que es portable, es así que se lo ejecutó en dos máquinas de la red para usarlo como servidor en una de ellas y en la otra como cliente.

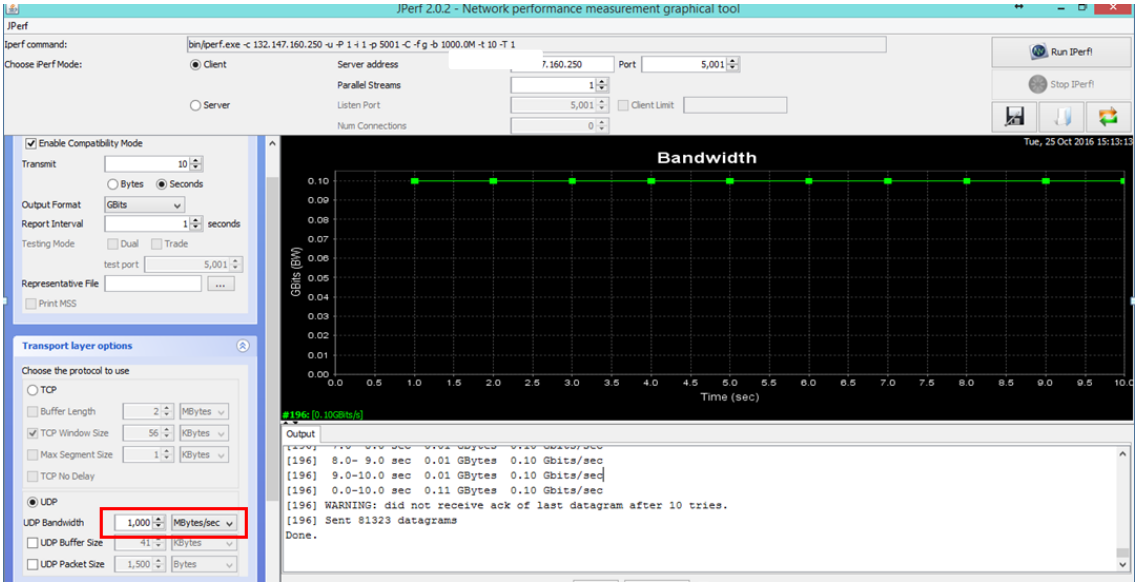


Figura 19. Tráfico de red soportado en oficina matriz.

Como se pude evidenciar en la gráfica anterior, en color verde se muestra que la red de la oficina matriz soporta el tráfico de 1 Gbps generado por el software Jperf, sin embargo, la velocidad real de transferencia de un archivo es en promedio de 95.4 como lo muestra la figura 20. Esto se debe a que la tarjeta de red del computador soporta velocidades de 10/100 Mbps y no 10/100/1000 Mbps.

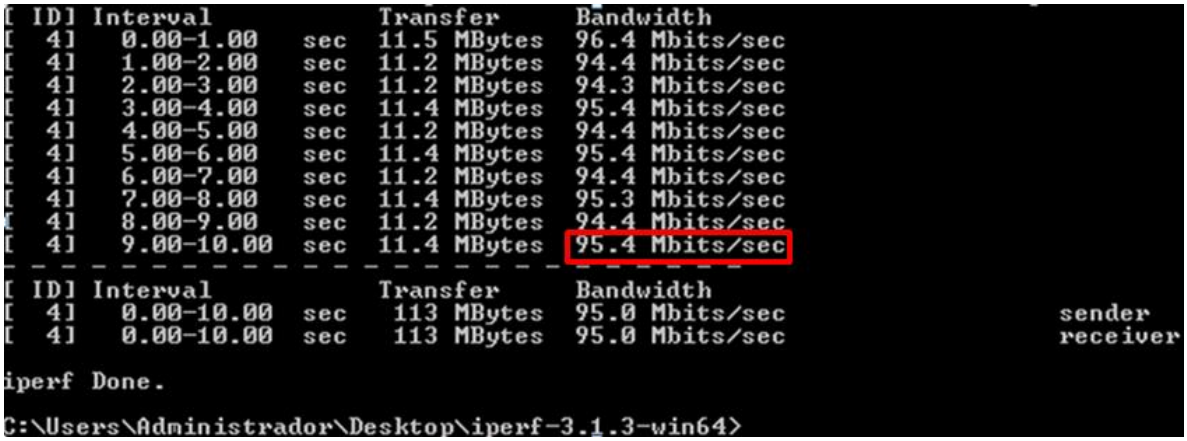


Figura 20. Transferencia de archivos entre dos PCs utilizando Jperf

3.3.1.5 Ancho de banda de Internet contratado

La cooperativa tiene contratado 30 Mbps con su proveedor de servicios de internet principal (con la empresa TE UNO), a manera de ejemplo en la figura 21 se muestra la medición realizada vía web del servicio de internet principal. Mientras que el servicio de internet backup de 7 Mbps se lo contrata a la empresa Punto Net. Los dos servicios de internet se encuentran centralizados en la oficina matriz, conectados cada uno a una interfaz del firewall.

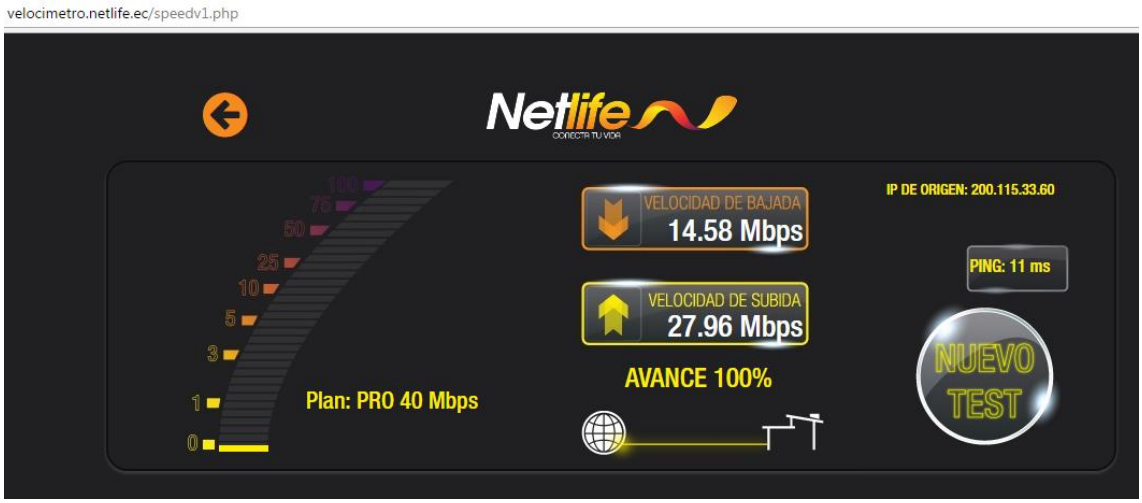


Figura 21. Medición del ancho de banda de Internet principal.

3.3.1.6 Monitoreo a la base de datos

Mediante la utilización del software “Topas Monitor”, se realizó el monitoreo de la base de datos con el objeto de identificar el consumo por transacción realizada.

La figura 22 en el campo Network refleja el consumo de ancho de banda de total de 1.43 Mbps, el campo Runqueve indica 5 usuarios generando este ancho de banda, por lo que una consulta seria de 300Kbps desde el aplicativo Core Bancario.

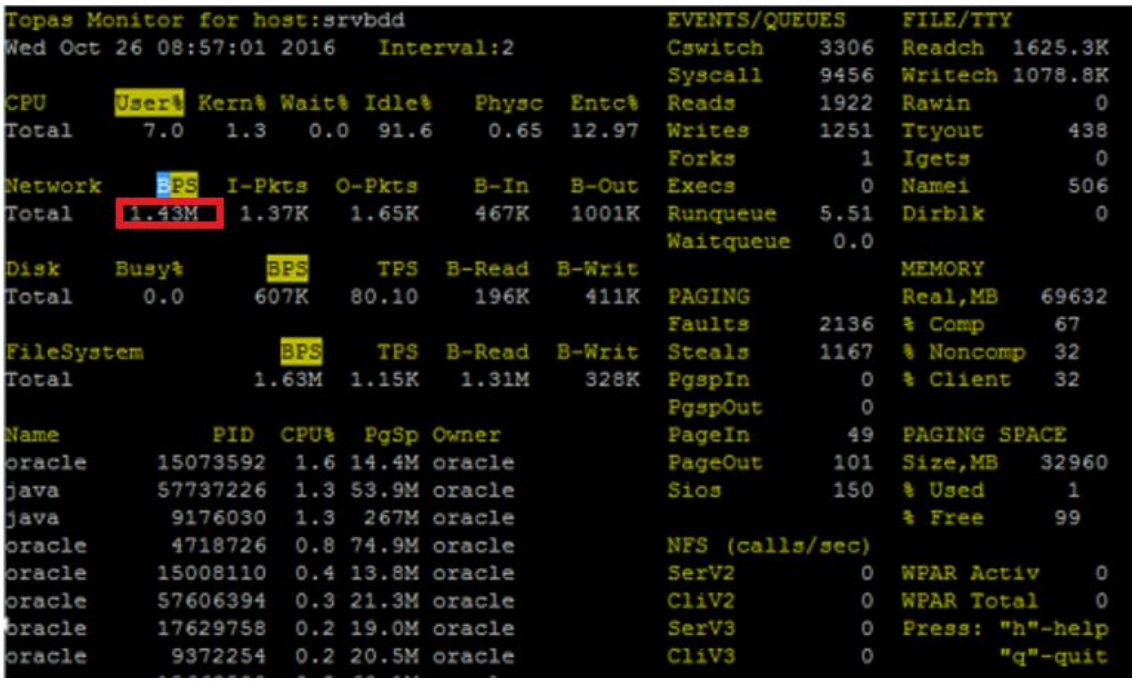


Figura 22. Monitoreo de la base de datos

3.3.1.7 Direccionamiento IP

En el edificio Matriz se tiene un esquema de dimensionamiento fijo y dinámico a nivel de la LAN y WLAN respectivamente para los terminales o host, en cuanto a los servidores se tiene configurado una IP fija en cada uno de ellos.

La dirección de red establecida es la 118.16.0.0 con máscara 255.255.0.0, esta dirección de red es usada para todos los terminales o host, mientras que para los servidores su direccionamiento es 192.168.80.0 con mascara 255.255.255.0.

3.3.1.8 Red Telefónica

Se dispone de una red telefónica interna de VoIP (voz sobre un protocolo de internet) y telefonía analógica, esto debido a que actualmente se está migrando a telefonía VoIP con la compra e instalación de centrales telefónicas IP basadas en Asterisk.

En el edificio Matriz y en nueve agencias de la institución se tiene instaladas centrales telefónicas IP; en cuanto al resto de agencias se maneja telefonía IP con la ayuda de un Gateway para facilitar la comunicación por IP entre agencias. Cabe mencionar que en cada agencia se dispone de una central telefónica análoga de marca Panasonic cuya función es la de un PBX la cual dispone de tres entradas para líneas analógicas como mínimo (véase Figura 23).

Una de las entradas de línea se conecta al Gateway de voz, para permitir la interconexión de telefonía IP a otras agencias.

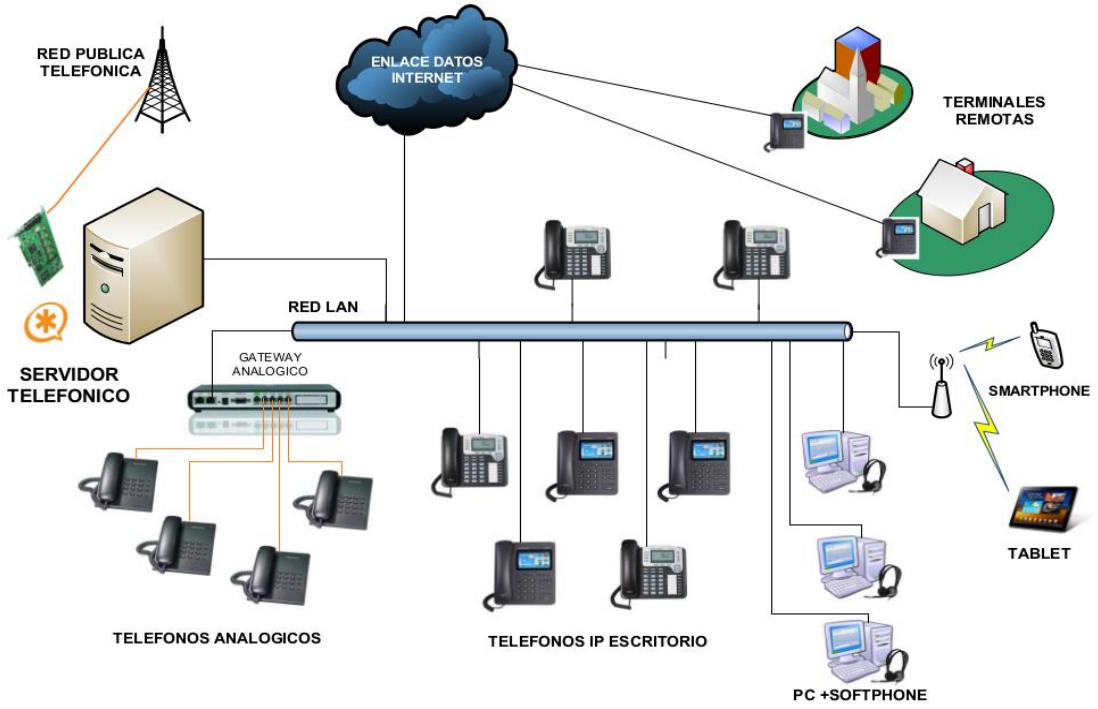


Figura 23. Diagrama de telefonía IP

Tomado de: (Aguilar, 2015)

3.3.1.9 Equipamiento informático de la red

La información de marca, modelo y sistema operativo en cuanto a los equipos de cómputo y servidores ha sido omitida para este documento por confidencialidad de la misma (véase tabla 4).

Tabla 4.

Resumen de equipos de cómputo

	COMPUTADORES	SUBTOTAL
EDIFICIO MATRIZ	190	190
AGENCIAS	350	350
	TOTAL	**540**

3.3.1.10 Servidores

A continuación, se detalla los servidores en términos generales que actualmente tiene en funcionamiento la institución financiera (véase tabla 5).

Tabla 5.

Servidores Datacenter

NOMBRE DEL SERVIDOR	FUNCIÓN DEL SERVIDOR
Active Directory	Control de usuario
CENTRAL IP	Voz IP
BALANCEADOR	Balanceador de aplicativos web
CORE APP1	Core Bancario
CORE APP2	Core Bancario
IBM720	Base de Datos
IBM750	Base de Datos
FILTRO	Firewall
IMPERVA	Firewall de Base de Datos

3.3.1.11 Sistema de Video Conferencia

Del total de agencias a nivel nacional, tan solo 18 de ellas cuentan en sus instalaciones con un sistema de video conferencia de la marca AVER, el cual se compone de una cámara (Estática y giratoria de 360°) véase figura 24, las cámaras antes mencionada se conectan a la red de datos de forma alámbrica.

Figura 24. Equipos de videoconferencia

Con este sistema de videoconferencia se puede conectar en simultaneo 8 agencias desde la oficina matriz.

3.4 Aplicaciones y servicios

3.4.1 Aplicaciones

3.4.1.1 Administración de la red

La administración de la red se la realiza mediante la utilización del protocolo SNMP el cual facilita el poder intercambiar información de administración entre dispositivos de red para enviarla al servidor denominado Pandora (software libre).

3.4.1.2 Monitoreo de la red

El monitoreo de la red a nivel WAN es realizado gracias a la ayuda del proveedor de servicios de internet (TE UNO), el cual facilita la herramienta web demonida Cacti para la verificación del estado de los enlaces de datos e internet contratados. Y a nivel a LAN se dispone del aplicativo Whatsup Gold el

cual es un software gratuito de monitoreo de redes y servidores con el cual se conoce la salud de los mismos.

3.4.1.3 Seguridad de la red

Antivirus Eset

En cuanto a seguridad de antivirus para dispositivos finales se dispone de un servidor de antivirus con la marca Eset y su producto ESET Internet Security.

Firewall de base de datos

Imperva es la marca del servidor que dispone actualmente la cooperativa para brindar la seguridad, realizar auditoria del acceso y para proveer de protección en tiempo real contra los ataques de las bases de datos.

3.4.2 Servicios

La Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., centraliza sus servidores y tráfico de red desde su edificio matriz hacia todas sus agencias con el propósito de establecer comunicación con sus aplicativos y demás servicios demandados por colaboradores y socios. A continuación, se detallan los servicios que se brindan actualmente desde la matriz hacia sus agencias:

- ✓ Core Bancario o servidor de aplicaciones el cual sirve para realizar las transacciones bancarias que los socios requieren a diario.
- ✓ Sistema de video conferencia, el cual utiliza los enlaces backup de 18 agencias para permitir la comunicación de 18 equipos de audio y video (uno por agencia), mismos que fueron distribuidos por regiones (entiéndase por regiones la unión de una o más agencias) a nivel nacional.
- ✓ Voz sobre IP que interconecta todas las agencias ya sea con centrales digitales o mediante la utilización de Gateway de voz.
- ✓ Aplicativo de correo electrónico Office 365, mismo que tiene 2 tipos de acceso: vía web y vía configuración del cliente de correo Outlook.

También se dispone de aplicativos que ofrecen servicios a los socios, dichos aplicativos se conectan desde la cooperativa hacia las empresas externas, ejemplo:

- ✓ Conexión vía web con servicios del Banco Central de Ecuador.
- ✓ Conexión con servicios de BAND RED.

En cuanto a los servicios que brinda la institución, se expone a continuación la estructura actual por capas de la red de la cooperativa tomando como referencia el modelo jerárquico de CISCO.

A nivel de capa de Acceso

Por cada piso y bloques del edificio matriz se dispone de switches de acceso que interconectan los diferentes dispositivos finales.

A nivel de capa de Distribución

No se evidencia equipos que estén configurados y trabajando en este nivel.

A nivel de capa de Core

Se dispone de un switch de core el cual soporta todo el tráfico de la red proveniente de la capa de acceso y servidores. En esta capa es donde actualmente se han configurado VLANs de voz y datos. Además, se centraliza la comunicación hacia los servicios finales como las conexiones hacia el exterior, ejemplo: la conexión al servidor de correo Office 365 y empresas afines.

4. REDISEÑO DE LA RED

4.1 Visión general

En el presente capítulo se realizará un nuevo diseño para la red de datos de la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., incluyendo sus agencias de operación, tomando como punto de partida el análisis de la situación actual del capítulo dos.

Se llevará a cabo en base al análisis de tráfico de datos realizado anteriormente en el punto 3.3.1.4, los cálculos para determinar el ancho de banda requerido para cada uno de los servicios de:

- ✓ Core Bancario o servidor de aplicaciones.
- ✓ Sistema de video conferencia.
- ✓ Voz sobre IP.
- ✓ Correo electrónico Office 365.

Para el dimensionamiento de la red multiservicios y sus aplicaciones se lo realizará considerando parámetros de redundancia y gestión mediante la utilización del modelo jerárquico por capas sugerido por CISCO.

Finalmente, se mostrará un diseño de red de alta disponibilidad considerando la seguridad según el estándar PCI–DSS y bajo la referencia del estándar ISO 27000.

4.2 Determinación de requerimientos

Esta parte es primordial para el diseño de la red multiservicios, puesto que es necesario tomar en cuenta que la red sea segura, confiable, este disponible y sea tolerante a fallos, permitiendo que se pueda garantizar el correcto funcionamiento de la red.

4.2.1 Requerimientos de datos

En cuanto a las necesidades que se requiere para cumplir con el buen performance de las aplicaciones y servicios dentro de la red multiservicios, tenemos que se debe:

- ✓ Calcular el ancho de banda necesario para el correcto funcionamiento del correo institucional Office 365.
- ✓ Conocer cuánto ancho de banda es necesario para el acceso WEB de los usuarios.
- ✓ Establecer mediante cálculos el ancho de banda para el acceso a la base de datos desde el aplicativo Core Bancario.
- ✓ Saber la demanda de ancho de banda para la descarga de archivos.

4.2.2 Requerimientos de voz

Se utilizará la tecnología VoIP, por lo cual se requiere dimensionar el ancho de banda a utilizar al establecer VoIP.

4.2.3 Requerimientos de video

El servicio de videoconferencia hoy en día es vital dentro de la institución financiera por las ventajas que presenta al permitirle a la cooperativa reducir a cero los gastos de movilización de su personal en el caso de capacitaciones, es por ello requiere:

- ✓ Determinar el ancho de banda necesario para el sistema de video conferencia sea de óptima calidad.

4.2.4 Determinación de Tasa de crecimiento de la red

En los últimos diez años la cooperativa tuvo un crecimiento en su red de datos de alrededor de un 30%. Este proyecto determina que con el objeto de lograr una solución que satisfaga las necesidades de la institución y su crecimiento, es que es necesario tomar en cuenta este factor. Para el fin conjuntamente con el personal de tecnología se estima que: la cooperativa demandará un crecimiento del 30% en un futuro de diez años.

4.2.5 Selección del modelo de la red

Con respecto al modelo jerárquico de CISCO el cual será tomado como referencia para el rediseño de la red la cooperativa tenemos que:

A nivel de capa de Acceso

En esta capa no se evidencia el establecimiento de un filtro de comunicación con la red, como por ejemplo: proteger a nivel lógico los puertos de los switches ubicados en cada piso bloque o agencia. O un filtro de acceso de redes virtuales VLANs.

A nivel de capa de Distribución

La red de la institución financiera no cuenta con una segmentación de red, es decir la red actual no se constituye en subredes.

No se evidencia la unificación de los datos recibidos de la capa de acceso antes de que estos sean transmitidos a la capa de núcleo.

En este nivel se debería segmentar el tráfico y dominios de broadcast a través de la creación de VLANs.

Es en esta capa donde se debería proveer el enrutamiento, filtrado con políticas y control de acceso para los datos provenientes de la capa inferior, mediante la utilización de VLANs, o el uso de reglas de tráfico que se puede implementar.

A nivel de capa de Core

La cooperativa no dispone de redundancia a nivel de switch de core al contar con tan solo un conmutador en este nivel, mismo que soporta actualmente todo el tráfico de red, es decir, en caso de falla del switch de core la conectividad de la cooperativa sería nula si llegase a fallar dicho equipo.

En definitiva, la red de la institución no sigue un modelo jerárquico, el cual es importante ya que dividir la red en secciones permite diagnosticar con mayor exactitud el origen de alguna falla en caso de existirla.

Finalmente, la institución financiera necesita conocer cuáles son los requisitos de seguridad de la norma PCI DSS que ha cumplido y cuales debe cumplir

para que la información de tarjetas de crédito se pueda transmitir de forma segura dentro de la red empresarial.

4.2.6 Selección de la tecnología de la red

Puesto que la red de la institución debe soportar la transmisión de datos a altas velocidades, además de disponer de aplicaciones de tiempo real como: telefonía IP y videoconferencia, se concluye que; el flujo de información que circula por la red demanda de una conexión de tipo Gigabit-Ethernet para la interconexión a nivel las distintas capas del modelo jerárquico.

4.3 Topología de red

El diseño de la red multiservicios para la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., estará basado en un modelo jerárquico, el cual consta de tres capas o niveles: acceso, distribución y núcleo.

4.3.1 Diseño del modelo jerárquico por niveles

La figura 25 muestra un ejemplo de la topología de red a ser diseñada en el presente capítulo en base al modelo jerárquico por niveles.

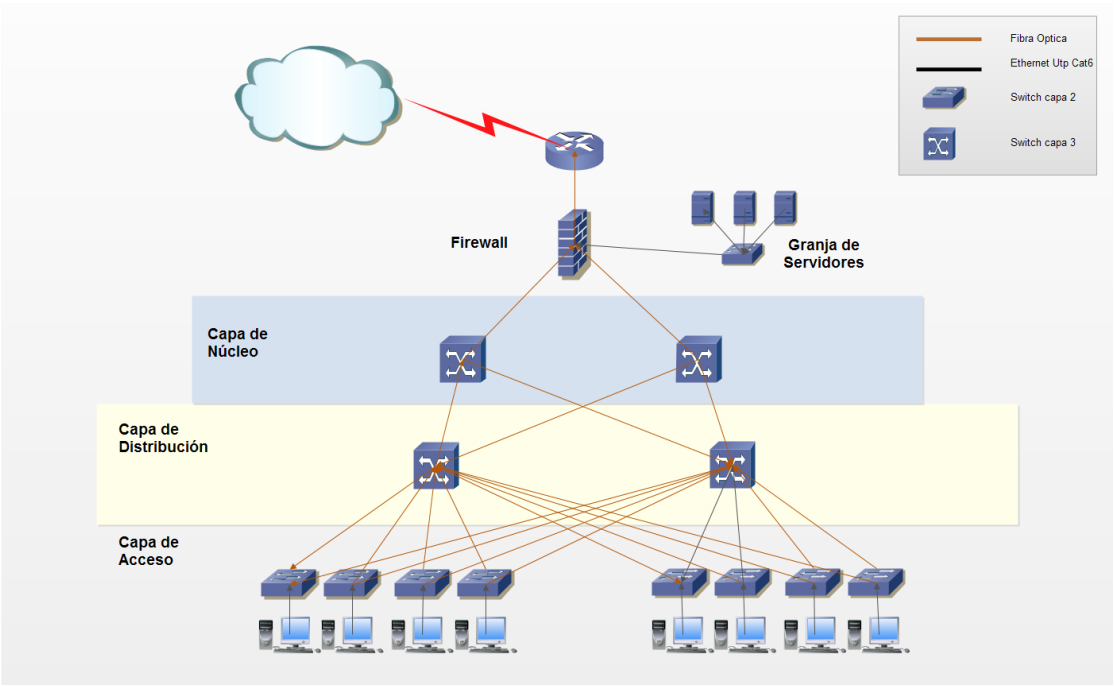


Figura 25. Topología de red a diseñar

4.3.2 Capa de acceso

Esta capa dará acceso a los terminales finales de la red, como son: PCs, teléfonos IP, y demás dispositivos.

Estos dispositivos para poder acceder a todos los servicios que ofrece la red se conectarán a un switch de acceso, el cual a su vez se enlazará a los switches de distribución para operar la información generada por el usuario final.

4.3.3 Capa de distribución

En esta capa los dispositivos se encargarán de funciones tales como la administración de las VLANs, la segmentación de la red, implementación de las ACLs (listas de control) para el control y filtrado de paquetes, diferenciación de datos, manejo de seguridad, entre otras.

Así mismo para proveer de alta disponibilidad a la red esta capa debe tener conexión con la capa de núcleo.

4.3.4 Núcleo de la red

Es la capa encargada de entregar a la red de datos un alto rendimiento y desempeño, las tareas que se realiza en esta capa por ejemplo son: enrutamiento, conmutación de paquetes, entre las diferentes VLAN`s, etc.

4.3.5 Elección de equipos para la red

La red necesita simplificar algunas de las tareas tales como: la administración, la seguridad, la calidad de servicio, entre otras. Es por ello que se debe tomar en cuenta ciertos factores al momento de realizar la elección de los dispositivos que van a ser utilizados dentro de la red.

4.3.5.1 Administración de los Equipos

Los dispositivos al momento de ser seleccionados deben contener ciertas características de gestión para que puedan ser administrados remotamente.

Por ejemplo, deben soportar protocolos de autentificación y encriptación de datos tales como: SNMP, RMON, SSH, etc.

4.3.5.2 Escalabilidad

Los dispositivos de red deben ser capaces de acoplarse a nuevas aplicaciones, servicios, y expansiones que ocurran en la red, es por ello que se menciona esta característica debido a que la red seguirá con su crecimiento.

4.3.5.3 Calidad de Servicio y Seguridad

Dentro de las redes multiservicios se debe aplicar calidad de servicio (QoS) para que se pueda priorizar el tráfico importante del menos importante, así como también, es vital el establecer políticas de seguridad dentro de la red. Por todo lo expuesto anteriormente las características de los equipos a adquirir deben cumplir con los siguientes parámetros dentro de su funcionalidad: filtrado de puerto mediante direcciones MAC, soporte de VLAN`s, configuración de listas de control de acceso (ACL), protocolos como IEEE 802.1p e IEEE 802.1X. (Ramón, 2014)

Después de haber mencionado algunas características generales que los equipos de red deben cumplir, a continuación, se describe algunas de las características específicas para los equipos a utilizarse en cada una de las capas del diseño de red.

4.4 Diseño de la red pasiva

Se entiende como red pasiva a la estructura la cual soporta a la red, es decir, se trata de los componentes por donde se transmiten los datos pero sin generarlos, modificarlos o cambiarlos cuando cruzan por ella, dichos componentes son necesarios para que se produzca la transmisión.

La Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., dentro de la Oficina Matriz, dispone de un sistema de cableado estructurado que brinda el soporte adecuado a la red de datos. Además, en cada piso se encuentran distintos departamentos; en cada uno de estos pisos se ubica un cuarto de telecomunicaciones con el propósito de cumplir la recomendación de la norma EIA/TIA 568-C la cual manifiesta que la distancia máxima del cableado horizontal no debe superar los 90 metros.

