# ESCUELA POLITÉCNICA NACIONAL

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

## DISEÑO DE LA INFRAESTRUCTURA DE COMUNICACIONES DE VOZ, DATOS Y VIDEO PARA EL PPA (PROGRAMA DE PROVISIÓN DE ALIMENTOS)

**PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN**

**EDISON XAVIER GUAMBUGUETE GUAMÁN**
edison_xavier123@hotmail.com

**Director: ING. FERNANDO FLORES CIFUENTES**
fflores@mailfie.epn.edu.ec

**Quito, Enero 2012**

# DECLARACIÓN

Yo, Edison Xavier Guambuguete Guamán, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

**EDISON XAVIER GUAMBUGUETE GUAMÁN**

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Edison Xavier Guambuguete Guamán, bajo mi supervisión.

**Ing. Fernando Flores Cifuentes**

**DIRECTOR DEL PROYECTO**

# AGRADECIMIENTOS

*A Dios por todas sus bendiciones que me ha concedido durante el transcurso de toda mi vida y por la fortuna que me dio al ser parte de una gran familia y contar con el respaldo de grandes amigos.*

*A mi madre María del Carmen y padre Ramiro que siempre me han apoyado y han confiado en mí, los cuales me han inculcado la constancia, la dedicación, la responsabilidad y sobre todo, a dar todo para lograr mis objetivos y no darme por vencido ni en las peores circunstancias.*

*A mamita July, un ejemplo de mujer luchadora, trabajadora e inteligente que siempre me ha bendecido y guiado desde niño.*

*A mis hermanos y sobrinos, Alex, Carlitos, Daniela, David, Fernando, Stefy los cuales, aún siendo pequeños me enseñan a ver la felicidad en las cosas más simples que quizás antes no las tomaba en cuenta.*

*A mis hermanas, Mafer, Anita, Vanessa con las que crecí y añoramos años, gracias, mil gracias por estar siempre a mi lado.*

*A mis ñaños Lucy, Luis, Aníbal, Pablo, Juan Carlos por su apoyo incondicional durante todo el transcurso de mi vida y por enseñarme con su ejemplo a superarme y ser cada vez una mejor persona.*

*A mis grandes amigos, con los cuales se compartió grandes momentos de la vida politécnica y con los cuales nos seguiremos apoyando de la misma manera como lo hicimos en clases.*

*A mis profesores por su guía y enseñanzas para ser un profesional con amplios conocimientos y ética, en especial al Ing. Fernando Flores por su guía en el desarrollo de mi proyecto de titulación.*

## DEDICATORIA

*Para toda mi familia, en especial a mi madre que siempre me ha apoyado y por la cual seguiré luchando para ser cada día una mejor persona.*

***Edison Xavier***

# ÍNDICE DE CONTENIDO

# ÍNDICE DE FIGURAS

**CAPÍTULO I: FUNDAMENTOS TEÓRICOS**



**CAPÍTULO II: ANÁLISIS DE LA SITUACIÓN ACTUAL**

**CAPÍTULO III: DISEÑO DE LA INFRAESTRUCTURA DE RED**



**CAPÍTULO IV: IMPLEMENTACION DEL SISTEMA DE CABLEADO ESTRUCTURADO Y PRUEBAS DE LA INFRAESTRUCTURA DE RED**

# ÍNDICE DE TABLAS

**CAPÍTULO IV: IMPLEMENTACION DEL SISTEMA DE CABLEADO ESTRUCTURADO Y PRUEBAS DE LA INFRAESTRUCTURA DE RED**



**CAPÍTULO V: COSTO REFERENCIAL DE LA SOLUCIÓN**

# ANEXOS

# RESUMEN

En el presente proyecto se presenta el diseño de una solución completa de la infraestructura de comunicaciones de voz, datos y video para el Programa de Provisión de Alimentos (PPA), el cual se ha basado en el estudio de la situación actual de Programa en cuanto a usuarios, recursos, servicios y aplicaciones con los cuales deberá contar en las nuevas instalaciones.

En el primer capítulo se describen los fundamentos teóricos en los cuales de basa el desarrollo del proyecto. En el segundo capítulo se realiza un análisis de la situación actual del PPA como parte de la infraestructura de comunicaciones del Ministerio de Inclusión Económica y Social (MIES), el cual nos permita identificar los requerimientos en cuanto a recursos, servicios y aplicaciones necesarios para el desarrollo de las actividades del PPA en las nuevas instalaciones.

En el tercer capítulo, en base a los requerimientos analizados se diseña la infraestructura de comunicaciones. El proyecto incluye el diseño del Sistema de Cableado Estructurado, red LAN, red WLAN, además se toma en cuenta que la infraestructura de comunicaciones deberá soportar servicios en tiempo real y sobre todo voz sobre IP. Se dará una opción de los servicios Intranet usando Software Libre. Finalmente se realiza un análisis de riesgos de los activos informáticos y se realiza recomendaciones para resguardar dicha información.

En el cuarto capítulo se realiza la implementación del Sistema de Cableado Estructurado en dónde se enfoca en el proceso de certificación, además se realiza el prototipo del *datacenter* con todos los servicios Intranet, así como seguridad perimetral para el desarrollo de las actividades del PPA.

En el quinto capítulo se calcula el costo referencial de la solución, tomando en cuenta costos recurrentes y no recurrentes y se analizará la rentabilidad del proyecto. Finalmente se realizarán las conclusiones y recomendaciones para el mantenimiento de la infraestructura de comunicaciones diseñada.

# PRESENTACIÓN

Las TICs en grandes, pequeñas y medianas empresas tanto privadas como gubernamentales están teniendo gran trascendencia en su desarrollo y en el cumplimiento de metas de las mismas. Las TICs han hecho que las empresas no tengan fronteras y puedan exponer sus productos y servicios ante el mundo.

El Programa de Provisión de Alimentos al ser una institución gubernamental se encuentra en la necesidad de contar con una infraestructura de comunicaciones unificadas de voz, datos y video que le permitan desarrollar sus actividades con los recursos, servicios y aplicaciones suficientes.

El PPA desde sus inicios ha sido uno de los Programas Sociales más activo del gobierno actual, fue el creador de las ferias inclusivas, en la cual permiten que pequeños productores se asocien y se conviertan en proveedores de alimentos para el Estado. Además el PPA trabaja en conjunto con todos los Programas Sociales como el INFA (Instituto de la Niñez y la Familia), IEPS (Instituto Nacional de Economía Popular y Solidaria), PAE (Programa Aliméntate Ecuador), entre otros en la provisión de alimentos.

El importante aporte del PPA al Estado ha hecho que el Programa crezca de forma exponencial, creando la necesidad de buscar un lugar más amplio donde desarrolle sus actividades contando con una infraestructura de red, servicios y aplicaciones que le permitan desarrollar sus actividades.

# CAPÍTULO I

# 1. FUNDAMENTOS TEÓRICOS

## 1.1. SISTEMA DE CABLEADO ESTRUCTURADO[1][2]

El Sistema de Cableado Estructurado es un enfoque sistemático del cableado de voz, datos y video de forma organizada, basándose en estándares que faciliten su administración y garanticen la efectividad y eficiencia del mismo.

El Sistema de Cableado Estructurado permite dar una solución completa de conectividad en redes de información basándose en estándares y teniendo en cuenta que admita tecnologías actuales y futuras que garanticen el rendimiento y confiabilidad del sistema.

### 1.1.1. ESTÁNDARES DEL SISTEMA DE CABLEADO ESTRUCTURADO

Los estándares más comunes en los que se basa el Sistema de Cableado Estructurado son propuestos por la TIA (Asociación de la Industria de las Telecomunicaciones), EIA (Asociación de Industrias de Electrónica) las cuales se encuentran acreditadas por ANSI (Instituto Nacional Americano de Normalización). Las normas más utilizadas son:

#### 1.1.1.1. ANSI/TIA/EIA-568-C

Este estándar reemplaza al estándar ANSI/TIA/EIA 568 B, se encuentra aprobado por la ANSI desde alrededor de 3 años. Se debe tener en cuenta que la vida útil de los documentos reconocidos por ANSI es de 5 años. Los cambios más significativos son:

Todas las enmiendas realizadas en la norma ANSI/TIA/EIA 568 B son compiladas en un solo documento en el nuevo estándar.

El estándar ANSI/TIA/EIA 568 B no especifica los requerimientos para un Sistema de Cableado Estructurado en sitios poco comunes como estadios, aeropuertos, etc, por lo cual ANSI/TIA/EIA 568 B.1 fue tomado como estándar por omisión. En el estándar ANSI/TIA/EIA 568 C se desarrolla un documento genérico para uso cuando un estándar específico no esté disponible, el estándar es ANSI/TIA/EIA 568 C.0.

#### 1.1.1.2. ANSI/TIA/EIA-568-C.0

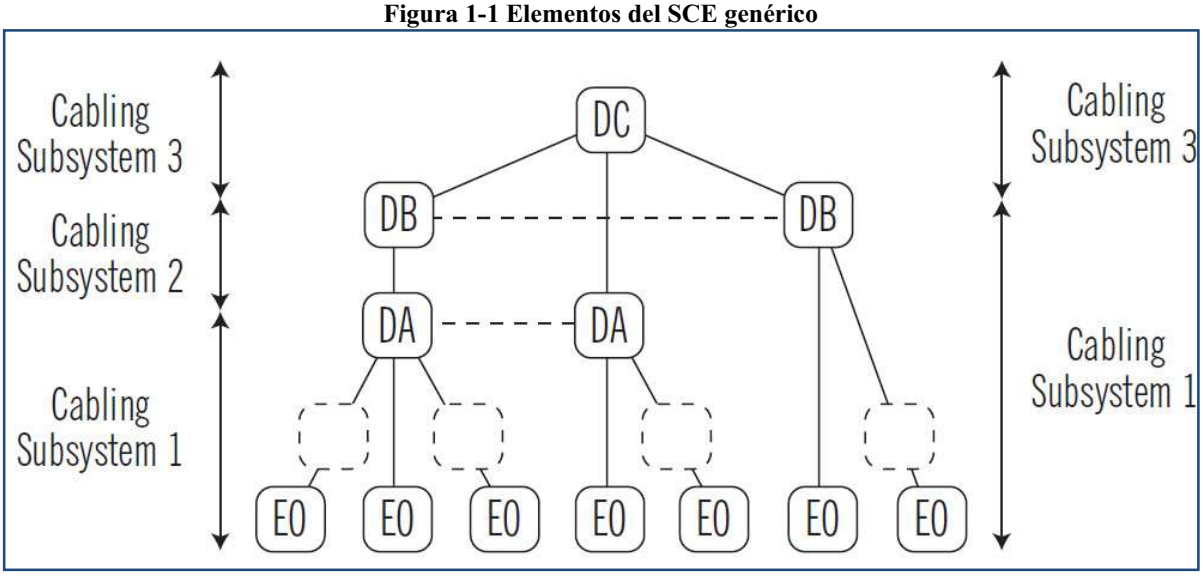
El objetivo de esta norma es la planificación e instalación de un Sistema de Cableado Estructurado genérico que se acople a todo tipo de instalaciones. La norma especifica los requisitos para la estructura del cableado, topologías, distancias, instalación, pruebas de rendimiento y el cableado a través de fibra óptica.

Esta norma reemplaza a ANSI/TIA/EIA-568-B.1 y sus enmiendas.

La nomenclatura de esta norma cambia. En la Figura 1-1 se muestra los elementos funcionales de un Sistema de Cableado Estructurado bajo la norma ANSI/TIA/EIA-568-C.0 donde a los segmentos de cableado se los llama “Subsistemas de Cableado”, a los puntos de conexión se los llama “Distribuidor” y al distribuidor final se lo llama “Salida de Equipos”.

- Distribuidor C (DC) representa la conexión cruzada principal (MC).
- Distribuidor B (DB) representa la conexión cruzada intermedia (IC).
- Distribuidor A (DA) representa la conexión cruzada horizontal (HC).
- El equipo de salida (EO) representa la toma de telecomunicaciones y el conector.
- Cableado opcional - - - - - - - - -
- Punto de consolidación

**Figura 1-1 Elementos del SCE genérico**




La norma establece una topología tipo estrella dónde no puede haber más de dos distribuidores entre el DC y EO. La tensión del cable par trenzado balanceado no debe exceder de 110N (25 libras-fuerza) durante la instalación, el interior del radio de curvatura mínimo será de cuatro veces el diámetro del cable.

#### 1.1.1.3. ANSI/TIA/EIA-568-C.1

El objetivo y ámbito de esta norma es la planificación y la instalación de un Sistema de Cableado Estructurado en edificios comerciales en un ambiente de campus. Es un estándar que da la facilidad de implementar un SCE multiproducto y multifabricante, además el estándar es compatible con una amplia gama de aplicaciones como voz, datos y video.

Esta norma reemplaza a ANSI/TIA/EIA-568-B.1 y sus enmiendas. Los cambios más significativos son:

- Incluye como SCE reconocidos a la Categoría 6A.
- Incluye el cableado de fibra óptica multimodo 850 nm de 50/125 um.
- El cableado STP de 150 ohmios, el cableado categoría 5, el cableado coaxial de 50 ohmios y 75 ohmios ya no son medios reconocidos.

Este estándar no cambia de nomenclatura y continúa con los subsistemas; Entrada de Servicios, Cuarto de Equipos, Cuarto de Telecomunicaciones, Cableado Vertical, Cableado Horizontal y Área de trabajo.

#### 1.1.1.4. ANSI/TIA/EIA-568-C.2

El objetivo de esta norma es especificar el cable y sus componentes para cable par trenzado balanceado de cobre categoría 3, categoría 5E, categoría 6 y categoría 6A.

Las categorías reconocidas son:

- **Categoría 3**.- cable UTP de 100 ohmios y componentes de hasta 16 MHz de ancho de banda.
- **Categoría 5e**.- cable UTP de 100 ohmios y componentes de hasta 100 MHz de ancho de banda.
- **Categoría 6**.- cable UTP de 100 ohmios y componentes de hasta 250 MHz de ancho de banda.
- **Categoría 6A**.- cable UTP de 100 ohmios y componentes de hasta 500 MHz de ancho de banda. Adicionalmente cumple con requerimientos de *alien crosstalk* para soportar sistemas de transmisión 10GBASE-T.

#### 1.1.1.5. ANSI/TIA/EIA-568-C.3

El objetivo de esta norma es especificar el rendimiento del medio de transmisión y sus componentes para un Sistema de Cableado Estructurado de fibra óptica.

Esta norma reemplaza a ANSI/TIA/EIA-568-B.3.

En la Tabla 1-1 se detalla los parámetros de rendimiento de la fibra óptica, en dónde se las nombra con sus nuevas nomenclaturas

**Tabla 1-1[1] Parámetros de rendimiento de fibra óptica**

Optical Fiber Cabling Systems

| Optical Fiber and Cable Type[2] | Wavelength (nm) | Maximum Attenuation (dB/km) | Minimum Overfilled Modal Bandwidth-Length Product (MHz • km)[1] | Minimum Effective Modal Bandwidth-Length Product (MHz • km)[1] |
|---|---|---|---|---|
| 62.5/125 μm | | | | |
| Multimode | 850 | 3.5 | 200 | Not required |
| TIA 492AAAA (OM1) | 1300 | 1.5 | 500 | Not required |
| 50/125 μm | | | | |
| Multimode | 850 | 3.5 | 500 | Not required |
| TIA 492AAAB (OM2) | 1300 | 1.5 | 500 | Not required |
| 850-nm | | | | |
| Laser-Optimized | | | | |
| 50/125 μm Multimode | 850 | 3.5 | 1,500 | 2,000 |
| TIA 492AAAC (OM3) | 1300 | 1.5 | 500 | Not required |
| Single-Mode | | | | |
| Indoor-Outdoor | | | | |
| TIA 492CAAA (OS1) | 1310 | 0.5 | - | - |
| TIA 492CAAB (OS2)[3] | 1550 | 0.5 | - | - |
| Single-Mode | | | | |
| Inside Plant | | | | |
| TIA 492CAAA (OS1) | 1310 | 1.0 | - | - |
| TIA 492CAAB (OS2)[3] | 1550 | 1.0 | - | - |
| Single-Mode | | | | |
| Outside Plant | | | | |
| TIA 492CAAA (OS1) | 1310 | 0.5 | - | - |
| TIA 492CAAB (OS2)[3] | 1550 | 0.5 | - | - |

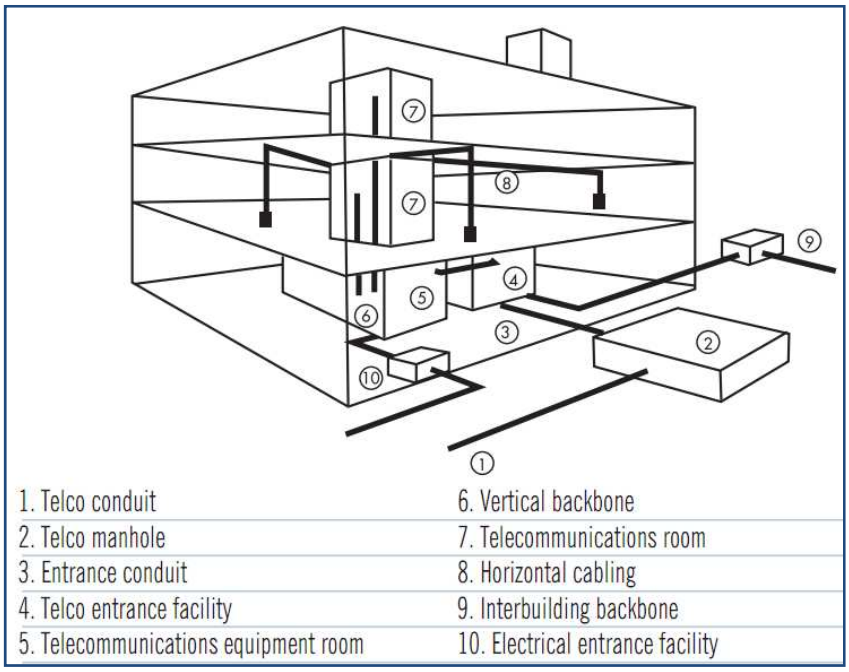
#### 1.1.1.6. ANSI/TIA/EIA-569-B

El estándar ANSI/TIA/EIA-569-B especifica las rutas y espacios para telecomunicaciones en edificios comerciales, estandarizando las prácticas de diseño y construcción de rutas de cableado horizontal, cableado vertical, área de trabajo, cuarto de equipos, cuarto de telecomunicaciones y acometida que garantice la operatividad, flexibilidad, administración y tiempo de vida de las rutas y espacios en Sistemas de Cableado Estructurado de voz, datos y video.

La Figura 1-2 muestra las rutas y espacios del cableado horizontal y vertical.

[1] Tabla tomada de: http://www.anixter.com/AXECOM/AXEDocLib.nsf/0/61vkiffo/$file/sec_14.pdf?openelement

**Figura 1-2 Rutas y espacios de cableado horizontal y vertical**




#### 1.1.1.7. ANSI/TIA/EIA 606 A

Especifica criterios de administración del Sistema de Cableado Estructurado proporcionando criterios de etiquetado, código de colores y documentación que facilite la detección y resolución de problemas así como ampliaciones y modificaciones sin tener que reestructurar todo el sistema.

#### 1.1.1.8. ANSI/TIA/EIA 607

Especifica criterios de instalación del sistema de puesta a tierra de todo el Sistema de Cableado Estructurado que aseguré la protección ante energía electrostática tanto a usuarios como a operadores del sistema.

### 1.1.2. SUBSISTEMAS DEL CABLEADO ESTRUCTURADO

El Sistema de Cableado Estructurado se ha dividido en varios subsistemas que permiten su estudio, administración y detección de fallas.

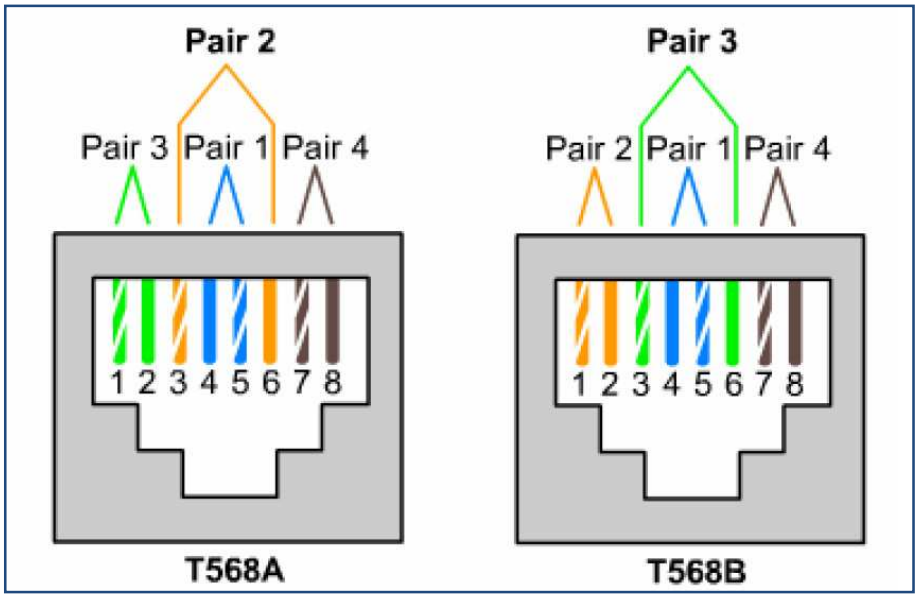
#### 1.1.2.1. Subsistema Cableado Horizontal

El Subsistema de Cableado Horizontal está formado por todos los componentes involucrados en el enlace permanente (cable horizontal, salida de telecomunicaciones en el área de trabajo, terminaciones mecánicas en ambos extremos y patch cords del rack) que existe desde el rack del cuarto de telecomunicaciones a la salida de telecomunicaciones en el Área de Trabajo en una topología física tipo estrella.

Cada cable de cuatro pares en las salidas de telecomunicaciones deberá terminar en un jack de 8 posiciones. Todo el Sistema de Cableado Estructurado debe ser de la misma categoría.

La Figura 1-3 muestra la asignación de pines T568A y T568B.

**Figura 1-3 Asignación de pines T568A y T568B**




La longitud máxima del enlace permanente es de 90 metros, los cuales junto con los patch cords del área de trabajo y los patch cords de interconexiones y conexiones cruzadas en el rack de comunicaciones no deben sobrepasar los 100 metros.

La Tabla 1-2 muestra las distancias máximas soportadas por los cables de acuerdo a su categoría y aplicación.

**Tabla 1-2[2] Máxima distancia soportada por aplicación**

| Cabling Lengths | | | |
|---|---|---|---|
| **Application** | **Media** | **Distance m (ft.)** | **Comments** |
| Ethernet 10BASE-T | Category 3, 5e, 6, 6A | 100 (328) | |
| Ethernet 100BASE-TX | Category 5e, 6, 6A | 100 (328) | |
| Ethernet 1000BASE-T | Category 5e, 6, 6A | 100 (328) | |
| Ethernet 10GBASE-T | Category 6A | 100 (328) | |
| ASDL | Category 3, 5e, 6, 6A | 5,000 (16,404) | 1.5 Mbps to 9 Mbps |
| VDSL | Category 3, 5e, 6, 6A | 5,000 (16,404) | 1,500 m (4,900 ft.) for 12.9 Mbps; 300 m (1,000 ft.) for 52.8 Mbps |
| Analog Phone | Category 3, 5e, 6, 6A | 800 (2,625) | |
| FAX | Category 3, 5e, 6, 6A | 5,000 (16,404) | |
| ATM 25.6 | Category 3, 5e, 6, 6A | 100 (328) | |
| ATM 51.84 | Category 3, 5e, 6, 6A | 100 (328) | |
| ATM 155.52 | Category 5e, 6, 6A | 100 (328) | |
| ATM 1.2G | Category 6, 6A | 100 (328) | |
| ISDN BRI | Category 3, 5e, 6, 6A | 5,000 (16,404) | 128 kbps |
| ISDN PRI | Category 3, 5e, 6, 6A | 5,000 (16,404) | 1.472 Mbps |

Los tipos de medios de transmisión reconocidos para el Subsistema de Cableado Horizontal son:

- Cable UTP y STP de 4 pares 100 ohmios (Categoría 3, 5E, 6 y 6A)
- Fibra Óptica multimodo
- Fibra Óptica monomodo

#### 1.1.2.2. Subsistema Cableado Vertical

El Subsistema de Cableado Vertical permite la conectividad entre los diferentes cuartos de telecomunicaciones con el cuarto de equipos y las diferentes acometidas de servicios de la LAN.

Los tipos de medios de transmisión para la transmisión del cableado horizontal son:

- Cable par trenzado balanceado 100 ohmios (Categoría 3, 5E, 6 y 6A)
- Fibra óptica multimodo: recomendada 62.5/125um y permitida 50/125 um

[2] Tabla tomada de: http://www.anixter.com/AXECOM/AXEDocLib.nsf/0/61vkiffo/$file/sec_14.pdf?openelement

- Fibra óptica monomodo

#### 1.1.2.3. Subsistema Cuarto de Equipos

El Subsistema Cuarto de Equipos es un lugar centralizado para equipos de telecomunicaciones, vigilancia y controles de acceso, en este lugar se encuentran los equipos de conectividad principales, servidores, equipos de telefonía IP, etc. El cuarto de equipos se diferencia del cuarto de telecomunicaciones por la criticidad de equipos que alberga. Cuando el área de servicio es demasiado reducida el cuarto de equipos y cuarto de telecomunicaciones son ubicados en el mismo lugar.

#### 1.1.2.4. Subsistema Cuarto de Telecomunicaciones

El Cuarto de Telecomunicaciones es el lugar donde se encuentran los equipos de distribución del Subsistema de Cableado Horizontal, convirtiéndose en un punto de transición entre el Subsistema de Cableado Vertical y Horizontal.

#### 1.1.2.5. Subsistema Entrada de Servicios

El Subsistema Entrada de Servicios consiste en la acometida de los diferentes servicios de telecomunicaciones provistos por los diferentes proveedores de Internet, telefonía, entre otros y desde el cual se los distribuye al cableado vertical.

#### 1.1.2.6. Subsistema Área de Trabajo

El área de trabajo consiste en el área donde el usuario desarrolla sus actividades y desde donde accede a los recursos de la LAN. El área consiste desde la toma de telecomunicaciones hasta la estación de trabajo.

Cada área de trabajo debe ser provista por mínimo dos enlaces permanentes, sin embargo el uso de telefonía IP ha hecho que este número se reduzca a uno solo enlace, siempre y cuando se tome en cuenta redundancia de enlaces no instalados pero si tendidos para posibles cambios y ampliaciones.

#### 1.1.2.7. Subsistema Puesta a tierra

El Subsistema de Puesta a Tierra especifica los requisitos mínimos de la conexión a tierra del Sistema de Cableado Estructurado que evite cargas electrostáticas que pudieran generarse en los equipos pasivos y canaletas del SCE, la cual podría causar daños tanto a los equipos de conectividad como a los operadores del SCE.

## 1.2. REDES DE INFORMACIÓN[3][4][5]

Las Redes de Información es el conjunto de computadores y dispositivos periféricos que se comunican entre si a través de protocolos para el intercambio de información.

Las Redes de Información se comunican a través de protocolos establecidos por organismos internacionales.

### 1.2.1. ARQUITECTURA DE REDES DE INFORMACIÓN

Las Redes de Información se basan en arquitecturas formadas por capas, donde cada capa está constituida por protocolos que realizan una función específica. Las arquitecturas por capas facilitan el diseño, estudio, implementación y resolución de problemas de Redes de Información.

La Arquitectura sobre la cual se basa la red Internet es TCP/IP la cual está formada por una pila de protocolos TCP/IP que permiten la comunicación entre redes independientes a través de conmutación de paquetes. La conmutación de paquetes fracciona la información a ser transmitida en paquetes los cuales son enviados a través de diferentes caminos a través de ruteadores.

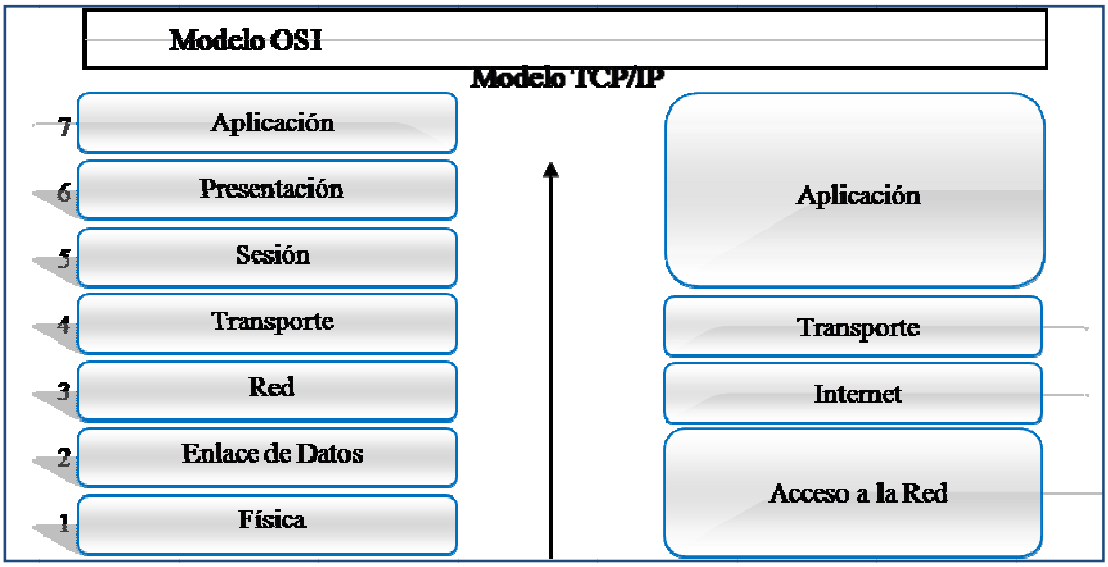
En Redes de Información las arquitecturas por capas son tratadas a través de modelos de referencia entre los que se destacan el modelos de referencia OSI y el modelo de referencia TCP/IP. Estos modelos de referencia establecen una consistencia entre los protocolos y servicios de red.

#### 1.2.1.1. Modelo de referencia TCP/IP[6]

El modelo de referencia TCP/IP define los servicios de entrega de paquetes no confiable (no orientado a la conexión) y el servicio de transporte extremo a extremo sobre el cual funcionan los servicios de aplicación.

En la Figura 1-4 se muestra el modelo de referencia TCP/IP, el cual se encuentra formado por cuatro capas; Aplicación, Transporte, Internet e Interfaz de Red, las cuales también pueden describirse en términos del modelo de referencia OSI. En el modelo OSI la capa de Acceso a la red y la capa Aplicación del modelo TCP/IP están subdivididas para describir funciones particulares.

**Figura 1-4 Relación: Modelo de referencia OSI y TCP/IP**




##### *1.2.1.1.1. Capa Aplicación*

La capa Aplicación permite la interacción entre las aplicaciones y el usuario, interactúa con la capa Transporte para el envío y recepción de los mensajes de las diferentes aplicaciones. Algunos protocolos más comunes en el modelo TCP/IP son HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), SSH (Secure Shell), DNS (*Domain Name System*), etc, los cuales son utilizados para intercambiar datos entre programas que se ejecutan en el host origen y host destino.

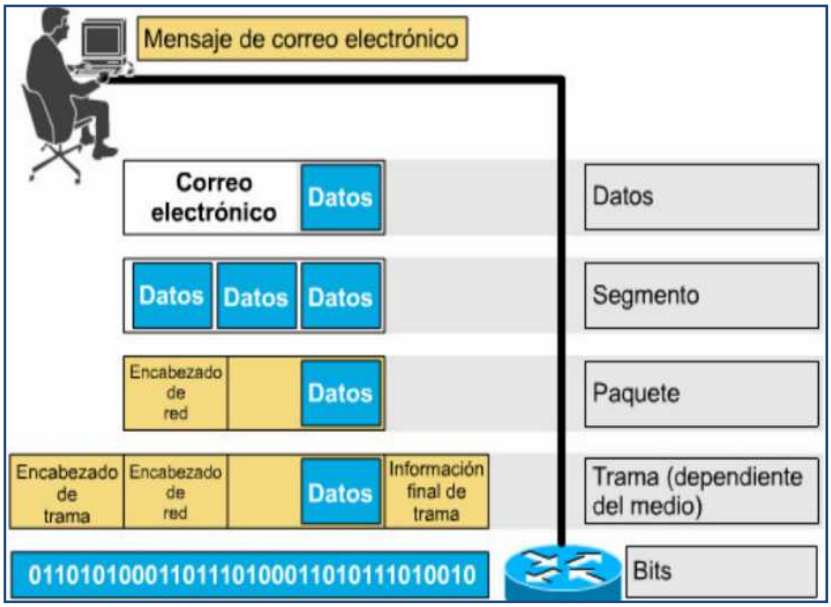
#### *1.2.1.1.2. Capa Transporte*

La capa Transporte es la encargada del establecimiento y liberación de la comunicación extremo a extremo entre los diferentes procesos de la capa aplicación del host origen y destino. Los dos protocolos más comunes son el protocolo TCP (Protocolo de Control de Transmisión) y el protocolo UDP (Protocolo de Datagramas de Usuario).

Todas las capas adicionan información de control a su carga útil (*Payload Data Unit PDU*) para el control en la entrega de información, la cual es retirada cuando es recibida en el destino. El PDU de la capa transporte se lo llama “segmento”.

En la Figura 1-5 se muestra el encapsulamiento de los datos a través de las capas TCP/IP.

**Figura 1-5 Encapsulamiento de Datos**




**Protocolo TCP**

Es un protocolo orientado a la conexión que sincroniza los extremos para el manejo de flujo de paquetes, es un protocolo confiable ya que asegura que los datos lleguen a su destino mediante la retransmisión del paquete en caso de falla. Este protocolo permite distinguir diferentes aplicaciones a través de puertos.

**Protocolo UDP**

Es un protocolo no orientado a la conexión poco confiable ya que no asegura que los datos lleguen a su destino. Es un protocolo utilizado por aplicaciones en tiempo real que son tolerables a la pérdida o errores de información pero su entrega rápida es vital.

#### *1.2.1.1.3. Capa Internet*

La capa Internet es la encargada del intercambio de los paquetes procedentes de la capa Transporte a través de la red entre hosts finales identificados. En esta capa se realiza el encapsulamiento de la información proveniente de la capa Transporte en paquetes a los cuales se les añade información del host origen y destino para su enrutamiento a través de la red.

Los protocolos más comunes son el protocolo IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*) e IGMP (*Internet Group Management Protocol*)

**Protocolo IP**

El protocolo IP es conocido como el protocolo del mejor esfuerzo, es un protocolo no confiable, no orientado a la conexión debido a que no provee ningún mecanismo para determinar si un paquete llega o no a su destino, dejando el control de errores y control de flujo a protocolos de capas superiores. La cabecera del paquete IP contiene las direcciones IP origen y destino las cuales son utilizadas para su respectivo ruteo.

**Protocolo ICMP**

El protocolo ICMP es usado por el protocolo IP para intercambiar mensajes de control y error entre los nodos, también es utilizado por los hosts para determinar si el host con el que desea comunicarse es accesible. ICMP es encapsulado dentro del paquete IP.

Las aplicaciones más comunes que utilizan ICMP con *Ping* y *Traceroute*. *Ping* mide el tiempo que tarda hasta alcanzar un destino y determina si es accesible o no y *Traceroute* determina la ruta para alcanzar un destino.

**Protocolo IGMP**

El Protocolo IGMP es utilizado para el intercambio de información entre host y routers acerca de la pertenencia a un grupo *multicast*. Los mensajes IGMP se encapsulan dentro de paquetes IP.

#### *1.2.1.1.4. Capa Interfaz de Red*

La capa Interfaz de Red o Acceso es la encargada de interactuar con el hardware de la red. En el modelo de referencia TCP/IP el protocolo de capa Acceso no se encuentra definido, teniendo libertad de elección de la plataforma para la comunicación.

### 1.2.1.2. Modelo de referencia OSI

El modelo de referencia OSI (Interconexión de Sistemas Abiertos) fue creado por la Organización Internacional de Estandarización (ISO). A diferencia del modelo TCP/IP el modelo OSI esta formado por 7 capas y no define servicios o protocolos en cada capa, únicamente especifica las funciones de cada una.

La capa de Acceso de TCP/IP se subdivide en capa Física y Capa Enlace. La capa Física se encarga de la transmisión de los bits a través de un medio físico, mientras que la Capa Enlace se ocupa del direccionamiento físico a través de un control de errores y control de flujo.

Las capas Internet y Transporte del modelo TCP/IP corresponden al mismo nivel del modelo OSI.

La capa Aplicación del modelo TCP/IP corresponden a la capa Sesión, capa Presentación y capa Aplicación del modelo OSI donde la capa Sesión es la encargada del establecimiento y mantenimiento de diálogos entre las aplicaciones origen y destino, la capa Presentación es la encargada de la sintaxis de los datos para que estos sean interpretados correctamente por las aplicaciones y por último la Capa Aplicación es la encargada de la interacción entre los usuarios y la red.

### 1.2.2. REDES DE ÁREA LOCAL (LAN)

Las Redes de Área Local son usadas para interconectar equipos informáticos que se encuentren dentro de un área de cobertura limitada, pudiendo ser un edificio o un entorno de alrededor de 200 metros. Una LAN se encuentra formada por computadoras, servidores, equipos de conectividad (switches, routers), equipos de telefonía IP, firewall, etc. Los medios de transmisión usados en redes LAN incluyen cables de cobre y fibra óptica.

