



FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS



REDISEÑO DE LA INFRAESTRUCTURA DE RED PARA LA
COOPERATIVA DE AHORRO Y CRÉDITO PABLO MUÑOZ VEGA



AUTOR

Edwin Paúl Tipán Calero

AÑO

2018



FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA INFRAESTRUCTURA DE RED PARA
LA COOPERATIVA DE AHORRO Y CRÉDITO PABLO
MUÑOZ VEGA

Trabajo de titulación presentado en conformidad a los requisitos para obtener el
título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Msc. Carlos Marcelo Molina Colcha

Autor

Edwin Paúl Tipán Calero

Año

2018

DECLARACIÓN PROFESOR GUÍA

Declaro haber dirigido el trabajo, “Rediseño de la Infraestructura de Red para la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega”, con el estudiante Edwin Paúl Tipán Calero, en el semestre 2018-1, 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.

Carlos Marcelo Molina Colcha

Magister en Tecnologías de la Información y Comunicación (TIC)

CI: 170962421-5

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo, “Rediseño de la Infraestructura de Red para la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega”, del estudiante Edwin Paúl Tipán Calero, en el semestre 2018-1, 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: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

Edwin Paúl Tipán Calero

CI: 171195356-0

AGRADECIMIENTOS

Agradezco a mi familia cercana quienes me han brindado apoyo en todas las etapas de la carrera.

Particularmente agradezco a mi padre Rosendo Tipán, ya que sin su apoyo habría sido imposible cursar los años de Universidad.

Agradezco el apoyo invaluable del Ing. Carlos Molina, pues sin su guía oportuna no habría podido llevar este proyecto a feliz término.

DEDICATORIA

Dedico este proyecto a mi hijo, Christian, quien al llegar a este mundo me mostró que siempre se puede hacer más por la familia y que todo empieza por la superación personal.

RESUMEN

La Cooperativa de Ahorro y Crédito “Pablo Muñoz Vega” es una entidad de intermediación financiera según lo señala la Resolución 85-019-DC de 24 de octubre de 1985 emitida por la Superintendencia de Bancos y Seguros. Actualmente cuenta con 65.447 asociados, distribuidos en las diferentes provincias de Carchi, Imbabura, Pichincha y Sucumbíos. Esta entidad financiera ha experimentado un crecimiento en los últimos tiempos, razón por la cual ha requerido mejorar sus sistemas informáticos y su infraestructura de red.

Capítulo 1. En este capítulo se tratarán todos los criterios, normativas, estándares y fundamentos tecnológicos actuales que permitirán desarrollar los siguientes Capítulos en lo referente a levantamiento de información y diseño de la solución para la entidad. Se revisan criterios relevantes de las normas ANSI EIA / TIA 942 y 568-B a la luz de los cuales se levantará la información de línea base del estado de la red.

Capítulo 2. En este capítulo se realizará el levantamiento de la información actual del estado y servicios de red en la Cooperativa que servirá como línea base. Se toma en cuenta la normativa de la SEPS adoptada de la Resolución JB-2014-3066 SBS, la cual realiza recomendaciones referentes a la seguridad de la información, las operaciones y la continuidad del negocio para luego pasar a analizar la red y servicios en base a las normas ANSI EIA / TIA revisadas en el Capítulo 1. Se realizará una tabla donde se especifican los problemas hallados y que serán posteriormente tratados en el diseño de la solución.

Capítulo 3. En este capítulo se realizará el diseño de la solución para la red de la Cooperativa, tomando siempre en cuenta los criterios definidos en los capítulos previos con los cuales se procederá a aplicar la metodología Top-Down para el desarrollo propuesto. Se usarán protocolos y esquemas de Networking de tal forma que el resultado sea una red escalable, redundante, jerárquica y con elevados niveles de disponibilidad.

ABSTRACT

The Savings and Credit Cooperative "Pablo Muñoz Vega" is a financial intermediation entity as indicated in Resolution 85-019-DC of October 24, 1985 issued by the Superintendence of Banks and Insurance. Currently it has 65447 associates, distributed in the different provinces of Carchi, Imbabura, Pichincha and Sucumbíos. This financial institution has experienced growth in recent times, which is why it has required improving its computer systems and its network infrastructure.

Chapter 1. This chapter will deal with all the criteria, regulations, standards and current technological foundations that will allow developing the following Chapters in relation to information gathering and design of the solution for the entity. Relevant criteria of the ANSI EIA / TIA 942 and 568-B standards are reviewed in light of which the baseline information of the state of the network will be lifted.

Chapter 2. In this chapter, the current state information and network services will be collected in the Cooperative that will serve as the baseline. The regulations of the SEPS adopted from Resolution JB-2014-3066 SBS are taken into account, which makes recommendations regarding the security of information, operations and business continuity, to then analyze the network and services based on to the ANSI EIA / TIA standards reviewed in Chapter 1. A table will be made where the problems found are specified and which will be later treated in the design of the solution.

Chapter 3. In this chapter, the design of the solution for the Cooperative's network will be carried out, always taking into account the criteria defined in the previous chapters with which the Top-Down methodology will be applied for the proposed development, networking protocols and schemes will be used in such a way that the result is a scalable, redundant, hierarchical network with high levels of availability.

ÍNDICE

INTRODUCCIÓN	1
1. CAPÍTULO I. MARCO TEÓRICO	5
1.1. Subsistemas en el Estándar ANSI EIA/TIA 942.....	5
1.1.1. Subsistema Infraestructura	8
1.1.1.1. Topología para un Centro de Datos	8
1.1.1.2. Elementos de un Centro de Datos	9
1.1.2. Subsistema Arquitectura.....	11
1.1.2.1. Puerta de acceso y techo.....	11
1.1.2.2. Iluminación	12
1.1.2.3. Piso falso.....	12
1.1.3. Subsistema Eléctrico	12
1.1.4. Subsistema Mecánico.....	13
1.1.4.1. Condiciones ambientales a tomar en cuenta	13
1.1.4.2. Pasillo frío y caliente	14
1.2. Subsistemas en el estándar ANSI EIA/TIA 568-B	15
1.2.1. ANSI EIA/TIA 568-B.1	23
1.2.2. ANSI EIA/TIA 568-B.2	23
1.2.3. ANSI EIA/TIA 568-B.3	24
1.3. Conceptos generales de redes	25
1.3.1. Redes LAN	25
1.3.1.1. 802.3 Redes Ethernet	26
1.3.1.2. IEEE 802.1Q	26
1.3.1.3. IEEE 802.1p.....	27
1.3.1.4. IEEE 802.1w	27
1.3.1.5. IEEE 802.11 WLAN.....	27
1.3.2. Redes WAN.....	28
1.3.2.1. Multi Protocol Label Switching	28
1.1.1. Redes SAN.....	29

2. CAPÍTULO II. LEVANTAMIENTO DE LA

LINEA BASE	31
2.1. Resolución JB-2014-3066 SBS.....	31
2.1.1. Continuidad del Negocio.....	31
2.1.3. Lineamientos generales.....	32
2.1.4. Levantamiento Continuidad del Negocio	34
2.2. Levantamiento Centro de Datos (EIA / TIA 942).....	35
2.2.1. Subsistema de Infraestructura	35
2.2.1.1.1. Cableado estructurado Rack principal.....	36
2.2.2. Subsistema Arquitectura.....	38
2.2.2.1. Puertas de acceso	39
2.2.2.2. Techo	39
2.2.2.3. Piso	39
2.2.2.4. Seguridad física	39
2.2.2.5. Paredes.....	40
2.2.3. Subsistema Eléctrico	40
2.2.3.1. Proveedor de servicio eléctrico	41
2.2.3.2. Tableros eléctricos	41
2.2.3.3. Tomacorrientes	41
2.2.3.4. Luminarias.....	42
2.2.3.5. Generador eléctrico.....	42
2.2.3.6. UPS.....	42
2.2.3.7. Protección eléctrica	42
2.2.4. Subsistema Mecánico.....	43
2.2.4.1. Aire acondicionado.....	43
2.2.4.2. Seguridad ambiental	44
2.2.5. Resumen de problemas detectados en el Centro de Datos por cada uno de los Subsistemas.....	45
2.3. Levantamiento subsistema cableado pisos (EIA / TIA 568b).....	48
2.3.1. Subsistema Área de Trabajo	48

2.3.2.	Subsistema Horizontal	50
2.3.3.	Subsistema Vertical o Backbone Ascendente	50
2.3.4.	Subsistemas de Administración	51
2.3.5.	Subsistema de Sala de Equipos	51
2.3.6.	Resumen de problemas detectados en cada uno de los subsistemas	51
2.4.	Levantamiento infraestructura tecnológica de red	53
2.4.1.	Diagnóstico de recursos de red	53
2.4.2.	Equipos en los racks	57
2.4.3.	Topología de la red	60
2.4.4.	Telefonía IP	61
2.4.5.	Conexión de los Switches	63
3.	CAPÍTULO III. DISEÑO Y PROPUESTA DE LA SOLUCIÓN	64
3.1.	Reúso de equipos	64
3.2.	Diseño en descenso (Top-Down)	64
3.3.	Fase 1. Análisis de los requerimientos	65
3.3.1.	Metas del negocio	65
3.3.2.	Metas técnicas	67
3.3.3.	Red actual	68
3.3.4.	Tráfico actual	68
3.4.	Fase 2. Desarrollo del diseño lógico	69
3.4.1.	Diseño de la topología de red	69
3.4.2.	Diseño de los modelos de direccionamiento	70
3.4.3.	Definición de los protocolos para Switching y Routing	74
3.4.3.1.	Switching:	74
3.4.3.2.	Routing	77
3.4.3.3.	Red de almacenamiento SAN (Storage Area Network):	78
3.4.4.	Desarrollo de las estrategias para la seguridad de la red	82
3.4.4.1.	Confidencialidad	82
3.4.4.2.	Integridad	86

3.4.4.3.	Disponibilidad	88
3.4.4.4.	Autenticación.....	89
3.4.5.	Desarrollo de las estrategias para la administración de la red	90
3.4.5.1.	AAA (Authentication, Authorization, and Accounting)	90
3.4.5.2.	SMNP (Simple Network Management Protocol)	91
3.4.5.3.	NTP (Network Time Protocol)	93
3.4.5.4.	Servidores en redundancia con Arquitectura de Nube privada de Oracle.	94
3.5.	Fase 3. Centro de Datos, nuevo diseño físico.....	96
3.5.1.	Diseño físico Centro de Datos EIA / TIA 924	97
3.5.1.1.	Cableado horizontal	97
3.5.1.2.	Cableado vertical	98
3.5.2.	Subsistema Arquitectura	99
3.5.2.1.	Requerimientos	99
3.5.3.	Subsistema Eléctrico	100
3.5.3.1.	Requerimientos	100
3.5.4.	Subsistema Mecánico.....	101
3.5.4.1.	Requerimientos	101
3.6.	Subsistemas de cableado estructurado (EIA / TIA 568B)..	101
3.6.1.	Requerimientos subsistemas de cableado estructurado	102
3.6.1.1.	Subsistema Backbone vertical	102
3.7.	Infraestructura tecnológica de red	102
3.7.1.	Requerimientos switching	102
3.7.2.	Requerimientos routing.....	103
3.7.3.	Requerimientos red SAN	103
3.7.4.	Requerimientos de ancho de banda	104
3.8.	Indicadores de Éxito	107
3.9.	Análisis Técnico-Económico	109
4.	CONCLUSIONES Y RECOMENDACIONES.....	111
4.1.	Conclusiones	111
4.2.	Recomendaciones.....	112

REFERENCIAS	114
ANEXOS	117

INTRODUCCIÓN

Antecedentes

La Cooperativa de Ahorro y Crédito Pablo Muñoz Vega es una entidad de intermediación financiera cooperativista que capta recursos de personas con capacidad de ahorro y apoya a socios con necesidad de crédito.

Su casa matriz ubicada en la calle Colón y 10 de Agosto de la ciudad de Tulcán fue fundada en 1964, es una de las cooperativas más grandes del Ecuador, tiene 7 agencias en distintos puntos del país y más de 60.000 socios.

Las cooperativas de ahorro y crédito son organizaciones controladas por sus miembros, quienes eligen un comité de vigilancia, el cuál toma decisiones respecto de su rumbo.

Estas entidades son vigiladas por las entidades, Superintendencia de Economía Popular y Solidaria y Superintendencia de Bancos y Seguros.

La cooperativa desde sus inicios ha ido evolucionando en su infraestructura de red, desde las más insipientes tecnologías hasta los sistemas más actuales, sin embargo, este crecimiento se ha dado de una manera poco planificada y con pocas o ninguna consideración técnica y de diseño, lo cual ha provocado constantes paradas en los servicios a los socios. Esto incluso podría traer sanciones desde la SEPS dependiendo del tiempo sin servicio, sin contar con la pérdida de la confianza de los usuarios.

Actualmente la Cooperativa ha empezado un proceso de migración de su anterior core financiero Cobis hacia un software llamado Finacial. Este proceso ha puesto de relieve todas las falencias acumuladas en la infraestructura de red y de comunicaciones.

El nuevo sistema financiero tiene una nueva arquitectura en capas, lo cual también supone nuevos requerimientos dentro de la red en general, haciendo patente que se debe realizar un rediseño urgente.

Cabe destacar que inclusive la página web donde reside un sistema de transacciones en línea fue atacado y vulnerado, poniendo en serio riesgo la infraestructura y la información financiera.

Alcance

El alcance de este proyecto es rediseñar la infraestructura de red de la Cooperativa mencionada, optimizando los recursos tecnológicos existentes.

Dentro del alcance se incluyen:

- Hacer un análisis de la situación de la infraestructura tecnológica actual del Centro de Procesamiento de Datos en la Matriz, ancho de banda y transaccionalidad.
- Diseñar el nuevo esquema de infraestructura tecnológica para el core del negocio en cuanto a seguridades, arquitectura de red, enlaces, ancho de banda, que se aplicará en la Cooperativa, el cual estará alineado con las necesidades particulares de la entidad y las mejores prácticas de los representantes de cada marca de tecnología o estándares requeridos tales como ANSI EIA/TIA 942 y 568-B, la metodología de diseño de redes descendente (top-down) y la Resolución JB-2014-3066 de la Superintendencia de Economía Popular y Solidaria (SEPS) y la Superintendencia de Bancos y Seguros (SBS) para el Subsistema de Infraestructura de Red y tomando en cuenta los recursos de TI con los que cuenta la entidad.

Justificación

Una Cooperativa de Ahorro y Crédito, como ente financiero en donde se ha confiado no solo dinero de los socios sino también su información monetaria, muy sensible, debe estar soportada por una infraestructura de comunicaciones e información muy robusta y segura.

Existen normativas vigentes que exigen estándares de disponibilidad,

confiabilidad y seguridad que deben ser cumplidas, dentro de las cuales se tienen las normativas dadas por la SBS y que fueron heredadas por la SEPS tal es el caso de la Resolución JB-2014-3066 (Anexo A), relacionadas con la incorporación de medidas de seguridad en el manejo de sus canales electrónicos, también con las recomendaciones de los estándares ANSI EIA/TIA 942 y 568-B y la metodología del diseño de redes descendente (Top-Down) para el Subsistema de Infraestructura de Red a fin de garantizar la disponibilidad, confiabilidad y seguridad en la continuidad de las operaciones del negocio.

Objetivos

Objetivo General

Rediseñar la infraestructura de red de la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega, optimizando los recursos de tecnología de información existentes.

Objetivos específicos

- Realizar el levantamiento de información de la infraestructura física y lógica de la red de datos de la Matriz de CPMV, que permita conocer el estado actual y sirva de línea base para establecer los requerimientos de mejora del Subsistema de Infraestructura de Red mediante la aplicación de los lineamientos del estándar ANSI EIA / TIA-942.
- Diseñar la nueva infraestructura de red de la sucursal Matriz de la Cooperativa, considerando un modelo jerárquico y redundante, optimizando los recursos tecnológicos con los que cuenta la entidad tomando como referencia la metodología de diseño de redes descendente (Top-Down).

Metodología

Se recurrirá al método exploratorio en el momento de partir con la observación y diagnóstico del estado actual de la infraestructura de la red.

A continuación, la metodología más adecuada a usar es el método inductivo, debido a la aplicación de criterios de Tecnologías de la Información para pasar a postular la forma de implementar las soluciones a los problemas identificados

El primer paso del primer método elegido consiste en la aplicación de herramientas de diagnóstico y reconocimiento de direccionamiento IP y dispositivos dentro de la red, luego se elaboran *Layouts* con la información levantada.

El postulado de las soluciones tomará como criterio base a: hojas de datos, *whitepapers*, casos de éxito, de cada equipo y la tecnología que representa.

1. CAPÍTULO I. MARCO TEÓRICO

Este capítulo trata sobre los fundamentos teóricos a ser aplicados durante el proceso de rediseño de la infraestructura de red de la Cooperativa Pablo Muñoz Vega en la Agencia Matriz ubicada en la ciudad de Tulcán, provincia del Carchi.

Se toma el estándar ANSI EIA/TIA 942 para describir los aspectos que se alinean con el proyecto; se revisan las particularidades de cada uno de los subsistemas aplicados al mismo, tales como de Infraestructura de red, Arquitectura (a nivel de obra civil), Eléctrica y Mecánica.

Finalmente se revisan los criterios técnicos del estándar ANSI EIA/TIA 568B, los cuales establecen parámetros para el diseño o implementación de sistemas pasivos de red.

1.1. Subsistemas en el Estándar ANSI EIA/TIA 942

Centro de Datos:

Un Centro de Datos es un área física destinada al procesamiento de datos y comunicaciones, está integrada por varios espacios o áreas funcionales, según se muestra en la Figura 1 (ADC's Optical Distribution Frame, 2008).

- Un Cuarto de Entrada (ER)
- Un Área de Distribución Principal. (MDA)
- Un Área de Distribución Horizontal. (HDA)
- Un Área de Distribución de Zonas. (ZDA)
- Un Área de Distribución de Equipos. (EDA)

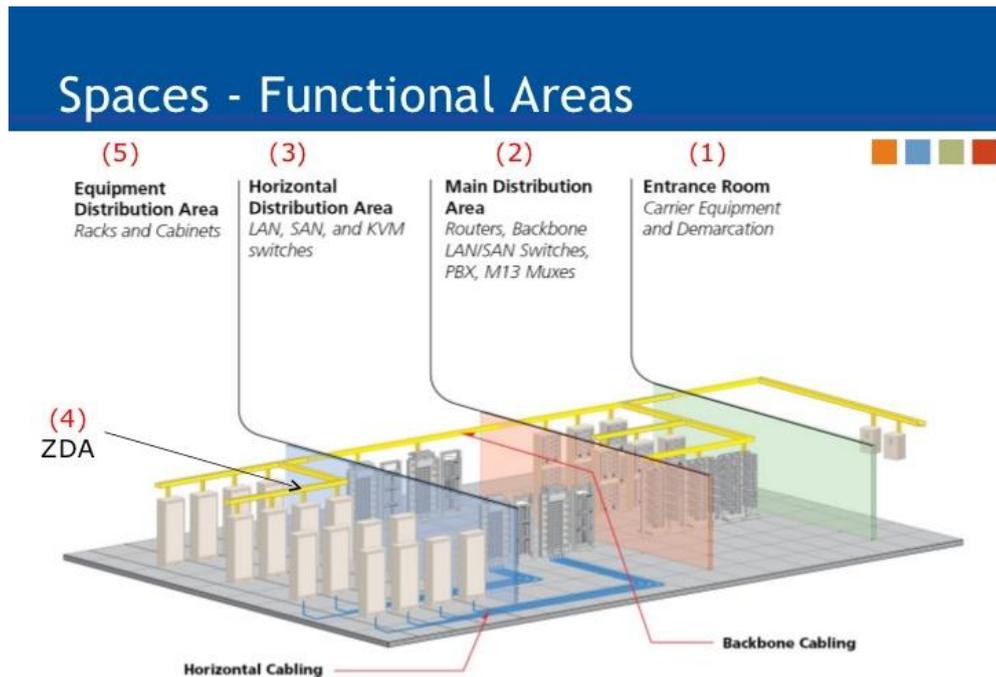


Figura 1. Centro de datos.

Tomado de (ADC Telecommunications, Inc, 2008).

Para que un determinado espacio o área física sea considerada un Centro de Datos o cuarto de Cómputo, debe tener como mínimo los siguientes sistemas de soporte e infraestructura dimensionados para atender la capacidad nominal “N” del Cuarto de Cómputo:

- Un perímetro seguro que mantenga el ambiente controlado, este perímetro deberá estar construido con elementos resistentes al fuego para mínimo una hora, según lo establece NFPA 75, y las paredes deben cubrir toda la altura del recinto.
- Los materiales de construcción interna del Cuarto de Cómputo deben estar de acuerdo a NFPA 75 y NFPA 101.
- Un sistema mecánico de aire acondicionado de Precisión, para mantener controlada la carga térmica generada por la capacidad “N”, controlando los parámetros de temperatura y humedad de acuerdo a lo

- estipulado en ASHRAE “The Thermal Guidelines for Data Processing Environments”.
- Un sistema Eléctrico de respaldo de energía, que permita mantener la carga “N” operando durante un corte de energía.
 - Un sistema de Respaldo de Energía Generador y/o Baterías para al menos mantener operando el Centro de Datos con su capacidad “N”, 12 horas continuas.
 - Un sistema automático de Detección de incendios basado detección puntual tipo fotoeléctrica y/o iónica, con un panel de Control y notificación según NFPA 75 y NFPA 2001, que cubra todo el Cuarto de Cómputo.
 - Un sistema de Supresión de incendios con agente Limpio listado bajo NFPA 2001 que cubra todo el ambiente del Cuarto de Cómputo incluyendo si existen bajo pisos elevados y sobre cielos falsos.
 - Una sala independiente para almacenaje de respaldos de información (cintas)

Estándar ANSI EIA/TIA 942

La Telecommunication Industry Association (TIA) publicó en abril de 2005 el Estándar TIA-942, cuyo fin busca determinar criterios de normativas técnicas y unificar los requerimientos para el diseño en las áreas de comunicaciones y de tecnología respectivamente. Está basada en las normas TIA-568 y TIA-569. Asimismo, aplica las instrucciones establecidas por la norma TIA-606.

Este Estándar es concebido para el uso de diseñadores quienes necesitan una comprensión y entendimiento del diseño de un Centro de Datos que incluye los principales temas relevantes para una correcta implementación relacionados

con los subsistemas de Telecomunicaciones (Infraestructura de red), Arquitectura y los sistemas eléctrico y mecánico.

Además, determina la infraestructura de soporte para los subsistemas antes mencionados, mismos que se enfocan a la planificación de facilidades, la selección del sitio, las topologías que clasifican un Centro de Datos de acuerdo a su disponibilidad, el sistema de protección contra fuego, el sistema de seguridad, la automatización o control, el diseño de red, el comisionamiento y la capacitación.

A continuación, se describe los ítems de los subsistemas que el estándar establece para cada uno de ellos (TIA, 2014).

1.1.1. Subsistema Infraestructura

Para este subsistema la norma establece los requerimientos de cableado, topologías, equipos e infraestructura de telecomunicaciones para ofrecer un óptimo servicio informático a la empresa.

1.1.1.1. Topología para un Centro de Datos

La norma establece un área de distribución principal junto con la conexión principal y horizontal.

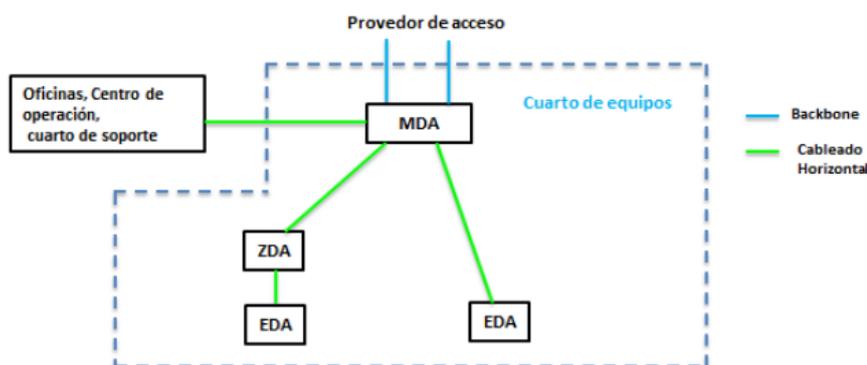


Figura 2. Topología de un Centro de Datos.

Tomado de (TIA, 2014).

1.1.1.2. Elementos de un Centro de Datos

Un centro de datos que cumple con la norma ANSI EIA / TIA 942 está conformado por varios elementos que se aprecian en la siguiente figura:

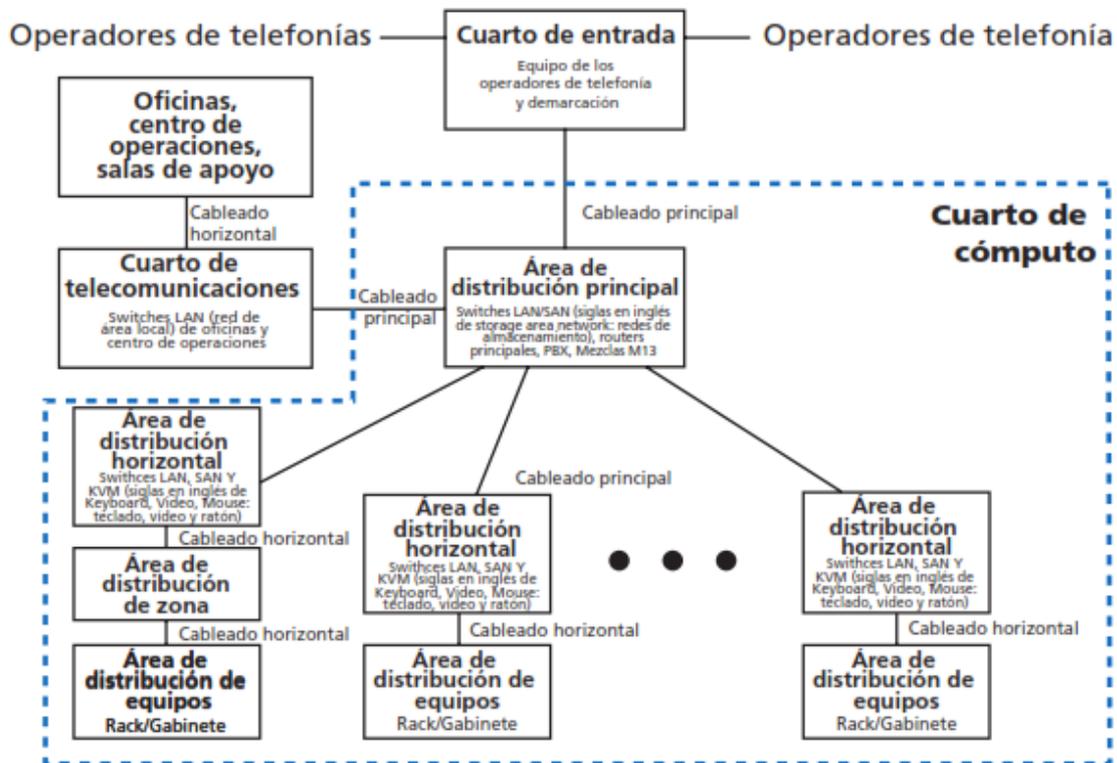


Figura 3. Diagrama de un Centro de Datos.

Tomado de (TIA, 2014).

Los espacios de telecomunicaciones de los centros de datos incluyen algunos elementos como: MDA, HAD, ZDA, EDA, cuarto de equipos y el cuarto de entrada; a continuación, se presenta la funcionalidad de cada uno de ellos

- Cuarto de telecomunicaciones o TR (uno o más)
- Cuarto de equipos
- Cuarto de entrada
- Área de distribución principal (MDA)
- Área de distribución horizontal (HDA) (una o varias)
- Área de distribución de equipos (EDA)

- Área de distribución de zona (ZDA)

Los espacios de telecomunicaciones de centros de datos incluyen algunos elementos como: MDA, HAD, ZDA, EDA, cuarto de equipos y el cuarto de entrada; a continuación, se presenta la funcionalidad de cada uno de ellos:

1.1.1.2.1. Cuarto de telecomunicaciones (TR)

Espacio que soporta el cableado a zonas exteriores al cuarto de equipos, en caso de ser necesario se puede combinar el MDA y HDA, puede existir más de un cuarto de telecomunicaciones si se requiere.

1.1.1.2.2. Cuarto de equipos (ER)

Es el cuarto principal de la empresa, el que brinda los servicios de telecomunicaciones a los diferentes departamentos o áreas de trabajo de una empresa. Aquí se alojan equipos pesados de gran tamaño que deben encontrarse trabajando en óptimas condiciones ambientales y físicas

1.1.1.2.3. Área de distribución principal (MDA)

Espacio ubicado dentro del ER, donde se encuentra el punto de distribución principal o conexión cruzada principal para el cableado y elementos como: routers de núcleo, switches, LAN, SAN y PBX, y equipos de aprovisionamiento del proveedor. Debe de ser ubicado en un punto central del lugar para no exceder longitudes máximas de cables, si se encuentra en una habitación cerrada debe de contar con los sistemas HVAC, PDU y UPS, en lo que se refiere a aspectos arquitectónicos, eléctricos y mecánicos debe ser igual que en ER.

1.1.1.2.4. Área de distribución horizontal (HDA)

Es el punto de distribución para el cableado horizontal, conexiones cruzadas y equipos activos de distribución de cable en la zona de distribución de equipos. En este espacio se instala racks separados de fibra óptica, cable UTP y

coaxial, además se colocan switches y patch panels para minimizar la longitud del patch cord.