A nivel de agencias, la cooperativa dispone de un cuarto de telecomunicaciones por agencia, que mediante el cableado horizontal conecta los distintos dispositivos de red.

Cuando se instaló el cableado estructurado en la oficina matriz (año 2013), según el administrador de la red se tomó en cuenta un crecimiento del 30% en cada departamento, esto para facilitar que existan puertos suficientes puertos y espacios para el cableado estructurado en al menos un periodo de 10 años, con el propósito de no tener que realizar cambios en el sistema por adiciones de usuarios, cambios de ubicaciones, etc.

La institución financiera actualmente en cuanto a la red pasiva cumple con las recomendaciones de la norma TIA/EIA (568-A, 569, 606), dicha información se evidencia en los planos tanto de la oficina matriz como de la agencia San Rafael (véase anexos 2, 3 y 4), por lo tanto, en este capítulo no se va a desarrollar el diseño de la red pasiva al encontrarse conforme la norma lo estipula.

4.5 Dimensionamiento del tráfico de red

La cooperativa en su rediseño necesita contar con un dimensionamiento del tráfico para obtener un mejor provecho de la misma, en este diseño tendremos en cuenta servicios correo electrónico, acceso a la web, acceso a la base de datos desde el aplicativo Core Bancario, descargas de archivos, videoconferencia y VoIP.

A continuación, realizaremos los cálculos necesarios para el dimensionamiento del ancho de banda de los servicios.

4.5.1 Cálculo del ancho de banda del correo electrónico.

La cooperativa cuenta con correo electrónico licenciado llamado Office 365, mediante este servicio se realiza anuncios de actividades que se realicen en la institución, requerimientos solicitados desde otros departamentos, gestión de reuniones entre otro tipo de actividades.

Se ha evidenciado que el correo electrónico necesita de un buen ancho de banda por lo que es necesario poder contar con este cálculo para un mejor dimensionamiento.

La información que se puede enviar por correo es muy variable, además que dependerá del tipo de información que se esté enviando.

Para realizar el cálculo del ancho de banda del correo electrónico se ha tomado desde las estadísticas de la administración de Office 365 un valor promedio de 190kb, ya que en su mayoría los correos enviados dentro de la institución financiera poseen imágenes y texto, además se evidenció que en una hora se reciben en promedio 10 correos electrónicos por usuario dentro de la organización, con estos datos podemos realizar el cálculo del ancho de banda que se requiere.

$$AB = \frac{190kb}{1\ mail} \times \frac{10\ mail}{1\ hora} \times \frac{1\ hora}{3600\ seg} \times \frac{8\ bits}{1\ byte} = 4{,}22\ Kbps$$

(Ecuación 1)

4.5.2 Cálculo del ancho de banda para acceso a la WEB

Para la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., resulta esencial trabajar con internet y acceso al mismo, debido a que trabaja con instituciones que le proveen de servicios. En base a los accesos que se reporta por medio del firewall se encuentra que las páginas más visitadas son las del gobierno y de información que ayudan en las labores diarias de los empleados, obteniendo un tiempo de carga por página de 3 segundos.

Para poder identificar el tamaño de una página web se ha utilizado una herramienta web de nombre GTMETRIX y teniendo en cuenta que páginas son visitadas con regularidad en la institución se determina que el tamaño a considerar para una página web es de 375 kb por cada página.

$$AB = \frac{375kb}{1\ pag} \times \frac{1\ pag}{3\ seg} \times \frac{8\ bits}{1\ byte} = 1000Kbps$$

(Ecuación 2)

4.5.3 Cálculo del ancho de banda para el acceso a la base de datos

Este servicio es el más importante en la institución debido a que el aplicativo Core Bancario accede las 24 horas del día a la base de datos, es por ello que es necesario realizar un dimensionamiento del ancho de banda para el acceso a la base de datos.

El acceso es en tiempo real ya que brinda un servicio continuo a los usuarios, esperando siempre que las consultas a la base de datos sean eficientes y sin retraso. Mediante el monitoreo en la base de datos realizado en el punto 3.3.1.6, se obtiene que una transacción tiene en tamaño 300Kb y el tiempo de respuesta es de 30 segundos, con los siguientes datos se obtiene el siguiente calculo.

$$AB = \frac{300kb}{1\ transaccion} \times \frac{1\ transaccion}{30\ seg} \times \frac{8\ bits}{1\ byte} = 80\ Kbps$$

(Ecuación 3)

4.5.4 Cálculo del ancho de banda para la descarga de archivos

Para la descarga de archivos se tomó como referencia que en promedio el tamaño de un archivo es de 3MB, se considerado en la descarga todo tipo de archivos como documento, imágenes, audio, video, etc. También se consideró que en una hora un usuario descarga 5 archivos en promedio, con los datos obtenidos podemos calcular el ancho de banda.

$$AB = \frac{3000kb}{1\ desacarga} \times \frac{5\ descargas}{1\ hora} \times \frac{1\ hora}{3600\ seg} \times \frac{8\ bits}{1\ byte} = 33{,}33\ Kbps$$

(Ecuación 4)

Cabe mencionar que dentro de la descarga de archivos se considera archivos adjuntos de correo electrónico en formatos: Pdf, Word, Excel.

4.5.5 Cálculo de ancho de banda necesario para videoconferencia

Una llamada de videoconferencia con calidad para negocios según lo investigado en la página de Grupoact, se considera que al menos debe manejar 30 cuadros por segundos para poder garantizar los requisitos mínimos

para el audio y el video. En la tabla 6, se detallan los anchos de banda que se recomienda para Videoconferencia vía IP.

Tabla 6.

Ancho de banda para videoconferencia.

VIDEO CONFERENCIA VÍA IP	
Calidad	**Ancho de Banda**
15 cuadros por segundo	256 Kbps
30 cuadros por segundo	512 Kbps

El ancho de banda ideal para la transmisión de videoconferencia por IP es de 512 Kbps como lo muestra la tabla anterior. Para efectos de este proyecto el ancho de banda considerado es de 512 Kbps.

Para determinar el ancho de banda requerido para la videoconferencia en simultáneo con ocho agencias desde la oficina matriz, se multiplica el total de agencias que utilizarán la videoconferencia por el ancho de banda requerido para la transmisión de la videoconferencia (ver tabla 6).

$$ABVideoconferencia = 8\ x\ 512\ Kbps\ =\ 4096\ Kbps$$

(Ecuación 5)

El cálculo se lo realizó en base a como se enlazan en videoconferencia los equipos de la marca AVER adquiridos por la cooperativa, es así que el equipo ubicado en la oficina matriz solo permite realizar hasta ocho conexiones en simultaneo del total de dieciocho agencias que disponen de los equipos.

4.5.6 Cálculo de las tramas de voz

Para este cálculo es necesario utilizar un códec, porque de esto dependerá el resultado que nos dará el tamaño de los datos y debe sumarse otros parámetros.

- ✓ El códec a utilizarse es el G.729.
- ✓ Para el encapsulamiento de capa 2 se utilizará Ethernet.

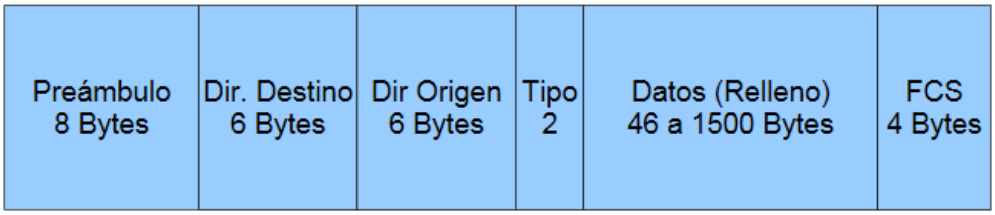


Figura 26. Trama Ethernet

Tomado de: Iesjuandelacierva, s.f.

Se debe tomar en consideración que para el encapsulamiento de Ethernet se utiliza los campos MAC Destino, MAC origen, Type y FCS que suman un total de 18 bytes adicionales (véase Figura 26).

A continuación, se muestra en la tabla 7 el tamaño original de la Trama Ethernet.

Tabla 7.

Tamaño de la Trama Ethernet

TAMAÑO DE LA TRAMA ETHERNET	
Cabecera IP	20 bytes
Cabecera UDP	12 bytes
Cabecera RTP	8 bytes
Encapsulamiento Ethernet	18 bytes
Payload (Voz)	20 bytes

$$Tamaño\ de\ la\ trama = 20 + 18 + 8 + 12 + 20 = 78\ bytes$$

(Ecuación 6)

El peso del encabezado en la trama a ser transmitida en enlaces de bajo ancho de banda requiere de una compresión en los encabezados de capa3 y capa4, este tipo de compresión de llama RTP y reduce los 40 bytes a 2 o 4 bytes (véase Figura 27).

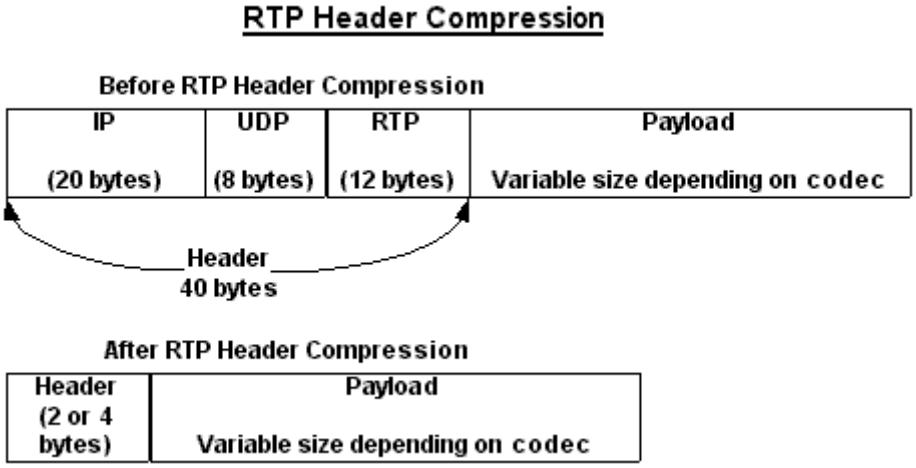


Figura 27. Compresión RTP

Tomado de: Cisco, s.f.

Dando como resultado un tamaño menor de la Trama Ethernet (véase tabla 8).

Tabla 8.

Tamaño de la Trama Ethernet utilizando compresión

TAMAÑO DE LA TRAMA ETHERNET APLICANDO COMPRESIÓN RTP	
Cabecera IP/UDP/RTP	2
Encapsulamiento Ethernet	18 bytes
Payload (Voz)	20 bytes

$$Tamaño\ de\ la\ trama = 20 + 18 + 2 = 40\ bytes$$

(Ecuación 7)

Es necesario realizar la conversión del tamaño de la Trama Ethernet a bits.

$$bits = 40\ bytes \times \frac{8\ bits}{1\ byte} = 320\ bits$$

(Ecuación 8)

4.5.6.1 Cálculo del ancho de banda por llamada

El códec utilizado para la digitalización de voz indica que se generan 50 tramas en un segundo.

Multiplicando el tamaño de cada trama por la cantidad de tramas que se envían por segundo se obtienen el ancho de banda requerido.

$$ABVoIP = 320\ bits/trama\ x\ 50\ tramas/seg. =\ 16000\ bps/llamada$$

(Ecuación 9)

4.5.6.2 Cálculo del ancho de banda transmisión VoIP

En la institución se utilizará un máximo de diez llamadas concurrentes generadas, utilizando CODEC G.729 sobre un enlace Ethernet con RTP.

$$BW\ requerido =\ 16000\ bps\ \times 10 =\ \ 160Kbps$$

(Ecuación 10)

4.5.7 Ancho de banda total requerido para datos.

Después de haber calculado el ancho de banda de las aplicaciones que serán utilizadas por los usuarios de la red de la institución financiera, se realizara el cálculo del ancho de banda total que se requiere para datos. Hay que tener en cuenta la simultaneidad para la sumarización del ancho de banda; esta definición indica el número de usuarios que utilizan concurrentemente los diferentes servicios.

Para una mejor comprensión se presenta en la tabla 9 los usuarios por área, la cual tiene la cantidad de usuarios reales y potenciales; siendo los usuarios reales los que actualmente existen y usuarios potenciales aquellos que se están considerando a futuro en el diseño, pero deben ser considerados todos debido a que los sitios de trabajo pueden ser ocupados y utilizan la red de voz y datos.

Tabla 9.

Tabla usuarios reales y potenciales

Departamentos	Usuarios Reales	Usuarios Potenciales	Total Usuarios
FINANCIERO	18	4	22
SISTEMAS	15	5	20
CALLCENTER	13	4	17
COMERCIAL	10	6	16
OPERARACIONES	11	5	16
FABRICA DE CREDITO	12	4	16
TTHH	10	4	14
SEGURIDAD	11	3	14
RIESGOS	7	3	10
ADMINISTRATIVO	6	2	8
JURIDICO	5	3	8
AUDITORIA	4	3	7
GERENCIA	3	2	5
DESARROLLO ORGANIZACIONAL	3	2	5
COBRANZAS	3	2	5
SEGUROS	2	2	4

Ahora se define en la tabla 10 la simultaneidad por aplicación.

Tabla 10.

Índices de Simultaneidad

Aplicación	Índice de Simultaneidad
Correo Electrónico	20%
Acceso a la Web	10%
Acceso a la Base de Datos	30%
Descarga de Archivos	20%

Finalmente, en la siguiente tabla se desglosa el ancho de banda necesario por departamento.

Tabla 11.

Total de ancho de banda requerido para datos

Aplicación	Departamento	AB Requerido Kbps	Índice de Simultaneidad [%]	# Usuarios	AB kbps
Correo electrónico	FINANCIERO	4.22	0.2	22	18.57
	SISTEMAS			20	16.88
	CALLCENTER			17	14.35
	COMERCIAL			16	13.50
	OPERARACIONES			16	13.50
	FABRICA DE CREDITO			16	13.50
	TTHH			14	11.82
	SEGURIDAD			14	11.82
	RIESGOS			10	8.44
	ADMINISTRATIVO			8	6.75
	JURIDICO			8	6.75
	AUDITORIA			7	5.91

	GERENCIA			5	4.22
	DESARROLLO ORGANIZACIONAL			5	4.22
	COBRANZAS			5	4.22
	SEGUROS			4	3.38
Ancho de banda total para correo electrónico				187	157.83
Acceso a la WEB	FINANCIERO	1000	0.1	22	2200.00
	SISTEMAS			20	2000.00
	CALLCENTER			17	1700.00
	COMERCIAL			16	1600.00
	OPERARACIONES			16	1600.00
	FABRICA DE CREDITO			16	1600.00
	TTHH			14	1400.00
	SEGURIDAD			14	1400.00
	RIESGOS			10	1000.00
	ADMINISTRATIVO			8	800.00
	JURIDICO			8	800.00
	AUDITORIA			7	700.00
	GERENCIA			5	500.00
	DESARROLLO ORGANIZACIONAL			5	500.00
	COBRANZAS			5	500.00
	SEGUROS			4	400.00
Ancho de banda total para acceso a la web				187	18700.00
Acceso base de datos	FINANCIERO	80	0.3	22	528.00
	SISTEMAS			20	480.00
	CALLCENTER			17	408.00
	COMERCIAL			16	384.00
	OPERARACIONES			16	384.00

	FABRICA DE CREDITO			16	384.00
	TTHH			14	336.00
	SEGURIDAD			14	336.00
	RIESGOS			10	240.00
	ADMINISTRATIVO			8	192.00
	JURIDICO			8	192.00
	AUDITORIA			7	168.00
	GERENCIA			5	120.00
	DESARROLLO ORGANIZACIONAL			5	120.00
	COBRANZAS			5	120.00
	SEGUROS			4	96.00
Ancho de banda total para acceso a base de datos				187	4488.00
Descarga de Archivos	FINANCIERO	33.33	0.2	22	146.65
	SISTEMAS			20	133.32
	CALLCENTER			17	113.32
	COMERCIAL			16	106.66
	OPERARACIONES			16	106.66
	FABRICA DE CREDITO			16	106.66
	TTHH			14	93.32
	SEGURIDAD			14	93.32
	RIESGOS			10	66.66
	ADMINISTRATIVO			8	53.33
	JURIDICO			8	53.33
	AUDITORIA			7	46.66
	GERENCIA			5	33.33
	DESARROLLO ORGANIZACIONAL			5	33.33
	COBRANZAS			5	33.33

	SEGUROS			4	26.66
Ancho de banda total para descargas de archivos				187	1246.54
ANCHO DE BANDA TOTAL PARA DATOS					24592.37

Como se puede apreciar en la tabla anterior se requiere 24.59 Mbps en total de ancho de banda para datos, por lo cual el ancho de banda contratado por la cooperativa que es de 120 Mbps si soporta la carga de tráfico actual que demanda la red.

4.5.8 Ancho de banda requerido para voz

Para la voz se efectúa un proceso parecido al cálculo del ancho de banda anteriormente realizado para los datos, se aprovecha la tabla 9 antes elaborada de los usuarios potencias y reales de cada departamento para tomar en cuenta en el cálculo de la ecuación 11.

Multiplicar el total de usuarios que utilizarán la VoIP por índice de simultaneidad y por el ancho de banda para la transmisión VoIP del punto 4.5.6.2, con esto se determinará el ancho de banda requerido para voz.

Para el cálculo de la VoIP se considera un índice de simultaneidad del 20 %, es así que 37 usuarios al menos estarían utilizando el servicio de manera simultánea, a continuación el valor de la ecuación 11 es el obtenido.

$$ABVoIP = 187x\ 0.20\ x\ 160\ Kbps\ =\ 5984\ Kbps$$

(Ecuación 10)

4.5.9 Ancho de banda de la conexión a Internet

Se trata del flujo de información que saldrá al Internet o también llamado (el tráfico que sale de la red interna hacia la nube), haciendo énfasis en que no todo el tráfico que cursa por la red sale a la nube, por lo cual esto último será considerado cuando se dimensione el ancho de banda que se requiera contratar.

A continuación en la Tabla 12 se muestran los servicios que tiene salida a la nube.

Tabla 12.

Servicios que tiene salida a la nube

SERVICIO	ANCHO DE BANDA EXTERNO [Kbps]
Correo electrónico	157.83
Acceso a la WEB	18,700.00
Descarga de Archivos	1,246.54
Video Conferencia	4,096.00
ANCHO DE BANDA TOTAL HACIA LA NUBE	24,200.37

Nota: Cabe mencionar que los valores de las llamadas concurrentes generadas y los índices de simultaneidad, son valores estimados en conjunto con departamento de infraestructura de la cooperativa, ya que al momento no se dispone de valores reales debido a que anteriormente no se ha realizado un dimensionamiento parecido al de este proyecto.

4.6 Diseño de la red activa

El diseño de la red activa contempla todos los equipos relacionados a datos voz y video, tales como estaciones de trabajo y teléfonos IP. Para la adquisición y utilización de equipos ya existentes en la empresa, se debe tener en cuenta las características mínimas necesarias que requiere la red para mejorar el funcionamiento.

4.6.1 Estaciones de trabajo

Son todos los computadores que están dentro de la red, con los cuales los usuarios interactúan con la red, aprovechando todos los recursos que esta última pone a su disposición.

La institución financiera en la actualidad posee estaciones de trabajo que se encuentran en buen estado y funcionando óptimamente con sistemas operativos licenciados, por lo cual se seguirá usando las mismas estaciones de trabajo fijas y portátiles. El departamento de infraestructura de la cooperativa, cuenta con un sistema de rotación y adquisición de nuevos equipos en base a su presupuesto anual, las características tecnológicas para adquirir un nuevo equipo es responsabilidad del personal del área de infraestructura. Sin embargo, a continuación se presenta una recomendación para nuevas adquisiciones:

- ✓ Procesador: Intel Core i7 de 5ra Generación
- ✓ Sistema Operativo: Windows 8.1 Pro 64 o Windows 10
- ✓ Memória RAM: 6GB o 8GB 1600 MHz DDR3
- ✓ Disco duro: 500GB o 1TB (7200 rpm)
- ✓ Red: Gigabit integrado 10M/100M/1000M

4.6.2 Servidores

En cuanto a los servidores, al igual que las estaciones de trabajo se encuentran funcionando óptimamente en relación a la carga de trabajo y nivel de información que manejan.

4.6.3 Equipos activos de la red

En este punto serán considerados los equipos activos de la red como lo son: switch de acceso, switch de distribución, switch de core y routers.

En base al dimensionamiento de la red, será indispensable la adquisición de equipos con el fin de obtener una red que sea capaz de soportar aplicaciones y servicios en tiempo real pero que también se aplique dentro de ella la calidad de servicio (QoS).

El modelo jerárquico es la base del presente proyecto de rediseño de red por lo cual a continuación se presenta las características que deben cumplir los dispositivos activos de la red.

4.6.3.1 Switch de acceso

Con el fin de poder acceder a los servicios que brinda la red, los equipos terminales se los va a conectar a los denominamos switches de acceso. En base a la necesidad de establecer un tipo de seguridad en este nivel de la red y tomando en cuenta el crecimiento futuro de la misma que se estima sea del 30%, a continuación, se presenta en la tabla 13 las características mínimas que deben disponer los *switches* de acceso.

Tabla 13.

Características de los switches de acceso

Parámetros	Características
Puertos Ethernet	24 / 48 puertos full duplex 10/100/1000 Mbps con conector RJ45
Puertos Uplink	2 puertos uplink de 10Gbps
Capa OSI	2
Manejo de VLAN`s	Manejo, configuración y administración de VLANs
Calidad de Servicio	Capacidad para manejar priorización de tráfico, IEEE 802.1p
Telefonía IP	Soporte para paquetes de telefonía IP.
Estándares	IEEE 802.1d ;
	IEEE 802.1p ;
	IEEE 802.1q ;
	IEEE 802.1x ;
	IEEE 802.1w ;
	IEEE 802.3u ;
	IEEE 802.3x ;
	IEEE 802.3af
Protocolos	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON

Administración	Soporte de protocolos de gestión y administración remota.
	GUI; SNMP; Telnet; CLI
Autenticación	Manejo de seguridad para la autenticación de los dispositivos conectados a la red
Alimentación	Power over Ethernet Plus (PoE+, 802.3at)

La tabla 14 indica la cantidad de switches de acceso que se necesitan por cada agencia y oficina matriz.

Tabla 14.

Número de switches de acceso necesarios

Ubicación	Piso	Número de Puertos	Cantidad
Oficina Matriz	Planta Baja	28	1 Switch de 48 puertos
	1ra Planta alta	30	1 Switch de 48 puertos
	2da Planta alta	37	1 Switch de 48 puertos
	3ra Planta alta	13	1 Switch de 24 puertos
	4ra Planta alta	2	1 Switch de 24 puertos
	Bloque "A"	39	1 Switch de 48 puertos
	Bloque "B"	23	1 Switch de 48 puertos
	Bloque "C"	17	1 Switch de 48 puertos
34 Agencias	N/A	30	34 Switch de 48 puertos

Cabe mencionar que la institución financiera cuenta con 8 switch de acceso de la marca CISCO, los cuales se encuentran en la actualidad funcionando en condiciones normales dentro de la oficina matriz, mientras que en las agencias al igual que la telefonía IP, 9 de las 34 agencias cuentan con switch de acceso de capa 2 administrables, por lo que se sugiere se cambien los switch de las restantes 25 agencias.

4.6.3.2 Switch de distribución

Esta capa sirve para conectar de la capa de acceso a la capa de núcleo, resulta ser una capa intermedia. Aquí es donde se va a tener la agregación de enlaces redundantes de LAN a WAN, de WAN a WAN, de LAN a LAN, los cuales sirven para distribuir la información de una parte de la red desde el nivel de acceso con otra parte de la red que también está a nivel de acceso ya que todo esto es modular. Los equipos de esta capa manejaran los filtros de seguridad a nivel de servicios de la red como las listas de control de accesos (ACL), enrutamiento entre VLANs, conexiones de diferentes dominios de enrutamiento como por ejemplo (la conexión de EIGRP de un sistema autónomo y EIGRP de otro sistema autónomo), también se manejará redundancia entre módulos y balanceo de cargas (para su aprovechamiento cuando se tiene más de un enlace entre diferentes módulos de la red habría que balancear las cargas para que los dos enlaces se utilicen y no usar solo uno dejando al otro solo de respaldo). Finalmente, es aquí donde se realizarán las sumarizaciones de la red.

En cuanto a la oficina matriz de la institución, dentro de la estructura de la nueva red se debe considerar conectar los ocho switches de capa acceso al nivel de distribución, por lo cual se utilizarán dos switches en esta parte del modelo jerárquico, siendo el primero utilizado para brindar servicios de la capa de distribución y el otro se configurará de manera que ofrezca redundancia a la red. Esto permitirá evitar la saturación y disponer de alta disponibilidad en la nueva propuesta de diseño de red.

A continuación, se presenta en la tabla 15 las características mínimas que deben disponer los switches de distribución los cuales se sugiere sean adquiridos.

Tabla 15.

Características de los switches de distribución

Parámetros	Características
Puertos Ethernet	12/24 puertos de 10/100/1000 Mbps con conector RJ45
Puertos Uplink	2 puertos uplink de 10Gbps
Capa OSI	3
Velocidad	Enlaces con capacidad para alta velocidad hacia las capas de core y acceso.
Manejo de VLAN`s	Manejo, configuración y administración de VLANs
Calidad de Servicio	Capacidad para manejar priorización de tráfico, IEEE 802.1p
Seguridad	Soporte a ACL estándar y extendidas en todos los puertos
Telefonía IP	Soporte para paquetes de telefonía IP.
Estándares	IEEE 802.1d ;
	IEEE 802.1p ;
	IEEE 802.1q ;
	IEEE 802.1x ;
	IEEE 802.1w ;
	IEEE 802.3u ;
	IEEE 802.3x ;
	IEEE 802.3af
Protocolos	IP; IPv6; OSPF; RIPv2; IGM; BGP; DHCP. Soporte para el Protocolo Spanning Tree.
Administración	Soporte de protocolos de gestión y administración remota.
	GUI; SNMP; Telnet; CLI
Autenticación	Manejo de seguridad para la autenticación de los dispositivos

	conectados a la red.
Alimentación	Power over Ethernet Plus (PoE+, 802.3at)

La tabla 16 indica la cantidad de switches de distribución que se necesitan para la oficina matriz.

Tabla 16.

Número de switches de distribución necesarios

Ubicación		**Cantidad de switches de distribución**	**No. de Puertos Uplink 10 Gbps**	**Puertos Adicionales 10/100/1000 Mbps**
Oficina Matriz	Rack 1	1	4	8
	Rack 2			
	Rack 6			
	Rack 7			
	Rack 3	1	4	8
	Rack 4			
	Rack 5			
	Rack 8			

4.6.3.3 Switch de core

La capa de núcleo provee de conectividad de alta velocidad, a esta capa se va a conectar la capa de distribución, en esta capa de núcleo no se debe configurar ningún filtro ya que en esta parte del modelo jerárquico se recomienda contar con las interfaces más rápidas, los equipos más veloces y con más memoria para con ello proveer de enrutamiento rápido. Esta capa también proveerá de confiabilidad y tolerancia a fallas ya que existirán equipos

y enlaces redundantes. Esta parte de la red se escala agregando equipos más rápidos. Por otra parte, no se debe hacer en esta capa inspección de tráfico, configurar listas de acceso, filtros o calidad de servicio (QoS) ya que todo el tráfico debe ser rápido hacia el exterior de la red.

La ubicación de los switches de core será en el cuarto de comunicaciones de la oficina matriz o Data Center. Con relación a las 34 agencias se hará una unificación en un solo equipo a nivel de core o también llamado núcleo contraído. La justificación para realizar dicha unificación es que la cantidad de tráfico demandada por parte de las agencias es inferior a la procesada en la oficina matriz.

A continuación, se presenta en la tabla 17 las características a considerar a nivel de switch de core, esto tomando en cuenta la gran cantidad de información que este equipo manejará.

Tabla 17.

Características de los switches de core

Parámetros	Características
Puertos Ethernet	12 puertos 100/1000/10000 Mbps con conector RJ45
Puertos	2 puertos uplink de 10Gbps
Capa OSI	Capa 2/ 3
Manejo de VLAN`s	Manejo, configuración y administración de VLANs
Calidad de Servicio	Capacidad para manejar priorización de tráfico, IEEE 802.1p
Seguridad	Soporte a ACL estándar y extendidas en todos los puertos
Telefonía IP	Soporte para paquetes de telefonía IP.
	Capacidad para el manejo, priorización y clasificación de tráfico de voz sobre IP (VoIP).
Estándares	IEEE 802.1d ;
	IEEE 802.1p ;
	IEEE 802.1q ;
	IEEE 802.1x ;
	IEEE 802.1w ;
	IEEE 802.3u ;
	IEEE 802.3x ;
	IEEE 802.3af
Protocolos	IP; OSPF; RIPv2; IGM; BGP; DHCP. Soporte para el Protocolo Spanning Tree.
Administración	Soporte de protocolos de gestión y administración remota.
	GUI; SNMP; Telnet; CLI
Autenticación	Manejo de seguridad para la autenticación de los dispositivos

	conectados a la red.
Alimentación	Power over Ethernet Plus (PoE+, 802.3at)

4.6.3.4 Router

Es el núcleo de las comunicaciones de la institución financiera debido a que interconecta las redes desde su oficina matriz hacia sus agencias y viceversa, también es la puerta de acceso desde y hacia otras redes e internet. Quien administra estos equipos es el ISP llamado TE UNO ya que son de su propiedad y los conecta mediante su red de MLSP. A continuación en la tabla 18 se detallan características técnicas de los routers instalados.