#### 1.2.2.1. Arquitectura de Redes de Área Local

En la Figura 1-6 se muestra la arquitectura de redes LAN, la cual se encuentra normalizada por la IEEE 802, la cual no utiliza todas las capas del modelo OSI y no necesita que la arquitectura sea orientada a la conexión. El modelo de referencia IEEE 802 divide la capa de enlace del modelos ISO/OSI en dos subcapas (LLC y MAC).

**Figura 1-6 Normas LAN adoptadas por la ISO**


Subcapa LLC (Control Lógico de Enlace).- proporciona una interfaz común independiente de la tecnología, sus funciones principales son el control de flujo y control de errores.

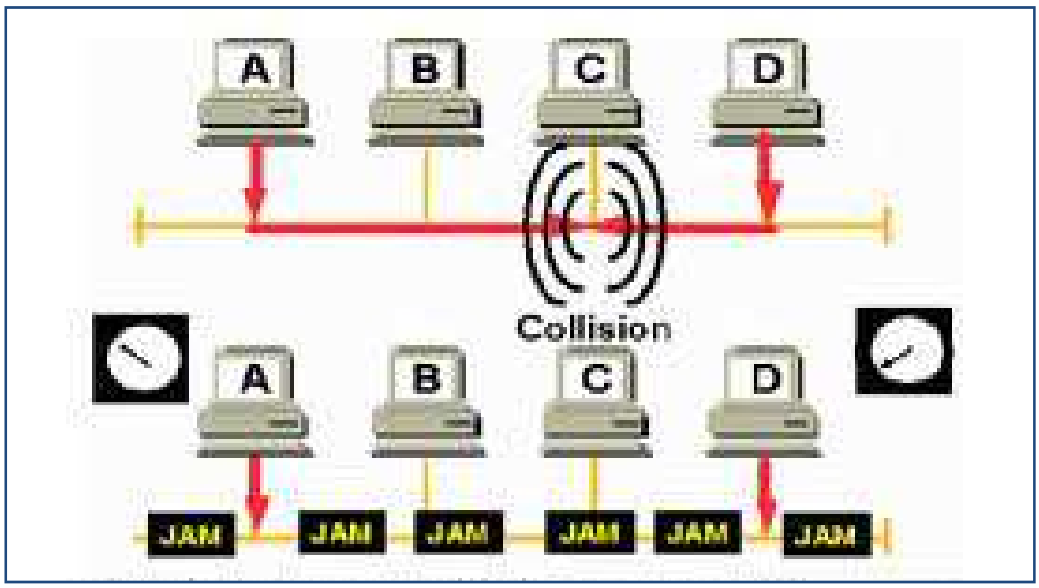
Subcapa MAC (Control de Acceso al Medio).- determina la asignación del canal para la transmisión, sus funciones principales son el sincronismo de trama, transparencia de datos, direccionamiento y detección de errores.

#### 1.2.2.1. Tecnologías de Redes de Área Local[7]

Las tecnologías de redes LAN más importantes se encuentran normalizadas por la IEEE 802.3 (*Ethernet*), la cual se basa en el acceso múltiple por escucha de portadora y detección de colisión (CSMA/CD).

La Figura 1.7 muestra es esquema de colisión en el modelo CSMA/CD de Ethernet.

**Figura 1-7 CSMA/CD**



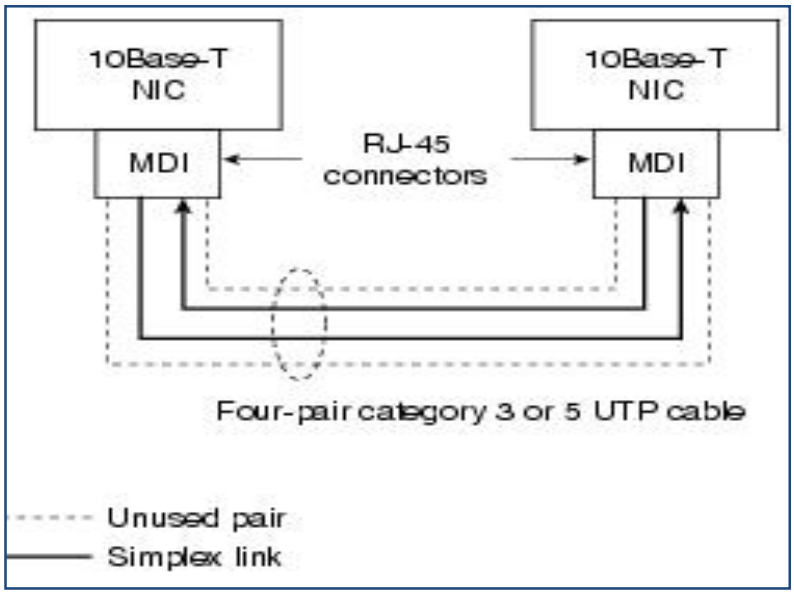

##### *1.2.2.1.1. Ethernet*

Ethernet en un principio se definió para una LAN con topología tipo bus, con cable coaxial grueso operando a 10 Mbps para luego cambiar a cable UTP utilizando una topología física tipo estrella y una topología lógica tipo bus.

Ethernet-10Base-T define una versión Ethernet de 10 Mbps con codificación Manchester sobre dos pares de cable UTP. Aunque el estándar fue creado para soportar cable telefónico, también se lo usa con dos pares o cuatro pares de cable UTP categoría 3 y 5. Las terminaciones son a través de interfaces de 8 pines RJ45.

La Figura 1-8 muestra el enlace típico 10BaseT, en el cual únicamente se utilizan dos pares y dos pares se encuentran sin ser utilizados.

**Figura 1-8 Enlace típico 10Base-T**




*1.2.2.1.2. Fast Ethernet*

El incremento de la velocidad de transmisión a 100 Mbps no fue una tarea simple por lo cual se desarrollaron tres estándares separados sobre cable UTP, cada una fue definida con diferente codificación (100Base-TX, 100Base-T4 y 100Base-T2).

Fast Ethernet 100Base-TX está diseñado para utilizar dos pares de cable UTP categoría 5, el proceso de codificación utilizado es 4B/5B y soporta transmisión *full-duplex* y *half-duplex*[3].

Fast Ethernet 100Base-T4 utiliza los cuatro pares del cable UTP categoría 3 y 5. Dos de los cuatro pares están configurados para soportar transmisiones *half-duplex*, los otros dos pares están configurados para modos de transmisión simples, en una sola dirección. El modo de transmisión *full-duplex* no es soportado. Usa el esquema de codificación 8B6T.

Fast Ethernet 100Base-T2 utiliza dos pares del cable UTP categoría 3 o superior y soporta los modos de operación *half-duplex* y *full-duplex*

[3] *Full-Duplex* se refiere a la comunicación que permite canales de envío y recepción simultáneos.
*Half-Duplex* se refiere a la comunicación que pueden transmitir en los dos sentidos, pero no de forma simultánea.

#### *1.2.2.1.3. Gigabit Ethernet*

Gigabit Ethernet 1000Base-T cuenta con un modo de operación *full-duplex* sobre los 4 pares del cable UTP categoría 5 o superior. Se encuentra estandarizado en la norma IEEE 802.3ab y en la norma IEEE 802.3z como Gigabit Ethernet 1000Base-X.

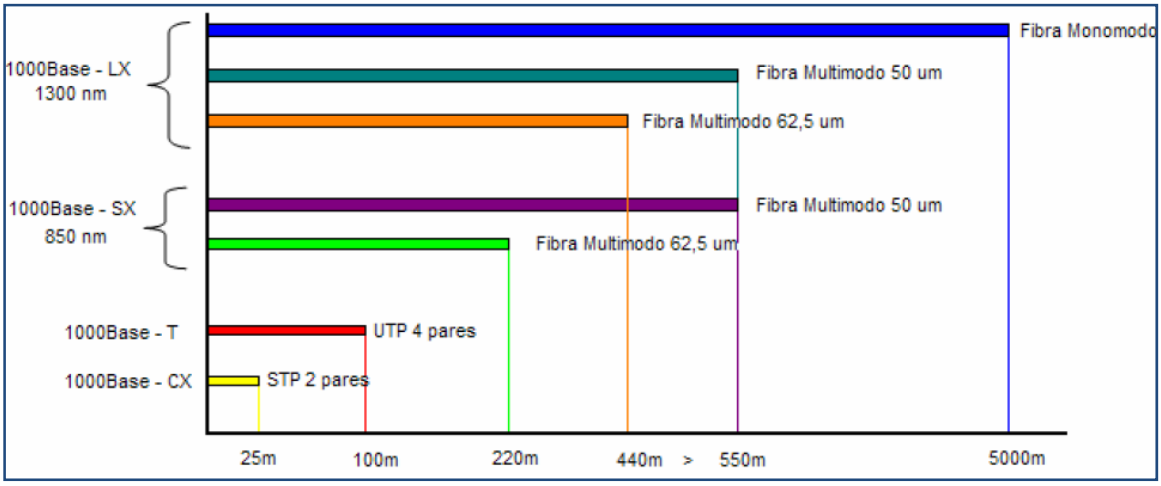
Emplea como medio de transmisión los 4 pares del cable UTP con una distancia de 100 metros, trabaja en modo de operación *full-duplex* y utiliza Modulación de Amplitud de Pulsos 5 (PAM-5).

La tecnología Gigabit Ethernet utiliza ráfagas de tramas y extensión de portadora en donde la trama aumenta de 512 bits a 512 bytes.

Gigabit Ethernet 1000Base-CX utiliza dos pares del cable STP y es utilizado en subsistemas de cableado vertical debido a su alcance de apenas 25 metros.

La Figura 1-9 muestra el alcance máximo de acuerdo a la tecnología Gigabit Ethernet.

**Figura 1-9 Alcance máximo Gigabit Ethernet**




#### *1.2.2.1.4. 10-Gigabit Ethernet*

Es la norma más reciente y define Ethernet 10 Gbps sobre fibra (IEEE 802.3ae) y cobre (IEEE 802.3an), la cual elimina el modo *half-duplex*, operando únicamente en enlaces *full-duplex*.

10GBASE-T utiliza cable UTP categoría 6A a una distancia de 100 metros y con cable categoría 6 a 55 metros. La modulación utilizada es a través de amplitud por pulsos con 16 niveles (PAM-16).

### 1.2.3. REDES LAN INALÁMBRICAS (WLAN) [8]

Las redes inalámbricas se encuentran en constante cambio y están siendo usadas en todos los lugares, ya sean estas entidades públicas o privadas convirtiéndose en una opción a las redes LAN cableadas o como una extensión de las mismas.

Entre las ventajas que tienen las redes LAN inalámbricas se tiene:

- Ofrece movilidad a los usuarios.
- Facilidad de instalación e incorporación de un nuevo usuario a la red.
- Ofrece flexibilidad de acceso a la red en lugares inaccesibles por la red cableada.
- Ofrece una red de comunicaciones escalable.
- Permite la interconexión entre edificios a través de enlaces punto a punto.
- Un beneficio tangible es la reducción de costos.

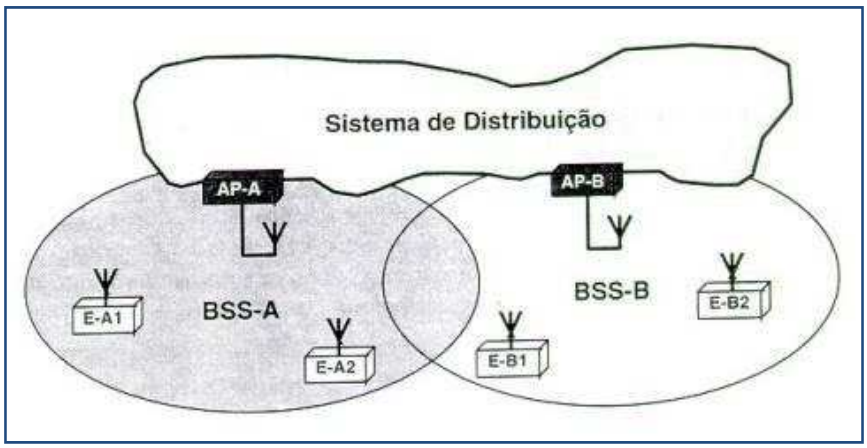
Si bien las redes LAN cableadas e inalámbricas proveen de conectividad a los usuarios en la red, éstas cuentan con diferencias que van más allá de las físicas. Las diferencias radican en la forma como es encapsulada la trama y su método de transmisión. Las diferencias son las siguientes:

- Las redes LAN Ethernet se basan en el acceso múltiple por escucha de portadora y detección de colisión (CSMA/CD) mientras que las WLAN se basan en el acceso múltiple por escucha de portadora y evita la colisión (CSMA/CA). La detección de colisión no es posible en WLAN porque el hosts no transmite y recibe al mismo tiempo, por lo cual no puede detectar la colisión. En su lugar de eso utiliza los protocolos RTS (*Request to Send*) y CTS (*Clear to Send*) que evitan la colisión.

- La trama WLAN es diferente a una trama LAN, en las tramas WLAN se requiere información adicional en su cabecera.

En la Figura 1-10 se muestra la arquitectura WLAN, la cual está formada por un conjunto de estaciones que constituyen un BSS (Conjunto de Servicios Básicos) que coordinan su acceso al medio a través de un proceso de asociación, el área de cobertura del BSS constituye un BSA (Área de Servicios Básicos). Los BSS tienen la posibilidad de comunicarse entre si a través de un sistema de distribución formando un ESS (Conjunto de Servicios Extendido) mediante el cual se proporciona acceso a la red cableada.

**Figura 1-10 Arquitectura WLAN**




### 1.2.3.1. Estándares IEEE 802.11

La IEEE define el estándar IEEE 802.11 que especifica las características para la conexión inalámbrica. Trabaja a una banda de frecuencia de 2.4 Ghz a velocidades de 1 y 2 Mbps con FHSS (*Frecuency Hopping Spread Spectrum*) y DSSS (*Direct Secuence Spread Spectrum*).

La familia de protocolos IEEE 802.11 están definidas por su velocidad de transmisión, técnicas de modulación, entre otros.

**IEEE 802.11b.-** opera en la banda de frecuencia de 2.4 GHz con velocidades de transmisión de hasta 11 Mbps. A velocidades de 1 y 2 Mbps utiliza el mismo código de

modulación de 802.11 (DSSS) mientras que a velocidades de transmisión de 5.5 y 11 Mbps utiliza CCK (Codificación de Código Complementario). Este estándar tiene 11 canales de 22 MHz cada uno, lo cual resulta en tres canales no sobrelapados, es decir que tres *Access Points*[4] pueden ocupar la misma área.

**IEEE 802.11a.-** opera en la banda de frecuencia de 5 GHz con velocidades de transmisión de 6 a 54 Mbps y utiliza como técnica de modulación OFDM (*Ortogonal Frecuency Division Multiplexing*). Los canales de 802.11a operan a 20 MHz cada uno, se tiene ocho canales no sobrelapados, es decir que ocho *Access Points* pueden ocupar la misma área.

**IEEE 802.11g**.- opera en la banda de frecuencia de 2.4 GHz. Es compatible con 802.11b cuando utiliza su misma modulación (DSSS) llegando a una velocidad de transmisión máxima de 11 Mbps y mediante OFDM alcanza velocidades de transmisión de 54 Mbps. Este estándar tiene tres canales no sobrelapados, es decir que tres *Access Points* pueden ocupar la misma área.

#### 1.2.3.2. Seguridad en redes inalámbricas

Todo sistema para considerarse seguro debe cumplir con requerimientos de autenticación, confidencialidad, integridad y disponibilidad.

La autenticación en redes WLAN consiste en verificar la identidad que un usuario en realidad es quien dice ser, la autenticación puede ser en un solo sentido (usuario) o en doble sentido, en cuyo caso se autentica el usuario y la red WLAN a la cual desea asociarse el usuario.

La confidencialidad consiste en garantizar la privacidad de la información a través de mecanismos de encripción, en donde solo el dueño o destinatario tendrán acceso de la información.

La integridad consiste en prevenir la modificación no autorizada de la información.

[4] *Access Point* es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

La disponibilidad del sistema consiste en su control de vulnerabilidades y amenazas y su capacidad de recuperación en caso que haya sido vulnerado.

Medidas de seguridad a tener en cuenta en una red WLAN son las siguientes:

- Se debe tener un registro de las máquinas y usuarios autorizados a tener acceso a la WLAN de acuerdo al cual se debe realizar un escaneo para realizar el filtrado respectivo, el cual puede ser en base a protocolos, dirección IP, dirección MAC y SSID.

Los estándares de seguridad más comunes en Redes Inalámbricas son:

- **WEP (*Wired Equivalency Protocol*).-** es un protocolo que provee de autenticación, confidencialidad e integridad mediante el algoritmo RC-4 con claves de 64 y 128 bits. WEP utiliza la misma clave para autenticación y encripción lo cual hace que sea un estándar de seguridad poco confiable ya que sus tramas al ser capturadas son de fácil desencripción.
- **IEEE 802.1x y EAP (*Extensible Authentication Protocol*).-** 802.1x es un protocolo de control de acceso que restringe la conexión a redes inalámbricas a través de EAP, el cual define el formato de las tramas de autenticación con las que se solicita acceso a un servidor de autenticación Radius (*Remote Authentication Dial-In User Service*).
- **WPA (*Wifi Protect Access*).-** provee autenticación a través de 802.1x y PSK (*preshared key*), la encripción la realiza por medio de TKIP (*Temporal Key Integrity Protocol*). WPA2 no cambia la forma de autenticación pero la encripción lo realiza con una variante de AES que hace que la contraseña vaya cambiando cada cierto tiempo.

La Tabla 1-3 muestra de forma cronológica la evolución de la seguridad en redes WLAN.

**Tabla 1-3Evolución de la seguridad en redes WLAN**

| 1997 | 2001 | 2003 | 2004 to Present |
|---|---|---|---|
| WEP | 802.1x EAP | WPA | 802.11i/WPA2 |
| • Basic Encryption<br>• No Strong Authentication<br>• Static, Breakable Keys<br>• Not Scalable<br>• MAC Filters and SSID Cloaking Also Used to Complement WEP | • Dynamic Keys<br>• Improved Encryption<br>• User Authentication<br>• 802.1x EAP (LEAP, PEAP)<br>• RADIUS | • Standardized<br>• Improved Encryption<br>• Strong, User Authentication (e.g., LEAP, PEAP, EAP-FAST) | • AES Strong Encryption<br>• Authentication<br>• Dynamic Key Management |

Si bien se toman las precauciones de seguridad mencionadas anteriormente, también depende en gran parte de la seguridad suministrada a la WLAN desde la red cableada. En los equipos de conectividad se deberán crear listas de acceso que restrinja y limite el tráfico que circulará por la red inalámbrica. A nivel de firewall se deberá proteger a la WLAN de redes externas y dependiendo de la criticidad de la información manejada en la red será necesario el uso de IPS (Sistema de Protección de Intrusos) e IDS (Sistema de Detección de Intrusos). A nivel institucional se deberán crear políticas de acceso a la WLAN.

### 1.2.4. DIRECCIONAMIENTO IP EN REDES TCP/IP

La dirección IP es un identificador único asignado a un host (interfaz de red) para ser identificado en una red. La dirección IP esta representada por un valor binario de 32 bits, los cuales se representan por cuatro campos separados por puntos. La dificultad de recordar una dirección IP llevó al desarrollo del sistema de resolución de nombres de dominio (DNS) la cual relaciona una dirección IP con un nombre.

Para que un hosts pueda ser identificado en Internet debe constar con una dirección IP asignada por la IANA que es un organismo internacional encargado de asignar direcciones IP públicas.

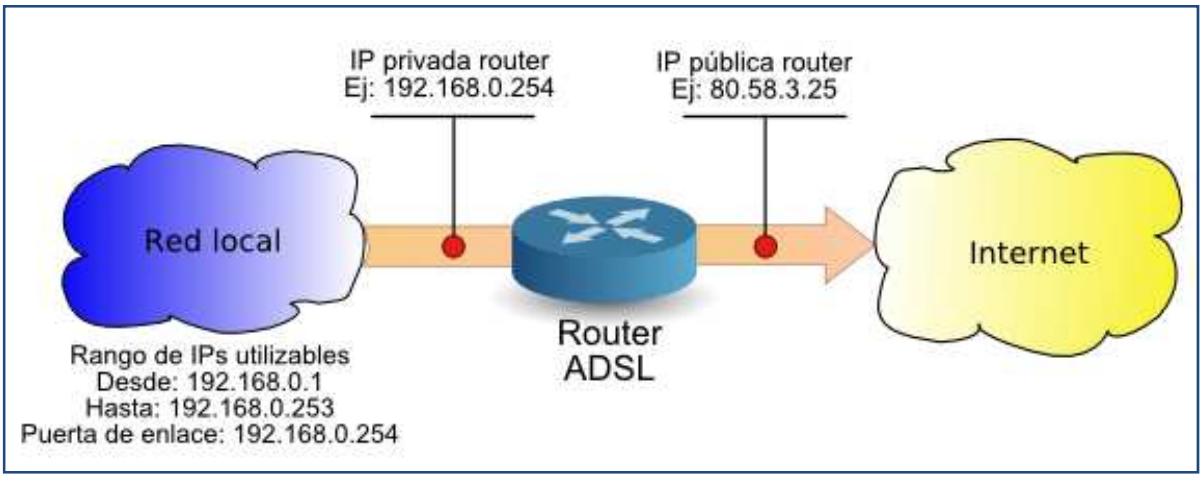
Una dirección IP esta formada por dos partes, por un lado, aquella que identifica la red a la que pertenece el host y por otro lado, aquella que identifica al host dentro de la red. Para determinar qué parte de la dirección pertenece a la red y qué parte pertenece al host se debe especificar la máscara de subred.

Las direcciones IP se clasifican entre dirección IP Públicas y Privadas. Las direcciones IP Privadas son aquellas que no se encuentran conectadas de forma directa con Internet (se conectan por medio de un proxy o router) tienen asignado un rango de direcciones IP para su funcionamiento interno.

- Clase A: una única dirección de red: 10.0.0.0 hasta 10.255.255.255
- Clase B: 16 redes de rango: 172.16.0.0 hasta 172.31.255.255
- Clase C:256 direcciones de red: 192.168.0.0 hasta 192.168.255.255

La Figura 1-11 muestra un ejemplo de direcciones IPs Públicas en el lado de Internet e IPs Privadas en el lado de la Red Local.

**Figura 1-11 Direcciones Públicas y Privadas**




Existen direcciones especiales utilizadas para funciones especiales

- La red 127.0.0.0 está reservada para funciones de *loopback*[5].

[5] La dirección de loopback es utilizada por los hosts para dirigir el tráfico hacia ellos mismos, es utilizado en tareas de diagnóstico de conectividad y validez del protocolo de comunicación.

- Una red con el número de red seteado en 255 y el número de host también en 255 está reservada para funciones de *broadcast*[6].
- Una dirección IP con los números de hosts seteado en 255 está reservada para direccionar todos los hosts a una red.

En un principio se trabajaba con redes basadas en clases, que asignaban un cierto rango de direcciones IP de acuerdo al tamaño de la red, sin embargo esto conllevaba en ciertos casos a un desperdicio de direcciones IP, por lo cual, en la actualidad se utilizan subredes, VLSM (*Variable Length Subnet Mask*) y CIDR (*Classless Inter Domain Routing*).

#### 1.2.4.1. Subredes

Las subredes segmentan a la red, las subredes se crean dividiendo el número de host en número de subred y número de host. Las subredes reducen el tráfico de la red ya que únicamente los paquetes destinados a otra subred pasarán a través del router optimizando de esta forma el rendimiento de la red, se crean más dominios de *broadcast* pero con menor tráfico.

#### 1.2.4.2. VLSM

Se emplea para la segmentación de la red cuando el número de hosts en cada subred es variable. A cada subred se le asigna una máscara diferente dependiendo del número de host que alberga.

#### 1.2.4.3. CIDR

Es un proceso de sumarización que representa en una sola dirección IP con su respectiva máscara a un conjunto de rutas reduciendo de esta forma el tamaño de las tablas de enrutamiento en los routers.

[6] Broadcast es la transmisión de un paquete que será recibido por todos los dispositivos en una red.

## 1.3. TELEFONÍA IP [9]

La telefonía IP es un servicio que hace uso de la tecnología VoIP (Voz sobre IP) la cual permite la transmisión de voz a través del protocolo IP en redes de datos. El servicio de telefonía IP ha llegado a tener gran importancia en el mundo empresarial debido a su desarrollo exponencial, rentabilidad y sobre todo porque se encuentra al alcance de todos.

### 1.3.1. FUNCIONAMIENTO DE LA TELEFONÍA IP

La señal de voz es una onda analógica que necesita transformarse a digital para ser transmitida, esto se logra a través de códecs, los cuales además comprimen la secuencia de datos y proporcionan cancelación de eco lo cual conlleva al ahorro de ancho de banda.

Otra forma de optimizar el ancho de banda es a través de la supresión de silencio, con el cual se evita el envío de paquetes de voz entre silencios en conversaciones.

Luego de transformada la señal de voz a digital con su respectiva compresión, ésta se encapsula en paquetes IP para su transmisión. El proceso contrario se lleva a cabo en recepción.

### 1.3.2. VENTAJAS DE LA TELEFONÍA IP

Permite una convergencia de servicios sobre una misma infraestructura de red, lo cual conlleva a una administración centralizada, además los costos de implementación disminuyen.

Una ventaja tangible es la reducción de costos por llamada, la cual implica el costo del consumo de Internet cuando la llamada es de teléfonos IP a convencionales, mientras que las llamadas dentro de la LAN son gratuitas.

La telefonía IP no solo conlleva la transmisión de voz, si no que integra servicios adicionales como; identificación de llamadas, servicio de llamadas en espera, filtro de llamadas entre otros, los cuales, al contrario de la telefonía convencional son gratuitos.

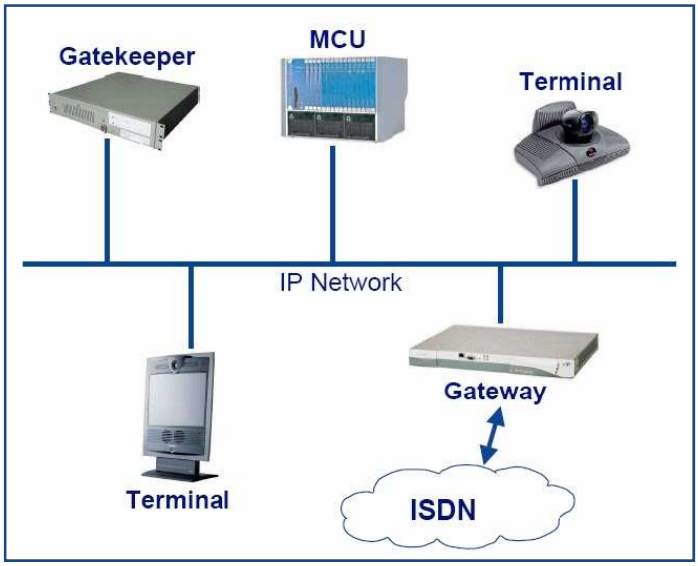
Ofrece movilidad, ya que es posible realizar llamadas desde lugares remotos a través de *softphones*[7] con conexión a internet.

Una desventaja destacable es que la telefonía IP al contrario de la telefonía convencional depende de una conexión a la red eléctrica sin la cual el servicio deja de funcionar.

### 1.3.3. ARQUITECTURA DEL SISTEMA DE TELEFONÍA IP

El estándar VoIP establece para el servicio de Telefonía IP los siguientes elementos (Figura 1-12):

**Figura 1-12 Arquitectura Telefonía IP**




**Terminales**.- es un extremo de la red donde se encuentran los dispositivos utilizados por el usuario para acceder al servicio de Telefonía IP. Generalmente son los teléfonos IP y *softphones*.

[7] Softphone es un software que corre en una computadora que permite hacer y recibir llamadas por Internet con VoIP.

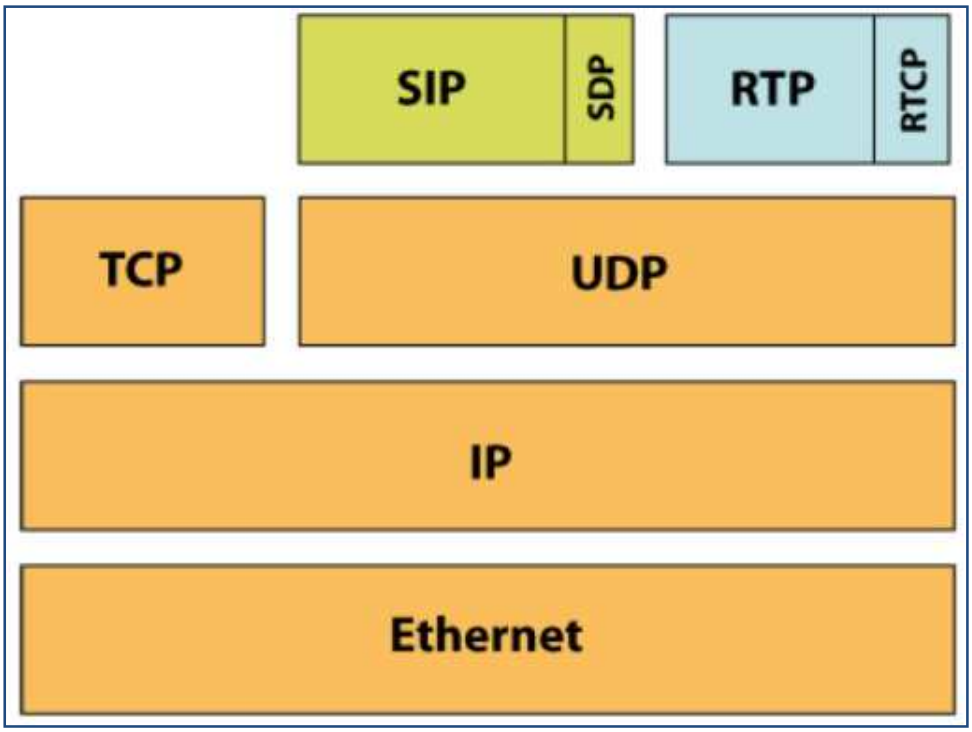
**Gateway**.- es un extremo que proporciona comunicaciones bidireccionales entre la telefonía IP y la red telefónica convencional, es el encargado de hacer transparente dicha comunicación.

**Gatekeeper**.- está encargado de realizar la traducción de direcciones y el control de acceso a la red de los terminales y gateways, también gestiona el ancho de banda de la red determinando el número de llamadas simultáneas.

### 1.3.4. PROTOCOLOS

Existen muchos protocolos involucrados en la transmisión de voz sobre IP los cuales se dividen en protocolos de transporte, protocolos de señalización y protocolos de enrutamiento dinámico. Los protocolos involucrados en una llamada SIP se muestran en la Figura 1-13.

**Figura 1-13 Protocolos involucrados en una llamada SIP**



#### 1.3.4.1. Protocolos de Transporte

##### *1.3.4.1.1. RTP (Real-Time Transport Protocol)*

Es un protocolo de capa sesión encargado de transmitir información de audio y video a través de Internet. RTP adiciona números de secuencia a los paquetes IP para su respectiva entrega en su destino. Se encapsula en UDP, por lo cual no garantiza la entrega de la información, dejándole el control de errores a la capa Aplicación.

##### *1.3.4.1.2. RTCP (RTP Control Protocol)*

Trabaja en conjunto con RTP, se encarga de la transmisión periódica de paquetes de control. Envía información básica sobre los participantes de la sesión, se encapsula sobre RTP. RTCP realiza el control de flujo de RTP.

#### 1.3.4.2. Protocolos de Señalización

Los protocolos de señalización cumplen funciones de establecimiento de sesión, control del progreso de llamada, entre otras, se encuentran en la capa sesión del modelo OSI. Entre los protocolos más comunes se encuentran los siguientes:

##### *1.3.4.2.1. SIP (Protocolo de Inicio de Sesión)*

SIP es un protocolo de señalización para voz sobre IP encargada de la inicialización, modificación y terminación de sesiones de comunicación multimedia entre usuarios.

SIP se encarga de la localización, disponibilidad y verificación de la capacidad del usuario, gestiona la sesión en cuanto a transferencia, terminación y modificación de los parámetros de las sesiones.

##### *1.3.4.2.2. IAX (Inter-Asterisk eXchange Protocol)*

Como su nombre lo indica es un protocolo creado para la señalización en Asterisk, el cual se ha desarrollado debido al crecimiento en cuanto al uso de servidores de telefonía IP Asterisk. IAX se encarga de la transmisión de datos multimedia optimizando el ancho de banda.

## 1.4. SEGURIDAD DE LA INFORMACIÓN[10]

En toda institución pública o privada la información ha llegado a ser un activo que al igual que los demás activos tangibles pueden llegar a ser esenciales para la continuidad del negocio y en consecuencia necesitan ser protegidos de tal forma que garanticen su confidencialidad, integridad y disponibilidad.

El crecimiento de las redes de información, su convergencia con los diferentes servicios y su acceso desde cualquier parte del mundo de forma remota hace que la información cada vez se encuentre más expuesta a un número cada vez mayor de amenazas y vulnerabilidades.

La seguridad de la información se logra implementando un adecuado conjunto de controles; en software, hardware, procesos, políticas y hasta en estructuras organizacionales.

Es importante que una empresa identifique sus requerimientos de seguridad a través de la identificación de sus activos informáticos y de la evaluación de riesgo de los mismos. El análisis de riesgo identifica las amenazas de los activos, evalúa la vulnerabilidad y la probabilidad de ocurrencia de acuerdo a su impacto potencial.

### 1.4.1. EVALUACIÓN Y ADMINISTRACIÓN DE RIESGOS

El análisis de riesgo es la base para el establecimiento de políticas de seguridad, es el fundamento sobre el cual se establecen las diferentes normas de protección. Los resultados de la evaluación de riesgo ayudan a guiar y determinar los controles necesarios de acuerdo al daño comercial en caso de fallas en la seguridad. Los controles de seguridad deben estar sujetos a la legislación vigente nacional e internacional del lugar en donde se las aplique.

#### 1.4.1.1. Análisis de Riesgos

El análisis de riesgos implica determinar lo siguiente:

- Lo que se necesita proteger
- De quién se lo necesita proteger
- Y de qué forma protegerlo

Los riesgos se clasifican por el nivel de importancia del activo informático y por la severidad de su pérdida. No se debe invertir demasiados recursos para proteger activos informáticos que no son vitales para la continuidad del negocio.

Existen múltiples metodologías y herramientas que nos permiten realizar un análisis de riesgo. La metodología base es la siguiente:

- Identificación de activos informáticos
- Definición del impacto
- Definición de la probabilidad de ocurrencia
- Identificación de amenazas
- Definición de riesgos
- Identificación de medidas de seguridad
- Políticas de seguridad
- Acciones correctivas

Todas las definiciones e identificaciones mencionadas se las realiza de acuerdo a la realidad de cada empresa.

##### *1.4.1.1.1. Identificación de activos informáticos*

Los activos informáticos son todos aquellos que almacenan, procesan y usan la información, tales como; hardware, software, usuarios, servicios, aplicaciones, etc, los cuales se clasifican en base a su criticidad para el negocio utilizando los tres componentes principales de la seguridad de la información.

- Confidencialidad.- protección de la información sensible contra divulgación no autorizada.

- Integridad.- protección de la información sensible contra cambios y alteraciones no autorizadas.
- Disponibilidad.- protección de la información para que pueda ser requerida en cualquier momento. También se refiere a la capacidad de recuperación frente pérdidas de información o fallos en la misma.

Los activos informáticos de acuerdo a su confidencialidad deben ser valorados de acuerdo a la información manejada por cada activo (Ejm: públicos, internos, confidenciales y estrictamente confidenciales).

Los activos informáticos de acuerdo a su integridad y disponibilidad deben ser valorados de acuerdo a la información manejada por cada activo (Ejm: bajo, promedio, importante, crítico).

#### *1.4.1.1.2. Definición del impacto*

Constituye el tipo de impacto que puede recibir una determinada empresa de acuerdo a aspectos en áreas como; resultados, clientes, operaciones, regulaciones, reputación, etc.

#### *1.4.1.1.3. Definición de probabilidad de ocurrencia*

Se calcula la probabilidad de ocurrencia de los hechos y se las orientas a una frecuencia anualizada.

#### *1.4.1.1.4. Identificación de amenazas*

La identificación de amenazas se la realiza por cada activo de información crítico. Las amenazas más comunes pueden ser ambientales, tecnológicas y humanas.

- Amenazas ambientales.- dependerán exclusivamente de las condiciones físicas, geográficas, climatológicas y estructural donde se encuentran los activos informáticos. Un ejemplo de amenazas ambientales son las siguientes:
    - Inundación

  - Fuego
  - Daño sísmico
  - Daño por erupción volcánica, etc.
- Amenazas humanas.- las amenazas humanas de las debe clasificar de acuerdo a la ubicación de las personas (internas, externas) y de acuerdo a su nivel de conocimiento técnico (estructuradas, no estructuradas).
  - Las amenazas externas estructuradas corresponden a personas con intensión y determinación de provocar daño (crackers).
  - Las amenazas externas no estructuradas corresponde por ejemplo a un cracker no dañino motivado por su ambición de conocimiento técnico.
  - Las amenazas internas estructuradas corresponden por ejemplo a un empleado insatisfecho que desea causar daño y cuenta con los conocimientos técnicos y acceso a la información.
  - Las amenazas internas no estructuradas corresponden generalmente a descuidos en el tratamiento de la información por parte de usuarios, administradores y otros.
- Amenazas tecnológicas.- están asociadas en particular con la tecnología informática que utiliza el activo informático, por ejemplo sistemas operativos, bases de datos, aplicaciones, hardware, comunicaciones, etc.