Está localizado en ER y el número de conexiones depende de la capacidad de la bandeja de cable. En cuanto se refiere a requisitos arquitectónicos y eléctricos son los mismos que se detallaron para ER.

1.1.1.2.5. Área de distribución de equipos (EDA)

Es donde el HC termina en los patch panels, aquí se encuentran conectados equipos finales como: sistemas informáticos, ordenadores y equipos de telecomunicaciones y comunicación; debe haber paneles de energía suficientes proporcionados para cada bastidor, se permite conexiones punto a punto entre equipos que no deben exceder a 15 m y debe ser entre bastidores adyacentes.

1.1.1.2.6. Área de distribución de zona (ZDA)

Es opcional y puede ir entre el HDA y EDA permitiendo la reconfiguración frecuente, es un área de distribución donde deben limitarse a servir un máximo de 288 conexiones de cable coaxial o par trenzado para evitar la congestión de cables en especial cuando van por el techo o suelo.

1.1.2. Subsistema Arquitectura

Debe permitir alojar equipos de gran tamaño, no debe estar ubicado en lugares que limiten su funcionalidad

1.1.2.1. Puerta de acceso y techo

La norma específica que las puertas deben ser de acceso desde el exterior, deslizante o extraíble de 1m de ancho y 2,13 de alto como mínimo, se debe contar con una puerta de seguridad que permita el acceso únicamente de personal autorizados; además el techo con una altura de 2,6 m desde el piso a cualquier obstáculo.

1.1.2.2. Iluminación

El lugar debe contar con 500 lux de iluminación en el plano horizontal y 200 lux en el vertical y con alimentación eléctrica independiente, para crear un espacio con una buena iluminación; esta cantidad de lux debe ser medida a 1 m de altura desde el piso en medio de los pasillos, para asegurar el nivel de iluminación adecuado que propone la norma ANSI/TIA-942.

1.1.2.3. Piso falso

El piso falso y las paredes deben de ser de color claro, bien selladas con propiedades antiestáticas, el suelo debe soportar la carga distribuida de equipos y cableado de 12 KPa y carga suspendida al piso de 2,4 KPa.

1.1.3. Subsistema Eléctrico

Unos de los subsistemas más importantes es el eléctrico porque permite la continuidad del negocio. La norma recomienda que este sistema se instale de forma subterránea y que cuente con lo siguiente: tablero eléctrico, suministro de alimentación ininterrumpida, generador, unidades de distribución de poder.

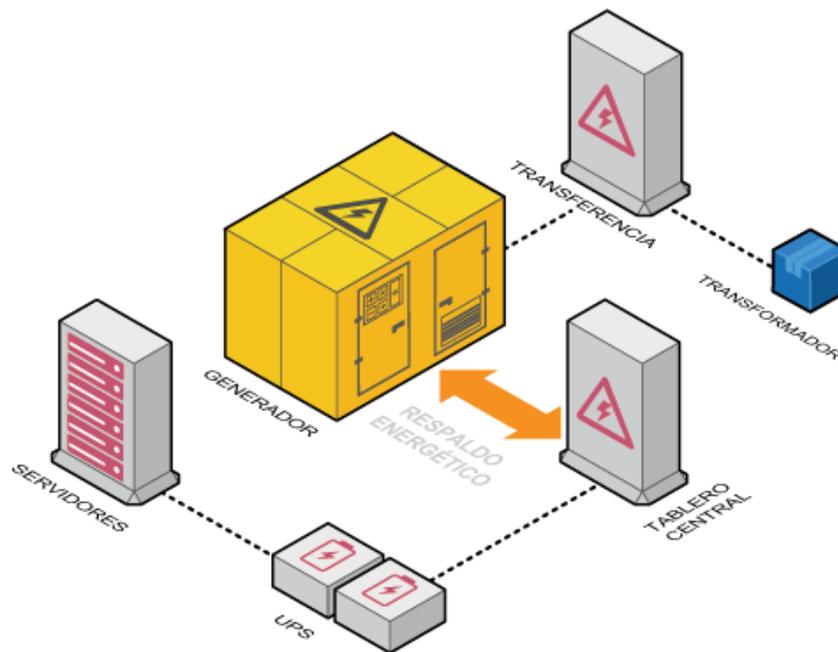


Figura 4. Sistema eléctrico.

Tomado de (Power Host, 2018).

1.1.4. Subsistema Mecánico

Este subsistema determina el espacio adecuado para que los equipos que se encuentran alojados en el Centro de Datos trabajen bajo condiciones ambientales óptimas.

1.1.4.1. Condiciones ambientales a tomar en cuenta

Según el “Sistema de Ventilación, Calefacción y Aire Acondicionado, por sus siglas en inglés HVAC, Heating, ventilation, and air conditioning” se necesita contar con un ambiente de climatización mediante circuitos de control de temperatura, a través de unidades de distribución de energía (PDU). El sistema requiere contar con los siguientes parámetros para su operación.

Tabla 1.

Parámetros de operación. Tomado de (TIA, 2014).

Descripción	Valor
Temperatura	20 a 25 °C
Humedad relativa	40 a 55%

1.1.4.2. Pasillo frío y caliente

Para que se tenga una mejor circulación del aire, la norma establece crear pasillos fríos y calientes colocando a los bastidores/gabinetes a una distancia frontal libre de 1 a 1,2 m y un espacio trasero libre de 0,6 a 1m. La Figura4 y la tabla 2 describen la distribución de pasillos fríos y calientes.

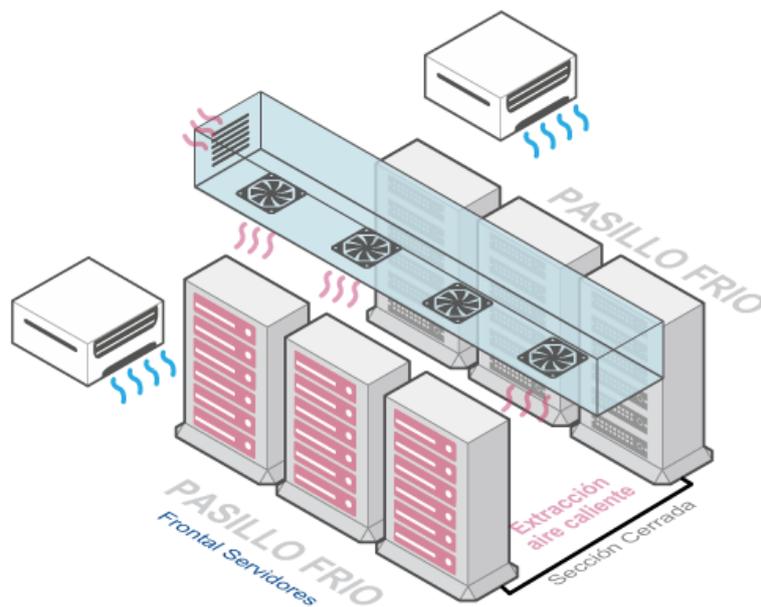


Figura 5. Distribución de pasillos frío y caliente.

Tomado de (Power Host, 2018).

Tabla 2.

Ubicación de pasillos fríos y calientes. Adaptado de (TIA, 2014).

Pasillo	Ubicación
Frío	<ul style="list-style-type: none"> - Colocar delante de los bastidores o gabinetes - Pisos de acceso con placas perforadas - En la parte de abajo de la distribución de energía eléctrica
Caliente	<ul style="list-style-type: none"> - Colocar detrás de bastidores o gabinetes. - Bajo el piso de acceso de coloca bandejas de cables de telecomunicaciones

1.2. Subsistemas en el estándar ANSI EIA/TIA 568-B

Determina los requisitos mínimos para la implementación de un cableado de telecomunicaciones común para edificios comerciales, considerando varios productos de diferentes proveedores. Los componentes que conforman un cableado estructurado se detallan en la Figura 6:

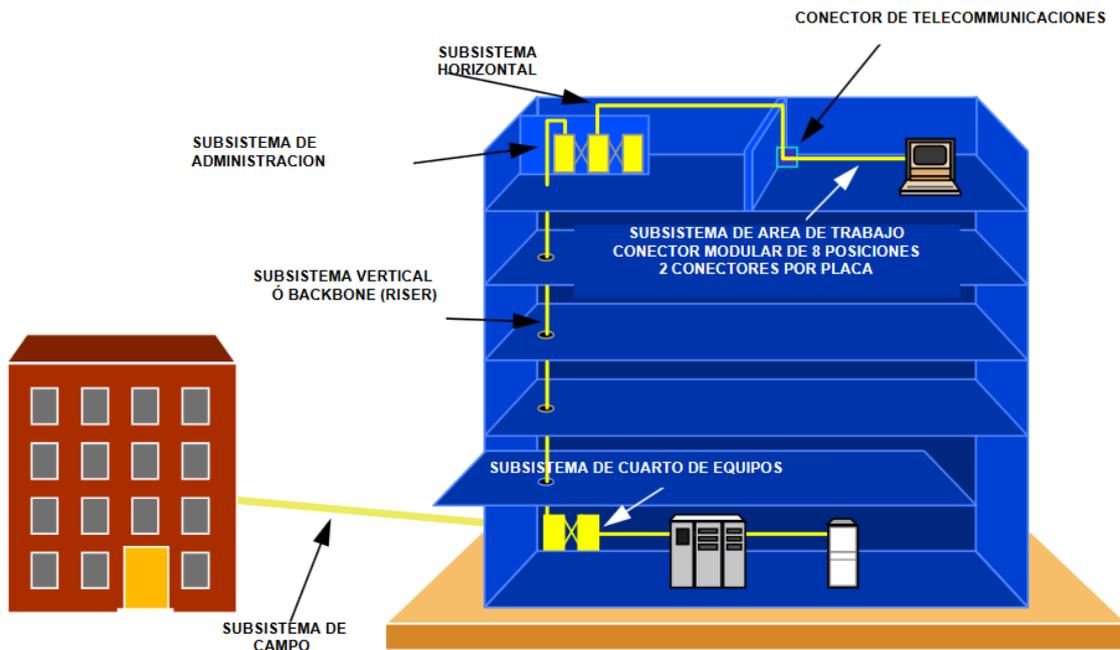


Figura 6. Componentes de un cableado estructurado.

Tomado de (Universidad Central de Venezuela, 2018).

Instalaciones de entrada. - Se refiere al punto físico desde donde se instala el cableado estructurado.

- Requiere contar con el equipamiento necesario (cables, equipos de conexión/protección) para conectar los elementos internos y externos con otros edificios; en su diseño se tiene que utilizar la norma TIA/EIA-569-A.
- Se utilizan las normas TIA/EIA-607 y TIA/EIA-758 para los elementos de unión y aterrizaje y para el cableado dorsal para un Campus.

Cuarto de equipo. -Es el sitio designado para albergar el equipo de telecomunicaciones, así como también para el equipo electrónico que administra la red local, tal como se muestra en la Figura 6.

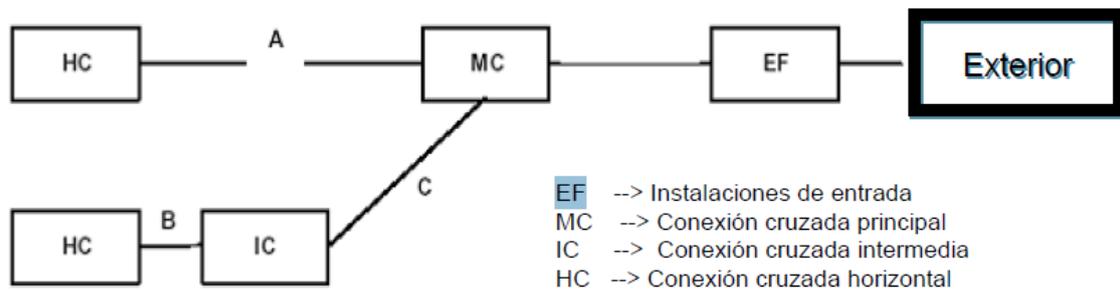


Figura 7. Jerarquía de cableado vertical, dorsal o backbone.

Adaptado de (Telecommunications Industry Association, 2001).

Cableado vertical, dorsal o backbone. -Permite la interconexión de los armarios o cuartos de telecomunicaciones con el cuarto de equipo, se requiere que el diseño soporte un período de 3 a 10 años para soportar el crecimiento.

Incluye:

- Conexiones cruzadas principales e intermedias y cordones de parcheo
- Cables verticales y conectores
 - o Cable par trenzado (UTP o ScTP; Se utiliza el Estándar ANSI/TIA/EIA-568-B.2)
 - o Cable de fibra óptica multimodo (62.5/125µm ó 50/125 µm) y monomodo (9/125 µm); Se utiliza el Estándar ANSI/TIA/EIA-568-B.3)

- Se utiliza la topología tipo estrella para la conexión, teniendo en cuenta lo siguiente:

Nomenclatura:

ER = Cuarto de equipo
 HC = Conexión cruzada horizontal
 IC = Conexión cruzada intermedia
 MC = Conexión cruzada principal
 TR = Armario o Cuarto de Telecomunicaciones
 WA = Área de trabajo

Nota:

- Sólo 1 conexión intermedia (IC) entre el MC y el HCER
- No más de 2 niveles de conexiones cruzadas

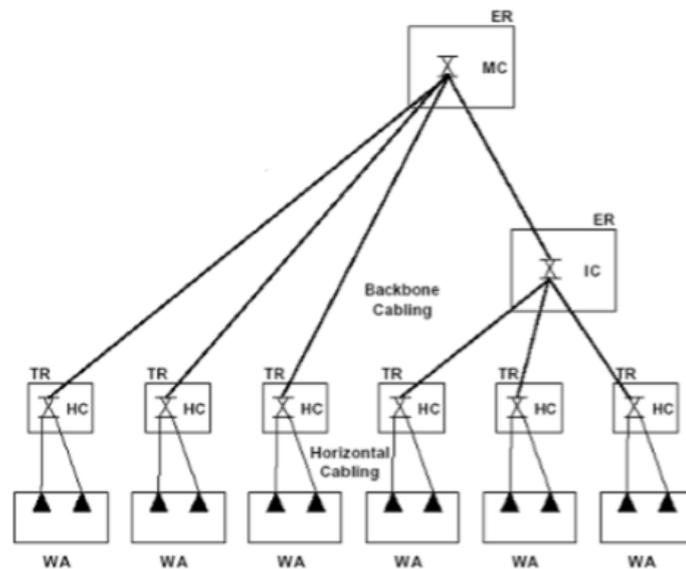


Figura 8. Interconexión de los armarios o cuartos de telecomunicaciones con el cuarto de equipo.

Adaptado de (Telecommunications Industry Association,) 2001.

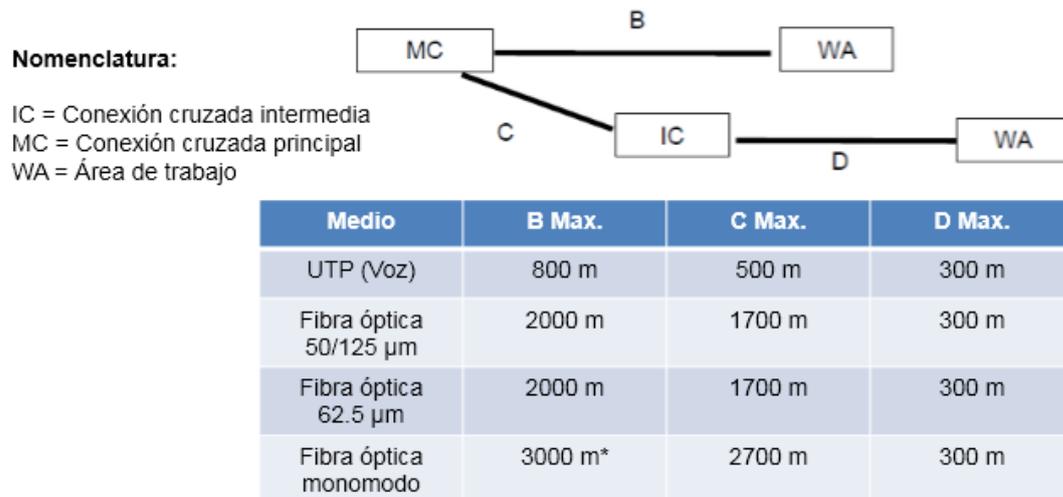


Figura 9. Distancias máximas permitidas.

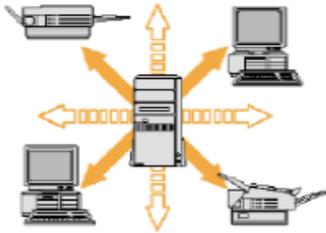
Adaptado de (Telecommunications Industry Association, 2001).

Armario o cuarto de telecomunicaciones. -Su función es la de establecer la interconexión con el cableado horizontal/vertical y el cuarto de telecomunicaciones.

Cableado horizontal. - Es el cableado que se extiende y realiza la interconexión entre el Cuarto o Armario de Telecomunicaciones y el Área de Trabajo.

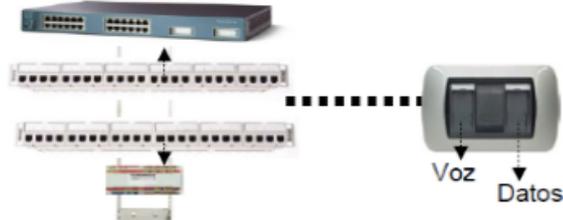
- En el diseño de requieren los servicios de: Voz, datos, vídeo, redes de área local (LAN), entre otros sistemas de señalización (seguridad, etc.); además se necesita estimar el crecimiento y reducir los mantenimientos.

La conexión debe ser topología en estrella



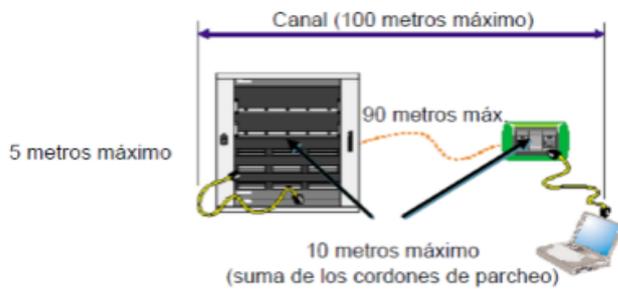
Cada conector de un Área de Trabajo debe estar conectado a su correspondiente en el Cuarto de Telecomunicaciones o en un panel de parcheo

Equipo activo para datos



Equipo activo para voz

Distancia máxima 90 metros (independientemente de si es cobre o fibra óptica)



Cable par trenzado (UTP o ScTP; Estándar ANSI/TIA/EIA-568-B.2)



Cable de fibra óptica multimodo (62.5/125µm ó 50/125 µm) y monomodo (9/125 µm); Estándar ANSI/TIA/EIA-568-B.3)



Figura 10. Cableado horizontal.

Adaptado de (Telecommunications Industry Association, 2001).

Área de trabajo. -Se refiere al espacio y al equipo de trabajo de un usuario.

Mínimo de dos conectores RJ45 por Área de Trabajo



Voz y datos



Voz y datos

Cada cable de "4 pares" debe terminar en un Jack modular RJ45 (de 8 pines) en cada Área de Trabajo.

La salida de telecomunicaciones y el cable deben de cumplir con los requerimientos de TIA/EIA 568-B.2 y TIA/EIA 568-B.3



Instalación junto a las tomas de corriente eléctricas necesarias (con canalizaciones separadas)



Cat 5E



Cat 5E



Cat 5E

- Utilizar cordones de parcheo de la misma categoría de los otros componentes
- Los cordones utilizan cable estándar (multifilar), más flexible para uso rudo.
- La distancia máxima de los cordones no puede superar los 5 metros
- No elaborarlos en campo

Configuraciones T568B y T568A

Pin en jack	T568B		T568A	
	Color del cable	Par	Color del cable	Par
1	Bianco - naranja	2	Bianco - verde	3
2	Naranja	2	Verde	3
3	Bianco - verde	3	Bianco - naranja	2
4	Azul	1	Azul	1
5	Bianco - azul	1	Bianco - azul	1
6	Verde	3	Naranja	2
7	Bianco - café	4	Bianco - café	4
8	café	4	café	4

Conectores y Acopladores de fibra óptica

Los conectores y acopladores permitidos son para fibra 62.5/125um y 50/125 um



Lado Armario



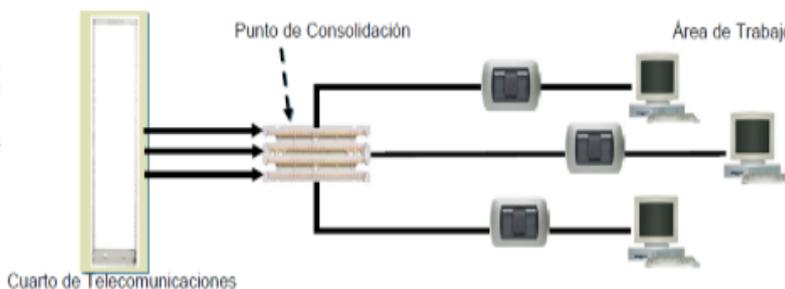
Lado usuario

Figura 11. Especificaciones a tomar encuentra en el área de trabajo.

Adaptado de (Telecommunications Industry Association, 2001).

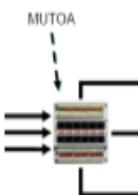
Punto de Consolidación

- Es un punto de conexión intermedio (opcional) entre el rack y las tomas en las placas, realizado a través de plug/jack o sistema 110
- Sólo se permite uno por corrida de cable
- Mínimo a 15 metros del Armario o Cuarto de Telecomunicaciones
- Conexiones cruzadas no se deben usar en puntos de consolidación

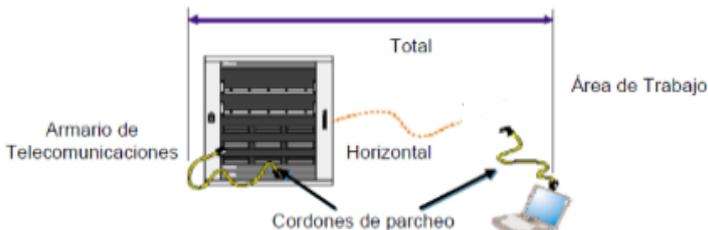


Distancias máximas (independientemente del tipo de cable o conexión)

MUTOA (Salidas multiusuario)



- Es la opción en donde los cordones de parcheo van directamente del MUTOA a la computadora
- Máximo 12 salidas de telecomunicaciones
- Es la solución ideal para cambios a futuro
- Los cordones de parcheo son ruteados directamente del MUTOA a cada computadora



Longitud cableado horizontal	Cordones de parcheo (Área de Trabajo y cuarto de Telecomunicaciones)	Total
90	10	100
85	14	99
80	18	98
75	22	97
70	27	97

Figura 12. Distancias máximas para áreas de trabajo.

Adaptado de (Telecommunications Industry Association, 2001).

La Asociación de Industrias Electrónicas (EIA, Electronic Industries Alliance) y la Asociación de la Industria de las Telecomunicaciones (TIA, Telecommunications Industry Association), establecen varios estándares para el cableado estructurado de voz y datos.

ANSI/TIA/EIA- 568 Revisión «B» se subdivide en tres documentos, esto es: ANSI/TIA/EIA-568-B.1-2001, ANSI/TIA/EIA-568-B.2-2001 y ANSI/TIA/EIA-568-B.3-2000.

1.2.1. ANSI EIA/TIA 568-B.1

Requerimientos Generales.

Esta norma, base fundamental de las demás normas de cableado y relacionadas, establece las especificaciones para el diseño e instalación de un sistema de cableado genérico, define los requisitos y recomendaciones en cuanto a su estructura, configuración, interfaces, instalación, parámetros de desempeño y verificación.

- Adenda1: Establece como requisitos mínimos de curvatura, bajo condiciones de no carga, 6mm (0.25 in) para cable multifilar (para patch cords) de UTP de 4 pares y 50mm (2 in) para cable multifilar de ScTP de 4 pares
- Adenda 2: Aborda las Especificaciones de Puesta y Unión a Tierra para Cableado Horizontal de Par Trenzado Balanceado Apantallado.
- Adenda 3: Precisa las Distancias Soportadas y Atenuación de Canal para Aplicaciones de Fibra Óptica, Clasificadas por Tipo de Fibra.
- Adenda 4: Hace explícito el Reconocimiento de la Categoría 6 y del Cableado de Fibra Óptica Multimodo 50/125 μ m Optimizado para Láser 850nm.

1.2.2. ANSI EIA/TIA 568-B.2

Componentes de cableado de par trenzado balanceado.

Esta norma especifica los requisitos mínimos para componentes reconocidos de par trenzado balanceado de 100, usados en cableados de telecomunicaciones en edificios y campus (cable, conectores, hardware de conexión, cordones y jumpers).

- Adenda1: Especifica los requisitos para pérdida de inserción y de retorno NEXT y ELFEXT, retardo de propagación y sesgo de retardos para cableado, cables y hardware de conexión de 100 categoría 6; pérdida de

retorno y NEXT para cordones modulares. Para el cable y cableado de NEXT y ELFEXT se han previsto exigencias que presuponen el peor de los casos en mediciones pares a par, así como en suma de potencias (poder sum). Proporciona asimismo recomendaciones de balance para cable y hardware de conexión categoría 6.

- Adenda 2: Revisa algunas cláusulas relacionadas en su mayoría con los parámetros NEXT y PSNEXT.
- Adenda 4: Establece requisitos de Confiabilidad de Conexión sin Soldadura para Hardware de Conexión de Cobre.

1.2.3. ANSI EIA/TIA 568-B.3

Componentes de Cableado de Fibra Óptica

Define los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica. Esta norma pormenoriza los requisitos mínimos para componentes de fibra óptica usados en cableados de telecomunicaciones en edificios y campus, tales como cable, conectores, hardware de conexión, cordones, jumpers y equipo de pruebas en campo.

- Adenda 1: Especificaciones Adicionales de Desempeño de Transmisión para Cables de Fibra Óptica de 50/125 μ m y los requisitos adicionales de componente y transmisión para cable de fibra óptica de 50/125 μ m capaz de soportar transmisiones seriales 10 Gb/s hasta 300m usando láser de 850nm.
- Adenda 3: Expone las consideraciones adicionales para determinación de pase o fallo para pérdida de inserción y pérdida de retorno. Pone de relieve que, debido a consideraciones de exactitud, los valores medidos de pérdida de inserción menores a 3dB se usarán sólo como valores informativos y no se tomarán en cuenta sus valores relacionados de pérdida de retorno.

1.3. Conceptos generales de redes

Las redes son un medio eficiente para compartir recursos informáticos entre fuentes de información y consumidores. Los grupos de redes que se van a utilizar dentro del diseño de la red de la Cooperativa se especifican a continuación.

1.3.1. Redes LAN

Son redes de ámbito local enmarcadas en el espacio físico del edificio o infraestructura arquitectónica al que brindan servicio.

Este tipo de red está definido por el IEEE dentro del proyecto 802, el cual a su vez contiene varios grupos de trabajo con estándares que definen diferentes tipos de tecnologías integradas e interoperables. Las redes IEEE 802 usan comunicaciones basadas en tramas en una variedad de medios para conectar diversos dispositivos digitales independientemente de la tecnología informática y el tipo de datos. Sin embargo, el alcance de las normas IEEE 802 no está limitado a las capas físicas (PHY) y capas de enlace de datos (DLL) (The Institute of Electrical and Electronics Engineers, Inc, 2014).

Se citan de manera general los estándares que se usarán en el presente proyecto.

La siguiente figura muestra los estándares y prácticas recomendadas actualmente por la IEEE.

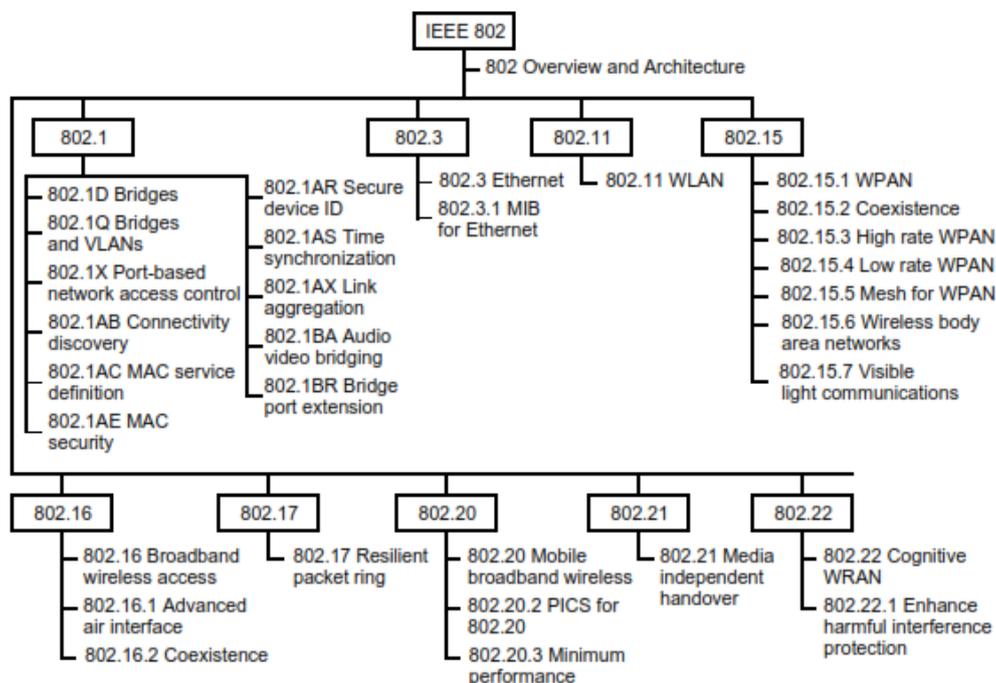


Figura 13. Familia actual de estándares y prácticas recomendadas.