Tabla 18.

Características de los routers

4 puertos Gigabit Ethernet (10/100/1000) con conectores tipo RJ45.
Puertos full dúplex
Capacidad para manejar priorización de tráfico basada en el protocolo IEEE 802.1p para calidad de servicio (QoS).
Soporte de enrutamiento estático y protocolos de enrutamiento dinámicos.
Manejo de listas de control (ACLs).
2 interfaces seriales para las conexiones WAN.
Soporte de protocolos de gestión y administración remota.
Soporte para VLANs mediante el protocolo IEEE 802.1Q.
Soporte para VPN.
Soporte para protocolo de enlaces WAN.
Soporte de alimentación Power over Ethernet Plus (PoE+, 802.3at).

4.6.4 Telefonía IP

La cooperativa cuenta tanto en la oficina matriz como en nueve de sus agencias con una solución de telefonía IP la cual se basada en la utilización un

dispositivo que realiza la conversión de analógico a digital entre la PSTN y la red IP (Gateway), este último va conectado al servidor IP quien se encarga de gestionar las llamadas.

En cuanto a las 25 agencias restantes actualmente las llamadas telefónicas entre ellas se las realiza utilizando la PSTN contactada a una centralita analógica y para el uso de la telefonía IP existe una limitación la cual es que solo se puede usar un puerto para voz IP, mismo que es proporcionado por un Gateway que está conectado en un extremo a la centralita y el otro extremo al switch de cada agencia. Para solventar este problema se recomienda que se implemente el mismo modelo ya establecido de telefonía IP instalado en la oficina matriz y nueve de sus agencias, de la misma manera se recomienda se tome en cuenta los cálculos realizados en el punto 4.5.6.2 con respecto al dimensionamiento de ancho de banda, el propósito de la solución es que al comunicarse entre treinta y cuatro agencias por VoIP la reducción de costos sea significativa en comparación al uso de la PSTN entre las agencias.

4.6.4.1 Servidor de llamadas IP

Se encarga de convertir las señales de voz a datos mediante diferentes protocolos tales como: SIP y H.323 para posteriormente ser enviados dentro de una red IP. Además de realizar el control de llamadas IP.

El servidor de llamadas utilizado se basa en Asterisk (completa solución de centralita IP), la empresa SIDEVOX provee actualmente a la institución financiera un appliance llamado CONTACVOX el cual es una modificación de Asterisk.

4.6.4.2 Especificaciones de los equipos para la telefonía IP

Al establecer un completo sistema de telefonía IP para la institución, se requiere de teléfonos IP y de un equipo servidor de llamadas por agencia, el cual será quien gestione todo el tráfico de VoIP. A continuación, en la tabla 19 se menciona los parámetros básicos a tomar en cuenta para la adquisición de los teléfonos IP.

Tabla 19.

Características de los teléfonos IP

Parámetros	Características
Puertos	2 puertos RJ45 10/100 Mbps
Interfaces FXO	24
Codecs de Voz	G.711 ; G.723 ; G.726 ; G.729
Cancelación de Eco	Sí
Supresión de Silencios	Sí
Manejo de VLAN`s	Sí
Estándares	IEEE 802.1p ; IEEE 802.1q ; H.323 ; SIP v2 ; 802.3af ; MPLS
Protocolos	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON
Administración	GUI; SNMP; Telnet; CLI

El servidor de llamadas IP instalado actualmente tanto la oficina matriz como en las nueve agencias presenta las siguientes características (véase tabla 20):

Tabla 20.

Características del servidor de llamadas IP

Parámetros	Características
Procesador	3 GHz x64
Memoria RAM	1 GB
Disco duro	250 GB
Puertos	PCI Gigabit Ethernet (1000 Mbps) con conectores RJ45
Protocolos	SIP
Codec	G.729
Capacidad	20 usuarios
Servicio	Llamada en espera Buzón de voz Directorio telefónico Conferencia
Administración	SNMP

En resumen:

- ✓ Equipos que se requiere adquirir considerando aplicar redundancia en el rediseño de la red (véase tabla 21).

Tabla 21.

Equipos requeridos para aplicar redundancia.

Nombre del equipo	Cantidad
Switch de distribución	2
Switch de núcleo	1

- ✓ Equipos que se reutilizará en el rediseño a nivel de oficina matriz (véase tabla 22).

Tabla 22.

Equipos a reutilizar para el rediseño en oficina matriz.

Nombre del equipo	**Cantidad**
Switch de acceso	8
Switch de núcleo	1
Central telefónica	1
Videoconferencia	1
Firewall	2
Servidores	7
Servidor de Base de datos	1

- ✓ Equipos que se reutilizará en el rediseño a nivel de agencias (véase tabla 23).

Tabla 23.

Equipos a reutilizar para el rediseño en agencias.

Nombre del equipo	**Cantidad**
Switch de acceso	8
Central telefónica	1
Videoconferencia	1

4.7 Diseño lógico de la red

El diseño lógico define la especificación funcional que se usa en el diseño físico de la red, es decir, se establece los parámetros para que los diferentes equipos de la red se comuniquen.

Resulta muy importante definir un esquema lógico al momento de diseñar una red, pues este esquema lógico permitirá entender cómo funcionará la red con el objetivo de obtener el mayor performance de la misma.

A continuación, se mencionan algunas características importantes para diseñar un correcto esquema lógico, estas son: el direccionamiento IP, configuración de VLAN´s y DMZ.

4.7.1 Plan de direccionamiento IP

Con el direccionamiento IP a cada uno de los equipos de usuarios de la red se les asigna de una dirección IP, esto les permitirá conectarse a la red para poder utilizar los servicios que la misma brinda.

En la institución financiera existen 190 puntos de red en la oficina matriz y 30 puntos de red en cada una de las agencias, estos puntos se los utiliza tanto para voz como para datos. Por consecuente se decide utilizar el esquema VLSM (Máscaras de subred de longitud variable). Se eligió el esquema VLSM porque permite el ahorro de direcciones IP y crea de una red lógica jerárquica. Asimismo, para el direccionamiento en la oficina matriz se utiliza una dirección privada de clase B la cual es 172.16.0.0/13, mientras que para las agencias se utilizará la dirección 172.100.0.0/14 Para el segmento de la zona desmilitarizada (DMZ) se escoge la IP de clase A 10.0.0.0/24. Para los servidores se asigna la 192.168.50.0/24, así como para la telefonía IP se determina la subred 192.168.10.0/24, finalmente, las impresoras utilizarán el rango de IPs correspondiente a la red 192.168.30.0/24 (véase tabla 24).

Tabla 24.

Direccionamiento IP – Oficina Matriz

SEGMENTO	IP Necesarias	Subred	Prefijo	Direcciones IPs válidas	Mascara de Subred	Dirección de Broadcast	Hosts disponibles
FINANCIERO	22	172.16.0.0	/26	172.16.0.1 - 172.16.0.62	255.255.255.192	172.16.0.63	62
SISTEMAS	20	172.16.0.64	/26	172.16.0.65 - 172.16.0.126	255.255.255.192	172.16.0.127	62
CALLCENTER	17	172.16.0.128	/26	172.16.0.129 - 172.16.0.190	255.255.255.192	172.16.0.191	62
COMERCIAL	16	172.16.0.192	/26	172.16.0.193 - 172.16.0.254	255.255.255.192	172.16.0.255	62
OPERARACIONES	16	172.16.1.0	/26	172.16.1.1 - 172.16.1.62	255.255.255.192	172.16.1.63	62
FABRICA DE CREDITO	16	172.16.1.64	/26	172.16.1.65 - 172.16.1.126	255.255.255.192	172.16.1.127	62
TTHH	14	172.16.1.128	/26	172.16.1.129 -	255.255.255.192	172.16.1.191	62

				172.16.1.190			
SEGURIDAD	14	172.16.1.192	/26	172.16.1.193 - 172.16.1.254	255.255.255.192	172.16.1.255	62
RIESGOS	10	172.16.2.0	/26	172.16.2.1 - 172.16.2.62	255.255.255.192	172.16.2.63	62
ADMINISTRATIVO	8	172.16.2.64	/26	172.16.2.65 - 172.16.2.126	255.255.255.192	172.16.2.127	62
JURIDICO	8	172.16.2.128	/26	172.16.2.129 - 172.16.2.190	255.255.255.192	172.16.2.191	62
AUDITORIA	7	172.16.2.192	/26	172.16.2.193 - 172.16.2.254	255.255.255.192	172.16.2.255	62
GERENCIA	5	172.16.3.0	/26	172.16.3.1 - 172.16.3.62	255.255.255.192	172.16.3.63	62
DESARROLLO ORGANIZACIONAL	5	172.16.3.64	/26	172.16.3.65 - 172.16.3.126	255.255.255.192	172.16.3.127	62
COBRANZAS	5	172.16.3.128	/26	172.16.3.129 - 172.16.3.190	255.255.255.192	172.16.3.191	62
SEGUROS	4	172.16.3.192	/26	172.16.3.193 - 172.16.3.254	255.255.255.192	172.16.3.255	62

IMPRESORAS	20	192.168.30.0	/24	192.168.30.1 - 192.168.30.254	255,255,255,000	192.168.30.255	254
SERVIDORES	30	192.168.50.0	/24	192.168.50.1 - 192.168.50.254	255,255,255,000	192.168.50.255	254
DMZ	15	10.0.0.0	/27	10.0.0.1 - 10.0.0.30	255,255,255,224	10.0.0.31	30
VOIP	170	192.168.10.0	/24	192.168.10.1 - 192.168.10.254	255,255,255,000	192.168.10.255	254

Tabla 25.

Direccionamiento IP – 34 Agencias

AGENCIA	IP Necesarias	Subred	Prefijo	Direcciones IPs válidas	Mascara de Subred	Dirección de Broadcast	Hosts disponibles
1	30	172.17.0.0	/24	172.17.0.1 - 172.17.0.254	255.255.255.0	172.17.0.255	254
2	30	172.17.1.0	/24	172.17.1.1 - 172.17.1.254	255.255.255.0	172.17.1.255	254
3	30	172.17.2.0	/24	172.17.2.1 - 172.17.2.254	255.255.255.0	172.17.2.255	254
4	30	172.17.3.0	/24	172.17.3.1 - 172.17.3.254	255.255.255.0	172.17.3.255	254
5	30	172.17.4.0	/24	172.17.4.1 - 172.17.4.254	255.255.255.0	172.17.4.255	254
6	30	172.17.5.0	/24	172.17.5.1 - 172.17.5.254	255.255.255.0	172.17.5.255	254
7	30	172.17.6.0	/24	172.17.6.1 - 172.17.6.254	255.255.255.0	172.17.6.255	254

8	30	172.17.7.0	/24	172.17.7.1 - 172.17.7.254	255.255.255.0	172.17.7.255	254
9	30	172.17.8.0	/24	172.17.8.1 - 172.17.8.254	255.255.255.0	172.17.8.255	254
10	30	172.17.9.0	/24	172.17.9.1 - 172.17.9.254	255.255.255.0	172.17.9.255	254
11	30	172.17.10.0	/24	172.17.10.1 - 172.17.10.254	255.255.255.0	172.17.10.255	254
12	30	172.17.11.0	/24	172.17.11.1 - 172.17.11.254	255.255.255.0	172.17.11.255	254
13	30	172.17.12.0	/24	172.17.12.1 - 172.17.12.254	255.255.255.0	172.17.12.255	254
14	30	172.17.13.0	/24	172.17.13.1 - 172.17.13.254	255.255.255.0	172.17.13.255	254
15	30	172.17.14.0	/24	172.17.14.1 - 172.17.14.254	255.255.255.0	172.17.14.255	254
16	30	172.17.15.0	/24	172.17.15.1 - 172.17.15.254	255.255.255.0	172.17.15.255	254
17	30	172.17.16.0	/24	172.17.16.1 -	255.255.255.0	172.17.16.255	254

				172.17.16.254			
18	30	172.17.17.0	/24	172.17.17.1 - 172.17.17.254	255.255.255.0	172.17.17.255	254
19	30	172.17.18.0	/24	172.17.18.1 - 172.17.18.254	255.255.255.0	172.17.18.255	254
20	30	172.17.19.0	/24	172.17.19.1 - 172.17.19.254	255.255.255.0	172.17.19.255	254
21	30	172.17.20.0	/24	172.17.20.1 - 172.17.20.254	255.255.255.0	172.17.20.255	254
22	30	172.17.21.0	/24	172.17.21.1 - 172.17.21.254	255.255.255.0	172.17.21.255	254
23	30	172.17.22.0	/24	172.17.22.1 - 172.17.22.254	255.255.255.0	172.17.22.255	254
24	30	172.17.23.0	/24	172.17.23.1 - 172.17.23.254	255.255.255.0	172.17.23.255	254
25	30	172.17.24.0	/24	172.17.24.1 - 172.17.24.254	255.255.255.0	172.17.24.255	254
26	30	172.17.25.0	/24	172.17.25.1 - 172.17.25.254	255.255.255.0	172.17.25.255	254

27	30	172.17.26.0	/24	172.17.26.1 - 172.17.26.254	255.255.255.0	172.17.26.255	254
28	30	172.17.27.0	/24	172.17.27.1 - 172.17.27.254	255.255.255.0	172.17.27.255	254
29	30	172.17.28.0	/24	172.17.28.1 - 172.17.28.254	255.255.255.0	172.17.28.255	254
30	30	172.17.29.0	/24	172.17.29.1 - 172.17.29.254	255.255.255.0	172.17.29.255	254
31	30	172.17.30.0	/24	172.17.30.1 - 172.17.30.254	255.255.255.0	172.17.30.255	254
32	30	172.17.31.0	/24	172.17.31.1 - 172.17.31.254	255.255.255.0	172.17.31.255	254
33	30	172.17.32.0	/24	172.17.32.1 - 172.17.32.254	255.255.255.0	172.17.32.255	254
34	30	172.17.33.0	/24	172.17.33.1 - 172.17.33.254	255.255.255.0	172.17.33.255	254

4.7.2 Diseño y distribución de VLANS

Es necesario segmentar la red separando por departamentos el tráfico de datos mediante la utilización de VLANs con el propósito de aprovechar de mejor manera el ancho de banda de la red y así conservar la confidencialidad de la información que se intercambia en la misma.

Tanto en el switch de distribución principal como el switch de distribución secundario se procederá a la creación de las VLANs, con la ayuda del protocolo de enlace troncal los demás switches compartirán dichas VLANs, estas reducirán la latencia de la red.

En este rediseño, se otorgará permisos para compartir recursos a cada departamento asociado a un VLAN, así como también se va a tomar en cuenta la asignación de permisos especiales para uso de ciertos servicios de red a determinados grupos de usuarios como es el caso de la Gerencia.

En la tabla 26, se muestra la distribución de las VLANs por departamento.

Tabla 26.

VLANs

SEGMENTO	NOMBRE DE VLAN	Subred
FINANCIERO	VLAN10	172.16.0.0
SISTEMAS	VLAN20	172.16.0.64
CALLCENTER	VLAN30	172.16.0.128
COMERCIAL	VLAN40	172.16.0.192
OPERARACIONES	VLAN50	172.16.1.0
FABRICA DE CREDITO	VLAN60	172.16.1.64
TTHH	VLAN70	172.16.1.128
SEGURIDAD	VLAN80	172.16.1.192
RIESGOS	VLAN90	172.16.2.0
ADMINISTRATIVO	VLAN100	172.16.2.64
JURIDICO	VLAN110	172.16.2.128
AUDITORIA	VLAN120	172.16.2.192
GERENCIA	VLAN130	172.16.3.0
DESARROLLO ORGANIZACIONAL	VLAN140	172.16.3.64
COBRANZAS	VLAN150	172.16.3.128
SEGUROS	VLAN160	172.16.3.192
IMPRESORAS	VLAN170	192.168.30.0
SERVIDORES	VLAN180	192.168.50.0
DMZ	VLAN190	10.0.0.0
VOIP	VLAN200	192.168.10.0

4.7.3 DMZ (Zona desmilitarizada)

La Zona Desmilitarizada se trata de una red local situada entre la red interna de una compañía y una red externa, generalmente la Internet.

La DMZ tiene como objetivo que las conexiones internas y externas a la DMZ se permitan, por otro lado, que las conexiones desde la DMZ sólo sean permitidas a la red externa, mientras que las maquinas locales en la DMZ no se conecten a la red interna. La DMZ se usa para acceder desde fuera a los servidores internos de la red, como servidores de e-mail, Web y DNS.

Este tipo de configuración permite proteger a la intranet, en caso de ataques a la DMZ de la red. Cada segmento de la red estará conectado de forma que se pueda separar la DMZ, la intranet y la red externa. Por lo que se utilizará:

- ✓ Dos puertos del firewall que se conecten a un puerto de cada switch de core, pertenecientes a la subred de servidores, para separar la DMZ.
- ✓ Dos puertos del firewall que se conecten a un puerto de cada switch de core para conectarse a la red interna.
- ✓ Un puerto del firewall que se conecte a un puerto del router del ISP, para conectarse a la red externa.

4.8 Seguridad en la red

Orientados a proveer condiciones seguras y confiables en la red de datos se diseñan métodos y técnicas de seguridad. En base a lo anterior se puede prevenir e identificar el acceso no autorizado a la red de datos para proceder a bloquear a los llamados “intrusos”; además con este tipo de control sube la productividad al tener menos interrupciones en el trabajo reduciendo así lo costos que podrían producir las violaciones de seguridad.

4.8.1 Seguridad perimetral de la red

La información manejada al interno de la red resulta ser vulnerable de accesos externos debido a que la red de datos está conectada al Internet, por lo tanto, es de vital importancia la seguridad perimetral en la red, en la institución financiera al hablar de seguridad perimetral se hace referencia al firewall tipo appliance de la marca Check Point que se encuentra actualmente implementado y funcionando, esta solución de seguridad básicamente cumple con las siguientes funciones:

- ✓ Control de acceso, al bloquear las redes a accesos no permitidos desde el interior, así como desde redes externas
- ✓ Proteger elementos tanto de hardware como de software los cuales son parte de la red interna.
- ✓ Permitir niveles de acceso por usuario, tanto para usuarios internos como para usuarios externos de la red.

4.8.2 Firewall

Dentro de la institución financiera en base a la recomendación realizada por la empresa EBTEL quienes son especialistas en seguridad perimetral, se administra un firewall de la marca Check Point, el cual está instalado en el punto donde la red se conecta a una red externa o al Internet y la red interna, con este equipo se han implantado políticas de control de acceso entre las redes antes mencionadas. De esta manera se previene el acceso no autorizado de intrusos desde redes externas, se analiza la información que ingresa o sale al intranet y se filtra la misma utilizando reglas determinadas.

El firewall con el que cuenta la institución financiera actualmente presenta las siguientes características:

Tabla 27.

Características del Firewall

Firewall
Manejar filtros en base a la dirección IP, para controlar la navegación en internet.
Tamaño del Disco 300 GB.
Tamaño de la RAM 2048 MB.
Puertos de red 10/100/1000 Mbps.
Soporte de Administración mediante SNMP.
Manejo de IPV4 e IPV6 (Dual Stack), VPN.
Permitir la implementación de VLANs, NAT, enrutamiento estático y dinámico.

4.8.3 Dimensionamiento del Firewall Corporativo

El Firewall corporativo, maneja grades volúmenes de tráfico al estar ubicado en la capa de core de la red, por ello debe presentar altas prestaciones debido a que a este equipo se conectarán los 2 switches de core que se presenta como propuesta en este rediseño, además de también estar conectado el router del ISP. En la tabla 28 se visualiza en número de puertos necesarios para el firewall.

Tabla 28.

Número de puertos para el Firewall

Firewall	SW_Core1	SW_Core1	Router ISP
Puerto	Gi0/1-GI0/2	Gi0/3-GI0/4	Gi0/5- Gi0/6
Total (Puertos)	2	2	2
	6		

En base a la tabla 28, se necesita 6 puertos para el firewall, en función de la escalabilidad se determina que se requiere un firewall que tenga al menos 6

puertos Gigabit Ethernet. Por lo cual se requiere mantener el firewall actualmente instalado, debido a que el mismo dispone de los 12 puertos.

4.9 Nuevo diseño de red

Lo anteriormente expuesto con respecto al capítulo 4 ha servido de base para realizar el nuevo diseño de red, donde se muestra claramente un diseño jerárquico de red, el cual se muestra a continuación.

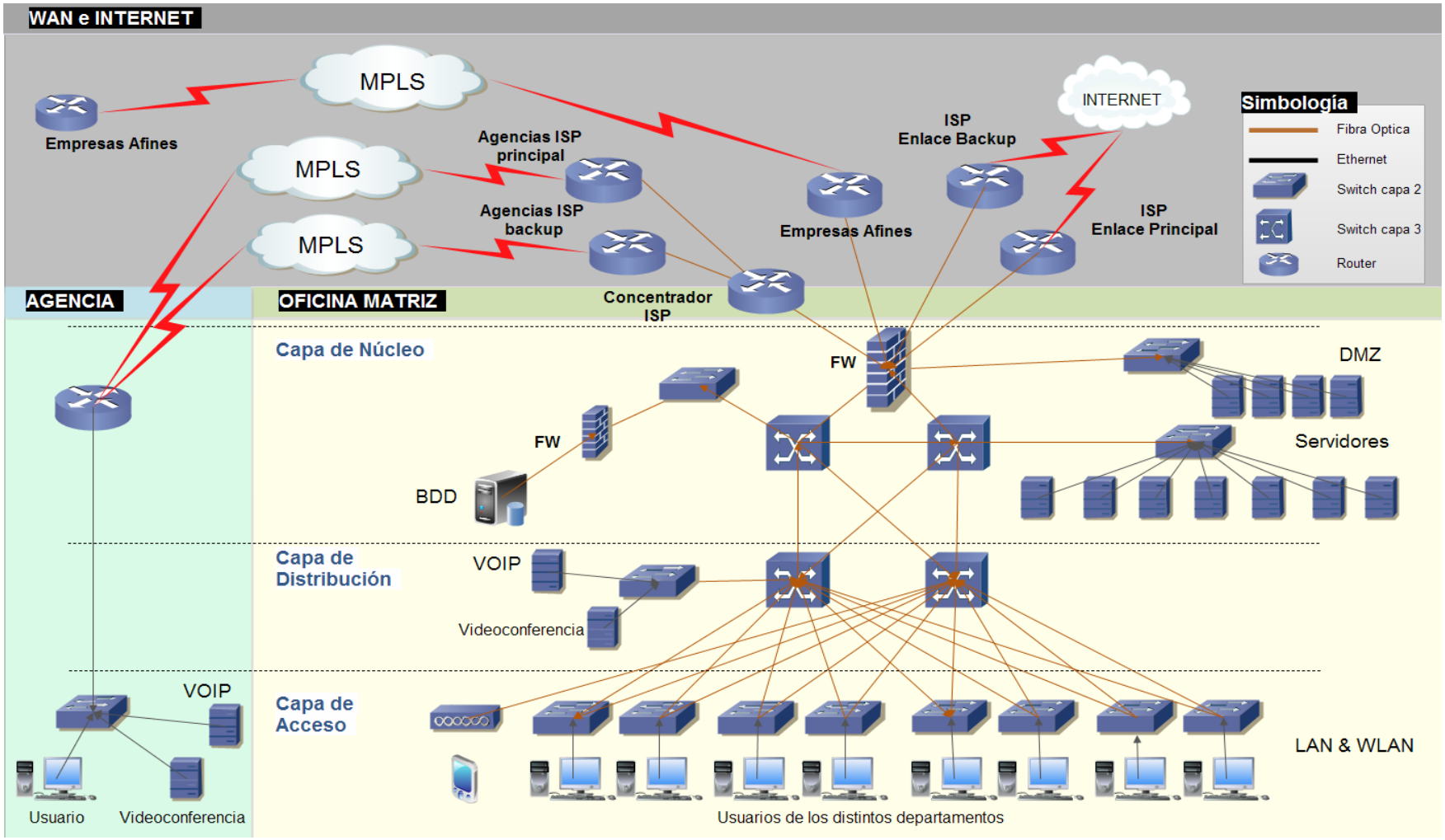


Figura 28. Nuevo diseño de red para la Cooperativa 29 de Octubre Ltda.

4.10 Calidad de Servicio (QoS)

4.10.1 Elección del modelo de Calidad de Servicio (QoS)

Se puede resumir que el diseño actual se trata de un servicio del mejor esfuerzo (Best Effort), pero debido a que no ofrece niveles de servicio para aplicaciones en tiempo real resulta que no es el más adecuado, puesto que existe la necesidad de un ancho de banda reservado para que una red funcione sin problema al manejar diferentes tipos de servicio como el de VoIP, los cuales se caracterizan por tener altos niveles de congestión.

En el caso de esta institución financiera el ancho de banda de internet no es un problema como ya se mencionó en un apartado del capítulo 3, que su capacidad es de 30 Mbps, por el contrario, a nivel de enlace WAN si es limitado siendo su capacidad para cada agencia de 2 Mbps, esto hace necesario la implementación de calidad de servicio en las redes que actualmente se manejan, para hacer un uso óptimo de los recursos y obtener el menor tiempo de retardo, latencia y pérdida de paquetes. Todo esto con la finalidad de conseguir buenos resultados en cuanto a tiempos de respuesta.

Existe disponibilidad de dos modelos que permiten implementar calidad de servicio (QoS) en una red, tal como se mencionó en el ítem 2.8.1, el modelo de Servicios Diferenciados (DiffServ) y el modelo de Servicios Integrados (IntServ).

En base a las desventajas y ventajas mostradas en la sección 2.8.1, se concluye que el modelo más adecuado para ser utilizado en el esquema de implementación de calidad de servido (QoS) por las ventajas que ofrece sobre IntServ, es el DiffServ.

4.10.2 Selección de parámetros y métodos para QoS

Para la implementación de calidad de servicio (QoS), se ha elaborado un cuadro el cual se muestra en la tabla 29, aquí se resume los parámetros para la implementación de QoS.

Tabla 29.

Parámetros seleccionad os para la implementación de QoS

	Parámetro	**Método**
Asignar ancho de banda en forma diferenciada	Clasificación de tráfico	ACL
	Marcado de tráfico	DSCP
Administrar la congestión de la red	Manejo de congestión de paquetes	CBWFQ / LLQ
	Evasión de congestión	WRED

4.10.3 Parámetros de calidad de servicio para la oficina matriz

La metodología a aplicarse en cuanto a la asignación de ancho de banda a cada una de las clases en la oficina matriz se detalla a continuación.

El uso de ancho de banda de las aplicaciones que operan desde de la oficina matriz se las puede apreciar en la tabla 30, para la asignación del porcentaje de reserva de ancho de banda aplicando calidad de servicio (QoS) es realizado de la siguiente manera: se divide el consumo de cada una de las aplicaciones para el 70% que es el coeficiente correspondiente al umbral mínimo de descarte. (Acurio, 2015).

A continuación, se realiza el cálculo del porcentaje para uso de canal WAN de las aplicaciones de software y de red según los valores obtenidos en el punto 4.5.

Tabla 30.

Asignación de ancho de banda para uso de canal WAN.

#	Aplicación de Software	Kbps	Kbps QoS
1	Voz sobre IP	5984	8548.57
2	Sistema de video conferencia	4096	5851.43
3	Core Bancario	4488	6411.43
4	Correo	157.83	225.47
5	Descarga de archivos	1246.54	1780.77
6	Acceso a la web	18700	26714.29

La columna llamada “Kbps QoS” de la tabla anterior es producto del cálculo (Kbps / 0.70).

Después de haber obtenido de cada aplicación los porcentajes de uso del canal WAN, con el objetivo de agruparlas en clases de servicio se debe evaluar la concurrencia de uso de las aplicaciones, caso contrario se debe crear clases para cada aplicación.

En la tabla 31, se visualiza la repartición del ancho de banda a las clases de servicio y la asignación de las mismas a las aplicaciones.

Tabla 31.

Asignación ancho de banda de la Oficina Matriz.

Clase	Aplicación	Valor DSCP	Ancho de Banda [%]
VOIP	VoIP	EF	5
VIDEO_V	Video Conferencia	AF41	22
APLICACIONES	Core Bancario	AF31	5
OTRAS	BASES DE DATOS	AF21	8
	CORREO	AF22	
	ANTIVIRUS	AF23	
POR DEFECTO	OTROS	Default	

4.11 Norma PCI DSS

El propósito fundamental de esta sección es incorporar los requerimientos de seguridad de la norma PCI DSS, mismos que fueron tomados en cuenta al momento de plantear el nuevo diseño de la red multiservicios en los puntos 4.5 al 4.7.

Cumplir con los requerimientos de seguridad de la norma PCI DSS beneficiará a la institución financiera significativamente ya que su red de datos no será fácilmente vulnerable a los ataques de ciberdelincuentes.

En la tabla 32 se muestra la matriz que resume los requisitos que la institución financiera cumple con respecto a la norma PCI DSS.

Tabla 32.