##### *1.4.1.1.5. Definición de riesgos*

La definición de riesgos de seguridad de la información se basa en una consideración sistemática de los siguientes puntos:

- Impacto potencial de una falla de seguridad.- en las que se debe tener en cuenta las potenciales consecuencias que puede provocar la pérdida de confidencialidad, integridad o disponibilidad de la información y de los recursos asociados a la misma.

- Probabilidad de ocurrencia de dicha falla.- en la que se debe tomar en cuenta las amenazas y vulnerabilidades predominantes y si es el caso, los controles actualmente implementados.

#### *1.4.1.1.6. Identificación de medidas de seguridad.*

Una vez identificados los riesgos críticos no aceptables a través del análisis de riesgos se deben escoger los controles adecuados para disminuirlos a través de estándares de seguridad tales como ISO/IEC 27000, COBIT, ITIL, etc.

Las medidas de seguridad se las realiza sobre cada activo informático determinado como crítico. Se debe especificar los requerimientos obligatorios mínimos para el uso correcto y la protección de la información y proveer un marco para todas las actividades relacionadas con la seguridad dentro de la institución.

Las medidas y controles de seguridad, dependiendo del caso, tienen como propósito eliminar, reducir, aceptar, transferir e incluso incrementar los riesgos de cada uno de los activos informáticos.

#### *1.4.1.1.7. Políticas de Seguridad*

Las políticas de seguridad son un conjunto de normas estructuradas de forma jerárquica que definen la forma en que una institución responde a los riesgos de seguridad de la información.

Las políticas de información permiten definir un plan de acción para riesgos extremos o altos y define responsabilidades de los propietarios de cada uno de los activos informáticos.

#### *1.4.1.1.8. Acciones correctivas*

El análisis de riesgo es un proceso que se lo debe realizar de forma periódica y debe mantenerse actualizada dependiendo del crecimiento de la institución, de nuevos cambios organizacionales y de cambios en la información manejada.

Se analiza los activos informáticos que puedan tener controles excesivos para reducirlos y enfocar esfuerzos en los activos informáticos de mayor criticidad.

### 1.4.2. ESTANDAR DE SEGURIDAD ISO

La Organización Internacional para la Estandarización (ISO) define la serie de normas ISO/IEC 27000, las cuales especifican las mejores prácticas en Seguridad de Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Las normas con las que cuenta esta serie son:

- ISO/IEC 27001 Sistemas de Administración de la Seguridad de la Información
- ISO/IEC 27002 Código de Práctica
- ISO/IEC 27003 Análisis de Riesgos
- ISO/IEC 27004 Métricas para la Seguridad de la Información

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande convirtiéndose en la base para la gestión de la seguridad de la información. También permite que la gestión de la seguridad de la información de una organización sea certificada.

El Anexo A de la norma ISO 27001 es el mas utilizado debido a que de acuerdo a esta norma se consigue la certificación. En esta norma se enumeran 133 controles de seguridad estructurados en 11 cláusulas.

La norma ISO 27001 contiene los siguientes puntos:

- A.5 Políticas de Seguridad.- su objetivo es establecer políticas de acuerdo a los requerimientos comerciales de la empresa y a leyes y regulaciones para que sean aprobadas por la gerencia.

- A.6 Organización de la seguridad de la información.- su objetivo es establecer un marco referencial para la implementación, verificación y mantenimiento de la seguridad dentro de la institución.
- A.7 Gestión de Activos.- su objetivo es la identificación de los activos informáticos y la asignación de los mismos a un propietario o responsable.
- A.8 Seguridad relacionada con el personal.- su objetivo es evitar o reducir el robo, fraude o mal uso de los activos informáticos mediante la asignación de responsabilidades a empleados, contratistas y terceros.
- A.9 Seguridad física y del entorno.- su objetivo es impedir el acceso físico no autorizado a la institución de personas u instancias que pudieran causar daño o interferencia a la información.
- A.10 Gestión de comunicaciones y operaciones.- su objetivo es establecer responsabilidades y procedimientos para la gestión y operación de los medios de procesamiento de la información.
- A.11 Control de acceso.- su objetivo es controlar el acceso a la información y procesos.
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de la información.- su objetivo es garantizar que la seguridad sea parte integral de los sistemas de información (infraestructura, aplicaciones, productos, servicios, entre otras).
- A.13 Gestión de los incidentes de seguridad de la información.- su objetivo es realizar acciones correctivas oportunas frente fallas en la seguridad de la información.
- A.14 Gestión de la continuidad del negocio.- su objetivo es proteger los procesos críticos ante fallas en la seguridad de la información o en el peor de los casos asegurar su reanudación inmediata.
- A.15 Cumplimiento.- su objetivo es evitar las violaciones de las políticas de seguridad, ley o legislación.

Esta norma incluye el ciclo PDCA (*Plan-Do-Check-Action*) de Planificación, Implementación, Verificación y Mantenimiento.

#### 1.4.2.1. Fase de planificación

La fase de planificación esta formada por los siguientes pasos:

- Determinación del alcance del SGSI
- Redacción de una política de SGI
- Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos
- Evaluación de la magnitud de los riesgos
- Identificación de opciones para el tratamiento de riesgos
- Selección de controles para el tratamiento de riesgos
- Aprobación de la gerencia para los riesgos residuales
- Aprobación de la gerencia para la implementación del SGSI
- Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

#### 1.4.2.2. Fase de implementación

La fase de implementación incluye las siguientes actividades:

- Redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuáles, cuándo y con que presupuesto se debería implementar los controles.
- Implementación del plan de tratamiento del riesgo
- Implementación de los controles de seguridad correspondientes
- Determinación de cómo medir la eficacia de los controles
- Realización de programas de concienciación y capacitación de empleados
- Gestión del funcionamiento normal del SGSI
- Gestión de los recursos del SGSI
- Implementación de procedimientos para detectar y gestionar incidentes de seguridad.

#### 1.4.2.3. Fase de Verificación

La fase de verificación incluye lo siguiente:

- Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, etc
- Revisiones periódicas de la eficacia del SGSI
- Medición de la eficacia de los controles
- Revisión periódica de la evaluación de riesgos
- Auditorías internas planificadas
- Revisión por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras.
- Actualización de los planes de seguridad
- Mantenimiento de registros de actividades e incidentes

#### 1.4.2.4. Fase de Mantenimiento

La fase de verificación incluye lo siguiente:

- Implementación en el SGSI de las mejoras identificadas
- Toma de medidas correctivas y preventivas
- Comunicación de actividades y mejoras a todos los grupos de interés
- Asegurar que las mejoras cumplan con los objetivos previstos

Los controles de la norma ISO 27002 tienen los mismos nombres que el Anexo A de la norma ISO 27002 con la diferencia que la ISO 27002 ofrece lineamientos detallados sobre cómo implementar los diferentes controles.

# CAPÍTULO II

# 2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DE COMUNICACIONES

## 2.1. INTRODUCCIÓN

Mediante decreto ejecutivo No. 1636, del 25 de marzo del 2009, se crea el Programa de Provisión de Alimentos (PPA) como entidad adscrita al Ministerio de Inclusión Económica y Social (MIES), con autonomía técnica, administrativa y financiera.

### 2.1.1. OBJETIVOS

Satisfacer los requerimientos de adquisiciones de alimentos de los programas sociales de alimentación y nutrición que cumplan con las especificaciones de calidad establecidas por los Programas.

Proveer servicios complementarios de certificación, almacenamiento y distribución, que permitan garantizar la provisión oportuna y de calidad de los alimentos requeridos por los programas.

Generar oportunidades que permitan incorporar a pequeños productores locales en los procesos de compra, promover innovaciones a los procesos que dinamicen la provisión de alimentos y servicios complementarios de certificación, almacenamiento y distribución.

### 2.1.2. MISIÓN[8]

La misión del Programa de Provisión de Alimentos es garantizar a los programas sociales de alimentación y nutrición del Estado, la provisión de alimentos y servicios

[8] http://www.ppa.gov.ec/index.php?option=com_content&view=article&id=44&Itemid=34

complementarios, facilitando la incorporación de pequeños productores como proveedores de los programas, en concordancia con la política de inclusión económica y social.

### 2.1.3. VISIÓN[9]

La visión del Programa de Provisión de Alimentos es ser el aliado estratégico de los programas sociales de alimentación y nutrición del estado, en la gestión operativa y logística, contribuyendo al cumplimiento de sus objetivos y metas.

### 2.1.4. UBICACIÓN ACTUAL

**Figura 2-1 Edificio matriz MIES**

El Programa de Provisión de Alimentos se encuentra actualmente funcionando en parte de los pisos tres y cuatro del edificio matriz del Ministerio de Inclusión Económica y Social ubicado en la Robles E3-33 y Páez, Quito – Ecuador (Figura 2-1).

[9] http://www.ppa.gov.ec/index.php?option=com_content&view=article&id=45&Itemid=54

### 2.1.5. NUEVA UBICACIÓN

**Figura 2-2 Nuevo edificio donde se trasladará el PPA (cuarto piso).**

El Programa de Provisión de Alimentos trasladará sus oficinas al cuarto piso del ex edificio ORI, ubicado en la Av. Orellana y 9 de octubre, previa la remodelación del espacio físico e implementación de la infraestructura de comunicaciones (Figura 2-2).

La Figura 2-3 muestra las obras de remodelación de las nuevas instalaciones del PPA.

**Figura 2-3 Etapa de remodelación de las nuevas instalaciones (cuarto piso).**

### 2.1.6. ANTECEDENTES

El Programa de Provisión de Alimentos es una entidad que se encuentra en proceso de estructuración, por lo que en la actualidad no cuenta con un espacio físico asignado exclusivamente para su funcionamiento.

El espacio físico asignado al PPA es reducido para el desarrollo de sus actividades, motivo por el cual las autoridades del MIES y PPA han acordado que el PPA traslade sus oficinas al piso cuatro del edificio ex ORI ubicado en la Av. Orellana y 9 de octubre.

El edificio al que trasladará sus oficinas el PPA fue ocupado por el ORI, siendo su distribución física inapropiada para el funcionamiento de las oficinas del PPA por lo que fue necesario remodelar las oficinas de acuerdo a las necesidades del Programa. Al finalizar los trabajos de remodelación, el Programa contará con oficinas funcionales pero carentes de infraestructura de comunicaciones de voz y datos. Por ello se ha abordado el proyecto de diseño e implementación de la infraestructura de comunicaciones la cual se la deberá implementar por etapas de acuerdo a las asignaciones presupuestarias del Estado.

El diseño de infraestructura de comunicaciones del PPA debe en lo posible seguir la línea del Software Libre, dado que es una entidad gubernamental, por lo cual se deberá buscar soluciones basadas en Software Libre de iguales o mejores prestaciones que las soluciones propietarias.

### 2.1.7. ORGANIGRAMA.

La Figura 2-4 muestra la estructura organizacional del Programa de Provisión de Alimentos, la cual se alinea con su misión estratégica y se sustenta en la filosofía de aseguramiento de la calidad en la gestión.

**Figura 2-4 Estructura orgánica del Programa de Provisión de Alimentos.**[10]


El funcionamiento del PPA se encuentra gobernado por procesos de compras de alimentos requeridos por los diferentes programas sociales en los cuales se hace énfasis en la inclusión de pequeños productores. Según su estructura orgánica sus competencias con las siguientes.

- Investigación y Estudios.- se encarga de la búsqueda de proveedores de alimentos y servicios complementarios que cumplan todos los requerimientos de calidad.
- Planificación.- se encarga de elaborar las bases de procesos de adquisición de alimentos y servicios de acuerdo a los modelos requeridos por el INCOP y cumpliendo las leyes de inclusión económica. Son los responsables de ingresar información al INCOP, monitorear los procesos y seleccionar la mejor oferta.
- Desarrollo Institucional.- se encarga de la parte financiera del programa y de cada uno de los procesos de compras. Certifica el presupuesto, actualiza anticipo, pagos parciales y liquidaciones de contratos.

10

http://www.ppa.gov.ec/index.php?option=com_content&view=article&id=49:estructura_organica&catid=25&Itemid=58

- Jurídico.- se encarga de la parte legal de los procesos de compra, supervisa la existencia y calificación de las diferentes ofertas, verifica el cumplimiento de las especificaciones de los procesos de compra, gestiona el proceso contractual, notariza los contratos y son los encargados de dar como cerrado un contrato.
- Logística y Monitoreo.- se encarga de la supervisión de la calidad, certificación, almacenamiento, distribución y facturación de los alimentos.

#### 2.1.7.1. Departamento de Gestión de Tecnologías de la Información GTI-PPA

***Misión***

Aplicar eficaz y eficientemente las tecnologías de tratamiento informático en apoyo a los objetivos, políticas y estrategias del Programa de Provisión de Alimentos.

***Atribuciones y responsabilidades.***

- Asesorar a las autoridades y funcionarios de la Institución en los campos informático y tecnológico.
- Formular proyectos y estrategias para el desarrollo tecnológico.
- Coordinar la implementación de sistemas informáticos en las unidades o procesos organizacionales.
- Elaborar y coordinar la ejecución de los planes tecnológicos y de contingencias.
- Colaborar en la evaluación de la gestión de toda la Unidad.
- Administración de redes de comunicaciones, bases de datos, correo electrónico, internet y otros servicios instalados.
- Capacitar a los usuarios en las tecnologías de la información y comunicaciones.
- Desarrollar normas tecnológicas internas de uso de hardware y de servicios instalados.

## 2.2. DESCRIPCIÓN DEL SISTEMA DE COMUNICACIONES DE VOZ Y DATOS

### 2.2.1. INFRAESTRUCTURA DE RED DE DATOS

El PPA utiliza la infraestructura de comunicaciones del MIES, por lo que GTI-PPA no es la encargada de la administración y gestión de su segmento de red, ya que no es propietaria de los equipos de conectividad, servidores, servicios y otros de los que hace uso, únicamente es propietario de las estaciones de trabajo.

Debido a que la administración y gestión de la red está a cargo del departamento de Gestión de Tecnología de Información del Ministerio (GTI-MIES), no se tiene el suficiente acceso a la información de la situación actual del segmento de red asignado al PPA, por lo que se realizará únicamente el análisis interno del segmento de red para recolectar datos que permitan diseñar la nueva infraestructura de red.

### 2.2.2. DETERMINACIÓN DEL NÚMERO DE USUARIOS

Los funcionarios que laboran actualmente en el PPA, tienen asignado para desempeñar su trabajo un computador y un teléfono IP. El PPA a pesar de gestionar la adquisición de alimentos de los programas de Alimentación Escolar (PAE), Instituto de la Niñez y la Familia (INFA), Programa de Protección Social (PPS), Aliméntate Ecuador, Instituto Nacional de Economía Popular y Solidaria (IEPS), no dispone de ninguna forma de conectividad con los mismos, lo cual se debe prever en el diseño de la infraestructura de comunicaciones del PPA, contemplando potenciales usuarios remotos a futuro, incluyéndose en este tipo de usuarios las diferentes bodegas de almacenamiento de alimentos y proveedores.

Los usuarios de la infraestructura de red son en la actualidad 26 los cuales se listan en la Tabla 2-1 distribuidos por departamentos.

**Tabla 2-1 Listado de los usuarios de acuerdo a su organización departamental.**

| USUARIOS DE LA RED | | |
|---|---|---|
| No. | **DEPARTAMENTO** | **FUNCIONARIOS** |
| 1 | COORDINACIÓN NACIONAL | Coordinador Nacional |
| 2 | | Secretaria |
| 3 | SUBCOORDINACIÓN NACIONAL | Subcoordinador Nacional |
| 4 | | Analista de soporte informático |
| 5 | | Analista informático |
| 6 | | Analista informático (Vacante) |
| 7 | INVESTIGACIÓN Y ESTUDIOS | Directora de Investigación y Estudios |
| 8 | | Supervisor de Mercados |
| 9 | | Investigadora de Mercados |
| 10 | COORDINACIÓN JURÍDICA | Coordinador Jurídico |
| 11 | | Analista Jurídico |
| 12 | | Analista Jurídico (Vacante) |
| 13 | PLANIFICACIÓN Y COMPRAS | Director de Planificación y Compras |
| 14 | | Supervisora de Planificación y Compras |
| 15 | | Analista de Planificación y Compras |
| 16 | SERVICIOS INSTITUCIONALES | Director de Desarrollo Institucional |
| 17 | | Contador General |
| 18 | | Analista de Presupuesto |
| 19 | | Analista Financiero |
| 20 | | Analista de Presupuesto |
| 21 | | Planificación y Talento Humano |
| 22 | LOGÍSTICA Y MONITOREO | Directora de Logística y Monitoreo |
| 23 | | Supervisor de Administración de Contratos |
| 24 | | Analista de Administración de Contratos |
| 25 | | Analista de Administración de Contratos |
| 26 | | Analista de Administración de Contratos |
| 27 | | Analista de Administración de Contratos |
| 28 | | Analista de Administración de Contratos |
| 29 | | Vacante |

### 2.2.3. EQUIPOS DE LA RED DE DATOS

#### 2.2.3.1. Estaciones de trabajo y periféricos

Las estaciones de trabajo son los únicos activos fijos, a nivel informático, con los que cuenta el PPA, los mismos que fueron adquiridos en abril del 2010, siendo equipos con características apropiadas para el desarrollo de las actividades de los diferentes funcionarios. El equipamiento con el que cuenta el PPA es el siguiente:

- Se cuenta con 27 PCs de escritorio de similares características, de las cuales una es usada como servidor Antivirus, además se cuenta con 4 portátiles las cuales son usadas por los funcionarios para trabajar fuera de las oficinas del PPA.
- Debido a la gran cantidad de documentos que se imprimen, el PPA cuenta con 10 impresoras IP de las cuales 7 son láser (*LaserJet* P2055dn) y 3 son matriciales (FX-2190).
- En cumplimiento a disposiciones legales es necesario almacenar la documentación en formato digital por lo que se cuenta con 2 escáneres IP (HP N8420).
- Se cuenta con 2 proyectores (EPSON *ProLite* 1735W) que permiten conexión inalámbrica.
- Todas las estaciones de trabajo cuenta con un UPS (ALTEK 1062P) para el computador y el teléfono.

La Tabla 2-2 detalla el equipamiento de equipos informáticos con los que cuenta el PPA.

**Tabla 2-2 Estaciones de trabajo y periféricos**

| EQUIPAMIENTO DE ESTACIONES DE TRABAJO | | | |
|---|---|---|---|
| Cantidad | Equipo | Características | Imagen |
| 27 | Computador | Hewlett-Packard HP<br>QuadCore Intel Core 2 Quad<br>Memoria: 4 GB<br>Disco Duro: Hitachi (320 GB, 7200 RPM, SATA-II) |  |
| 3 | Portátil | Hewlett-Packard HP<br>Mobile DualCore Intel Core 2 Duo, 2100 MHz<br>Memoria: 2 GB<br>Disco Duro: 320 GB |  |
| 1 | Portátil | Hewlett-Packard HP<br>DualCore Intel Core i5, 2133 MHz<br>Memoria: 2 GB<br>Disco Duro: Hitachi (320 GB, 7200 RPM, SATA-II) |  |
| 7 | Impresora | LaserJet P2055dn<br>Tecnología de impresión: láser<br>Conectividad: Ethernet 10/100/1000, USB 2.0 de alta velocidad |  |
| 3 | Impresora | EPSON Matricial FX-2190<br>Impresora matriz: De carro ancho y 9 agujas<br>Velocidad: 680 cps a 12 cpp / 566 cps a 10 cpp<br>Compatibilidad: ESC/P, Windows, IBM PPDS, Oki Microline |  |
| 2 | Escáner | HP N8420<br>Velocidad de escaneado: hasta 25 ppm/50 ipm (blanco y negro, 200 ppp); Hasta 20 ppm/40 ipm (color, 150 ppp) |  |

Continúa

| | | | |
|---|---|---|---|
| 2 | Proyector | EPSON ProLite 1735W<br>Wireless LAN 802.11 a/b/g<br>Brillo: 3000 lúmenes<br>Tecnología 3LCD Epson de 3-chips |  |
| 27 | UPS | ALTEK 1062P<br>Capacidad: 625 VA/280W<br>PC Back Up Time: de 5 a 20 minutos |  |

Las características técnicas de cada uno de los computadores y periféricos del PPA se detallan en el Anexo 2.1, además se cuenta con actas de entrega-recepción de cada uno de los funcionarios a los que se los responsabiliza de cada uno de los equipos (Anexo 2.2).

Para conocer el nivel de satisfacción del rendimiento de los equipos descritos se realizó una encuesta (Anexo 2.3) a los funcionarios del PPA.

A la pregunta No 1: ***¿Cómo considera el rendimiento de su computador?***

En la Figura 2-5 se observa que el 100% de los encuestados consideran “Muy Bueno” el rendimiento de los equipos. ya que son nuevos y con características suficientes para correr los programas instalados y desarrollar sus diferentes actividades.

**Figura 2-5 Rendimiento de los computadores**

A la pregunta No 2: ***¿Cómo considera el rendimiento de los periféricos al servicio del programa?***

Al igual que las estaciones de trabajo, los equipos periféricos son nuevos y se encuentran en perfectas condiciones de operación. En la Figura 2-6 se observa que la mayor parte de los usuarios considera su rendimiento como “Muy Bueno” teniendo también un pequeño porcentaje en “Excelente” y “Bueno”.

**Figura 2-6 Rendimiento de los periféricos**


### 2.2.3.2. Análisis de los racks y equipos de conectividad.

La topología física de la red es tipo estrella, las estaciones de trabajo y teléfonos IP se encuentran conectadas a los rack aéreos ubicados en cada piso; los cuales no son de uso exclusivo del PPA. Todo el equipamiento instalado en cada uno de los racks se encuentra bajo la administración del departamento de Gestión de Tecnologías de Información del Ministerio (GTI-MIES) por lo cual no se tiene acceso a su configuración.

La Figura 2-7 muestra la ubicación del rack de acceso.

**Figura 2-7 Rack aéreo de acceso**

Los racks se encuentran ubicados en una de las esquinas de cada unos de los pisos, siendo complicado su acceso. Además no se dispone de la señalización y ventilación necesaria, Estas observaciones serán tomadas en cuenta para corregirlas en el diseño de la distribución del nuevo rack.

El rack y switches mencionados no son propiedad de PPA, se deben adquirir los equipos de conectividad necesarios para la nueva infraestructura de comunicaciones.

#### 2.2.3.3. Direccionamiento IP (Datos).

El Ministerio tiene asignado un mismo dominio de broadcast TCP/IP. El direccionamiento IP se realiza de acuerdo a la subred 10.2.0.0/16 con puerta de enlace 10.2.70.247 cuyos DNS primario y secundario son 10.2.70.11 y 10.2.70.13 respectivamente, teniendo un total de 65534 direcciones IP disponibles, de las cuales el PPA en sus computadores, portátiles, impresoras y escáneres tiene asignado el rango de direcciones de la 10.2.100.1 a 10.2.100.254. El direccionamiento IP dado al PPA no se encuentra basado en ningún tipo de segmentación de red lo cual deberá ser corregido en el diseño de la nueva infraestructura de comunicaciones.

La direcciones IP asignadas a las estaciones de trabajo y teléfonos no son mediante DHCP por lo que cada máquina está configurada con una dirección IP estática. El direccionamiento IP se encuentra detallado en la Tabla 2-3.

**Tabla 2-3 Direccionamiento IP Datos.**

| DIRECCIONAMIENTO IP | | | | | | |
|---|---|---|---|---|---|---|
| No. | Equipos | Hostname | Dirección IP | Gateway | DNS Prim. | DNS Sec. |
| | **COORDINACIÓN NACIONAL** | | | | | |
| 1 | Coordinador Nacional | 25TPPACN170103 | 10.2.100.35/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 2 | Impresora | | 10.2.100.43/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 3 | Portátil Coordinador | 04PPPAIM170103 | 10.2.100.48/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 4 | Portátil Ministerio | 03PPPALM170103 | 10.2.100.52/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 5 | Secretaria | 05TPPACN170103 | 10.2.100.15/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 6 | Impresora | | 10.2.100.42/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 7 | Escáner | | 10.2.100.47/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | **SUBCOORDINACIÓN NACIONAL** | | | | | |
| 8 | Subcoordinador Nacional | 24TPPACN170103 | 10.2.100.34/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 9 | Analista de soporte informático | 09TPPADSI170103 | 10.2.100.19/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 10 | Analista informático | 14TPPADSI170103 | 10.2.100.24/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 11 | Servidor Antivirus | 01SPPADSI170103 | 10.2.100.37/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 12 | Impresora ricoh | | 10.2.100.185/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | **INVESTIGACIÓN Y ESTUDIOS** | | | | | |
| 13 | Directora | 02TPPADIE170103 | 10.2.100.12/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 14 | Supervisor de Mercados | 01TPPADIE170103 | 10.2.100.11/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 15 | Investigadora de Mercados | 04TPPADIE170103 | 10.2.100.14/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 16 | Portátil | 02PPPAPC170103 | 10.2.100.51/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 17 | Impresora | | 10.2.100.44/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | **COORDINACIÓN JURÍDICA** | | | | | |
| 18 | Coordinador | 15TPPACN170103 | 10.2.100.25/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 19 | Analista | 22TPPACN170103 | 10.2.100.32/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 20 | Impresora | | 10.2.100.45/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | | | | | | |

Continúa

| | | | | | | |
|---|---|---|---|---|---|---|
| | **PLANIFICACIÓN Y COMPRAS** | | | | | |
| 21 | Director | 07TPPADP170103 | 10.2.100.17/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 22 | Supervisora | 08TPPADP170103 | 10.2.100.18/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 23 | Analista | 06TPPADP170103 | 10.2.100.16/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 24 | Portátil | 02PPPADP170103 | 10.2.100.50/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 25 | Impresora | | 10.2.100.41/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | **SERVICIOS INSTITUCIONALES** | | | | | |
| 26 | Director | 13TPPADSI170103 | 10.2.100.23/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 27 | Contador General | 12TPPADSI170103 | 10.2.100.22/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 28 | Analista de Presupuesto | 10TPPADSI170103 | 10.2.100.20/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 29 | Analista Financiero | 11TPPADSI170103 | 10.2.100.21/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 30 | Analista de Presupuesto | 23TPPADSI170103 | 10.2.100.33/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 31 | Planificación y Talento Humano | 16TPPADSI170103 | 10.2.100.26/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 32 | Impresora DGL | | 10.2.100.40/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| | **LOGÍSTICA Y MONITOREO** | | | | | |
| 33 | Directora | 19TPPADGL170103 | 10.2.100.29/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 34 | Supervisor de Admin. Contratos | 03TPPADGL170103 | 10.2.100.13/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 35 | Analista de Admin. de Contratos | 17TPPADGL170103 | 10.2.100.27/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 36 | Analista de Admin. de Contratos | 18TPPADGL170103 | 10.2.100.28/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 37 | Analista de Admin. de Contratos | 21TPPADGL170103 | 10.2.100.31/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 38 | Analista de Admin. de Contratos | 03TPPADIE170103 | 10.2.100.30/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 39 | Analista de Admin. de Contratos | 26TPPADGL170103 | 10.2.100.36/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 40 | Portátil | 03PPPADGL170103 | 10.2.100.49/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 41 | Impresora DSI | | 10.2.100.39/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |
| 42 | Escáner | | 10.2.100.46/16 | 10.2.70.247 | 10.2.70.11 | 10.2.70.13 |

### 2.2.4. EQUIPOS DE LA RED DE VOZ

El PPA cuenta con el servicio de telefonía IP distribuido a cada estación de trabajo por el mismo circuito de datos del computador. Los teléfonos IP con los que cuenta el PPA son de dos marcas, 3COM y FANVIL los cuales tienen dos puertos RJ45 en los que se conectan a la LAN y al computador respectivamente (Figura 2-8). Ambos tipos de teléfonos utilizan el adaptador de energía eléctrica, los FANVIL necesariamente deben utilizarlos ya que no soportan PoE. Las características técnicas de los teléfonos IP se detallan en el Anexo 2.1.

Al igual que la red de datos, la red de telefonía IP se encuentra administrada por GTI-MIES por lo cual no se tiene acceso a la información de configuraciones de la central telefónica y teléfonos IP.

**Figura 2-8 Conexiones (de izquierda a derecha): Alimentación eléctrica, a la PC, al Switch.**

#### 2.2.4.1. Teléfonos IP

Los teléfonos VoIP con los que cuenta el PPA son un total de 26, cada funcionario tiene en su estación de trabajo un teléfono. Se dispone de teléfonos de dos marcas (FANVIL y 3COM) los cuales son los más básicos en su marcas. Los telefonos con los que cuenta el PPA se detallán en la Tabla 2-4.

**Tabla 2-4 Teléfonos IP**

| EQUIPAMIENTO DE LA RED DE VOZ | | | |
|---|---|---|---|
| No | Equipo | Características | Gráfico |
| 15 | Teléfono IP FANVIL | FANVIL BW320<br>WAN: 10/100Base- T RJ-45 para LAN<br>LAN: 10/100Base- T RJ-45 para PC<br>Soporta 2 líneas SIP y IAX2, SIP 2.0 (RFC3261) |  |
| 11 | Teléfono IP 3COM | 3Com® 3101 Basic Phone<br>Mobile DualCore Intel Core 2 Duo, 2100 MHz<br>Dual-port 10/100 switched Ethernet<br>Soporta plataformas 3Com NBX y 3Com basado en SIP VCX |  |

### 2.2.4.2. Direccionamiento IP (Voz)

Los teléfonos IP se encuentran en el mismo dominio de broadcast de la red de datos. Los teléfonos tienen asignados direcciones IP en el rango de 10.2.72.20 a 10.2.72.100 de forma estática con gateway 10.2.72.1. En la Tabla 2-5 se encuentra detallado el tipo de teléfono de cada funcionario, la distribución de extensiones y el direccionamiento IP de los teléfonos.

**Tabla 2-5 Distribución de teléfonos y su direccionamiento IP**

| TELÉFONOS IP | | | | | |
|---|---|---|---|---|---|
| No. | Equipos | Tipo Fono. IP | Ext. | Direccionamiento IP | |
| | | | | Dirección IP | Gateway |
| | **COORDINACIÓN NACIONAL** | | | | |
| 1 | Coordinador Nacional | 3COM | 1822 | 10.2.72.24/16 | 10.2.70.1 |
| 2 | Secretaria | 3COM | 1819 | 10.2.72.25/16 | 10.2.70.1 |
| | **SUBCOORDINACIÓN NACIONAL** | | | | |
| 3 | Subcoordinador Nacional | FANVIL | 1350 | 10.2.72.26/16 | 10.2.70.1 |
| 4 | Analista de soporte informático | FANVIL | 1467 | 10.2.72.28/16 | 10.2.70.1 |
| 5 | Analista informático | FANVIL | 1466 | 10.2.72.27/16 | 10.2.70.1 |

Continúa

| | | | | | |
|---|---|---|---|---|---|
| | **INVESTIGACIÓN** | | | | |
| 6 | Directora de Investigación y Estudios | 3COM | 1965 | 10.2.72.31/16 | 10.2.70.1 |
| 7 | Supervisor de Mercados | FANVIL | 1354 | 10.2.72.39/16 | 10.2.70.1 |
| 8 | Investigadora de Mercados | FANVIL | 1355 | 10.2.72.40/16 | 10.2.70.1 |
| | **COORDINACIÓN JURÍDICA** | | | | |
| 9 | Coordinador Jurídico | 3COM | 1053 | 10.2.72.33/16 | 10.2.70.1 |
| 10 | Analista Jurídico | FANVIL | 1353 | 10.2.72.52/16 | 10.2.70.1 |
| | **COMPRAS** | | | | |
| 11 | Director de Planificación y Compras | 3COM | 1821 | 10.2.72.34/16 | 10.2.70.1 |
| 12 | Supervisora de Planificación y Compras | FANVIL | 1351 | 10.2.72.32/16 | 10.2.70.1 |
| 13 | Analista de Planificación y Compras | FANVIL | 1352 | 10.2.72.35/16 | 10.2.70.1 |
| | **SERVICIOS INSTITUCIONALES** | | | | |
| 14 | Director de Desarrollo Institucional | 3COM | 1054 | 10.2.72.43/16 | 10.2.70.1 |
| 15 | Contador General | FANVIL | 1468 | 10.2.72.29/16 | 10.2.70.1 |
| 16 | Analista de Presupuesto | FANVIL | 1473 | 10.2.72.41/16 | 10.2.70.1 |
| 17 | Analista Financiero | FANVIL | 1469 | 10.2.72.30/16 | 10.2.70.1 |
| 18 | Analista de Presupuesto | FANVIL | 1474 | 10.2.72.42/16 | 10.2.70.1 |
| 19 | Planificación y Talento Humano | 3COM | 1967 | | 10.2.70.1 |
| | **LOGÍSTICA Y MONITOREO** | | | | |
| 20 | Directora de Logística y Monitoreo | FANVIL | 1470 | 10.2.72.36/16 | 10.2.70.1 |
| 21 | Supervisor de Administración de Contratos | 3COM | 1820 | 10.2.72.44/16 | 10.2.70.1 |
| 22 | Analista de Administración de Contratos | FANVIL | 1472 | 10.2.72.38/16 | 10.2.70.1 |
| 23 | Analista de Administración de Contratos | 3COM | 1126 | 10.2.72.45/16 | 10.2.70.1 |
| 24 | Analista de Administración de Contratos | 3COM | 1609 | 10.2.72.46/16 | 10.2.70.1 |
| 25 | Analista de Administración de Contratos | 3COM | 1709 | 10.2.72.47/16 | 10.2.70.1 |
| 26 | Analista de Administración de Contratos | FANVIL | 1471 | 10.2.72.37/16 | 10.2.70.1 |

### 2.2.5. APLICACIONES Y SERVICIOS.

#### 2.2.5.1. Aplicaciones usadas en las estaciones de trabajo.

El PPA como entidad gubernamental se encuentra en el proceso de migración a software libre de su plataforma a nivel de usuario, si bien el sistema operativo con el que trabajan todavía es propietario (Windows 7 Profesional) las aplicaciones como el cliente de correo (Thunderbird) y la suite ofimática (openOffice) utilizan Software Libre. La Tabla 2-6 muestra el software instalado en cada una de las máquinas, divididas por departamentos.

**Tabla 2-6 Aplicaciones utilizadas en las estaciones de trabajo.**

| APLICACIONES | | | | | | | |
|---|---|---|---|---|---|---|---|
| **PROGRAMAS** | **USUARIOS – DEPARTAMENTOS** | | | | | | |
| | Coordinación | Investigación | Compras | Desarrollo Institucional | Jurídico | Logística | Gestión Tecnológica |
| OpenOffice.org 3.1 [español] | √ | √ | √ | √ | √ | √ | √ |
| Mozilla Thunderbird (3.0.4) | √ | √ | √ | √ | √ | √ | √ |
| Mozilla Firefox (3.5.2) | √ | √ | √ | √ | √ | √ | √ |
| ESET Smart Security | √ | √ | √ | √ | √ | √ | √ |
| Software contable (SRI) | | | | √ | | | |
| Software contable (Master Field) | | | | √ | | | |
| EVEREST Ultimate Edition v5.30 | √ | √ | √ | √ | √ | √ | √ |
| Adobe Flash Player 10 ActiveX | √ | √ | √ | √ | √ | √ | √ |
| Adobe Flash Player 10 Plugin | √ | √ | √ | √ | √ | √ | √ |
| Adobe Reader 9.2 - Español | √ | √ | √ | √ | √ | √ | √ |
| Advanced IP Scanner v1.5 | | | | | | | √ |
| Alfresco Community Edition | | | | | | | √ |
| Complemento Guardar como PDF o XPS de | √ | √ | √ | √ | √ | √ | √ |

Continúa

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Microsoft | | | | | | | |
| Compresor WinRAR | √ | √ | √ | √ | √ | √ | √ |
| Cool PDF Reader 3.0 | √ | | | | | | √ |
| GPL Ghostscript 8.60 | | | | | | | √ |
| GPL Ghostscript Fonts | | | | | | | √ |
| GSview 4.8 | | | | | | | √ |
| Windows Live | √ | √ | √ | √ | √ | √ | √ |
| Intel(R) Graphics Media Accelerator Driver | √ | √ | √ | √ | √ | √ | √ |
| Java(TM) SE Development Kit 6 Update 16 | √ | √ | √ | √ | √ | √ | √ |
| Media Player Codec Pack 3.9.5 | √ | √ | √ | √ | √ | √ | √ |
| Microsoft .NET Framework 4 Client Profile | √ | √ | √ | √ | √ | √ | √ |
| Microsoft Office 2007 | | | | | | | √ |
| Microsoft Visio Professional 2002 | | | | | | | √ |
| MozBackup 1.4.10 | | | | | | | √ |
| Oracle VM VirtualBox 3.2.4 | | | | | | | √ |
| PDF Complete Special Edition | √ | √ | √ | √ | √ | √ | √ |
| Realtek High Definition Audio Driver | √ | √ | √ | √ | √ | √ | √ |
| siise [español (españa, tradicional)] | | | | | | | √ |
| SIISE_CONEXION | | | | | | | √ |
| Tecnología de gestión activa Intel® | √ | √ | √ | √ | √ | √ | √ |
| VLC media player 1.0.5 1.0.5 | √ | √ | √ | √ | √ | √ | √ |
| XnView 1.96.5 1.96.5 | √ | √ | √ | √ | √ | √ | √ |
| HP Support Assistant | √ | √ | √ | √ | √ | √ | √ |
| HPAsset component for HP Active Support Library | √ | √ | √ | √ | √ | √ | √ |
| ActiveCheck component for HP Active Support Library 3.0.0.2 | √ | √ | √ | √ | √ | √ | √ |

Para conocer las aplicaciones que los funcionarios habitualmente utilizan en sus actividades laborales y el nivel de satisfacción del paquete de ofimática (*OpenOffice*) y el cliente de correo (*Thunderbird*), programas que fueron migrados a Software Libre se realizaron las preguntas 3, 4 y 5 en la encuesta (ANEXO 2.3).