Tomado de (The Institute of Electrical and Electronics Engineers, Inc, 2014).

1.3.1.1. 802.3 Redes Ethernet

Estándar de topología de red de área local, ampliamente utilizado, desarrollado por DEC, Intel y Xerox y que soporte velocidades de transmisión desde 10, 100, 1000 y 10000 Mbps.

1.3.1.2. IEEE 802.1Q

Protocolo de capa 2, VLAN protocolo de creación de redes o segmentos lógicos en un mismo medio físico. El estándar al que pertenece este protocolo especifica un tipo de etiquetado de tramas a nivel de capa 2 para identificar el número o ID de VLAN al que pertenece. La Tabla 15 nos muestra los segmentos lógicos y los respectivos números de VLAN a ser usados.

1.3.1.3. IEEE 802.1p

Protocolo de capa 2, QoS Calidad de Servicio, permite priorización de tráfico basado en colas donde se diferencian servicios de tal forma que las VLAN con más tráfico no comprometan el rendimiento de las demás. En el caso del proyecto en desarrollo se usará este protocolo para la priorización de tráfico dirigido a los servidores de bases de datos y del tráfico de telefonía IP.

1.3.1.4. IEEE 802.1w

Protocolo de capa 2, RSTP gestión de lazos con un tiempo de convergencia inferior al clásico protocolo STP generalmente usado (cuyo tiempo de convergencia es igual a 50 seg.), en lugar de los estados de STP de blocking, listening, learning, forwarding y disabled. Este protocolo será usado para completar el esquema redundante de los switches en la Cooperativa.

1.3.1.5. IEEE 802.11 WLAN

Estándar que define características físicas y lógicas de una red de área local de tipo inalámbrico. La capa física establece el tipo de codificación que se manejará a nivel del flujo de datos digitales como DSSS, Infrarrojo, FHSS, etc.

La capa de enlace esta a su vez compuesta de dos capas, una llamada MAC o de Control de Acceso al Medio y LLC o de Control de Enlace Lógico.

Existen en la actualidad varios estándares usados de manera general, tales como:

802.11a	5 GHz	54 Mbps
801.11g	2,4 GHz	54 Mbps
802.11n	2,4 GHz	300 Mbps
802.11ac	5+2,4 GHz	1,3 Gbps

1.3.2. Redes WAN

Infraestructura que define características físicas y lógicas de una red de área extendida, la cual puede interconectar redes LAN distribuidas regional o internacionalmente. Las redes WAN están típicamente administradas por Proveedores de Servicio (SP) o Proveedores de Servicio de Internet (ISP). (Introduction to Networks, 2016, p 23.)

- Las redes WAN interconectan redes LAN sobre amplias áreas geográficas como entre ciudades, provincias, países y continentes.
- Las redes WAN están administradas típicamente por múltiples Proveedores de Servicio.
- Las redes WAN típicamente proveen enlaces de velocidades inferiores en comparación a las redes LAN.

Internet es un ejemplo clásico de una red WAN. Para el caso del proyecto actual los enlaces WAN serán provistos por proveedores independientes mediante tecnología MPLS.

1.3.2.1. Multi Protocol Label Switching

MPLS es una tecnología de reenvío de paquetes que utiliza etiquetas en orden para tomar decisiones de reenvío de datos. Con MPLS, el análisis de encabezado de la capa 3 se hace apenas una vez (cuando el paquete ingresa el dominio MPLS). El examen de la escritura de la etiqueta conduce la expedición de paquete subsiguiente. MPLS proporciona estas aplicaciones beneficiosas:

- Virtual Private Networking (VPN)
- Ingeniería de tráfico (TE)
- Calidad del servicio (QoS)
- Cualquier transporte sobre MPLS (átomo)

Además, disminuye la expedición por encima en los routers del núcleo. Las tecnologías MPLS son aplicables a cualquier protocolo de capa de red. (Preguntas frecuentes sobre MPLS para principiantes, 2017)

1.1.1. Redes SAN

Modelo de comunicación dedicada que sirve para la interconexión y provisión de almacenamiento. En general es una red que se encuentra separada de la red LAN y cuyos elementos se parecen mucho a los de una red de área local:

- Interfaces de red o HBA (velocidades nominales 1, 2, 4, 8, 16 Gbps)
- Conexiones de fibra óptica con protocolo Fibre Channel (FC)
- Switches de SAN
- Routers de SAN
- Directores de SAN
- Gateways de SAN
- Equipos de almacenamiento
- Servidores
- Librerías de cinta

Este tipo de red provee características fundamentales como baja latencia, velocidad, disponibilidad, seguridad.

El gráfico siguiente es un ejemplo clásico de una red SAN:

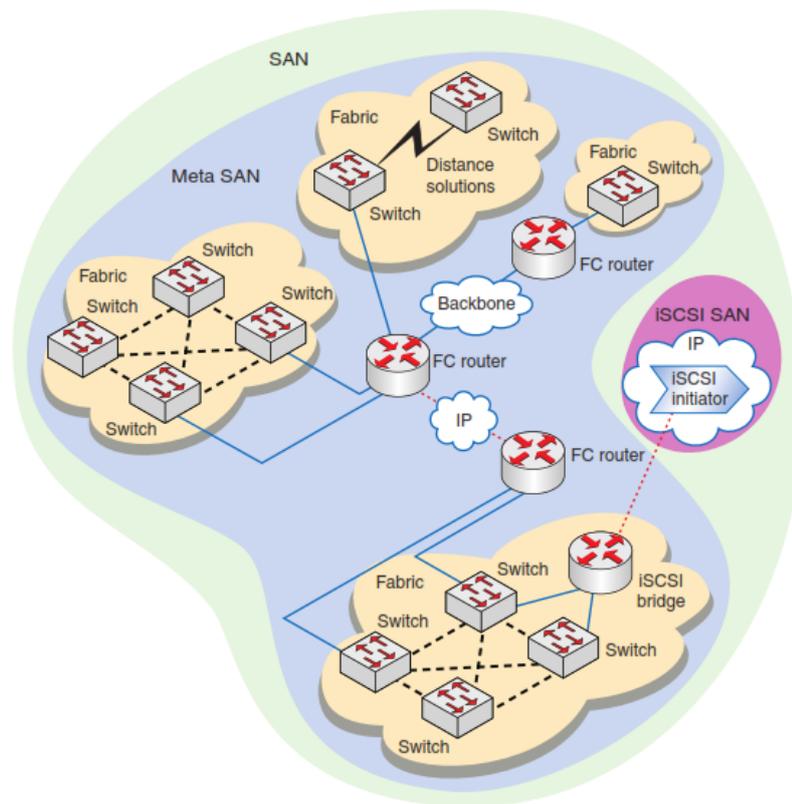


Figura 14. Ejemplo de una red SAN.

Tomado de (Lippitt & Smith, 2014).

2. CAPÍTULO II. LEVANTAMIENTO DE LA LINEA BASE

Se empieza por identificar los lineamientos que se establecen en la Resolución JB-2014-3066 de 2 de septiembre de 2014 por la Superintendencia de Bancos y Seguros del Ecuador (SBS), el cual tiene como eje la Continuidad del Negocio.

Posterior se realiza el análisis de la situación de la infraestructura tecnológica actual del Centro de Datos en la Matriz de Coop. Pablo Muñoz Vega tomando como referencia la norma ANSI/TIA-942 y ANSI/TIA-568 B 1, B2 y B3 para la evaluación en los diferentes subsistemas de Telecomunicaciones (Infraestructura de red), Arquitectura y los sistemas eléctrico y mecánico.

2.1. Resolución JB-2014-3066 SBS

La resolución citada busca que las instituciones financieras que se encuentran bajo la SBS, incorporen medidas de seguridad en los canales electrónicos, así como también disposiciones específicas relacionadas con las operaciones y continuidad del negocio. (SBS, 2014)

2.1.1. Continuidad del Negocio

El capítulo V “De la gestión del riesgo operativo” del libro I “Normas generales para la aplicación de la Ley General de Instituciones de Sistema Financiero”, establece un plan y una administración de la continuidad del negocio, en el caso del plan, se busca contar con procedimientos para cada institución y de esta forma asegurar la continuidad del negocio en el caso de producirse eventos inesperados; de igual manera para la administración se requiere de un proceso permanente que garantice la continuidad de las operaciones del negocio a través del mantenimiento del plan de continuidad (SBS, 2014).

2.1.3. Lineamientos generales

Según el “ARTICULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio”.

En ese sentido la Resolución JB-2014-3066 establece para las instituciones financieras tomar como referencia el estándar ISO 22301 en lo que concierne a la administración de la continuidad del negocio. A continuación, se describe lo que se requiere tomar en cuenta.

- **Definir:**

Objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto. Permite la administración de la continuidad.

- **Conformar:**

Un comité de continuidad del negocio. El comité está conformado por varios funcionarios de la institución, siendo parte de este, un funcionario de la unidad de riesgos, los responsables de:

La administración de la continuidad, del área de tecnología de la información, de talento humano, el auditor interno y el máximo representante de las áreas involucradas en el proceso de administración de la continuidad.

- **Determinar:**

Responsabilidades del comité del negocio. Según las responsabilidades asignadas a los integrantes del comité, se tiene que: monitorear la implementación del plan, proponer cambios, actualizaciones, revisar presupuestos, seguimiento a potenciales amenazas, coordinar acciones preventivas, seguimiento a las medidas adoptadas, entre otras.

- **Análisis de impacto y principales escenarios:**

Se requiere realizar análisis de impacto de los principales productos y servicios cuando se tenga interrupción de los procesos que los soportan. Sobre los escenarios de riesgos se utiliza una metodología para la evaluación de los mismos, tomando en cuenta las fallas que ocurran y la probabilidad de que se repitan.

- **Evaluación y selección de estrategias de continuidad del proceso**

Para la mantener la continuidad de los diferentes procesos se necesita conocer los procesos de soporte, los que están asociados a la infraestructura alterna, los de seguridad de la información y del personal, y sobre el equipamiento que se requiera para dichos procesos.

- **Pruebas del plan de continuidad**

Con el propósito de aplicar y comprobar la efectividad en la continuidad del negocio se requiere realizar pruebas que permitan verificar y realizar los ajustes correspondientes.

- **Difusión**

Está enfocado a establecer procedimientos para la socialización, entrenamiento y cumplimiento del plan.

- **Administración.**

Se pretende incorporar el proceso de administración integral del riesgo al proceso de continuidad del negocio, ambos buscan actualizarse y complementarse.

- **Plan de continuidad del negocio**

La Figura 15 y Tabla 3 describen los principales procedimientos del plan de continuidad del negocio a considerar:



Figura 15. Procedimientos del plan de continuidad del negocio.

Adaptado de (SBS, 2014).

Tabla 3.

Procedimientos mínimos. Adaptado de (SBS, 2014).

Definir	Definir	Definir
<ul style="list-style-type: none"> • Escenarios, procesos y alertas críticas • Roles y responsabilidades • Criterios de innovación y activación del plan • Acciones y procedimientos a ejecutarse antes, durante y después de ocurrido un incidente • Tiempos máximos de interrupción y de recuperación de cada proceso. 	<ul style="list-style-type: none"> • Acciones y procedimientos para trasladar las actividades de la institución • Información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación • Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia • Interacción con los medios de comunicación 	<ul style="list-style-type: none"> • Comunicación con los grupos de interés • Establecimiento de un centro de comando (considerar al menos un sitio principal y uno alternativo). • El centro principal de procesamiento ante eventos de desastres debe estar dentro de los parámetros establecidos en el plan y no debe estar expuesta a los mismos riesgos del sitio principal.

Resolución JB-2014-3066 SBS – Situación actual

2.1.4. Levantamiento Continuidad del Negocio

El giro del negocio está dado por la disponibilidad de los servicios del core financiero, que en este caso es el sistema Financiera mismo que está escrito en Visual C++ y que se afianza en una base de datos Oracle Standard Edition 11g

R2. Este sistema provee los servicios de los que dependen todos los departamentos de la Cooperativa.

La Cooperativa cuenta con un sitio alterno ubicado en la Agencia Ibarra, donde se tienen los siguientes elementos:

- 1 servidor HP Proliant DL380 G7 con Oracle Linux 6 y Base de Datos Oracle Standard Edition 11gR2.
- 1 equipo HP Deskpro G3 con Windows 7 como servidor de Aplicativo Financiamiento.
- Software DB-Visit para replicar la base de datos en sentido Activo-Pasivo y viceversa.

2.2. Levantamiento Centro de Datos (EIA / TIA 942)

Se realiza el levantamiento de la línea base, lo cual implica la identificación del estado actual de la infraestructura en el Centro de Datos de la Cooperativa.

2.2.1. Subsistema de Infraestructura

La Figura 17 describe la distribución de los racks de los equipos de servidores y de comunicaciones.

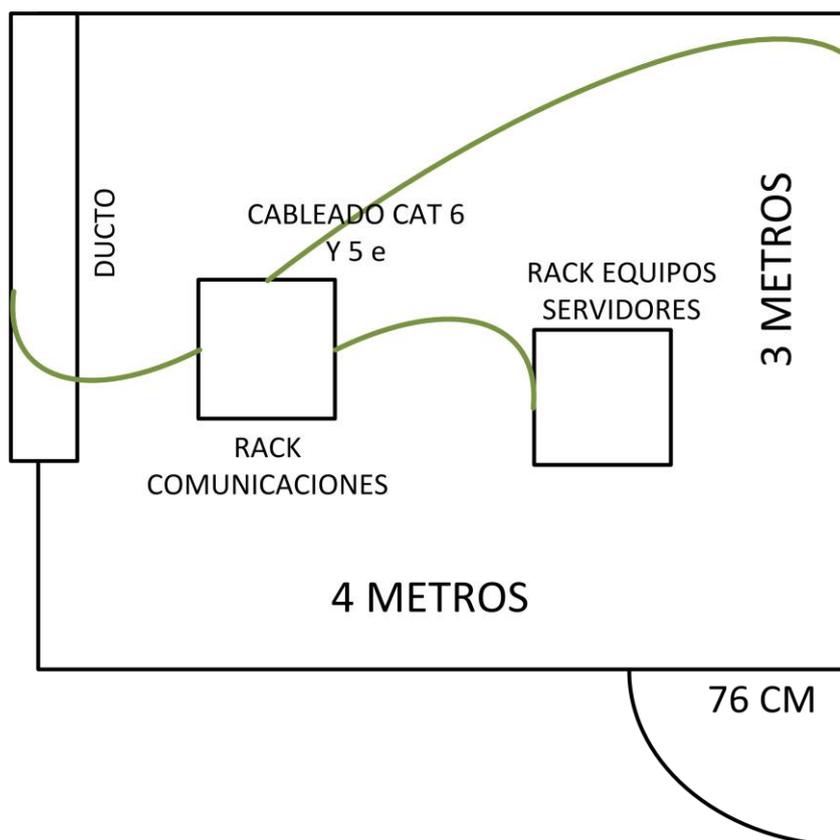


Figura 16. Subsistema de Infraestructura.

Así mismo la Figura 17 muestra la distribución de los cables de fibra de las operadoras y de troncales entre switches que ingresan por el ducto y se dirigen al rack de comunicaciones bajo el piso técnico, los cables de cobre CAT 6 y 5e pasan entre racks y se dispersan sin orden bajo el mismo.

2.2.1.1.1. Cableado estructurado Rack principal

Para los puntos de voz y datos la CPMV cuenta con un rack de 42 U a través del cableado horizontal.

Posee enlaces de fibra óptica, los mismos que conectan con las diferentes sucursales; además alberga los diferentes switches, routers, patch panels, regletas de energía eléctrica y la bandeja de fibra óptica.

A continuación, se presenta un resumen:

- Dos racks de tipo armario sin sus paneles.
- Rack de comunicaciones:
 - 3 patch panel 24 puertos CAT 6 DATOS y VOZ marca Leviton
 - 2 patch panel 24 puertos CAT 5e VOZ analógica Genéricos
 - Dispensador de fibra multimodo 3 pares hacia switches de distribución y acceso (1 piso, 2 piso, Consultorios Médicos)
 - 2 organizadores de cable horizontal 2"x2"
 - 2 regletas eléctricas PDU 8 tomas 110v
 - Aquí están montados los equipos routers de CNT, TELCONET, mismos que proveen enlaces de datos y de internet.
 - Están montados aquí los dos equipos Firewall GPA-300 y GPX 650
 - Está conectada aquí la central telefónica PC Asterisk.

En la Figura 18 se muestran los equipos que se encuentran en este rack.

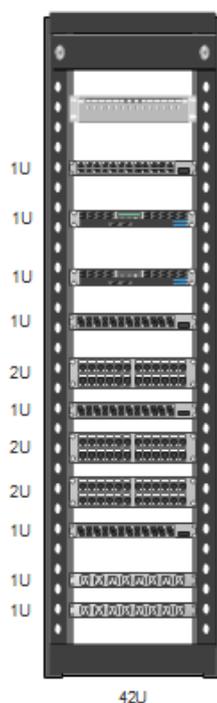


Figura 17. Rack principal.

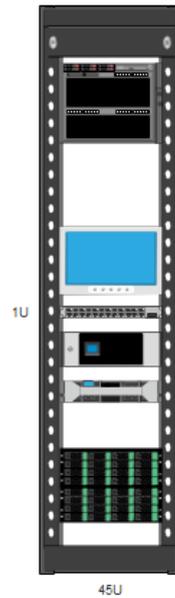


Figura 18. Rack de servidores.

2.2.2. Subsistema Arquitectura

El área donde se sitúa el Centro de Datos se encuentra en el tercer piso de la Agencia Matriz. Actualmente se cuenta con el espacio que se detalla:

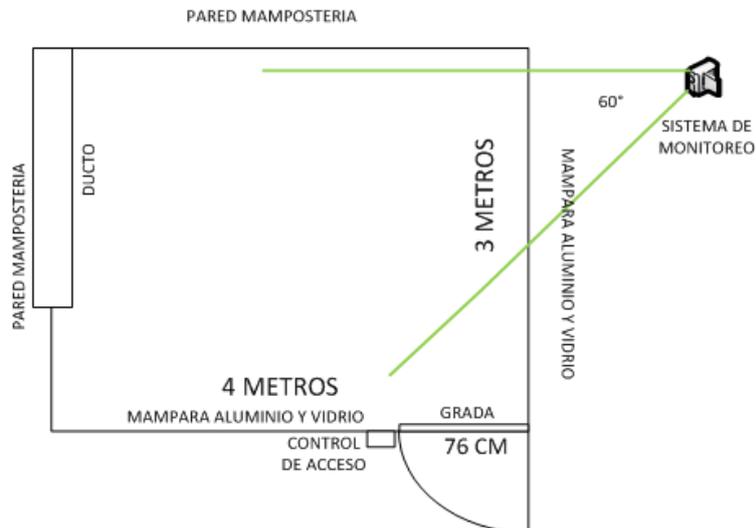


Figura 19. Subsistema Arquitectura.

2.2.2.1. Puertas de acceso

Se tiene acceso al lugar mediante una puerta una interna, de material de aluminio con vidrio protector de metal en su interior, cuyas dimensiones son: 2,55 m de alto por 76cm de ancho.

2.2.2.2. Techo

El techo es de losa enlucida, tiene una distancia al techo desde el contrapiso a la losa 2,25 m, y al techo desde el piso técnico 1,95m

2.2.2.3. Piso

Piso técnico baldosas 61x61 cm, área total 12m² Steel Access floor.

2.2.2.4. Seguridad física

Posee un sistema de control de acceso por tarjeta o tag y el monitoreo con única cámara IP.

Cámaras de seguridad

Tabla 4.

Cámaras de seguridad.

CANT	EQUIPO	MODELO	MARCA	DIRECCION IP
1	PC CÁMARAS SEGURIDAD	GRABACION	CLON	150.150.10.35
1	PC CÁMARAS SEGURIDAD	GRABACION	CLON	150.150.10.32
1	PC SISTEMAS DE ACCESO		CLON	150.150.10.10 3

2.2.2.5. Paredes

Construidos con material sólido de concreto armado, pintadas de color verde claro, no cuentan con propiedades antiestáticas; la pared es de 0,16 m de ancho. Además, se cuenta con una pared de yeso de dimensiones 1,35 m x 1,42 m, la misma que presenta aberturas en la parte que une con el techo y piso, facilitando la entrada de polvo al sitio y no permite que el cuarto de equipos se encuentre sellado. Las paredes internas del sitio son paredes de yeso, las mismas que no permiten el montaje de equipos pesados en el lugar. Postes de acero fijos y ducto hacia la terraza del 4° piso, cubierto de panel de aglomerado y con cubierta superior con domos de acrílico.

2.2.3. Subsistema Eléctrico

Es de vital importancia para el funcionamiento de los equipos que se encuentran alojados en la CPMV, a continuación, la Figura 20 presenta características generales.

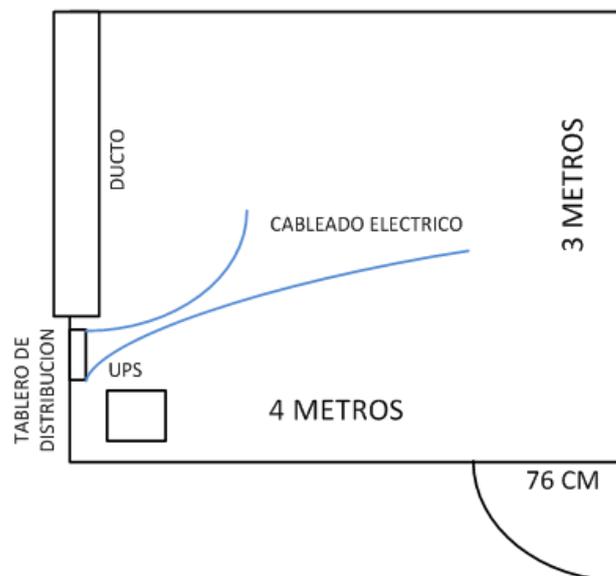


Figura 20. Subsistema eléctrico.

2.2.3.1. Proveedor de servicio eléctrico

La Cooperativa tiene un solo proveedor de servicio eléctrico EMELNORTE, con una negociación oficial con demanda y registro horario en media tensión; acometida trifásica de 220 V con neutro.

2.2.3.2. Tableros eléctricos

Posee tableros eléctricos de tipo residencial circuito único 110v, se enlaza del medidor de la empresa, el mismo que a su vez se conecta con el tablero de transferencia automática, permitiendo de esta manera el uso del generador en caso de existir ausencia del suministro eléctrico que provee la empresa eléctrica.

2.2.3.3. Tomacorrientes

En la infraestructura del actual cuarto de equipos se encuentran localizadas 6 tomacorrientes instalados en pared los mismos que sirven para la conexión de los diferentes equipos que se encuentran en el área, los mismos que se encuentran distribuidos como se muestran en la tabla:

Tabla5.

Medición de corriente y voltaje del cuarto de equipos.

N° Tomacorriente	Tipo de tomacorriente	Voltaje (V)	Corriente (A)
1	Doble	119,8V - 119,9 V	18,82 A - 18,84 A
2	Doble	119,6V - 119,8 V	19,85 A - 19,89 A
3	Doble	127,5V - 127,9V	19,99 A –20 A

De lo cual se obtiene que todos los tomacorrientes instalados en el sitio se encuentra funcionando, pero se puede apreciar la fluctuaciones de tensión que pueden afectar a los dispositivos conectados a la red, es por ello que no deben superar una fluctuación de $\pm 10\%$ del valor nominal (MDP, s.f), que es de 120

V, es decir que la variación permitida está entre los 108 V a 132 V, y los valores medidos se encuentran dentro del rango aceptable de fluctuaciones, por lo que se considera que la alimentación eléctrica es correcta y no afectar el funcionamiento de los equipos eléctricos conectados a la misma.

2.2.3.4. Luminarias

Posee lámparas de aluminio y vidrio 4mm, vidrio estándar, localizadas en los extremos del cuarto a 0,65m de distancia de la pared.

2.2.3.5. Generador eléctrico

Posee un generador eléctrico, grupo electrógeno 15 KVA para toda la Matriz, respuesta de 4 minutos, tanque de reserva de diesel para 4 horas, ubicado en el primer piso.

2.2.3.6. UPS

Cuenta con un UPS monofásico 6 KVA TRIP-LITE, Carga 80% respaldo 10 minutos. El UPS se acciona de inmediato al momento que se produce un corte del servicio de energía eléctrica contratado, hasta que el generador realice su función, a continuación, se indican algunas características del mismo.

- Potencia: funciona a una potencia de 6 kVA.
- Voltaje de entrada: 220V a 60Hz.
- Factor de potencia: > 0,89.

2.2.3.7. Protección eléctrica

Se tiene algunos mecanismos que permiten mantener el lugar protegido contra algún acontecimiento eléctrico, que pueda causar daños tanto a personas como equipos, como por ejemplo el UPS sirve como dispositivo de protección contra sobre tensiones; para la protección contra sobre corriente se usa los breakers CC, además se cuenta con cajas de protección vía breakers para protección contra incendios ocasionados por la parte eléctrica.

2.2.4. Subsistema Mecánico

Cuenta con un aire acondicionado de confort de 36 KBTU que permite que los equipos no se sobrecalienten mientras operan, proporcionando la climatización del área.

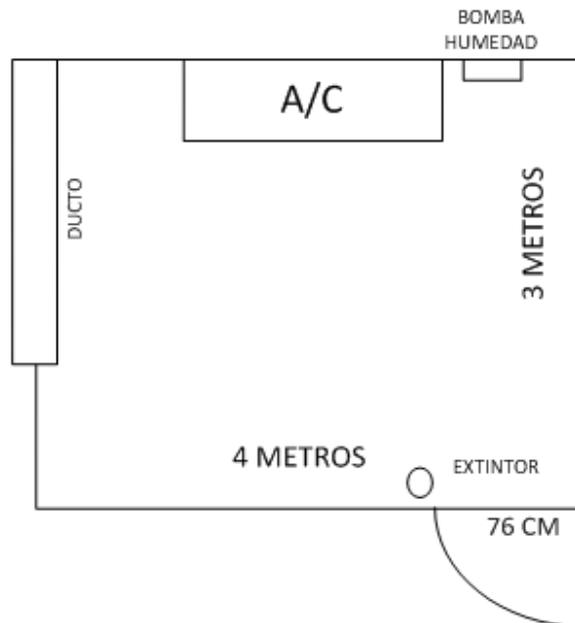


Figura 21. Subsistema Mecánico.

2.2.4.1. Aire acondicionado

El aire acondicionado protege a los equipos del calor excesivo brindando una refrigeración de 36000 Btu/ hora, funciona de manera automática gracias a sus controles fáciles de usar; actualmente está funcionando a una temperatura entre 17 y 19 °C, el mismo que tiene la función de proporcionar enfriamiento toda el área señalada. A continuación, se presentan sus características:

- Voltaje de entrada: voltaje monofásico de 208/203 V.
- Consumo total de energía: 2 Kw
- Dimensiones: 1,50 x 1,02 x 0,32 (ancho x profundidad x altura)
- Condiciones de operación: entre 65° - 95° F.

2.2.4.2. Seguridad ambiental

En cuanto se refiere a seguridad ambiental, existen pocos mecanismos instalados que permitan manejar situaciones como incendios de la manera más rápida, a continuación, se presentan algunos mecanismos con los que cuenta el área:

Extintor de incendios: se cuenta con un extintor de agente polvo químico, PSE-1604 2,3 Kg colocado en frente de la puerta exterior del área de recursos informáticos; además en ocasiones se encuentra en mantenimiento y no es posible su uso.

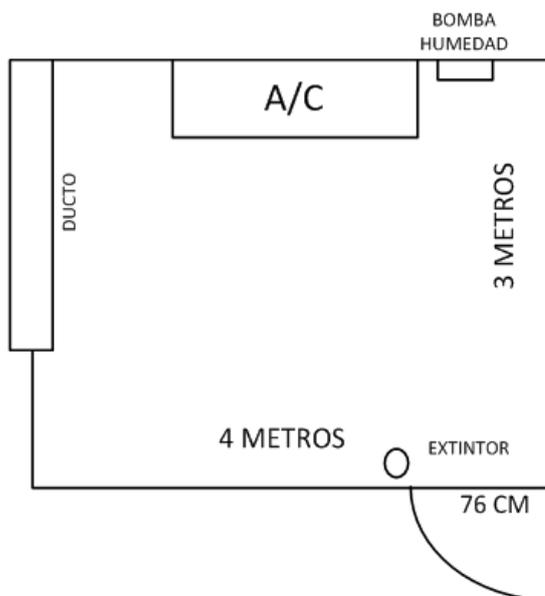


Figura 22. Distribución actual de los equipos de seguridad ambiental.

2.2.5. Resumen de problemas detectados en el Centro de Datos por cada uno de los Subsistemas.

Del análisis realizado se detalla en la Tabla 6 los problemas encontrados en los diferentes subsistemas.

Tabla 6.

Problemas detectados en los subsistemas.

Nombre del Subsistema	Elemento analizado	Norma ANSI EIA /TIA-942		Observaciones
		Cumple	No cumple	
Infraestructura	CANALIZACION No se tienen un enrutamiento del cable por pasillo caliente		NO	Los cables pasan bajo el piso falso sin orden.
	CABLE Cableado no certificado		NO	Cat 6 y 5e
Nombre del Subsistema	Elemento analizado	Norma ANSI EIA /TIA-942		Observaciones
		Cumple	No cumple	
Arquitectura	PAREDES Paredes de vidrio inseguras, no son de seguridad		NO	Vidrio no es material indicado.