Requisitos que la cooperativa cumple - Norma PCI DSS

Requisito	**Nombre**	**Descripción**	**¿Cumple la Norma?**
Requisito 3:	Proteja los datos del titular de la tarjeta que fueron almacenados	Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos. También se deberían considerar otros métodos eficaces para proteger los datos almacenados oportunidades para mitigar posibles riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario; truncar los datos del titular de la tarjeta si no se necesita el PAN (número de cuenta principal) completo y no enviar el PAN (número de cuenta principal) utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea.	SI

Requisito 4:	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	La información confidencial se debe cifrar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación siguen siendo los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.	SI
Requisito 5:	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.	El software malicioso, llamado "malware", incluidos los virus, los gusanos (worm) y los troyanos (Trojan), ingresa a la red durante muchas actividades de negocio aprobadas incluidos los correos electrónicos de los trabajadores y la utilización de Internet, de computadoras portátiles y de dispositivos de almacenamiento y explota las vulnerabilidades del sistema. El software antivirus deberá utilizarse en todos los sistemas que el malware, por lo general, afecta para proteger los sistemas contra las amenazas de software maliciosos actuales o que eventualmente se desarrollen. Se puede considerar la opción de incluir otras soluciones antimalware como complemento del software antivirus; no obstante, estas soluciones adicionales no reemplazan la implementación del software antivirus.	SI

Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras	Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas deben contar con los parches de software correctos para evitar que personas malintencionadas o software maliciosos usen, de manera indebida, o pongan en riesgo los datos del titular de la tarjeta.	SI
Requisito 7:	Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo.	SI

Requisito 9:	Restringir el acceso físico a los datos del titular de la tarjeta	Cualquier acceso físico a datos o sistemas que alojen datos de titulares de tarjetas permite el acceso a dispositivos y datos, así como también permite la eliminación de sistemas o copias en papel, y se debe restringir correctamente. A los fines del Requisito 9, “empleados” se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que estén físicamente presentes en las instalaciones de la entidad. "Visitante” se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones durante un tiempo no prolongado, generalmente no más de un día. “Medios” hace referencia a todos los medios en papel y electrónicos que contienen datos del titular de la tarjeta.	SI
Requisito 10:	Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de	Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el rastreo, alertas y análisis cuando algo no funciona bien. Determinar la causa de un riesgo es muy difícil, si no imposible, sin los registros de la actividad del sistema.	SI

	las tarjetas		
Requisito 11:	Pruebe con regularidad los sistemas y procesos de seguridad.	Las vulnerabilidades son descubiertas continuamente por personas malintencionadas e investigadores y son introducidas mediante software nuevo. Los componentes, procesos y software personalizado del sistema se deben probar con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico.	SI
Requisito 12:	Mantener una política que aborde la seguridad de la información de todo el personal	Una política de seguridad sólida establece el grado de seguridad para toda la entidad e informa al personal lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos. A los fines del Requisito 12, el término "personal" hace referencia a los empleados de tiempo completo y parcial, a los empleados temporales, a los contratistas y consultores que "residen" en las instalaciones de la entidad o que tienen acceso al entorno de datos del titular de la tarjeta.	SI

Tomado de (Council, 2013)

De los requisitos de la norma PCI DSS, en el presente trabajo se analizarán de forma específica los que se resume en la tabla 33.

Sin embargo, los demás parámetros son considerados de forma implícita en el diseño y gestión de la red y políticas de seguridad de la misma.

Tabla 33.

Requisitos de la norma PCI DSS a analizar.

Requisito	Descripción
Requisito 1:	Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas
Requisito 2:	No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Requisito 8:	Identificar y autenticar el acceso a los componentes del sistema

4.11.1 Matrices de requerimientos

Las matrices elaboradas en esta sección fueron elaboradas en base a la revisión de los sistemas y documentación presentada por la cooperativa, además de las entrevistas realizadas al administrador de la red en el mes de Octubre 2016. En las matrices se realiza un análisis de la situación actual de la red de la cooperativa y también se considera si el rediseño de red propuesto anteriormente da cumplimiento a cada uno de los tres requisitos planteados de la norma PCI DSS.

A continuación, se detallan los campos que contiene la matriz:

- ✓ **Objetivo a evaluar**: se enumera el título del requisito la norma PCI DSS.
- ✓ **N°**: se menciona el sub requisito de la norma.
- ✓ **Procedimiento:** consta el detalle del sub requisito de la norma.
- ✓ **Comentario:** se describe las observaciones realizadas a la institución financiera en base a la revisión de los sistemas y documentación

presentada por la cooperativa y las entrevistas realizadas al administrador de la red.

- ✓ **¿La situación actual cumple la Norma?:** da a conocer si la situación actual de la red de la cooperativa en cuanto al cumplimiento de la norma.
- ✓ **¿El rediseño cumple la norma?:** da a conocer si la situación si el rediseño de la red cumple la norma.
- ✓ **Recomendación:** se describe las recomendaciones realizadas a la cooperativa en base a la revisión de los sistemas y documentación presentada por la cooperativa y las entrevistas realizadas al administrador de la red.

Nota: La información en cuanto a la documentación que evidencien los comentarios de las matrices de requerimientos no será publicada en esta tesis debido a que el área de Seguridad de la Información de la cooperativa la considera como confidencial, por lo cual este trabajo escrito se limitará a realizar un análisis en base a la información que se recolecte al llenar las matrices.

Los requisitos expuestos en las matrices de los requerimientos 1, 2 y 8 de la norma PCI DSS, hace referencia al documento “Normas de seguridad de datos” en su versión 3.0 (véase tabla 34).

Tabla 34.

Matrices de los requerimientos 1, 2 y 8

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas						
Empresa Auditada:	Cooperativa de Ahorro y Crédito “29 de octubre” Ltda					
Responsable:	Wladimir Muñoz					
Supervisa:	Santiago Hernández					
Objetivos a evaluar	**Nº**	**Procedimiento**	**Comentario**	**¿La situación actual cumple la Norma?**	**El rediseño cumple la Norma?**	**Recomen-dación**
1.1 Establezca e implemente normas de configuración para firewalls y routers que incluyan lo siguiente:	1.1	Inspeccione las normas de configuración de firewalls y routers y otros documentos especificados a continuación para verificar el cumplimiento e	La Cooperativa cumple con este requerimiento de la norma PCI DSS, puesto que el departamento de infraestructura	SI		

		implementación de las normas.	mediante el instructivo llamado “Conexión de Internet y Cambios de Configuración al Firewall”, y la documentación denominada “Administración de Redes” aprueba las conexiones de red, de tal forma que los solicitantes del servicio llenen y firmen formularios de responsabilidad de uso del servicio de red. Con respecto a los cambios reales realizados en las configuraciones de firewalls, se tiene una			
1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers	1.1.1.a	Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente:		SI		
		•Conexiones de red •Cambios en las configuraciones de firewalls y routers				
	1.1.1.b	Para obtener una muestra de las conexiones de red, entreviste al personal responsable y revise los registros para verificar que se hayan aprobado y probado las conexiones		SI		

		de red	matriz donde se registran las pruebas y aprobaciones de los cambios.			
	1.1.1.c	Identifique una muestra de los cambios reales realizados en las configuraciones de firewalls y routers, compárela con los registros de cambio y entreviste al personal responsable para verificar que los cambios se hayan probado y aprobado.		SI		

1.1.2 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.	1.1.2.a	Revise los diagramas y observe las configuraciones de red para verificar que exista un diagrama de red actual que documente todas las conexiones con los datos de los titulares de tarjetas, incluso las redes inalámbricas.	La Cooperativa si dispone del diagrama de red, en el cual se identifica como está conectado el entorno de datos de titulares de tarjetas y las distintas redes a su alrededor, en el diagrama se puede identificar el servidor "Card Controller" que es quien controla la transaccionalidad de las tarjetas de pago. Con respecto a las redes inalámbricas, la Cooperativa dispone de una red inalámbrica funcionando en el	NO	SI	Se recomienda actualizar el diagrama de red ya que el mismo no incluye la red inalámbrica.
	1.1.2.b	Entreviste al personal responsable para verificar que el diagrama esté		SI		

		actualizado.	edificio matriz la cual es usada por Directores, Subgerentes y el Gerente General, los permisos para dicha red están limitados exclusivamente al uso del Core Financiero, por ende, el tráfico			
1.1.3 El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes	1.1.3	Revise el diagrama de flujo de datos y entreviste al personal para verificar lo siguiente en el diagrama: • Muestra los flujos de datos de titulares de tarjetas entre los sistemas y las redes. • Se mantiene al día y está actualizado según los	La institución no se dispone del diagrama requerido en este ítem	NO	NO	Se recomienda realizar el diagrama requerido en este ítem

		cambios implementados en el entorno.				
1.1.4 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	1.1.4.a	Revise las normas de configuración de firewalls y controle que incluyan los requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna	Este ítem se cumple de la siguiente manera: La Cooperativa tiene configurado un solo firewall, en el cual cada de las interfaces que este dispone están separadas en segmentos de red diferentes. Por otro lado, se ha verificado	SI		

	1.1.4.b	Verifique que el diagrama de red actual concuerde con las normas de configuración de firewalls diagramas de red.	que concuerde las configuraciones realizadas en el firewall el con el diagrama de red. Finalmente, existe en el firewall la respectiva configuración de red que separa los distintos segmentos de red como lo son la red interna, DMZ, etc.	SI		
	1.1.4.c	Revise las configuraciones de red para verificar que haya un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna, de acuerdo con las normas de configuración documentadas y los diagramas de red.		SI		

1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.	1.1.5.a	Verifique que las normas de configuración de firewalls y routers incluyan la descripción de los grupos, las funciones y las responsabilidades para la administración de los componentes de la red.	La Cooperativa dispone del manual de funciones de la institución financiera en el cual se detalla que existe distintos tipos de perfiles, por ejemplo: existe usuarios para administración del sistema con permisos totales y por otro lado existen usuarios con menos privilegios para el ingreso al firewall. En base al manual de funciones se realizan las configuraciones de para la asignación de responsabilidades, agrupación y funciones	SI		
	1.1.5.b	Entreviste al personal responsable de administrar los componentes de la red para confirmar que las funciones y las responsabilidades se hayan asignado según lo documentando.		SI		

			de los usuarios.			
1.1.6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros. Entre los servicios, protocolos o puertos inseguros, se incluyen, a modo de ejemplo, FTP, Telnet,	1.1.6.a	Verifique que las normas de configuración de firewalls y routers incluyan una lista documentada de todos los servicios, protocolos y puertos, incluso una justificación de negocio para cada uno, por ejemplo, HTTP (protocolo de transferencia de hipertexto) y SSL (protocolo de capa de conexión segura), SSH (Secure Shell) y VPN (red privada virtual).	La cooperativa si dispone de documentos de la configuración realizada en el firewall listando los parámetros requeridos en este ítem. Está configuración está realizada por cada una de las interfaces del firewall. Una vez que se identificó los servicios protocolos y puertos inseguros permitidos se pudo observar la documentación de las	SI		

POP3, IMAP y SNMP versión 1 y versión 2.	1.1.6.b	Identifique los servicios, protocolos y puertos inseguros permitidos y verifique que se hayan documentado las funciones de seguridad de cada servicio.	funciones de seguridad de cada servicio. Finalmente se verificó lo requerido por la norma en el punto 1.1.6.b y se verificó las configuraciones de las políticas implementadas en el firewall, a manera de ejemplo se puede mencionar que existe una configuración la cual abre determinados puertos y el resto por política de firewall se bloquean.	SI		
	1.1.6.c	Revise las configuraciones de firewalls y routers para verificar que se hayan implementado las funciones de seguridad para cada servicio, protocolo y puerto inseguros.		SI		
1.1.7 Requisito de la revisión de las normas de firewalls y routers, al	1.1.7.a	Verifique que las normas de configuración de firewalls y routers soliciten	Por parte de la Cooperativa recién se actualizaron los	NO	NO	Se recomienda que

menos, cada seis meses.		la revisión de las reglas, al menos, cada seis meses.	instructivos este año, y en el mes de octubre 2016 se creó el subproceso de seguridad de servidores. Por lo cual el cumplimiento de este requisito se lo realizará en medida que se cumpla los primeros 6 meses.			en el mes de abril se efectúe la revisión de las reglas de firewall.
	1.1.7.b	Examine la documentación relacionada con las revisiones de las reglas y entreviste al personal responsable para verificar si las reglas se revisan, al menos, cada seis meses.		----	---	
1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de	1.2	Revise las configuraciones de firewalls y routers y realice las siguientes acciones para verificar que se restringen las conexiones entre redes no confiables y todo componente del sistema en el entorno de	La Cooperativa mediante reglas de firewall restringe la conexión entre redes en las que no se puede confiar y todo lo que compone el sistema de entorno de datos de titulares de tarjetas. En	SI		

titulares de tarjetas.		datos de titulares de tarjetas:	cuanto a las normas de configuración de firewalls si se identifica el tráfico que entra y sale al CDE. Así también se verificó que se restrinja al mínimo necesario el tráfico que entra y sale para el CDE. Finalmente, todo el tráfico entrante y saliente se niega de manera específica como lo indica la norma PCI DSS.			
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.	1.2.1.a	Revise las normas de configuración de firewalls y routers para verificar que identifican el tráfico entrante y saliente necesario para el entorno de datos de titulares de tarjetas.		SI		
	1.2.1.b	Revise las configuraciones de firewalls y routers para verificar que el tráfico entrante y saliente esté restringido a la cantidad necesaria para el entorno de datos de titulares de tarjetas.		SI		

	1.2.1.c	Revise las configuraciones de firewalls y routers para verificar que todo tráfico entrante y saliente se niegue de manera específica, por ejemplo, mediante una declaración explícita “negar todos” o una negación implícita después de una declaración de permiso.		SI		
1.2.2 Asegure y sincronice los archivos de configuración de routers.	1.2.2.a	Revise los archivos de configuración del router para verificar que están protegidos contra el acceso no autorizado.	NO APLICA, no se tiene la administración de los routers, los routers son administrados por el ISP.	----	----	
	1.2.2.b	Revise las configuraciones del router y verifique que estén		----	----	

		sincronizadas, por ejemplo, que la configuración en ejecución (o activa) coincida con la configuración de inicio (que se usa cuando la máquina se reinicia).				
1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el	1.2.3.a	Revise las configuraciones de firewalls y routers, y verifique que se hayan instalado firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta	La cooperativa tiene configurada una regla de firewall que niega el tráfico entre la red inalámbrica y el CDE.	SI		
	1.2.3.b	Verifique que los firewalls nieguen o, si el tráfico es necesario para fines		SI		

entorno inalámbrico y el entorno de datos del titular de la tarjeta.		comerciales, permitan solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.				
1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.	1.3	Revise las configuraciones de firewalls y routers, que incluye, entre otros, el router de estrangulamiento de Internet, el router DMZ y el firewall, el segmento de titulares de tarjetas de DMZ, el router de perímetro y el segmento de la red interna del titular de la tarjeta, y realice lo siguiente a fin de	La cooperativa mediante regla de firewall bloquea la exposición del CDE hacia el internet.	SI		

		determinar que no exista un acceso directo entre la Internet y los componentes del sistema en el segmento de red interna de los titulares de tarjeta:				
1.3.1 Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado	1.3.1	Revise las configuraciones de firewalls y routers, y verifique que se haya implementado una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	La Cooperativa si tiene implementada una DMZ mediante regla de firewall.	SI		

1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	1.3.2	Revise las configuraciones de firewalls y routers, y verifique que se restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	La Cooperativa tiene configurada en el firewall una regla, por lo cual cumple con este ítem requerido.	SI		
1.3.3 No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.	1.3.3	Revise las configuraciones de firewalls y routers, y verifique que no se permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno de datos del titular de la tarjeta.	La Cooperativa tiene creada una regla de firewall para no permitir tráfico directo desde la internet al CDE	SI		
1.3.4 Implementar medidas antisuplantación para detectar y bloquear	1.3.4	Revise las configuraciones de firewalls y routers, y verifique que se hayan	La cooperativa no tiene realizadas estas configuraciones a nivel de firewall, se las tiene	NO	NO	Se recomienda que se

direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna).		implementado medidas contra la suplantación, por ejemplo, las direcciones internas no se pueden transferir de Internet a la DMZ.	implementadas a nivel del antivirus.			impleme nten medidas contra la suplanta ción a nivel de firewall.
1.3.5 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.	1.3.5	Revise las configuraciones de firewalls y routers, y verifique que el tráfico saliente proveniente del entorno de datos del titular de la tarjeta a Internet esté explícitamente autorizado.	La Cooperativa tiene definida una regla de firewall que corta la salida al internet al tráfico que proviene del CDE.	SI		

1.3.6 Implemente la inspección completa, también conocida como filtrado dinámico de paquetes. (Es decir, sólo se permite la entrada a la red de conexiones "establecidas").	1.3.6	Revise las configuraciones de firewalls y routers y, verifique que el firewall realice una inspección completa (filtrado de paquetes dinámico). (Sólo se debe permitir la entrada de conexiones establecidas, y sólo si están asociadas a una sesión establecida anteriormente).	La Cooperativa no tiene implementado en el firewall la opción para cumplir con este ítem.	NO	NO	Se recomienda se implemente la configuración de firewall solicitada en este ítem.
1.3.7 Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna	1.3.7	Revise las configuraciones de firewalls y routers, y verifique que los componentes del sistema que almacenan datos del titular de la tarjeta (como	La Cooperativa a la base de datos esta la sitúa en una subred segregada, es decir en la red de servidores mas no en la DMZ.	SI		

segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.		una base de datos) se encuentren en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables				
1.3.8 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.	1.3.8.a	Revise las configuraciones de firewalls y routers, y verifique que se hayan implementado métodos para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde redes internas a Internet.	La Cooperativa en base a las reglas de administración de firewall otorga permisos de ingreso al firewall con distintos privilegios. Es así que solo ciertos usuarios pueden ver si modificar las direcciones IP de las interfaces y el enrutamiento en la configuración del firewall.	SI		
	1.3.8.b	Entreviste al personal, revise la documentación y verifique que no se autorice la divulgación de		SI		

		ninguna dirección IP privada ni de información de enrutamiento a entidades externas.				
1.4 Instale software de firewall personal en todos los dispositivos móviles o de propiedad de los trabajadores que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder a la red. Las configuraciones de firewalls incluyen lo siguiente: • Los	1.4.a	Revise las políticas y las normas de configuración para verificar lo siguiente: • El software de firewall personal se debe incluir en todos los dispositivos móviles o de propiedad de los trabajadores que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usen para acceder a la red. • Los	La Cooperativa tiene instalado el software de firewall personal en como parte de la funcionalidad del antivirus. Así también el área de seguridad de la información ordenó la instalación de un software llamado DLP (prevención de pérdida de datos) en laptops y demás dispositivos finales, que entre sus funciones tiene como finalidad el bloqueo de	SI		Se recomienda presentar las políticas y las normas relacionadas con este ítem debidamente documentadas.

parámetros específicos de configuración se definen para cada software de firewall personal. • El software de firewall personal funciona activamente. • Los usuarios de dispositivos móviles o de propiedad de los trabajadores no pueden alterar el software de firewall personal.		parámetros específicos de configuración se definen para cada software de firewall personal. • El software de firewall personal está configurado para funcionar activamente. • El software de firewall personal está configurado para que los usuarios de dispositivos móviles o de propiedad de trabajadores no puedan alterarlo.	dispositivos para no permitir la salida de datos, por ejemplo: bloqueo de puertos USBs. En cuanto a dispositivos móviles, es política de la institución no trabajar con ellos.			
1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls	1.5	Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para	La Cooperativa si tiene la documentación con respecto a este ítem, dicho documento se llama “Instructivo de administración y	SI		

estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		administrar los firewalls cumplan con lo siguiente: • Estén documentados. • Estén implementados. • Sean de conocimiento para todas las partes afectadas.	monitoreo de red" dentro del subproceso "Seguridad y Control de los Recursos Tecnológicos".			
Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores						
Empresa Auditada:	Cooperativa de Ahorro y Crédito "29 de octubre" Ltda					
Responsable:	Wladimir Muñoz					
Supervisa:	Santiago Hernández					
Objetivos a evaluar	**Nº**	**Procedimiento**	**Comentario**	**¿La situación actual cumple la Norma?**	**¿El rediseño cumple la Norma?**	**Recomen-dación**

2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los	2.1.a	Escoja una muestra de los componentes del sistema e intente acceder a los dispositivos y aplicaciones (con la ayuda del administrador del sistema) con las cuentas y contraseñas predeterminadas por el proveedor y verifique que se hayan cambiado TODAS las contraseñas predeterminadas (incluso las de los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS [puntos de ventas], las	La Cooperativa cuenta con el instructivo de “Seguridad y Control de los Recursos Tecnológicos”, el cual indica que se debe cambiar los valores por defecto que deja configurados el proveedor y también se deshabilita las cuentas de usuario que no son necesarias al momento de poner en funcionamiento un sistema en la red, en base al instructivo anteriormente mencionado se probó el acceso a uno de los	NO	NO	Se recomienda revisar la configuración del SNMP, ya que el administrador de red no está seguro si este protocolo está manejando cuentas predeter

terminales de POS (puntos de venta), las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.		cadenas comunitarias de SNMP [protocolo simple de administración de red]). (Utilice los manuales y las fuentes de los proveedores que se encuentran en Internet para encontrar las cuentas y las contraseñas proporcionadas por estos).	sistemas y en efecto, el sistema no tenía en su usuarios y clave de acceso valores predeterminados, en cuanto a los POS para puntos de ventas que menciona el ítem la Cooperativa no dispone de los mismos. Finalmente, con respecto a las cadenas SNMP el administrador de red no está seguro de que maneje en su configuración cuentas predeterminadas.			minadas.
	2.1.b	Para la muestra de los componentes del sistema, verifique que todas las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los software de seguridad, las				

		aplicaciones, los sistemas, los terminales de POS [puntos de ventas], SNMP [protocolo simple de administración de red], etc.) se hayan eliminado o estén deshabilitadas.				
	2.1.c	Entreviste al personal, revise la documentación de respaldo y verifique lo siguiente: • Se cambien todos los valores predeterminados proporcionados por los proveedores (incluso las contraseñas predeterminadas de sistemas operativos, software que prestan	La cooperativa si cumple con este ítem ya que al revisar la documentación de respaldo incluida en el “Subproceso de Aseguramiento de Recursos Tecnológicos” se determinó que si se procede a cambiar todas las	SI		

		servicios de seguridad, cuentas de aplicaciones y sistemas, terminales de POS [puntos de ventas], cadenas comunitarias de SNMP [protocolo simple de administración de red], etc.), antes de instalar un sistema en la red.	configuraciones por defecto realizadas por el proveedor antes de poner en funcionamiento un nuevo sistema dentro de la red. Además de forma periódica las cuentas de usuario innecesarias se inhabilitan y se borran.			
		• Las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los software de seguridad, las aplicaciones, los sistemas, los terminales de POS [puntos de ventas], SNMP [protocolo simple de administración				

		de red], etc.) se cambien o inhabiliten antes de instalar un sistema en la red.				
2.1.1 En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transmiten datos del titular de la tarjeta, cambie TODOS los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica	2.1.1.a	Entreviste al personal y revise la documentación de respaldo para verificar lo siguiente: • Las claves de cifrado predeterminadas se cambiaron al momento de la instalación.	NO APLICA, debido a la política de la institución de no trabajar con ellos dispositivos móviles.	---	---	

al momento de la instalación, incluidas, a modo de ejemplo, las claves de cifrado inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias SNMP (protocolo simple de administración de red).		• Las claves de cifrado se cambian cada vez que una persona que tenga conocimiento de estas cesa en sus funciones o se traslada a otro cargo en la empresa.				
	2.1.1.b	Entreviste al personal, revise las políticas y procedimientos y verifique lo siguiente:		---	---	
		• Las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas se cambian al momento de la instalación.				
		• Las frases/contraseñas predeterminadas de los				

		puntos de accesos se cambian al momento de la instalación.				
	2.1.1.c	Revise la documentación proporcionada por el proveedor, inicie sesión en los dispositivos inalámbricos con la ayuda del administrador del sistema y verifique lo siguiente:		---	---	
		• No se usan las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas.				

		• No se usan las contraseñas/frases predeterminadas de los puntos de acceso.				
	2.1.1.d	Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que el firmware de los dispositivos inalámbricos se actualice a fin de admitir el cifrado sólido para lo siguiente: • Autenticación en redes		---	---	

		inalámbricas.				
		• Transmisión en redes inalámbricas.				
		Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que se hayan cambiado los otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda.		---	---	
2.2 Desarrolle normas	2.2.a	Examine las normas de	Al examinar las normas	SI		

de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria. Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo: • Center for Internet Security (CIS) •		configuración de sistemas de la organización correspondientes a todos los tipos de componentes de sistemas y verifique que las normas de configuración de sistemas concuerden con las normas de alta seguridad aceptadas en la industria.	de configuración de los sistemas de la Cooperativa se verificó que estén de acuerdo a lo solicitado en el ítem 2.2.a. Adicionalmente la institución financiera dentro del instructivo “Seguridad y Control de los Recursos Tecnológicos” existe una plantilla donde se dice que la norma utilizada y que se aplica es la ISO 27001. En relación al cumplimiento del punto 2.2.b, actualmente no se han puesto en producción nuevos			
	2.2.b	Revise las políticas, entreviste al personal y verifique que las normas de configuración de sistemas se actualicen a medida que se identifiquen nuevas vulnerabilidades, tal como se define en el Requisito 6.1.		SI		

International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	2.2.c	Revise las políticas, entreviste al personal y verifique que se apliquen las normas de configuración de sistemas al configurar y comprobar que se instalaron nuevos sistemas antes de instalar un sistema en la red.	servicios como para comprobar que se cumpla este ítem. Finalmente se verificó que se cumpla con el ítem 2.2.d en cuanto a las normas de configuración de sistemas	SI		
	2.2.d	Verifique que las normas de configuración de sistemas incluyan los siguientes procedimientos para todos los tipos de componentes del sistema:		SI		
		• Cambiar los valores predeterminados de los proveedores y eliminar las cuentas predeterminadas innecesarias.				