A la pregunta No 3: ***¿Qué aplicaciones son las que usted utiliza en el desarrollo de sus actividades laborales?***

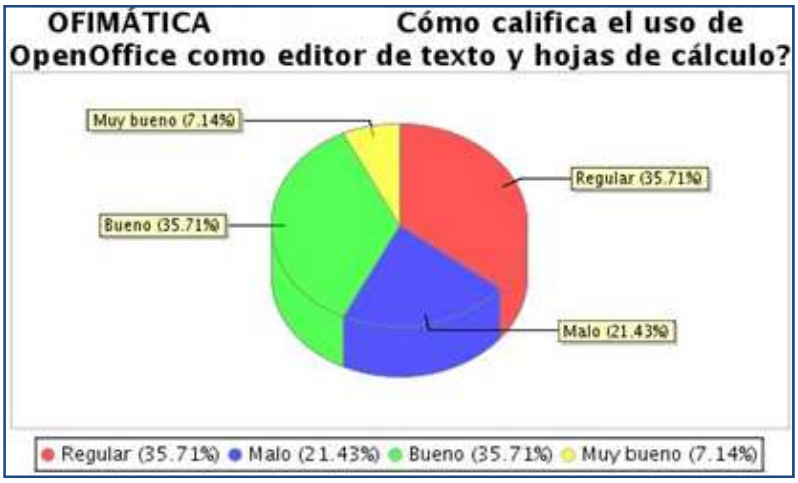
La Figura 2-9 muestra que el 100% de los encuestados utilizan los servicios de telefonía, correo electrónico, internet y el sistema de administración SICOPPA, alrededor del 43% usan el servicio de videoconferencia a través de *Skype* el cual se ve deteriorado por el mal servicio de internet con el que se cuenta, el 29% utilizan el servicio chat personal ya que no se cuenta con un servicio institucional similar.

**Figura 2-9 Aplicaciones más utilizadas**


A la pregunta No 4: ***¿Cómo califica el uso de openOffice como editor de texto y hojas de cálculo?***

La Figura 2-10 muestra que el 36% de los encuestados lo califica como “Regular”, el otro 36% lo califica como “Bueno”, el 21% lo califica como “Malo” y solo el 7% lo califica como “Muy bueno”, con estos resultados se puede apreciar que los usuarios no se acostumbran al cambio de la suite ofimática *Microsoft Office* a *OpenOffice* o que la capacitación recibida no fue la suficiente, además actualmente se utiliza la versión 3.0 siendo la última versión estable la 3.3, software que deberá ser actualizado.

**Figura 2-10 Nivel de satisfacción de openOffice**




A la pregunta No 5: ***¿Qué tan amigable es el cliente de correo Thunderbird?***

Al contrario de *OpenOffice* en la Figura 2-11 se observa que el cliente de correo *Thunderbird* ha sido aceptado de mejor manera, esto debido a que su entorno es muy similar al *Outlook de Microsoft*. El 36% de los encuestados lo consideran como "Muy bueno", el 50% lo considera como "Bueno" y apenas el 14% lo considera como "Regular" que es un pequeño porcentaje a los cuales se les tomará en cuenta para una capacitación.

**Figura 2-11 Nivel de satisfacción del cliente de correo Thunderbird.**

#### 2.2.5.2. Internet

Para el PPA el servicio de Internet es crítico, ya que además de las diversas consultas en Internet, los funcionarios están en constante interacción con los sistemas informáticos de los diferentes programas sociales, sistemas de entidades gubernamentales y sobre todo con el INCOP. Los sistemas informáticos con los que trabaja el PPA son:

##### *2.2.5.2.1. Sistemas de Programas Sociales*

**SUBYT (Administración de Bodegas y de Transporte).-** es una herramienta informática desarrollada por el Programa Aliméntate Ecuador (PAE) para sistematizar los procesos de Administración, Transporte y Bodega. Es un sistema desarrollado en tres capas que presenta información del estado de stock en bodega y de seguimiento de orden de compras.

**SIPAE (Sistema de la Investigación de la Problemática Agraria del Ecuador).-** funciona como una cooperativa de investigación y análisis de propuestas políticas agrarias que hace circular los resultados entre las instituciones miembros y hacia el exterior.

##### *2.2.5.2.2. Sistemas de Entidades Gubernamentales*

**INCOP (Sistema Nacional de Contratación Pública).-** cuenta con una herramienta informática que permite transparentar los procesos de contratación entre proveedores y contratantes, controlando que esos procesos sean justos y accesibles a todo público. Esta herramienta es usada constantemente por el PPA para la adquisición de alimentos, dándole igual oportunidad al pequeño y gran productor nacional. Cabe recalcar que el PPA es la segunda entidad gubernamental que más procesos de compra en el INCOP realiza, lanzando un promedio de 3 procesos de compra al día.

**ESIGEF (Sistema Integrado de Gestión Financiera).-** es una herramienta web de gestión financiera, utilizado por el departamento de desarrollo institucional del PPA para el registro de transacciones financieras de la entidad.

**ESIPREN (Sistema Presupuestario de Remuneraciones y Nómina).-** es una herramienta web que utiliza el PPA para la aprobación de la nómina y el registro de las afectaciones financieras que la nómina genera.

**SIGOB (Sistema de Información para la Gobernabilidad).-** es un sistema en el cual el PPA monitorea el cumplimiento de sus metas, agendas de actividades interministeriales, compromisos presidenciales, decretos ejecutivos, indicadores y estadísticas, gabinetes sectoriales y ejecución presupuestaria.

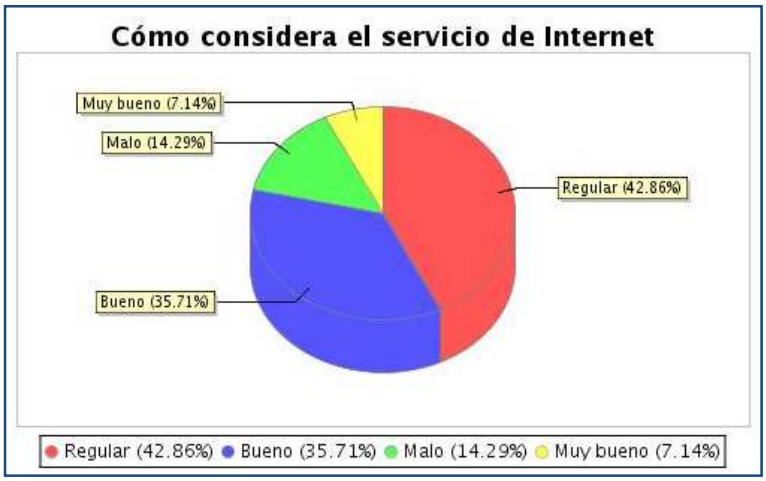
**SIPLAN (Sistema Integrado de Planificación).-** es una herramienta informática que permite la articulación de la planificación nacional con el presupuesto a través de la alineación de los Objetivos Estratégicos Institucionales, en este caso del PPA, al Plan Nacional del Desarrollo a nivel de objetivos, políticas, metas e indicadores; además se vincula con el Sistema de Inversión Pública (SIP) y el ESIGEF.

Según la encuesta realizada (Anexo 2.2) en la pregunta 6 se pretende conocer el nivel de servicio del Internet.

A la pregunta No 6: ***¿Cómo considera el servicio de Internet?***

El servicio de Internet es uno de los más deficientes con los que cuenta actualmente el PPA, solo aquellos funcionarios que se conectan al anillo presidencial cuenta con un nivel de disponibilidad aceptable En la Figura 2-12 (resultado de la encuesta) se observa que el 14% lo cataloga como “Malo”, el 43% lo considera “Regular”, el 36% lo considera “Bueno”, y únicamente el 7% lo considera “Muy bueno”.

**Figura 2-12 Nivel de satisfacción del servicio de Internet**




Estas observaciones serán tomadas en cuenta al momento de dimensionar el enlace al ISP, evitando cometer los mismos errores y teniendo claro lo crítico del servicio para el desarrollo de las actividades del PPA.

Cabe mencionar que todos los procesos de contratación del PPA los realiza por medio del INCOP, cuyos procesos se encuentran limitados por tiempos (días, incluso horas) por lo que no contar con el servicio de Internet hace que procesos se caigan o se declaren desiertos, lo que provocaría problemas legales, políticos y lo más importante se retrasaría la compra de alimentos para los programas sociales.

#### 2.2.5.3. Telefonía

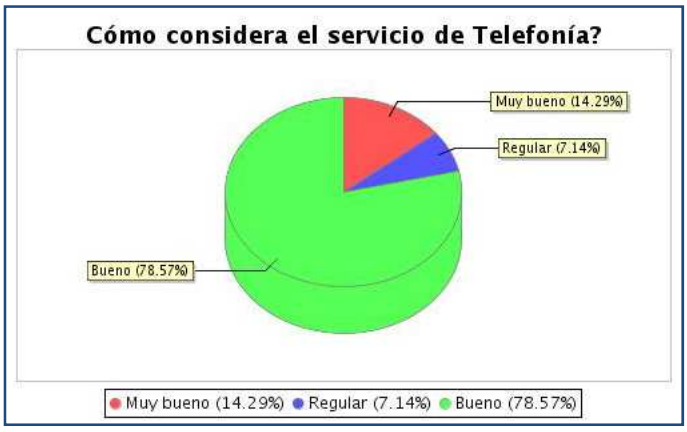
Si bien no se cuenta con información de la topología de la red de voz, ni la configuración de los equipos, se ha hecho el inventario de los teléfonos IP con los que cuenta el PPA, ya que es muy posible, que en un principio los teléfonos IP sean utilizados por el PPA en las nuevas instalaciones mientras se cuenta con el dinero para adquirir teléfonos nuevos.

Con el fin de conocer el nivel de servicio de la Telefonía IP y del rendimiento de los teléfonos IP se ha realizado la pregunta 7 en la encuesta de satisfacción (ANEXO 2.2).

A la pregunta No 7: ***Cómo considera el servicio de Telefonía?***

Con el servicio de Telefonía no se ha tenido mayor problema, la única observación es que ambos tipos de teléfonos IP son los más básicos en su respectiva marca por lo que en horas pico se percibe interferencia y cruce de llamadas pero que se solucionan volviendo a marcar. En Figura 2-13 se observa que el 14% lo considera como “Muy bueno”, el 79% lo considera “Bueno”, y el 7% como “Regular”.

**Figura 2-13 Nivel de satisfacción del servicio de Telefonía IP**




### 2.2.5.4. Página Web

En la Figura 2-14 se observa la página web informativa (*www.ppa.gob.ec)* con la que cuenta el PPA, la ‘pagina se encuentra en un servidor administrado por el MIES y está montada sobre joomla 1.5.22 en un servidor Windows server 2003.

**Figura 2-14 Página web PPA (www.ppa.gob.ec)**

Actualmente se ha registrado el dominio del PPA con una dirección IP pública proporcionada por GTI-MIES, con la cual se ha podido salir a Internet desde el 15 de junio del 2010. Si bien el diseño inicial fue realizado por GTI-MIES, luego el control se la trasladó a GTI-PPA.

Al publicar el sitio web se ha buscado proyectar la imagen del PPA por que se ha cambiado la estructura de la página de acuerdo a sus procesos y estructura orgánica (Figura 2-15).

**Figura 2-15 Diagrama de distribución y organización de la página web**

<table>
<tr><th colspan="2">NUESTRO PROGRAMA</th><th>LEY DE TRANSPARENCIA</th><th>DOCUMENTOS</th><th>CONSULTAS</th><th>MAPA DEL SITIO</th><th>CONTACTO</th></tr>
<tr><td colspan="2">VISION<br>MISION<br>OBJETIVOS</td><td>ESTRUCTURA ORGANICA</td><td>ESPECIFICACIONES TECNICAS DE PRODUCTOS</td><td>PROCESO DE COMPRA DE ALIMENTOS</td><td rowspan="11"></td><td>SUGERENCIAS</td></tr>
<tr><td colspan="2">DIRECTORIO</td><td>LEYES Y REGLAMENTOS</td><td>REQUISITOS PARA SER PROVEEDORES</td><td>FERIAS INCLUSIVAS</td><td rowspan="10">OFERTAS DE NUEVOS PRODUCTOS</td></tr>
<tr><td rowspan="6">COMUNICACION</td><td rowspan="2">AGENDA DE EVENTOS</td><td>METAS Y OBJETIVOS</td><td>FICHAS TECNICAS</td><td>PROVEEDORES</td></tr>
<tr><td>DISTRIBUTIVO DE SUELDOS</td><td>BROCHURE DE FERIAS Ajustar fila de tabla</td><td>PRODUCTOS</td></tr>
<tr><td>NOTICIAS</td><td>FORMULARIOS</td><td rowspan="8"></td><td>ARTES</td></tr>
<tr><td>GALERIA DE FOTOS</td><td>PRESUPUESTO</td><td>INDICADORES SIGOB</td></tr>
<tr><td>GALERIA DE VIDEOS</td><td>AUDITORIAS</td><td rowspan="7"></td></tr>
<tr><td>DOCUMENTOS</td><td>CONTRATOS</td></tr>
<tr><td colspan="2" rowspan="3"></td><td>PLANES Y PROGRAMAS</td></tr>
<tr><td>RENDICION DE CUENTAS</td></tr>
<tr><td>VIATICOS</td></tr>
</table>

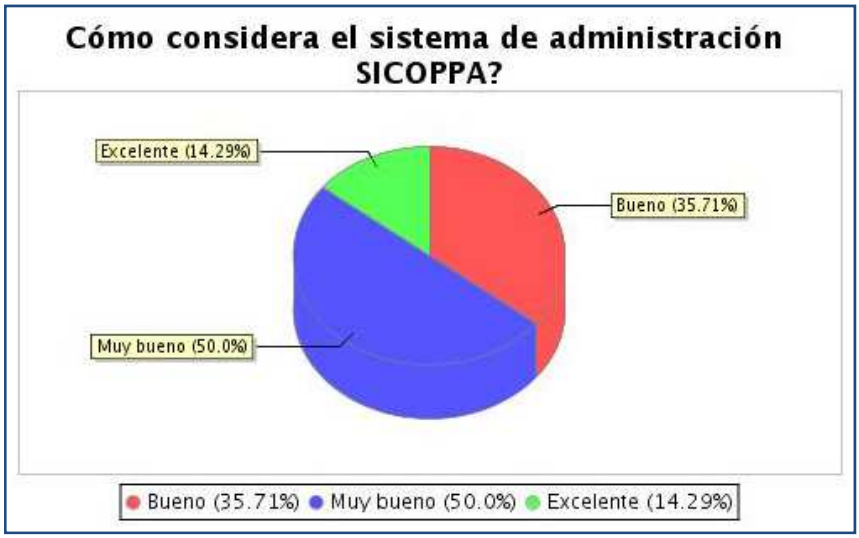
### 2.2.5.5. Sistema de Administración SICOPPA.

El sistema de administración SICOPPA se encuentra en la fase de desarrollo por parte de GTI-PPA, ciertos módulos del sistema actualmente se encuentran ya en producción para su respectiva depuración. El sistema permite registrar todos los estados por lo que pasa un proceso de compra. Una descripción más a fondo de SICOPPA se encuentra en el Anexo 2.3.

Según la encuesta realizada (Anexo 2.2), en la pregunta 9 se pretende conocer en cuanto ha aportado el sistema SICOPPA a los diferentes funcionarios en la toma de decisiones y evaluación de resultados.

***A la pregunta No 9: Cómo considera el sistema de administración SICOPPA?*** En la Figura 2-16 se observa que debido a la gran ayuda que resulta el sistema SICOPPA para los diferentes funcionarios del PPA, el 14% de los encuestados lo considera "Excelente", el 50% lo considera "Muy bueno", y el 36% lo considera "Bueno".

**Figura 2-16 Nivel de satisfacción del sistema de administración SICOPPA**




### 2.2.6. DESCRIPCIÓN DE LA SEGURIDAD

La seguridad informática se encuentra administrada por GTI-MIES por lo que no se tiene información de su configuración, políticas, y equipos con los que cuenta, además no es de mucha ayuda, ya que al no ser propiedad del PPA no se puede contar con los mismos para la implementación de la nueva infraestructura de red.

A nivel institucional se cuenta con un servidor Antivirus, el cual es administrado por GTI-PPA. El sistema de seguridad utilizado es el *ESET Smart Security* 4 que utiliza el antivirus *ESET NOD 32* junto con un cortafuegos personal y módulos contra correo no

deseado, los cuales forman un sistema contra ataques y software mal intencionado que evitan poner en peligro los equipos del PPA.

La tecnología utilizada es capaz de eliminar la penetración de virus, *spyware*, troyanos, gusanos, *adware, rootkits* y otros ataques que proceden de Internet sin entorpecer el rendimiento del sistema ni perturbar el equipo *Smart Security*.

*ESET Smart Security* está formado por módulos, de los cuales el PPA utiliza los que se detallan en la Tabla 2-7.

**Tabla 2-7 Servidor Antivirus**

| **ANTIVIRUS Y ANTIESPÍA** | |
|---|---|
| **Característica** | **Descripción** |
| Desinfección mejorada | El sistema antivirus desinfecta y elimina de forma inteligente la mayoría de las amenazas detectadas sin requerir la intervención del usuario. |
| Archivos de actualización más pequeños | Los procesos de optimización del núcleo generan archivos de actualización de menor tamaño que en la versión 2.7. Además, se ha mejorado la protección de los archivos de actualización contra daños. |
| Protección de los clientes de correo más conocidos | Ahora es posible analizar el correo entrante no sólo en MS Outlook, sino también en Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird. |
| Diversas mejoras secundarias | Acceso directo a sistemas de archivos para lograr una gran velocidad y un excelente rendimiento.<br>Bloqueo del acceso a los archivos infectados.<br>Optimización para el Centro de seguridad de Windows, incluido Vista. |
| | |
| **Cortafuegos Personal** | |
| **Característica** | **Descripción** |
| Análisis de comunicación de red de capa baja | El análisis de comunicación de red en la capa del vínculo de datos permite al firewall personal de ESET superar una serie de ataques que, de otra forma, no se podrían detectar. |
| Compatibilidad con IPv6 | El firewall personal de ESET muestra las direcciones IPv6 y permite a los usuarios crear reglas para ellas. |
| Supervisión de archivos | Supervisión de los cambios en los archivos ejecutables para superar la |

Continúa

| | |
|---|---|
| ejecutables | infección. Se puede permitir la modificación de archivos de aplicaciones firmadas. |
| Análisis de archivos integrado con HTTP y POP3 | Análisis de archivos integrado en los protocolos de aplicación HTTP y POP3. Los usuarios estarán protegidos cuando naveguen por Internet o descarguen mensajes de correo electrónico. |
| Sistema de detección de intrusiones | Capacidad para reconocer el carácter de la comunicación de red y diversos tipos de ataques de red y una opción para prohibir automáticamente dicha comunicación. |
| Compatibilidad con el modo automático, de aprendizaje, basado en las directrices, interactivo y automático con excepciones. | Los usuarios pueden seleccionar si las acciones del firewall se ejecutarán automáticamente o si desean establecer reglas interactivamente. La comunicación en el modo basado en las directrices se administra según las reglas definidas por el usuario o por el administrador de red. En el modo de aprendizaje, se pueden crear y guardar automáticamente las reglas; este modo se recomienda para la configuración inicial del firewall. |
| Sustitución del cortafuegos de Windows integrado | Sustituye al firewall de Windows integrado y también interactúa con el Centro de seguridad de Windows de modo que el usuario siempre está informado sobre su estado de seguridad. La instalación de ESET Smart Security desactiva el firewall de Windows de forma predeterminada. |

## 2.3. ANÁLISIS DE REQUERIMIENTOS

En base al análisis de la situación actual de la infraestructura de comunicaciones sobre la cual el PPA realiza sus actividades se desprenden los siguientes requerimientos para el diseño de la red:

- Se deberá diseñar el Sistema de Cableado Estructurado que soporte un ancho de banda suficiente para aplicaciones de voz, datos y video según las normas y estándares internacionales para tal efecto.
- Se deberá diseñar la estructura lógica y física de la red LAN según la estructura organizacional del Programa de tal forma que evite cuellos de botella y tráfico de datos innecesario.

- Se deberá diseñar la red inalámbrica como complemento de la red cableada para el acceso a la red LAN en lugares en donde no se ha provisto puntos de red y dónde es necesario el uso de conexión inalámbrica.
- Se deberá dimensionar los equipos de conectividad, servidores, periféricos y otros, de acuerdo al nivel de tráfico a manejar en la red, niveles de seguridad y administración.
- La infraestructura de comunicaciones deberá constar con políticas de seguridad de la información que resguarden a la misma.
- Se deberá diseñar un sistema de monitoreo para gestionar la red según las normas y políticas de seguridad de la información establecidas.

Los servicios y aplicaciones con los que dispondrá el PPA son:

**Servicio de Internet**

Debido a la importancia que tiene este servicio para el PPA por la gran cantidad de transacciones que se realizan a través de este medio se deberá realizar el análisis de tráfico a Internet para la contratación del ancho de banda adecuado del enlace al ISP y contar con métodos de redundancia del servicio.

**Servicio de Telefonía IP**

El servicio de telefonía IP es el segundo servicio en orden de prioridad, después de Internet, que el PPA hace uso para sus actividades. Se deberá realizar el análisis del tráfico del servicio de telefonía IP para la respectiva contratación de troncales, de tal forma que no se pierdan llamadas.

Además se deberá dar una opción del servicio de Telefonía IP a través de software libre que se ejecute bajo una plataforma hardware debidamente dimensionada para su correcto funcionamiento.

Además el PPA al ser una entidad que trabaja directamente con los programas sociales debe mantener una comunicación con los mismos, por lo que se prevé la telefonía IP como un medio de comunicación.

**Servicio de Correo Electrónico**

El servicio de correo electrónico es una de las herramientas imprescindibles en cualquier ambiente de trabajo y el PPA no es la excepción, por lo cual se deberá constar con dicho servicio de forma eficiente. El servicio de correo electrónico es utilizado por todos los funcionarios del PPA y les permite constar con una comunicación interactiva.

**Sistema de Administración SICOPPA (Sistema de Compras PPA)**

A pesar de encontrarse en su etapa de desarrollo, ciertos módulos del sistema SICOPPA ya se encuentran en producción, siendo de gran utilidad para todos los funcionarios en cuanto a la administración de contratos, resumen de resultados, identificación de productos, proveedores y toma de decisiones. Según la encuesta, alrededor del 93% del personal hace uso de este sistema, los cuales manifiestan su satisfacción con el sistema. El desarrollo del sistema de administración SICOPPA se encuentra a cargo de GTI-PPA.

**Servicio de Mensajería Instantánea**

Es uno de los servicios con los que no cuenta el PPA y que es demandado por sus usuarios, como parte de la infraestructura del Ministerio se hacía uso del servicio de mensajería instantánea pública como yahoo, gmail, etc, exclusivamente para mandos superiores. En la infraestructura de comunicaciones del PPA se deberá ofrecer el servicio de mensajería instantánea privada de uso interno.

**Servicio de Videoconferencia**

Este servicio es uno de los más requeridos por el Programa, pero que se encuentra limitado por el ancho de banda que se maneja en el Ministerio. Es uno de los servicios

de gran importancia para el Programa para poder entablar conversaciones con los diferentes proveedores de alimentos que se encuentran en las diferentes provincias.

De forma específica será de gran ayuda para el coordinador nacional, el cual viaja constantemente y al mismo tiempo debe coordinar reuniones en el PPA, y para el departamento de Logística, los cuales son los encargados de la supervisión de los alimentos, lo cual hace que deban viajar a las diferentes bodegas de almacenamiento de alimentos y los cuales deben mantener al mismo tiempo reuniones en las instalaciones del PPA.

**Servicio de Videoseguridad**

Al pasar a ser independientes de los servicios del Ministerio, la seguridad del personal y activos fijos pasan a ser administrados por el PPA, por lo que se crea la necesidad de constar con cámaras que registren los diferentes acontecimientos, este servicio se lo dispondrá utilizando el protocolo TCP/IP a través la infraestructura de comunicaciones de voz, datos y video del PPA.

**Servicios Intranet**

Se deberá disponer de todos los servicios Intranet necesarios para poner en marcha el funcionamiento de la red, entre los servicios Intranet que se dispondrán son: servicio de directorio, servicio DNS, servicio DHCP, página *web*, servicio de transferencia de archivos FTP, servicio de impresión y demás servicios que sean necesarios para el correcto funcionamiento de las actividades del PPA y permita que la red sea administrable y segura.

**Aplicaciones a nivel de usuario**

Entre las aplicaciones a nivel de usuario, el principal inconveniente encontrado es la falta de adaptación a la suite ofimática *openOffice* a pesar de haberse realizado una capacitación de 20 horas por parte de *SasLibre* (empresa que impulsa el software libre en Ecuador).

Se ha llegado a la conclusión que hay que educar de forma directa a cada uno de los usuarios en sus problemas particulares a través de un *help desk* que no solo solucione el problema, si no que enseñe al usuario a resolver su dificultad cuando se presente nuevamente dicho problema, además, el PPA se encuentra utilizando la suite *OpenOffice 3.0* la cual deberá ser actualizada a la versión *OpenOffice 3.3*.

# CAPÍTULO III

# 3. DISEÑO DE LA INFRAESTRUCTURA DE RED

## 3.1. INTRODUCCIÓN

La infraestructura de red convergente de voz, datos y video en las nuevas instalaciones del Programa de Provisión de Alimentos brindará a sus usuarios un completo sistema de comunicación que les permita desarrollar sus actividades con bienes y servicios apropiados.

El Programa de Provisión de Alimentos al ser una entidad gubernamental debe cumplir el decreto 1014 que prioriza el uso de Software Libre que brinde iguales o mejores prestaciones que el software propietario en las instituciones públicas.

Se diseñará una infraestructura de comunicaciones que permita que el traslado a las nuevas instalaciones sea transparente para los usuarios. Se diseñarán los servicios que son requeridos por el PPA, entre los que se encuentra el diseño de una red inalámbrica básica que permita al personal del PPA y proveedores el uso de portátiles para el acceso a servicios Intranet, así como su salida al Internet con las medidas de seguridad adecuadas. Se diseñarán enlaces VPN que permita la conexión remota de los usuarios del PPA que necesiten acceso a los servicios Intranet del PPA de forma remota.

Un aspecto sumamente importante a tomar en cuenta en el diseño de la Intranet es el personal con el que se cuenta para la administración de la red. Actualmente el departamento GTI-PPA se encuentra formado por dos Ingenieros en Sistemas, los cuales se encuentran desarrollando el sistema de administración SICOPPA y son los encargados de dar soporte a los usuarios de la red por lo cual la infraestructura de comunicaciones debe ser de fácil administración.

## 3.2. ESTIMACIÓN DEL CRECIMIENTO DE USUARIOS DE LA RED

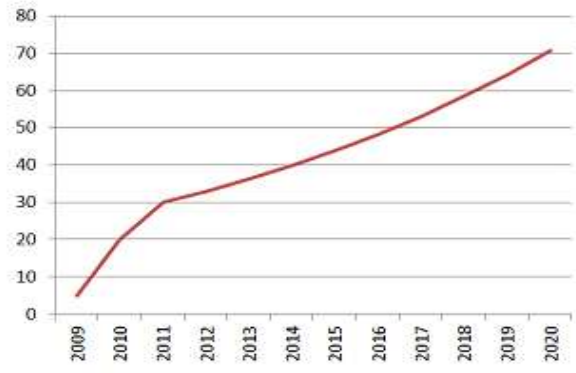
En sus inicios, en el 2009, el Programa inicio sus actividades con únicamente 5 funcionarios, llegando el 2010 a contar con 20 funcionarios ya establecidos por departamentos, los cuales fueron paulatinamente creciendo llegando a inicios del 2011 un total de 26 funcionarios. Según el crecimiento esperado durante todo el 2011 de acuerdo a las peticiones de personal de los diferentes departamentos, se espera contar con 4 funcionarios más. Por lo cual para finales del 2011 se estima un total de 30 usuarios.

Si bien no se tiene un rango de tiempo suficiente para medir el índice de crecimiento del Programa, por medio del departamento de recursos humanos se sabe que el crecimiento para los próximos años se estabilizará a un 10% debido a que el Programa está llegando a consolidarse.

Cabe recalcar que el crecimiento que ha tenido el Programa ha sido uno de los motivos principales para la creación de una infraestructura de comunicaciones de voz, datos y video independiente del Ministerio. La Tabla 3-1 muestra el crecimiento aproximado en los próximos 10 años.

**Tabla 3-1 Estimación del crecimiento de personal de PPA**

| Año | Usuarios |
|---|---|
| 2009 | 5 |
| 2010 | 20 |
| 2011 | 30 |
| 2012 | 33 |
| 2013 | 36 |
| 2014 | 40 |
| 2015 | 44 |
| 2016 | 48 |
| 2017 | 53 |
| 2018 | 58 |
| 2019 | 64 |
| 2020 | 71 |



Según lo pronosticado se espera contar con alrededor de 71 usuarios para el 2020, los cuales deberán ser tomados en cuenta en el diseño de la red, permitiendo su integración sin recurrir a cambios muy grandes en la infraestructura de la red.

Para el dimensionamiento de la red no se han tomado en cuenta al personal de logística que trabaja en el almacenaje, transporte y distribución de los diferentes alimentos.

## 3.3. DIMENSIONAMIENTO DE TRÁFICO

La determinación del tráfico que circulará por la red permitirá evitar cuellos de botella, congestionamiento en la red y asegurar la disponibilidad de los diferentes servicios de la red. Además permitirá detectar los diferentes tipos de tráfico que circularán por la red, con el fin de obtener datos sobre los servicios de red más utilizados, permitiendo establecer un patrón en cuanto al uso de la red.

La estimación del tráfico que se prevé manejar en la infraestructura de comunicaciones del PPA se realizará mediante el estudio del tráfico del segmento de red asignado al PPA por parte del Ministerio.

GTI-PPA no tiene acceso a la administración de la red del Ministerio, por lo cual no es posible la instalación de una herramienta informática que permita medir el tráfico del segmento de red del PPA por lo que se calculará el tráfico a través de datos proporcionados por GTI-PPA y por medio de la encuesta de satisfacción realizada a los diferentes funcionarios.

### 3.3.1. ENLACE A INTERNET

El servicio de Internet deberá asegurar su calidad y disponibilidad contratando el ancho de banda necesario para satisfacer la demanda de los funcionarios del PPA e instalando dos enlaces (principal y secundario), de tal forma que el Programa disponga de redundancia de enlaces de Internet con ISPs (Proveedores de Servicio de Internet)

diferentes y balanceo de carga en el esquema (Activo/Activo) que impida que uno de los enlaces permanezca ocioso.

En un principio el correo electrónico y la página web se encontrará en un servidor fuera de la institución (*hosting*) debido a la falta de personal destinado a su administración y a la falta de presupuesto para adquirir el hardware necesario por lo cual el ancho de banda de Internet deberá soportar dichas aplicaciones. En el diseño de red se tomará en cuenta estos servicios los cuales deberán ser parte de la Intranet cuando se cuente con lo necesario en cuanto a hardware, software, personal de administración y disposición económica para su adquisición.

Los servicios que accederán a Internet en condiciones normales serán:

- Correo electrónico
- Descarga de archivos de Internet
- Navegación web
- Telefonía IP
- Videoconferencia
- Videoseguridad
- Conexiones VPN

#### 3.3.1.1. Correo Electrónico

Para estimar el tamaño del correo se ha observado la bandeja de entrada y salida de correos de funcionarios (un ejemplo se encuentra en el Anexo 3-1) en los cuales se ha observado que los tamaños de los correos son muy variables, llegando un correo a pesar hasta 10 MB debido a que no se cuenta con una política que limite el tamaño de los correos electrónicos y no se hace control de correos personales (que son los que mas tamaño tienen) razón por la cual no se estimará el promedio de dichos correos para el dimensionamiento del tráfico de la infraestructura de comunicaciones del PPA.

En la infraestructura de comunicaciones del PPA se limitará el tamaño de los correos electrónicos a 2MB y se lo dará uso únicamente para asuntos laborales, por lo que se

tomará como tamaño promedio de un correo 1MB y se considerará que el tiempo máximo de lectura o descarga de un correo sea de 1 minuto. Además para el cálculo aproximado del tráfico generado por el correo electrónico se tomará como usuarios simultáneos los analizados en el Anexo 3.2.

Cálculo

- Tamaño del correo promedio: 1MB
- Tiempo de descarga máximo: 1minuto
- Usuarios simultáneos: 3

$$Capacidad_{correo} = Usuario\ simultáneos * \frac{Tamaño\ promedio\ email.}{Tiempo\ de\ descarga\ satisfactoria.}$$

$$Capacidad_{correo} = 3 * \frac{1000\ KB.}{60\ s.} * \frac{8Kb}{1KB} = 400\ Kbps$$

Se tendrá un tráfico de 400 Kbps.

#### 3.3.1.2. Descarga de Archivos

Un factor importante a la hora de medir el tráfico que va a manejar la red es la descarga de archivos de sitios gubernamentales, de los cuales se debe obtener todos los documentos e información necesaria para los diferentes procesos de compras. Se ha notado que el peso promedio de los archivos descargados es de 2MB y en la infraestructura de red del PPA se diseñará como tiempo máximo de descarga 2 minutos. El número de usuarios simultáneos es de 2 y es tomado del Anexo 3.2.

Cálculo:

- Peso promedio de descarga: 2 MB
- Tiempo de descarga máximo: 2 minutos
- Usuarios simultáneos: 2

$$Capacidad_{descargas} = Usuario\ simultáneos * \frac{Tamaño\ promedio\ descargas}{Tiempo\ de\ descarga\ satisfactoria.}$$

$$Capacidad_{Descarga} = 2 * \frac{2000KB.}{120\ s.} * \frac{8Kb}{1\ KB} = 266.64\ Kbps$$

Se tendrá un tráfico de 266.64 Kbps.

#### 3.3.1.3. Navegación Web

Para el desempeño de sus actividades funcionarios del Programa de Provisión de Alimentos interactúan con sitios web gubernamentales como: Ministerio de Finanzas, Instituto Ecuatoriano de Seguridad Social, Sistema de Gestión Documental Quipux, Instituto Nacional de Contratación Pública (INCOP) y otros.

Actualmente la navegación a través de Internet se encuentra sumamente restringida de acuerdo a las políticas del Ministerio, las cuales no son compartidas por el PPA especialmente por el departamento de Investigación, el cual se ve mermado en su capacidad de investigación. Por tal motivo es necesario plantear políticas que filtren la navegación web de acuerdo a las necesidades del PPA.

De acuerdo a las páginas más visitadas por funcionarios del PPA se observó que el tamaño promedio de las páginas es de aproximadamente de 100KB y se diseñará para un tiempo de carga promedio de 30 segundos. Para el siguiente cálculo se considera 5 usuarios concurrentes de acuerdo al Anexo 3.2.

Cálculo:

- Tamaño promedio de la página: 100 KB
- Tiempo de descarga máximo: 120 segundos
- Usuarios simultáneos: 5

$$Capacidad_{Web} = Usuario\ simultáneos * \frac{Tamaño\ promedio}{Tiempo\ de\ descarga}$$

$$Capacidad_{Web} = 5 * \frac{100\ KB.}{120s.} * \frac{8Kb}{1KB} = 33.33Kbps$$

Se tendrá un tráfico de 33.33 Kbps.

#### 3.3.1.4. Conexiones VPN.

Los funcionarios del PPA, especialmente el área de Logística y Coordinación Nacional harán uso de conexiones VPN para acceder a los servicios Intranet, realizar videoconferencias y acceder a su escritorio de forma remota.

El acceso a dichos servicios se los realizará vía VPN ya que viajarán por Internet y dependerán de la calidad de servicios a ofrecer. Para el cálculo del ancho de banda necesario para las conexiones remotas tipo VPN se analizarán los servicios a los que se accederá por este medio.

#### 3.3.1.5. Servicios Intranet

Los servicios Intranet que deberán ser accedidos a través de conexiones VPN son los servicios de DHCP, DNS, telefonía IP y al sistema de administración SICOPPA.

El servicio de telefonía hará uso de 39.2 Kbps[11] (lo cual será explicado en el cálculo de tráfico telefónico). Para el acceso al sistema de administración SICOPPA se asignará un ancho de banda de 192 Kbps[12].

Teniendo los datos preliminares sobre los servicios que más ancho de banda ocuparán en la conexión VPN para el acceso a los servicios Intranet, se asignará un ancho de banda de 256 Kbps en los cuales se encuentra incluido el ancho de banda necesario para los servicios de DHCP, DNS e impresión.

#### 3.3.1.6. Videoconferencia

La videoconferencia es un servicio en tiempo real el cual debe cuidar los tiempos de retraso (latencia) y la diferencia de retraso (*jitter*). Una calidad aceptable de un sistema de

[11] Ancho de banda utilizado en telefonía IP a través del codificador G,711
[12] Ancho de banda utilizado por el sistema de administración SICOPPA, dato obtenido de GTI-PPA

videoconferencia debe permitir entre 15 y 30 imágenes por segundo con un rango total de retraso de 125 a 150 milisegundos.

La Tabla 3-2 muestra el ancho de banda necesario para videoconferencia vía IP de acuerdo a la calidad de la imagen y una estimación de *overhead*.