	DIMENSIONES	SI		
	Distancia piso falso techo			1,95 m
	Puerta de acceso insegura		NO	Aluminio y vidrio
	Rampa de acceso No existe		NO	Grada
	Área de datacenter junto a posible zona de humedad por lluvia.		NO	Junto a ducto de cables hacia terraza.
Nombre del Subsistema	Elemento analizado	Norma ANSI EIA /TIA-942		Observaciones
		Cumple	No cumple	
Eléctrico	Sistema eléctrico monofásico	SI		Estándar previo
	No existe distribución en tableros basado en estándar		NO	Tableros de tipo doméstico.
	Cableado eléctrico no enrutado por pasillo frio		NO	Los cables pasan bajo el piso falso sin orden.
	Capacidad del UPS insuficiente,		NO	Apenas 6 KVA, 85%
	UPS monofásico	SI		Estándar previo
	Único punto de falla, un solo UPS		NO	
	Único punto de falla un		NO	

	solo grupo electrógeno generador compartido por toda la Coop.			
	Sistema de iluminación insuficiente.		NO	Luminarias domésticas.
	Sistema de tierra insuficiente, compartido por toda la agencia Matriz		NO	Valores superiores a 0,01 v
	No existe un sistema de malla de alta frecuencia		NO	
	No se tiene un dispositivo TVSS		NO	
	Un solo circuito eléctrico para los PDU en los racks.		NO	Desde el UPS
	No se tiene un dispositivo pararrayos.		NO	
Nombre del Subsistema	Elemento analizado	Norma ANSI EIA /TIA-942		Observaciones
		Cumple	No cumple	
Mecánico	Aire acondicionado no es de precisión, no controla humedad, equipos con signos de óxido en los chasis.		NO	33 KBTU solo extrae humedad condensada, sin evaporador.
	No se tiene un sistema de extinción de incendios		NO	Se tiene un extintor man.
	No existen sensores de humo, etc.		NO	

2.3. Levantamiento subsistema cableado pisos (EIA / TIA 568b)

Como parte del levantamiento de la línea base se realiza la identificación del estado actual de la infraestructura del cableado estructurado en la agencia Matriz Cooperativa.

La siguiente imagen ilustra la distribución de los subsistemas por pisos de acuerdo al estándar EIA / TIA 568B

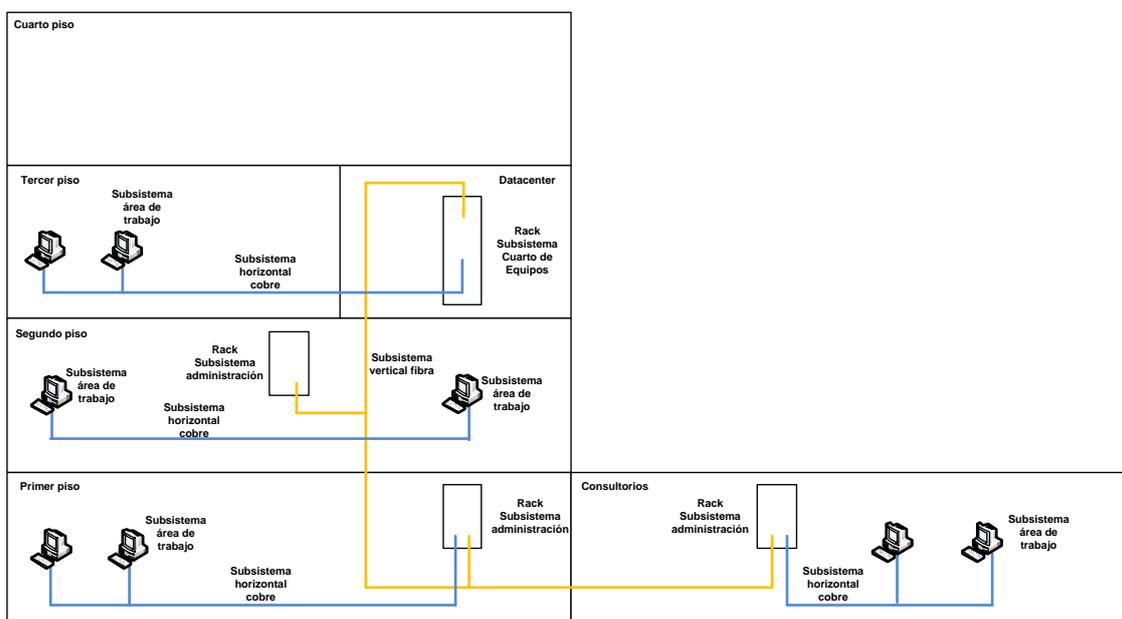


Figura 23. Distribución actual de los subsistemas de cableado estructurado.

2.3.1. Subsistema Área de Trabajo

La Cooperativa Pablo Muñoz Vega cuenta con varios departamentos y se encuentran distribuidas de acuerdo a lo descrito en la Tabla 7.

Tabla 7.

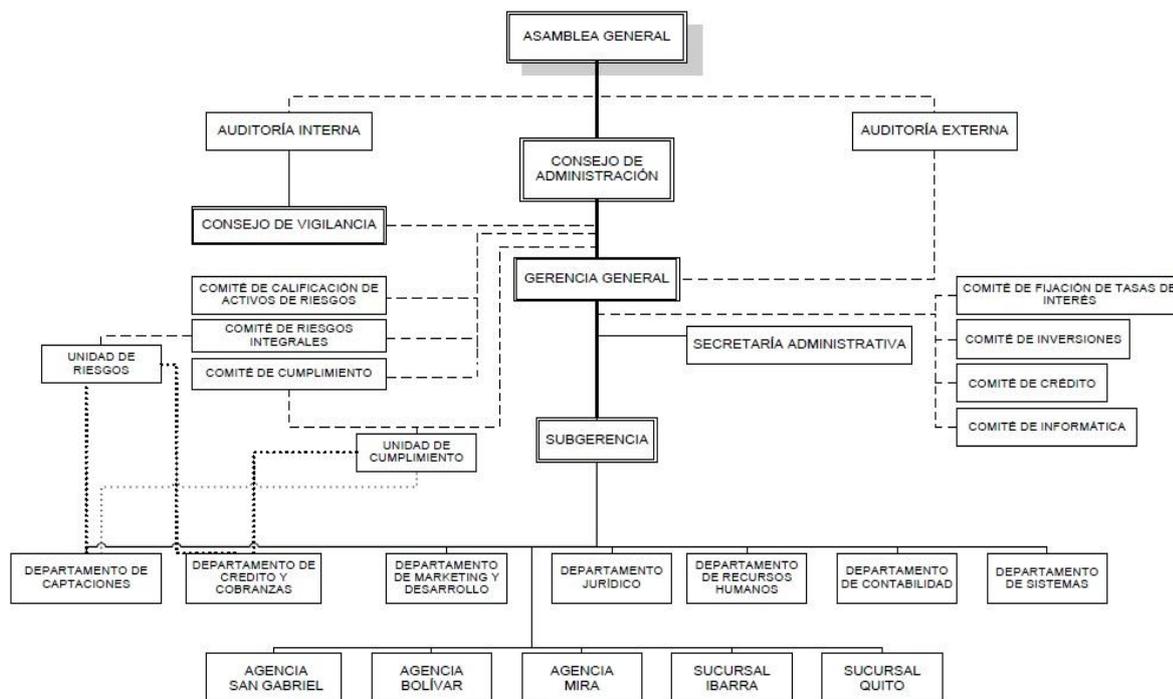
Áreas de trabajo de la Coop. Pablo Muñoz Vega.

Piso	Matriz	Datos	Voz
3 piso	Datacenter reflejos	24	

	racks		
3 piso	Auditoría	5	4
	Contabilidad	4	3
	Subgerencia	2	1
	Sistemas	8	7
	Sala de reuniones	1	1
	Oficial de seguridades	2	1
	Riesgos	2	1
	Cámaras	7	
2 piso	Asesores de crédito	6	5
	Cartera	4	3
	Cobranzas	4	4
	RRHH	2	1
	Tesorería	2	1
	Depto. legal	3	2
	Gerencia	2	1
	Secretaría	2	1
	Marketing	2	1
	Cámaras	7	
1 piso	Atención al cliente	4	3
	Cajero automático	1	
	Cajas	5	
	Supervisor de cajas	3	1
	Cámaras	8	
	Consultorios	4	3
	Guardianía	1	1
		115	45

Los requerimientos de comunicaciones se dan de acuerdo a los departamentos que componen la Cooperativa y que se detallan en el gráfico siguiente.

Figura 24. Organigrama de la Cooperativa Pablo Muñoz Vega.



Posee cajas modulares con face plates dobles dependiendo del caso con Jacks CAT 6 y CAT 5e para los servicios de red y telefonía respectivamente.

2.3.2. Subsistema Horizontal

Posee cable UTP de categorías 6 y 5e para la distribución del cableado horizontal para los diferentes departamentos y áreas de negocios, para datos y telefonía respectivamente. El cableado es enrutado por canaletas plásticas con división, anti flama y con accesorios.

2.3.3. Subsistema Vertical o Backbone Ascendente

Está basado en fibra óptica OM4 multimodo que se conecta entre los subsistemas de administración (IDF) hacia el subsistema del cuarto de equipos (MDF) tal como se muestra en la figura 26.

El subsistema está organizado con dispersores, patch panels y organizadores de cable en cada rack, sin embargo, solo existe un par de fibra desde el MDF a cada IDF.

2.3.4. Subsistemas de Administración

Los subsistemas están organizados en racks (IDF) de 24 UR donde se hallan Patch Panels modulares con Jacks CAT6 y CAT5e para los servicios de datos y telefonía respectivamente, se tienen los respectivos patch cords para la conexión hacia el Switch y organizadores de cable. Se tiene un subsistema en el primer piso en el área de Cajas, en el segundo piso en el área de Tesorería y en área de Consultorios Médicos. Se tienen también una caja dispersora de fibra Multimodo.

2.3.5. Subsistema de Sala de Equipos

Este subsistema está incluido en el punto 2.2.1.1. Racks, y dado que ya se abordó dentro de dicho apartado no se mencionará nuevamente.

2.3.6. Resumen de problemas detectados en cada uno de los subsistemas

Del análisis realizado se detalla en la Tabla 8 los problemas encontrados en los diferentes subsistemas.

Tabla 8.

Problemas detectados en los subsistemas.

Nombre del Subsistema	Elemento analizado	Norma ANSI EIA / TIA - 568b		Observaciones
		Cumple	No cumple	
Área de Trabajo	Cajas modulares	SI		Plásticas anti flama
	Face plates	SI		Dos posiciones con tapa ciega para determinados casos.
	Jacks CAT 6 y 5e	SI		Modulares CAT 6 y CAT5e
Horizontal	Cable UTP CAT 6	SI		Cable certificado
	Cable UTP CAT 5e	SI		Cable certificado
	Cable enrutado por canaleta plástica con división	SI		Anti flama con accesorios
Vertical o Backbone	Fibra Multimodo		NO	Par de fibra MM OM4 50/125 faltan más pares para redundancia
	Fibra enrutada por ductos	SI		
	Fibra enrutada por canaleta plástica con división	SI		Anti flama con accesorios
Administración (IDF)	Racks modulares	SI		24 UR
	Patch panels cobre CAT 6 y CAT 5e	SI		Modulares
	Jacks CAT 6 y 5e	SI		Modulares CAT 6 y CAT5e
	Dispensor Fibra MM	SI		

2.4. Levantamiento infraestructura tecnológica de red

2.4.1. Diagnóstico de recursos de red

La Tabla 9 describe los recursos de TI con los que cuenta la Cooperativa Pablo Muñoz Vega. En la primera captura de la aplicación de la herramienta IPScanner arrojó una revisión a nivel de capa2 y 3 del modelo OSI dentro de la red y emite un resultado con los dispositivos activos.

Tabla 9.

Recursos de TI. Resultados de ejecución de IPScanner.

Nombre	IP	Http	Carpetas compartidas	Fabricante
150.150.10.1	150.150.10.1			Routerboard.com
150.150.10.2	150.150.10.2	Cisco IOS http config		Cisco Systems, Inc
150.150.10.3	150.150.10.3	Cisco IOS http config		Cisco Systems, Inc
150.150.10.4	150.150.10.4	Cisco IOS http config		Cisco Systems, Inc
150.150.10.5	150.150.10.5			Gateprotect
150.150.10.7	150.150.10.7	Cisco IOS http config		Cisco Systems, Inc
150.150.10.13	150.150.10.13			Gateprotect
150.150.10.14	150.150.10.14			Super Micro Computer, Inc.
Actualizaciones	150.150.10.17	Microsoft IIS httpd 7.5		Hewlett Packard
srv-app-trx	150.150.10.18	IIS7 (Microsoft IIS httpd 7.5)		VMware, Inc.
150.150.10.20	150.150.10.20			VMware, Inc.
150.150.10.21	150.150.10.21	" + ID_EESX_Welcome + " (VMware ESX 4.0 Server httpd)		IBM Corp
150.150.10.22	150.150.10.22	" + ID_EESX_Welcome + " (VMware ESX 4.0 Server httpd)		Hewlett Packard
150.150.10.23	150.150.10.23			Hewlett Packard
150.150.10.24	150.150.10.24			VMware, Inc.

cpmv	150.150.10.25			Oracle Corporation
WTFSSERVER	150.150.10.26	Microsoft IIS httpd 7.5	Users	VMware, Inc.
150.150.10.29	150.150.10.29	" + ID_EESX_Welcome + " (VMware ESX 4.0 Server httpd)		IBM Corp
FWmonitor-PC	150.150.10.30		shared	VMware, Inc.
150.150.10.31	150.150.10.31	nginx 1.2.2		VMware, Inc.
Pc_camaras	150.150.10.32		Users, VIDEOS J	Hewlett Packard
WIN- E79RMKQQF00	150.150.10.33			Hewlett Packard
wswitchtrx	150.150.10.34	IIS7 (Microsoft IIS httpd 7.5)	Users	VMware, Inc.
camaras2-PC	150.150.10.35			Hewlett Packard
SVRDIRECTACT	150.150.10.38			VMware, Inc.
150.150.10.39	150.150.10.39			Hangzhou Hikvision
svrad	150.150.10.40			VMware, Inc.
apps-fbs	150.150.10.41	IIS7 (Microsoft IIS httpd 7.5)	ESTRUCTUR AS, FE, Herramientas Financial, Publicaciones Financial	VMware, Inc.
150.150.10.43	150.150.10.43	Apache2 Ubuntu Default Page: It works (Apache httpd 2.4.7)		VMware, Inc.
150.150.10.44	150.150.10.44			VMware, Inc.
av01	150.150.10.45			VMware, Inc.
cajeros-conecta	150.150.10.46	EAP 6 (Apache Tomcat/Coyote JSP engine 1.1)		VMware, Inc.
SVRGREENSOF T1	150.150.10.47	This site is running TeamViewer. (TeamViewer httpd)		VMware, Inc.
svrgreensoft2	150.150.10.48	IIS7 (Microsoft IIS httpd 7.5)	ORION	VMware, Inc.
svrbbdgreensoft	150.150.10.49			VMware, Inc.

svrappgreensoft	150.150.10.50	IIS7 (Microsoft IIS httpd 7.5)		VMware, Inc.
svrftp	150.150.10.51	IIS7 (Microsoft IIS httpd 7.5)	ESCANEO 3 PISO	VMware, Inc.
150.150.10.52	150.150.10.52			VMware, Inc.
DesarrolloSifiz	150.150.10.74	IIS7 (Microsoft IIS httpd 7.5)		VMware, Inc.
toshibacpmv	150.150.10.78			PEGATRON CORPORATION
portatilhp	150.150.10.79			QUANTA COMPUTER INC.
adminswf	150.150.10.82	IIS7 (Microsoft IIS httpd 7.5)		Hewlett Packard
AdminDesarrollo	150.150.10.84	IIS7 (Microsoft IIS httpd 7.5)		Hewlett Packard
150.150.10.103	150.150.10.103	lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)		Paradox Security Systems Ltd
APPS-CPMV	150.150.10.110	En construcción (Microsoft IIS httpd 6.0)		VMware, Inc.
DIEBOLD-CPMV606	150.150.10.111			DFI Inc.
150.150.10.112	150.150.10.112			Private
150.150.10.113	150.150.10.113			IBM Corp
150.150.10.115	150.150.10.115			IBM Corp
150.150.10.116	150.150.10.116			IBM Corp
SEGUTUL1	150.150.10.140			Hewlett Packard
programador4	150.150.10.141	IIS7 (Microsoft IIS httpd 7.5)		Hewlett Packard
Programador3	150.150.10.146	IIS7 (Microsoft IIS httpd 7.5)		Hewlett Packard
OPERADORGf	150.150.10.147			Hewlett Packard
NPIA17ED6	150.150.10.153	HP LaserJet P2055dn 150.150.10.153 (Virata- EmWeb 6.2.1)		Hewlett Packard
NPI33AEAF	150.150.10.155			Hewlett Packard
NPIC7829B	150.150.10.172	HP LaserJet Pro M201dw		Hewlett Packard

		150.150.10.172 (gSOAP 2.7)		
150.150.10.182	150.150.10.182	Bienvenido al Asistente de servicio (Apache Tomcat/Coyote JSP engine 1.1)		IBM Corp
windows7prueba-	150.150.10.202			VMware, Inc.
150.150.10.203	150.150.10.203			VMware, Inc.
150.150.10.223	150.150.10.223			Hewlett Packard
150.150.10.240	150.150.10.240	HiperPBX - P�gina de Ingreso (Apache httpd 2.2.3)		Intel Corporate
150.150.10.246	150.150.10.246	Endpoint Protector - Reporting and Administration Tool (nginx)		VMware, Inc.
150.150.10.249	150.150.10.249	Coop "Pablo Mu�oz Vega" (Apache httpd 2.4.7)		VMware, Inc.
150.150.10.250	150.150.10.250			Cisco Systems, Inc
150.150.10.251	150.150.10.251			
150.150.10.252	150.150.10.252			VMware, Inc.
150.150.10.254	150.150.10.254			Hewlett Packard

2.4.2. Equipos en los racks

La Tabla 10 describe la ubicación de los diferentes racks y switches.

Tabla 10.

Distribución de Rack, Switches.

DISTRIBUCION DE EQUIPOS POR UBICACIÓN					
SUBSISTEMA INFRAESTRUCTURA COMUNICACIONES					
UBICACIÓN RACK DATACENTER					
CANT	EQUIPO	MODELO	MARCA	DIRECCION IP	SERVICIO
1	SWITCH	WSC 4506E	CISCO	150.150.10.7	SW CORE
1	ROUTER	CCR1036	MIKROTIK	150.150.10.1	ENRUTAMIENT O ENTRE AGENCIAS
1	FIREWALL	GPA500	GATEPROTECT	150.150.10,5	FIREWALL BANCA EN LINEA
1	FIREWALL	GPX650	GATEPROTECT	150.150.10.13	FIREWALL GENERAL
1	ROUTER TELCONET	890	CISCO	150.150.10.251	ENLACES DE DATOS AGENCIAS
1	ROUTER CNT	890	CISCO	150.150.10.250	ENLACES DE DATOS AGENCIAS
1	CPU ASTERISK LINUX	CENTRAL TELEF	CLON	150.150.10.240	TELEFONIA IP
SUBSISTEMA INFRAESTRUCTURA COMUNICACIONES					
UBICACIÓN RACK PRIMER PISO					
1	SWITCH	WS-C3560	CISCO	150.150.10.3	
SUBSISTEMA INFRAESTRUCTURA COMUNICACIONES					

UBICACIÓN RACK SEGUNDO PISO					
1	SWITCH	WS-C2960	CISCO	150.150.10.4	
SUBSISTEMA INFRAESTRUCTURA COMUNICACIONES					
UBICACIÓN RACK CONSULTORIOS					
1	SWITCH	WS-C2960	CISCO	150.150.10.2	

El segundo rack alberga lo siguiente:

- 2 servidor IBM X38650 X5
- 2 servidor HP DL380 G7
- 1 storage IBM Storwize v3700
- Monitor, teclado y mouse para KVM
- 2 PC cámaras de seguridad
- 1 PC sistema de acceso de la agencia Matriz

Tabla 11.

Distribución de Rack, Servidores.

CANT	EQUIPO	MODELO	MARCA	DIRECCION IP	SERVICIO
1	SERVIDOR	PROLIANT DL380 G7	HP	150.150.10.23	BASE DE DATOS ORACLE 11GR2
1	SERVIDOR	PROLIANT DL380 G7	HP	150.150.10.22	VMWARE, AMBIENTE DE DESARROLLO Y PRUEBAS
1	STORAGE	STORWIZE V3700	IBM	150.150.10.116	ALMACENAMIENTO PARA LA BASE DE DATOS ORACLE 11GR2
1	SERVIDOR	X3850 X5	IBM	150.150.10.21	VMWARE, APLICATIVO FINANCIAL, CAJEROS, BANCA EN LINEA, PAGINA

					WEB Y CORREO ELECTRÓNICO, NTP SERVER.
1	SERVIDOR	X3850 X5	IBM	150.150.10.29	VMWARE: SERVIDOR RELAY CORREO, FABRICA DE CREDITO, MONITOREO FIREWALLS, DLP, NAS RESPALDOS.

Los servidores y los servicios con los que cuenta el rack se detallan en la siguiente tabla.

Tabla 12.

Servicios entregados.

N°	Servidor / servicio	Equipo	Observaciones
1	Correo – Zimbra	IBM (virtualizado)	<ul style="list-style-type: none"> - Realiza la gestión de mensajería de CPMV. - Se definió un espacio de almacenamiento por usuario de 10 MB.
2	Active Directory	IBM (virtualizado)	<ul style="list-style-type: none"> - Tiene como sistema operativo Windows server 2008
3	Antivirus	IBM (virtualizado)	<ul style="list-style-type: none"> - Cuenta con una licencia corporativa del antivirus Nod32
4	Financial	IBM (virtualizado)	<ul style="list-style-type: none"> - Sistema core financiero.
5	Base de datos – Oracle 11G R2	HP (al chasis)	<ul style="list-style-type: none"> - Base de datos producción

2.4.3. Topología de la red

La Figura 25 detalla la siguiente topología con la que cuenta actualmente la Coop. Pablo Muñoz Vega.

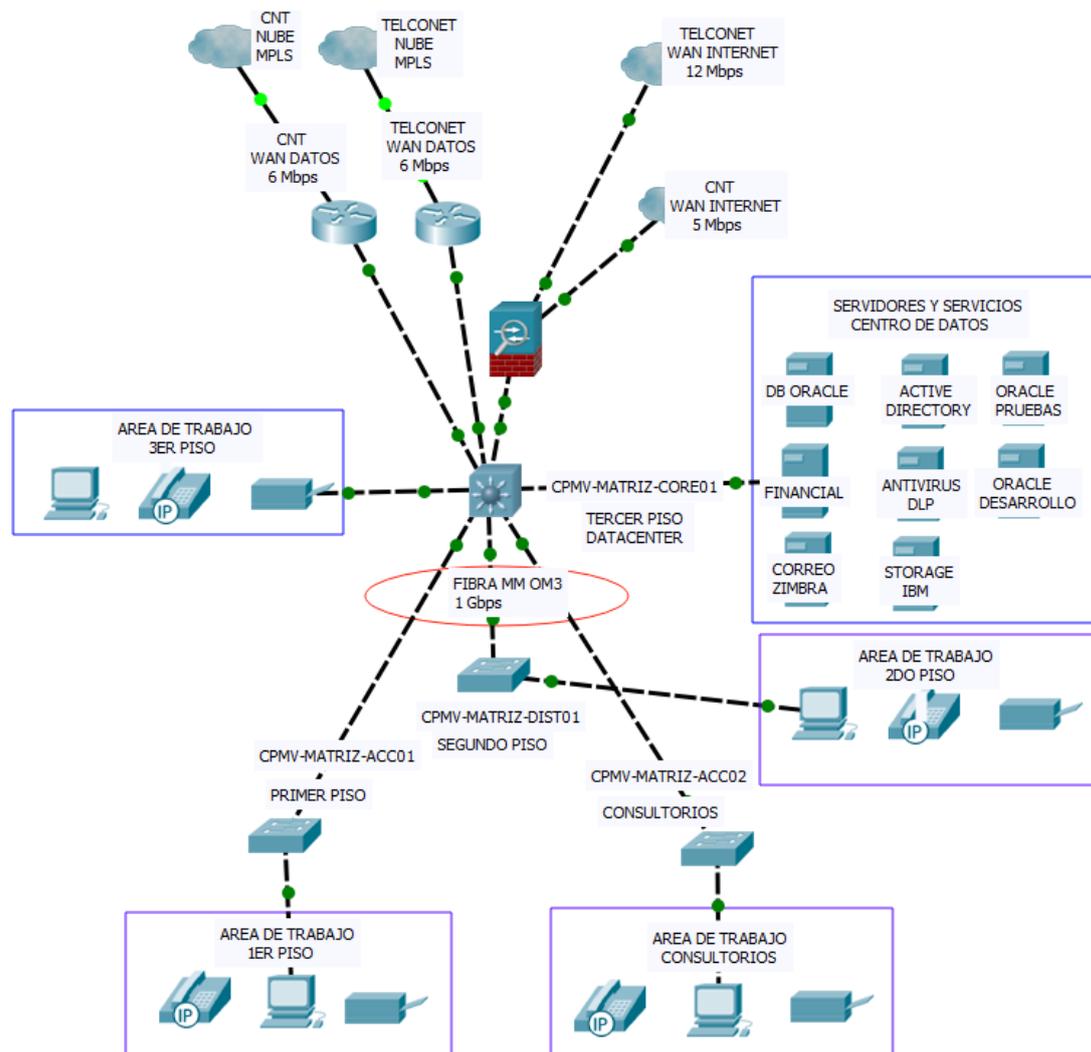


Figura 25. Topología de la Cooperativa Agencia Matriz.

En la Tabla 13 se muestran los segmentos de red hallados en toda la Cooperativa y agencias, datos, telefonía, impresoras, cajeros en el mismo segmento.

2.4.4. Telefonía IP

La Cooperativa cuenta con una central telefónica IP genérica Asterisk, la cual tiene las siguientes características:

- CPU Clon Intel Pentium D 1.8 GHz, 4 GB RAM, 320 GB disco.
- Linux Centos 6.2 x64

- Asterisk V13
- Tarjeta Digium 8 puertos FXO para líneas PSTN
- Gateway IP GSM 4 canales (base celular)
- 44 teléfonos SIP marca Grandstream
- 1 dispositivo ATA to SIP con teléfono analógico Panasonic

Tabla 13.

Segmentos de red descubiertos.

Agencias	Segmento de red	router Telconet	router Cnt	router / firewall puerta de enlace
Matriz	150.150.10.0/24	150.150.10.251	150.150.10.250	150.150.10.1
San Gabriel	150.150.20.0/24	150.150.20.251	150.150.20.250	150.150.20.1
Bolívar	150.150.30.0/24	150.150.30.251	150.150.30.250	150.150.30.1
Mira	150.150.40.0/24	150.150.40.251	150.150.40.250	150.150.40.1
Ibarra	150.150.50.0/24	150.150.50.251	150.150.50.250	150.150.50.1
Quito	150.150.60.0/24	150.150.50.251	150.150.60.250	150.150.60.1
Lago Agrio	150.150.70.0/24	150.150.70.251	150.150.70.250	150.150.70.1

2.4.5. Conexión de los Switches

La Figura 26 describe la conexión de los diferentes switches de la Cooperativa.

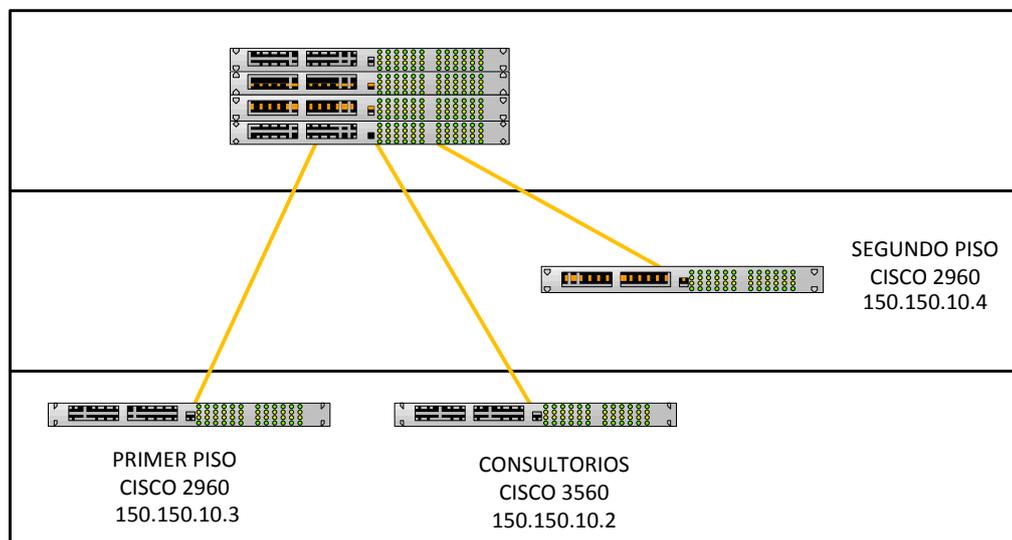


Figura 26. Distribución de los Switches.