		• Implementar solo una función principal por servidor a fin de evitar que coexistan funciones que requieran diferentes niveles de seguridad en el mismo servidor.				
		• Habilitar solo los servicios, protocolos, daemons, etc., necesarios, según lo requiera la función del sistema.				
		• Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros.				
		• Configurar los				

		parámetros de seguridad del sistema para evitar el uso indebido.				
		• Eliminar todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.				
2.2.1 Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor. (Por	2.2.1.a	Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones del sistema y verifique que se haya implementado solo una función principal en cada servidor.	La Cooperativa a nivel de servidores dispone de una plataforma virtualizada en VMWARE en la cual cada servidor tiene implementado solo una función principal	SI		

ejemplo, los servidores web, servidores de base de datos y DNS se deben implementar en servidores separados).	2.2.1.b	Si se utilizan tecnologías de virtualización, inspeccione las configuraciones del sistema y verifique que se haya implementado una sola función principal por componente de sistema o dispositivo virtual.		SI		
2.2.2 Habilite solo los servicios, protocolos y daemons, etc., necesarios, según lo requiera la función del sistema.	2.2.2.a	Seleccione una muestra de los componentes del sistema, inspeccione los servicios del sistema, daemons y protocolos habilitados y verifique que solo se habiliten los servicios o protocolos necesarios.	La cooperativa mediante regla de firewall habilita solo los servicios o protocolos necesarios. En cuanto a los servicios, daemons o protocolos habilitados son seguros ya que han sido	SI		

	2.2.2.b	Identifique los servicios, daemons o protocolos habilitados que no sean seguros, entreviste al personal y verifique que estén configurados de conformidad con las normas de configuración documentadas.	configurados conforme al instructivo “Seguridad y Control de los Recursos Tecnológicos””	SI		
2.2.3 Implemente funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSec VPN, para proteger los	2.2.3	Inspeccione los parámetros de configuración y verifique que las funciones de seguridad se hayan documentado e implementado en todos los servicios, daemons o protocolos no seguros.	Los parámetros de configuración y funciones de seguridad están implementados y funcionando como, por ejemplo: IPsec en el firewall, para páginas web SLL, para conexiones ftp se utiliza el S-FTP, en cuanto a la documentación sobre	NO	NO	Se recomienda realizar documentación sobre este ítem

servicios no seguros, como NetBIOS, archivos compartidos, Telnet, FTP, etc.			este ítem no se dispone de la misma.			
2.2.4 Configure los parámetros de seguridad del sistema para evitar el uso indebido.	2.2.4.a	Entreviste a los administradores del sistema o a los gerentes de seguridad para verificar que conocen las configuraciones comunes de parámetros de seguridad de los componentes del sistema.	En cuanto a este ítem, los sistemas han sido configurados de manera segura por el administrador del sistema conjuntamente con el oficial de seguridad de la información aplicando los parámetros de seguridad que cada componente del sistema recomienda aplicar.	SI		
	2.2.4.b	Revise las normas de configuración de sistemas y verifique que incluyan los valores comunes de los parámetros de		SI		

		seguridad.				
	2.2.4.c	Seleccione una muestra de los componentes del sistema e inspeccione los parámetros de seguridad comunes para verificar que se hayan configurado correctamente, según las normas de configuración		SI		
2.2.5 Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web	2.2.5.a	Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones y verifique que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos,	La cooperativa al momento de instalar un sistema operativo en un nuevo servidor realiza una instalación personalizada del mismo donde se selecciona solo las funcionalidades	---	---	Se recomienda realizar la respectiva documentación

innecesarios.		drivers, funciones, subsistemas, sistemas de archivos, etc.).	concretas a utilizarse, de esta manera se garantiza que funcionalidades innecesarias no se ejecuten. Pero no se evidencia documentación en cuanto a este ítem.			en cuanto a este ítem.
	2.2.5.b	Revise la documentación y los parámetros de seguridad, y verifique que las funciones habilitadas estén documentadas y admitan la configuración segura.		NO	NO	
	2.2.5.c	Revise la documentación y los parámetros de seguridad, y verifique que solo la funcionalidad documentada esté presente en la muestra de componentes del sistema.		NO	NO	

2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y otros tipos de acceso administrativo que no sea de consola.		Seleccione una muestra de los componentes del sistema y verifique que el acceso administrativo que no sea de consola se cifre al realizar lo siguiente:	El administrador de red cuando inicia sesión en cada sistema utiliza las tecnologías mencionadas en el ítem 2.3	SI		
	2.3.a	Observe a un administrador mientras inicia sesión en cada sistema y revise las configuraciones de los sistemas a fin de controlar que se invoca un método sólido de cifrado antes de que se solicite la contraseña del administrador.	A manera de ejemplo, al ingresar a utilizar los servicios de la cooperativa vía remota, se evidencia que se invoca un método de cifrado al establecerse la comunicación vía VPN. Así mismo se determina que con los comandos como Telnet y otros están	SI		Se recomienda hacer uso de un cifrado mediante una criptografía sólida cuando

	2.3.b	Revise los servicios y los archivos de parámetros en los sistemas a fin de determinar que Telnet y otros comandos de inicio de sesión remotos inseguros no están disponibles para acceso sin consola.	inhabilitados para ser usados. En cuanto al ítem 2.3.c, no se usa criptografía sólida como por ejemplo: AES, TDES, RSA, ECC, ElGamal, etc. Finalmente no se evidencia documentación alguna respecto al punto 2.3.	SI		se inicie sesión por parte del administrador en cada sistema. Así mismo, se recomienda realizar la documentación una vez que se impleme
	2.3.c	Observe a un administrador mientras inicia sesión en cada sistema y verifique que el acceso del administrador a cualquier interfaz de administración basada en la Web esté cifrado mediante una criptografía sólida.		NO	SI	

	2.3.d	Revise la documentación del proveedor y entreviste al personal a fin de controlar que se implemente una criptografía sólida para la tecnología usada de acuerdo con las mejores prácticas de la industria y las recomendaciones del proveedor.		NO	SI	nte una criptografía sólida.
2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS.	2.4.a	Revise el inventario del sistema para verificar que haya una lista de componentes del hardware y del software con una descripción de la función/uso de cada componente.	La cooperativa si dispone de un inventario del sistema, dentro de ella se verificó que exista un listado en el cual se describa las funciones de los componentes tanto de hardware	SI		

			como de software. Dicho inventario se actualiza cada año conforme a los cambios realizado durante ese período de tiempo.			
	2.4.b	Entreviste al personal y verifique que el inventario esté actualizado.				
2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros	2.5	Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros	La cooperativa implementa a cabalidad lo requerido en el ítem 2.5, dicha información ha sido documentada y se encuentra a disposición de todas las partes afectadas para su lectura en la	SI		

parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		parámetros de seguridad cumplen con lo siguiente: • Estén documentados. • Estén implementados. • Sean de conocimiento para todas las partes afectadas.	intranet.			

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema.						
Empresa Auditada:	Cooperativa de Ahorro y Crédito “29 de octubre” Ltda					
Responsable:	Wladimir Muñoz					
Supervisa:	Santiago Hernández					
Objetivos a evaluar	**Nº**	**Procedimiento**	**Comentario**	**¿La situación actual cumple la Norma?**	**¿El rediseño cumple la Norma?**	**Recomendación**
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la	8.1.a	Revise los procedimientos y confirme que definen procesos para cada uno de los siguientes puntos, desde el 8.1.1 hasta el 8.1.8.		---	---	
	8.1.b	Verifique que se implementen los procedimientos para la administración de identificación de usuarios				

siguiente manera:		mediante las siguientes acciones:				
8.1.1 Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.	8.1.1	Entreviste al personal administrativo y confirme que todos los usuarios tengan asignada una ID exclusiva para tener acceso a los componentes del sistema o los datos del titular de la tarjeta.	La cooperativa tiene realiza una asignación de una ID única para cada usuario ingrese a los componentes del sistema, de esta manera el acceso del usuario al sistema es controlado.	SI		
8.1.2 Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación.	8.1.2	En el caso de una muestra de ID de usuarios privilegiados e ID de usuarios generales, evalúe las autorizaciones asociadas y observe los parámetros del sistema a fin de verificar que todas las ID de usuarios y las ID	La cooperativa no dispone documentación respecto a este ítem.	NO	NO	Se recomienda elaborar la documentación que se refiere al

		de usuarios privilegiados se hayan implementado solamente con los privilegios especificados en la aprobación documentada.				ítem 8.1.2
8.1.3 Cancele de inmediato el acceso a cualquier usuario cesante.	8.1.3.a	Seleccione una muestra de los usuarios cesantes en los últimos seis meses y revise las listas de acceso de usuarios actuales, tanto para acceso local como remoto, para verificar que sus ID se hayan desactivado o eliminado de las listas de acceso.	La cooperativa realiza la revisión de las listas de los usuarios cesantes y actuales con acceso local cada mes, inactivándolos y eliminándolos según sea la solicitud del departamento de Talento Humano, pero no se realiza una revisión de los usuarios activos que tenga acceso remoto. Con	NO	NO	Se recomienda realizar la revisión de los usuarios activos que tenga acceso remoto.
	8.1.3.b	Verifique que todos los métodos de autenticación físicos, como tarjetas		SI		

		inteligentes, tokens, etc., se hayan devuelto o desactivado.	respecto al ítem 8.1.3.b, los métodos para autenticar el acceso son devueltos al departamento de infraestructura para posteriormente ser desactivados.			
8.1.4 Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.	8.1.4	Observe las cuentas de usuarios y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.	La cooperativa realiza la revisión de las cuentas de usuarios cada mes, por tanto se eliminan o se inactivan según sea el caso.	SI		
8.1.5 Administre las ID que usan los proveedores para acceder, respaldar o mantener los componentes del	8.1.5.a	Entreviste al personal y observe los procesos de administración de cuentas que usan los proveedores para acceder, respaldar o mantener los	La cooperativa habilita las cuentas de usuario para el acceso en el caso de que el proveedor las solicite y con presencia de una	SI		

sistema de manera remota de la siguiente manera: • Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. • Se deben monitorear mientras se usan.		componentes del sistema a fin de verificar que las cuentas que usan los proveedores para acceder de manera remota cumplen con lo siguiente:	persona interna que se haga responsable de la supervisión de las acciones que dicho proveedor realice remotamente, además las cuentas de usuarios son deshabilitadas si no están en uso.			
		• Se inhabilitan cuando no se usan.				
		• Se habilitan solo cuando el proveedor las necesita y se deshabilitan cuando no se usan.				
	8.1.5.b	Entreviste al personal y observe los procesos para verificar que se monitoreen las cuentas de acceso remoto de los proveedores mientras se utilizan.		SI		

8.1.6 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.	8.1.6.a	En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de autenticación se encuentren configurados de manera que se solicite que se bloquee la cuenta del usuario después de realizar, como máximo, seis intentos de inicio de sesión no válidos.	La cooperativa cumple con este sub requerimiento al bloquear la cuenta de usuario al agotarse los intentos de inicio de sesión permitidos, en este caso seis. De igual manera se sigue el mismo procedimiento de bloqueo de cuenta de usuario para los proveedores.	SI		

	8.1.6.b	**Procedimientos de pruebas adicionales para los proveedores de servicios:** Revise los procesos internos y la documentación del cliente/usuario y observe los procesos implementados a fin de verificar que las cuentas de usuarios no consumidores se bloqueen de forma temporal después de realizar, como máximo, seis intentos no válidos de acceso.		SI		

8.1.7 Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.	8.1.7	En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que solicite que, al bloquear la cuenta de un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.	La cooperativa no tiene una política que cumpla con el requerimiento del ítem 8.1.7	NO	NO	Se recomienda actualizar las políticas para cumplir con el requerimiento del ítem 8.1.7

8.1.8 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente.	8.1.8	En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que las funciones de tiempo máximo de inactividad del sistema/sesión se encuentren establecidas en 15 minutos o menos.	La cooperativa tiene establecida la política dentro del active directory para que las estaciones de trabajo sean bloqueadas después de estar inactivas por un lapso de 15 minutos o más. Una vez que el equipo se bloquee para volver a ingresar le solicitará contraseña.	SI		
8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios	8.2	Para verificar que los usuarios se autentiquen con una ID exclusiva y una autenticación adicional (por ejemplo, una contraseña/frase) para acceder a los datos	La cooperativa hace especial énfasis en el manejo de la autenticación de los usuarios para ingresar al sistema que maneja información de datos	SI		

no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios: • Algo que el usuario sepa, como una contraseña o frase de seguridad • Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente. • Algo que el usuario sea, como un rasgo biométrico.		del titular de la tarjeta, realice lo siguiente: • Revise la documentación que describe los métodos de autenticación utilizados. • Para cada tipo de método de autenticación utilizado y para cada tipo de componente del sistema, observe una autenticación para verificar que funcione de forma coherente con los métodos de autenticación documentado.	de tarjeta habientes, pues se utiliza dos tipos de autenticación, el primero se trata de una ID única y como segundo método el sistema le solicita que ingrese una frase al usuario, misma que fue grabada la primera vez que ingreso al sistema.			

8.2.1 Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida.	8.2.1.a	Evalúe la documentación del proveedor y los parámetros de configuración del sistema para verificar que las contraseñas se protegen durante la transmisión y el almacenamiento mediante una criptografía sólida.	La cooperativa utiliza el sistema de encriptación HSM, con este sistema se protege las contraseñas cuando son transmitidas por la red y almacenadas en la base de datos.	SI		
	8.2.1.b	En el caso de una muestra de componentes del sistema, revise los archivos de las contraseñas para verificar que sean ilegibles durante el almacenamiento.		SI		
	8.2.1.c	En el caso de una muestra de los componentes del sistema, revise la transmisión de		SI		

		datos para verificar que las contraseñas sean ilegibles durante la transmisión.				
8.2.2 Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos tokens o genere nuevas claves.	8.2.2	Revise los procedimientos de autenticación para modificar las credenciales de autenticación y observe al personal de seguridad a fin de verificar que, si un usuario solicita el restablecimiento de una credencial de autenticación por teléfono, correo electrónico, Internet u otro método no personal, la identidad del usuario se verificará antes de modificar la credencial de autenticación.	NO APLICA	---	---	

8.2.3 Las contraseñas/frases deben tener lo siguiente: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	8.2.3.a	En el caso de una muestra de los componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de la contraseña del usuario se encuentren configurados de manera que soliciten, al menos, la siguiente solidez o complejidad: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	La complejidad al momento de establecerse o resetearse una contraseña si cumple con los parámetros expuestos en este ítem.	SI		

De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.	8.2.3.b	**8.2.3.b Procedimientos de pruebas adicionales para los proveedores de servicios:** Revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de usuarios no consumidores cumplan, al menos, con la siguiente solidez o complejidad: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos.	Con relación a los proveedores de servicios se solicita aplicar contraseñas a las cuentas de usuarios con la misma complejidad antes mencionada.	SI		

8.2.4 Cambie la contraseña/frase de usuario, al menos, cada 90 días.	8.2.4.a	En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña, al menos, cada 90 días.	La cooperativa tiene establecida como política para el cambio de contraseña de los usuarios de active directory, la cual se realiza en cada noventa días. Con respecto a los proveedores, no se especifica en la documentación de las políticas que las contraseñas de usuarios no consumidores se cambien periódicamente.	SI		Se recomienda considerar dentro de las políticas que todo tipo de usuario, sin excepción alguna, debe cambiar la contraseña de usuario.
	8.2.4.b	**Procedimientos de pruebas adicionales para los proveedores de servicios**: Revise los procesos internos y la documentación del cliente/usuario y verifique		NO	NO	

		lo siguiente: • Las contraseñas de usuarios no consumidores se deben cambiar periódicamente. • Se debe orientar a los usuarios no consumidores sobre cuándo y en qué situaciones deben cambiar las contraseñas.				
8.2.5 No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas.	8.2.5.a	En el caso de una muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las	Las medidas tomadas con respecto a la configuración de los componentes del sistema de la cooperativa, tienen establecida como política que el sistema	SI		Se recomienda especificar en la documentación de las

		contraseñas se encuentren configurados para que soliciten que las nuevas contraseñas no sean iguales a las últimas cuatro contraseñas utilizadas.	no acepte contraseñas que ya han sido utilizadas anteriormente. En relación a los proveedores, no se especifica en la documentación de las políticas que las contraseñas no puedan ser iguales a las cuatro últimas utilizadas con anterioridad.			políticas de acceso a los sistemas que los proveed
	8.2.5.b	**8.2.5.b Procedimientos de pruebas adicionales para los proveedores de servicios:** Revise los procesos internos y la documentación del cliente/usuario para verificar que las nuevas contraseñas de usuarios no consumidores no puedan ser iguales a las últimas cuatro contraseñas utilizadas		NO	NO	ores no podrán hacer uso de las cuatro últimas contrase ñas en caso de el sistema solicitarl

		anteriormente.				es cambio de contraseña para acceder al sistema.
8.2.6 Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso.	8.2.6	Revise los procedimientos de contraseña y observe al personal de seguridad para verificar que las primeras contraseñas para nuevos usuarios, y las contraseñas restablecidas para usuarios existentes, se configuren en un valor único para cada usuario y	La cooperativa en su política de “Seguridad y Control de los Recursos Tecnológicos” establece que las primeras contraseñas asignadas a nuevos usuarios tengan un valor único, así mismo estas se deben ser cambiadas después de	SI		

		se cambien después del primer uso.	usarlas por primera vez. Esto también se aplica para las contraseñas que se han pedido se restablezcan.			
8.3 Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores.		---	---	---	---	
8.3.1 Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE	8.3.a	Revise las configuraciones de la red y/o sistema, según sea el caso, para verificar que la autenticación de múltiples	Para el acceso remoto existe un solo método de autenticación, un computador fuera de la red puede realizar el	NO	NO	Se recomienda establecer dos

para el personal con acceso administrativo.		factores se requiere para todo el acceso administrativo que no es de consola en el CDE.	acceso solo ingresando la contraseña, esto podría exponer los datos del titular de la tarjeta debido a que es más fácil el ingreso con un método que con dos métodos e autenticación.			métodos de autentificación con el propósito de exponer los datos del propietario de la tarjeta.
	8.3.b	Observe un grupo de empleados (por ejemplo, usuarios y administradores) que se conectan de manera remota al CDE y verifique que se usen, al menos, dos de los tres métodos de autenticación.		NO	NO	
8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios, que incluye lo siguiente: •	8.4.a	Revise los procedimientos y entreviste al personal para verificar que los procedimientos y las políticas de autenticación se distribuyen a todos los usuarios.	La cooperativa cuenta con una política de autenticación y claves que indica procedimientos para autenticar todos los usuarios en base a sus	NO	NO	Se recomienda una actualizar la política incluyen

Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para no seleccionar contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.	8.4.b	Revise los procedimientos y las políticas de autenticación que se le entregan a los usuarios y verifique que incluyan lo siguiente: • Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para los usuarios para que no seleccionen contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas	lineamientos específicos. Pero la institución financiera no reparte la política de autenticación a los usuarios.	----	----	do los lineamientos de cambio de contraseña, además de capacitar al personal para que tengan conocimientos de la política y que se les

	8.4.c	Entreviste a un grupo de usuarios y verifique que conozcan los procedimientos y las políticas de autenticación.		----	----	entregue la misma.
8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: • Las ID de usuario genérico se deben desactivar o eliminar. • No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás	8.5.a	En el caso de una muestra de los componentes del sistema, revise las listas de ID de usuarios y verifique lo siguiente: • Las ID de usuario genéricas se deben desactivar o eliminar. • No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas.	Según los datos otorgados por el administrador del sistema todos los usuarios tienen su propia ID. Pero al momento de verificar el acceso al servidor de los usuarios encargados, estos tienen ID y contraseñas compartida para acceder al mismo, en el caso de suceder algún imprevisto o problema	NO	NO	

funciones críticas • Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.		• Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.	por lo tanto no se sabría sobre quién debe caer la responsabilidad.			
	8.5.b	Revise las políticas y los procedimientos de autenticación y verifique que las contraseñas y las ID de grupo y compartidas u otros métodos de autenticación estén explícitamente prohibidos.		NO	NO	
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o	8.6.a	Revise las políticas y los procedimientos de autenticación para verificar que los procedimientos que usan	La cooperativa para identificar usuarios autorizados utiliza tarjetas inteligentes, por el contrario no usa	SI		

lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: • Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. • Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.		mecanismos de autenticación, como tokens de seguridad físicos, tarjetas inteligentes y certificados, estén definidos e incluyan lo siguiente: • Los mecanismos de autenticación se asignan a una sola cuenta y no se comparten entre varias. • Los controles físicos y lógicos se definen para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.	tokens, ni certificados, es decir solo utiliza un mecanismo de autentificación el cual se asigna a una sola cuenta, por tanto la cuenta autenticada correctamente usa los mecanismos de autenticación asignados a ella para acceder.			

	8.6.b	Entreviste al personal de seguridad y verifique que se asignen mecanismos de autenticación a una sola cuenta y que no se compartan entre varias.		SI		
	8.6.c	Examine los parámetros de configuración del sistema y los controles físicos, según corresponda, para verificar que se implementen controles a fin de garantizar que solo la cuenta deseada usa esos mecanismos para acceder.		SI		
8.7 Se restringen todos los accesos a cualquier base de datos que	8.7.a	Revise los parámetros de configuración de la aplicación y de la base de	Existen dos encargados de acceder a la base de datos solo	NO	NO	Se recomienda que

contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera:		datos, y verifique que todos los usuarios estén autenticados antes de acceder.	pueden acceder a información básica del titular de la tarjeta tal como lo recomienda la norma, pero los dos tienen el mismo usuario y la misma contraseña para acceder, incrementando el riesgo de que se realice algún acto malicioso con los datos del titular de la tarjeta. Además se verificó que lo requerido en el ítem 8.7.b sea realizado solo mediante procedimientos almacenados. Así mismo se verificó que			cada persona encargada de manejar la información de la base de datos tenga su usuario y contraseña y los permisos necesarios según su perfil aprobado.
• Todo acceso, consultas y acciones de usuario en las bases de datos se realizan, únicamente, mediante métodos programáticos.	8.7.b	Revise los parámetros de configuración de la base de datos y de la aplicación para verificar que el acceso de todos los usuarios, las consultas del usuario y las acciones del usuario (por ejemplo, mover, copiar, eliminar) en la base de datos se realicen únicamente mediante métodos programáticos (por		SI		

		ejemplo, a través de procedimientos almacenados).	solo los administradores de la base de datos tienen habilitado el acceso directo y de consulta a la base de datos, esto es realizado por medio del aplicativo IMPERVA, dicho aplicativo se trata de un firewall implementado para la base de datos. Finalmente en base a la creación de roles y perfiles en el firewall de la base de datos se cumple lo requerido por la norma en el ítem			
• Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas en estas.	8.7.c	Evalúe los parámetros de control de acceso de la base de datos y los parámetros de configuración de la aplicación de la base de datos y verifique que el acceso directo del usuario a la base de datos, o las consultas a esta, esté limitado a los administradores de la base de datos.		SI		

• Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos (no las pueden usar los usuarios ni otros procesos que no pertenezcan a la aplicación).	8.7.d	Revise los parámetros de control de acceso de la base de datos, los parámetros de configuración de la aplicación de la base de datos y las ID de aplicaciones relacionadas para verificar que solo las aplicaciones pueden usar las ID de la aplicación (y no los usuarios u otros procesos).	8.7.d	SI		
8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén	8.8	Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos de identificación y	La cooperativa si tiene política de seguridad documentada al igual que procedimientos, los cuales son difundidos para su lectura mediante la intranet.	SI		

documentados, implementados y que sean de conocimiento para todas las partes afectadas.		autenticación cumplen con lo siguiente:				

Tomado de (Council, 2013)

4.11.2 Resultados de la revisión de la norma PCI DSS

Luego de haber realizado el análisis de los requisitos 1, 2, 8 y de la norma PCI DSS en base a las matrices del punto 4.11.1 se obtuvieron los siguientes resultados que a continuación se detallan:

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.

1.1. En este punto se verificó que se haya establecido e implementado normas de configuración para firewalls, así como su cumplimiento, y se determinó que:

- ✓ La cooperativa, en el caso de los routers no tiene implementado normas de configuración debido a que dichos routers son administrados por el proveedor de servicios de internet (ISP).
- ✓ El diagrama de red no evidencia la existencia de una red inalámbrica por lo que no se sabe con exactitud la ubicación de dicha red dentro de la cooperativa.
- ✓ No existe un diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.
- ✓ No se efectúa la revisión de las normas de firewalls debido a que en el instructivo elaborado por la cooperativa no se especificaba contar con dicha documentación relacionada con las revisiones de las reglas.

1.2. Se verificó que se haya desarrollado configuraciones para firewalls que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas, el resultado fue:

- ✓ La cooperativa no asegura ni sincroniza los archivos de configuración de routers debido a que estos son administrados por el proveedor de servicios. De ser necesario la institución financiera solicitaría esta información a su ISP.

1.3. Se verificó que se prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas y de este análisis se obtuvo:

- ✓ No existe implementadas medidas antisuplantación a nivel de firewall para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.

1.4. Se verificó que se haya instalado software de firewall personal en todos los dispositivos móviles o de propiedad de los trabajadores que tengan conexión a Internet cuando están fuera de la red, y se determinó que:

- ✓ La cooperativa no tiene debidamente documentada la información sobre la instalación de software de firewall personal.

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

2.1. Se observó que siempre se cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red, los resultaron fueron:

- ✓ El administrador de red desconoce si existen configuradas contraseñas predeterminadas como las utilizadas por las cadenas comunitarias de SNMP (protocolo simple de administración de red.

2.2. Inspeccionar los parámetros de configuración y verificar que las funciones de seguridad se hayan documentado e implementado en todos los servicios, daemons o protocolos no seguros, de esta verificación se obtuvo:

- ✓ La cooperativa no ha documentado parámetros de configuración y las funciones de seguridad.
- ✓ No se evidencia documentación para la eliminación de todas las funcionalidades innecesarias de las configuraciones de los componentes del sistema.

2.3. Se observó que se cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido, se determinó:

- ✓ No se tiene implementado el uso de un cifrado mediante una criptografía sólida cuando se inicia sesión por parte del administrador en cada sistema.

2.4. Se verificó que se lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS y obtuvo como resultado:

- ✓ Los componentes del sistema como firewall y servidores que manejan información de los tarjetahabientes se encuentran inventariados como la norma PCI DSS lo recomienda.

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema.

8.1. Se verificó que se haya definido e implementado las políticas y procedimientos para garantizar la correcta administración de la identificación de todos usuarios, en los componentes del sistema y de este análisis se obtuvo:

- ✓ Con respecto a los ID de usuarios privilegiados e ID de usuarios generales no existe documentación alguna donde consten los que tipos de privilegios tiene aprobados.
- ✓ No se realiza una revisión de los usuarios activos que tenga acceso remoto.

8.2. Se evaluó que exista una correcta administración de autenticación de todos los usuarios en los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios: algo que el usuario sepa, (contraseña o frase de seguridad), algo que el usuario tenga (tarjeta inteligente) o algo que el usuario sea, (rasgo biométrico), y se obtuvo como resultado:

- ✓ La cooperativa no describe todos los métodos de autenticación dentro de la política.
- ✓ No se especifica dentro de la política que las contraseñas de los proveedores se cambien periódicamente, así como también no se menciona que no puedan ser iguales a las últimas cuatro utilizadas anteriormente

8.3. Se observó que se incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la red por parte del personal y obtuvo como resultado:

- ✓ Cuando se accede remotamente existe un solo método de autentificación, pero la normativa indica que debe de existir dos métodos de autenticación para el acceso remoto.

8.4. Verificar que se documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios incluyendo los lineamientos sobre cómo seleccionar credenciales de autenticación sólida, así también de cómo los usuarios deben proteger las credenciales de autenticación, instrucciones para no seleccionar contraseñas utilizadas anteriormente e instrucciones para cambiar contraseñas y los resultados de esta evolución fueron:

- ✓ La cooperativa no difunde la política de autenticación a los usuarios.

8.5. No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera, los resultaron fueron:

- ✓ Los usuarios que acceden al servidor mantienen el mismo usuario y contraseña de forma general.

8.6. Se verificó si la cooperativa usa otros mecanismos de autenticación, en el caso de usarlos que estos se asignen a una sola cuenta y no compartirlos entre varias, además verificar que se implementen controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder y se determinó que:

- ✓ La cooperativa no se usa otros mecanismos de autentificación como tokens, tarjetas inteligentes y certificados.

Los resultados que se obtuvieron con respecto a la entrevista realizada al administrador de redes en base a las matrices de los requerimientos 1, 2, 8 de la norma PCI DSS a la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., permite evidenciar que el mayor nivel de cumplimiento con el 80% lo tiene en el requerimiento 1. “Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas”. Seguido del requerimiento 2 “No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos

por los proveedores” con un 79.17% y finalmente con un 71.43% el requerimiento 8 “Identificar y autenticar el acceso a los componentes del sistema”, con relación a lo anteriormente expuesto podríamos afirmar que el requerimiento 8 podría presentar mayor riesgo para la organización, puesto que, a nivel de infraestructura de redes y afines, estos 3 requerimientos deben cumplirse en un 100%.

4.11.3 PCI DSS aplicado al rediseño de la red

Las matrices realizadas del punto 4.11.1, reflejan dentro de campo “Recomendación” la respectiva solución a los subrequisitos de la norma PCI DSS que actualmente no se cumplen, cada solución con respecto a mejorar la infraestructura de redes es tomada en cuenta en este rediseño. Es así que se mejoró el diseño de la red actual en el punto 4.9 con el objetivo de identificar todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.

El presente rediseño con respecto al firewall considera que se debe realizarse las configuraciones e instructivos abajo mencionados en correspondencia al requisito 1 de la norma PCI DSS:

- ✓ Realizar el diagrama de flujo de datos de titulares de tarjetas entre los sistemas.
- ✓ Revisar las reglas de firewalls al menos, cada seis meses.
- ✓ Implementar medidas antisuplantación en el firewall para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.
- ✓ Implementar la configuración de firewall, la cual realice una inspección completa (filtrado de paquetes dinámico).

De la misma manera este proyecto en relación al requisito 2 de la norma PCI DSS considera que se debe realizarse las siguientes configuraciones e instructivos:

- ✓ Eliminar o deshabilitar las cuentas predeterminadas innecesarias, por ejemplo: las contraseñas predeterminadas utilizadas por las cadenas comunitarias de SNMP (protocolo simple de administración de red).
- ✓ Documentar las funciones de seguridad de los servicios implementados como: daemons o protocolos no seguros
- ✓ De acuerdo a los parámetros de seguridad las cuales indican que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos, etc.). Documentar las funciones habilitadas que admiten la configuración segura.
- ✓ Documentar y hacer uso de un cifrado mediante una criptografía sólida cuando se inicie sesión por parte del administrador en cada sistema.

En último lugar y no por ello menos importante, este rediseño haciendo referencia al requisito 8 de la norma PCI DSS considera que se debe realizarse las configuraciones e instructivos a continuación descritas.

- ✓ Elaborar la respectiva documentación sobre los ID de usuarios privilegiados e ID de usuarios generales.
- ✓ Se recomienda realizar la revisión de la lista de los usuarios activos que tengan acceso remoto.
- ✓ Actualizar las políticas para que, al bloquear la cuenta de un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.
- ✓ Especificar dentro de la política que las contraseñas de usuarios no consumidores se cambien periódicamente.
- ✓ Especificar dentro de la política que las contraseñas de usuarios no consumidores, que no puedan ser iguales a las últimas cuatro utilizadas anteriormente.
- ✓ Establecer dos métodos de autentificación en el caso de que se quiera acceder al sistema.

- ✓ Actualizar la política incluyendo los lineamientos de cambio de contraseña, además de capacitar al personal para que tengan conocimientos de la política y que se les entregue la misma.
- ✓ Cada persona encargada de manejar la información de la base de datos debe ingresar a la base de datos con su usuario y contraseña, por ende, dicha persona debe tener los permisos necesarios según su perfil previamente aprobado.