**Tabla 3-2[13] Ancho de banda para videoconferencia**

| Calidad | Ancho de Banda | Consumo real de ancho de banda |
|---|---|---|
| cuadros /segundo | (Kbps) | + 25% (overead) (Kbps) |
| 15 | 128 | 160 |
| 30 | 192 | 240 |

Para la aplicación de videoconferencia en el PPA se asignará 256 Kbps de ancho de banda

El cálculo total de conexiones VPN estará dado por:

$$Conexión_{VPN} = Capacidad_{Servicios\ Intranet} + Capacidad_{Videoconferencia}$$

$$Conexión_{VPN} = 256\ Kbps + 256\ Kbps = 512\ Kbps$$

El servicio VPN será utilizado por las personas que necesiten trabajar fuera de las instalaciones del PPA, generalmente salen dos personas hacia las bodegas y a realizar investigaciones, por lo cual se estima que simultáneamente una persona hará uso de dicho servicio.

#### 3.3.1.7. Cálculo total del enlace a Internet

Teniendo el cálculo de los diferentes tipos de tráfico significativos que manejará la red se procede a realizar el cálculo del enlace a Internet

El cálculo del enlace al ISP estará dado por los siguientes tráficos:

[13] Datos tomados de: www.grupoact.com.mx/archivos/Consideraciones%20para%20Videoconferencia%20IP.pdf

$$Enlace_{ISP} = Correo\ electrónio + Descarga\ archivos + Web + Conexiones\ VPN$$

$$Enlace_{ISP} = 400\ + 266.64 + 33.33 + 512\ (Kbps)$$

$$Enlace_{ISP} = 1212\ (Kbps)$$

El ancho de banda necesario en la actualidad es de 1212 Kbps.

Para determinar el ancho de banda que es necesario contratar en cada uno de los enlaces, es necesario establecer procesos críticos que requieren el servicio de Internet para su ejecución, los cuales deben ser priorizados sobre los demás en el caso de que uno de los enlaces no este disponible.

La Tabla 3-3 muestra el resumen de las capacidades de los servicios que deben acceder a Internet en la actualidad.

**Tabla 3-3 Ancho de banda de servicios que acceden a Internet**

| Servicios | | Condiciones Normales (Kbps) | Prioritarios (Kbps) |
|---|---|---|---|
| Correo electrónico | | 400 | 400 |
| Descarga de archivos | | 266.64 | 266.64 |
| Web | | 33.33 | 33.33 |
| Conexiones VPN | Servicios Intranet | 256 | 0 |
| | Videoconferencia | 256 | 0 |
| TOTAL | | 1212 | 700 |

Mediante la misma metodología y tomando en cuenta el número de usuarios simultáneos en los próximos 3 años del Anexo 3-2 se calcula el tráfico estimado que será necesario contratar. La Tabla 3-4 muestra el tráfico estimado en los próximos 3 años.

**Tabla 3-4 Ancho de banda necesario en los próximos 3 años**

| Servicios | Condiciones Normales (Kbps) | Prioritarios (Kbps) |
|---|---|---|
| Correo electrónico | 533.33 | 533.33 |
| Descarga de archivos | 400 | 400 |
| Web | 46.67 | 46.67 |

Continúa

| | | | |
|---|---|---|---|
| Conexiones VPN | Servicios Intranet | 256 | 0 |
| | Videoconferencia | 256 | 0 |
| TOTAL | | 1492 | 980 |

Según los datos obtenidos del cálculo de tráfico a internet se recomienda la contratación de 1536 Kbps de ancho de banda para acceso a Internet, los cuales serán proporcionados a través de dos enlaces de diferentes ISPs entre los cuales será balanceada toda la carga a Internet.

En condiciones normales se deberán disponer de todos los servicios mencionados, mientras que en caso de fallar uno de los servicios se deberá priorizar el servicio en la Intranet, sacrificando las conexiones VPN por lo cual se deberá contratar enlaces de 768 Kbps respectivamente.

#### 3.3.1.8. Consideraciones a tomar en cuenta en la contratación del servicio de Internet

GTI-PPA deberá solicitar al Proveedor de Servicio de Internet (ISP) los siguientes requerimientos técnicos.

- El proveedor deberá proporcionar enlaces de 768 Kbps cada uno en una relación 1:1 (Sin nivel de compartición).
- El proveedor deberá dar la posibilidad de extender el ancho de banda previa notificación.
- El enlace debe ser proporcionado por fibra óptica, deberá permitir la implementación a futuro de nuevos servicios como priorización de tráfico para transmisión de datos, videoconferencia, video vigilancia, telefonía IP y otros que no impliquen cambios significativos en la acometida.
- El proveedor deberá realizar una visita técnica para la verificación de la canalización interna hacia el cuarto de equipos para la acometida de Internet.

- El proveedor deberá garantizar una disponibilidad de mayor o igual al 99.6%.
- El proveedor permitirá la resolución del dominio y subdominios del PPA en servidores de su red. El nivel de disponibilidad para el servicio de DNS debe guardar concordancia con la disponibilidad del servicio de Internet.
- El proveedor deberá monitorear el enlace en tiempo real al cual tenga acceso GTI-PPA a través de un sitio Web, donde se pueda observar las estadísticas de la utilización del ancho de banda del enlace.

GTI-PPA deberá garantizarse que el ISP con el cual se contratará el servicio de Internet sea confiable, para lo cual deberá solicitar lo siguiente:

- El proveedor deberá mantener acuerdos de *Peering*[14] Internacional con Proveedores en Estados Unidos y constar con al menos dos rutas de salida en su acceso internacional.
- El proveedor deberá tener su *backbone* MPLS[15] (*Multiprotocol Label Switching*).
- La red del proveedor deberá estar interconectada por lo menos con dos redes de otros ISPs locales para el intercambio de tráfico de Internet a través del NAP[16] (*Network Access Point*) Ecuador.
- El proveedor deberá presentar un certificado de ser miembro de AEPROVI (Asociación Ecuatoriana de Proveedores de Valor Agregado e Internet) y que posee interconexión directa con el NAP de esta institución.

### 3.3.2. TRÁFICO TELEFÓNICO

El tráfico de telefonía IP depende en gran parte del codificador utilizado en las centrales telefónicas. Para el cálculo del tráfico telefónico se deberá tomar en cuenta el ancho de

[14] Peering es un acuerdo bilateral para la interconexión de redes de Internet administrativamente independientes para el intercambio de tráfico.
[15] MPLS es un mecanismo de transporte de datos que opera en la capa de enlace de datos y la capa de red del modelo OSI, diseñado para unificar el servicio de transporte de datos basada en circuito y las basadas en paquetes.
[16] NAP es el punto donde concurren las redes de las diferentes empresas proveedoras del servicio de Internet.

banda que ocupa una conversación de telefonía IP y el número de conversaciones simultáneas que el PPA utiliza durante un hora de mayor flujo de trabajo. Para el entorno LAN se utilizará el códec G.711 de mayor calidad dónde la velocidad será de 100/1000 Mbps mientras que para el entorno WAN se utilizará el códec G.729 que utiliza menor ancho de banda.

#### 3.3.2.1. Ancho de Banda por canal

Encontrar el ancho de banda necesario para VoIP (Voz sobre IP) radica en encontrar la tasa de paquetes y el tamaño del paquete, los cuales dependen del codificador que se utilice y del encabezado de cada uno de los protocolos que intervienen en la encapsulación de la trama de voz (RTP[17], UDP, IP y el protocolo de nivel de enlace). La Tabla 3-5 muestra las características de los códec más utilizados en telefonía IP.

**Tabla 3-5[18] Códec más utilizados en telefonía IP**

| *Códec* | *Bandwidth* | *Sample period* | *Frame size* | *Frames/packet* | *Ethernet Bandwidth* |
|---|---|---|---|---|---|
| G.711 (PCM) | 64 Kbps | 20 ms | 160 | 1 | 95.2 Kbps |
| G.723.1A (ACELP) | 5.3 Kbps | 30 ms | 20 | 1 | 26.1 Kbps |
| G.723.1A (MP-MLQ) | 6.4 Kbps | 30 ms | 24 | 1 | 27.2 Kbps |
| G.726 (ADPCM) | 32 Kbps | 20 ms | 80 | 1 | 63.2 Kbps |
| G.728 (LD-CELP) | 16 Kbps | 2.5 ms | 5 | 4 | 78.4 Kbps |
| G.729a (CS-CELP) | 8 Kbps | 10 ms | 10 | 2 | 39.2 Kbps |
| AMR-WB/G.722.2 (ACELP) | 6.6 Kbps | 20 ms | 17 | 1 | 38.0 Kbps |

El ancho de banda viene dado por la siguiente ecuación[19]:

$$BW = \frac{H + (N\ x\ Lt)}{Tt\ x\ N}\ x\ 8$$

[17] RTP (*Real Time Protocol*) es un estándar creado por la IETF para la transmisión fiable de voz y video a través de Internet.
UDP (*User Datagram Protocol*) es un protocolo de capa transporte no orientado a la conexión.
[18] Datos tomados de: http://www.adiptel.com/soluciones/calidad_servicio.php
[19] Fórmula tomada de: www.idris.com.ar/lairent/pdf/ART0001%20-%20Calculo%20de%20ancho%20de%20banda%20en%20VoIP.pdf

Dónde:

- H = Longitud de la sobrecarga (cabeceras)
- N = Cantidad de tramas por paquete
- Lt = Longitud de la trama
- Tt = Tiempo de cada trama

Cálculo de la longitud del paquete

La señal de voz se encapsula en RTP, el cual a su vez se encapsula en UDP y éste se encapsula en IP los cuales en conjunto se encapsulan en la trama de capa enlace a utilizar.

La cabecera de cada uno de los protocolos son: la cabecera de RTP es variable pero cuando se trata únicamente de audio la cabecera tiene 12 bytes, la cabecera de UDP tiene 8 bytes, la cabecera de IP es variable, pero generalmente tiene 20 bytes llegando hasta 60 bytes. A nivel de capa de enlace, depende de la tecnología a utilizar, en este caso se utilizará Ethernet cuya cabecera tiene 38 bytes (cabecera, *trailer*[20] y *bytes* de sincronización)

En la Tabla 3-6 se especifica las cabeceras que son añadidas a la VoIP en cada una de las capas ISO/OSI.

**Tabla 3-6 Cabeceras de VoIP**

| Capa | Protocolo | Longitud Cabecera (bytes) |
|---|---|---|
| Sesión | RTP | 12 (variable) |
| Transporte | UDP | 8 |
| Red | IP | 20 (hasta 60) |
| Enlace | Ethernet | 38 |

[20] Tráiler es información adicional de la trama Ethernet que va en el final que permite admitir la detección de errores en la trama

Se tiene que la cabecera total estará formada por 78 bytes.

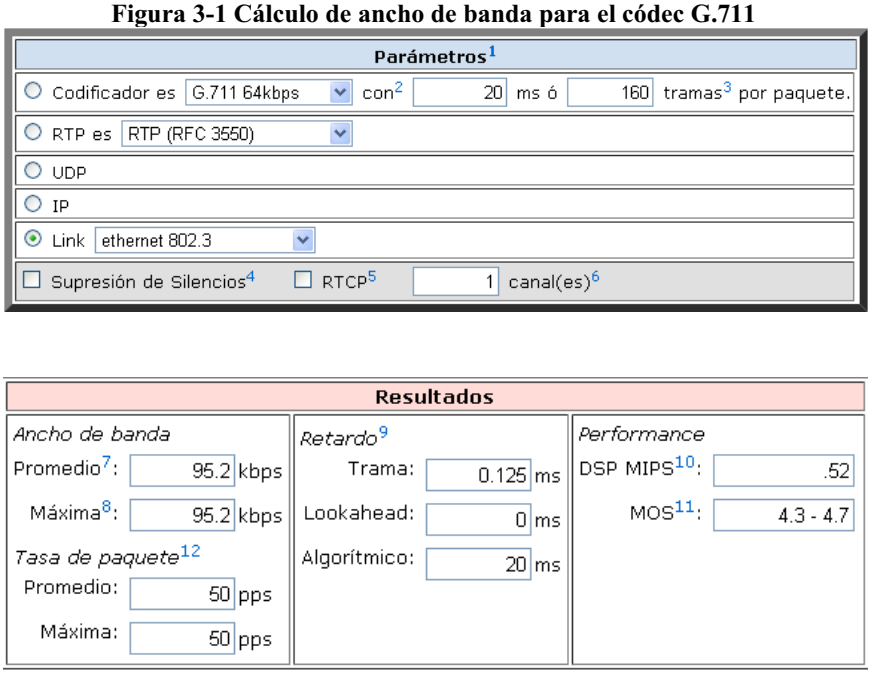
Para el códec G.711 a utilizar en la LAN se tiene:

- H = 78 bytes (Tabla 3-6)
- N = 1 (Tabla 3-5)
- Lt = 160 bytes (Tabla 3-5)
- Tt = 20 ms (Tabla 3-5)

$$BW = \frac{78\ bytes + (1\ x\ 160\ bytes)}{20\ ms\ x\ 1}\ x\ 8 = 95.2\ Kbps$$

En la Figura 3-1 se observa que el tráfico telefónico ha utilizar en la LAN son corroborados con la calculadora online (http://www.bandcalc.com/).

**Figura 3-1 Cálculo de ancho de banda para el códec G.711**




Para el códec G.729 a utilizar en la WAN se tiene:

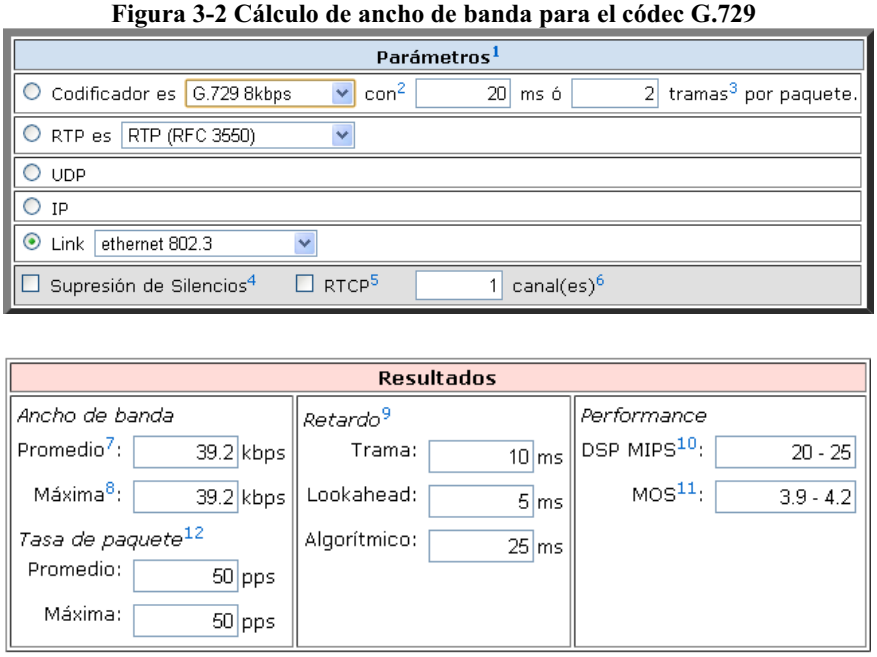
- H = 78 bytes (Tabla 3-6)
- N = 2 (Tabla 3-5)

- Lt = 10 bytes (Tabla 3-5)
- Tt = 10 ms (Tabla 3-5)

$$BW = \frac{78\ bytes + (2\ x\ 10\ bytes)}{10\ ms\ x\ 2}\ x\ 8 = 39.2\ Kbps$$

En la Figura 3-2 se observa que el tráfico telefónico ha utilizar en la WAN son corroborados con la calculadora online (http://www.bandcalc.com/).

**Figura 3-2 Cálculo de ancho de banda para el códec G.729**




### 3.3.2.2. Troncales Telefonía IP

Una vez calculado el tráfico telefónico de cada canal se procede al cálculo de troncales IP que la central telefónica IP deberá manejar, para lo cual es necesario conocer el número de llamadas en un día de mayor flujo de trabajo y su duración promedio, los cuales son tomados del análisis realizado en el Anexo 3-3. El cálculo del tráfico telefónico se realizará con la fórmula de Erlang B.

$$A = C\ x\ T\ (Erlang)$$

Dónde:

- A = Flujo de tráfico
- C = Número de llamadas en una hora de mayor flujo de trabajo
- T = Tiempo promedio de duración de las llamadas

El flujo de tráfico es:

$$A = \frac{38\ llamadas}{1\ hora}\ x\ 3\ minutos\ (Erlang)$$

$$A = 1.9\ (Erlang)$$

Se diseñará para tener bloqueos del 1% en llamadas realizadas o recibidas.

Teniendo el flujo de tráfico y la probabilidad de bloqueo se procede a encontrar el número de canales necesarios según la tabla Erlang B del Anexo 3.4.

La Tabla 3-7 muestra el resumen de los datos obtenidos de los cálculos.

**Tabla 3-7 Cálculo de troncales para telefonía IP**

| CÁLCULO DE ENLACES TRONCALES IP DE TELEFONÍA | |
|---|---|
| Número máximo de llamadas en una hora: | 38 |
| Duración promedio de las llamadas (min): | 3 |
| Flujo de tráfico (Erlangs) | 1.9 |
| Probabilidad de bloqueo % | 1 |
| Número de canales: | **6** |

Se deberá disponer de 6 troncales digitales para telefonía IP, las cuales trabajarán con una probabilidad de bloqueo de 1%.

#### 3.3.2.3. Cálculo del ancho de banda para Telefonía IP

Teniendo el número de canales y el ancho de banda por canal se procede al calcular el tráfico que deben manejar las troncales para el servicio de telefonía IP.

La Tabla 3-8 muestra el número de canales y la capacidad total de las troncales de telefonía IP.

**Tabla 3-8 Cálculo de ancho de banda para el servicio de Telefonía IP**

| Ambiente | Códec | Número de canales | Ancho de Banda/canal (Kbps) | Capacidad (Kbps) |
|---|---|---|---|---|
| WAN | G.729 | 6 | 39.2 Kbps | 235.2 |

El ancho de banda para el servicio de telefonía IP es actualmente de 236 Kbps.

Se proyectará el número de canales con su respectivo ancho de banda para los próximos 5 años debido a la vida útil aproximada de los equipos para telefonía IP. Se estima que dentro de 5 años se tendrá alrededor de 50 usuarios.

Para el cálculo se utilizará la siguiente fórmula:

$$A_1 = \frac{U_f}{U_o}\ x\ A_o$$

Dónde:

- A1 = Flujo de tráfico proyectado
- Ao = Flujo de tráfico actual
- Uf = Usuarios proyectados
- Uo = Usuarios Actuales

El flujo de tráfico proyectado es

$$A_1 = \frac{50}{30}\ x\ 1.9\ (Erlang)$$
$$A_1 = 3.17\ (Erlang)$$

De la misma manera se diseñará para que el flujo de tráfico proyectado tenga un porcentaje de bloqueo del 1%.

Con la misma metodología se procede a calcular el número de canales necesarios y su respectivo ancho de banda.

La Tabla 3-9 muestra el número de canales para los usuarios proyectados y su ancho de banda en los próximos 5 años.

**Tabla 3-9 Número de troncales y ancho de banda para el servicio de Telefonía IP en los próximos 5 años**

| PROYECCIÓN DE ENLACES TRONCALES IP DE TELEFONÍA | |
|---|---|
| Flujo de tráfico (Erlangs) | 3.17 |
| Probabilidad de bloqueo % | 1 |
| Número de canales: | 8 |
| Ancho de banda | 313.6 Kbps |

De los resultados obtenidos se tiene que en los próximos 5 años se deberá contratar 2 canales más que satisfagan el tráfico generado por los 50 usuarios proyectados, además la central IP deberá ser capaz de escalar a dicha cantidad de usuarios y tráfico.

## 3.4. ESQUEMA DE INFRAESTRUCTURA DE RED INTEGRADA

La infraestructura de comunicaciones deberá ser de alta velocidad, que permita integrar voz, datos, video, además deberá soportar novedades tecnológicas de forma escalable y deberá ser reutilizable por los próximos 10 años.

El esquema de red será basado en la tecnología Ethernet de topología física tipo estrella siguiendo el modelo jerárquico núcleo – distribución – acceso. El tamaño de la red del PPA permite obviar la capa de distribución por el momento, permitiendo la integración de dicha capa sin mayor problema mientras la infraestructura de red crezca. El esquema de red se basará en el *stack* de protocolos TCP/IP.

Los servicios y seguridades de la Intranet serán manejados de acuerdo a la criticidad de los datos y nivel de disponibilidad esperados de los mismos.

### 3.4.1. DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO (SCE).

El Sistema de Cableado Estructurado proporcionará una solución completa de conectividad basada en estándares que garanticen un adecuado rendimiento y

confiabilidad y permitan admitir tecnologías actuales y futuras, el sistema deberá ser diseñado tomando en cuenta un crecimiento a futuro de alrededor de 10 años, además estará orientado hacia oficinas dinámicas que permitan modificaciones y ampliaciones sin necesidad de reestructurar todo el SCE.

La solución que se entregará es una red de alta velocidad Gigabit Ethernet. El SCE será categoría 6A, el cual ofrece un rendimiento con velocidades de hasta 10GB trabajando a una frecuencia de 500MHz a una distancia máxima de 100 metros.

El SCE propuesto presenta una topología tipo estrella en donde las conexiones se concentrarán en el cuarto de equipos, lugar donde se ubicará el rack de telecomunicaciones, se trabajará con la norma ANSI/TIA/EIA-568-C.1 que especifican el cableado de telecomunicaciones en Edificios Comerciales.

El cable debe cumplir los requerimientos de desempeño de Canal Categoría 6A del estándar ANSI/TIA/EIA-568-C.2 e ISO/IEC 11801:2002/Amd1:2008 Clase EA hasta 500 MHz que permita aplicaciones actuales u futuras, tales como Ethernet (10BASE-T), Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T), 10 Gigabit Ethernet (10GBASE-T), Token Ring, ATM 155 Mbps, TP-PMD 100 Mbps, ISDN, video análogo y digital, así como voz análoga y digital (VoIP y telefonía IP), así como cumplir con los requisitos de IEEE 802.3an 10Gigabit Ethernet.

El número de puntos de red se establecerán de acuerdo al número de usuarios, teléfonos IP, periféricos IP y al espacio físico asignado al PPA. Se dispondrá de un solo punto de red para cada área de trabajo, el cual manejará datos y telefonía IP, para tal efecto los teléfonos IP deberán contar con un mini switch que permita la conexión con la LAN y el computador.

El Subsistema de Cableado Horizontal se ubicará en el cuarto piso del edificio del IEPS (Instituto Ecuatoriano de Economía Popular y Solidaria), lugar donde se realizarán obras civiles de remodelación, las mismas que deberán ir de la mano con la instalación

del SCE para realizar el recorrido del cableado a través de inserción en paredes y no utilizar en lo posible canaletas decorativas.

Todos los funcionarios del PPA cuentan en su área de trabajo de un computador y un teléfono IP y comparten en cada uno de los departamentos una impresora de red. Los puntos de red necesarios se listan en la Tabla 3-10.

**Tabla 3-10 Dimensionamiento de puntos de red**

| DIMENSIONAMIENTO DE PUNTOS DE RED | | |
|---|---|---|
| **DEPARTAMENTO** | **EQUIPOS** | **DATOS/VOZ** |
| COORDINACIÓN NACIONAL | Usuarios | 2 |
| | Asesor | 1 |
| | Impresora | 2 |
| | Escáner | 1 |
| SUBCORDINACIÓN NACIONAL | Subcoordinador | 1 |
| | Asesor | 1 |
| | Impresora | 1 |
| GESTIÓN TECNOLÓGICA | Usuarios | 2 |
| | Equipo pruebas | 1 |
| | Impresora | 1 |
| INVESTIGACIÓN Y ESTUDIOS | Usuarios | 3 |
| | Impresora | 1 |
| COORDINACIÓN JURÍDICA | Usuarios | 2 |
| | Impresora | 1 |
| PLANIFICACIÓN Y COMPRAS | Usuarios | 3 |
| | Vacante | 1 |
| | Impresora | 1 |
| | Escáner | 1 |
| SERVICIOS INSTITUCIONALES | Usuarios | 6 |
| | Impresora DGL | 1 |
| LOGÍSTICA Y MONITOREO | Usuarios | 7 |
| | Vacantes | 2 |
| | Impresora DSI | 1 |
| VARIOS | Access Point | 2 |
| | Sala de reuniones | 3 |

Continúa

| | | |
|---|---|---|
| | Sala de Equipos | 2 |
| | Archivo | 1 |
| | Archivo - Copiado | 1 |
| | Control de acceso | 1 |
| | Cámara IP | 1 |
| **SUMATORIA** | | **54** |

Para la ubicación de los puntos de red se definió la división física de las oficinas, la ubicación de los escritorios y ubicación de los diferentes dispositivos IP. La distribución de los puntos de red de acuerdo a la división de las oficinas y ubicación de las estaciones de trabajo se observan en el Anexo 3.4.

La distancia máxima del enlace permanente[21] hacia el punto de red más lejano se estima de 50 metros, distancia que no excede a los 90 metros determinados en la norma ANSI/TIA/EIA 568-C.0. Se dejarán 6 derivaciones de cableado de una longitud hacia el área de trabajo más lejana que permita ampliaciones sin la necesidad de tender nuevos cables.

El SCE es dividido en subsistemas para facilidad de diseño, implementación y administración. Los subsistemas realizarán funciones determinadas para proveer servicios de datos, voz y video en toda la planta del PPA.

Los subsistemas con los que constará el SCE del PPA es el siguiente:

- Punto de demarcación
- Cuarto de equipos
- Cuarto de telecomunicaciones
- Subsistema de cableado horizontal
- Subsistema de cableado vertical
- Área de trabajo

[21] Enlace permanente es aquel que va desde el face plate del área de trabajo al patch panel del rack de comunicaciones, no se toma en cuenta al patch cord de comunicación con el computador y con los equipos de conectividad en el rack.

- Administración

#### 3.4.1.1. Diseño del Subsistema de cableado horizontal

El Subsistema de cableado horizontal corresponde a la sección del SCE que va desde el cuarto de equipos hasta el área de trabajo. El sistema de cableado horizontal será realizado sobre cielo falso con gypsum el cual tendrá un espacio para maniobrar de 15 centímetros. Al tratarse de un área amplia cuyas oficinas se encuentran divididas por paneles modulares, las bajantes hacia los puntos de red se realizarán a través de pared y a través de las columnas de los paneles, únicamente en casos especiales se hará uso de canaletas plásticas decorativas.

Un de los aspectos a tomar en cuenta en el diseño de las canalizaciones es el diámetro del cable categoría 6A, el cual es mucho más grueso (23 AWG[22]) y pesado, lo que lo hace menos fácil de manipular. Las canalizaciones deberán prever el espacio suficiente, radio de curvatura y anclajes de mayor resistencia. El SCE deberá seguir las recomendaciones de la norma ANSI/TIA/EIA-569-B que especifica las prácticas de diseño y construcción de recorridos y espacios de telecomunicaciones en edificios comerciales

##### *3.4.1.1.1. Cielo falso*

Sobre el cielo falso se instalará una canaleta de datos principal, la cual recorrerá la parte frontal, lateral derecha y posterior de las instalaciones como se muestra en el plano del Anexo 3.4, pasando por el cuarto de telecomunicaciones desde donde se distribuirá el cableado hacia los diferentes puntos de red de las estaciones de trabajo. La canaleta deberá ser tipo escalerilla metálica lo suficientemente ancha para transportar todos los cables, deberá anclarse al techo y la manipulación de los cables se realizará por la parte de abajo, esto debido al poco espacio para maniobrar en el cielo falso.

[22] AWG (*American Wire Gauge*) es una referencia de clasificación de diámetros de conductores eléctricos.

Para el cableado de energía eléctrica normal y regulada será necesario el uso de una segunda canaleta metálica tipo escalerilla, como se muestra en el plano del Anexo 3.4, la cual deberá guardar una distancia mínima de 40 cm de la escalerilla de datos para evitar *crosstalk*[23], así mismo se deberá coordinar la ubicación de lámparas que guarde en lo posible la misma distancia de la canaleta de datos. En el caso que la canaleta de datos y la eléctrica no se las pueda ubicar lo suficientemente separadas, la canaleta de datos deberá ser cubierta en su totalidad. Todas las canaletas deberán estar aterrizadas.

La canaleta de datos principal tendrá cajas de paso en sitios estratégicos desde donde se distribuirán los cables a través de tubería metálica a las diferentes áreas de trabajo, no deberán salir las corridas de cables desde cualquier punto de la canaleta de datos principal. De las diferentes cajas de paso los cables serán conducidos a través de tubería metálica rígida, el número de cables a transportar por dicha escalerilla no debe ser mayor a 3.

Las cajas de paso colocadas en la canaleta de datos deberá reflejarse en el techo falso a través de tapas pláticas que permitan localizar los cables y facilite posteriores cambios, ampliaciones y corrección de fallas, esto debido a que el techo es hecho con gypsum.

La acometida del servicio de Internet se realizará por medio de postería, el medio físico por el cual se proveerá el servicio será fibra óptica, por lo que se deberá instalar tubería metálica rígida de 1 pulgada desde la acometida que llegará a la pared del cuarto piso hasta el cuarto de equipos. Sabiendo la importancia de dicho servicio y que el mismo constará con redundancia de enlaces de diferentes ISP se deberán instalar dos ductos de las mismas características por la cual ingresará el enlace redundante u otros servicios de televisión por cable, enlace de telefonía, etc. Se deberá realizar radios de curvatura de 45 grados en los lugares necesarios hasta llegar al cuarto de telecomunicaciones.

[23] Crosstalk es el acoplamiento magnético que se producen entre dos elementos de un circuito provocando la atenuación en el elemento perturbado.

#### *3.4.1.1.2. Bajantes*

Los paneles deberán constar con columnas lo suficientemente amplias para transportar tanto los cables de datos, como los de energía eléctrica, los mismos que deberán permanecer separados durante todo el trayecto hasta llegar a los puntos de red. Los paneles deberán tener columnas dividas para dichos propósitos o por lo contrario los cables de energía eléctrica deberán pasar por tubería metálica de ½ pulgada evitando que los cables de datos y eléctricos se junten en el trayecto hacia las estaciones de trabajo.

Las bajantes a través de paredes serán conducidas a través de tubería metálica rígida o BX[24] de un diámetro adecuado al número de cables a transportar, en los casos que se encuentre paredes con diafragma el cableado se realizará a través de canaleta plástica. De la misma forma, los cableados de electricidad y telecomunicaciones deberán viajar en ductos diferentes.

En los lugares donde sea necesario el uso de canaletas plásticas decorativa se deberá tomar en cuenta que el cable de datos debe ir en un compartimiento separado al cableado eléctrico, además se tiene que cuidar que el radio de curvatura mediante la colocación de accesorios cumpla con la norma (mínimo 4 veces el diámetro del cable UTP).

### 3.4.1.2. Diseño del subsistema de cableado vertical

Si bien, el PPA funcionará en la actualidad solo en el cuarto piso, se dejará una canalización vertical hacia el cuarto de equipos del resto del edificio, en el caso de necesitar una comunicación con las instituciones que laboran en el edificio.

El cable vertical a utilizarse es el mismo cable del tendido horizontal (UTP CAT-6A) ya que el tipo de cable de cobre a utilizar maneja tráfico de hasta 10GB, por lo que no es necesario el uso de fibra óptica.

[24] Tubería metálica semi-flexible

#### 3.4.1.3. Diseño del subsistema de área de trabajo

El área de trabajo es el lugar donde los usuarios interactúan con los equipos de telecomunicaciones, en el PPA todas las áreas de trabajo constarán con un computador y un teléfono IP, las impresoras y escáneres IP serán compartidos por departamentos.

Las salidas de telecomunicaciones estarán ubicadas en el borde inferior de los paneles a través de cajas dexon que permitan tener un ángulo de curvatura adecuado para el cable UTP CAT-6A. Se cuidará que cada salida de telecomunicaciones se encuentre cerca de una salida de energía eléctrica regulada y normal.

El cable deberá terminar en un *jack*[25] modular 8 posiciones con una asignación de pines T568B cumpliendo los requisitos de IEC 60603-7.

Las especificaciones técnicas de los *patch cord*[26] son las siguientes:

- Ensamblados en fábrica
- Deberán cumplir con la norma ISO/EIA 11801:2001 y ANSI/TIA/EIA 568-C.2.
- Resistente a la corrosión por humedad, temperaturas extremas y partículas contaminantes.
- Se entregará dos *patch cords* por punto de red, uno de 3 pies la llegada al *patch panel* y uno de 7 pies para la conexión con el computador.

Las especificaciones técnicas de los *jacks* son las siguientes:

- Diseñados para la terminación de cables de par trenzado balanceado de cuatro pares.
- Deberán cumplir con la norma ISO/EIA 11801:2001 y ANSI/TIA/EIA 568-C.2.
- Deberán tener los tabs de conexión a tierra incorporados, no se deberá usar *jacks* con conexiones a tierra por separado.
- Su diseño debe permitir su montaje en orientación plana o angular.

[25] Jack es el conector hembra donde se coloca el conector RJ45

[26] Patch cord es el cable que va de el toma terminal del área de trabajo al computador o del patch panel al conmutador.

- Deberá disponer de conectores frontales RJ45 para conexión de cables calibre 22 a 26 AWG.
- Debe disponer de una tapa protectora para polvo que prevenga el ingreso de contaminantes.

Las especificaciones técnicas de los *face plates*[27] son las siguientes:

- Deberán tener porta etiquetas con protector transparente de acrílico.
- Deberán cumplir con la norma ISO/EIA 11801:2001 y ANSI/TIA/EIA 568-C.2.
- Deberán adaptarse a configuraciones de uso vertical y horizontal.

#### 3.4.1.4. Diseño de los subsistemas de cuarto de telecomunicaciones, cuarto de equipos y acometida de entrada de servicios.

El cuarto de telecomunicaciones y el cuarto de equipos se encontrarán físicamente en el mismo lugar debido al tamaño de la red, el espacio de piso a servir y al reducido espacio asignado para dicho propósito. El cuarto de equipos ocupará un área de 6 metros cuadrados y una altura de 2 metros y estará ubicado en el área de sistemas como se muestra en el plano del Anexo 3.4.

El área de informática y el cuarto de telecomunicaciones deberán ser separados por paredes de hormigón por motivos de seguridad de los equipos de telecomunicación, deberá tener piso de baldosa y paredes de loza para mantener el lugar libre de polvo y electricidad estática.

Las especificaciones técnicas del rack de telecomunicaciones son las siguientes:

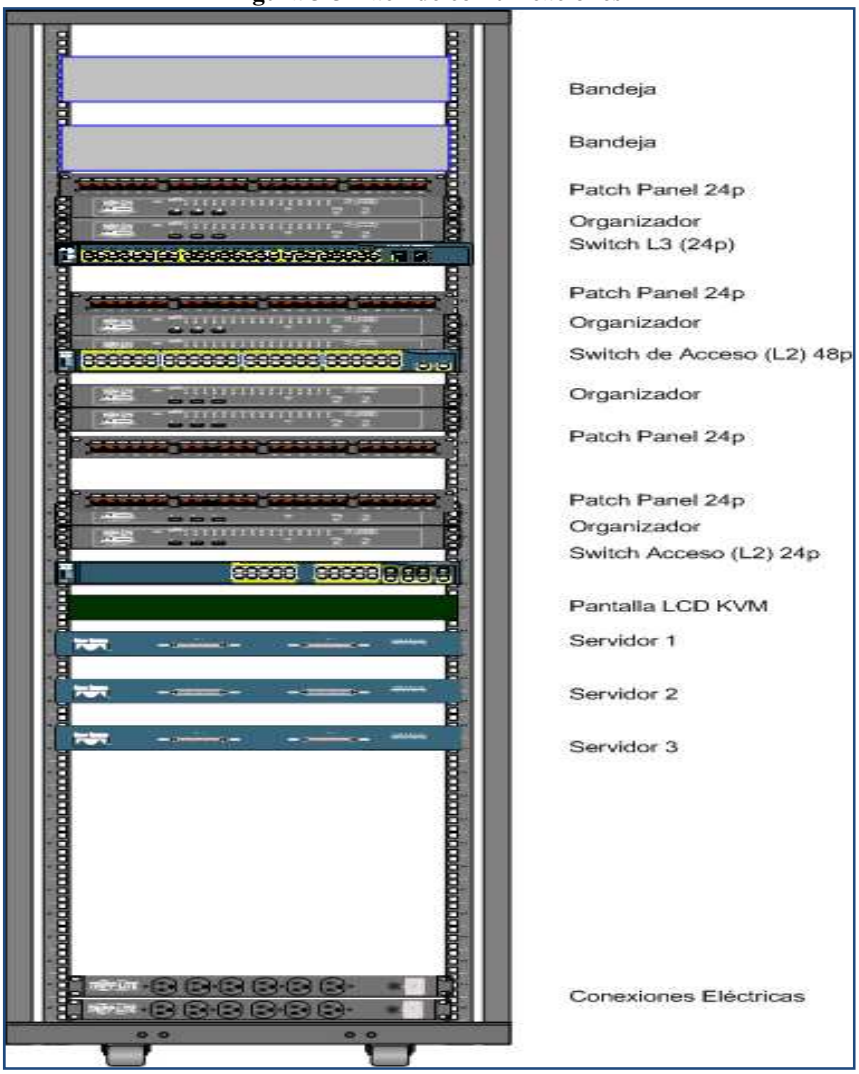
- Rack cerrado desmontable.
- Rack de 42 UR (unidades de rack), ancho de 24 pulgadas y fondo de 40pulgadas.
- Puerta frontal de acero laminado en frío, cerradura giratoria de manija y vidrio.