La Cooperativa posee una red LAN interna para todos los departamentos y áreas de negocios. Los proveedores del servicio de Internet son, el operador CNT y el operador Telconet, cuyas capacidades entregadas son de 5 MB y 12 MB respectivamente a través de fibra óptica. Los enlaces de datos con cada operador son de 6 Mbps en los dos casos para la Agencia Matriz y de 2 Mbps para cada Agencia externa.

En un capítulo posterior, en la Tabla 14 se especifica el tráfico actual en el switch de core de la Agencia Matriz separado por aplicación.

3. CAPÍTULO III. DISEÑO Y PROPUESTA DE LA SOLUCIÓN

El Diseño de la solución final se realiza aplicando los criterios tecnológicos, conociendo los requerimientos puntuales, los estándares y topologías vigentes y tomando como referencia la metodología de diseño de redes descendente (top-down), debido a que los equipos de enrutamiento y switching son de dicha marca (CISCO) y así garantizar la calidad de la solución

El objetivo de esta metodología es representar con mayor precisión los requerimientos del usuario final de la Cooperativa Pablo Muñoz Vega, que por lo general no se toman en cuenta a la hora del diseño de la red. De igual manera se busca que el proyecto sea gestionado mediante fases, entre ellas, las de documentación e implementación, para posterior continuar con las fases de ejecución, monitoreo y optimización de la red propuesta.

3.1. Reúso de equipos

Con base en la Tabla 10, donde se especifican varios equipos de marca Cisco capa3 y capa2, y con base en la Figura25 donde se especifica que la infraestructura de switching no está jerarquizada y no es redundante se propone reutilizar los mismos para establecer un esquema jerárquico y redundante.

En los casos en los que debido al diseño propuesto exista la necesidad de adquirir equipos para completar el esquema, se sugerirán los modelos adecuados y que se integren de manera transparente y que cumplan con los requerimientos del diseño propuesto.

3.2. Diseño en descenso (Top-Down)

“El diseño de redes debe ser un proceso completo, que asocie las necesidades del negocio a la tecnología disponible, para generar un sistema que maximice el éxito de una organización (Oppenheimer, 2010).”

Implementar una red LAN va más allá que la adquisición de equipos de conectividad, encenderlos y conectarlos. En el caso de las redes WAN va más allá que solamente solicitar servicios a las operadoras locales y recibir conexiones entre puntos remotos.

De acuerdo a este esquema no se empieza asignando direcciones IP, todo lo contrario, se empieza por los lineamientos generales referentes a las necesidades de la Cooperativa alineadas al giro del negocio y que fueron definidas dentro de las normativas de la SBS tratadas en el Capítulo 2. Se continúa por establecer las áreas de servicio, los aplicativos, en particular el sistema Financial, mismo que corresponde al giro del negocio y Bases de Datos Oracle. Tomando como referencia el modelo OSI, se empieza por la capa 7.

Se debe apuntar a entender los flujos de datos, clases de datos, que o quienes acceden a ellos. Se apunta a identificar a continuación la ubicación de los grupos de usuarios. Se busca establecer un modelo lógico antes que el físico. A continuación, se desarrollan las fases correspondientes al método:

3.3. Fase 1. Análisis de los requerimientos

Se parte con el levantamiento de información mediante entrevistas al personal técnico y de las diferentes áreas de negocio.

3.3.1. Metas del negocio

Mediante entrevista con el personal administrativo se determina que es mandatorio seguir con las normativas de la SEPS tal como reza el Capítulo 2, punto 1 del presente proyecto de titulación (SBS, 2014) dentro de los cuales se establecen generalidades relativas a la continuidad del negocio.

Un documento controlado interno de la Cooperativa indica lo siguiente en su introducción: “La recuperación de desastres y eventos críticos es un aspecto muy importante en la operatoria de una organización. Un factor crítico de este aspecto es la recuperación de la operación de la tecnología interna. En

realidad, la recuperación del negocio debe tener precedencia sobre la recuperación de los sistemas de tecnología interna ya que el negocio es el responsable de la continuidad de las operaciones, y por lo tanto del servicio a los clientes.

El negocio puede experimentar toda clase de interrupciones que pueden ir desde desastres naturales catastróficos o actos de terrorismo hasta eventos técnicos elementales, por lo que las organizaciones necesitan recursos, planes y organización administrativa para garantizar la recuperación y continuidad del negocio.

Existe confusión entre los conceptos de Continuidad del Negocio y Recuperación de Desastres, por lo que es importante notar que la Recuperación de Desastres normalmente se enfoca en la tecnología necesaria por recuperar los datos en la ocurrencia de un desastre, mientras que la continuidad del negocio se enfoca más bien en la continuación del negocio como una entidad.

De esta forma, la planificación de la continuidad del negocio va de la mano con la planificación de la recuperación de desastres además de la planificación de los procesos y recursos.” (Departamento de TI, 2017).

De acuerdo a lo anterior la meta del negocio es mantener operaciones a pesar de situaciones consideradas “desastre” a la vez que se ofrece mejor soporte al cliente interno y externo. Esto directamente se refiere al servidor de aplicativo de Core Financiero “Financial” y al servidor de base de datos Oracle 11gR2.

El tiempo máximo que tienen como ventana, dado por la SEPS es de 4 horas, tiempo en el cual los elementos básicos del giro del negocio deben volver a operar.

3.3.2. Metas técnicas

Dentro del mismo documento Plan de Contingencias del Departamento de TI, basado en un análisis de riesgo, realizado puertas adentro en la Cooperativa, se establecen las amenazas con riesgos Altos y Críticos, que atañen directamente al área técnica.

Dentro de estas metas se hallan las siguientes:

- Redundancia de la infraestructura y servicios
- Disponibilidad de la infraestructura y servicios
- Seguridad de la información

Las metas técnicas se justifican adicionalmente con las reuniones realizadas oportunamente, posteriores al levantamiento de la Línea Base, con los técnicos de Departamento de TI y del Departamento de Seguridades donde se exponen, validan y aceptan los resultados del diagnóstico que se refleja en la información que se aprecia en el Capítulo 2 de este proyecto. Dicha información fue levantada en ciertos casos y en otros fue entregada por parte del Departamento de TI de la Cooperativa.

En dichas reuniones se recibe información referente al crecimiento en los últimos 3 años. Se menciona que la cantidad de equipos ha crecido en total por todas las agencias de Cooperativa en un valor promedio de 10%. Se usará este valor como parámetro para el diseño de la Solución a proponerse.

Adicionalmente los técnicos indican que la Cooperativa mantiene una política de adquisición de hardware de infraestructura activa de red donde dan prioridad a equipos remanufacturados sobre equipos nuevos. Los técnicos justifican esta política en el hecho de que los primeros se adquieren con garantía mínima de un año y con soporte con acuerdos SLA (Service Level Agreement) donde se especifican parámetros de servicio que satisfacen a la operación de la Entidad Financiera y con diferencias de precios de hasta un

40% en relación a los equipos nuevos y sin ataduras de renovaciones de garantías anuales.

3.3.3. Red actual

La red actual, como se mencionó previamente y se aprecia en las *Figuras 25 y 26*, no muestra un esquema jerárquico ni se halla redundada.

La captura de segmentos de red con IPScanner que se presentó en la Tabla 9, tampoco muestra un esquema acorde con la RFC 1918 de la IETF (Internet Engineering Task Force) numeral 3, el cual muestra los bloques de direcciones IP reservados por la IANA (Internet Assigned Numbers Authority) para redes locales o privadas.

Es importante mencionar que los enlaces de datos de proveedores como CNT o Telconet, entregan la conectividad directamente en una dirección IP dentro del segmento LAN de cada agencia, lo cual no permite establecer reglas de acceso o políticas de seguridad de manera eficiente.

Adicionalmente en la revisión particular de cada uno de los switches de la Cooperativa no se hallaron segmentos de capa 2 VLAN (802.1Q VLAN tagging)

3.3.4. Tráfico actual

La Tabla 14, muestra el resultado de mediciones realizadas en base al switch CISCO 4506e donde están conectados los servidores y demás hardware de red. De acuerdo a los técnicos del departamento de Ti de la Cooperativa estos datos reflejan el tráfico acumulado que se dirige hacia el switch de core de la Matriz y que se reparte hacia los servidores respectivos.

Tabla 14.

Datos de ancho banda medido en el switch de core.

TABULACIÓN DE ANCHO DE BANDA –SWITCH PRINCIPAL MATRIZ TULCÁN						
DESCRIPCIÓN	MAX (Kb/s)		MIN (Kb/s)		AVERAGE (Kb/s)	
	INPUT	OUTPUT	INPUT	OUTPUT	INPUT	OUTPUT
Core Financiero	3,92	4,66	2,41	3,76	3,17	4,21
Base de Datos	738,84	7,30	458,08	4,65	59,85	5,98
Aplicaciones	625,00	3,12	427,00	592,00	526,00	1,86
Active Directory & APP Exteriores	765,00	181,00	159,00	154,00	462,00	167,50
Cámaras	1,46	62,61	1,36	58,31	1,41	60,46

3.4. Fase 2. Desarrollo del diseño lógico

3.4.1. Diseño de la topología de red

Se propone el siguiente esquema de topología, mismo que consiste en la interconexión redundante de switches en esquema jerárquico con capas definidas de acuerdo a las mejores prácticas sugeridas por CISCO según la Figura 27.

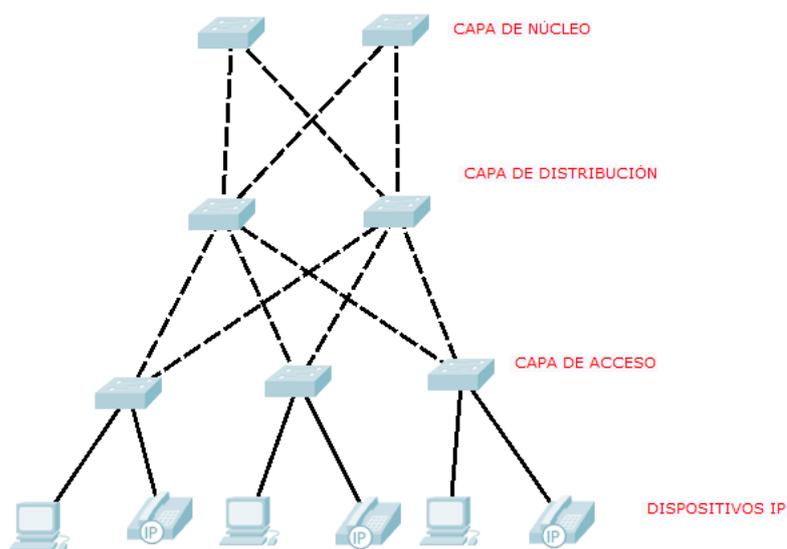


Figura 27. Topología lógica propuesta.

3.4.2. Diseño de los modelos de direccionamiento

Las Tablas 9 y 10 muestran el actual diseño lógico, el cual será reemplazado por otro diseño tomando en cuenta las recomendaciones de la IETF (RFC 1918).

De acuerdo al análisis realizado con los técnicos del Departamento de TI de la Cooperativa, se estableció un esquema para la Agencia Matriz y que luego podrá ser aplicado en las demás Agencias. Esto último no es parte del alcance del presente proyecto, por lo cual no se profundiza.

El subneting propuesto aquí considera un crecimiento de 10% en hosts para los próximos 3 años, tomando en cuenta la información previa recibida por los técnicos del Departamento de TI y que fue expuesta en el punto 3.3.2. Metas técnicas. El direccionamiento IP de las Agencias esta dimensionado con recomendaciones particulares referentes a cantidades de direcciones IP del Departamento de TI.

La Tabla 15 define el diseño propuesto para el direccionamiento IP y VLANS.

Tabla 15.

Direccionamiento IP LAN propuesto.

MATRIZ					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Servidores	172.16.110.0 / 26	110	47	52	62
Telefonía	172.16.110.64 / 26	111	45	50	62
Impresión	172.16.110.128 / 28	112	5	6	14
Vlan administrativa switching	172.16.110.144 / 27	113	20	22	30
Vlan administrativa servidores	172.16.110.160 / 27	114	20	22	30
Usuarios	172.16.111.0 / 24	115	115	127	254
Red Wifi Directivos y TI	172.16.112.0 / 26	116	40	44	62
SAN GABRIEL					

Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.120.0 / 27	120	14	15	30
Telefonía	172.16.120.32 / 27	121	4	4	30
Servidores	172.16.120.64 / 29	122	3	3	6
Vlan administrativa switching	172.16.120.72 / 29	123	2	2	6
Vlan administrativa servidores	172.16.120.80 / 29	124	1	1	6
Impresión	172.16.120.88 / 29	125	2	2	6
MIRA					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.130.0 / 27	130	8	9	30
Telefonía	172.16.130.32 / 27	131	4	4	30
Servidores	172.16.130.64 / 29	132	3	3	6
Vlan administrativa switching	172.16.130.72 / 29	133	2	2	6
Vlan administrativa servidores	172.16.130.80 / 29	134	1	1	6
Impresión	172.16.130.88 / 29	135	1	1	6
BOLIVAR					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.140.0 / 27	140	8	9	30
Telefonía	172.16.140.32 / 27	141	4	4	30
Servidores	172.16.140.64 / 29	142	3	3	6
Vlan administrativa switching	172.16.140.72 / 29	143	2	2	6
Vlan administrativa servidores	172.16.140.80 / 29	144	1	1	6
Impresión	172.16.140.88 / 29	145	1	1	6
IBARRA					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.150.0 / 27	150	21	23	30
Telefonía	172.16.150.32 / 27	151	12	13	30
Servidores	172.16.150.64 / 29	152	4	4	6
Vlan administrativa switching	172.16.150.72 / 29	153	2	2	6
Vlan administrativa servidores	172.16.150.80 / 29	154	2	2	6
Impresión	172.16.150.88 / 29	155	3	3	6

QUITO					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.160.0 / 27	160	21	23	30
Telefonía	172.16.160.32 / 27	161	12	13	30
Servidores	172.16.160.64 / 29	162	4	4	6
Vlan administrativa switching	172.16.160.72 / 29	163	2	2	6
Vlan administrativa servidores	172.16.160.80 / 29	164	2	2	6
Impresión	172.16.160.88 / 29	165	3	3	6
LAGO AGRIO					
Equipos	Segmento IP	VLAN	Host actual	Host +10%	Host max
Usuarios y cámaras	172.16.170.0 / 27	170	8	9	30
Telefonía	172.16.170.32 / 27	171	4	4	30
Servidores	172.16.170.64 / 29	172	3	3	6
Vlan administrativa switching	172.16.170.72 / 29	173	2	2	6
Vlan administrativa servidores	172.16.170.80 / 29	174	1	1	6
Impresión	172.16.170.88 / 29	175	1	1	6

La Tabla 16 define el diseño propuesto para el direccionamiento IP WAN. En este diseño se ha tomado en cuenta que los proveedores Telconet y CNT levantarán entre sus equipos router hacia nuestras interfaces WAN el protocolo de router virtual VRRP.

El direccionamiento propuesto no considera crecimiento sin embargo se tienen dos direcciones IP libres por segmento, en caso de requerirse para nuevos proveedores de enlaces de datos.

Tabla 16.

Direccionamiento IP WAN propuesto.

PLAN DIRECCIONAMIENTO IP WAN						
DIRECCION IP				ROUTER TELCONET	ROUTER CNT	OBS
MATRIZ						
10	254	254	0			RED / 29
10	254	254	1	X		IP REAL
10	254	254	2	X		IP VRRP
10	254	254	3		X	IP REAL
10	254	254	4			FIREWALL
10	254	254	7			BROADCAST
SAN GABRIEL						
10	254	254	8			RED / 29
10	254	254	9	X		IP REAL
10	254	254	10	X		IP VRRP
10	254	254	11		X	IP REAL
10	254	254	12			FIREWALL
10	254	254	15			BROADCAST
MIRA						
10	254	254	16			RED / 29
10	254	254	17	X		IP REAL
10	254	254	18	X		IP VRRP
10	254	254	19		X	IP REAL
10	254	254	20			FIREWALL
10	254	254	23			BROADCAST
BOLIVAR						
10	254	254	24			RED / 29
10	254	254	25	X		IP REAL
10	254	254	26	X		IP VRRP
10	254	254	27		X	IP REAL
10	254	254	28			FIREWALL
10	254	254	31			BROADCAST
IBARRA						
10	254	254	32			RED / 29
10	254	254	33	X		IP REAL
10	254	254	34	X		IP VRRP
10	254	254	35		X	IP REAL
10	254	254	36			FIREWALL
10	254	254	39			BROADCAST

QUITO						
10	254	254	40			RED / 29
10	254	254	41	X		IP REAL
10	254	254	42	X		IP VRRP
10	254	254	43		X	IP REAL
10	254	254	44			FIREWALL
10	254	254	47			BROADCAST
LAGO AGRIO						
10	254	254	48			RED / 29
10	254	254	49	X		IP REAL
10	254	254	50	X		IP VRRP
10	254	254	51		X	IP REAL
10	254	254	52			FIREWALL
10	254	254	55			BROADCAST

3.4.3. Definición de los protocolos para Switching y Routing

Debido a que este proyecto basa su criterio de diseño en buenas prácticas de CISCO para los equipos existentes de la misma marca, se recurrirá a usar los siguientes protocolos:

3.4.3.1. Switching:

3.4.3.1.1. IEEE 802.1Q

Protocolo de capa 2, VLAN protocolo de creación de redes o segmentos lógicos en un mismo medio físico. La Tabla 15 nos muestra los segmentos lógicos y los respectivos números de VLAN a ser usados.

Para el diseño se ha tomado como base el uso del modo VTP transparente, lo cual significa que las VLANs serán configuradas manualmente en cada Switch.

Este modo es similar a configurarlo en Modo Off, con la salvedad que los anteriores avisos o logs de VTP son reenviados, por ejemplo:

```
(config)# vtp mode server
(config)#interface vlan 2
(config-if)#description VLAN SERVIDORES
(config-if)#exit
```

```
(config)#interface range GigabitEthernet 1/1/1GigabitEthernet 1/1/12
(config-if-range)#switchport mode access
(config-if-range)#switchport access vlan 110
```

3.4.3.1.2. IEEE 802.1p

Protocolo de capa 2, QoS Calidad de Servicio, permite priorización de tráfico basado en colas donde se diferencian servicios de tal forma que las VLAN con más tráfico no comprometan el rendimiento de las demás. Se refiere a los estándares IETF RFC 2211(Specification of the controlled load network element service) e IETF RFC 2212 (Specification of guaranteed quality of service) sera aplicado a:

VLAN 110 de servidores, se recurre a forzar Control de Flujo Prioritario en una interfaz en la que se halla conectado un servidor, por ejemplo:

```
(config)#interface GigabitEthernet 1/1/15
(config-if)#untagged cos 3
(config-if)#priority-flow-control mode on
(config-if)#exit
```

VLAN 111 de telefonía, se recurre al uso de Auto QoS, por ejemplo:

```
(config-if)# auto qos voip trust
```

3.4.3.1.3. ETHERCHANNEL PAgP

Protocolo de capa 2, propietario de CISCO compatible con IEEE 802.3, agrupa de manera lógica varios enlaces de similar velocidad hasta un máximo de 8, sumando la velocidad nominal de cada uno. Se realiza entre puertos de similar velocidad, no se puede mezclar velocidades. Se aplicará entre todos los switches con 2 enlaces de fibra Multimodo OM3 hacia interfaces 1 Gigabit en cada uno de los switches de acuerdo a la Figura 24. La configuración modelo para cada par de puertos se da en el siguiente ejemplo:

```
(config)#interface range gigabitethernet1/1/1 -2
(config-if-range)#switchport mode access
```

```
(config-if-range)#switchport access vlan 110
(config-if-range)#channel-group 1 mode desirable non-silent
(config-if-range)#end
```

3.4.3.1.4. IEEE 802.1w

Protocolo de capa 2, RSTP gestión de lazos con un tiempo de convergencia inferior al clásico protocolo STP generalmente usado (cuyo tiempo de convergencia es igual a 50 seg), en lugar de los estados de STP de blocking, listening, learning, forwarding y disabled, RSTP tiene solo tres estados, discarding, learning y forwarding con lo cual los tiempos de convergencia, de acuerdo al estándar, es igual o menor a 10 seg. A continuación, un ejemplo de la configuración a ser utilizada:

```
(config)#spanning-tree mode pid-pvst
```

La Figura 28 muestra el diseño lógico propuesto:

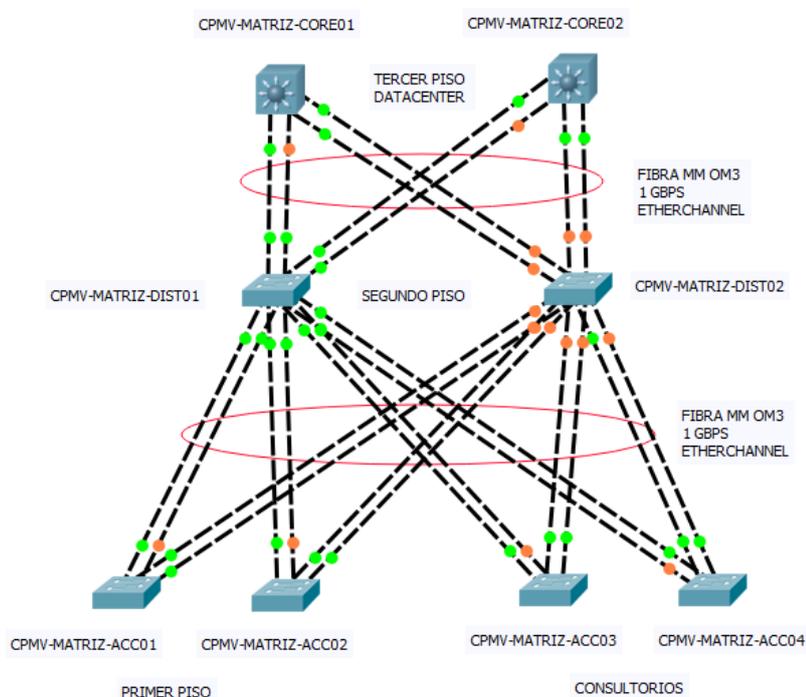


Figura 28. Diseño lógico de Switching propuesto.

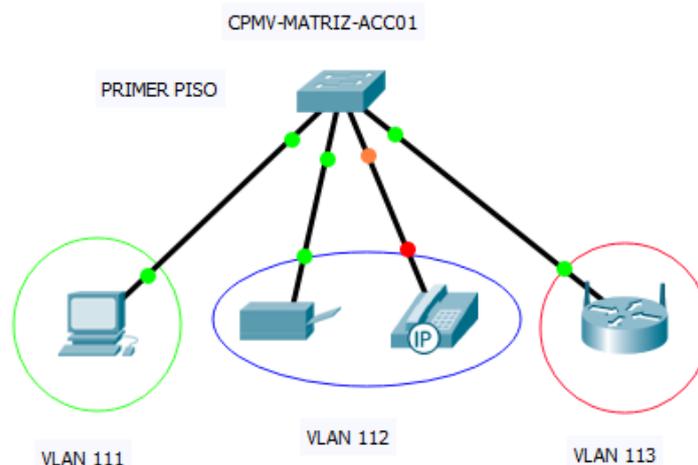


Figura 29. Diseño lógico de Switching de acceso propuesto.

3.4.3.2. Routing

VRRP RFC 3768 y RCF 5798: Virtual Router Redundancy Protocol, es un protocolo que funciona en las capas 2 y 3 del Modelo OSI, soluciona el problema de redundancia en puertas de enlace al agrupar varios routers en un grupo VR (Virtual Router). La Tabla 16 muestra el diseño propuesto para ser usado con las dos operadoras contratadas para el efecto, el cual provee una dirección IP WAN virtual y en el fondo dos routers responden en sus direcciones IP reales al tráfico.

El diseño propuesto estará basado en las funciones de enrutamiento de los dispositivos de borde firewall en HA (Alta Disponibilidad)

No se recurrirá al uso de protocolos de enrutamiento entre subredes ni entre segmentos WAN de las Agencias puesto que el enrutamiento será estático en cada dispositivo de borde y también que los enlaces WAN llegan directamente a los puertos de dichos dispositivos. Los proveedores como CNT y Telconet realizan las tareas de enrutamiento dentro de sus nubes MPLS. La Figura 30 muestra el diseño lógico a ser aplicado

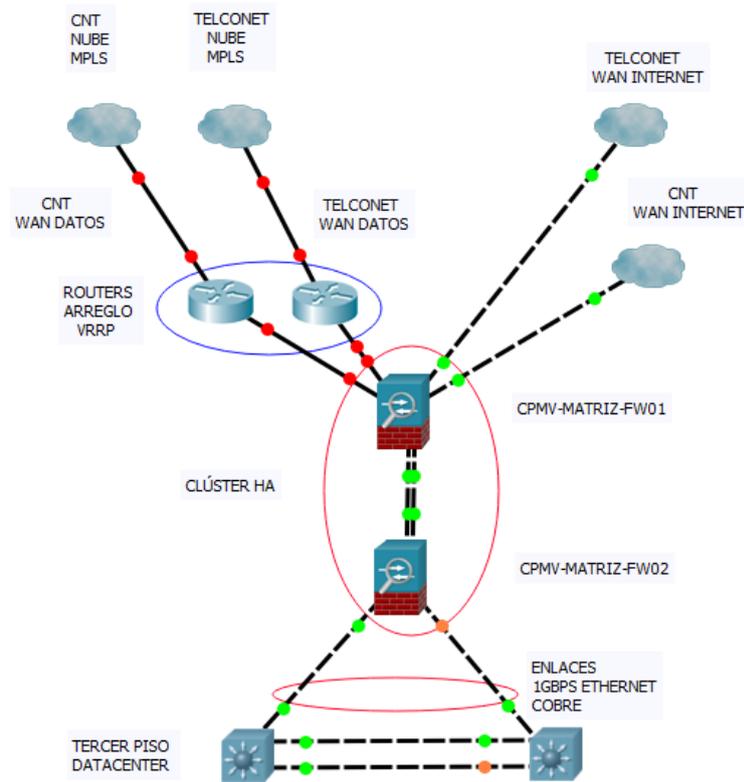


Figura 30. Diseño lógico de Enrutamiento propuesto.

3.4.3.3. Red de almacenamiento SAN (Storage Area Network):

La propuesta considera el diseño de una red de almacenamiento local (SAN) para lo cual se recurre a la topología SWITCHED FABRIC

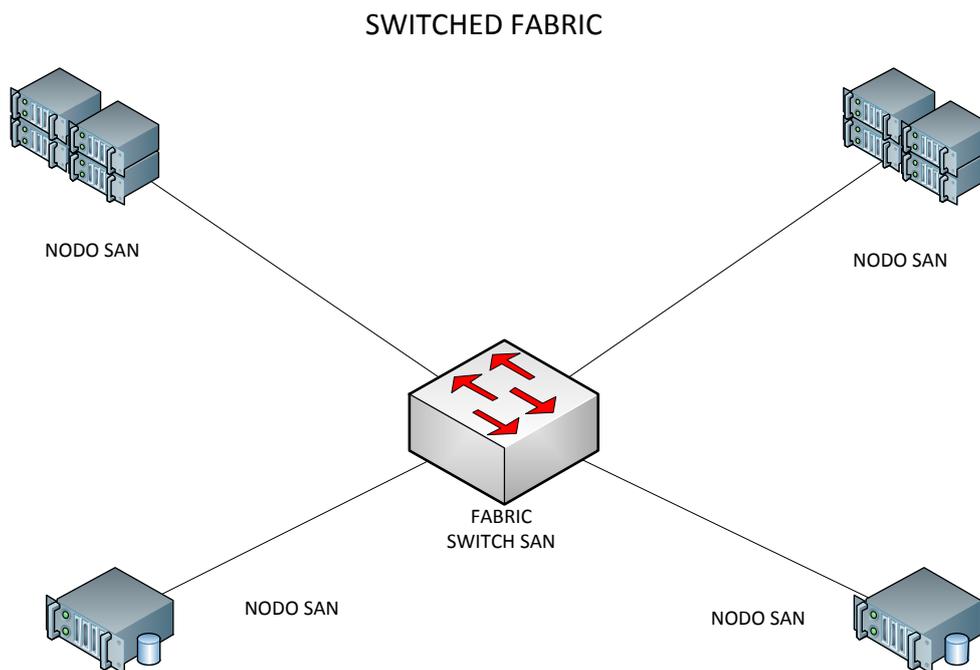


Figura 31. Topología propuesta para el diseño de la red SAN.

Los elementos requeridos para este diseño son los siguientes:

FABRIC:

- 2 switches de SAN (Redundancia) Fabric SAN
- 2 equipos storage (IBM Storwize) Nodo SAN
- 2 tarjetas HBA FC single port (Fibre Channel) por servidor como Nodos SAN

Las características generales de la red de almacenamiento propuesta son las siguientes:

- Capacidades elevadas de ancho de banda:
 - 2, 4, 8, 16 Gbps
 - Se usará 8Gbps.
- Integridad de los datos:
 - Protocolos CRC de 32 bits

- Alta disponibilidad:
 - FABRIC Switch basado en dos equipos de 24 puertos SFP 8 Gbps conectados de forma redundante en dos vías.
 - Dos controladoras FC por Nodo en Failover (storage) y en modo Multipath (servidores)
 - Capacidad para establecer sitios alternos geográficamente separados como contingencia de almacenamiento.
- Escalabilidad:
 - Capacidad para integrar más dispositivos Fabric SAN o Nodos SAN.
 - Compatibilidad con dispositivos 2, 4,8, 16 Gbps.
 - Capacidad para integrar dispositivos Gateway para interconectar redes SAN remotas.
- Confidencialidad:
 - Capacidad para crear zonas de almacenamiento donde se comparten LUNs y se especifican las direcciones físicas WWN (pWWN) autorizadas de los controladores o adaptadores HBA FC en cada dispositivo Nodo SAN, sean storage o servidores respectivamente.
- Autenticación:
 - Enforce WWN, el arreglo Fabric SAN aceptará conexiones por puerto y por identificación vía WWN (World Wide Name) exclusivamente. Ningún WWN no aceptado podrá acceder a las LUN.
- Administración:
 - Consola única de gestión y administración.
 - Provisión de MIIB para integración de los equipos Fabric SAN con el esquema SNMP previamente implementado.