4.12 Norma ISO/IEC 27000

En el mundo actual, la mayoría de organizaciones comerciales y gubernamentales tienen sus sistemas de información conectados por red, la cooperativa 29 de octubre se alinea a la ISO27001 que trata de la seguridad de la información pero hemos identificado que también podemos obtener más referencias de la norma ISO/IEC 27033, está dos normas serán las referencias para nuestra evolución, la norma ISO/IEC 27033 se compone de las siguientes partes, bajo el título general de la tecnología de la información - Técnicas de seguridad - Seguridad de red :

- ✓ Parte 1: Generalidades y conceptos
- ✓ Parte 2: Directrices para el diseño e implementación de seguridad de la red
- ✓ Parte 3: Los escenarios de referencia de una red - Amenazas, técnicas de diseño y problemas de control
- ✓ Parte 4: Protección de las comunicaciones entre redes que utilizan pasarelas de seguridad
- ✓ Parte 5: Protección de las comunicaciones a través de redes que utilizan redes privadas virtuales (VPN)
- ✓ Parte 6: Asegurar el acceso a la red IP inalámbrica. (ISO, 2015)

Los siguientes documentos, en su totalidad o en parte, se toman como referencia normativa en este documento (ISO/IEC 27033) y son indispensables para su aplicación.

- **ISO / IEC 7498** (todas las partes), Tecnología de la información - Interconexión de sistemas abiertos - Modelo de referencia básico: Denominación y direccionamiento
- **ISO / IEC 27001**, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos
- **ISO / IEC 27002**, Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información
- **ISO / IEC 27005**, Tecnología de la información - Técnicas de seguridad - Información de gestión de riesgos de seguridad (ISO, 2015)

Además, las conexiones de red (véase figura 21) pueden identificarse de diferentes formas:

- Dentro de la organización,
- Entre las diferentes organizaciones,
- Entre la organización y el público en general.

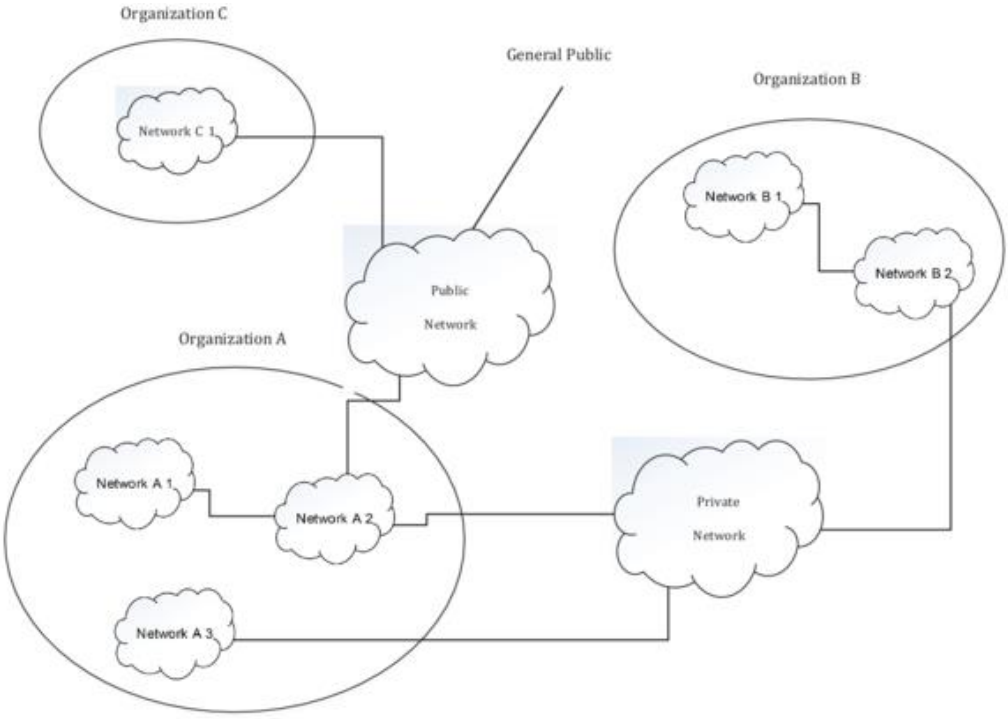


Figura 21. Tipos generales de conexión de red

Tomado de: Cisco, s.f.

En este contexto, las industrias de telecomunicaciones y tecnología de la información están buscando soluciones de seguridad integrales rentables, encaminadas a proteger las redes contra ataques maliciosos y acciones incorrectas, y el cumplimiento de los requisitos de negocio para la confidencialidad, integridad y disponibilidad de la información y los servicios. (ISO, 2015)

El propósito de esta Norma es proveer una pauta precisa sobre los aspectos de seguridad de la administración, operación y uso de redes de sistemas de información, y sus interconexiones. Otro punto es sobre las personas dentro de una organización que son responsables de la seguridad de la información en general, y la seguridad de la red, en particular, deben ser capaces de adaptar el material en esta norma internacional para satisfacer sus requisitos específicos. Sus principales objetivos son los siguientes.

- ✓ **ISO / IEC 27033-1**, para definir y describir los conceptos asociados con, y proporcionar orientación sobre la gestión de seguridad de la red. Esto incluye la provisión de una visión general de seguridad de la red y las definiciones relacionadas, y orientación sobre cómo identificar y analizar los riesgos de seguridad de red y luego definir los requisitos de seguridad de red. También introduce la forma de lograr arquitecturas de seguridad técnicas de buena calidad, y los aspectos de riesgo, diseño y control de red asociado con escenarios típicos y áreas de la red "tecnología". (ISO, 2015)
- ✓ **ISO / IEC 27033-2** , para definir cómo las organizaciones deben lograr la calidad de la red de seguridad técnicas arquitecturas, diseños e implementaciones que garanticen la adecuada seguridad de la red a sus entornos de negocio, utilizando un enfoque coherente en la planificación, diseño e implementación de seguridad de la red, como se relevante, ayudado por el uso de modelos / marcos (en este contexto, un modelo / marco se utiliza para describir una representación o descripción que muestra la estructura y el alto nivel de funcionamiento de un tipo de seguridad arquitectura / diseño técnico), y es relevante para todos

personal que esté involucrado en la planificación, diseño e implementación de los aspectos arquitectónicos de seguridad de la red (por ejemplo, arquitectos y diseñadores de red, los administradores de red, y los agentes de seguridad de red). (ISO, 2015)

- ✓ **ISO / IEC 27033-3**, para definir los riesgos específicos, técnicas de diseño y problemas de control asociados con escenarios de red comunes. Es relevante para todo el personal que participe en la planificación, diseño e implementación de los aspectos arquitectónicos de seguridad de la red (por ejemplo, arquitectos y diseñadores de red, los administradores de red, y los agentes de seguridad de red). (ISO, 2015)
- ✓ **ISO / IEC 27033-4**, para definir los riesgos específicos, técnicas de diseño y cuestiones de control para asegurar el flujo de información entre las redes que utilizan pasarelas de seguridad. Es relevante para todo el personal que participe en la planificación detallada, diseño e implementación de pasarelas de seguridad (por ejemplo, arquitectos y diseñadores de red, los administradores de red, y los agentes de seguridad de red). (ISO, 2015)
- ✓ **ISO / IEC 27033-5**, para definir los riesgos específicos, técnicas de diseño y cuestiones de control para proteger las conexiones que se establecen usando redes privadas virtuales (VPN). Es relevante para todo el personal que participe en la planificación detallada, diseño e implementación de seguridad de VPN (por ejemplo, arquitectos y diseñadores de red, los administradores de red, y los agentes de seguridad de red). (ISO, 2015)
- ✓ **ISO / IEC 27033-6**, para definir los riesgos específicos, técnicas de diseño y problemas de control de IP para asegurar las redes inalámbricas. Es relevante para todo el personal que participe en la planificación detallada, diseño e implementación de seguridad para redes inalámbricas (por ejemplo, arquitectos y diseñadores de red, los administradores de red, y los agentes de seguridad de red). (ISO, 2015)

Se hace hincapié en que esta Norma Internacional proporciona orientación adicional detallada sobre la aplicación de los controles de seguridad de red que se describen en un nivel estandarizado básico en la norma ISO / IEC 27002.

A menos que se indique lo contrario, a lo largo de esta parte de la norma ISO / IEC 27033 la guía se hace referencia es aplicable a las redes actuales y / o previstas, pero sólo se hará referencia como "redes" o "la red".

Se ha tomado como referencia los siguientes aspectos de la norma ISO27001 y de la norma ISO27033 y que interactúan con la norma PCI/DSS:

A continuación, se muestra en la tabla 35 la guía que hace referencia a la norma ISO.

Tabla 35.

Guía que hace referencia a la norma ISO.

Política de seguridad		
Objetivo de control	**Descripción**	**Justificación**
Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes	Documento de gestión de seguridad de la información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes
	Revisión de la política	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
Planeación y aceptación del sistema		
Minimizar el riesgo de fallas en los sistemas.	Gestión de capacidad	Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.

	Aceptación del sistema	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
Protección contra software malicioso y código móvil		
Proteger la integridad del software y la información.	Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
	Controles contra códigos móviles	Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código

		móvil no autorizado
Respaldo (back-up)		
Mantener la integridad y disponibilidad de los servicios de procesamiento o de información y comunicaciones.	Back-up o respaldo de la información	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
Gestión de seguridad de redes		
Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.	Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
	Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e

		incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos encasa o sean abastecidos externamente.
Gestión de medios		
Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.	Gestión de los medios removibles	Deben existir procedimientos para la gestión de medios removibles.
	Eliminación de medios	Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
	Procedimiento de manejo de la información	Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
	Seguridad de documentación del sistema	Se debe proteger la documentación de un acceso no autorizado.
Monitoreo		

Detectar actividades de procesamiento o de información no autorizadas.	Registro de auditoria	Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
	Uso del sistema de monitoreo	Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
	Protección de la información del registro	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
	Registros del administrador y operador	Se deben registrar las actividades del administrador y operador del sistema.
	Registro de fallas	Las fallas se deben registrar, analizar y se

		debe tomar la acción apropiada.
	Sincronización de relojes	Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
Control de acceso a redes		
Evitar el acceso no autorizado a los servicios en red.	Política sobre el uso de servicios en red	Los usuarios solo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar
	Autenticación del usuario para conexiones externas	Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
	Identificación del equipo de red	Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.

	Protección del puerto de diagnóstico remoto	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
	Segregación en redes	Los servicios de información, usuarios y sistemas de información se deben segregar en las redes
	Control de conexión de redes	Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales
	Control de routing de redes	Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones

		comerciales.
Computación móvil y tele-trabajo		
Asegurar la seguridad de la información cuando se utilice medios computación móvil y teletrabajo.	Computación móvil y comunicaciones	Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
	Tele-trabajo	Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo
Procesamiento correcto en las aplicaciones		
Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.	Validación de data de insumo	El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
	Control de procesamiento interno	Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la

		información a través de errores de procesamiento o actos deliberados.
	Integridad del mensaje	Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
	Validación de data de output	Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
Controles criptográficos		
Proteger la confidencialidad ad, autenticidad o integridad de la información a través de medios criptográficos.	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	Gestión clave	Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía

		en la organización.
Seguridad de los archivos del sistema		
Garantizar la seguridad de los archivos del sistema.	Control de software operacional	Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
	Protección de la data de prueba del sistema	Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
	Control de acceso al código fuente del programa	Se debe restringir el acceso al código fuente del programa.
Seguridad en los procesos de desarrollo y soporte		
Mantener la seguridad del software e información del sistema de aplicación.	Procedimientos de control de cambios	La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las

		operaciones o seguridad organizacional.
	Restricciones sobre los cambios en los paquetes de software	No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
	Filtración de información	Se deben evitar las oportunidades de filtraciones en la información.
	Desarrollo de outsourced software	El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.
Gestión de vulnerabilidad técnica		
Reducir los riesgos resultantes de la explotación de vulnerabilidad es técnicas publicadas.	Control de vulnerabilidades técnicas	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas

		vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

Tomado de: (Tola, 2015)

5. ANÁLISIS DE COSTOS

5.1 Análisis de costos de la red activa

El análisis de costos con relación a la parte activa de la red Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., incluye los equipos de conectividad, como switches, teléfonos IP, centrales telefónicas IP, etc. Se realizará el análisis de los costos de los fabricantes Cisco, Juniper para los equipos de conectividad, en tanto que para teléfonos IP se valorará Avaya y Grandstream.

Tanto Cisco, Juniper y Grandstream son distribuidores de equipos de conectividad, además prestan un buen rendimiento y desempeño en sus equipos; en nuestro mercado Juniper no tiene la aceptación que tiene Cisco, pero hemos identificado que tiene buena calidad de equipos, también se ha considerado que es fabricante americano y que ha venido tomando fuerza dentro del país.

Basado en lo antes mencionado y en los requerimientos que ya se establecieron en el capítulo 4, realizaremos el análisis del costo de los equipos para la capa de acceso, distribución, core y telefonía IP.

5.1.1 Switch de Acceso

Los switches de acceso cumplen con los requerimientos identificados y con las características mínimas para buen desempeño del punto 4.6.3.1, para esta capa utilizaremos en cisco el SW-2960-S CISCO y el Juniper EX2200 24P/24T; en la siguiente tabla 34 se indican los equipos de los cuales se puede hacer uso.

Tabla 36.

Costo de switch de Acceso.

Fabricante	Modelo	Precio	IVA 14%	Total
Cisco	SW-2960-S	$ 1718.7	$ 240.62	$ 1959.32
Juniper	1160	$ 1160	$ 162.40	$ 1322.40

Tabla 37.

Costo total de switch de Acceso.

Fabricante	Cantidad	Valor Unitario	Valor Total
Cisco	25	$ 1718.7	$ 42967.5
Juniper	25	$ 1160	$ 29000

5.1.2 Switch de Distribución

Para los switches de distribución se seleccionaron los siguientes modelos WS-C3650-24TS de Cisco y el modelo EX3300 de Juniper ya que cumplen con las especificaciones de los requerimientos indicados en el punto 4.6.3.2, en la siguiente tabla 36 se muestra los costos.

Tabla 38.

Costo de switch de distribución.

Fabricante	Modelo	Puertos	Precio	IVA 14%	Total
Cisco	WS-C3650-24TS	24	$ 3540.56	$ 495.68	$ 4036.24
Juniper	EX3300 24P/24T-DC	24	$ 2066.25	$ 289.28	$ 2355.53

Tabla 39.

Costo total de switch de distribución.

Fabricante	Cantidad	Valor Unitario	Valor Total
Cisco	2	$ 3540.56	$ 7081.12
Juniper	2	$ 2066.25	$ 4132.5

5.1.3 Switch de core

La elección del Switch de Core es importante, debido a que es el responsable de conmutar lo más rápido posible y proveer de redundancia a la red.

En base a los requerimientos seleccionamos los switches que cumplen con las recomendaciones del punto 4.6.3.3 y estos son el Cisco Catalyst 3750X-12S-S y el Juniper QFX3500. En la tabla 38 se indica los costos de los equipos Cisco y Juniper.

Tabla 40.

Costo de switch de core.

Fabricante	Modelo	Puertos	Precio	IVA 14%	Total
Cisco	WS-3750X-24S-S	24	$ 10371.8	$ 1452.06	$ 11823.89
Juniper	QFX3500	24	$ 15992.8	$ 2238.99	$ 18231.74

Tabla 41.

Costo total de switch de core.

Fabricante	Cantidad	Valor Unitario	Valor Total
Cisco	2	$ 10371.83	$ 20743.66
Juniper	2	$ 15992.75	$ 31985.5

5.1.4 Telefonía IP

5.1.4.1 Teléfonos IP

Para la red de voz utilizamos la alternativa de utilizar teléfonos IP Cisco, Avaya o Grandstream, lo que se debe considerar en el coste de las mismas en caso de su adquisición. En la tabla 40 se detallan los costos de cada una de las marcas antes mencionadas.

Tabla 42.

Costo teléfonos IP.

Fabricante	Modelo	Precio	IVA 14%	Total
Cisco	SPA303-G1	160	$ 22.40	$ 182.40
Avaya	1210	104	$ 14.56	$ 118.56
Grandstream	GXP 1610	54	$ 7.56	$ 61.56

Tabla 43.

Costo total teléfonos IP.

Fabricante	Cantidad	Valor Unitario	Valor Total
Cisco	500	$ 160	$ 80000
Avaya	500	$ 104	$ 52000
Grandstream	500	$ 54	$ 27000

5.1.4.2 Servidor de telefonía IP

En cuento al costo de los servidores de telefonía IP se consideró cotizar las marcas Grandstream y SERVVOX, a continuación se detallan los costos de los mismos.

Tabla 44.

Costo servidor de telefonía IP.

Fabricante	Modelo	Precio	IVA 14%	Total
Grandstream	Ucm6104	$ 3400	$ 476.00	$ 3876.00
SERVVOX	SR110	$ 3070	$ 429.80	$ 3499.80

Tabla 45.

Costo total de los servidores de telefonía IP.

Fabricante	Cantidad	Valor Unitario	Valor Total
Grandstream	25	$ 3400	$ 85000
SERVVOX	25	$ 3070	$ 76750

5.1.5 Costo Norma PCI-DSS

En este proyecto el cumplimiento de los requisitos de la norma PCI DSS no generan costos adicionales, a más de los costos de equipos que se considera que se deben adquirir para establecer un modelo de red jerárquico, como se menciona en el punto 5.1.6, ya que los requisitos 1, 2 y 8 de la norma están orientados a auditar la infraestructura de redes y afines.

5.1.6 Costo total

Tomando la información de los anteriores numerales del capítulo 5, se realiza un consolidado para obtener el valor que tendría implementar la red en la institución financiera.

En la siguiente tabla se muestra el resumen por cada fabricante:

Tabla 46.

Costo total por fabricante.

Detalle	Cisco	Juniper	Avaya teléfonos	Grandstream teléfonos/central IP	SERVVOX central IP
Capa de acceso	$ 42967.50	$ 29000.00	N/A	N/A	N/A
Capa de distribución	$ 7081.12	$ 4132.50	N/A	N/A	N/A
Capa de Core	$ 20743.66	$ 31985.50	N/A	N/A	N/A
Central telefónica	N/A	N/A	N/A	$ 85000.00	$ 76750.00
Telefonía IP	$ 80000.00	N/A	$ 52000.00	$ 27000.00	N/A
Subtotal	$ 150792.28	$ 65118.00	$ 52000.00	$ 112000.00	$ 76750.00
IVA	$ 21110.92	$ 9116.52	$ 7280.00	$ 15680.00	$ 10745.00
Total	$ 171903.20	$ 74234.52	$ 59280.00	$ 127680.00	$ 87495.00

5.1.7 Parámetros para la selección de una alternativa

Para poder obtener la mejor alternativa de solución al momento de implementar una red, se debe sustentar en algunos parámetros que establezcan la razón de su elección. Los parámetros deben tener un enfoque amplio y no centrarse solamente en el aspecto económico, también en factores técnicos como garantía, soporte, personal capacitado, etc.

Para el tema de la garantía y soporte técnico las empresas manejan los mismos acuerdos para la garantía tanto en software como en hardware cubre

hasta un plazo de 90 días y el reemplazo de los equipos siempre y cuando se haya verificado que no ha sido por mala utilización.

Cisco propone extender la garantía mediante un contrato de soporte técnico el cual indica que personal especializado estará a cargo de los equipos a través de recursos que ayuden al acceso de los equipos de cisco.

El soporte técnico de cisco tiene durabilidad de un año en el instante de la entrega, cada equipo cuenta con su propia garantía.

La duración de la garantía en hardware se mantiene si el usuario final continúa siendo el propietario del equipo.
Para Juniper se asemeja a la garantía y soporte que ofrece cisco, garantía de 90 días desde la entrega del equipo y se activa el soporte técnico por un año. Así mismo cada equipo cuenta con su garantía propia, también el usuario final debe ser el propietario del equipo.
Para la telefonía IP los fabricantes CISCO, AVAYA, GRANDSTREAM, SERVVOX, mantienen la garantía en sus equipos y soporte técnico, además el asesoramiento e implementación de las centrales y teléfonos IP.

5.1.8 Selección de la mejor alternativa

Con respecto a lo mencionado anteriormente se recomienda optar por una solución Cisco en caso de querer implementar la red jerárquica expuesta en el punto 4.9 (Nuevo diseño de la red)

En caso de telefonía IP se opta por Grandstream para los teléfonos IP y SRVVOX para el servidor, ya que la Cooperativa de ahorro y crédito” 29 de octubre”, ya tiene en nueve de las 34 agencias instalado centrales telefónicas IP de marca SRVVOX, como se puede evidenciar la instalación es para las agencias no para la oficina matriz, esto debido a que ya se encuentra funcionando con telefonía IP.

La selección de esta recomendación se da por el siguiente análisis.

Aspecto económico. - En las cotizaciones de los equipos que se requiere para la red, se observa que el costo total de la red con equipos CISCO es similar a las demás marcas, pero Cisco tiene confiabilidad como empresa en el mercado de las telecomunicaciones, para servidor de telefonía IP el costo menor es SRVVOX, mientras que la mejor opción para la adquisición de teléfonos IP es Grandstream.

Aspecto Técnico. - Cisco cumple con las características técnicas mínimas para las necesidades de la institución financiera, para la telefonía IP SRVVOX y Grandstream cumple con las características técnicas solicitadas.

Garantía y Soporte Técnico. - Cisco en este aspecto cuenta con varios Partner dentro del mercado y ofrece mayor aptitud en este factor.
Para telefonía IP SRVVOX y Grandstream presenta las mismas condiciones respecto a estos dos puntos.
Administración de la Red. - La administración de la red es más sencilla en Cisco, esto debido a que el sistema operativo IOS de CISCO esta difundido en el mundo de las redes. En telefonía IP no se complica para la administración de la red porque es compatible con lo que actualmente se tiene instalado.

Personal Capacitado. - Cisco tiene mucha fuerza en el país, y por ende profesional en certificaciones Cisco como CCNA y CCNP, por lo que conseguir personal para la administración de la red no resulta complejo y no es muy costoso conseguir las certificaciones. Respecto a este punto en la telefonía IP no presenta mayor inconveniente debido a que está basada en Linux y es factible adquirir conocimiento.

En conclusión, este proyecto de titulación sugiere la utilización de equipos cisco en base al modelo de capas propuesto en el capítulo 4.

- En la capa de acceso se debe utilizar switches de marca Cisco, modelo SW-2960-S.
- En la capa de distribución se debe utilizar switches de marca Cisco, modelo WS-C3650-24TS.

- En la capa de Core se debe utilizar switches de marca Cisco, modelo WS-3750X-24S-S.

Para la telefonía IP se debe utilizar equipos de la marca Grandstream:

- Teléfonos IP de marca Grandstream modelo GXP 1610.
- Centrales telefónicas SERVVOX modelo SR110.

La selección de equipos a utilizar tanto para el modelo jerárquico de capas y telefonía IP se la realizó en base a criterios analizados anteriormente como: personal capacitado, aspecto económico, soporte técnico, facilidad de la administración. Además, los equipos que se sugiere utilizar ayudarán a que la red de la institución financiera sea en su totalidad convergente.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

En el capítulo uno, la ayuda de las definiciones, conceptos y estándares, permiten tener una idea mucho más clara de lo que se necesita para el cumplimento del rediseño de la red multiservicios considerando el estándar PCI-DSS y como referencia la norma ISO/EC 27000, dentro de la Cooperativa 29 de Octubre.

El análisis de la situación actual de la red la Cooperativa 29 de Octubre brindó una amplia perspectiva para saber cómo se encuentra la institución financiera y cuáles son sus primordiales ausencias, así como sus nuevos requerimientos y servicios.

También en el análisis de la situación actual de la red nos ayudó a identificar como está estructurada la red en su parte lógica y en su parte física, identificando que el firewall de la entidad financiera tiene un rol importante para la administración de la red.

Otro parámetro que se desprende del análisis de la estructura de la red es la identificación de los elementos red activa.

Para el rediseño de la red integrada de voz y datos de la cooperativa 29 de octubre, se eligió el modelo de red jerárquico fundamentado en tres capas: acceso, distribución y núcleo; este modelo brinda a la red gran elasticidad, escalabilidad y seguridad a la red, ya que cada capa tiene definida sus propias funciones.

En cuanto al cableado estructurado ya diseñado por la institución financiera, proporciona un adecuado esquema y capacidad de adaptación para un crecimiento de la red y así poder implementar aplicaciones o servicios en el futuro, todo esto debido a que cumple con el margen del 30% de crecimiento y la topología de la red es estrella extendida debido a las características propias de la institución, además de ser la topología recomendada por los estándares de cableado estructurado, agrega ventajas como flexibilidad, movilidad y facilidad en la administración de los puntos de red.

En el rediseño de la red multiservicios se propone redundancia a nivel de la capa de distribución y capa de core, esta redundancia nos ayudara a evitar la caída total de la red de datos de la institución financiera.

La Cooperativa de ahorro y crédito “29 de octubre” cuenta con una integración de comunicación de voz en la red de datos, para este propósito utiliza la tecnología de transmisión de VoIP, esta tecnología tiene beneficios económicos y técnicos al utilizarse en su red interna al poderla administrar directamente gracias a su interfaz web, esta tecnología se encuentra implantada en la oficina matriz y algunas de las agencias, por lo que se propone seguir con la implementación en las demás agencias.

La institución financiera cuenta con equipos que están funcionando al momento, los cuales tienen las características necesarias para el rediseño de la red y estos están en condición de ser utilizados, se han evaluado posibles soluciones para que sean incrementadas conforme al rediseño planteado. Para ello se analizó las soluciones de los fabricantes CISCO, JUNIPER, para las capas del rediseño y la para la telefonía IP CISCO, AVAYA, GRANDSTREAM.

Para la selección de los equipos que darán conectividad, se han considerado características como seguridad, soporte, flexibilidad, compatibilidad con los equipos que se tiene en la institución y que van a ser de utilidad en el rediseño, mediante estos parámetros se estableció que la medida más practica tanto técnica como económica es CISCO.

En cuanto a la telefonía IP como ya se cuenta con esta tecnología implementada con dos fabricantes y en base a la propuesta económica se evidencia que es factible seguir la implementación de telefonía IP.

Dentro de la simulación de la red se puede apreciar lo importante que resulta establecer QoS, ya que al integrar datos y voz, esta última no puede sufrir retardos ni verse afectada de ninguna manera independientemente de los datos que puedan transmitirse por la red.

El rediseño propuesto resulta porque es necesario mantener una redundancia y tener menos perdidas en los servicios, con el tiempo la red de datos podría verse afectada debido algún daño en los equipos, generando inconvenientes entre los socios quienes son los que desean acceder a los servicios que ofrece la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda.

Parte del rediseño de la red de la institución es producto de poder trabajar con tarjetas de crédito, por lo cual las entidades de tarjeta de crédito exigen seguir los lineamientos del estándar PCI DSS. El estándar PCI DSS da la guía de como resguardar los datos del tarjeta habiente, procesarlos, almacenarlos y trasmitirlos de forma segura.

También es parte de esta propuesta tomar como referencia lo indicado en la norma ISO/EC 27000, la cual proporciona guías sobre la seguridad de la información.

Mediante los estándares PCI DSS y ISO/EC 27000 habrá un mejor control de la información, prestando a los usuarios seguridad, integridad y confiabilidad. Además reconocer de manera eficaz los potenciales incidentes que la red presente. La Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., al momento puede brindar seguridad, integridad, confiabilidad y evidenciar algunos eventos pero estos parámetros deben ser mejorados debido a la aspiración de trabajar con tarjetas de crédito, de igual forma el resultado indica que es necesario hacer una inversión y agregar definiciones que indican los estándares para el trabajo con tarjetas crédito.

6.2 Recomendaciones

Se recomienda tener claros los conceptos a manejar en el rediseño, puesto que proporcionarán un mejor desenvolvimiento en la propuesta, también el conocimiento ayudará a tomar decisiones en el desarrollo del proyecto.

La recomendación con respecto al análisis del estado actual y rediseño de la red la institución financiera es que se debe mantener diferenciado las zonas que intervendrán en la propuesta para entregar información real.

Mantener un correcto levantamiento de la información del estado actual de la institución financiera permite tener claro y preciso lo que se requiere para el rediseño, como recomendación se define que la información tomada sea tratada con cuidado, sigilo y de forma directa por quien este ha cargo.

Se recomienda para la utilización de los estándares siempre utilizar los actualizados y aprobados por los diferentes organismos de estandarización. Además que ayudaran a la C Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., con la obtención de la certificación.

En la propuesta, el dimensionamiento del tráfico que soporta la red es considerado con valores promedios actuales para los diferentes servicios, puesto que estos valores se modifican constantemente o dependen de la actividad de la organización, por ejemplo accesos a la web, o descargas de archivos, por lo que se recomienda al momento de la implementación realizar nuevamente el dimensionamiento del tráfico para no tener inconvenientes futuros.

Es recomendable que se realicen mantenimientos preventivos a los equipos activos de la red, la sugerencia es de al menos 2 mantenimientos anuales.

Se recomienda que personal a cargo de la administración y operación de la red de voz y datos, mantenga actualizado la red respecto a parches o actualizaciones que se necesite realizar, pero si el administrador no se encuentra capacitado se recomienda brindar la adecuada preparación y así poder tener controlado el funcionamiento de la red.

Es recomendable que la Institución mantenga actualizada la documentación de los diferentes procesos, manuales, SLA de los proveedores y demás información que cumpla con los estándares especificados en esta propuesta. Además ayudará al nuevo personal que ingrese a trabajar para que tenga una mejor administración de la red de la Institución.