[27] Face plate es la toma terminal donde se colocan los jacks en el área de trabajo

- Puerta posterior de acero laminado en frío con cerraduras rápidas tipo universal.
- Dos bandejas internas metálicas para soporte de equipos.
- Tres organizadores horizontales de 2 UR.
- Dos regletas para rack de toma corrientes internas verticales, bornera de conexión a tierra y dos ventiladores incorporados en la parte superior.
- El rack debe estar conectado a tierra.
-

La distribución y organización del rack de comunicaciones se observa en la Figura 3-3:

**Figura 3-3 Rack de comunicaciones**



La distribución y organización de los diferentes equipos de conectividad, servidores, patch panel y organizadores permitirán una mejor administración del SCE. El rack de 42U se encontrará ocupado en 33U quedando disponibles 9U para futuras ampliaciones.

Las especificaciones técnicas del *patch panel*[28] son las siguientes:

- Ensamblado en fábrica
- Deberá cumplir con las normas ISO/IEC 11801:2002 y ANSI/TIA/EIA 568-C.2. Debe estar hecho en configuración de 48 puertos o dos *patch panels* de 24 y tener un terminal para conexión a tierra que acepte cable AWG-6.

El rack deberá tener un espacio mínimo en la parte frontal y posterior de 80cm libres para trabajar con los equipos cumpliendo con las especificaciones ANSI/EIA-310.

#### 3.4.1.5. Administración, etiquetado y pruebas del SCE

Todos los elementos del SCE incluyendo: cables, *faceplates, jacks, patch panel*, *jack* del *patch panel*, rack, cuarto de telecomunicaciones, cuarto de equipos deberán contar con una identificación única de acuerdo a lo indicado por la norma ANSI/TIA/EIA 606A.

Se etiquetarán todos los puntos de red, canaletas y *patch panel* de acuerdo a la nomenclatura más común (# rack-# *patch panel*- # punto de red), dado que solo se tiene un rack y que el crecimiento estimado no llega a la instalación de un segundo rack, la nomenclatura será desde el *patch panel* en adelante.

Entonces el modelo de etiquetado será:

$$Número\ de\ Patch\ Panel + Número\ de\ punto\ de\ red$$

$$Ejm: PP1 - D54$$

Las especificaciones técnicas del etiquetado y administración son las siguientes:

[28] Patch panel es el elemento ubicado en el rack donde llegan los cables del Sistema de Cableado Estructurado.

- Todas las identificaciones deberán ser efectuadas con una máquina etiquetadora para evitar su rápido deterioro, las etiquetas no deberán ser hechas en impresoras de tinta, matricial o a mano.
- Todos los cables deberán agruparse por zonas usando cintas tipo velcro.
- Se debe realizar los planos *As-Built*[29] del SCE donde se encuentren especificados los puntos de datos, ubicación del cuarto de equipos, racks, nodos, trayectoria de escalerillas, ductería y canaletas.
- Se debe realizar una descripción de la nomenclatura de identificación de los elementos de conectividad.
- Se debe realizar las respectivas pruebas de certificación, de las cuales se obtendrá un reporte.
- Se debe obtener el certificado de calibración del equipo para certificación del sistema de cobre y de fibra óptica si fuese el caso.
- Toda la documentación se deberá almacenar en formato impreso y electrónico y considerarse información confidencial y de uso exclusivo del Programa de Provisión de Alimentos.

#### 3.4.1.6. Subsistema Puesta a Tierra del SCE

La puesta a tierra del SCE será de tipo protección que evita que la carcasa o cubierta metálica de equipos eléctricos represente un potencial eléctrico respecto a tierra que pueda significar un peligro para el operario u usuario de dichos equipos. Los materiales a conectar al subsistema de puesta a tierra serán partes metálicas sin tensión, tales como la ductería metálica, el rack de telecomunicaciones, blindajes metálicos de los cables y demás accesorios pasivos del sistema de cableado estructurado.

La malla de tierra se ubicará en el parqueadero ubicado a un costado del edificio donde se buscará el lugar apropiado. El aterrizaje deberá estar acordes con la ANSI/TIA/EIA 607-A

Las especificaciones técnicas de la puesta a tierra son las siguientes:

[29] Plano As Built es el que refleja el detalle de las trayectorias y componentes del SCE.

- Malla armada de mínimo 3 varillas *copperweld*[30].
- Cable para instalación a tierra #2 AWG de cobre desnudo.
- Varilla de cobre: 1.8 metros de longitud y 16 mm de diámetro.
- Las varillas y el conductor se enterrarán hasta una profundidad de 70 cm bajo el nivel del piso.
- La instalación a tierra deberá indicar una medición menor de 5 ohmios.
- La canalización del subsistema de puesta a tierra se realizará a través de tubería metálica en exteriores y a través de techo falso y canaletas plásticas en interiores.
- La soldadura entre las varillas *copperweld* y el cable de conducción será exotérmica que asegure la conductividad.
- La preparación de la tierra se dispondrá de gel químico para mejorar la conductividad del terreno, no se aceptarán soluciones caseras (sal común).

#### 3.4.1.7. Selección del UPS del SCE

El sistema de cableado estructurado, equipos de conectividad, computadores y demás periféricos de red deberán constar de una protección centralizada ante cortes de energía y otro tipo de fallas mediante un UPS (*Uninterruptible Power Supply*) que permita suministrar de energía eléctrica regulada en un intervalo de tiempo corto durante el fallo de suministro por parte de la empresa eléctrica.

El dispositivo deberá ser capaz de proporcionar estabilidad ante cortes de energía, sobretensión, caídas de tensión, picos de tensión, ruido eléctrico, inestabilidad en la frecuencia y distorsión sinusoidal, las cuales provocarían daños en los equipos activos de la red.

El cálculo de la capacidad del UPS requerido se establece en la Tabla 3-11.

[30] La varilla copperweld es un elemento bimetálico compuesto por un núcleo de acero y una película externa de cobre lo que le permite una adecuada difusión a tierra de las corrientes de falla.

**Tabla 3-11Cálculo de capacidad del UPS**

| DESCRIPCIÓN DE EQUIPO | NÚMERO DE EQUIPOS | VOLTAJE (V) | WATIOS (W) | INTENSIDAD (A)= W / V | PICO POTENCIA (40% más de W) | TOTAL POTENCIA |
|---|---|---|---|---|---|---|
| | | c/u | c/u | c/u | c/u | |
| PC's | 35 | 120 | 240 | 2.00 | 336 | 11760 |
| Servidores | 3 | 120 | 460 | 3.83 | 644 | 1932 |
| Switches | 3 | 120 | 150 | 1.25 | 210 | 630 |
| Router | 1 | 120 | 80 | 0.67 | 112 | 112 |
| Firewall | 1 | 120 | 80 | 0.67 | 112 | 112 |
| Access Point | 2 | 120 | 100 | 0.83 | 140 | 280 |
| | | | | | **TOTAL** | **14546** |

De acuerdo al estudio de carga se deberá hacer uso de un UPS de 15 KVA.

Las características técnicas que debe cumplir el UPS se detallan en la Tabla 3-12.

**Tabla 3-12 Requerimientos técnicos: UPS**

| CARACTERÍSTICAS UPS | |
|---|---|
| **Equipo** | Capacidad total: 15 KVA |
| **Características generales** | Debe ser modular, los módulos individuales de potencia serán de 4 KVA. Todos los módulos serán idénticos y en operación normal compartirán simultáneamente la carga. Las baterías igualmente serán modulares con control electrónico individual y capacidad de ser aislado en caso de presentar falla alguno de ellos, sin afectar el funcionamiento. El reemplazo de cualquier módulo se podrá realizar en caliente sin afectar el funcionamiento. |
| | Bypass automático y manual, Transformador de aislamiento de salida. |
| | Tarjeta de comunicaciones en red IP, capacidad para instalar una segunda tarjeta de control como redundancia |
| | Disponibilidad para instalar bancos de baterías externos |
| | Disponibilidad para apagado remoto de emergencia |
| **Normas y certificaciones que debe cumplir** | UL Standard 1778 |
| | IEEE C62.41, Category A & B |
| | CSA 22.2, No. 107.1 |

Continúa

| | |
|---|---|
| | FCC Part 15, Sub Part B, Class A |
| | National Fire Protection Association (NFPA 70) |
| | IEC 62040-3 (formerly NEMA PE-I) |
| **Características de entrada** | Voltaje AC de entrada : 208 VAC o 240 VAC nominal, monofásica |
| | 2 hilos mas tierra |
| | Rango de variación de entrada 176 a 248 VAC |
| | Frecuencia: 40 a 70 Hz. |
| | Corriente de Distorsión de entrada: 5 % THD máximo a plena carga |
| | Factor de potencia de entrada: 0.98 a 100% de la carga. |
| | Protección contra transientes : Acorde con IEEE C62.41, Categoría B |
| **Características de salida** | Configuración del Voltaje: 240/120 VAC o 208/120 VAC 3 cables mas tierra |
| | Regulación de Voltaje: +/- 3% |
| | Frecuencia: 60 Hz, +/- 0.5%. |
| | Rango de sincronización de la frecuencia con Bypass: seleccionable entre 0.5 a 5.0 Hz/seg |
| | Distorsión de voltaje 3% THD máximo con 100% de carga lineal, 7% THD máximo al 100% de carga no lineal |
| | Capacidad de sobrecarga: >100% - 110% de manera continua, 111% - 150% por 10 segundos, 151% - 200% por 0.25 segundos. El UPS transfiere a bypass cuando cualquiera de las condiciones excede >201% por 2 ciclos previniendo lo que puede ser un corto circuito. El UPS deberá permitir preprogramar el porcentaje máximo de carga permitido a la salida a fin de ser notificado en el caso de exceso de ese umbral, evitando sobrecargas. |
| | Transformador de aislamiento de salida incorporado en el mismo gabinete del UPS |
| **Baterías** | Baterías Internas: Los módulos de las baterías serán inteligentes y en su interior llevarán las baterías selladas libres de mantenimiento con retardante de llama. El UPS debe poder instalarse dentro de centros de cómputo de conformidad con las exigencias UL Standard 1778. |
| | Baterías Externas: Los bancos externos contendrán baterías selladas libres de mantenimiento con retardante de llama. |

Continúa

| | |
|---|---|
| | Tiempo de soporte: El UPS incorporará los módulos de baterías internas y externas necesarios para brindar un soporte a plena carga de 20 minutos mínimo. Sin embargo de requerirse tiempos adicionales permitirá adicionar más bancos externos de baterías. |
| | Recarga de baterías. El UPS debe incorporar un circuito de compensación de carga de las baterías en función de la temperatura, lo que permitirá incrementar el tiempo de vida útil de las baterías. |
| **Condiciones Generales** | Temperatura ambiente de operación del UPS 0° C a +40° C |
| | Humedad Relativa de operación: 5 a 95% sin condensación. |
| | Ruido audible no debe exceder 62 dBA medidos a un metro del equipo. |
| | El equipo debe ser diseñado para soportar descargas electrostáticas de hasta 15 KV sin daño y sin afectar la carga crítica. |
| | Certificado legalizado del fabricante de ser el distribuidor autorizado en el Ecuador, garantizando localmente el servicio y suministro de partes y repuestos, comprobable en las bodegas del ofertante. |

#### 3.4.1.8. Materiales a utilizar en el SCE

Teniendo definida la topología física de la red, las salidas de telecomunicaciones de las diferentes áreas de trabajo, el cuarto de telecomunicaciones y el hecho de que el cableado se realizará sobre techo falso se debe realizar un cálculo aproximado de los materiales y cantidad de los mismos a utilizar en su implementación y que sirvan como base para la cotización.

Para el cálculo del cable se establecerá el recorrido sobre el techo falso, la bajante por los paneles serán de 2.4 metros (altura total del piso), en el cuarto de telecomunicaciones se tomarán 5 metros como distancia hasta llegar al patch panel (3m para crecimiento y 2m la distancia hasta el rack), en el área de trabajo se dejará 30 cm de holgura para su manipulación. El cálculo del cable se muestra en el Anexo 3.3.

La Tabla 3-13 resume los materiales y la cantidad aproximada de los mismos de acuerdo al cálculo realizado en el Anexo 3.5.

**Tabla 3-13 Lista de materiales: Sistema de Cableado Estructurado**

| LISTA DE MATERIALES | | | |
|---|---|---|---|
| | Material | Unidad | Cantidad |
| Cables Categoría 6A | Cable UTP, Categoría 6A. | m | 1726 |
| | Patch cord de 3 pies, Categoría 6A. | u | 54 |
| | Patch cord de 7 pies, Categoría 6A. | u | 54 |
| Salidas de Telecomunicaciones | Jack Cat. 6A with cover | u | 108 |
| | Faceplate simple | u | 54 |
| | Cajetín rectangular PVC DEXSON de 40 mm | u | 54 |
| Rack de Telecomunicaciones | Rack de piso cerrado de 42 UR | u | 1 |
| | Patch panel modular de 48p, Cat. 6A. | u | 1 |
| | Patch panel modular de 24p, Cat. 6A. | u | 2 |
| | Organizadores horizontales de 2 UR | u | 3 |
| | Bandejas metálicas | u | 2 |
| | Regletas verticales de toma corrientes | u | 1 |
| | Bornera de instalación a tierra | u | 1 |
| | Ventiladores incorporados | u | 2 |
| Canalización | Canaletas metálicas 20x7 con división | m | 50 |
| | Tubería EMT 3/4" | m | 250 |
| | Canaleta plástica 40x25 con división. Marca DEXSON | m | 10 |
| | Acometida telefónica y de internet | m | 60 |
| | Cajas de paso | u | 12 |
| Puesta a tierra | 3 varillas de cobre copperweld | u | 3 |
| | Cable # 2 AWG de cobre desnudo para instalación a tierra | m | 15 |
| | Gel químico para preparación de la tierra | gl | 1 |
| | Barra de cobre | u | 1 |
| | Soldadura exotérmica | gl | 1 |
| Energía eléctrica regulada | Supresor de transientes 3fases, 220-110 V | u | 1 |
| | UPS | u | 1 |
| Accesorios | Rejillas de revisión en cielo falso | u | 4 |
| | Misceláneos (tacos, tornillos, accesorios canaletas) | gl | 1 |

### 3.4.2. DISEÑO DE LA RED LAN

#### 3.4.2.1. Velocidad de transmisión

La velocidad de transmisión de la infraestructura de comunicaciones del PPA será Gigabit Ethernet, la cual manejará todos los servicios mencionados al inicio de este capítulo y deberá adaptarse a novedades tecnológicas en los próximos 10 años.

El esquema de red Gigabit Ethernet es posible gracias al SCE CAT-6A y a los computadores y periféricos cuyas tarjetas de red son Gigabit Ethernet. Los teléfonos IP utilizados en la actualidad por el PPA no son activos fijos del PPA por lo que se deberá adquirir teléfonos IP que trabajen a 1000 Mbps ya que se encontrarán entre el computador y la LAN y podrían ser causa de cuellos de botella disminuyendo el rendimiento del sistema.

#### 3.4.2.2. Escalabilidad, Expansión y Versatilidad

La escalabilidad esperada de los equipos de conectividad (switches, routers, servidores, etc) se estimada en 5 años debido al gran avance tecnológico que tienen estos equipos cada año, haciendo que su vida útil disminuya en esta proporción, razón por la cual las garantías que ofrecen los proveedores de dichos equipos es máximo de 5 años, además el constar con equipos de conectividad diseñados para tener una escalabilidad de más tiempo hace que sus recursos se encuentren sobredimensionados y sin ser utilizados.

#### 3.4.2.3. Esquema de conectividad

El esquema de conectividad se basará en el modelo jerárquico núcleo – distribución – acceso, la cual facilite el diseño, implementación, escalabilidad y administración del sistema. Cada una de las capas realizará una función específica que permita la corrección e identificación inmediata de fallas. En éste caso se trabajará con las capas núcleo y acceso de acuerdo al tamaño de la red.

La capa acceso será la encargada de proporcionar a los usuarios acceso a los servicios y aplicaciones de la Intranet, en está capa se encontrarán conectados todos los usuarios, teléfonos IP, cámaras IP y demás periféricos (impresoras IP, escáneres IP y otros) del Programa.

La capa núcleo actuará como punto de concentración del tráfico a Internet y de servicios Intranet, enrutará el tráfico entre los distintos grupos de trabajo del PPA y proporcionará servicios de seguridad y filtrado. En esta capa se encontrarán los servidores de los servicios Intranet y a donde llegarán los servicios de Internet, videoconferencia, etc.

Los equipos de conectividad se seleccionarán de acuerdo a su función y capa a ocupar dentro del diseño de la red, deberán satisfacer las ampliaciones y crecimiento de usuarios en los próximos 5 años y durante ese tiempo debe garantizar la adaptación de las futuras tecnologías, su velocidad de transmisión, el tráfico a manejar y sobre todo la compatibilidad con equipos que surjan en dicho tiempo. El esquema de conectividad se encontrará debajo de un sistema de seguridad perimetral firewall.

#### 3.4.2.4. Características técnicas de los switches de núcleo y acceso

Los equipos de conectividad a elegir deberán cumplir requerimientos de disponibilidad, escalabilidad, administración y redundancia de ser necesario.

En la capa de acceso de hará uso de switches de capa 2. De acuerdo al número de usuarios actuales, los enlaces al switch de núcleo y al crecimiento estimado en los próximos 5 años, se estima aumentarán 15 accesos más a la red según el estudio realizado, los equipos de conectividad de acceso deberán admitir esta cantidad de usuarios, debiendo contar con alrededor de 70 puertos.

En la capa núcleo se hará uso de switches de capa 3 en donde se encontrarán los servidores, en esta capa se encontrará un equipo firewall donde llegarán los diferentes servicios (Internet, Telefonía, etc.).

Las características técnicas de los switches de acceso y núcleo son las siguientes:

**Características Switch de Núcleo**

El switch de núcleo debe trabajar en las capas 1,2 y 3 del modelo ISO/OSI que permita la conmutación de paquetes, enrutamiento de paquetes y agregue una capa de seguridad mediante listas de control de acceso (ACLs).

Deberá disponer de 24 puertos fullduplex (Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T). Para la conexión con los switches de acceso deberá soportar mínimo 4 puertos Uplinks 10 Gigabit Ethernet de fibra óptica para futuros enlaces.

Deberán soportar protocolos de enrutamiento básicos no propietarios como RIP v1, RIP v2 y OSPF que permitirán el enrutamiento con las diferentes redes de los programas sociales del Gobierno.

La Tabla 3-14 muestra las características técnicas del switch de núcleo.

**Tabla 3-14 Requerimientos técnicos: Switch de núcleo**

| SWITCH DE NÚCLEO 24 PUERTOS. | |
|---|---|
| **CARACTERÍSTICAS** | **DESCRIPCIÓN** |
| Características Generales. | Switch de capa 3 |
| | 24 puertos full duplex (10Base-T, 100Base-TX, 1000Base-T) autosensing |
| | Debe soportar la opción UPLINKS de 4 puertos Gigabit ethernet SFP o 2 puertos 10 Gigabit ethernet SFP+. |
| | Factor de forma 1U |
| | Protocolos de interconexión de datos; Ethernet, Fast Ethernet, Gigabit Ethernet. |
| Requerimiento Capa 2 | Soporte ARP (*Local Proxy Address Resolution Protocol*). |
| | Soporte DHCP, IGMP (*Internet Group Management*), DTP (*Dynamic Trunking Protocol*), LACP (IEEE 802.3ad *Link Aggregation Control Protocol)* |
| | Soporte *Vlan Trunking Protocol* (VTP), VTP *pruning*, VTP *trunks*, VTP links. |
| | Soporte Auto QoS que simplifique la configuración de QoS para redes VoIP, clasifique tráfico y habilite la configuración de encolamiento. |

Continúa

| | |
|---|---|
| | Auto-negociación automática para modo de transmisión half o full duplex en todos los puertos para optimizar el ancho de banda. |
| | Auto MDIX que ajuste de forma automática el envío y recepción si un incorrecto tipo de cable es instalado en los puertos. |
| | Soporte para protocolo de descubrimiento de equipos de red directamente conectados |
| | Soporte Equal cost routing (ECR) para proveer balanceo de carga y redundancia en los enlaces uplinks de la LAN. |
| | Soporte STP (Spanning Tree IEEE 802.1D), 802.1 w (RSTP), 802.1 s (MSTP). |
| | No se require soporte IEEE 802.3af (Power over Ethernet) |
| Requerimiento Capa 3 | Soporte enrutamiento IP (estático, RIPv2, RIPng, OSPF, IGRP, BGPv4 y IS-ISv4). |
| | Soporte enrutamiento con IPv6 (OSPFv3,). |
| | Soporte Policy Based Routing (PBR). |
| | Soporte enrutamiento inter-VLAN IP. |
| Administración | Protocolos de Gestión Remota; SNMPv1, v2c y v3, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, HTTP, SSH-2. |
| Seguridad | Soporte Kerberos, TACACS+ and RADIUS |
| | Soporte ACL (Listas de Control de Acceso) de dirección MAC fuente y destino, dirección IP fuente y destino, puerto TCP/UDP fuente y destino |
| | IEEE 802.1x para el control de acceso a la red basada en puertos. |
| | Soporte AAA, Port Security |
| | Soporte prevención para DHCP Snooping |
| | Soporte prevención para ARP spoofing |
| | Soporte SSL |
| | Soporte SPAN (Switched Port Analyzer) que permita a un sistema de detección de intrusos (IDS) tomar acciones cuando un intruso sea detectado. |
| | Provisión de clasificación 802.1p (CoS) y del campo DSCP, utilizando marcado y reclasificación por paquete, en función de: dirección IP fuente y destino, dirección MAC fuente y destino, o número de puerto TCP/UDP de capa 4. |

**Características Switch de acceso**

En la capa de acceso deberán trabajar en la capas 1 y 2 del modelo ISO/OSI que permita la conmutación de paquetes y acceso a los usuarios y periféricos a la red. Será necesario la adquisición de dos switches capa 2 de 48 y 24 puertos respectivamente.

Cada puerto será fullduplex[31] (Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T). Para conexiones Uplink deberán soportar mínimo 2 puertos Uplinks 10 Gigabit Ethernet de fibra óptica.

Deberán soportar Power over Ethernet (IEEE 802.3af) que permita suministrar de energía eléctrica a dispositivos IP como teléfonos y cámaras IP que a su vez también soporten PoE.

La Tabla 3-15 muestra las características técnicas del switch de acceso.

**Tabla 3-15 Requerimientos técnicos: Switch de acceso**

| SWITCH DE ACCESO | |
|---|---|
| **CARACTERÍSTICAS** | **DESCRIPCIÓN** |
| Características Generales | 2 Switch de acceso (capa 2). |
| | De 48 y 24 puertos respectivamente fullduplex (10Base-T, 100Base-TX, 1000Base-T) de detección automática. |
| | 4 puertos ( SFP) |
| | Factor de forma: Montable en bastidor - 1U |
| | Protocolos de interconexión de datos; Ethernet, Fast Ethernet, Gigabit Ethernet. |
| Requerimientos. | Soporte DHCP Relay. |
| | Soporte Auto QoS que simplifique la configuración de QoS para redes VoIP (Voz sobre IP), clasifique tráfico y habilite la configuración de salida de cola. |
| | Soporte autonegociación automática para modo de transmisión half o full duplex en todos los puertos para optimizar el ancho de banda. |

Continúa

[31] Full dúplex es la cualidad de los elementos que permiten la entrada y salida de datos de forma simultánea.

| | |
|---|---|
| | Soporte DTP (*Dynamic Trunking Protocol*), (LACP (IEEE 802.3ad Link *Aggregation Control Protocol*). |
| | Auto MDIX que ajuste de forma automática el envío y recepción si un incorrecto tipo de cable es instalado en los puertos. |
| | Soporte de Spanning Tree IEEE 802.1D (STP), 802.1 w (RSTP), 802.1 s (MSTP), Spanning-Tree Root Guard (STRG). |
| | Soporte ARP (Local Proxy Address Resolution Protocol) |
| | Soporte Vlan Trunking Protocol (VTP), VTP pruning, VTP trunks, VTP links. |
| | Soporte configuración para optimizar diferentes tipos de tráfico: voz, video, multicast, y datos de alta prioridad (highpriority). |
| | Soporte IGMP (*Internet Group Management Protocol*) version 3, filtrado IGMP |
| | Soporte IEEE 802.3af (Power over Ethernet) |
| Seguridad. | Soporte 802.1p CoS, Weighted tail drop (WTD) |
| | Soporte SSHv2 y SNMPv3. |
| | Soporte autenticación TACACS+ y RADIUS. |
| | Soporte DHCP snooping, IGMP snooping y Port security. |
| Administración | Protocolos de Gestión Remota; SNMPv1, v2c y v3, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, HTTP, SSH-2. |

#### 3.4.2.5. Recomendaciones para la selección de los equipos de conectividad

Para la selección de los equipos de conectividad se ha elegido tres marcas reconocidas en el mercado (Cisco, HP, DLink), las cuales presentan una gran gama de equipos de conectividad como switches de acuerdo al tamaño de la red. Los equipos que se han presentado de las diferentes marcas son orientados a pequeñas y medianas empresas, debido a que se acoplan a la realidad del PPA.

Si bien se trabajará con equipos basados en normas y estándares, se debe elegir una misma marca tanto para el switch de núcleo como los switches de acceso debido que este tipo de equipos con cuentan únicamente con protocolo estandarizados, sino que cuentan con protocolos propietarios que garantizan la conectividad entre los mismo. Además se elegirá una misma línea debido a las garantías que deberá entregar el oferente al PPA, por la configuración de los equipos, mantenimiento y otros.

De la comparación realizada en el Anexo 3.6 de los equipos de conectividad se ha observado que los equipos Cisco presentan mejores características en cuanto a rendimiento, cumplen con todas las características técnicas requeridas y presentan mejores mecanismos de administración y seguridad. Además al ser Cisco una de las empresas líderes a nivel mundial en el área de *networking*, se cuenta con diferentes medios de soporte en caso de fallas.

Los equipos recomendados son:

- Para la capa núcleo se recomienda el switch WS- C3560G-24TS.
- Para la capa acceso se recomienda el switch de 48 puertos WS- 2960S-48LPD-L y el switch de 24 puertos WS- 2960S-24PD-L.

Si bien únicamente se realizó la comparación del switch de acceso de 48 puertos, los estándares y características son las mismas, únicamente cambia las características físicas y de potencia debido al número puertos.

Los equipos deben ser garantizados contra defectos de fabricación y fallas de instalación. El oferente con personal técnico especializado deberá dar respuesta *in situ* en caso de emergencia en un tiempo de no más de una hora en el esquema 8x5XNBD (*Next Bussines Day*).

### 3.4.3. ESQUEMA DE DIRECCIONAMIENTO IP Y VLANS

La estructura organizacional del PPA se encuentra muy bien definida, cada departamento tiene definido sus actividades, información y equipos periféricos comunes a sus intereses. Cada departamento cuenta con una impresora IP y sólo los departamentos que necesitan cuentan con un escáner IP, está distribución departamental ayuda a la organización lógica del PPA a través del direccionamiento IP y la asignación de VLANS, los dos mecanismos permitirán la segmentación de tráfico, ayudarán en la administración de la red complementada con un esquema de seguridad

para la información de cada departamento ya que se impide el acceso a VLANS a las que no pertenezca un usuario.

#### 3.4.3.1. VLANS

A nivel de capa 2 la red se encontrará segmentada de forma lógica a través del uso de VLANs, las cuales irán en relación con la arquitectura organizacional del PPA. Las VLANS serán configuradas en los switches de acceso y núcleo, por lo cual los equipos de conectividad de dichas capas deberán soportar la configuración de VLANS (IEEE 802.1Q).

La Tabla 3-16 muestra la asignación de VLANS que serán establecidas en la red junto con su identificador.

**Tabla 3-16 VLANS**

| VLAN | # VLAN |
|---|---|
| COORDINACIÓN Y SUBCOORDINACION | 10 |
| INVESTIGACIÓN Y ESTUDIOS | 20 |
| PLANIFICACIÓN Y COMPRAS | 30 |
| COORDINACIÓN JURÍDICA | 40 |
| SERVICIOS INSTITUCIONALES | 50 |
| LOGÍSTICA Y MONITOREO | 60 |
| GTI - PPA | 70 |
| SERVIDORES | 1 |
| EQUIPOS CONECTIVIDAD | 2 |
| TELEFONIA | 12 |

Las primeras siete VLANS corresponden a los diferentes departamentos establecidos en el PPA, las cuales además de tener acceso a la su respectiva VLAN, también accederán a la VLAN SERVIDORES la cual les proveerá de las aplicaciones y servicios de la Intranet y a la VLAN TELEFONÍA la cual les proveerá del servicio de telefonía IP a todos los departamentos.

Debido al esquema de una sola conexión para voz y datos realizada en el sistema de cableado estructurado es necesario que cada puerto del switch de acceso destinado a los usuarios tenga configurado las tres VLANs (su VLAN, SERVIDORES y TELEFONIA) a excepción del departamento GTI, el cual tendrá acceso a todas la VLANs para su respectiva gestión y administración.

En la VLAN SERVIDORES se encontrarán los servidores de la Intranet que presten servicios únicamente a los usuarios de la LAN, no se ubicarán en esta VLAN los servidores de correo electrónico y página web dado que son aquellos que interactúan con Internet y a los que se los ubicará dentro de una DMZ. Entre los servidores a ubicar dentro de esta VLAN se encuentran el servicio de directorio, servicio DHCP, servidor Antivirus, servidor de aplicaciones, servidor de Base de Datos.

En la VLAN EQUIPOS DE CONECTIVIDAD se encontrarán todos los equipos de conectividad como los switches, el equipo firewall, los Access Points, cámaras IP entre otros, a los cuales se les asignará una IP dentro de dicha subred y VLAN para su administración, a esta VLAN solo tendrá acceso GTI-PPA.

El tráfico de servicio de telefonía IP se deberá manejar en una VLAN diferente a la de SERVIDORES debido al tipo de tráfico y al diferente manejo que este recibe en cuanto a priorización de tráfico. Se creará la VLAN TELEFONIA a la cual se adherirán los teléfonos IP.

#### 3.4.3.2. Direccionamiento IP

El esquema de direccionamiento IP se realizará mediante subredes, a cada VLAN se le asignará una subred mediante VLSM[32] (*Variable Length Subnet Mask*). Para determinar el tamaño de subred a utilizar en cada VLAN se debe calcular el número de hosts por departamento y su proyección en los próximos 5 años.

[32] VLSM es un mecanismo que se implementan para el ahorro de direcciones IP, ya que a cada subred se le asigna un rango de direcciones de acuerdo a su número de host.

La Tabla 3-17 muestra el número de hosts por departamento que serán necesarios durante los próximos 5 años.

**Tabla 3-17 Número de host por departamento**

| CÁLCULO DE NÚMERO DE HOSTS POR DEPARTAMENTO | | | | |
|---|---|---|---|---|
| **DEPARTAMENTO** | **PCs E IMPRESORAS** | **PROYECCCIÓN HOSTS** | **NÚMERO BITS HOSTS** | **DIR. IPs VÁLIDAS** |
| COORDINACIÓN Y SUBCOORDINACION | 10 | 16 | 5 | 29 |
| INVESTIGACIÓN Y ESTUDIOS | 6 | 16 | 5 | 29 |
| PLANIFICACIÓN Y COMPRAS | 6 | 16 | 5 | 29 |
| COORDINACIÓN JURÍDICA | 5 | 16 | 5 | 29 |
| SERVICIOS INSTITUCIONALES | 8 | 16 | 5 | 29 |
| LOGÍSTICA Y MONITOREO | 13 | 16 | 5 | 29 |
| GTI - PPA | 6 | 16 | 5 | 29 |
| SERVIDORES | 10 | 16 | 5 | 29 |
| EQUIPOS CONECTIVIDAD | 10 | 16 | 5 | 29 |
| TELEFONIA | 30 | 50 | 6 | 61 |

Del cálculo se observa que las VLANs de datos necesitan 5 bits del último octeto para la asignación de direcciones IP a los hosts a excepción de la VLAN de telefonía la cual necesita 6 bits de hosts.

Se realiza el direccionamiento IP de acuerdo al número de hosts necesarios y se determina el número de direcciones de hosts válidas en cada subred, la dirección de subred. A cada subred se le debe restar la dirección de red, la dirección de *broadcast* y la dirección *gateway* de la vlan, las cuales no pueden ser utilizadas para hosts.

Para el direccionamiento IP se ha tomado como base la dirección 192.168.1.0. La Tabla 3-18 muestra el direccionamiento IP asignado a cada VLAN.

**Tabla 3-18 Direccionamiento IP**

| DIRECCIONAMIENTO IP | | | | |
|---|---|---|---|---|
| **DEPARTAMENTO** | **DIR. DE SUBRED/MÁSCARA** | **PRIMERA DIR. IP VÁLIDA** | **ÚLTIMA DIR. IP VÁLIDA** | **BROADCAST** |
| COORDINACIÓN Y SUBCOORDINACION | 192.168.1.0 / 27 | 192.168.1.1 | 192.168.1.30 | 192.168.1.31 |
| INVESTIGACIÓN Y ESTUDIOS | 192.168.1.32 / 27 | 192.168.1.33 | 192.168.1.62 | 192.168.1.63 |
| PLANIFICACIÓN Y COMPRAS | 192.168.1.64 / 27 | 192.168.1.65 | 192.168.1.94 | 192.168.1.95 |
| COORDINACIÓN JURÍDICA | 192.168.1.96 / 27 | 192.168.1.97 | 192.168.1.126 | 192.168.1.127 |
| SERVICIOS INSTITUCIONALES | 192.168.1.128 / 27 | 192.168.1.129 | 192.168.1.158 | 192.168.1.159 |
| LOGÍSTICA Y MONITOREO | 192.168.1.160 / 27 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 |
| GTI - PPA | 192.168.1.192 / 27 | 192.168.1.193 | 192.168.1.222 | 192.168.1.223 |
| SERVIDORES | 192.168.1.224 / 27 | 192.168.1.225 | 192.168.1.254 | 192.168.1.255 |
| EQUIPOS CONECTIVIDAD | 192.168.2.0 / 27 | 192.168.2.1 | 192.168.2.30 | 192.168.2.31 |
| TELEFONIA | 192.168.2.64 / 26 | 192.168.2.65 | 192.168.2.126 | 192.168.2.127 |

La asignación de direcciones IP a las estaciones de trabajo y teléfonos IP se realizará a través del servicio de DHCP (Protocolo de Configuración Dinámica de Hosts) mientras que servidores, equipos de conectividad y periféricos (impresoras y escáneres) se configurarán con direcciones IP estáticas debido a que son equipos que son buscados por los usuarios para utilizarlos, administrarlos o adquirir un servicio por lo que no deberán cambiar su dirección de forma continua.

### 3.4.4. DISEÑO DE LA WLAN

La red inalámbrica dará cobertura a todos los departamentos del PPA, convirtiéndose en un complemento de la red cableada, mediante la cual se proporciones a los usuarios una mayor movilidad y flexibilidad en el acceso a Internet y a todos los servicios de la Intranet.

La red inalámbrica permitirá movilidad de los usuarios, especialmente de equipos inalámbricos como teléfonos IP y cámaras IP y ofrecerá conectividad en lugares en donde no se haya provisto de puntos de red y se necesite conectividad de forma temporal.

Se crearán dos perfiles de usuario en la red inalámbrica. Uno para los usuarios internos, los cuales tendrán acceso a todos los servicios y aplicaciones de la Internet y otro para usuarios externos, los cuales únicamente tendrán acceso a Internet.

Para el diseño de la red inalámbrica se tomará en cuentas el área de cobertura, el número máximo de usuarios simultáneos, el tipo de construcción del edificio, la interconexión con la red cableada, la velocidad de transmisión y frecuencia de operación y la seguridad.

En un principio los equipos inalámbricos trabajarán como punto de acceso autónomo debido a la pequeña área de cobertura inalámbrica, pero deberán tener la posibilidad de acoplarse a una red de datos inalámbrica de comunicaciones más amplia.

#### 3.4.4.1. Área de cobertura

El área de cobertura de la WLAN comprenderá todos los departamentos del PPA principalmente a las dos salas de reuniones y al departamento de Coordinador Nacional, en los cuales se reciben a los diferentes proveedores, los cuales en su gran mayoría hacen uso de una portátil e Internet.

El área de cobertura depende principalmente de la frecuencia de operación, si el área a cubrir es un ambiente cerrado o abierto y de la ganancia de las antenas. Para tener mayor cobertura se trabajará en la frecuencia de 2.4 Ghz, el área a cubrir es un ambiente cerrado, lo cual disminuye el área de cobertura, los Access Point deberán poseer antenas de una ganancia considerable.

#### 3.4.4.2. Número máximo de usuarios simultáneos

Se tendrá alrededor de 11 equipos, pero se diseñará para el uso simultáneo de 15 equipos los cuales no sobre pasan a las consideraciones de IEEE 802.11g que admite hasta 50 usuarios simultáneos.

#### 3.4.4.3. Tipo de construcción del edificio

El tipo de construcción del edificio determina como las ondas electromagnéticas de la WLAN se propagan. La construcción del edificio es de hormigón, en el plano arquitectónico se puede observar la ubicación de las columnas y paredes. Una gran ventaja es que las divisiones entre los diferentes departamentos serán hechas con paneles de madera y vidrio los cuales son materiales que no atenúan la potencia de la señal en gran cantidad, haciendo que la cobertura de la WLAN se extienda.