El diseño propuesto para la Cooperativa busca consolidar el almacenamiento mediante una red SAN e integrarla a un modelo de Nube privada con tecnología de ORACLE VM server.

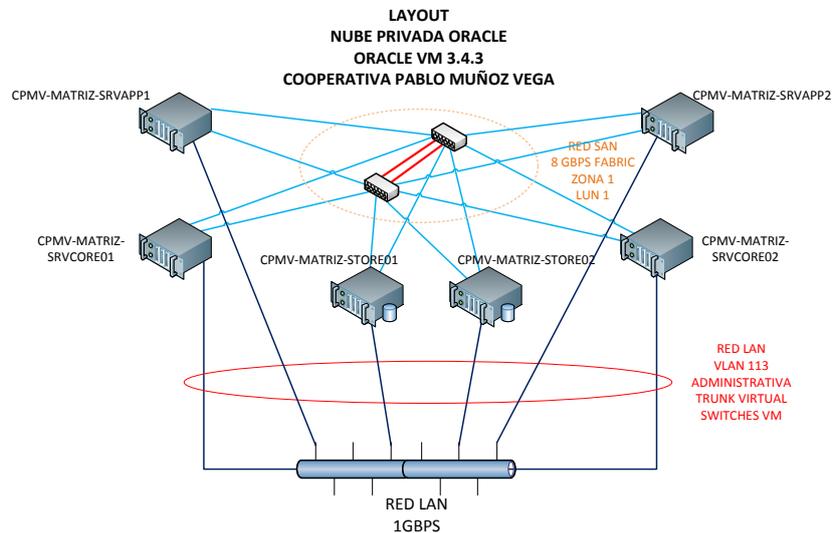


Figura 32. Diseño lógico punto a punto de Switching SAN propuesto para la infraestructura de nube privada ORACLE.

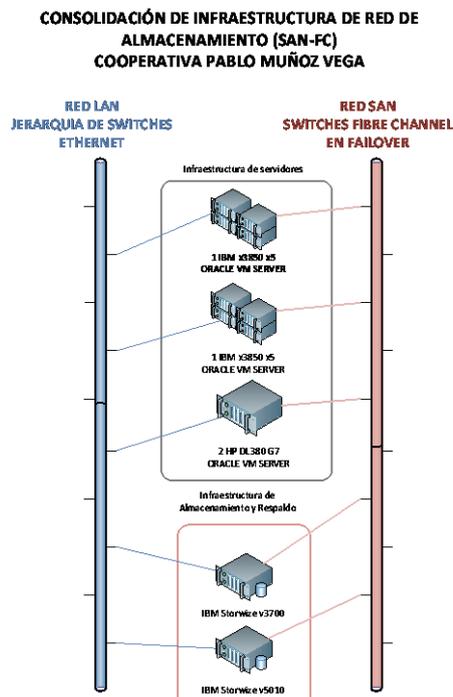


Figura 33. Diseño lógico de consolidación red de almacenamiento SAN

3.4.4. Desarrollo de las estrategias para la seguridad de la red

De acuerdo a la normativa de la SEPS se requiere dotar de especificaciones mínimas de seguridad generalmente aceptadas tales como:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación

3.4.4.1. Confidencialidad

El principal componente dentro de este ámbito es de la pila de equipos Firewall, los cuales en su función básica evitarán accesos no deseados a las redes donde resida la información y proveerán las políticas necesarias de acceso a recursos de red.

De acuerdo a la Tabla 14 la Cooperativa contará con dos dispositivos firewall de borde en Matriz, los mismos que se encargarán de proveer la seguridad entre los segmentos LAN, los segmentos WAN y seguridad en el acceso a los servicios en línea. Estos equipos se configuran en HA (alta disponibilidad).

La siguiente figura muestra la propuesta del diseño físico de seguridad con firewalls:

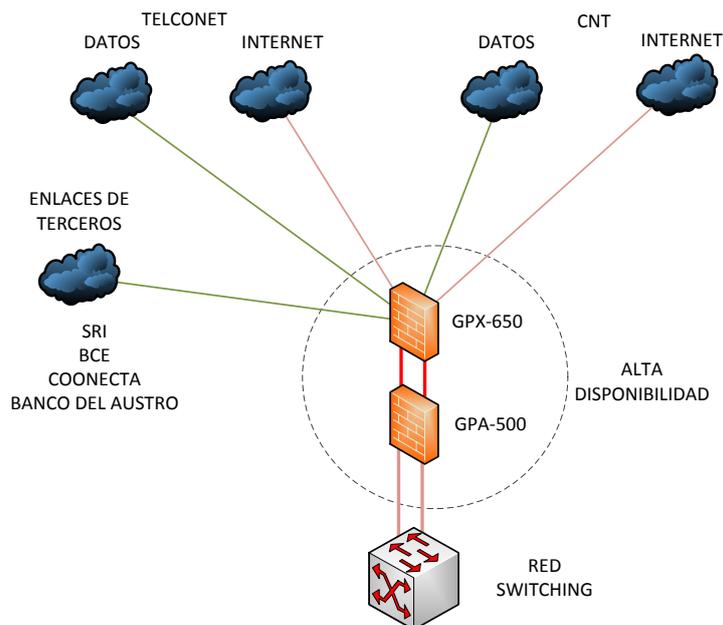


Figura 34. Esquema físico seguridad con firewalls.

Del lado de los esquemas lógicos de seguridad a ser implementados en los equipos de borde se tienen los siguientes:

- Seguridad por puerto (TCP/UDP, etc.) y protocolo a nivel LAN y WAN
 - La seguridad se levanta entre segmentos locales VLAN
 - La seguridad se levanta entre segmentos WAN
 - La seguridad se levanta para enlaces de terceros
- IDS / IPS (Detección de Intrusos y Prevención de Intrusos)
- URL content filter, basado en Proxy Transparente
- Application Filter, políticas de control a nivel de aplicación
- Antispam para el servidor de correo electrónico Zimbra
- Antivirus de Gateway
- Ipsec para los enlaces remotos (cajero - matriz)
- Control de DDoS

Cabe destacar que los mencionados equipos cuentan con las capacidades antes citadas.

Por el lado de los esquemas de seguridad que se levantan a nivel de los demás componentes de la red se tienen:

- Filtros locales: Seguridad por puerto (TCP/UDP):
 - Reglas de IPtables para Linux
 - Reglas de Firewall en los servidores Windows
 - Reglas de filtro de IP para servidores de virtualización
 - Reglas de filtro de IP para equipos de Switching
- Ipsec: Cifrado de paquetes IP

Para las comunicaciones entre servidores y determinados usuarios o equipos conforma las auditorías así lo exijan se implementa el esquema.

- Proporciona autenticación a nivel de red
- Se levanta dentro de uno de los servidores miembros del Active Directory (el servidor de cajeros automáticos) una GPO política de grupo que exige que las comunicaciones desde miembros de dicho grupo hacia este servidor se realicen exclusivamente con Ipsec. Esto tiene además el objetivo de cumplir con las observaciones de auditoría externa sobre la seguridad de la información de los usuarios.
- Se define como Algoritmo de Cifrado a AES128, soportado por la mayoría de versiones de Windows.
- Como complemento se activan las políticas correspondientes en el Firewall local de Windows para que dicho tráfico sea aceptado.

- Certificados SSL:
 - Activación de acceso con certificados SSL públicos, adquiridos a una entidad Certificador externa, para los servicios de Banca en Línea y servicios de correo electrónico.
 - Esto se realiza con el fin de asegurar las conexiones a los servicios en línea que ofrece la Cooperativa a los clientes internos y externos.
 - Se evitarán certificados de 1024 bits considerados inseguros y se preferirán certificados de 2048 bits como mínimo. Esto garantiza la seguridad de la información del usuario.

- DMZ: Zonas demilitarizadas
 - Los servidores de servicios en línea considerados como sensibles estarán dentro de una DMZ asignada de manera lógica con un mecanismo e interfaz de firewall, de esta manera se previene que, en el caso extremo de una intrusión al servidor, los demás segmentos de la red se vean vulnerados.
 - Servidores en DMZ, Banca el Línea, Correo electrónico con Zimbra.

- Acceso administrativo:
 - Definición de los dispositivos o equipos con su respectiva dirección IP, enlaces VPN que estarán autorizados a administrar la infraestructura de red.
 - Se instala en un equipo del área de seguridades la consola de administración propietaria de los equipos Gateprotect llamada Command Center.
 - Se definen políticas de acceso vía consola web con https y consola segura vía SSH.

3.4.4.2. Integridad

El diseño propuesto implica dos recomendaciones referentes a dos áreas de la información dentro de la Cooperativa:

Servidores:

- Base de datos Oracle 11g R2
 - La normativa de la SEPS requiere la implementación de un sistema que garantice la Integridad de la información contenida. Esto atañe directamente al giro del negocio dado que las bases de datos contienen toda la información financiera de la entidad y de los usuarios.
 - De los productos disponibles en el mercado, se evalúan las hojas de especificaciones de varios productos, hallando que IBM Guardium provee las funcionalidades necesarias tales como
 - Enmascaramiento de las bases de datos
 - Cifrado de las bases de datos
 - Evaluación de vulnerabilidades
 - Supervisión de actividad.

Para la implementación de este software se requiere la compra de las respectivas licencias y la provisión de una máquina virtual donde se implementa un servidor Oracle Linux 6 sobre el cual se levantan dichos servicios.

Equipos de usuario:

A nivel de usuario o equipos cliente la normativa de la SEPS también recomienda la implementación de un esquema que permita garantizar la Integridad de la información, para lo cual se definen estos componentes en el diseño de la propuesta.

- DLP (Data Loss Prevention)

- Provee un esquema único de prevención de acceso indebido a los recursos de información de usuario, tales como carpetas compartidas, correo electrónico, dispositivos de almacenamiento externo.
 - Se evalúan varios productos de software y se prefiere a Endpoint Protector de CoSoSys, el mismo que además de las funciones de DLP basado en políticas predefinidas también provee seguridad a nivel de dispositivos móviles. El producto se presenta como un Appliance Virtual que se instalará dentro de la nube privada de Oracle.
 - La consola de administración vía <https://> permite la gestión de los usuarios/dispositivos y la aplicación de políticas de tipo acceso / no acceso / información administrativa. De tal forma que se pueda evaluar el comportamiento de los usuarios y dispositivos y posterior mejora de las políticas aplicadas.
 - Basa su funcionamiento en un agente que se instala en los equipos cliente, para lo cual se creará una política en el Active Directory, la cual se encargará de distribuir e instalar dicho agente en los equipos que formen parte de una determinada Unidad Organizativa.
- Antivirus:
- La Cooperativa previamente ya contaba con un producto de seguridad para Endpoint llamado ESET Endpoint Security, el mismo que había sido implementado con base a un servidor Windows. El producto funciona de una manera adecuada, como se evidencia en la contención de los recientes ataques de Ransomware producidos a nivel mundial.
 - Se diseña un esquema en el que el antivirus ESET radique en un ambiente distribuido por agencias, de tal forma que las actualizaciones no dependan de la consola central en Matriz y se evite el consumo de ancho de banda de los enlaces de datos.

La siguiente figura muestra el esquema distribuido propuesto

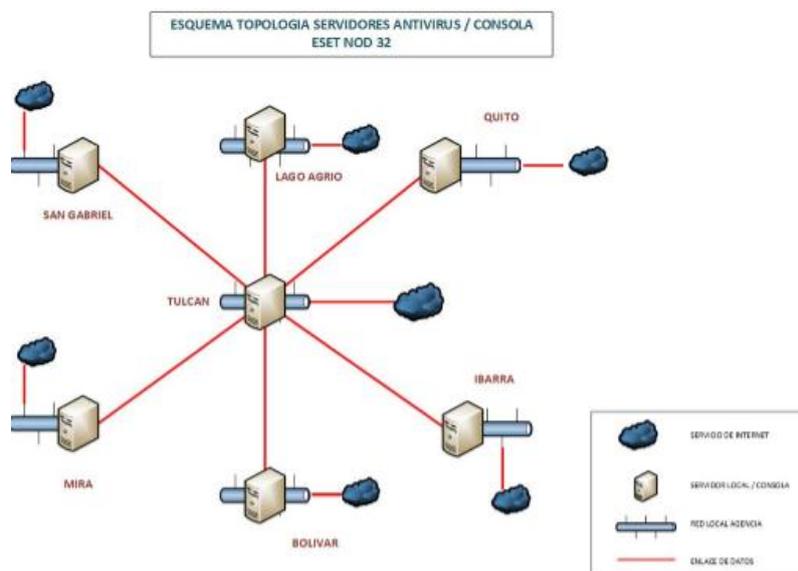


Figura 35. Esquema lógico ambiente distribuido antivirus.

3.4.4.3. Disponibilidad

Este punto está directamente relacionado con la exigencia de la normativa de la SEPS sobre la Continuidad del Negocio.

Referente a la disponibilidad de la información la Cooperativa tiene un manual de procedimientos de tipo confidencial donde se establecen entre otros los siguientes puntos que fueron ya ejecutados:

- Base de datos Oracle 11g R2 replicada hacia sitio alternativo en la Agencia Ibarra. La base de datos de réplica está alojada en un servidor HP Proliant DL380 G7 con Oracle Linux 6.9.
- La réplica esta implementada con base de un servicio de terceros llamado DBvisit el cual basa su funcionamiento en un servicio cargado en cada sistema operativo Linux, tanto en el servidor de Producción como en el servidor de Desarrollo. Este servicio lee directamente los DML de transacción de Oracle con base a los archive log y asienta en el servidor destino.

El mismo software tiene la capacidad de cambiar los roles entre servidores de Producción a Réplica y viceversa.

- El servidor de aplicativo Financiamiento también está distribuido en cada agencia de la Cooperativa, de tal forma que, en caso de la falta de los servidores en Matriz, inmediatamente se cambie de rol al servidor de Base de Datos y el aplicativo se mantenga disponible.
- Se establece que también es de carácter crítico el servicio de correo electrónico, por lo cual al servidor de correos Zimbra V8.6 se le dotará de un esquema de respaldo y recuperación de desastres por medio de un software de licenciamiento anual llamado Zextras, mismo que además provee funciones de mantenimiento del almacenamiento de correos.
- Se incluye dentro del diseño la provisión de un servidor adicional (relay) de correos con el afán de tener redundante el servicio. Para que este esquema sea exitoso se requiere que se provean los registros DNS A, MX, PTR necesarios para que el dominio cpmv.fin.ec resuelva hacia los servidores en orden de preferencia de 10 (principal) y 20 (relay).

3.4.4.4. Autenticación

Un componente importante en el esquema de seguridad implementado es la adición de políticas de acceso a la información muy bien definido y estructurado.

El Departamento de Seguridades de la Cooperativa sugiere un esquema que incluya la implementación de servicios con base a políticas de Active Directory de Windows. Las políticas tendrán estos alcances:

- Agencia
- Departamento

- Permisos especiales

Con este criterio se crearán Unidades Organizativas por Agencia, por Agencia y Departamento y por Grupos con permisos especiales.

3.4.5. Desarrollo de las estrategias para la administración de la red

Al carecer de esquemas de administración de la red y dado que el proyecto se ha alineado con las mejores prácticas de CISCO, se diseña el siguiente esquema:

3.4.5.1. AAA (Authentication, Authorization, and Accounting)

Basado en TACACS+ los requerimientos son los siguientes:

- Servidores Unix (BSD, SOLARIS, LINUX) con demonio TAC+, se requiere redundancia local o regional (2 más servidores virtuales)
- Equipos switches con IOS (Internetwork Operating System) v12.2 o superior. En caso de que los equipos no tengan esta versión mínima se procede a actualizarlos.
- La instalación del demonio Tac+ se realizará sobre servidores virtuales con Oracle Linux 6.9, por ejemplo (Ver Anexo F):

```
[root@tac.cpmv.fin.ec~]# cd /etc/yum.repos.d/
```

```
[root@tac.cpmv.fin.ec~]yum.repos.d/
```

```
# nano -w nux-misc.repo
```

Se crea un repositorio desde donde se obtiene TAC+:

```
[nux-misc]
```

```
name=Nux Misc
```

```
baseurl=http://li.nux.ro/download/nux/misc/el6/x86_64/
```

```
enabled=0
```

```
gpgcheck=1
```

```
gpgkey=http://li.nux.ro/download/nux/RPM-GPG-KEY-nux.ro
```

Guardar el archivo

Instalación de TAC+:

```
[root@tac.cpmv.fin.ec~]#yum --enablerepo=nux-misc install tac_plus
```

Configuración de un Switch de core para TACACS+:

```
CPMV-MATRIZ-CORE01(config)#aaa new-model
```

```
CPMV-MATRIZ-CORE01(config)#aaa authentication login default group
```

```
tacacs+ local
```

```
CPMV-MATRIZ-CORE01(config)#tacacs-server host 192.168.110.100
```

```
CPMV-MATRIZ-CORE01(config)#tacacs-server key 0 contraseñaCPMV
```

```
^z
```

3.4.5.2. SMNP (Simple Network Management Protocol)

Protocolo de capa 7 (Aplicación) en el modelo OSI, permite administrar y gestionar equipos agrupados en comunidades.

- Se utilizará un esquema SNMP V3 debido a la facilidad que ofrece para depurar y corregir errores.
- SNMP V3 ofrece opciones de autenticación y encriptación para la comunicación con los equipos origen de los traps.
- Requiere 2 servidores virtuales (BSD, LINUX) donde correrá el demonio Servidor SNMP en la versión 3. Los servidores están configurados en clúster ubicados regionalmente entre agencias para garantizar la disponibilidad de la plataforma administrativa.
- Los switches requieren un nivel mínimo de IOS V12.2.

- Los switches deben tener cargadas sus respectivas MIIB para que puedan ser gestionados y administrados, en caso de no tenerlas se descargan de `ftp://ftp.cisco.com/pub/mibs/supportlists`
- Se instala sobre los servidores redundantes de SNMP el software CACTI: Open Source Network Monitoring el cual es una versión potente y que no requiere la adquisición de licencias.

Por ejemplo:

(Instalado sobre clúster de servidores virtuales Oracle Linux 6.9)

```
[root@cacti.cpmv.fin.ec~]# yum install cacti
```

Las dependencias se resuelven automáticamente y se instala el software Cacti v1.0.0

Dentro de las dependencias más importantes que se levantan esta MySQL server v5.7.

Cacti también cuenta con un plug-in que levanta servicios de SYSLOG, sin embargo, este no está considerado en el presente diseño.

Se crean tareas de cron de Linux para que el software solicite información a los equipos administradores con intervalo de 5 minutos.

Se añade el servidor al servicio DNS de Active Directory de tal forma que el ingreso para la administración se realiza apuntando hacia esta dirección `http://cacti.cpmv.fin.ec/cacti` (dirección que únicamente sirve para acceso local y no se encuentra publicada al internet.) con las credenciales que fueron ingresadas durante la instalación con Yum.

3.4.5.3. NTP (Network Time Protocol)

Protocolo de capa 7 (Aplicación) en el modelo OSI. Dentro de las mejores prácticas sugeridas por CISCO se especifica este protocolo para ser implementado en redes modernas el cual permite tener una base para realizar análisis de rendimiento, el cual es un procedimiento de las funciones de administración de la red.

La figura 36 muestra la topología lógica del servicio diseñado:

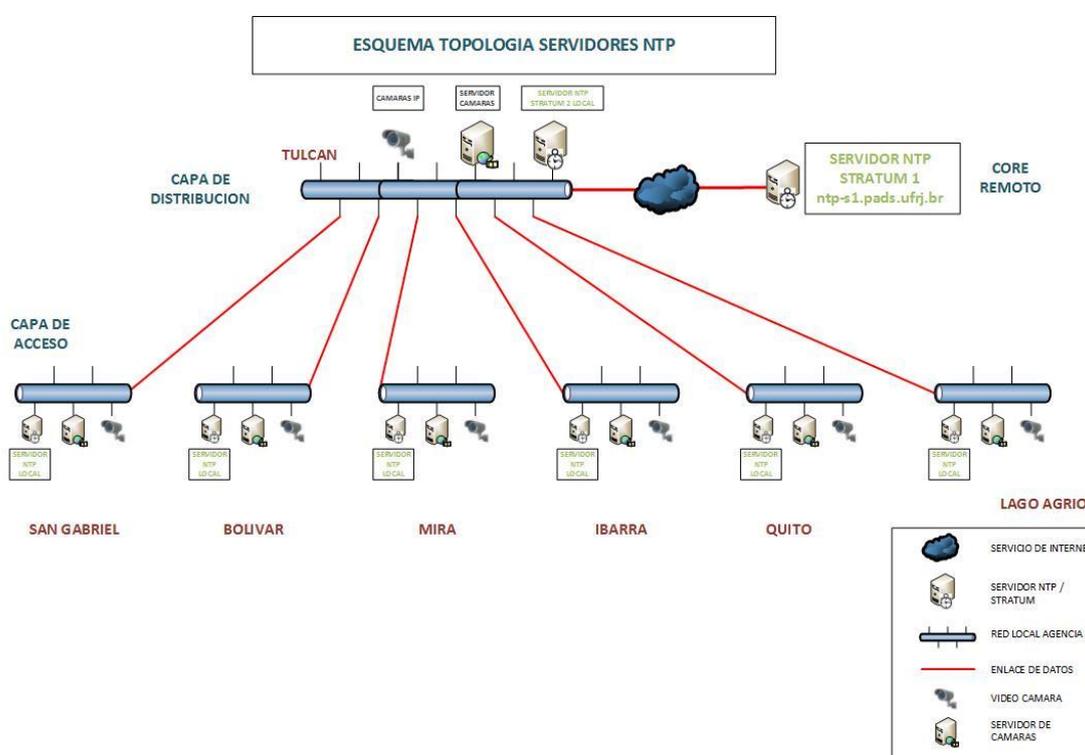


Figura 36. Esquema lógico ambiente distribuido NTP.

Los elementos constitutivos del diseño son:

matriz-ntp01.cpmv.fin.ec: Servidor Virtual FreeBSD (Unix) con demonio NTP configurado como STRATUM2 colgado de un reloj STRATUM de nivel 1 más cercano y libre en Brasil ntp-s1.pads.ufjf.br.

Configuración NTP (Ver Anexo G)

3.4.5.4. Servidores en redundancia con Arquitectura de Nube privada de Oracle.

En el punto 3.4.3.3., se especificó la red de almacenamiento SAN que brindará servicios de disco y respaldo a los servidores que se implementarán dentro del Subsistema de Arquitectura. La figura 37 muestra el esquema de capas en el que está basada la Arquitectura de Nube de Oracle:

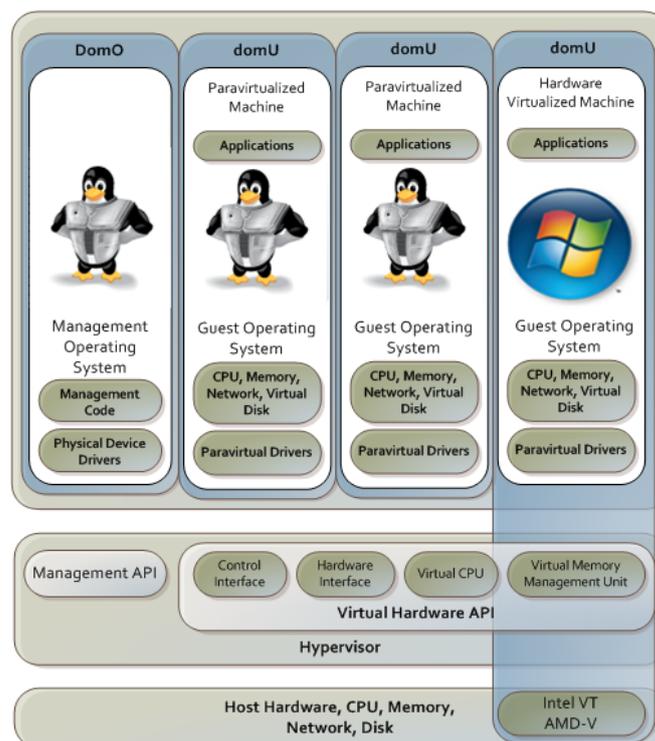


Figura 37. Arquitectura Nube Oracle.

Tomado de Oracle Corporation Inc., 2017.

La figura 38 muestra el esquema físico de las conexiones de los servidores que participan en la infraestructura de Nube privada de Oracle diseñada para la Cooperativa:

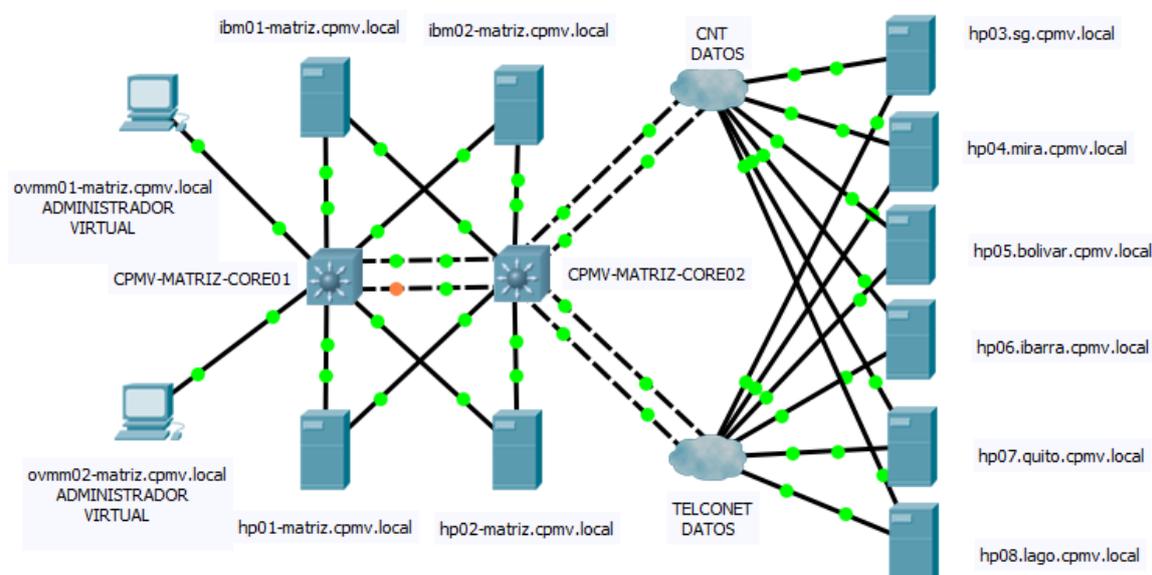


Figura 38. Arquitectura servidores participantes Nube privada Oracle.

3.4.5.4.1. Requerimientos Arquitectura Nube privada Oracle

Software:

- Oracle VM Server V 3.4.3 (en cada servidor participante)
- Oracle Enterprise Linux 6.9 (para los 2 administradores virtuales)
- Oracle VM Manager V 3.4.4 en cada administrador virtual.

Soporte:

- Soporte Oracle VM para cada servidor participante.

Equipos a reusar:

Matriz:

- 2 servidores IBM X3850 X5
- 2 servidores HP DL 380 G7

Agencias:

- 6 servidores HP DL 160 G6

3.5. Fase 3. Centro de Datos, nuevo diseño físico

Para el diseño de esta fase se toma como referencia la Tabla 12 donde se tabularon los problemas hallados a la luz de la norma EIA / TIA 942. En la tabla referida se organizaron por subsistemas los requerimientos.

La infraestructura física de la Cooperativa, está basada en el datacenter de la Agencia Matriz, por lo cual partiendo del levantamiento de la Línea Base realizada en el punto 2.3.1. se realiza el diseño correspondiente como se aprecia en la figura 33 a continuación:

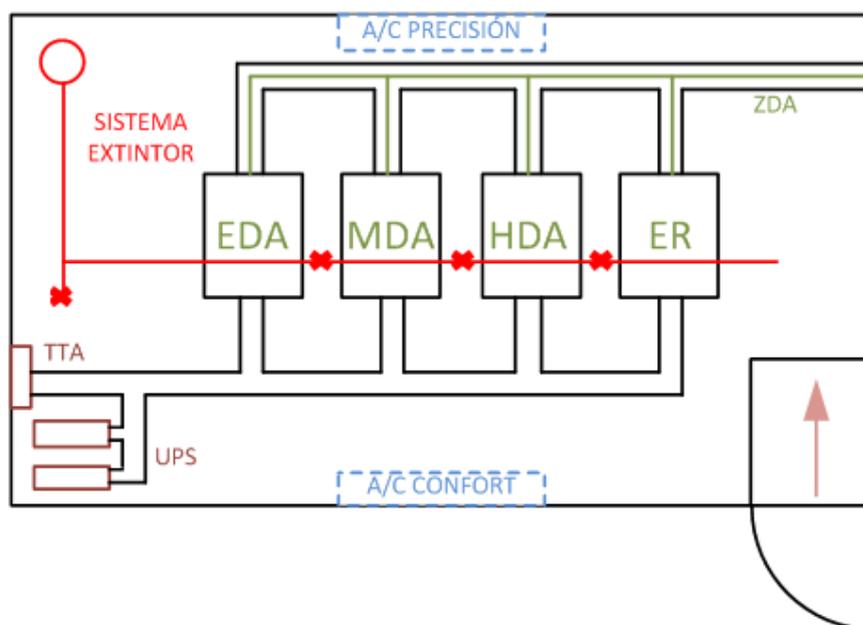


Figura 39. Diseño nuevo Centro de Datos.