Se recomienda cumplir y hacer cumplir los procesos de los estándares para no tener inconvenientes en la obtención de la certificación a la que la Cooperativa de Ahorro y Crédito “29 de octubre” Ltda., quiere acceder.

Se recomienda elaborar el plan de ejecución para minimizar el impacto en caso de implementación de este proyecto.

REFERENCIAS

Acurio, P. (2015). *Rediseño de una red multiservicios para la empresa elaborados cárnicos s.a.* Recuperado el 11 de noviembre de 2016 de http://dspace.udla.edu.ec/handle/33000/4488

Aguilar, S. (2015). *Análisis, diseño e implementación de un sistema de VOIP para el Hospital Un Canto a la Vida.* Recuperado el 14 de noviembre de 2016 de http://dspace.ups.edu.ec/handle/123456789/11608

Alvarez, F. (2007). *Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud (Registro nro. 8169).* Recuperado el 6 octubre de 2016 de http://bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf

Auditors, I. S. (2007). *Implantación y certificación en el estándar PCI DSS.* Recuperado el 20 de octubre de 2016 de http://www.isecauditors.com/sites/default/files/files/SIC-76_PCI-DSS_Como_cumplir.pdf

Baxter, S. (2005). *Desarrollo de un Servidor de Administración de Políticas para Vlans (VMPS).* Recuperado el 25 de octubre de 2016 de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/1059/1/TESIS%20VLAN.pdf

Coop. 29 de Octubre. (2016). *Misión y Visión*. Recuperado el 17 noviembre de 2016 de Cooperativa 29 de Octubre: https://www.29deoctubre.fin.ec

Council, P. S. (2013). *Requisitos y procedimientos de evaluación de seguridad.* Recuperado el 10 de noviembre de 2016 de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Del valle, E. (2012). *DISEÑO E IMPLEMENTACION DE VLANS.* Recuperado el 12 de octubre de 2016 de http://gye.ecomundo.edu.ec/doc_aula_virtual_ecotec/tareas/2012D/COM355/alum/2012290085_738_2012D_COM355_Dise_o_e_Implementacion_de_VLANs.pdf

ISO. (2015). *ISO/IEC 27033-1:2015.* Recuperado el 29 de noviembre de 2016 de https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-1:ed-2:v1:en

Logisman. (2014). *Familia ISO 27000: Seguridad de la Información.* Recuperado el 8 octubre de 2016 de http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

López, V. (2011). *Análisis de la paquetización de voz sobre IP empleando el protocolo de inicio de sesiones SIP con back to back User Agent (B2BUA) en una aplicación sobre redes WI-FI.* Recuperado el 5 de noviembre de 2016 de http://repositorio.espe.edu.ec/handle/21000/4845

Morales, N. (2016). *Diseño de la red multiservicios para el Proyecto Quijos de la Celec E.P.* Recuperado el 11 de octubre de 2016 de http://bibdigital.epn.edu.ec/handle/15000/15186

Normas ISO. (2016). *ISO 27001 Gestión de la Seguridad de la Información.* Recuperado el 16 de noviembre de 2016 de http://www.normas-iso.com/iso-27001

Pardo, C. (2013). *Capas del Modelo TCP/IP.* Recuperado el 20 noviembre de 2016 de http://modelozzy.blogspot.com/

Ramón, J. (2014). *Diseño y Simulación de una Red Integrada de voz y datos para la Unidad Educativa Temporal "Jaime Roldós Aguilera".* Recuperado el 20 de noviembre de 2016 de http://bibdigital.epn.edu.ec/handle/15000/8802

Tipán, M. (2005). *Implementación de VLANS en la red de Telconet para una interconexión segura entre las agencias y la matriz de una institución*

bancaria. Recuperado el 14 de noviembre de 2016 de http://bibdigital.epn.edu.ec/handle/15000/166

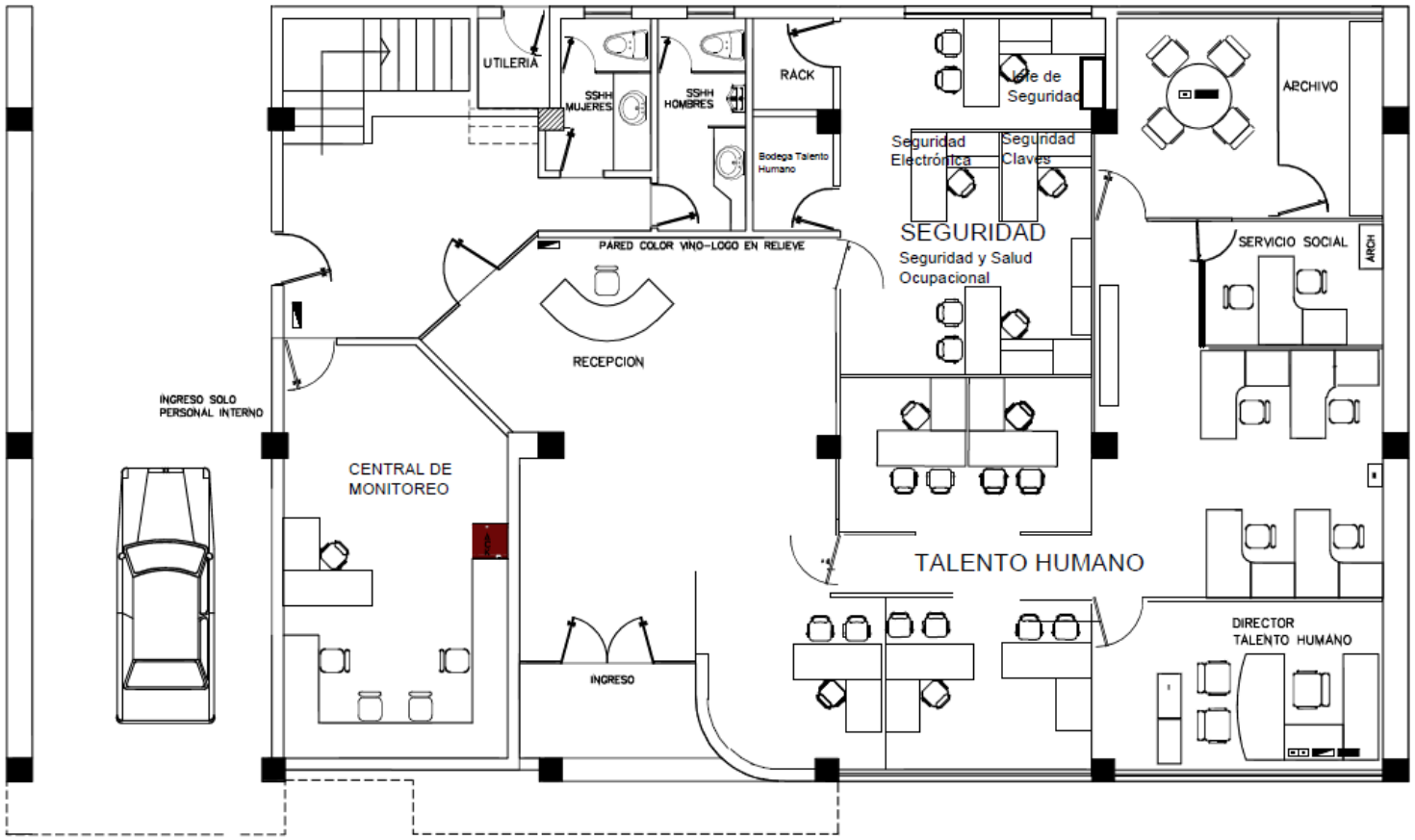
Tola, D. (2015). *Implementacion de un Sistema de Gestion de Seguridad de la Informacion para una empresa de consultoria y auditoria, aplicando la norma ISO/IEC 27001.* Recuperado el 15 de noviembre de 2016 de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/31114

Toro, C. (2009). *Rediseño de la red de comunicaciones de CIESPAL para que soporte aplicaciones de datos, voz y videoconferencia.* Recuperado el 21 de noviembre de 2016 de http://bibdigital.epn.edu.ec/handle/15000/1145

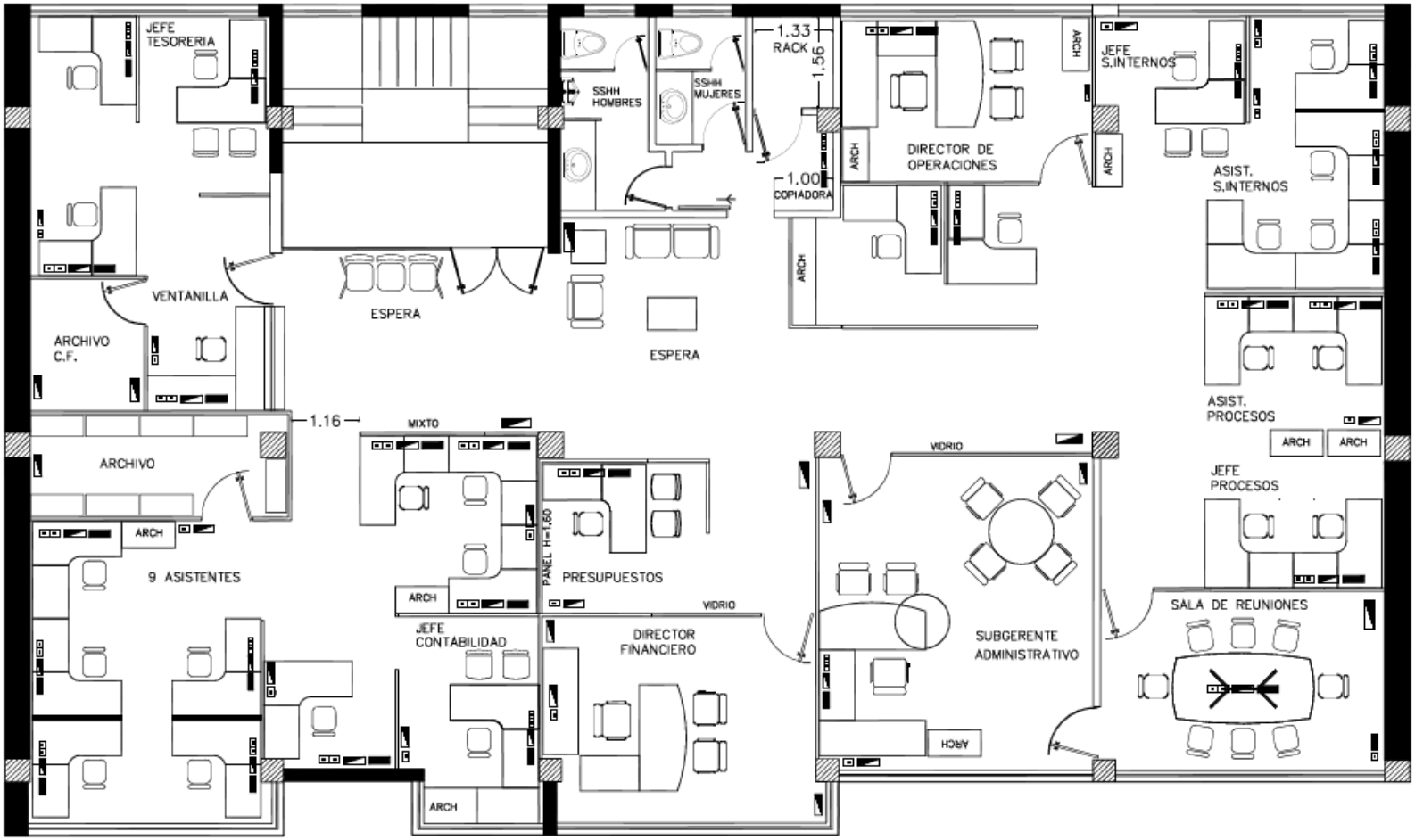
ANEXOS

Anexo 1 - Planos de planta de la oficina matriz

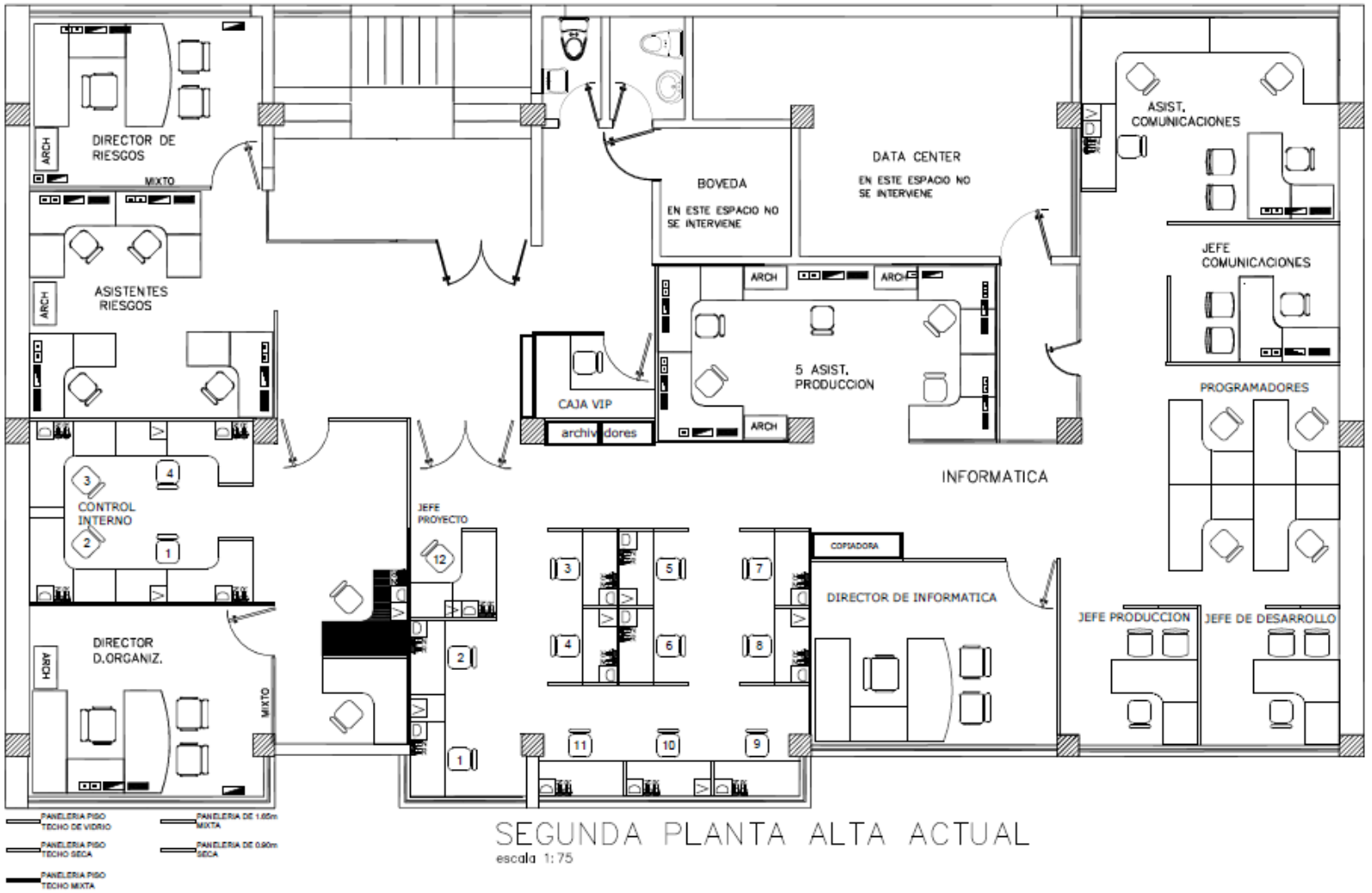
Planta Baja



Piso 1


JEFE TESORERIA
SSHH HOMBRES
SSHH MUJERES
1.33
RACK
1.56
DIRECTOR DE OPERACIONES
ARCH
JEFE S.INTERNOS
ASIST. S.INTERNOS
1.00
COPIADORA
VENTANILLA
ESPERA
ESPERA
ARCHIVO C.F.
ASIST. PROCESOS
1.16
MIXTO
ARCHIVO
VIDRIO
JEFE PROCESOS
9 ASISTENTES
PANEL H=1.60
PRESUPUESTOS
SALA DE REUNIONES
JEFE CONTABILIDAD
DIRECTOR FINANCIERO
SUBGERENTE ADMINISTRATIVO

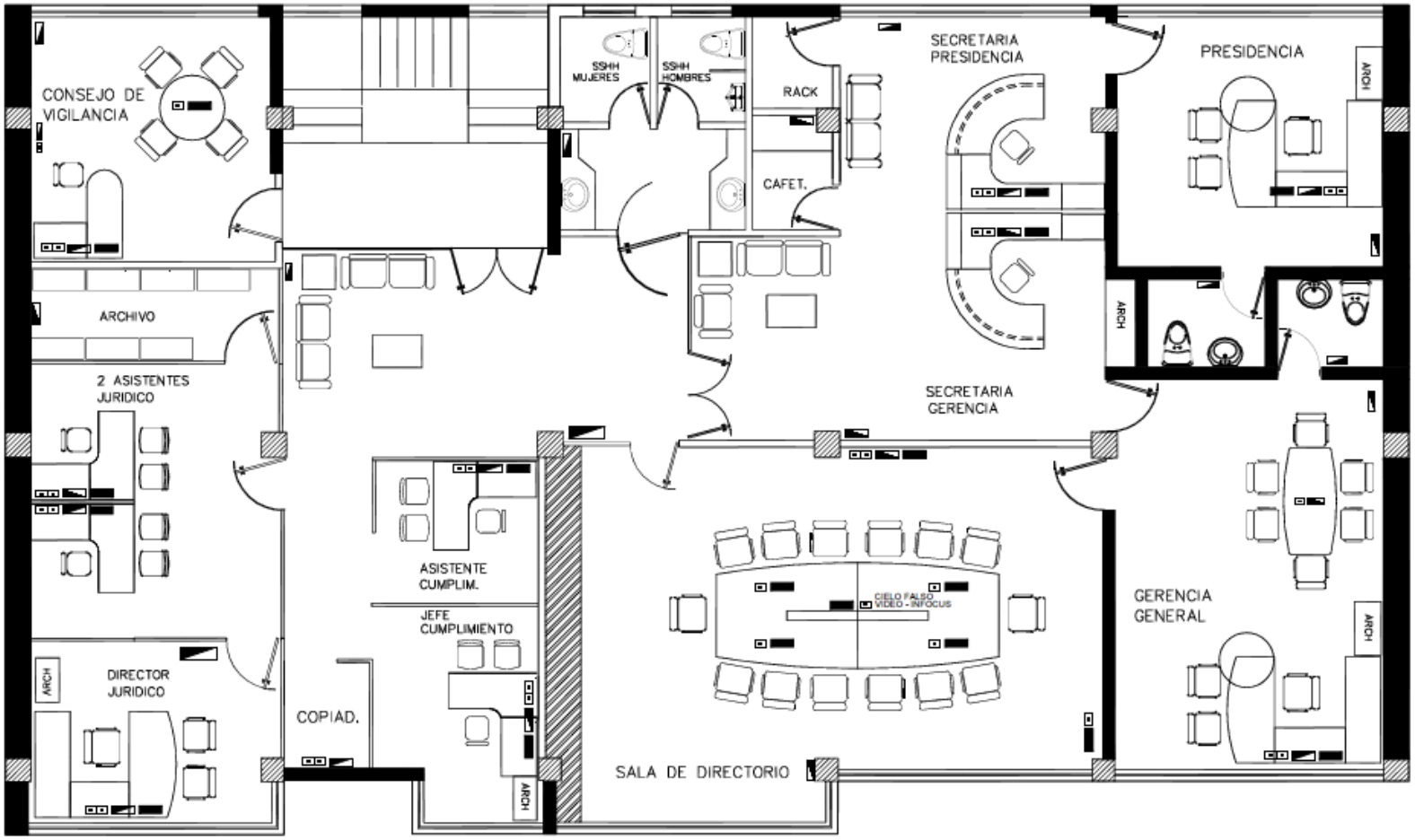
Piso 2



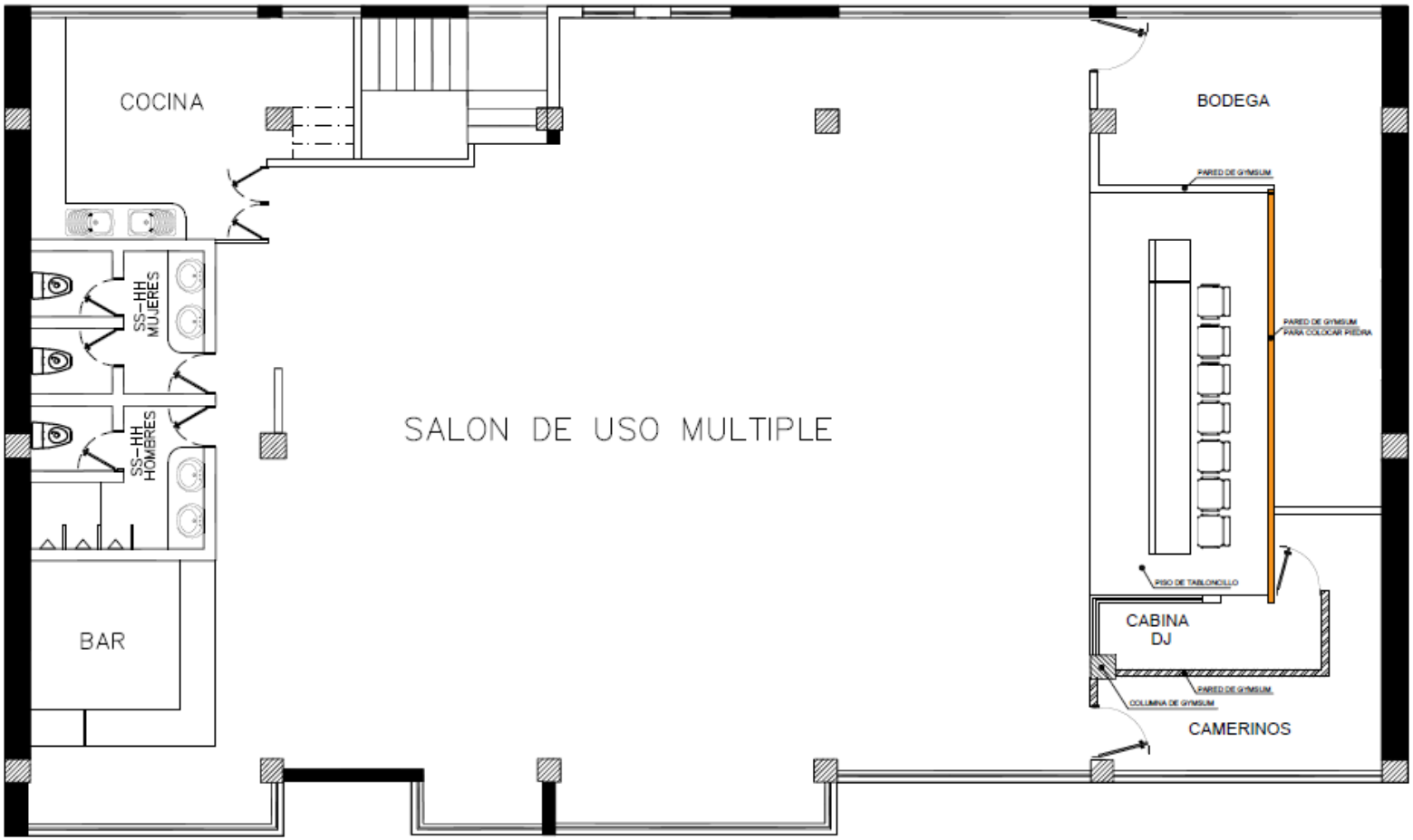
SEGUNDA PLANTA ALTA ACTUAL

escala 1:75

Piso 3

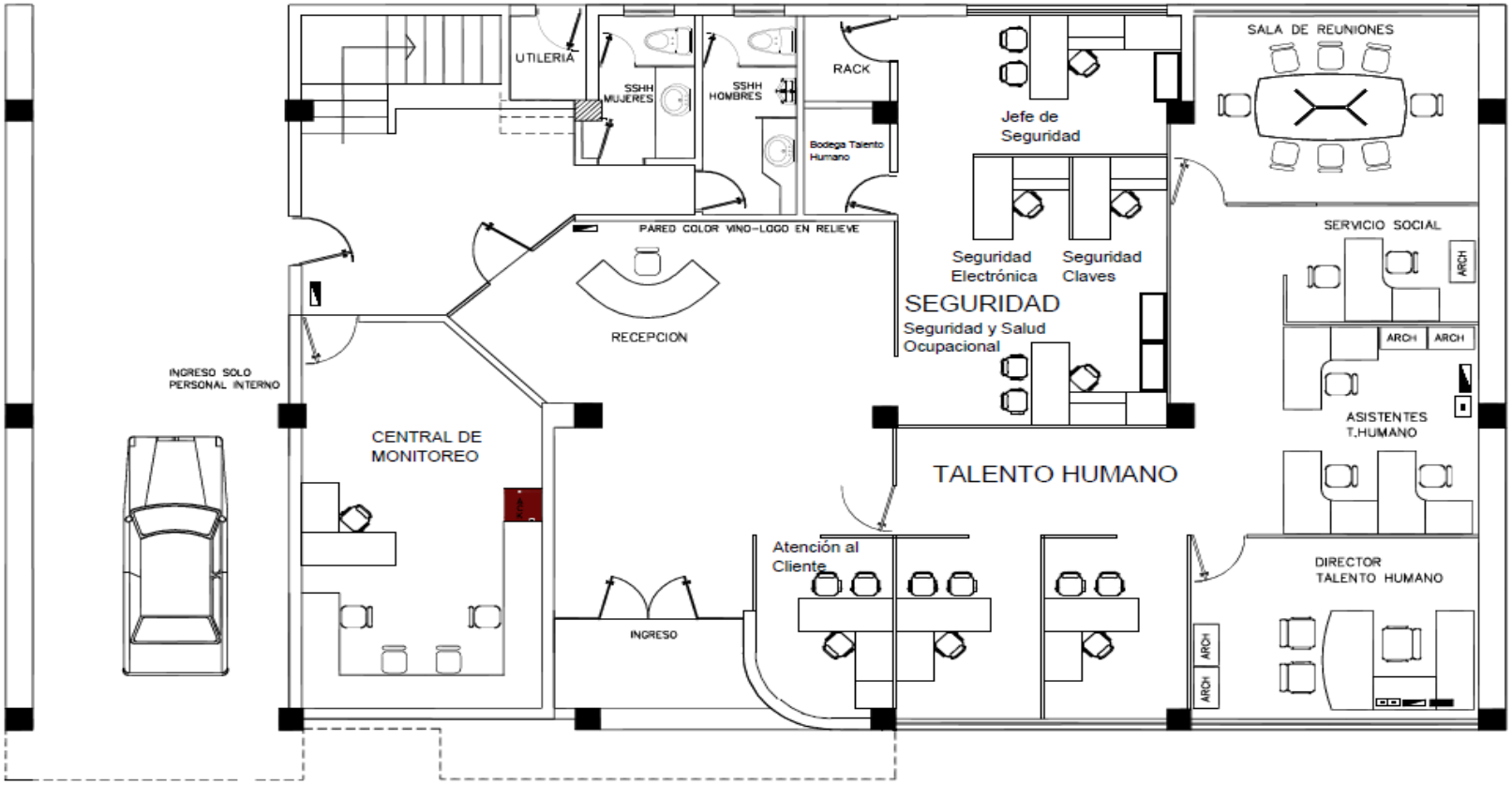

CONSEJO DE VIGILANCIA
SSHH MUJERES
SSHH HOMBRES
RACK
CAFET.
SECRETARIA PRESIDENCIA
PRESIDENCIA
ARCH
ARCHIVO
2 ASISTENTES JURIDICO
SECRETARIA GERENCIA
ASISTENTE CUMPLIM.
JEFE CUMPLIMIENTO
CIELO FALSO VIDEO - INFOCUS
GERENCIA GENERAL
DIRECTOR JURIDICO
COPIAD.
SALA DE DIRECTORIO

Piso 4


COCINA
SS-HH MUJERES
SS-HH HOMBRES
BAR
SALON DE USO MULTIPLE
BODEGA
PARED DE GYMSUM
PARED DE GYMSUM PARA COLOCAR PIEDRA
PISO DE TABLONCILLO
CABINA DJ
PARED DE GYMSUM
COLUMNA DE GYMSUM
CAMERINOS