#### 3.4.4.4. Conexión de la WLAN con la red cableada

La conexión de la WLAN a la red cableada fue tomada en cuenta en el diseño del sistema de cableado estructurado, en el número de puertos de los switches de acceso, en el direccionamiento IP. Se dispondrá de dos salidas de telecomunicaciones, una en cada extremo de las instalaciones para la ubicación de los *Access Points*. Los *Access Points* se ubicarán en el techo y tendrán la posibilidad de ser reubicados dependiendo del alcance y área de cobertura.

Tanto los switches de acceso como los *Access Points* deberán manejar PoE (*Power over Ethernet*) bajo la norma IEEE 802.3af, que permita que los *Access Points* sean alimentados de energía eléctrica a través del mismo cable de datos, sin embargo también se ubicará tomas de UPS cercanas a dichos puntos de red.

#### 3.4.4.5. Velocidad de transmisión y frecuencia de operación

La red inalámbrica será un complemento a la red cableada y no necesitará velocidades de operación sumamente grandes. El estándar con el que se trabajará es IEEE 802.11 g que permite velocidades de transmisión de hasta 54 Mbps.

La frecuencia de operación de IEEE 802.11g es de 2.4 GHz, la cual ofrece mayor propagación que la frecuencia de 5GHz utilizada por IEEE 802.11a.

En América Latina la banda de 2.4 GHz se encuentran definidas 11 canales utilizables para WIFI, de los cuales únicamente se pueden utilizar 3 que son el canal 1, el canal 6

y el canal 11, los demás se encuentran inhabilitados porque se superponen provocando interferencias.

El edificio en el que se encontrarán las instalaciones del PPA no tiene edificios contiguos que pudieran tener redes inalámbricas y provocar interferencia a la red inalámbrica del PPA. En el edificio actualmente se encuentra funcionando el IEPS (Instituto Nacional de Economía Popular y Solidaria) cuyo departamento de sistemas ha informado a GTI-PPA que toda su red inalámbrica se encuentra funcionando en el canal por defecto (canal 6).

Por las razones mencionadas, la red inalámbrica del PPA se encontrará configurada en el canal 11 para evitar interferencia con la red inalámbrica del IEPS.

#### 3.4.4.6. SSID y seguridad de acceso WLAN

Un sistema inalámbrico seguro debe cumplir con requerimientos de autenticación, confidencialidad, integridad y disponibilidad.

Para evitar que un usuario común identifique e intente conectarse a la red, el *broadcast* SSID (*Service Set Identifier*) será desactivado de tal forma que se mantenga oculto, además no se conservará el SSID por defecto de los equipos, el SSID deberá ser cambiado a un nombre difícil de predecir, por lo que el nombre del SSID no tendrá un nombre que tenga relación con el PPA.

En la red inalámbrica se permitirá el acceso a tráfico de internet, correo electrónico y transferencia de archivos y todos los demás protocolos serán bloqueados.

El estándar de seguridad ha utilizar será WPA2 (*Wi-Fi Protected Access 2*) que integra mecanismos de autenticación EAP (*Extensible Autentication Protocol*), algoritmos de encripción AES (*Advanced Encryption Standard*) y el protocolo de cifrado TKIP (*Temporal Key Integrity Protocol*).

Todos estos mecanismos de seguridad, ocultación de SSID harán que el acceso a la red inalámbrica sea únicamente permitida por GTI-PPA, además se deberá configurar el direccionamiento IP.

#### 3.4.4.7. Características técnicas del Access Point

Los equipos inalámbricos deberán trabajar en la banda de frecuencia ISM (*Industrial, Scientific and Medical*) de 2.4 GHz que permita su operación sin licencia. La FCC (*Federal Communications Commission*) permite su operación a equipos que utilizan 1 Watt o menos

Las características técnicas que deberán cumplir los equipos son:

- Deberán cumplir con la norma IEEE 802.11 a/b/g.
- Compatibles con fuentes de alimentación que cumplan con la norma IEEE 802.3af (PoE) dado que el *Access Point* se conectará a un puerto del switch de acceso que suministra de energía eléctrica a través de PoE.
- Certificado Wi-Fi para estándares IEEE 802.11 a/b/g.
- Deberán cumplir el estándar de seguridad WPA, WPA2, 802.11i y 802.1x.
- Soporte protocolos de encripción AES y el protocolo de cifrado TKIP.
- Soporte mecanismos de autenticación EAP: TLS, TTLS, PEAP.
- Soporte VLANs de acuerdo con la norma IEEE 802.1Q.
- Detección automática de Ethernet IEEE 802.3 10/100/1000 BASE-T.
- Antenas trabajando a frecuencias de 2.4 GHz y 5 GHz con ganancia mínima de 2.0 dBi con ángulo de apertura de 360 grados.
- Deberá soportar un esquema de seguridad AAA (*Autentication, Accounting, Autorization*) a través de RADIUS que permita en un futuro el manejo de perfiles de usuarios móviles.
- Control de acceso a través de MAC.
- Protocolos de gestión remota SNMP, telnet, http, HTTPS.

#### 3.4.4.8. Recomendaciones para la selección del Access Point

Para la selección del Access Point se ha elegido tres marcas reconocidas en el mercado (Cisco, HP, DLink). Los equipos que se han presentado de las diferentes marcas son orientados a pequeñas y medianas empresas, debido a que se acoplan a la realidad del PPA.

De la comparación realizada en el Anexo 3.6 de los Access Point se ha observado que los equipos Cisco presentan mejores características en cuanto a rendimiento, cumplen con todas las características técnicas requeridas.

Los equipos recomendados son:

- Para el acceso inalámbrico a la red de comunicaciones se recomienda el Access Point AP541N de la línea *Small Business*[33].

Los equipos deben ser garantizados contra defectos de fabricación y fallas de instalación. El oferente con personal técnico especializado deberá dar respuesta *in situ* en caso de emergencia en un tiempo de no más de una hora en el esquema 8x5XNBD (*Next Business Day*[34]).

### 3.4.5. ESQUEMA DE TELEFONÍA IP

El esquema de telefonía IP abarcará:

- Diseño de la red LAN para soportar VoIP.
- Diseño de las red WAN para soportar VoIP.
- Análisis de los requerimientos para VoIP.
- Definir el ancho de banda necesario para VoIP.
- Definir las características de Hardware para VoIP.

[33] Small Business es una categorización de los equipos de conectividad según el tamaño de la empresa.
[34] Next Business Day (NXBXD) es una garantía que es extendida por Cisco para sus equipos.

#### 3.4.5.1. Características de la red LAN para el soporte de VoIP

El servicio de telefonía IP requiere contar con una infraestructura de comunicaciones que soporte VoIP. Las características tomadas en cuenta para dicho propósito son:

- A nivel físico se diseñó un sistema de cableado estructurado categoría 6A que permite la implementación de aplicaciones de VoIP, en el cual se manejará una sola conexión para voz y datos mediante el uso de teléfonos IP que cuenten con un mini switch que permita la conexión al computador y a la LAN.
- A nivel lógico se diseñó un dominio de *broadcast* exclusivo para telefonía IP, al cual se le asigno una subred y una VLAN.
- A nivel de equipos de conectividad se estableció que los switches de núcleo y acceso deberán manejar calidad de servicio para la priorización del tráfico de voz y a nivel de switch de acceso deberá manejar *PoE* para el suministro de energía eléctrica a teléfonos IP.
- A nivel de firewall, el equipo deberá permitir conexiones con diferentes sedes que en los próximos años se formarán alrededor de todo el país como método de descentralización de la provisión de alimentos, sedes que deberán formar parte de la solución de telefonía IP mediante conexiones VPN.

#### 3.4.5.2. Análisis de los requerimientos para telefonía IP.

El servicio de telefonía IP será provisto a través de software libre, dado que se trata de una entidad gubernamental que debe cumplir el decreto 1014 que promueve el uso de software libre en las instituciones públicas.

La plataforma sobre la cual se instalará el servicio será Linux, debido a que es un sistema operativo orientado a servidores y sobre la cual se encuentra el software *Asterisk*, el cual se encuentra probado en varias instituciones públicas en donde su funcionamiento ha permanecido estable. Además es una opción que se adapta tanto a pequeñas y medianas empresas.

#### 3.4.5.3. Esquema de direccionamiento

El direccionamiento del servicio de telefonía IP se encuentra en la subred 192.168.2.64 / 26 (de acuerdo al direccionamiento IP de la red LAN diseñado) y cuenta con su VLAN específica (VLAN 12), haciendo que el tráfico de voz se encuentre en un solo dominio de *broadcast*, lo cual permite identificar a dicho tráfico para su respectiva priorización.

El plan de numeración en la nueva infraestructura de comunicaciones del PPA será la misma utilizada en la red del MIES, de tal manera que el cambio sea transparente al usuario. El plan de numeración fue detallado en el análisis de la situación actual del PPA.

#### 3.4.5.4. Características técnicas de la solución de telefonía IP

Las características técnicas de la solución de telefonía IP son las siguientes:

**CENTRAL TELEFÓNICA.**

- El servicio de telefonía deberá permitir una escalabilidad de mínimo 5 años, por lo que deberá ser dimensionado para un crecimiento de alrededor de 50 usuarios.
- Deberá soportar como mínimo los códec G.711 y G.729 para entornos LAN y WAN respectivamente.
- Los protocolos de señalización que deberá soportar son SIP (*Session Initiation Protocol*), H.323 y MGCP (*Media Gateway Controller*). Deberá permitir la conexión con centrales telefónicas de distintas marcas en modo *troncalizado* a través de SIP.
- La solución deberá permitir la conexión con la Red Telefónica Pública Conmutada (PSTN por sus siglas en inglés), para lo cual deberá constar con interfaces BRI (*Basic Rate Interface*), PRI (*Primary Rate Interface*), SIP.
- La solución deberá garantizar la compatibilidad con la señalización de los proveedores locales de telefonía IP.

- La central telefónica deberá acoplarse al firewall desde dónde se establecerán conexiones VPN para el acceso al servicio de telefonía IP de forma remota.
- El PPA actualmente hará uso de 10 líneas telefónicas.
- Se deberá disponer de un control de llamadas telefónicas a nivel interno y externo en el cual incluya la tarifación y restricción de llamadas.
- Deberá soportar IVR (Respuesta de Voz Interactiva) que permitan encaminar una llamada entrante a cada uno de los departamentos.
- Deberá proporcionar un sistema de mensajería unificada que de soporte para buzón de voz, sistema de registro, autenticación de usuarios para todos los usuarios, temporizador de llamadas, contestación automática de llamadas.
- Deberá permitir la creación de múltiples niveles de usuario y grupos sincronizados vía LDAP al servicio de directorio.
- La administración deberá realizarse mediante HTTP, SSH y debe permitir la generación de reportes por parte de los administradores.

Las herramientas secundarias con las que contará el servidor de telefonía IP son:

- Soporte para softphones.
- Sala de conferencias.
- Music –on-hold o de espera.
- Integración con clientes Thunderbird.
- Grabación de llamadas.
- Limitación de tiempo de llamada y niveles de servicio.

**TELÉFONOS IP**

Los teléfonos IP para los funcionarios del PPA no requiere de características especiales, únicamente se otorgará teléfonos IP del tipo ejecutivo a los directores de cada uno de los departamentos.

Los teléfonos IP para los diferentes funcionarios deberán tener las siguientes características:

- Soporte PoE.
- Dos puertos 10/100/1000 Mbps *autosensing* para la conexión al computador y a la LAN.
- Soporte los códecs G.711 y G.729.
- Soporte a nivel de capa 2 IEEE 802.1 p.
- Soporte VLANs
- Soporte protocolo de señalización SIP.
- Soporte DHCP, DNS.
- Identificador de llamadas
- Llamada en espera
- Transferencia de llamadas
- Administración vía Web

Los teléfonos IP para los directores de los diferentes departamentos a más de las características mencionas deberán constar con:

- Manos libres
- Características para conferencias

**SOFTPHONE**

Se deberá contar con *softphones* que permitan dar acceso al servicio de telefonía IP a visitantes y nuevos empleados del PPA, los cuales harán uso de dicho software mientras se adquiera nuevos teléfonos IP. Además los *softphones* serán utilizados por el personal principalmente del departamento de Logística, los cuales al salir a inspecciones accederán de forma remota a través de una VPN a los servicios Intranet, entre los cuales estará el servicio de telefonía IP.

El *softphone* deberá tener las siguientes características:

- Además de proveer del servicio de voz, deberá constar con servicios adicionales para videollamadas, mensajería instantánea a través de una interfaz simple.

- El software debe basarse en protocolos de señalización SIP.
- Los requerimientos del software deben coincidir con las características de las computadoras y portátiles del PPA.
- El software deberá ser compatible con sistemas operativos Windows y Linux, debido a que todos los sistemas operativos a nivel del cliente son Windows.
- Deberá tener la posibilidad de almacenar contactos, historial de llamadas, identificador de llamadas, grabación de llamas, entre otros.

Uno de los beneficios importantes es que brindará a los funcionarios del PPA movilidad, permitiéndole trasladarse del lugar de trabajo al aeropuerto, a hoteles y demás lugares donde se tenga una conexión WiFi y lo más importante es que la llamada se realizará sin costos adicionales, ya que la misma se realizará a través de Internet.

#### 3.4.5.5. Recomendación para la selección de la Central IP

El dimensionamiento del hardware para el servidor *Asterix* dependerá del número de llamadas simultáneas, de la duración promedio de las misma, y del número de canales (33 llamadas en una hora pico, 3 minutos promedio de duración de la llamada) y de las aplicaciones adicionales al servicio de telefonía IP. La Tabla 3-19[35] muestra los requerimientos mínimos del sistema según el propósito y número de canales.

**Tabla 3-19 Requerimientos mínimos para el servidor Asterisk**

| Propósito | Número de Canales | Procesador | Memoria |
|---|---|---|---|
| Sistema de Pruebas | No más de 5 | 400 MHz x86 | 256 MB |
| Sistemas SOHO (small office/home) | 5 a 10 | 1 GHz x86 | 512 MB |
| Sistema para pequeños negocios | Hasta 15 | 3 GHz x86 | 1 GB |
| Sistema mediano grande | Más de 15 | CPUs duales, posible múltiples servidores en arquitectura distribuida | |

[35] Tabla tomada de: Van Meggelen J., Smith J., Madsen L.; "Asterisk. The Future of Telephony". Ed. O'Reilly (2005).

La Tabla 3-20 detalla las características técnicas para servidor Asterisk.

**Tabla 3-20 Requerimientos técnicos: Servidor Asterisk**

| SERVIDOR ASTERISK | |
|---|---|
| **DESCRIPCIÓN** | **ESPECIFICACIONES** |
| Capacidad | 50 usuarios |
| Servidor | HP ProLiant DL320 G6 L5506 2,13 GHz Quad Core |
| Tipo | Para montaje en rack 19” |
| Tipo de procesador | |
| | Quad Core Intel® Xeon® E5640 Series Processors |
| Memoria RAM | 4GB PC3-10600R (DDR3) -1333 RDIMM (4X 2 GB), DIMMs de 2GB mínimo. |
| Unidades de disco rígido incluidas | 2 Discos duros SAS de 300 GB |
| Unidad óptica (CD/DVD R/W) | 1 Slim 12.7mm SATA DVDRW Optical Kit |
| Controladora de red | 2 NC382i Dual Port Multifunction Gigabit Server Adapters, TCP/IP Offload Engine, Accelerated iSCSI Support incluído |
| Conexión de almacenamiento estándar | Hot plug 2.5-inch SAS |
| Sistema Operativo | Sistema Operativo basado en GNU / Linux |
| Chasis (Factor de forma) | Rack |
| Número mínimo de puertos | Serial 2; Pointing Device (Mouse) – 1; Graphics -1; Keyboard – 1; VGA -2 (1 frontal, 1 posterior); Network RJ-45 -2; iLO 2 remote management port – 1; SD slot -1; USB 2.0 ports – 5 total ( 2 frontales, 2 posteriores, 1 interno) |
| Fuentes de poder requeridas | 2 fuentes de poder redundantes conectables en caliente de alta capacidad |
| Kit de montaje en rack | Debe incluir rieles deslizables para rack en gabinetes; especificar demás accesorios necesarios |
| Cables de poder | 2 Cables de poder, NEMA 5-15P a C13 de 15 Amps y 3m de longitud |
| Tipo de equipo | Nuevo (NO Refurbished o reacondicionados) adjuntar certificado del fabricante |

Continúa

| | |
|---|---|
| Principales funciones de la PBX | Soporte para protocolos SIP, IAX, no H.323 |
| | Codecs a soportar: ADPCM G.711 (A-law & μ-law) G.722, G.723.1 (pass through) G.729, GSM, iLBC. |
| Debe soportar las siguientes interfaces hacia la PSTN | Analógicas (al menos 10) |
| | Digitales o E1s (al menos 2) |
| | SIP Trunking |
| Puertos o Interfaces a la PSTN requeridos | 1 Tarjeta o gateway de voz de 4 puertos FXO (para líneas analógicas o bases celulares) |
| | • 1 Tarjeta o gateway de voz de 1 Puerto E1 (ISDN/PRI) |
| | • 1 Tarjeta o gateway de voz de 48 puertos FXS (para manejo de 10 teléfonos analógicos) |
| Requerimientos adicionales para PSTN | Conectividad para líneas o troncales IP/SIP |
| Capacidad máxima de Usuarios | Hasta 100 extensiones (SIP/IAX)registradas, sin licenciamiento |

El servidor deberá ser garantizado tanto en su hardware, software, configuración, soporte y capacitación.

#### 3.4.5.6. Recomendación para la selección de terminales IP

Para la selección de teléfonos IP se ha elegido tres marcas reconocidas en el mercado (Cisco, HP, Polycom), las cuales presentan una gran gama de equipos de telefonía IP acordes al tamaño de la red. Los equipos que se han presentado de las diferentes marcas son orientados a pequeñas y medianas empresas, debido a que se acoplan a la realidad del PPA.

Para la elección de teléfonos IP se ha tomado en cuenta que sean compatibles con la central IP Asterisk, la cual va a manejar el códec G.711 y G.729 y el protocolo de señalización SIP. Además se ha buscado teléfonos que trabajen con un mini switch que permita conectarse a la LAN y a la PC. Al tratarse de una red Gigabit Ethernet se ha escogido teléfonos cuyos puertos trabajen a 10/100/1000 Mbps que impidan que se formen cuellos de botella entre el equipo de conectividad y la PC.

De la comparación realizada en el Anexo 3.6 se ha observado que los equipos HP presentan mejores características en cuanto a rendimiento, cumplen con todas las características técnicas requeridas y presentan mejores mecanismos de administración y seguridad. Además al ser HP una de las empresas que mayor desarrollo ha tenido en cuanto a telefonía IP.

Los equipos recomendados son:

- Para los teléfonos IP para los diferentes funcionarios serán HP 3501.

Los teléfonos para los directores de cada departamento serán de la línea ejecutiva de la misma marca de los anteriores teléfonos, los cuales deberán mejores prestaciones de audio para conferencias. Por motivos de homologación de teléfonos, configuración, garantías y otros.

Los equipos recomendados son:

- Los teléfonos IP para los directores son HP 3503

En la actualidad se necesitarán 7 teléfonos HP 3503 para los directores de los 7 departamentos y 23 teléfonos HP 3501 para los demás funcionarios del PPA.

#### 3.4.5.7. Recomendación para la selección de terminales softphone

El MIES en la actualidad utiliza el software X-Lite[36], el cual cuenta con todos los requerimientos detallados anteriormente, además es un software gratuito compatible con Windows 7 (Sistema operativo en clientes del PPA) y sus requerimientos de hardware son compatibles con las computadoras del Programa.

### 3.4.6. SERVICIOS DE LA INTRANET[11]

Diseñada la infraestructura física y lógica de la red del PPA, es necesario el diseño de una Intranet corporativa que cuente con los servicios necesarios para el correcto desenvolvimiento de las actividades del PPA.

[36] http://www.counterpath.com/x-lite.html

El Programa de Provisión de Alimentos al ser una institución pública debe cumplir el decreto 1014 que promueve el uso de Software Libre que preste iguales o mejores prestaciones que el software propietario.

La Subsecretaría Informática del Ecuador recomienda que la migración de aplicaciones a Software Libre sea la siguiente.

En estaciones de trabajo

- Navegador de Internet
- Cliente de correo electrónico
- Suite de ofimática[37]
- Software especializado: inteligencia de negocios, gestión de proyectos, editor de imágenes, antivirus, GIS, etc.
- Sistema Operativo.

De las aplicaciones mencionadas, las tres primeras se encuentran ya migrados con *Mozilla Firefox*, *Mozilla Thunderbird* y *OpenOffice* respectivamente.

En cuanto a servidores la Subsecretaría Informática recomienda la migración en el siguiente orden.

- Servidor de aplicaciones
- Servidor de correo electrónico
- Servidor de archivos e impresión
- Servidor Web, en el caso de páginas estáticas. Servidor Web y base de datos en el caso de páginas dinámicas.
- Servidor de seguridades
- Directorio activo
- Servidor de base de datos

[37] Ofimática es al conjunto de hardware y software que permiten crear, editar, almacenar y transmitir información en una oficina.

A los cuales se les dará una opción a través de software libre

#### 3.4.6.1. Plataforma para la implementación de los servicios de la Intranet

La plataforma ha utilizar para la implementación de los servicios de la Intranet serán basados en GNU/Unix. Cabe destacar que las instituciones públicas se encuentran en procesos de migración del software propietario al software libre y el PPA no es la excepción por lo que el personal de GTI-PPA recibió un curso de capacitación en Administración de Servidores Linux, el cual se basó específicamente en la distribución CentOS.

#### 3.4.6.2. Servicio de DNS (*Domain Name System*)

El servidor DNS almacena información asociada a nombres de dominio a direcciones IP en redes, la resolución de nombres es transparente a aplicaciones cliente. El servicio de DNS permitirá direccionar todas las consultas internas como para que se puedan acceder a los recursos desde una red externa.

##### *3.4.6.2.1. Alternativas de Software*

Las alternativas para la implementación del servicio de DNS son las siguientes:

**BIND** (*Berkeley Internet Name Domain*) es el servidor DNS usado por defecto en Internet y se encuentra en la mayoría de distribuciones Unix y Linux, incorpora DNSSEC (DNS *Security Extensions*) que protege a usuarios de la redirección a sitios web fraudulentos y de direcciones no deseadas mediante la autenticación de la respuesta a una consulta DNS, incorpora TSIG (*Transaction Signature*) que provee una forma de autenticación de las actualizaciones de base de datos que se comparten entre servidores DNS e incorpora IPv6

**PowerDNS** es un servidor de código abierto, multiplataforma con licencia GPL que trabaja tanto en funciones de servidor autoritativo como recursivo, trabaja con diferentes tipos de bases de datos.

**Unbound** es un servidor de código abierto que trabaja como servidor recursivo y de cache, cuenta con seguridad DNSSEC. Se encuentra bajo la licencia BSD.

**Djbdns** fue basado en un principio en *Openbsd*, pero también correo sobre las plataformas Linux y FreeBSD, se caracteriza por ser diseñado de forma modular, enfocado a la seguridad y velocidad de procesamiento. Está compuesto por programas independientes que realizan una tarea específica, uno de sus mejores características es la de separar la caché DNS del servidor DNS evitando que las consultas al servidor DNS sean respondidas por la caché DNS, provocando un falso positivo.

**Dnsmasq** es un servidor liviano, fácil de configurar que integra los servicios de DHCP y TFTP, trabaja como servidor DNS recursivo y de caché, es un servidor de código abierto bajo licencia GPL. La Tabla 3-21 muestra la comparación entre los diferentes servidores DNS bajo Software Libre con código abierto de acuerdo a diferentes características.

**Tabla 3-21Comparación: Servidor DNS**

| Servidor | Características | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Autoritativo | Recursivo | Modo Esclavo | Caching | DNSSEC | TSIG | IPv6 | Licencia |
| **BIND** | Si | Si | Si | Si | Si | Si | Si (desde 9.x) | BSD |
| **djbdns** | Si | Si | Si | Si | No | No | No | Public domain |
| **Dnsmasq** | No | Si | No | Si | No | No | Si | GPL |
| **PowerDNS** | Si | Si | Si | Si | Si (desde 3.0) | Si (desde 3.0) | Si | GPL |
| **Unbound** | No | Si | No | Si | Si | Si | Si | BSD |

#### *3.4.6.2.2. Selección alternativa*

La alternativa escogida para la configuración del servidor de nombres de dominio es BIND la cual cuenta con todas las características indicadas en la tabla anterior, es el servidor más usado en Internet y viene por defecto en todas las distribuciones Linux, además se encuentra patrocinado por *Internet Systems Consortium* que es un

desarrollador y distribuidor de software de código abierto el cual ofrece una gran cantidad de documentación y soporte, mantenimiento y resolución de problemas.

#### 3.4.6.3. Servicio de DHCP (*Dynamic Host Configuration Protocol*)

La gestión del direccionamiento IP será manejado por el servicio de DHCP, el cual asignará la direcciones IP, máscara de red, ruta de enlace predeterminada, direcciones DNS, entre otros a computadores y teléfonos IP de forma dinámica en el rango establecido por la subred asignada, además reservará las direcciones IP para asignarlas de forma manual y estática a la VLAN de servidores y equipos periféricos.

##### *3.4.6.3.1. Alternativas de Software*

Las alternativas para la implementación del servicio de DHCP son ISC DHCP (*Internet Systems Consortium DHCP*) y Dual DHCP DNS Server los cuales trabajan bajo la plataforma GNU/Linux, son código abierto los cuales se encuentran en la capacidad de trabajar con múltiples redes, *DHCP Relay* y trabajan conjuntamente con el servidor DNS para la configuración de nombres de dominio. La Tabla 3-22 muestra un resumen de las características de dos servidores.

**Tabla 3-22Comparación: Servidor DHCP**

| Servidor | Características | | | | | | |
|---|---|---|---|---|---|---|---|
| | GNU/Linux | Gratuito | Múltiples Redes | DHCP Relay | Asignación de direcciones por MAC | Configuración de nombres de dominio | Trabajo con DNS |
| DHCP Server ISC | Si | Si | Si | Si | Si | Si | Si |
| Dual DHCP DNS Server | Si | Si | Si | Si | Si | Si | Si |

##### *3.4.6.3.2. Selección alternativa*

Si bien los dos servidores cuentan con las mismas características, se elegirá al servidor DHCP ISC debido a que se encuentra sumamente difundido, viene instalado en la gran mayoría de plataformas GNU/Linux y asegura compatibilidad con el servidor BIND que se eligió como servidor de nombres de dominio DNS ya que son desarrollados por ISC.

#### 3.4.6.4. Servidor de Correo Electrónico

El correo electrónico es uno de los servicios que mayor importancia tiene para la gran mayoría de empresas debido a la gran cantidad de actividades comerciales que se realizan a través de este medio. Si bien en un principio el servicio de correo electrónico y la página web se encuentran en un *hosting*, estos deberán ser previstos para su futura implementación dentro de la Intranet.

##### *3.4.6.4.1. Alternativas de Software*

Las alternativas de software para la configuración del servidor de correo electrónico son las siguientes:

**Open Xchange** a más de ser un sistema de correo electrónico es una suite de colaboración que proporciona a los usuarios un avanzado sistema de comunicación. El software incluye correo electrónico, filtro *anti-spam,* detector de virus, calendario, gestión de contactos, tareas, carpetas privadas, públicas, seguimiento de proyectos, foros de debate, los cuales se encuentran integradas a modo de portal.

**Sendmail** es el MTA más popular, compatible con sistemas Unix, de código abierto. Diseñado para la entrega rápida de mensajes, para el envío de correo externo a la intranet hace uso del servidor DNS para determinar el Host al que debe ser enviado el correo. Una función importante de Sendmail es el uso de *alias* para los usuarios, permitiendo la creación de listas de correo entre grupos.

**Postfix** es un agente de transporte de correo electrónico (MTA) que funciona sobre sistemas tipo Unix, mejorado en aspectos de seguridad, configuración y administración, presenta una arquitectura modular compuesta de varios procesos con usuarios no privilegiados, cada proceso corre con los permisos necesarios para realizar su tarea, evitando que algún proceso corra con el usuario *root* lo cual provocaría vulnerabilidades en el sistema. Su facilidad de configuración es un factor importante, además puede complmentarse con LDAP, SSL/TLS, SASL.

**Qmail** es un servidor de correo electrónico, compatible con sistema Unix, es distribuido como software de código abierto. Qmail se encuentra desarrollado por módulos que se ejecutan de forma separada, entre los que se encuentran las transacciones SMTP, gestión de encolamiento, distribución de mensajes, lo cual lo hace más seguro al no ser un software monolítico.

**Zimbra** a más de ser un software para el servicio de correo electrónico es una suite de colaboración que se basa en Postfix, MySQL, OpenLDAP, existen varias versiones las cuales son de código abierto pero también existe la versión de código cerrado que contienen diferentes mejoras

La Tabla 3-23 muestra un resumen de las características servidores antes mencionados.

**Tabla 3-23 Comparación: Servidor Correo Electrónico**

| Características | Servidor | | | | |
|---|---|---|---|---|---|
| | OpenXchange | Postfix | Qmail | Sendmail | Zimbra |
| Linux/Unix | Si | Si | Si | Si | Si |
| SMTP | Si | Si | Si | Si | Si |
| POP3 | Si | Si | Si | Si | Si |
| IMAP | Si | Si | No | Si | Si |
| SMTP - TLS | Si | Si | No | Si | Si |
| POP - TLS | Si | No | No | No | Si |
| IPv6 | Si | Si | ? | Si | Si |
| SSL | Si | Si | No | Si | Si |
| LDAP | | Si | | Si | Si |
| Licencia | Dual license (GPL) | Open source/IBM Public License | Public domain | Open source/Sendmail License | Open Source/Proprietary |

#### *3.4.6.4.2. Selección de alternativa*

Se ha escogido Postfix como agente de transporte de correo debido a su estructura modular, su seguridad implementada, su soporte para LDAP (*Lightweigh Directory*

*Access Protocol*), Base de datos (MySQL) y autenticación mediante SASL, además por su facilidad de administración, configuración y su abundante documentación

#### 3.4.6.5. Servidor de Directorio

El servicio de directorio es una base de datos optimizada para búsquedas y permite almacenar información organizada acerca de la red. Permite centralizar la información para ser administrada.

LDAP es el protocolo estándar del servicio de directorio designado por la IETF como la mejor opción de los directorios X.500, tiene su base en el protocolo DAP (*Directory Access Protocol).* LDAP es un protocolo simple para la actualización y búsqueda dentro de un directorio sobre TCP/IP.

El servicio de directorio actuará como servidor de autenticación y proporcionará información a los distintos servicios que permitan el control de acceso a los mismos, convirtiéndose en una parte vital del sistema al proporcionar el acceso a usuarios, recursos y otros objetos dentro de un sistema operativo independiente de la plataforma eliminando la redundancia de datos y automatizando su funcionamiento

##### *3.4.6.5.1. Alternativas de Software*

Entre las alternativas para la implementación del servicio de directorio a través de software libre se contemplaron las siguientes opciones:

**389 Directory Server** es un servidor basado en LDAP (*Lightweight Directory Access Protocol*) que trabaja bajo la plataforma Fedora, cuenta con una amplia documentación, gran cantidad de desarrolladores, permite administrar grupos y usuarios, administración gráfica y mediante consola, administración remota vía http, es totalmente de código abierto, se destaca por su capacidad de replicación Multimaster (MMR) que es la opción de escribir en dos o más maestros al mismo tiempo, compatibilidad y sincronización con MS Active Directory, Soporte SNMP, Integridad Referencial, Grupos estáticos y

dinámicos, Clases de Servicios. Fedora Directory Server y Samba, junto con DHCP y DNS proveen de un controlador de dominio a clientes Windows.

**OpenLDAP-Samba** es una implementación libre del protocolo LDAP que se basa en el estándar ISO X500 y que permite conectarse a cualquier otro sistema LDAP dado que soporta múltiples esquemas, trabaja bajo diferentes plataformas GNU/Linux y BSD. OpenLDAP permite organizar de manera jerárquica todo tipo de cuentas, grupos, puntos de montaje, cuentas de equipo, etc. OpenLDAP trabaja en conjunto con TLS, SASL, Kerberos, cuenta con soporte para LDAPv3.

La Tabla 3-24 muestra un resumen de las características de los servidores antes mencionados.

**Tabla 3-24 Comparación: Servidor de Directorio**

| **Características** | **Servidor** | |
|---|---|---|
| | **389 Directory Server** | **OpenLDAP** |
| Replicación | Replicación Multimaster | N-Way Multimaster Replication |
| Compatibilidad con MS Active Directory | Compatible | Compatible |
| Soporta SNMP | si | si |
| Integridad referencial | si | si |
| Grupos estáticos y dinámicos | si | si |
| Soporte LDAPv3 | si | si |
| Plataforma | Independiente de la plataforma | Independiente de la plataforma |
| Seguridad | SSLv3 | SSLv3 |
| | TLSv1 | TLSv1 |
| | SASL | SASL |

#### *3.4.6.5.2. Selección de alternativa*

De las alternativas presentadas se recomienda la configuración del servicio de directorio a través de *OpenLDAP-Samba* ya que ha demostrado ser un servidor con mejores prestaciones en cuanto a velocidad de respuesta siendo un servidor de código

abierto con mayor influencia en el mercado sobre el cual se encuentran desarrollando nuevas alternativas de servicio de directorio.

#### 3.4.6.6. Servicio Web

La página web de toda institución es la carta de presentación que da la cara al usuario. La página web del PPA se encuentra administrada por el departamento de informática del MIES por lo que deberá ser migrado a la infraestructura de comunicaciones del PPA.

La página web del PPA se encuentra formada por contenido informativo estático, el cual deberá pasará a ser dinámico cuando cuente con la aplicación web del sistema de administración SICOPPA donde se realizarán consultas a la base de datos.

En la página web se encuentra información acerca de la estructura organizacional del PPA, se publican metas, objetivos, presupuesto, auditorías, contratos, rendiciones de cuentas y demás información que debe cumplir con la Ley de Transparencia del Gobierno. Además se publican especificaciones técnicas de los productos que se van a adquirir por medio del INCOP, requisitos para ser proveedores, procesos de compra de alimentos y ferias inclusivas.

##### *3.4.6.6.1. Alternativas de software*

Entre las alternativas de software que se tienen para la implementación del servicio Web son las siguientes:

**Servidor HTTP Apache** es un servidor web desarrollado por *Apache Software Foundation* de código abierto compatible con plataformas Unix, Microsoft, Macintosh, está diseñado por módulos para las comunicaciones seguras vía TLS, autenticación de usuarios contra un servidor LDAP, control de tráfico y limitador de ancho de banda, páginas dinámicas.

**Servidor Apache Tomcat** es un servidor web desarrollado por *Apache Software Fundation* de código abierto, soporta Java Servlets y Java Server Pages

**Servidor HTTP Cherokee** es un servidor web de código abierto con licencia GPL, multiplataforma, escrito en C, soporta CGI, FastCGI, SSL/TLS, balanceo de carga, métodos de autenticación y dispone de un panel de administración web.

**Nginx** es un servidor web/proxy de código abierto bajo una variante de la licencia BSD, es multiplataforma. Entre las características se encuentran: soporte de http sobre SSL, balanceo de carga, tolerancia a fallos, soporte FastCGI[38].

La Tabla 3-25 muestra un resumen de las características de los servidores antes mencionados.

**Tabla 3-25 Comparación: Servidor Web**

| Características | Server | | | |
|---|---|---|---|---|
| | Apache HTTP Server | Apache Tomcat | Cherokee HTTP Server | Nginx |
| Autenticación de acceso básico | Si | Si | Si | Si |
| Autenticación de acceso dirigido | Si | Si | Si | No |
| HTTPS | Si | Si | Si | Si |
| Virtual hosting | Si | Si | Si | Si |
| CGI | Si | Si | Si | Si |
| FastCGI | Si | No | No | Si |
| Java Servlets | Implementa AJP | Si | Si | No |
| SSI | Si | Si | Si | Si |
| ASP.NET | Si | No | No | No |
| Consola de administración | Si | Si | Si | No |
| IPv6 | Si | ? | ? | Si |

#### *3.4.6.6.2. Selección de alternativa*

De las alternativas presentadas se recomienda la configuración del servidor web a través de Apache HTTP ya que cuenta con las características necesarios para la implementación de un sitio web seguro y dinámico, los cuales son requisitos indispensables para el PPA, además que cuenta con una amplia documentación y

[38] FastCGI es un protocolo para interconectar programas interactivos con un servidor web reduciendo la carga asociada al interconectar el servidor web y los programas CGI.

soporte dado por su entidad desarrolladora siendo el software para servicio web que se encuentra más difundido.

#### 3.4.6.7. Servicio FTP

El servicio FTP es uno de los más fundamentales en el PPA, ya que en la actualidad los archivos son gestionados a través de carpetas compartidas en cada una de las computadoras de los usuarios.

El servicio de FTP permitirá organizar los documentos compartidos de acuerdo al departamento que lo utiliza, permitiendo la implementación de un control de acceso mediante usuarios y passwords

##### *3.4.6.7.1. Alternativa de software*

Las alternativas de software para la implementación del servicio de FTP son las siguientes:

**ProFTPd** es un servidor FTP para plataformas Linux, está licenciado bajo GPL, puede ser configurado como múltiples servidor FTP virtuales, es capaz de trabajar sobre IPv6, esta diseñado de forma modular, cuenta con cifrado SSL/TLS, RADIUS, LDAP o SQL, permite tener múltiples servidores brindando servicio de ftp anónimo. Es de fácil configuración, se ejecuta como un usuario sin privilegios para disminuir la posibilidad de ataques.

**Pure-FTPd** es un servidor FTP bajo licencia BSD, es multiplataforma SSL/TLS usando la librería OpenSSL, permite la autenticación de usuarios a través de un servidor LDAP y ha sido probado de forma exitosa con OpenLDAP, permite limitar el ancho de banda distinguiendo cargas y descargas de información.