Este diseño nuevo afecta directamente a los componentes de los subsistemas del datacenter, dichos cambios serán descritos en los puntos que siguen, así como los requerimientos que implican adquisiciones.

3.5.1. Diseño físico Centro de Datos EIA / TIA 924

3.5.1.1. Cableado horizontal

Dado que el cableado categorías 6 (datos) marca Leviton y categoría 5e (voz) marca Nexxt de los pisos hacia el datacenter es relativamente nuevo y está organizado de manera adecuada en racks por piso, el diseño se centrará en el enrutamiento del mismo dentro del datacenter con base al estándar EIA/TIA 942.

Como se aprecia en la Tabla 8, se debe corregir el método de enrutamiento del cableado dentro del Centro de Datos, el mismo que usará canalización por bandeja metálica de 18cm de ancho por 7 cm de alto con división. Esta canalización usará cada compartimento para separar los cables de datos de los de voz y así mantener un orden que posteriormente permita la adición de cables hacia el Rack de MDF.

El estándar EIA/TIA 942 establece que los cables de red deben ser enrutados bajo el piso técnico disponible y por el pasillo frío, es decir donde existe la presencia de aire frío provisto por el Subsistema Mecánico de climatización de precisión.

3.5.1.1.1. Requerimientos

- 12m bandeja metálica 180x70 mm con división
- 12m tapa metálica 180x70 mm
- 4 curva y tapa plana 180 mm
- 3 uniones con tapa plana 180 mm
- 1 certificación de todos los puntos de voz y datos

3.5.1.2. Cableado vertical

El cableado vertical o de backbone está basado en pares de fibras Multimodo que van desde los Racks de IDF en cada piso hacia el Rack de MDF en el datacenter, están organizados con dispersores, patch panels y organizadores de cable, sin embargo, dado que solo existe un par de fibra desde el MDF a cada IDF, y en concordancia con el diseño propuesto en la Figura 24 se requerirán enlaces adicionales por los mismos ductos de enrutamiento de los cables de fibra actuales, pues tienen suficiente espacio.

3.5.1.2.1. Requerimientos

Rack MDF Datacenter hacia IDF 2 piso:

- 10 pares de fibra MM OM4 50/125
 - o 7 pares para enlazar los switches de core
 - o 3 pares de Backup
- 2 patch panel 12 puertos SC
- 20 puntos de fusión
- 7 patch cord 7 pies SC-LC OM4

Se reúsan:

- 1 par de fibra MM OM4 50/125
- 1 organizador de fibra
- 1 patch cord 7 pies SC-LC OM4

Tabla 17.

Resumen de soluciones para el diseño del subsistema de Infraestructura de Red.

Elemento analizado	Solución
Cableado No se tienen un enrutamiento del cable por pasillo caliente	Canalización con bandeja metálica 18x7cm con división, cada división llevará
Switch de core sin redundancia	Jerarquización switches
Cable Cableado no certificado	Certificación del cableado Cat 6 y 5e
Racks	Altura 1.80 m

3.5.2. Subsistema Arquitectura

Debido a que no es el alcance del presente proyecto profundizar en los subsistemas que no son parte constitutiva del subsistema de Infraestructura de Red se citan únicamente las soluciones propuestas por proveedores de dichos sistemas.

3.5.2.1. Requerimientos

Tabla 18.

Resumen de soluciones para el diseño del subsistema de Arquitectura.

CANT.	Solución
1	Ampliación datacenter a 7m x 4m Paredes de 15 cm de ancho
1	Acabados arquitectónicos (pintura ignífuga, pintura exterior, etc.)

1	Piso técnico o falso 28m2 1250 lb carga bruta, 800lb carga dinámica, 700 lb carga caída libre (baldosas de PVC antiestático, acero 2mm, cemento)
1	Sistema de bases de acero 30 cm alto
1	Rampa de acceso 100 X 120 X 30
1	Puerta metálica corta fuego 100 x 210 con sistema de seguridad y marco de metal, mirilla antibandálica y brazo cierra puerta.
1	Ventosa doble copa
1	Sistema de control de acceso biométrico
1	Sistema de monitoreo CCTV 4 puntos

3.5.3. Subsistema Eléctrico

Para este subsistema se propone de forma general la solución adecuada a las necesidades de la Cooperativa.

3.5.3.1. Requerimientos

Tabla 19.

Resumen de soluciones para el diseño del subsistema Eléctrico.

CANT.	Solución
1	Grupo electrógeno generador trifásico 22KVA, 85% de eficiencia al nivel de Tulcán 2.950 m. REQUIERE LA PROVISIÓN DE UN SITIO EN LA PLANTA BAJA
1	Canalización por pasillo frío con bandeja metálica 180x70 mm con división
1	Cableado alimentación trifásica desde circuito de calle o medidor (requiere provisión de 3 fases)
1	Cableado acceso hasta tableros de transferencia y sistemas de A/C
1	Cableado interno alimentación 220v y 110v Datacenter dos circuitos (N+1)
1	Instalación malla de tierra, malla de alta frecuencia
1	Enrutamiento de backbone de cableado eléctrico con bandeja metálica galvanizada
1	Tableros TTA 220v y ByPASS acometida 3 FASES
1	TVSS (DPS)

8	PDU bifásico (dos por rack, uno por circuito)
2	UPS bifásico 10 KVA en redundancia N+1
1	Sistema de iluminación con paneles LED
SISTEMA DE PARARRAYOS PROVISTO POR LA COOPERATIVA	

3.5.4. Subsistema Mecánico

Para el subsistema Eléctrico se propone una solución acorde a las necesidades levantadas en la línea base.

3.5.4.1. Requerimientos

Tabla 20.

Resumen de soluciones para el diseño del subsistema Mecánico.

CANT.	Solución
1	Sistema de A/C de precisión 33 KBTU
1	Reubicación sistema anterior de A/C pasillo frío
1	Instalación de cañerías de sistemas de A/C con escalerilla metálica superior, condensador exterior.
1	Sistema de detección de incendio (sensores)
1	Sistema de almacenamiento y distribución agente compatible con NFPA 2001 (Bombona con FM200 o Novec 1230 tubería negra y sprinklers)

Ver Anexo H: Cotización construcción Centro de Datos, subsistemas.

3.6. Subsistemas de cableado estructurado (EIA / TIA 568B)

Para este subsistema se propone de forma general una solución adecuada a las necesidades de la Cooperativa basa en la solución propuesta en el punto 3.5.1. Diseño físico Centro de Datos, esto se justifica en el hecho de que los subsistemas de cableado de la Matriz se interconectarán hacia el subsistema de infraestructura del Centro de Datos. No se requieren mayores modificaciones a los demás subsistemas dentro del estándar por lo cual solo se definirán los requerimientos del subsistema que debe ser intervenido.

3.6.1. Requerimientos subsistemas de cableado estructurado

3.6.1.1. Subsistema Backbone vertical

Rack IDF 2 piso hacia rack IDF primer piso

- 10 pares de fibra MM OM4 50/125
 - o 8 pares para enlazar los switches de core
 - o 2 pares de Backup
- 2 patch panel 12 puertos SC
- 20 puntos de fusión
- 8 patch cord 7 pies SC-LC OM4

Rack IDF 2 piso hacia rack IDF consultorios

- 10 pares de fibra MM OM4 50/125
 - o 8 pares para enlazar los switches de core
 - o 2 pares de Backup
- 2 patch panel 12 puertos SC
- 20 puntos de fusión
- 8 patch cord 7 pies SC-LC OM4
- 1 certificación de todos los puntos de fibra

3.7. Infraestructura tecnológica de red

Para este subsistema se propone de forma general la solución adecuada a las necesidades de la Cooperativa expuestas en el punto

3.7.1. Requerimientos switching

Equipos a reusarse:

- 1 Switch Cisco WS-C4506-E CPMV-MATRIZ-CORE01
- 1 Switch Cisco WS-C3560 CPMV-MATRIZ-DIST01
- 1 Switch Cisco WS-C2960 CPMV-MATRIZ-ACC01
- 1 Switch Cisco WS-C2960 CPMV-MATRIZ-ACC02

Equipos requeridos y que deben ser adquiridos:

- 1 Switch Cisco WS-C4506-E CPMV-MATRIZ-CORE02
48 puertos Gigabit
- 1 Switch Cisco WS-C3560 CPMV-MATRIZ-DIST02
48 puertos gigabit
- 1 Switch Cisco WS-C2960 CPMV-MATRIZ-ACC03
48 puertos Gigabit
- 1 Switch Cisco WS-C2960 CPMV-MATRIZ-ACC04
48 Puertos Gigabit
- 24 Transceivers Cisco SFP 1000Base-SX FO MM

Dado que en la actualidad la cantidad de puertos presentes en los equipos cubren las necesidades de conectividad física, la adición de los equipos activos de red adicionales dotará de puertos adicionales que superan la cifra promedio de crecimiento de la red de 10% para un período de tres años.

3.7.2. Requerimientos routing

Equipos a reusarse:

- Firewall Gateprotect GPX-650
- Firewall Gateprotect GPA-500

3.7.3. Requerimientos red SAN

Reusados

- Storage IBM Storwize V3700
- No se reusa una tarjeta HBA PCIe 4x FC 4G Dual Port presente en el servidor HP DL380 G7 de Base de Datos Oracle 11gR2.

Requeridos

- 6 tarjetas HBA PCIe 4x FC 8G Single Port por servidor.
- 2 switches SAN marca Brocade modelo 300, con 24 puertos disponibles, 14 puertos licenciados con módulos SFP 8G MMC.

- Storage IBM Storwize V7000

3.7.4. Requerimientos de ancho de banda

De acuerdo a los técnicos de la Cooperativa el peso ponderado de tráfico de cada agencia que pasa por el switch de core y se distribuye a los distintos servicios está distribuido de la siguiente forma:

Equipos de cómputo hacia servidores:

- Tulcán 68,86%
- San Gabriel 10%
- Bolívar 4%
- Mira 4%
- Ibarra 15%
- Quito 15%
- Lago Agrio 4%

Por lo cual se infiere que el tráfico local es 68,86% el cual es un parámetro a tomar en cuenta para el cálculo de ancho de banda del switching local. El 31,14% restante correspondería a tráfico WAN que directamente afecta a los enlaces de datos con cada proveedor.

Telefonía hacia Central Asterisk Matriz

- Tulcán 51,72%
- San Gabriel 6,9%
- Bolívar 4,6%
- Mira 4,6%
- Ibarra 13,79%
- Quito 13,79%
- Lago Agrio 4,6%

De estos valores el 51,72% es tráfico local y el restante 48,28% es tráfico WAN.

El sistema de cámaras en cada agencia graba de manera local y se monitorea remotamente por lo que no pesa mayormente sobre el ancho de banda requerido como se puede apreciar en la Tabla 14.

Los requerimientos de ancho de banda quedarían definidos tal como se aprecia en las siguientes tablas:

Tabla 21.

Requerimiento de ancho banda.

TABULACIÓN DE ANCHO DE BANDA – MATRIZ TULCÁN						
DESCRIPCIÓN	MAX (Kb/s)		MIN (Kb/s)		AVERAGE (Kb/s)	
	INPUT	OUTPUT	INPUT	OUTPUT	INPUT	OUTPUT
Core Financiero	3,92	4,66	2,41	3,76	3,17	4,21
Base de Datos	738,84	7,30	458,08	4,65	59,85	5,98
Aplicaciones	625,00	3,12	427,00	592,00	526,00	1,86
Active Directory & APP Exteriores	765,00	181,00	159,00	154,00	462,00	167,50
Cámaras	1,46	62,61	1,36	58,31	1,41	60,46
TOTAL	2.134,21	258,70	1.047,85	812,72	1.052,42	240,00
TRAFICO LOCAL	1.469,62	178,14	721,55	559,64	724,70	165,27
TRAFICO WAN	664,59	80,56	326,30	253,08	327,72	74,74
TABULACIÓN DE ANCHO DE BANDA – MATRIZ TULCÁN						
DESCRIPCIÓN	MAX (Kb/s)		MIN (Kb/s)		AVERAGE (Kb/s)	
	INPUT	OUTPUT	INPUT	OUTPUT	INPUT	OUTPUT
Telefonía Asterisk	511,00	449,00	365,00	299,00	438,00	374,00
TRAFICO LOCAL	351,87	309,18	251,34	205,89	301,61	257,54
TRAFICO WAN	159,13	139,82	113,66	93,11	136,39	116,46
REQUERIMIENTOS DE ANCHO DE BANDA TOTAL SERVICIOS MAS TELEFONÍA - MATRIZ TULCÁN						

DESCRIPCIÓN	MAX (Kb/s)		MIN (Kb/s)		AVERAGE (Kb/s)	
	INPUT	OUTPUT	INPUT	OUTPUT	INPUT	OUTPUT
TRAFICO TOTAL LOCAL	1.821,49	487,32	972,89	765,53	1.026,30	422,80
TRAFICO TOTAL WAN	823,72	220,38	439,96	346,19	464,12	191,20
REQUERIMIENTOS DE ANCHO DE BANDA TOTAL SERVICIOS MAS TELEFONÍA - MATRIZ TULCÁN CRECIMIENTO 10% 3 AÑOS						
DESCRIPCIÓN	MAX (Kb/s)		MIN (Kb/s)		AVERAGE (Kb/s)	
	INPUT	OUTPUT	INPUT	OUTPUT	INPUT	OUTPUT
TRAFICO TOTAL LOCAL	2.003,64	536,05	1.070,18	842,08	1.128,93	465,08
TRAFICO TOTAL WAN	906,09	242,41	483,96	380,81	510,53	210,32

Estos resultados definen el ancho de banda que se deberá tener disponible para el crecimiento planificado.

La red LAN deberá tener una eficiencia de 2.003,64 Kbps (2 Mbps) si se toma como valor referencial el valor máximo de tráfico que ingresa. Dado que la red LAN está diseñada para usar Gigabit, no se tendrá inconvenientes con el tráfico local durante el tiempo planificado.

Los enlaces WAN hacia Matriz deberán tener una eficiencia de 906,09 Kbps (aprox. 1 Mbps) para satisfacer las necesidades del tráfico de servicios importantes como Base de Datos y demás. Actualmente se tienen valores de 6 Mbps, por lo cual no se tendrán problemas durante el período de tres años planificados.

El tráfico de Internet medido en el equipo Firewall de borde Gateprotect en ninguno de los casos supera los 7 Mbps, puesto que la navegación está muy restringida y únicamente se permite el acceso a páginas específicamente necesarias como entidades bancarias y órganos de control estatal. Debido a que el enlace principal utilizado es el de Telconet y se tienen 12 Mbps no hay necesidad de ampliarlo. El enlace de Internet de CNT es de 5 Mbps y se usa

exclusivamente para los servicios de banca en línea y correo electrónico, el consumo medido promedio es de 2,5 Mbps por lo cual tampoco se necesita ampliarlo.

3.8. Indicadores de Éxito

Dado que no se basará en un estándar generalmente aceptado, que permita medir el éxito del diseño y la posterior aplicación de la solución aquí propuesta, se recurrirá a los criterios que se expresan en la normativa de la SEPS, referente a la disponibilidad y continuidad del negocio.

- Disponibilidad, los cálculos se basarán en la cantidad de horas máximas que la Cooperativa puede estar sin operar, de acuerdo a las recomendaciones específicas dadas por la SEPS de 4 horas por evento en un mes. Este parámetro se obtiene de la siguiente fórmula:

$$\text{Disp} = \frac{\text{Ttot (horas)} - \text{Tmant (horas)}}{\text{Ttot (horas)}} \quad (\text{Ecuación 1})$$

De donde:

Disp: es el valor de la disponibilidad

Ttot: es el valor del tiempo total disponible para producir

Tmant: es el valor del tiempo de parada para soporte

Aplicando la fórmula anterior para un período estándar de 1 (UN) mes se obtiene que la disponibilidad que la SEPS sugiere para la Cooperativa es de 99.45%, lo cual es un valor no muy elevado considerando que la práctica mundial es acercarse a los 5 nueves (99,999%)

Este valor de disponibilidad (99,45%) será el que se exigirá a todo sistema tecnológico que incida directamente en la Continuidad del Negocio.

Por ejemplo, en el caso de los componentes fundamentales de la solución es decir los equipos Switch CISCO 4506E, se necesita saber su disponibilidad en

esa porción del diseño Jerárquico redundante, para lo cual se recurre a la fórmula generalmente aceptada de cálculo de disponibilidad conocidos datos de MTBF (Mean time between failure) y MTTR (Mean time to repair).

$$\text{Disp} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \quad (\text{Ecuación 2})$$

De donde:

Protocolo de gestión enlaces:	RSTP
Tiempo de convergencia:	10 seg. (MTTR)
MTBF de los switches:	710119 Horas (Tomado de la hoja de datos del equipo)
Disp:	99,99999722%

Del resultado inferior se infiere que la disponibilidad en ese componente de la infraestructura diseñada supera a la disponibilidad solicitada por la SEPS (99,45%)

Es importante conocer estos datos, MTBF se obtiene de las hojas de datos de cada equipo en las páginas web del fabricante. MTTR es un parámetro de tiempo medido que indica cuanto tiempo le toma a un equipo o servicio ser levantado, en el caso de los switches en redundancia ese tiempo corresponde al tiempo de convergencia del protocolo de gestión de enlaces redundantes RSTP ante un fallo.

Se puede aplicar este mismo criterio a todos los demás componentes del sistema y dado que los tiempos de convergencia o activación de la contingencia no supera los 15 minutos (MTTR) (Ejemplo cambio de Activo-Pasivo Base de Datos Oracle) el esquema diseñado se mantiene dentro de la disponibilidad esperada.

3.9. Análisis Técnico-Económico

La propuesta para la Cooperativa incluye la realización de un análisis técnico donde se puedan apreciar los costos que implica la aplicación de la Propuesta, se empieza tomando los resultados de los requerimientos de los puntos donde se especifican requerimientos y se asientan en la siguiente tabla:

*Tabla 22.*Tabla de costos implementación propuesta de rediseño infraestructura tecnológica de red.

Punto	Detalle	valor U	valor T
3.5.1.3.1.			
4	Soporte Oracle VM por servidor	600,00	2.400,00
3.5.1.1.1.			
12	Metros bandeja metálica 180x70 con división	27,00	324,00
12	Metros tapa bandeja metálica 180x70	5,00	60,00
3	Uniones con tapa plana 180mm	7,00	21,00
160	Certificación punto de red	5,00	800,00
1	Mano de obra	200,00	200,00
3.5.1.2.1. 3.6.1.			
300	Metros fibra MM OM4 50/125 10 pares	7,00	2.100,00
6	Patch panel ODF 12 puertos SC fibra	75,00	450,00
60	Certificación y fusión puntos de fibra	8,00	480,00
23	Patch cord 7 pies SC-LC OM4	9,00	207,00
4	Racks 180cm	950,00	3.800,00
1	Enrutamiento de la fibra	300,00	300,00
3.7.1.			
1	Switch Cisco WS-C4506-E 48 puertos	5.103,00	5.103,00
1	Switch Cisco WS-C3560G 48 puertos	1.813,00	1.813,00
1	Switch Cisco WS-C2960G 48 puertos	1.701,00	1.701,00
1	Switch Cisco WS-C2960G 48 puertos	1.701,00	1.701,00
24	Transceiver SFP 1000Base-SX FO MM	39,20	940,80
3.7.3.			
6	Tarjetas HBA PCIe FC 8G SP	69,93	419,58
2	Switch SAN Brocade 300 24 port	2.098,60	4.197,20
1	Storage IBM Storwize V7000 G1	6.500,00	6.500,00
		SUBTOTAL EQUIPOS DE RED	22.375,58
		TOTAL	33.517,58

Nota: Los equipos activos de red son de tipo Refurbished y han sido cotizados en www.amazon.com, www.ebay.com, www.oracle.com a los cuales se les ha aplicado un 40% que es el promedio de carga por imposición tributaria y trámites de importación.

No se ponderan valores para los Requerimientos del punto 3.4. Desarrollo del diseño lógico debido a que los técnicos del Departamento de TI de la Cooperativa se encargan de la implementación de componentes de software que se hacen necesarios.

No se presentan valores para los requerimientos de los subsistemas Arquitectura, Eléctrico y Mecánico del Centro de Datos, dado que no es el alcance del presente proyecto, sin embargo, los requerimientos se especifican para ofrecer una visión general de todas las mejoras posibles en el área de TI.

Como se desprende de los requerimientos manifestados por los técnicos del Departamento de TI durante las reuniones realizadas para establecer las Metas Técnicas y especificados en el punto 3.3.2. de este proyecto, la Cooperativa tiene una preferencia por equipamiento Remanufacturado, por lo cual los valores fueron obtenidos guiados por ese criterio.

Tal como el estudio interno de la Cooperativa indica que el precio de un equipo Remanufacturado puede obtener precios de hasta un 40% menos en relación a un equipo nuevo, el valor del Subtotal de Equipos Activos de Red de USD 22.375,58 representa un ahorro de USD 14.917,05 que la Entidad dejaría de pagar.

Con esta inversión la Cooperativa obtiene los resultados esperados en concordancia con el diseño propuesto en el presente capítulo.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Se realizó un levantamiento del estado actual tanto de la parte física y lógica de la infraestructura. Este levantamiento sirvió como línea base para el desarrollo de las Fases de Diseño.

La infraestructura física levantada reveló que se estaban realizando inversiones en equipamiento pasivo y activo, sin embargo, dichas inversiones no se realizaban de la manera adecuada o basados en un marco referencial. Se recurrió a las recomendaciones de los estándares ANSI EIA / TIA 942 y 568B para determinar las falencias, y proponer las soluciones. El cableado de fibra óptica vertical resultó insuficiente para poder establecer un esquema jerárquico de red.

El diseño de la nueva infraestructura de red fue realizado tomando en cuenta parámetros las recomendaciones de la SEPS, las cuales tienen como objetivo garantizar la continuidad del negocio al exigir redundancia en las funciones de red más importantes. Para esto, tal como se especificó previamente, se recurrió a las recomendaciones de los estándares de ANSI EIA / TIA 942, 568B para determinar la ruta a seguir en el diseño. Sin embargo, se hizo indispensable seguir un marco metodológico para el diseño técnico de la solución, este marco fue provisto por el Método Top-Down de Cisco, el cual proveyó un entorno lógico y escalable para definir los elementos de la propuesta.

Una parte importante del diseño de la solución es el establecimiento de la Arquitectura de Nube privada de Oracle, la cual, toma del recurso redundante de almacenamiento de la SAN, el recurso redundante y jerárquico de la LAN y lo converge hacia los servidores IBM y HP tanto en Matriz como en Agencias y provee HA (alta disponibilidad) para los servicios virtualizados que corren dentro del esquema y en los cuales se basa el giro del negocio.

El reuso de los equipos de infraestructura que cumplen con las características requeridas por el diseño propuesto y la adquisición de equipos necesarios de

tipo Refurbished, de acuerdo a la política interna de adquisiciones de la Cooperativa garantizan un ahorro considerable en la inversión que se debe realizar para mejorar la red.

La solución propuesta permitirá asegurar y mejorar el rendimiento y la seguridad de la red, lo que conlleva a mejorar la productividad de la Entidad, pues al cumplir con los requerimientos del diseño se garantiza el servicio a los socios que realizan depósitos o inversiones.

4.2.Recomendaciones

Se recomienda tomar en cuenta que el diseño debe ser escalable pues servirá como base para futuro crecimiento en la Cooperativa. Se recomienda la adopción de la Metodología Top-Down para el rediseño de la red de datos para todas mejoras tecnológicas que se hagan necesarias a nivel tecnológico conforme se van requiriendo.

Se recomienda la adquisición de varios equipos para cubrir las exigencias de la solución, tal como se especifican en los requerimientos del Capítulo 3.

Se recomienda brindar especial atención a los términos de los acuerdos SLA que se firmen con los proveedores de los equipos de tipo Refurbished.

Se recomienda que conforme llega a la madurez y posterior baja de los equipos activos de red y servidores, se evalúen nuevas tecnologías y en caso de considerar introducir las en el esquema diseñado, establecer ambientes de Prueba y Desarrollo, en cuyo caso se establecerá la completa compatibilidad y posteriormente serán puestas a Producción.

Se recomienda tomar en cuenta que al establecer un esquema de Nube privada de Oracle se abren oportunidades enormes en el ámbito de la Continuidad del Negocio, pues al convertirse a este esquema se puede optar por redundar la Nube local con la Nube pública Oracle o de otros proveedores de Nube con tecnologías estándar. La adopción de este esquema incluso

permite la no dependencia de la adquisición de servidores nuevos de manera constante.

REFERENCIAS

- ADC Telecommunications, Inc. (2008). *ADC's Data Center Optical Distribution Frame: The Data Center's Main Cross-Connect* (1a ed.). Minnesota, EEUU.
- Beasley, J., & Nilkaew, P. (2014). *Networking Essentials* (4a ed.). Indianapolis, EEUU: Pearson.
- Cisco Systems. (2017). Preguntas frecuentes sobre MPLS para principiantes. Recuperado el 10 de febrero de https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc1
- Doodley, M., & Rooney, T. (2017). *DNS Security Management (IEEE Press Series on Networks and Services Management)* (1a ed.). NY, EEUU: Wiley.
- Empson, S. (2013). *CCNA Routing and Switching Portable Command Guide* (3a ed.). Indianapolis, EEUU: Cisco Press.
- Graziani, R., & Johnson, A. (2016). *Introduction to Networks Companion Guide* (5a ed.). Indianapolis, EEUU: Cisco Press.
- Lippitt, M., & Smith, E. (2014). *Networked Storage Concepts and Protocols* (3a ed.). EEUU: EMC Techbooks.
- Microsoft Official Academic Course. (2014). *Administering Windows Server 2021 R2* (1a ed.). Garamond, EEUU: Wiley.
- Negus, C., & Bresnahan, C. (2015). *Linux Bible* (9a ed.). Somerset, EEUU: Wiley.
- Oliviero, A., & Woodward, B. (2014). *Cabling: The Complete Guide to Copper and Fiber-Optic Networking* (5a ed.). Indianapolis, EEUU: Sybex.

- Oppenheimer, P. (2010). *Top-Down Network Design* (3a ed.). Indianapolis, EEUU: Cisco Press.
- Oracle Corporation Inc. (2017). Arquitectura de Nube Oracle. Recuperado el 10 de febrero de <https://docs.oracle.com>
- Power Host. (2018). *Power Host Datacenter*. Recuperado el 10 de febrero de <http://www.powerhost.cl/datacenter>
- SBS. (2014, 09 02). Resolución JB-2014-3066. 1. Quito, Ecuador.
- Stallings, W. (2013). *Comunicaciones y Redes de Computadoras* (7a ed.). DF, México: Pearson México.
- Tanenbaum, A., & Boss, H. (2014). *Modern Operating Systems* (4a ed.). NJ, EEUU: Pearson.
- Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras* (5a ed.). DF, México: Pearson México.
- Telecommunications Industry Association. (2000). *Commercial Building Telecommunications Cabling Standard 568-B.3-2000*. NY, EEUU: TELECOMMUNICATIONS INDUSTRY ASSOCIATION Standards and Technology Department.
- Telecommunications Industry Association. (2001). *Commercial Building Telecommunications Cabling Standard 568-B.1-2001*. NY, EEUU: TELECOMMUNICATIONS INDUSTRY ASSOCIATION Standards and Technology Department.
- Telecommunications Industry Association. (2001). *Commercial Building Telecommunications Cabling Standard 568-B.2-2001*. NY, EEUU: TELECOMMUNICATIONS INDUSTRY ASSOCIATION Standards and Technology Department.

The Institute of Electrical and Electronics Engineers, Inc. (2014). *802 ® IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture* (2a ed.). NY, EEUU.

TIA. (2014). *Telecommunications Infrastructure TIA-942*. Arlington, EEUU: TELECOMMUNICATIONS INDUSTRY ASSOCIATION.

Universidad Central de Venezuela. (2018). *SABER UCV*. Recuperado el 10 de febrero de <http://saber.ucv.ve/bitstream/123456789/507/3/APENDICE-dianca%20tesis.pdf>

Zen, V. (2011). *Laboratori ed esercizi per MikroTik RouterOS* (1a ed.). Pordenone, Italia: MikroTik Press.