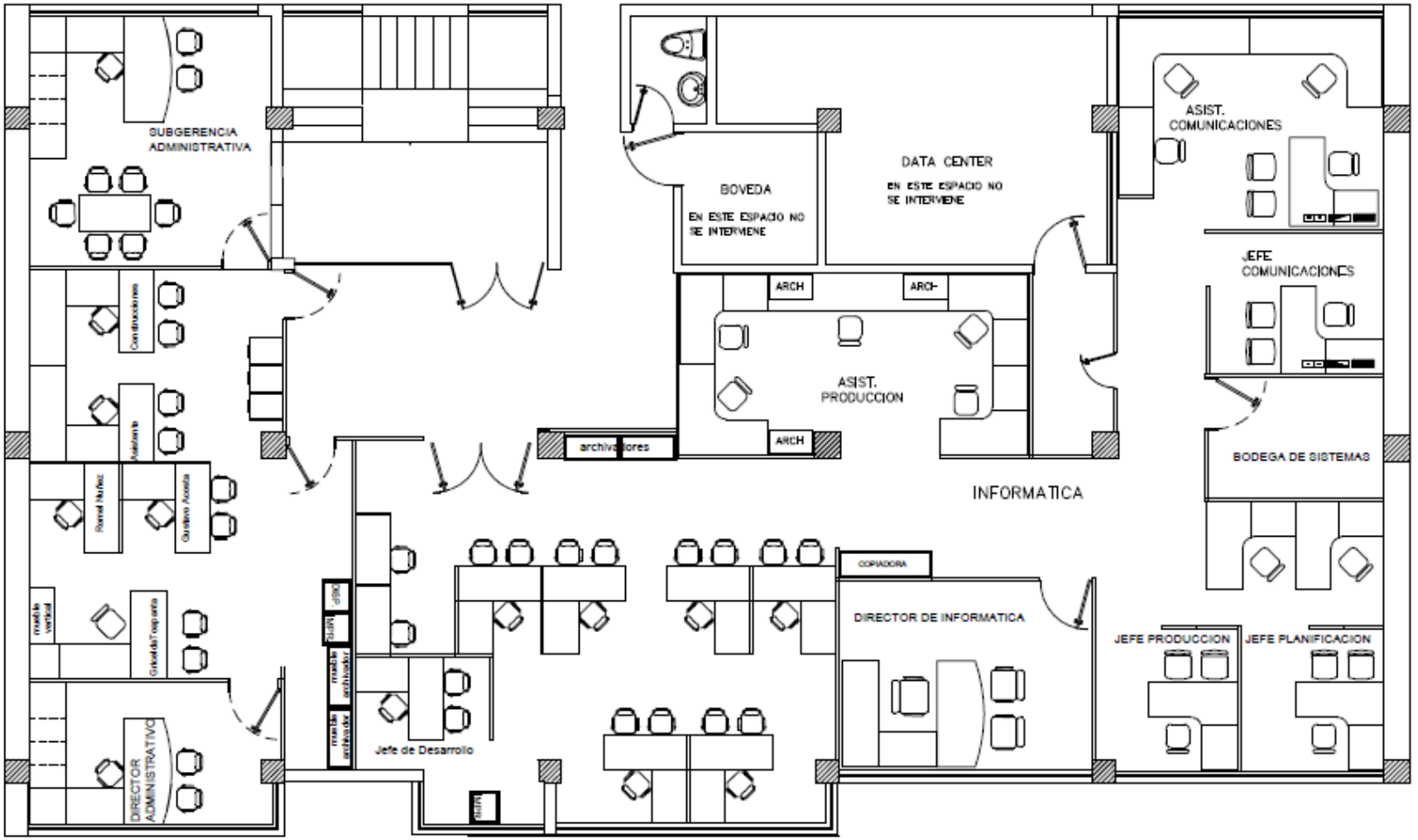
Anexo 2 - Planos de los bloques de la oficina matriz

Bloque A Planta Baja

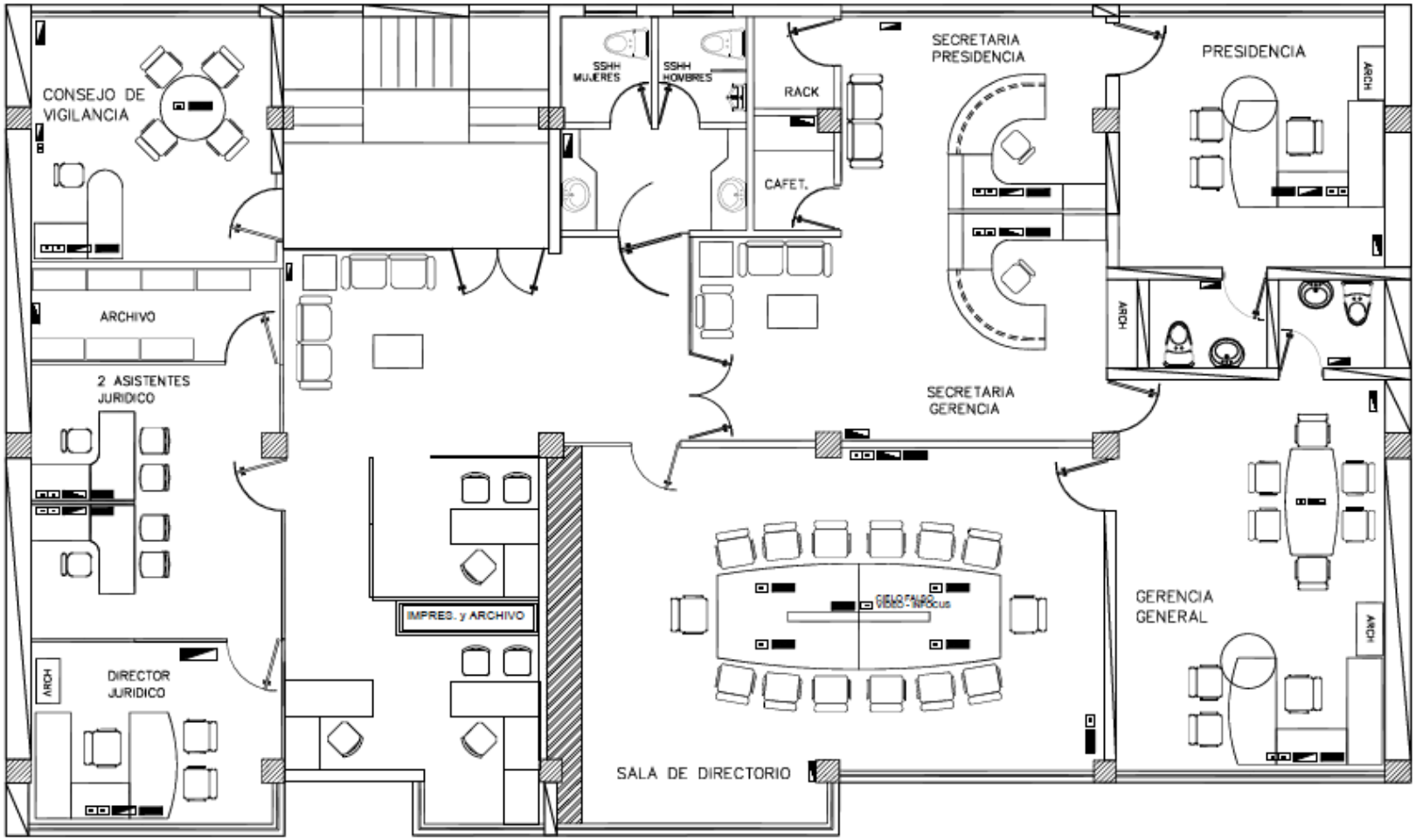


Bloque A Primera Planta

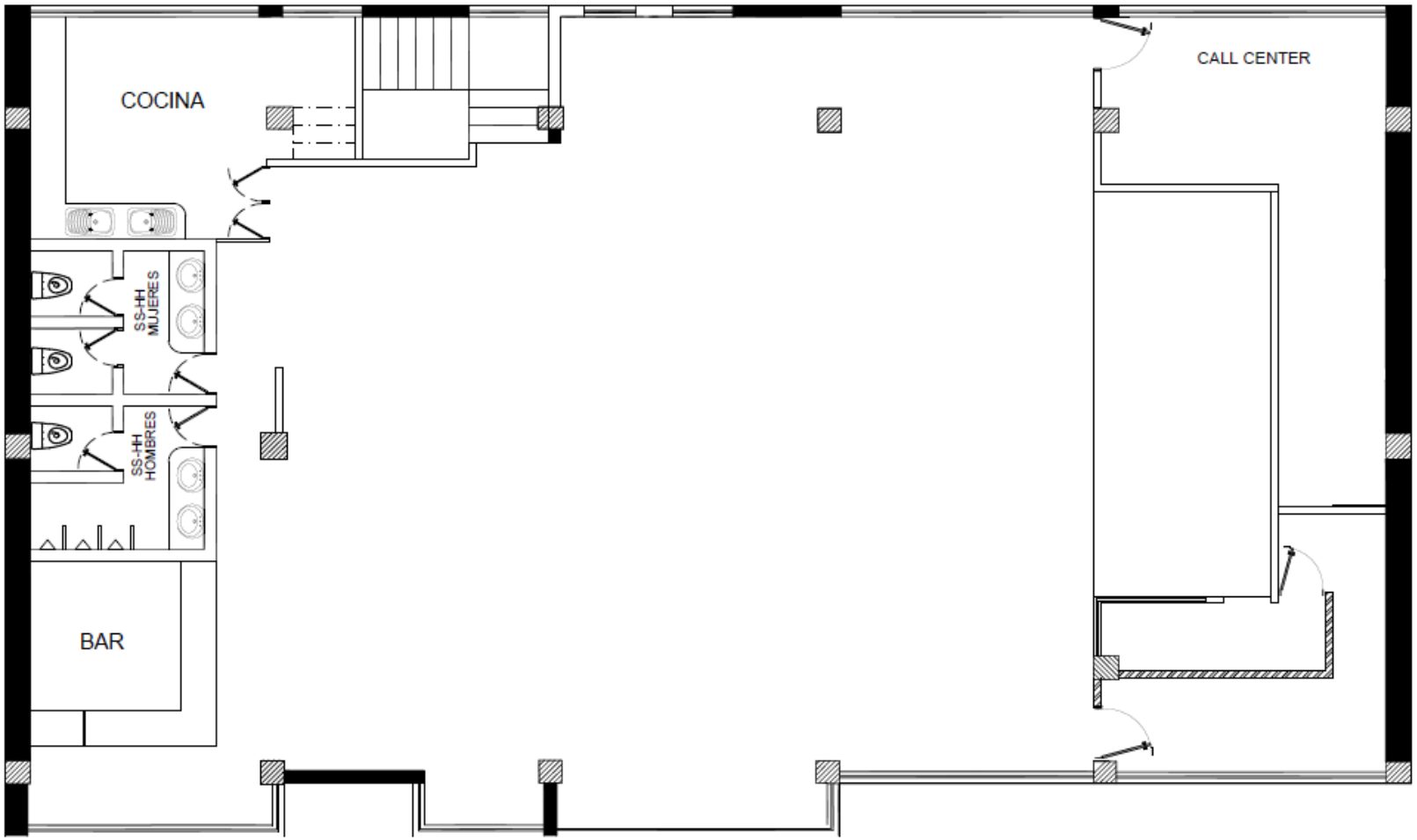
Bloque A Segunda Planta



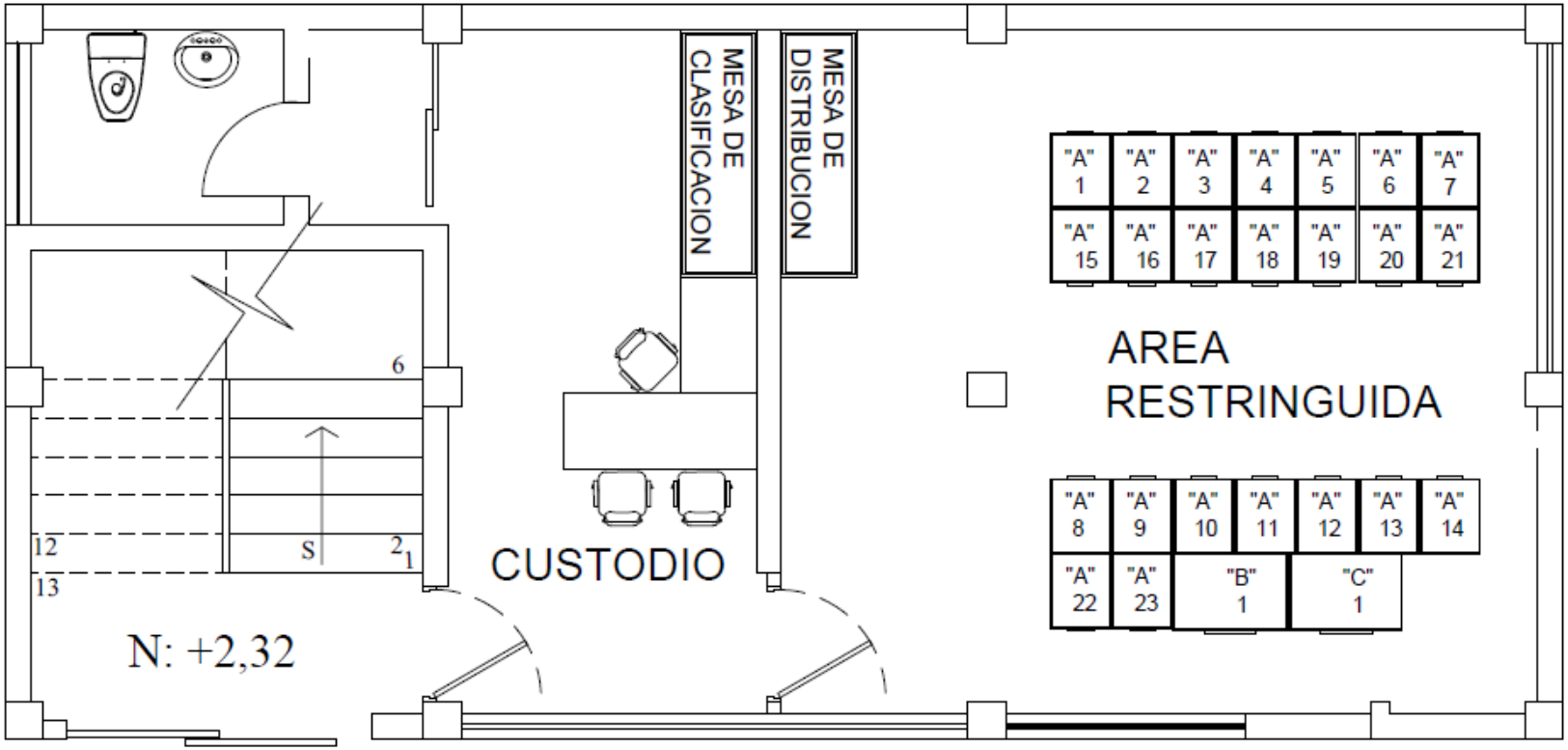
Bloque A Tercera Planta



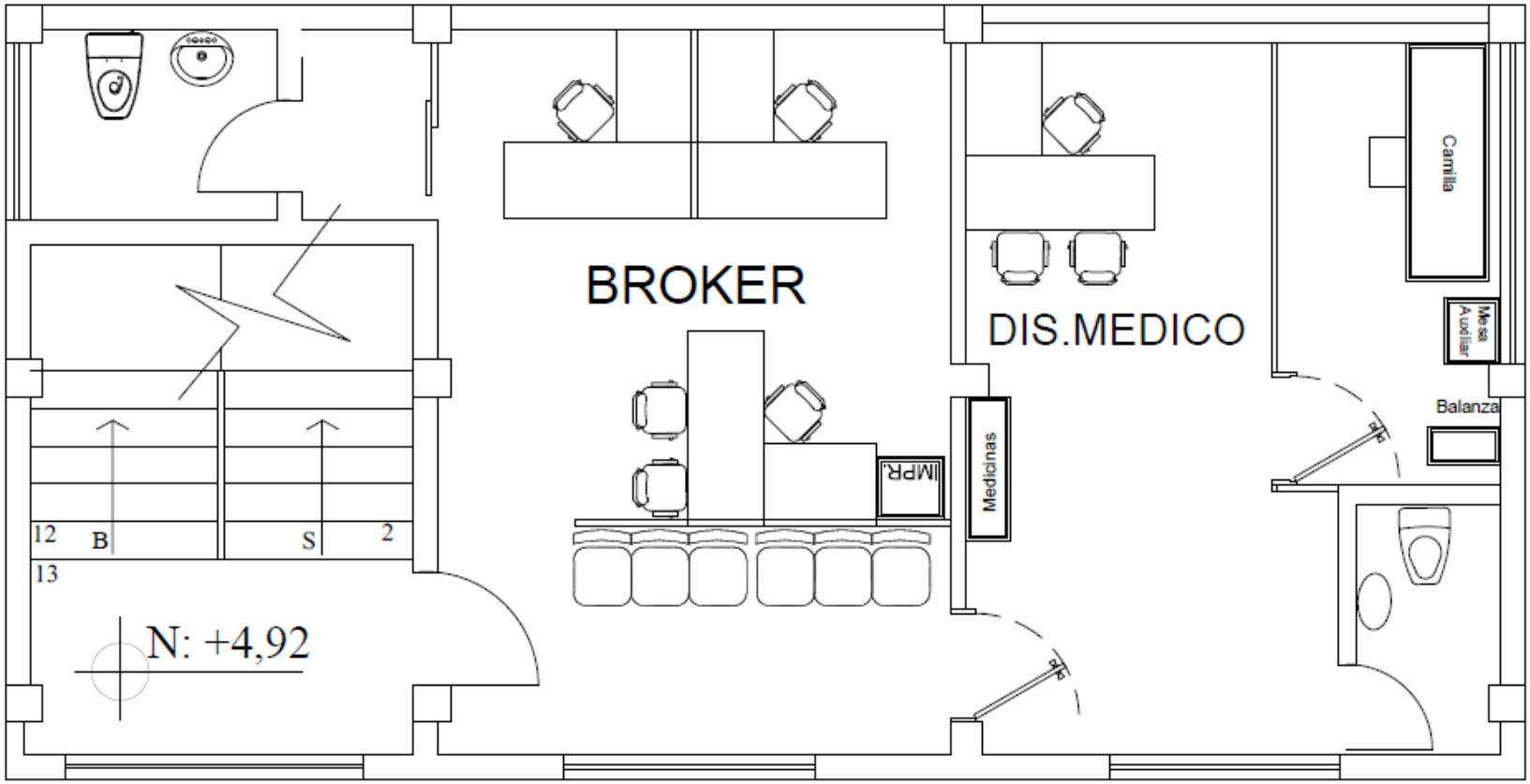
Bloque B Cuarta Planta



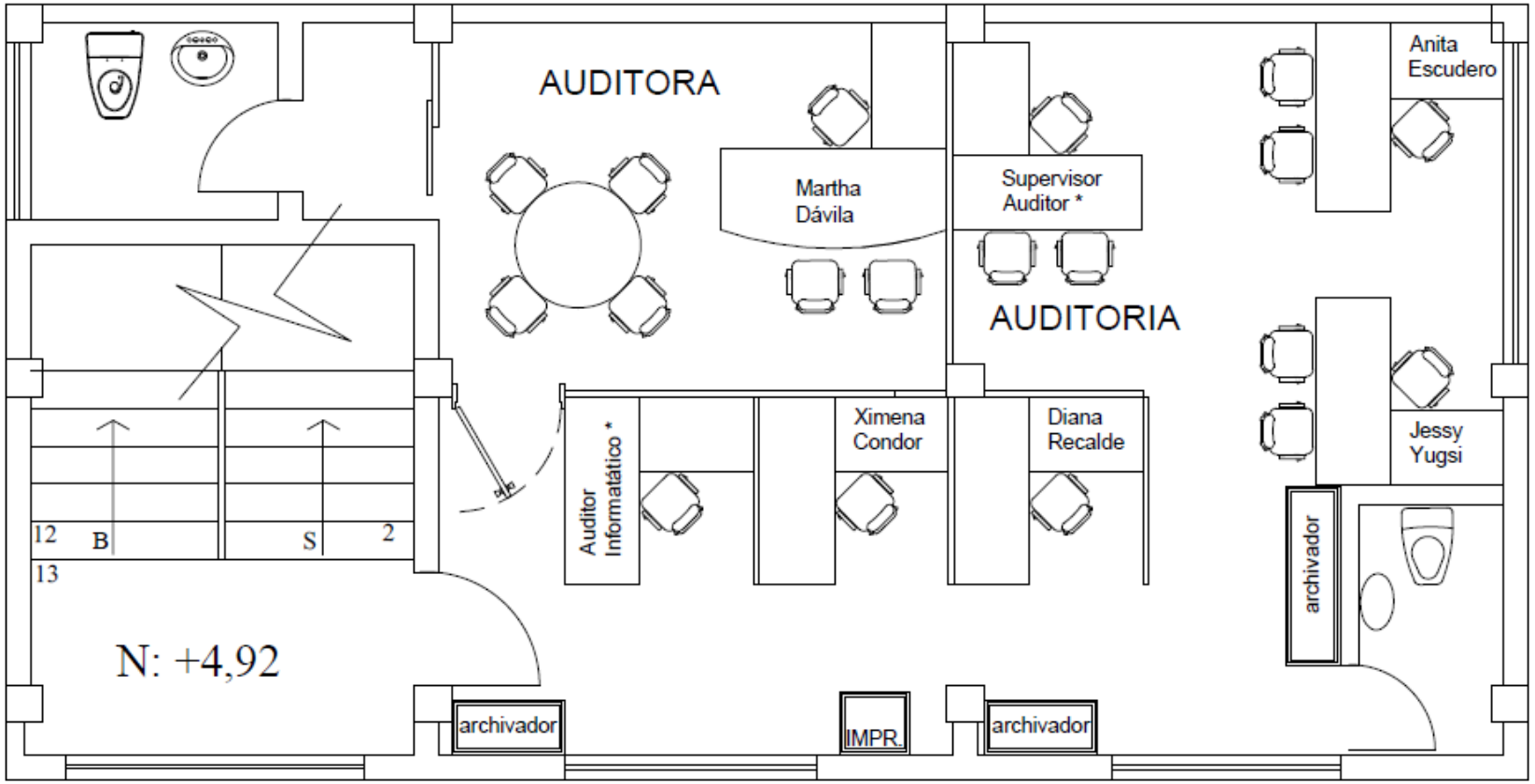
Bloque B Planta Baja



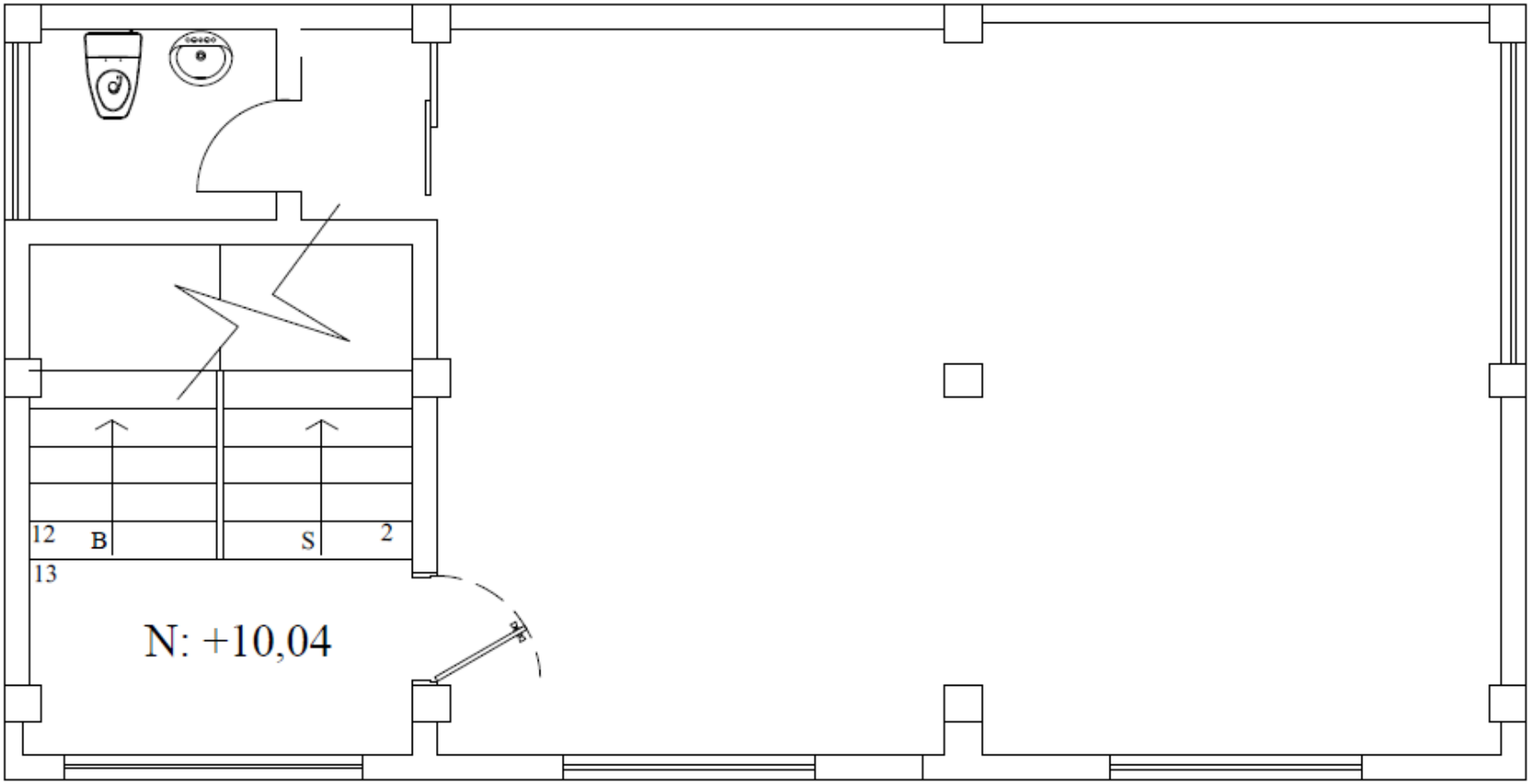
Bloqueo B Primera Planta



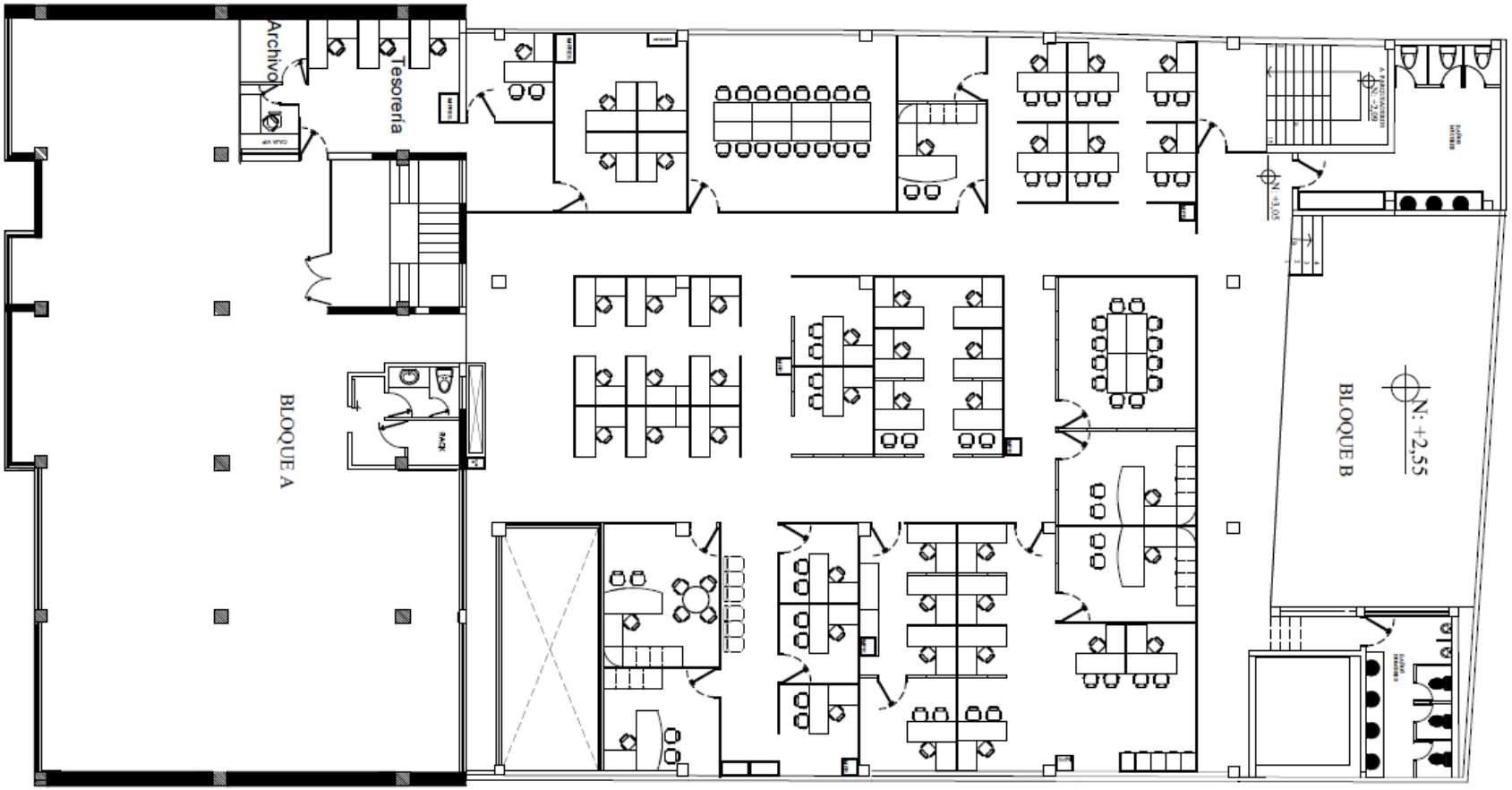
Bloque B Segunda Planta



Bloque B Tercera Planta



Bloque C Primera Planta



Bloque C Segunda Planta