ANEXOS

ANEXO A

Resolución SBS JB-2014-3066

Junta Bancaria del Ecuador

RESOLUCIÓN JB-2014-3066

LA JUNTA BANCARIA

CONSIDERANDO:

Que en título X "De la gestión integral y control de riesgos", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo V "De la gestión del riesgo operativo";

Que la norma contiene una serie de disposiciones específicas para la implementación de medidas de seguridad en los diferentes canales electrónicos a través de los cuales brindan servicios a sus clientes las instituciones financieras controladas por la Superintendencia de Bancos y Seguros;

Que del seguimiento trimestral del nivel de cumplimiento de las disposiciones contenidas en el citado capítulo V "De la gestión del riesgo operativo"; y del análisis de los resultados de las supervisiones in situ que ha venido realizando la Subdirección de Riesgo Operativo, se ha establecido la necesidad de realizar una reforma al referido capítulo V, con el propósito de que las instituciones financieras incrementen las medidas de seguridad en los canales electrónicos, mejoren los controles de gestión de la tecnología de la información y comunicaciones y mejoren la gestión del riesgo operativo; incluir disposiciones específicas relativas a la continuidad de las operaciones del negocio y la gestión de la seguridad de la información; e, implementar medidas de seguridad que mitiguen los fraudes relacionados con los cajeros automáticos y coadyuven a determinar los causales de los mismos en los procesos investigativos; y,

En uso de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero,

RESUELVE:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar los siguientes cambios:

ARTÍCULO 1.- En el capítulo V "De la gestión del riesgo operativo", del título X "De la gestión y administración de riesgos", efectuar las siguientes reformas:

1. En todo el texto del capítulo V reemplazar la frase "... tecnología de información..." por "... tecnología de la información ...".
2. En el artículo 2, efectuar las siguientes reformas:
 - 2.1 Reemplazar el numeral 2.18, por el siguiente

ANEXO B

Manual CPMV Plan Continuidad del Negocio (Confidencial)

 <p>COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA"</p>	<p>1 Planificación y Control 1.2 Gestión en Riesgos 1.2.4 Plan de Continuidad del Negocio</p>	<p>Código: PG-PC-GR 1.2.4 Revisión: 01</p>
DESCRIPCION DEL SUBPROCESO		
<p>Denominación del Subproceso: 1.2.4 Plan de Continuidad del Negocio</p> <p>Objetivo: Elaborar el plan de continuidad del negocio y plan de contingencias.</p> <p>Alcance: Aplica a todas las oficinas operativas.</p> <p>Referencias: <u>Documentación Interna:</u> -Plan de Continuidad del Negocio <u>Documentación Externa:</u> N/A</p> <p>Responsabilidades: Responsable del proceso: Jefe de Riesgos Responsable de revisión: Comité de Riesgos Responsable de aprobación: Consejo de Administración</p> <p>Definiciones: SEPS: Superintendencia de Economía Popular y Solidaria PCN: Plan de continuidad del negocio. BIA: análisis de impacto del negocio.</p> <p>Entradas: -Procesos Críticos. -Matrices que identifican el impacto financiero. -Establecimiento de tiempo de reanudación -Identificación de factores de riesgo</p>		

ANEXO C

Manual de Administración de la Información, Sitio Alterno. (Confidencial)

 <p>COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" INSTRUMENTAL</p>	<p>3. Administración de la Información 3.1 Tecnología de la Información 3.1.14 Habilitar Sitio Alterno y Principal</p>	<p>Código: PA-AI-TI 3.1.14 Revisión: 00</p>
1.- DESCRIPCIÓN DEL SUBPROCESO		
<p>Denominación del Subproceso: 3.1.14 Habilitación del Sitio Alterno y Principal</p> <p>Objetivo: - Habilitar el sitio alternativo para casos de contingencias y retorno a las actividades en el sitio principal</p> <p>Alcance: Toda la Cooperativa.</p> <p>Referencias:</p> <ul style="list-style-type: none">- Manual de Oracle- Plan de Contingencias del Departamento de TI <p>Responsabilidades:</p> <p>Responsable del proceso :Jefe de TI</p> <p>Responsable de revisión: Jefe de Riesgos</p> <p>Responsable de aprobación: Consejo de Administración</p> <p>Definiciones:</p> <p>BDD.-Base de datos de la Cooperativa</p> <p>DBA.- Administrador de Base de Datos</p> <p>Stand by.- Servidor de backup o de replicación.</p> <p>Entradas</p> <ul style="list-style-type: none">- Todos los procesos de la Cooperativa <p>Proveedores:</p> <ul style="list-style-type: none">- Todos los procesos- Servicios de Terceros <p>Actividades del proceso</p> <ul style="list-style-type: none">- Verifica existencia de comunicaciones		
Pág. 1		

ANEXO D

Plan de Contingencias Cooperativa (Confidencial)

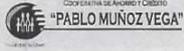
	Plan de Contingencias del Departamento de TI	Código	MA-AI-01
		Revisión	3
		Página	22

TABLA DE CONTENIDO

PLAN DE CONTINGENCIAS DEL DEPARTAMENTO DE TI.....	1
INTRODUCCIÓN	1
ALCANCE	1
OBJETIVOS	1
¿POR QUÉ DESARROLLAR UN PLAN DE CONTINGENCIAS?	2
ANÁLISIS DE RIESGO	2
MEDIDAS PREVENTIVAS	7
MEDIDAS PREVENTIVAS EN CUANTO A LAS AMENAZAS	7
MEDIDAS PREVENTIVAS EN RECURSOS DE TI	10
ROLES Y RESPONSABILIDADES	15
COMITÉ DE CONTINGENCIAS	15
EQUIPO DE CONTINGENCIAS.....	15
PERSONAL DE TI.....	15
PLAN DE RECUPERACION DE DESASTRES	15
ACCIONES FRENTE A LOS TIPOS DE RIESGO	18
CLASE DE RIESGO: INCENDIO O FUEGO – TERREMOTO O SISMO – DESTRUCCIÓN DE LA SALA DE SERVIDORES – DAÑO FÍSICO SERVIDOR BASE DE DATOS	18
PROCEDIMIENTO DURANTE OCURRA UN DESASTRE	19
PROCEDIMIENTO DESPUÉS DE OCURRIDO EL DESASTRE	19
ADMINISTRACIÓN Y CONTROL DEL DOCUMENTO	19
<i>Listas de distribución</i>	<i>19</i>
<i>Copias</i>	<i>19</i>
<i>Condiciones de seguridad</i>	<i>20</i>
<i>Responsables del mantenimiento</i>	<i>20</i>

CONFIDENCIAL

ANEXO E

Manual Administración de Riesgos. (Confidencial)

 COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" <small>INSTITUCIÓN FINANCIERA</small>	MANUAL DE LA ADMINISTRACIÓN INTEGRAL DE RIESGOS	Código	MA-GR-01
		Revisión	03
		Páginas	66

INDICE DE CONTENIDO

CAPÍTULO 1	5
1. Generalidades de Administración de Riesgos	5
1.1. Antecedentes.....	5
1.1.1. Misión de la Unidad de Administración Integral de Riesgos	5
1.2. Objetivos.....	5
1.3. Estructura para la Administración Integral de Riesgos	6
1.3.1. Estructura Organizacional.....	6
1.3.2. Comité de Administración Integral de Riesgos	7
1.3.3. Sesiones del Comité de Administración Integral de Riesgos	7
1.3.4. Unidad de Riesgos	8
1.4. Responsabilidades en la Administración de Riesgos	8
1.4.1. Consejo de Administración.....	8
1.4.2. Consejo de Vigilancia.....	8
1.4.3. Comité de Administración Integral de Riesgos	8
1.4.4. Representante Legal.....	9
1.4.5. Unidad de Riesgos	9
1.5. Políticas para la Administración Integral de Riesgos.....	10
1.6. Elementos para la Administración Integral de Riesgos.....	10
1.6.1. Proceso de la Administración Integral de Riesgos:.....	10
A) Identificación	10
B) Medición	11
C) Priorización.....	11
D) Control	11
E) Mitigación.....	11
F) Monitoreo.....	11
G) Comunicación	11
1.6.2. Tipos de Riesgo	11
A) Riesgo de Crédito.....	11
B) Riesgo de Liquidez	11
C) Riesgo de Mercado	11
D) Riesgo Operativo	12
E) Riesgo Legal	12
1.6.3. Procedimiento de La Administración Integral de Riesgos	12
A) Identificación	12
B) Medir.....	12
C) Priorizar	12
D) Controlar	12
E) Mitigar	12
F) Monitorear	13
G) Comunicar.....	13

ANEXO F

Configuración AAA TACACS+

Edición del archivo de configuración:

```
[root@tac.cpmv.fin.ec /]# nano -w /etc/tac_plus.conf
```

Modificación de:

```
#key = "your key here"
```

por:

```
key = "contraseñaCPMV"
```

Creación de una ACL:

```
acl = default {  
    permit = 192\168\113\.
```

Parámetros de cada host:

```
host = 192.168.113.7 {  
    prompt = "Ingrese su nombre de usuario y password Unix, Username: "
```

Parámetros específicos para el segmento 192.168.113.0/24:

```
group = admin {  
    login = PAM  
    acl = default  
    service = exec {  
        priv-lvl = 15  
    }  
}
```

```
cmd = username {  
    permit .*  
}  
cmd = enable {  
permit .*  
}  
cmd = show {  
    permit .*  
}  
cmd = exit {  
    permit .*  
}  
cmd = configure {  
    permit .*  
}  
cmd = interface {  
    permit .*  
}  
cmd = switchport {  
    permit .*
```

```
    }  
    cmd = description {  
        permit .*  
    }  
    cmd = no {  
        permit shutdown  
    }  
}
```

Creación de usuarios:

```
user = matrizadmin01 {  
    login = PAM  
    member = admin  
}
```

```
user = matrizadmin02 {  
    login = PAM  
    member = sysadmin  
}
```

Se habilita el acceso global de "enable" de cada equipo Cisco:

```
user = $enab15$ {  
}
```

Creación de los usuarios Unix:

```
[root@tac.cpmv.fin.ec etc]# useradd matrizadmin01 matrizadmin02  
[root@tac.cpmv.fin.ec etc]# passwd matrizadmin01  
[root@tac.cpmv.fin.ec etc]# passwd matrizadmin02
```

Inicio del demonio Tac+

```
[root@tac.cpmv.fin.ec etc]# /etc/init.d/tac_plus start
```

Adición del servicio al arranque de Linux:

```
[root@tac.cpmv.fin.ec etc]# chkconfig tac_plus on
```

ANEXO G

Configuración NTP

Instalación del demonio NTP:

```
# pkg_add -rv ntp
```

Actualización inicial desde servidor STRATUM1:

```
# ntpdate -v -b ntp-s1.pads.ufrj.br
```

Edición del archivo de configuración:

```
# nano -w /etc/rc.conf
    ntpdate_enable="YES"
    ntpdate_hosts="ntp-s1.pads.ufrj.br"
    restrict 192.168.113.0 mask 255.255.255.0 nomodify notrap nopeer
permiso de uso al segmento de switches y routers.
```

comprobación del estado del servicio de NTP:

```
# ntpq -pn localhost
```

se debe confirmar que se tiene "s2" (STRATUM2)

<agencia>-ntp01.cpmv.fin.ec: Servidor Virtual Oracle Linux 6.9 en cada agencia con demonio NTP configurado como servidor, colgado del servidor STRATUM2 en Matriz.

Configuración: Instalación del demonio

```
# yum -y install ntp ntpdate
```

Activación e inicio del demonio NTP:

```
# chkconfig ntpd on && service ntpd start
```

Prueba de funcionamiento colgado del servidor STRATUM2 de Matriz:

```
# ntpdate -u matriz-ntp01.cpmv.fin.ec
```

Edición del archivo de configuración:

```
# nano -w /etc/ntp.conf
restrict 192.168.123.0 mask 255.255.255.0 nomodify notrap
server 0. matriz-ntp01.cpmv.fin.ec iburst
```

Aplicación de los cambios:

```
# service ntpd restart
```

ANEXO H

Cotización construcción Centro de Datos, subsistemas.



Quito, 27 de octubre de 2017

Ing. Marcelo Caicedo
COOPERATIVA PABLO MUÑOZ VEGA

PROPUESTA IMPLEMENTACIÓN DATACENTER

1. PRESENTACIÓN

SP NETWORKS C.L. Es una empresa ecuatoriana dedicada a la provisión de servicios de consultoría orientada a la infraestructura de TI. Nuestra plantilla de profesionales es un equipo con sólida formación tecnológica y vasta experiencia, lo cual garantiza la calidad de nuestros productos.

2. LA PROPUESTA

A continuación se detalla la propuesta para la implementación de un Datacenter para la Agencia Matriz de la Cooperativa en la Ciudad de Tulcán.

La propuesta comprende la unificación del cableado de red actual Cat 6 con el nuevo Datacenter vía IDF con reflejos de puertos y el traslado de los equipos del Datacenter actual hacia las nuevas instalaciones.

DATACENTER BAJO NORMAS ANSI EIA/TIA 942-A Y ANSI EIA/TIA 568-B

Dimensiones proyectadas: 6m x 4m x 2,4m

SUBSISTEMA TELECOMUNICACIONES			
ORD	CANT	DESCRIPCION	
1	1	MDF cableado estructurado CAT 6a local entre racks, (patch panels de acceso y reflejo)	1.200,00
2	1	Cableado hacia IDF anterior (patch panels de reflejo)	2.507,00
3	4	Racks puerta malla 1720mm x 800mm x 1000mm (carga bruta 250 Kg)	4.400,00
4	1	Organizadores verticales y horizontales de cable	896,00
5	1	Patch cords de 3 y 7 pies.	1.830,00
6	1	Enrutamiento de backbone de cableado de datos superior con bandeja metálica galvanizada desde IDF	280,00
7	1	Enrutamiento de backbone de cableado de datos inferior con bandeja metálica galvanizada	700,00
8	1	Certificación de puntos de cableado CAT 6a	1.080,00
9	1	VALOR AGREGADO: Levantamiento de documentación (sistema de Networking integrado con la infraestructura previa)	
10	1	VALOR AGREGADO: Traslado y migración de equipos activos de red entre datacenter anterior y nuevo.	



SUBSISTEMA ARQUITECTURA			
11	1	Construcción 3 paredes laterales	3.360,00
12	1	Acabados arquitectónicos (pintura ignífuga, pintura exterior, etc.)	800,00
13	1	Piso técnico o falso 24m2 1250 lb carga bruta, 800lb carga dinámica, 700 lb carga caída libre (baldosas de pvc antiestático, acero 2mm, cemento)	4.500,00
14	1	Sistema de bases acero 30 cm alto	1.050,00
15	1	Rampa de acceso 100 X 120 X 30	600,00
16	1	Puerta metálica corta fuego 100 x 210 con sistema de seguridad y marco de metal, minilla antibandálica y brazo cierra puerta.	2.760,00
17	1	Sistema de control de incendios compatible con NFPA 75, central con visor y controles	10.120,00
18	1	Ventosa doble copa	95,00
19	1	Sistema de control de acceso biométrico incluida cerradura	1.320,00
20	1	Sistema de monitoreo CCTV IP Híbrido, 16 canales hib, 4 IP, 4 camaras IP domo IR, 12 meses grabacion	1.500,00
21	1	Sistema de control y gestion datacenter	3.240,00
SUBSISTEMA ELECTRICO			
22	1	Grupo electrógeno generador trifásico 22KVA, 85% de eficiencia al nivel de Tulcán 2.950 m. REQUIERE LA PROVISIÓN DE UN SITIO EN LA PLANTA BAJA	11.000,00
23	1	Cableado alimentación trifásica desde circuito de calle o medidor (requiere provisión de 3 fases)	2.200,00
24	1	Cableado acceso hasta tableros de transferencia y sistemas de A/C	1.600,00
25	1	Cableado interno alimentación 220v y 110v Datacenter dos circuitos (N+1)	2.100,00
26	1	Instalación malla de tierra, malla de alta frecuencia	3.100,00
27	1	Enrutamiento de backbone de cableado eléctrico con bandeja metálica galvanizada	600,00
28	1	Tableros TTA 220v y ByPASS acometida 3 FASES	4.560,00
29	1	TVSS (DPS)	500,00
30	8	PDU con medicion bifásico (dos por rack, uno por circuito)	2.240,00
31	2	UPS bifásico 10 KVA en redundancia N+1	6.800,00
32	1	Sistema de iluminación con paneles LED	910,00
SISTEMA DE PARARRAYOS PROVISTO POR LA COOPERATIVA			
SUBSISTEMA MECANICO			
33	1	Sistema de A/C de precisión 33 KBTU	16.000,00
34	1	Reubicación sistema anterior de A/C pasillo frío	600,00
35	1	Instalación de cañerías de sistemas de A/C con escalerilla metálica superior, condensador exterior.	300,00
36	1	Sistema de detección de incendio (sensores)	INC ORD 17
37	1	Sistema de almacenamiento y distribución agente compatible con NFPA 2001 (Bombona con FM200 o Novec 1230 tubería negra y sprinklers)	INC ORD 17
38	1	KVM USB 8 puertos con Monitor	1.800,00
39	1	FISCALIZACIÓN DATACENTER (CERTIFICADORA SGS)	10.000,00
El valor del proyecto llave en mano es de			106.548,00

GLOSARIO

Acontecimientos humanos: catástrofes artificiales, incluyendo, huelga general económica, el terrorismo (ecológico, cibernético, nuclear, biológicos, químicos), el sabotaje, la toma de rehenes, los disturbios civiles, ataque enemigo, el incendio, la histeria de masas, eventos especiales, accidentales.

Adaptador: Un dispositivo que es cualquiera o todos de los siguientes numerales: (1) diferentes tamaños o tipos de jack para conectarse con uno u otro o para conectarse a una toma de telecomunicaciones, (2) reordenamiento de pistas, (3) grandes cables con numerosos conductores que se despliegan en grupos más pequeños de conductores, (4) interconexión entre cables, (5) voltaje limitado y/ o polaridad y/ o rectificadores de conversión DC.

Administración de cables: Las estructuras físicas vinculadas a y / o dentro de armarios y bastidores para proporcionar horizontal y vías verticales para guiar y administrar la infraestructura de cableado. Al igual que en las vías que se definen en la norma TIA-569-B, las vías horizontales y verticales dentro de armarios y bastidores guía infraestructura de cableado de una manera diseñada y ordenada cuando se conecta a los equipos y la conectividad alojada dentro de los bastidores y / o gabinetes.

Agente limpio: Un extintor de incendios eléctricamente no conductor, volátiles o gaseoso que no deja residuos en la evaporación, y por tanto no se hace necesario ninguna limpieza después de su aplicación.

Aislamiento: Una estrategia de diseño que mitiga el riesgo de daño concurrente a algunos componentes en una instalación utilizando física, lógica, o sistemas de separación del sistema incluso físicos.

Alarma: Una señal visual y/o acústica que indica la presencia de calor, humo, otros productos de combustión o sistemas de mal funcionamiento o fallo de la seguridad dentro de una instalación.

Amenazas: Son todos los agentes que causan daño. Las amenazas se clasifican comúnmente como originarias de las temperaturas extremas, líquidos, gases, proyectiles, organismos, movimientos, o anomalías energéticas.

Área de distribución de equipos: El espacio de la sala de equipos de tecnología informática ocupado por racks o gabinetes de equipos.

Área de distribución horizontal (HDA): Un espacio en una sala de cómputo donde se encuentra una conexión cruzada horizontal y puede incluir switches LAN, switches SAN y teclado / vídeo / ratón (KVM) para el equipo situado en las zonas de distribución de equipos.

Área de distribución de la zona (ZDA): Un espacio en una sala de cómputo donde se encuentra una salida de la zona o un punto de consolidación.

Banco de cargas: Un dispositivo para simular un equipo real. El banco de carga es una carga eléctrica que está conectada a los sistemas de PDU, sistemas UPS o generadores en situaciones de prueba de carga.

Bandeja de cables: Una escalera, ranura, fondo sólido, o un sistema de pista de rodadura a un canal destinado, pero no limitado, al apoyo de cables.

Barra de tierra eléctrica principal (MEGB): Es la barra principal de puesta a tierra en el edificio, el conductor eléctrico de puesta a tierra de servicio del electrodo (s) y demás conductores a tierra y unidos están interconectados para establecer la ubicación principal de potencial para el edificio.

Cable: Un conjunto de uno o más conductores aislados o fibras ópticas, dentro de un aislante que se envuelven.

Cable ascendente: Cable de comunicaciones que se utiliza para implementar redes troncales ubicadas en los mismos o diferentes plantas.

Cable de conexión (patch cord): Una longitud de cable con un enchufe en uno o ambos extremos.

Cable de fibra óptica: Un conjunto que consta de una o más fibras ópticas.

Cable de rack: Diseñado y fabricado para su distribución vía horizontal y cableado en el interior dentro de las habitaciones de MDF o TR.

Cableado horizontal: (1) El cableado que incluye la toma de telecomunicaciones / conector y la conexión cruzada horizontal. (2) El cableado que incluye la salida del sistema de automatización del edificio o la primera terminación mecánica del punto de conexión horizontal y la conexión cruzada horizontal. (3) en un centro de datos, cableado horizontal es el cableado de la conexión cruzada horizontal (en el área de distribución principal o el área de distribución horizontal) a la salida de la zona de distribución de equipo o área de distribución de la zona.

Cableado centralizado: Una configuración de cableado del área de trabajo a una conexión cruzada usando extracción centralizada a través de cables, una interconexión o empalme en el cuarto de telecomunicaciones.

Cableado externo (OSP): Sistema de comunicaciones fuera de los edificios (conducto generalmente subterráneo y bóvedas, exterior / subterráneo, aéreos y enterrada y cable).

Cableado interior: Sistema de comunicaciones dentro de un edificio (cable, fibra óptica, cable coaxial, bastidores de equipos, y puntos de información).

Cableado vertical (Backbone): (1) Una instalación (vía, cable, conductores) entre cualquiera de los siguientes espacios: cuartos de telecomunicaciones (TRS), terminales comunes de piso que sirven a las instalaciones de entrada, cuarto de máquinas y cuarto de equipos comunes.(2) En un centro de datos, una instalación (vía, cable, conductores) entre cualquiera de los siguientes espacios: entrada habitaciones o espacios, principales áreas de distribución, áreas de distribución horizontal y cuarto de telecomunicaciones (TR).

Calor (protección contra incendios): Forma de energía que se manifiesta por alta temperatura.

Canal: El camino de transmisión de extremo a extremo entre dos puntos en los que el equipo específico de la aplicación es conectado.

Capa de acceso: La capa de acceso es el punto en el que los usuarios finales son permitidos ingresar a la red. En el ambiente de LAN, este punto de conexión es típicamente un puerto Ethernet conmutado que se le asigna a la VLAN.

Capa de distribución: Colección de switches entre la capa de núcleo y acceso. Los Switches de distribución pueden ser un switch y la combinación de enrutador externo, o un switch de múltiples capas.

Capacidad Nominal N: Es la capacidad de diseño del Data Center, la máxima capacidad a la que puede llegar.

Chaqueta del cable: Una cubierta sobre el conjunto de fibra óptica o el conductor que puede incluir uno o algunas fibras metálicas, resistencia, o chaquetas.

Centro de Datos: Un edificio o parte de un edificio cuya función principal es albergar un cuarto de cómputo y de soporte. Área que incluye el cuarto de Cómputo, Sala de Operaciones (NOC), Salas de Apoyo Eléctrico y Mecánico, Sala de Almacenamiento, Oficinas de soporte del Data Center, Cuartos de Telecomunicaciones sirviendo al Centro de Datos, Zona de Ingreso y Seguridad. Comúnmente conocido como "Data Center".

Cliente: (1) Un cliente interno o externo. (2) Una entidad de hardware o software, como en "cliente / servidor."

Conexión cruzada intermedia: Una conexión cruzada entre el primer nivel y segundo nivel de cableado vertical. También se conoce como la conexión cruzada horizontal (HC).

Conexión cruzada principal (MC): Un área de conexión cruzada de cables troncales de primer nivel, los cables de entrada y los cables de equipos

Conductor para telecomunicaciones (BCT, bonding conductor for telecommunications): Conductor que interconecta las infraestructuras de telecomunicaciones a los servicios de equipo del edificio (fuentes de poder, tierras).

Conectividad: Los paneles de conexión, cableado, conectores, y la gestión de cable utilizado para crear y mantener la electricidad y circuitos ópticos.

Control de calidad: Uno de las cuatro estrategias principales para el aumento de la fiabilidad, garantizando que la alta calidad está diseñada y puesta en práctica en la instalación, reduciendo así el riesgo de tiempo de inactividad debido a errores de instalación nuevos o desgaste prematuro.

Conexión cruzada horizontal (HC): Una conexión cruzada del cableado horizontal a otros cables (por ejemplo, horizontal, cableado principal, equipos).

Criticidad: La importancia relativa de una función o proceso, midiendo las consecuencias de su incumplimiento o incapacidad para funcionar.

Cuarto de entrada o espacio (telecomunicaciones): Un espacio en el que se lleva a cabo la unión entre las instalaciones inter o intra-red troncales de telecomunicaciones en el edificio.

Cuarto de equipos (telecomunicaciones): Un espacio centralizado con control ambiental que sirve a las telecomunicaciones y equipo de procesamiento de datos

Cuarto de máquinas: Un espacio cerrado que sirve para las necesidades de los sistemas mecánicos de edificios.

Cuarto de equipos de TI (Cuarto de Cómputo): Un espacio arquitectónico cuya función principal es la de dar cabida a equipos de procesamiento de datos.

Detección, (protección contra incendios): Los medios para detectar la presencia de calor, humo u otras partículas o productos de combustión.

Disponibilidad: (1) la probabilidad de que un sistema o componente está funcionando en un momento determinado; (2) la relación del tiempo total de un sistema o componente es funcionalmente dividida por la longitud del intervalo de tiempo para el que se determina la disponibilidad.

Distribuidor Principal (MD): (CENELEC EN 50173-5 e ISO / IEC 24764) distribuidores que se utilizan para realizar conexiones entre los principales subsistemas del subsistema de cableado de distribución, del subsistema red de cableado y cableado especificados en la norma ISO / IEC 11801 y EN 50173-1 y equipos activos. Equivalente a la conexión cruzada principal en ANSI/TIA-942.

Dominio: Una porción del árbol de jerarquía que se refiere a grupos generales de redes basadas en tipo de organización o la geografía.

Eficiencia de la infraestructura del centro de datos (DCIE): Un indicador de eficiencia para un centro de datos completo calculado como la reciprocidad de PUE: $\text{Potencia 1/PUE} = \text{equipo de TI} / \text{Potencia total facilidad} \times 100\%$.

Enlace (Link): Una vía de transmisión entre dos puntos, sin incluir los equipos terminales, cables del área de trabajo, y el equipo cables.

Enlace ascendente (uplinks): En referencia a la informática, una conexión entre capas en una red jerárquica. Uplinks son enlaces ópticos de fibra generalmente configurados en puertos Gigabit Ethernet (GE). (Uplinks Fast Ethernet también se pueden configurar utilizando fibra óptica o trenzado balanceado de par trenzado). Un enlace ascendente puede ser referido como una troncal.

Ensamblaje de cables troncales: Constan de dos o más enlaces de cableado, preconectorizado, del mismo o de diferentes tipos o categorías que bien pueden ser cubiertos por un aislante en general o las unidades individuales pueden estar unidos de forma continua para formar una sola unidad.

Equipo de cable: Un conjunto de cables o el cable utilizado para conectar el equipo al cableado horizontal o principal.

Equipos de tecnología de información (TI): Equipos de procesamiento de datos dentro del cuarto de cómputo.

Espacio de telecomunicaciones: Un área utilizada para alojar la instalación y la terminación de las telecomunicaciones equipos y cableado.

Espacios U cero: Espacio para accesorios de montaje en gabinetes que no consume ningún montaje en el espacio del rack, por lo general están entre el panel lateral y los lados de los equipos montados en el espacio de montaje unidad de rack.

Etiqueta: Un trozo de papel u otro material que se sujeta a algo y da información predefinida al respecto. Describe su identidad, trayectoria, ubicación o cualquier otra información importante sobre el producto o material.

Eventos naturales: Los desastres naturales, como la sequía, incendios, aludes, la nieve / hielo / granizo, tsunamis, huracán / tormentas tropicales, huracanes / tifones / ciclones, calor extremo / frío, agua de inundaciones, erupciones volcánicas, tornados, deslizamientos de tierra / alud de lodo, tormenta de polvo / arena, y la tormenta eléctrica.

Eventos tecnológicos: los desastres tecnológicos, incluyendo la liberación de materiales peligrosos, explosión / fuego, transporte accidente, el edificio / el derrumbamiento de estructuras, corte de energía / servicios públicos, la contaminación atmosférica extrema, accidente radiológico, rotura de la presa /

dique, la escasez de combustible / recurso, huelga, interrupción del negocio, colapso financiero, y la falta de comunicación.

Fibra multimodo: Una fibra óptica que lleva muchos caminos (modos) de la luz.

Fibra óptica: Cualquier filamento hecho de materiales dieléctricos que guía la luz.

Fibra óptica monomodo: Una fibra óptica que lleva sólo un camino (modo) de luz.

Fibra oscura o desocupada: Cable de fibra óptica instalada no utilizada.

Fiscalización del Edificio: En el sentido más amplio, un proceso para lograr, verificar y documentar que el rendimiento de un edificio y sus diferentes sistemas cumplen la intención del diseño y el dueño y las necesidades operativas de los ocupantes. El proceso ideal se extiende a través de todas las fases de un proyecto, desde el concepto de la ocupación y las operaciones.

Fuente de alimentación ininterrumpida (UPS): Un sistema que proporciona un suministro continuo de energía a una carga, utilizando la energía almacenada cuando la fuente normal de energía no está disponible o es de calidad aceptable, y hasta que la energía almacenada es utilizada por completo o la fuente normal de energía vuelve a una calidad aceptable, o lo que ocurra primero.

Gabinete (telecomunicaciones): Un recinto con una tapa con bisagra que se utiliza para las terminaciones de cables de telecomunicaciones, cableado y dispositivos de conexión.

Gestión del riesgo: El proceso de identificación de riesgos y el desarrollo de estrategias y las tácticas necesarias para eliminar, mitigar o gestionarlos.