**vsFTPd (*Very Secure FTP Daemon*)** es un servidor FTP orientado a sistemas Unix bajo licencia GPL (*GNU General Public License*). Soporta IPv6, encripción a través de SSL, el servidor por defecto en varias distribuciones Linux

La Tabla 3-26 muestra un resumen de las características de los servidores antes mencionados.

**Tabla 3-26 Comparación: Servidor FTP**

| **Características** | **Servidores** | | |
|---|---|---|---|
| | **ProFTPd** | **Pure-FTPd** | **vsftpd** |
| Plataforma | Linux, Mac OS X, Windows | Linux, Solaris, HPUX, Mac OS X y FreeBSD, | Linux/Unix |
| Seguridad | Autenticación LDAP, TLS/SSL , SQL o LDAP | Encripción TLS , Autenticación flexible, MySQL, PgSQL, LDAP. | Configuración flexible vía PAM, Encripción SSL |
| Licencia | GPL | BSD | GPL |
| Servidores FTP Virtuales | si | si | si |
| Soporta IPv6 | si | si | si |

#### *3.4.6.7.2. Selección de alternativa*

De las alternativas presentadas se recomienda la configuración del servidor FTP a través de *ProFTPd* ya que cuenta con las características necesarias de seguridad, permite la autenticación de los usuarios a través de un servidor LDAP y es el servidor FTP con el que trabaja por defecto el servidor http Apache, el cual se recomendó como solución para el PPA. Cuenta con una basta información y soporte por parte de su organización desarrolladora siendo uno de los servidores FTP más difundidos.

### 3.4.7. REQUERIMIENTOS DE HARDWARE DEL SERVIDOR

Una vez determinados los servicios requeridos por el PPA se deberá considerar los recursos suficientes para determinar los niveles de servicio adecuado. El hardware sobre el cual se implementarán los servicios deberá cumplir requerimientos de disponibilidad, capacidad de almacenamiento, capacidad de procesamiento y tamaño de memoria.

**Capacidad de Almacenamiento y Memoria**

El servicio de correo electrónico trabajará de forma conjunta con el servicio de antivirus y antispam por lo cual se dispondrá de un espacio en disco duro de 1GB por usuario y considerando el crecimiento de usuarios a 50, se tiene que se requieren como mínimo un espacio en disco duro de 50GB. La capacidad de memoria depende del número de transacciones realizadas en el servidor, siendo el servicio de correo electrónico uno de los más utilizados por el PPA se requiere de mínimo 512 MB de memoria RAM.

Para el servicio de base de datos donde se almacenarán lo concerniente al Sistema de Administración de Compras (SICOPPA) y Gestión Documental para lo cual se ha consultado con los desarrolladores del sistema, los cuales estiman se requiera un espacio en disco duro de 500GB y 1GB de memoria RAM.

Para el servicio de archivos se tomará en cuenta el peso de los archivos que se encuentran en el directorio compartido, los cuales tienen un peso total de alrededor de 10GB cuyos archivos han sido almacenados por alrededor de 1 año. Teniendo estos datos como antecedentes se estimará una almacenamiento dentro de 5 años para lo cual se requerirá un espacio en disco duro de 50GB. Para el servicio FTP se utilizará el software *proFTPd* cuyo requerimiento de memoria mínimo es de 256MB[39].

Para el servicio web no es necesario el uso de muchos recursos en cuanto a hardware debido a que la página web es meramente informativa, la cual irá cambiando de acuerdo al desarrollo del sistema de administración SICOPPA. Para el servicio web se requerirá un espacio en disco duro de 10GB y una memoria RAM de 128MB

Los servicios de DNS y DHCP no hacen uso de muchos recursos de hardware. El servicio de DNS únicamente contesta peticiones de nombres de dominio o direcciones IP y el servicio de DHCP entrega direcciones IP a los diferentes equipos de

[39] Dato obtenido de: http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-ftp

conectividad cuando éstos se conectan por primera vez a la red, por lo cual se requerirá un espacio en disco duro de no más de 20GB y memoria RAM de 256MB[40].

Para el servicio de directorio es necesario dimensionar de forma similar a una base de datos, dado que se almacenarán los datos de los usuarios de red, contraseñas, y datos de servicios que usarán información del directorio para el control de acceso. El servicio de directorio depende directamente del número de usuarios de red, para este caso se dimensionará para el uso de alrededor de 100 usuarios por lo que se reservará un espacio en disco duro de 20GB y una memoria RAM de 256MB[41].

La Tabla 3-27 muestra los requerimientos del sistema en almacenamiento y memoria RAM.

**Tabla 3-27 Servidor de Comunicaciones: Capacidad de almacenamiento y memoria**

| CAPACIDAD DE ALMACENAMIENTO Y MEMORIA | | |
|---|---|---|
| **Servidor** | **Almacenamiento [GB]** | **Memoria [MB]** |
| Correo Electrónico | 50 | 512 |
| Base de Datos | 500 | 1000 |
| FTP | 50 | 256 |
| Web | 10 | 512 |
| DNS y DHCP | 20 | 256 |
| Directorio | 20 | 512 |
| Total | 650 | 3048 |

### 3.4.7.1. Especificaciones técnicas del servidor de comunicaciones

La Tabla 3-28 detalla las especificaciones técnicas del servidor de comunicaciones.

[40] Dato obtenido de: http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-dhcp
[41] Dato obtenido de: http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-ldap

**Tabla 3-28 Requerimientos técnicos: Servidor de Comunicaciones**

| DESCRIPCIÓN | |
|---|---|
| Tipo | Para montaje en rack 19” |
| Factor de forma | 1U |
| Capacidad de almacenamiento | 2 Disco SAS de 500GB (cada uno) con capacidad de expansión a 4 discos duros internos |
| Tipo de memoria interna | DDR3 1066Mhz |
| Memoria caché interna | 12 MB Smart Cache |
| Velocidad de reloj | 2400 MHz |
| Tipo de núcleo | múltiple (4 Cores) |
| Velocidad de rotación del disco duro | 7.200 rpm |
| Controlador de almacenamiento | SAS RAID (RAID 0/1/1+0) |
| Ranuras de memoria= | 8 ranuras DIMM |
| Memoria interna (instalada) | 8 GB |
| Interfaces de red | Cantidad= 2 |
| | De 1Gbps c/u |
| | Instalación Plug-and-Play |
| | Estándares: |
| | IEEE 802.3 10Base-T Ethernet |
| | IEEE 802.3u 100Base-TX Fast Ethernet |
| | IEEE 802.3ab 1000Base-T Gigabit Ethernet. |
| | IEEE 802.3x Flow Control. |
| | ANSI/IEEE 802.3 Nway Auto-Negotiation. |
| | IEEE 802.1p Priority Tagging. |
| | IEEE 802.1q VLANs |
| Puertos de entrada y salida (E/S): | Serie= 1; Dispositivo de puntero= 1; Teclado= 1; Gráficos= 1 (posterior); Red RJ-45= 2; USB 2.0= 7 (2 frontales, 1 interno, 4 posteriores) |
| Unidades adicionales | DVD Writer |
| Fuentes de poder | Debe soportar 2 fuentes de poder redundantes conectables en caliente de alta capacidad |
| Arquitectura procesador | 64 bits |

#### 3.4.7.2. Alternativas del Servidor de Comunicaciones

Para la selección del servidor de comunicaciones se ha elegido tres marcas reconocidas en el mercado (HP, IBM, FUJITSU), las cuales presentan una gran gama de servidores de acuerdo a requisitos de procesamiento, memoria. Los equipos que se han presentado de las diferentes marcas son orientados a pequeñas y medianas empresas, debido a que se acoplan a la realidad del PPA.

Los tres servidores comparados superan las características requeridas para la implementación de los servicios requeridos por el PPA sin llegar a estar sobredimensionados, ya que se ha tomado en cuenta el crecimiento en usuarios, servicios y aplicaciones que tendrá el PPA en los próximos 5 años.

Por requerimientos de GTI-PPA se ha elegido servidores de tipo rack que proporciones espacio adicional para el crecimiento, ya que este tipo de servidores se encontrarán montados en el rack de comunicaciones los cual deberán contar con un KVM[42] (*Keyboard-Video-Mouse*) cuando el número de servidores crezca.

De la comparación realizada en el Anexo 3.6 de los servidores se ha observado que tanto el servidor IBM y HP son los que presentan mejores características en cuanto a rendimiento, cumplen con todas las características técnicas requeridas. Se ha decidido el uso del servidor HP por su experiencia probada con el trabajo con sistemas operativos GNU/Linux.

El equipo recomendado es:

- El servidor de comunicaciones recomendado es el HP ProLiant DL320.

### 3.4.8. SEGURIDAD DE LA INFORMACIÓN

En la actualidad son muchos los factores a tener en cuenta en lo relativo a la seguridad de la información, los planes de contingencia y continuidad del negocio son de gran

[42] Dispositivo de conmutación que permite controlar servidores y demás equipos informáticos con un solo monitor, teclado y mouse.

relevancia en cualquier proyecto TIC (Tecnologías de la Información y de la Comunicación). La pérdida de información, los ataques externos y las interrupciones esporádicas de los sistemas y servicios pueden causar importantes daños en el desarrollo corporativo ocasionando importantes pérdidas económicas.

La información manejada por toda institución del Estado es considerada como el activo más valioso, sin el cual no es posible la evaluación, seguimiento y toma de decisiones a nivel corporativo, razón por la cual se debe garantizar su integridad, confidencialidad y disponibilidad. El PPA deberá tener normativas que especifiquen el buen uso de los recursos y contenidos.

Garantizar la seguridad de la información conlleva a formular políticas del uso de la información a nivel de software, hardware, datos, documentación, usuarios y administración que mantengan la información libre de riesgo. Las políticas deberán ser planteadas por el departamento de GTI-PPA y aprobadas por el Director Nacional del PPA en conjunto con Recursos Humanos y deberán ir en concordancia con los objetivos del Programa ya que el gasto de controles debe equilibrarse con el daño comercial resultado de fallas en la seguridad.

La seguridad de la información del PPA será gestionada tomando en cuenta las recomendaciones de la norma ISO 27002:2005. En primera instancia se evaluará la información y sistemas que deberán ser protegidos, así como su nivel de seguridad. Luego se evaluará los posibles ataques a los que se encontrará expuesta dicha información para evitar dichas vulnerabilidades y riesgos para finalmente plantear políticas de seguridad y de administración de la red.

Actualmente la información se encuentra gestionada con las mínimas medidas de seguridad, pero de forma ordenada. La información tanto física como digital de cada uno de los procesos de compra pasan por los diferentes departamentos para ser tramita, siendo cada departamento el responsable de su seguridad cuando ésta llega a sus manos.

#### 3.4.8.1. Identificación de activos informáticos

Para garantizar la seguridad de la información es necesario diferenciar claramente los tipos de recursos informáticos con los que cuenta el PPA.

Los activos de información del PPA son:

Físicos

- Computadores personales y portátiles
- Servidores
- Equipos de conectividad (Switch, Router, Access Point, Firewall)

Lógicos

- Base de datos
- Software de aplicación
- Sistema Operativo
- Software contable
- Herramientas de desarrollo y utilidades

Información

- Archivos de data
- Contratos y acuerdos
- Documentación del sistema
- Manuales de usuario
- Planes de continuidad del negocio
- Acuerdos para contingencia

Servicios

- Página Web
- Directorio
- Transferencia de archivos
- Sistema de Administración SICOPPA

- Servicio de Internet
- Servicio de correo electrónico
- Servicios Intranet
- Sistema de Cableado Estructurado
- Servicio de Videoconferencia
- Servicio de Telefonía IP
- Servicios generales; iluminación, energía eléctrica, control de accesos, detección de incendios.

#### 3.4.8.2. Análisis de riesgo

El análisis de riesgo es el fundamento sobre el cual se basará las políticas de seguridad. El nivel de riesgo de los recursos se establecerá a través del impacto que tenga la información en caso de fallas de seguridad y de la probabilidad de ocurrencia.

En primer lugar se establecerá el nivel de criticidad de los activos informáticos según parámetros de confidencialidad, integridad y disponibilidad esperados cuando la seguridad de la información falle.

Los niveles de confidencialidad, integridad y disponibilidad deberán ser valoradas en conjunto con GTI-PPA. La Tabla 3-29 detalla los niveles de impacto en la continuidad de las operaciones del PPA de acuerdo a confidencialidad, integridad y disponibilidad.

**Tabla 3-29 Niveles de Confidencialidad, Integridad y Disponibilidad**

| Característica | Valor | Clase | Descripción |
|---|---|---|---|
| **Confidencialidad** | 1 | Público | Información que no representa riesgo para el PPA. |
| | 2 | Interno | Información utilizada en actividades laborales que representan riesgos mínimos al PPA. |
| | 3 | Confidencial | Información a cuyo acceso se debe tener autorización del responsable |
| | 4 | Estrictamente confidencial | Información que representa riesgos importantes para el PPA |
| **Integridad** | 1 | Bajo | EL PPA no se ve afectado con la pérdida de integridad |
| | 2 | Promedio | El PPA soporta hasta 2 semanas en restablecer la integridad |

Continúa

| | | | |
|---|---|---|---|
| | 3 | Importante | El PPA soporta hasta 1 semana en restablecer la integridad |
| | 4 | Vital | El PPA soporta hasta 2 días en restablecer la integridad |
| | 5 | Crítico | El PPA soporta hasta 3 horas en restablecer la integridad. |
| **Disponibilidad** | 1 | Bajo | El PPA no se ve afectado con la pérdida del activo informático |
| | 2 | Promedio | El PPA hasta 1 semanas sin el activo informático |
| | 3 | Importante | El PPA soporta hasta 2 días sin el activo informático |
| | 4 | Vital | El PPA soporta hasta 48 horas sin el activo informático |
| | 5 | Crítico | El negocio no funciona sin el activo informático |

Con los datos de la Tabla 3-29 se procede a valorar los niveles de disponibilidad, integridad y confidencialidad que tendrá cada uno de los activos informáticos en las peores condiciones, es decir, la factibilidad de que dichos activos fallen sin afectar la continuidad de operaciones del PPA.

En la Tabla 3-30 se muestra el factor de criticidad (FC) de cada uno de los activos informáticos y el promedio según su división.

**Tabla 3-30 Criticidad de Activos Informáticos**

| ACTIVOS INFORMÁTICOS | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo** | **Detalles** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Factor de Criticidad (FC)** | **Factor de Criticidad Promedio** |
| Físicos | Computadores personales y portátiles | 2 | 4 | 4 | 10 | 11 |
| | Servidores | 3 | 5 | 4 | 12 | |
| | Equipos de conectividad (Switch, Router, Access Point, Firewall) | 3 | 5 | 4 | 12 | |
| Lógicos | Base de datos | 4 | 5 | 5 | 14 | 12 |
| | Software de aplicación | 4 | 5 | 4 | 13 | |
| | Sistema Operativo | 3 | 5 | 4 | 12 | |
| | Software contable | 4 | 4 | 3 | 11 | |
| | Herramientas de desarrollo y utilidades | 3 | 4 | 2 | 9 | |

Continúa

| | | | | | | |
|---|---|---|---|---|---|---|
| Información | Archivos de data | 4 | 5 | 3 | 12 | 8 |
| | Contratos y acuerdos | 3 | 3 | 3 | 9 | |
| | Documentación del sistema | 3 | 3 | 2 | 8 | |
| | Manuales de usuario | 3 | 2 | 2 | 7 | |
| | Planes de continuidad del negocio | 3 | 2 | 2 | 7 | |
| | Acuerdos para contingencia | 3 | 2 | 2 | 7 | |
| Servicios | Página Web | 3 | 4 | 4 | 11 | 12 |
| | Directorio | 4 | 3 | 4 | 11 | |
| | Transferencia de archivos | 3 | 4 | 4 | 11 | |
| | Sistema de Administración SICOPPA | 4 | 5 | 4 | 13 | |
| | Servicio de Internet | 3 | 5 | 4 | 12 | |
| | Servicio de correo electrónico | 4 | 5 | 4 | 13 | |
| | Servicios Intranet | 3 | 5 | 4 | 12 | |
| | Sistema de Cableado Estructurado | 3 | 4 | 4 | 11 | |
| | Servicio de Videoconferencia | 4 | 4 | 4 | 12 | |
| | Servicio de Telefonía IP | 4 | 5 | 4 | 13 | |
| | Servicios generales; iluminación, energía eléctrica, control de accesos, detección de incendios. | 3 | 5 | 4 | 12 | |

Con los resultados obtenidos hasta le momento ya se tiene un indicio de los activos informáticos más críticos que necesitan mayores márgenes de seguridad y monitoreo.

Seguidamente se realiza la identificación de las amenazas para cada activo informático. Las amenazas pueden ser del tipo ambiental, humano y tecnológico, ésta clasificación

permitirá analizar, tomar medidas de seguridad e implementar controles para tratar las amenazas en conjunto.

Las amenazas ambientales dependerán de las condiciones físicas, geográficas, climatológicas y estructurales del lugar donde se encuentra el PPA. Las amenazas tecnológicas dependerán del hardware sobre el cual se almacene y procese el activo informático. Las amenazas humanas serán aquellas realizadas con conocimiento de causa o involuntarias, desde dentro y fuera del PPA y del nivel de conocimiento técnico de la persona involucrada.

Las amenazas y vulnerabilidades se detallan en la Tabla 3-31, en la cual se le asigna un código que ayude a asignar dichas amenazas a los diferentes activos informáticos.

**Tabla 3-31Amenazas y Vulnerabilidades**

| AMENAZAS Y VULNERABILIDADES | | | |
|---|---|---|---|
| | **Código** | **Amenaza** | **Vulnerabilidad** |
| Ambientales | 1 | Fuego | Falta de un sistema de detección de incendios |
| | 2 | Inundaciones | Falta de drenaje del edificio |
| | 3 | Desastres naturales | Ubicado en zona de rayos, y zona sísmica (Ecuador). |
| Humanas | 4 | Uso no autorizado de recursos | Falta de un sistema de control |
| | 5 | Errores fallas u omisión de controles | Falta de capacitación y concentración de usuarios |
| | 6 | Manejo inapropiado de datos sensibles | Falta de control y de sanciones |
| | 7 | Uso de contraseñas débiles | Falta de concientización del manejo de seguridad |
| | 8 | Acceso físico no autorizado | Falta de control y de sanciones |
| | 9 | Introducción de software malicioso, virus, etc. | Falta de servicio de antivirus, IDS, IPS |
| | 10 | Destrucción no autorizada de datos | Falta de control, sanciones y monitoreo de actividades |
| | 11 | Robo o acceso no autorizado de datos | Falta de sanciones severas |
| | 12 | Transferencia no autorizada de datos | Falta de sanciones severas |
| Técnicas | 13 | Cortes o alteración del suministro eléctrico/UPS | Falta de equipos de protección |
| | 14 | Fallas en el sistema de incendios y | Falta de mantenimiento |

Continúa

| | | | |
|---|---|---|---|
| | | acceso físico | |
| | 15 | Fallas en el hardware | Falta de mantenimiento y revisiones preventivas |
| | 16 | Fallas en el sistema base | Falta de mantenimiento y revisiones preventivas |
| | 17 | Fallas en las aplicaciones | Falta de mantenimiento y revisiones preventivas |
| | 18 | Fallas en la red interna | Falta de mantenimiento y revisiones preventivas |
| | 19 | Vulnerabilidades de software | Falta de actualizaciones del software y monitoreo de la red |
| | 20 | Ataque de denegación de servicio interno | Falta de monitoreo de la red |

Los niveles de amenaza estarán dados por la probabilidad de ocurrencia esperada de cada uno de los incidentes de la tabla anterior. Los niveles de vulnerabilidad estarán dados por el nivel de seguridad de la información con el que se espera contar frente a cada una de las amenazas mencionadas. La Tabla 3-32 muestra los niveles de amenazas y vulnerabilidad según GTI-PPA, en la cual se le asigna un valor de amenaza (VA) y un valor de vulnerabilidad (VV).

**Tabla 3-32 Niveles de Amenazas y Vulnerabilidades**

| | **Valor Amenaza (VA) y Valor Vulnerabilidad (VV)** | **Clase** | **Descripción** |
|---|---|---|---|
| **Amenazas** | 1 | Bajo | Se espera que ocurra una vez al año |
| | 2 | Medio | Se espera que ocurra 2 veces al año |
| | 3 | Alto | Se espera que ocurra cada mes. |
| **Vulnerabilidades** | 1 | Bajo | Controles débiles de la información |
| | 2 | Medio | Controles moderados de la información |
| | 3 | Alto | Controles adecuado de la información |

Finalmente teniendo los niveles de criticidad y las amenazas procede a analizar el riesgo de cada los activos informáticos.

**Tabla 3-33 Evaluación de Riesgos**

| EVALUACIÓN DE RIESGOS | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Grupo** | **Detalles** | **(FC)** | **Amenaza** | | | **FCx VAx VV** | **Riesgo promedio total** |
| | | | **Tipo** | **(VA)** | **(VV)** | | |
| Físicos | Computadores personales y portátiles<br>Servidores<br>Equipos de conectividad (Switch, Router, Access Point) | 11 | 1 | 1 | 2 | 22 | 40 |
| | | | 2 | 1 | 2 | 22 | |
| | | | 3 | 1 | 2 | 22 | |
| | | | 4 | 2 | 3 | 66 | |
| | | | 7 | 1 | 3 | 33 | |
| | | | 8 | 2 | 3 | 66 | |
| | | | 13 | 2 | 3 | 66 | |
| | | | 15 | 1 | 2 | 22 | |
| Lógicos | Base de datos<br>Software de aplicación<br>Sistema Operativo<br>Software contable<br>Herramientas de desarrollo y utilidades | 12 | 1 | 1 | 2 | 24 | 65 |
| | | | 2 | 1 | 2 | 24 | |
| | | | 3 | 1 | 2 | 24 | |
| | | | 4 | 2 | 3 | 72 | |
| | | | 5 | 3 | 3 | 108 | |
| | | | 6 | 1 | 2 | 24 | |
| | | | 7 | 3 | 2 | 72 | |
| | | | 8 | 3 | 3 | 108 | |
| | | | 9 | 3 | 3 | 108 | |
| | | | 10 | 2 | 2 | 48 | |
| | | | 12 | 2 | 3 | 72 | |
| | | | 16 | 2 | 3 | 72 | |
| | | | 17 | 2 | 3 | 72 | |
| | | | 19 | 2 | 3 | 72 | |
| | | | 20 | 2 | 3 | 72 | |
| Información | Archivos de data<br>Contratos y acuerdos<br>Documentación del sistema<br>Manuales de usuario<br>Planes de continuidad del negocio<br>Acuerdos para contingencia | 8 | 1 | 1 | 2 | 16 | 20 |
| | | | 2 | 1 | 2 | 16 | |
| | | | 3 | 1 | 2 | 16 | |
| | | | 4 | 1 | 2 | 16 | |
| | | | 6 | 1 | 2 | 16 | |
| | | | 8 | 1 | 2 | 16 | |
| | | | 10 | 2 | 2 | 32 | |
| | | | 11 | 2 | 2 | 32 | |
| Servicios | Página Web | 12 | 1 | 1 | 2 | 24 | 55 |
| | | | 2 | 1 | 2 | 24 | |

Continúa

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Directorio | | 3 | 1 | 2 | 24 | |
| | Transferencia de archivos | | 4 | 3 | 2 | 72 | |
| | Sistema de Administración SICOPPA | | 5 | 2 | 3 | 72 | |
| | Servicio de Internet | | 6 | 2 | 2 | 48 | |
| | Servicio de correo electrónico | | 7 | 3 | 2 | 72 | |
| | Servicios Intranet | | 8 | 3 | 2 | 72 | |
| | Sistema de Cableado Estructurado | | 9 | 3 | 2 | 72 | |
| | Servicio de Videoconferencia | | 10 | 2 | 3 | 72 | |
| | Servicio de Telefonía IP | | 11 | 1 | 3 | 36 | |
| | Servicios generales; iluminación, energía eléctrica, control de accesos, detección de incendios. | | 12 | 2 | 2 | 48 | |
| | | | 13 | 2 | 3 | 72 | |
| | | | 15 | 2 | 2 | 48 | |
| | | | 16 | 2 | 2 | 48 | |
| | | | 17 | 2 | 3 | 72 | |
| | | | 18 | 2 | 3 | 72 | |
| | | | 19 | 2 | 2 | 48 | |
| | | | 20 | 2 | 2 | 48 | |

El análisis de riesgo realizado muestra los activos lógicos y servicios que mayor riesgo tienen y sobre los cuales se deberá enfocar las políticas y normas de seguridad de la información. También se puede observar a través del factor de criticidad de la Tabla 3.30 que los activos lógicos y servicios que deberán garantizar niveles óptimos de confidencialidad, integridad y disponibilidad para la continuidad de las operaciones del PPA son:

- Base de Datos
- Software de Aplicación
- Correo electrónico
- Telefonía IP
- Servicio de Internet

La falta de garantías de funcionamiento de dichos datos, aplicaciones y servicios afectaría de forma significativa a los proveedores, programas sociales y demás entidades que dependen de la compra de alimentos, la continuidad de las operaciones

del PPA se verían sumamente mermados pudiendo traer consigo sanciones y la pérdida sustancial de la imagen del PPA.

#### 3.4.8.3. Políticas de Seguridad de la Información

Una vez definido los activos informáticos que necesitan ser protegidos, y las amenazas a las que se encontrarán expuestas dependiendo de las vulnerabilidades permitidas se procede a formular recomendaciones que permita eliminar, reducir, aceptar o trasladar el riesgo de la información.

##### *3.4.8.3.1. Servicios de correo electrónico e internet*

GTI-PPA deberá controlar el buen uso del servicio de Internet, aplicaciones web y correo electrónico institucional para evitar filtrado de información, por lo cual se deberá establecer políticas para su buen uso. Las medidas a tomar para el resguardo de la información son:

- Bloquear el acceso a servicio de email, redes sociales, llamadas, videoconferencia y chat públicos a todos los funcionarios. Se abrirá con excepción.
- Desinstalar programas de chat y videollamadas en computadoras no autorizadas.
- Bloquear la descarga de archivos ejecutables, audio y video que no pertenezcan a cuentas de correo institucionales.
- Prohibir y bloquear el envío/recepción de correos y adjuntos de cuentas institucionales de dominios públicos (ej. *Hotmail, Yahoo, Gmail*, etc).
- Restringir el tamaño máximo de envío y recepción de email a 2Mb por correo.
- Restringir el acceso y uso de programas FTP, TELNET, SSH desde las computadoras personales a usuarios finales.
- Prohibir y bloquear el envío de adjuntos por medio de programas chat (mensajería instantánea) en caso que se habilite el servicio.

- Prohibir y bloquear el respaldo de información gubernamental en servicios web públicos de archivado de información.
- Activar el filtrado de contenidos y sitios web para navegación en Internet.
- Formalizar la autorización (por parte de jefes inmediatos) para monitoreo de uso de servicios a funcionarios autorizados.
- Mantener listados actualizados de los funcionarios autorizados a usar servicios restringidos.

#### *3.4.8.3.2. Servicio de red de datos y comunicaciones*

Se deberá fortalecer la seguridad en la red de datos que eviten accesos no autorizados a cada uno de los servicios a nivel físico y lógico para lo cual se recomienda implementar políticas de acuerdo a los siguientes ítems.

- Creación de grupos de acuerdo departamentos y áreas, de tal forma que el acceso de forma lógica y física a departamentos a los que no pertenece un usuario se encuentre restringido. La creación de grupos se lo tomó en cuenta en el diseño de la red lógica en los que respecta a creación de VLANs y direccionamiento IP.
- Habilitar seguridades de acceso a redes inalámbricas. Lo cual fue tomado en cuenta en el diseño de la red inalámbrica.
- Habilitar acceso a red cableada e inalámbrica mediante el registro de direcciones MAC o protocolo 802.1X.
- Coordinar la ejecución de pruebas de vulnerabilidad o "*hacking*[43]" ético a la infraestructura de comunicaciones.

#### *3.4.8.3.3. Gestión de Información digital a nivel lógico*

Se deberán establecer mecanismos que eviten y detecten la introducción de códigos maliciosos, además se deberá evitar la fuga de información por medio de dispositivos

[43] Acceso no autorizado a sistemas mediante la violación de la seguridad.

externos no autorizados. Se recomienda la implementación de políticas de acuerdo a los siguientes ítems.

- Se deberá firmar un acta de responsabilidad respecto del uso, custodia y confidencialidad de información, servicios, sistemas y equipos a la que tendrá a acceso mientras trabaje en el PPA.
- Controlar el uso de redes internas y externas para transferencia de información sin autorización (RFID, *Bluetooth*, etc).
- Desinstalar programas de quemado de DVD, CDs, puertos inalámbricos y desactivar los dispositivos para evitar la fuga de información.
- Elaborar y difundir un documento de consejos para la creación de contraseñas seguras.
- Habilitar la caducidad de contraseñas cada cierto tiempo a nivel de base de datos, aplicaciones, dominios de red, correo electrónico, computadores personales y demás servicios a los cuales se realice control de acceso.
- Todos los activos (información, software, hardware, etc.) deberán tener asignada a un responsable del PPA.
- Copia de seguridad o respaldos
- Prohibición del uso de software no autorizado
- Instalación y actualización regular de software para la detección o reparación de códigos maliciosos en computadores, servidores, servicios y demás equipos de telecomunicaciones.

#### *3.4.8.3.4. Gestión de acceso a información digital a nivel físico*

Se deberá controlar el acceso de personas no autorizadas a equipos e instalaciones computacionales para lo cual se recomienda el establecimiento de políticas de acuerdo a los siguientes ítems.

- Implementar sistemas de seguridad física como sistemas CCTV (Circuito Cerrado de Televisión), Sistema de control de accesos, Sistema de detección de incendios.

- Habilitar clave de acceso al BIOS para el encendido de cada uno de los servidores ubicados en el cuarto de telecomunicaciones.
- Restringir uso de puertos infrarrojos y *bluetooth* de computadoras personales y portátiles para transferencia de información.
- Restringir el uso de puertos USB y lectoras de memorias flash.
- Minimizar el transporte de información sensible utilizando memorias flash, celulares, reproductores digitales, discos duros externos, etc.
- Inventariar computadoras de escritorio, portátiles, impresoras, copiadoras y demás dispositivos de red.
- Especialmente los equipos de telecomunicaciones se deberán ubicar y proteger para reducir las amenazas y peligros ambientales y sobre todo del acceso no autorizado, esto fue tratado en el diseño del sistema de cableado estructurado en lo referente a cuarto de telecomunicaciones y cuarto de equipos.
- Los equipos de telecomunicaciones deberán ser protegidos ante fallas e interrupciones de energía eléctrica, lo cual es solucionado a través de un USP que permita el funcionamiento continuo de los equipos. Además se recomienda la adhesión del circuito eléctrico del PPA al generador de energía del edificio.
- Se deberá planificar un mantenimiento de los equipos de forma periódica que asegure su continua disponibilidad e integridad

#### *3.4.8.3.5. Manejo de la seguridad dentro del PPA*

Si bien la seguridad de la información incluye aspectos técnicos, ésta se extiende al ámbito de la organización y contempla aspectos jurídicos, la seguridad de la información deberá ser parte de un nivel gerencial dentro del PPA, el cual deberá trabajar directamente con el Coordinador Nacional en la seguridad de la información.

El responsable de la seguridad de la información estará a cargo de:

- Supervisar la implementación del Programa de Seguridad de la Información dentro del PPA.
- Actualizar las políticas y normas de Seguridad de la Información.

- Coordinar las investigaciones de incidentes suscitados con la información del PPA.
- Deberá estar a cargo de un programa de concientización de los beneficios que se obtienen al implementar los planes de seguridad de la información sabiendo que aquello exige tiempo y esfuerzo.

#### 3.4.8.4. Hardware de Seguridad Perimetral

El hardware de seguridad deberá proporcionar protección al perímetro de la red del PPA, integrando en un mismo dispositivo funcionalidades avanzadas de filtrado y protección.

El equipo de seguridad deberá de ir de la mano con el nivel de riesgo de la información del PPA, lo cual hace que el equipamiento no solo se base en firewall y VPN, sino que deberá ofrecer servicios de:

- VPN SSL
- Antispam
- Antivirus
- Filtrado de contenido web
- IPS
- Servidor DNS
- Servidor Proxy

Debido a la importancia que tiene el servicio de Internet para el desarrollo de las actividades del PPA, es necesaria la inclusión de un mecanismo que permita maximizar el uso y la disponibilidad de las dos conexiones a Internet con las que se constará, permitiendo un balanceo de carga.

La infraestructura de comunicaciones del PPA constará con una DMZ (Zona Desmilitarizada) que agrupará y separará los servidores que serán expuestos a Internet de los servidores de la Intranet evitando de esta forma intrusiones o conexiones remotas no deseadas.

#### 3.4.8.5. Alternativas de equipo de seguridad perimetral

De acuerdo al nivel de seguridad de información necesaria para el PPA y por tratarse de una institución en crecimiento que no dispone de personal dedicado a la seguridad TI ni de una partida presupuestaria asignada a tal efecto se recomienda el uso de un sistema UTM (*Unified Threat Management*) que a más de funcionar como firewall ofrezca funciones de Antivirus, Antispam, Filtrado de contenido web y demás requerimientos en un solo equipo que garantice una gestión unificada de las amenazas.

Para la selección del servidor de comunicaciones se ha elegido tres marcas reconocidas en el mercado (Cisco, Checkpoint, DLink), las cuales presentan una gran gama de servidores de acuerdo a requisitos de procesamiento, memoria. Los equipos que se han presentado de las diferentes marcas son orientados a pequeñas y medianas empresas, debido a que se acoplan a la realidad del PPA.

Uno de los puntos importantes a la hora de escoger un equipo de seguridad UTM se debe tomar muy en cuenta las licencias de los servicios extras, tales como antivirus, antispam, URL *filtering*, los cuales son software soportados por los equipos pero tienen un valor extra por sus licencias, las cuales se las debe ir renovando y se pagan por la cantidad de usuarios.

De los tres equipos comparados el UTM de Checkpoint es el que mejores características de rendimiento presenta, pero los servicios adicionales no vienen con el equipo por los cuales hay que pagar licencias anuales, mientras que el equipo de Cisco, aunque presenta menor rendimiento (suficiente para los requerimientos del PPA) tiene los servicios adicionales integrados. En la decisión también ha pesado el hecho de tener dos puertos WAN con balanceo de carga.

El equipo recomendado es para seguridad perimetral del PPA es:

- El UTM recomendado es el Cisco SA 540.

### 3.4.9. ADMINISTRACIÓN Y MONITOREO DE LA RED

La administración y monitoreo de la red, dependerán en gran parte del correcto diseño de la infraestructura de comunicaciones, de las políticas de gestión de la información ya que esta organización de los las mismas permitirá una mejor evaluación de la red en conjunto.

La administración de la red se basará en el control, supervisión y monitoreo de la red de datos para lo cual es necesario el uso de una herramienta que permita ofrecer dichos servicios de manera confiable, cuyos resultados y estadísticas sean interpretados por el administrador de la red y permita conocer el estado actual y problemas de la red, en base a los cuales se tomará decisiones que eviten fallos y problemas futuros.

El software a utilizar para la administración y monitoreo de la red será basado en Software Libre. El sistema de administración deberá cumplir los siguientes requerimientos:

- Almacenar los datos obtenidos del monitoreo que permitan obtener reportes y tendencias del comportamiento de la red.
- Permita observar y analizar la red y su tráfico a través de una interfaz gráfica.
- Deberá generar reportes sustentados en base al estado de la red, cuya información deberá garantizar ser confiable.
- Permitirá conocer el estado de equipos de conectividad como routers, switches, servidores y firewall. Se deberá obtener información del estado en red, tiempo arriba, puertos abiertos, servicios, procesos corriendo, carga de CPU, carga de memoria física, espacio en disco, interfaces de red activas y otros.
- El sistema de administración deberá hacer uso del protocolo SNMP (*Simple Network Management Protocol*) que permita gestionar los diferentes elementos y componentes de red.

#### 3.4.9.1. Alternativas de Software

En la actualidad existen varias herramientas de Software Libre bajo licencia GPL para el monitoreo de la red entre las cuales se encuentran; *Nagios, Cacti, NetMRTG*, *OpenNMS, Opsview* entre otros.

Entre las alternativas de software mencionadas, las que más se destacan por su desarrollo, su frecuencia en emitir actualizaciones, por el soporte encontrado en el mercado son *Nagios* y *Cacti*, los cuales cumplen con los requerimientos exigidos por GTI-PPA para la administración de la red.

En la Tabla 3-34 se detalla la comparación de los dos sistemas de administración.

**Tabla 3-34Comparación: Software de Administración**

| **Software de Administración** | | |
|---|---|---|
| **Características** | **Cacti** | **Nagios** |
| Reportes IP SLA | Si | Via plugin |
| Agrupamiento lógico | Si | Si |
| Tendencias/Predicciones | Si | No |
| Auto descubrimiento | Via plugin | Via plugin |
| Agent | No | Si |
| SNMP | Si | Via plugin |
| Syslog | Si | Via plugin |
| Plugins | Si | Si |
| Triggers / Alertas | Si | Si |
| WebApp | Full Control | Full Control |
| Monitoreo distribuido | Si | Si |
| Almacenamiento de datos | RRDtool, MySQL | Flat file, SQL |
| Licencia | GPL | GPL |
| Mapas | Plugin | Si |
| Control de Acceso | Si | Si |
| IPv6 | Si | Si |

Si bien ambas herramientas cumplen con todas los requerimientos y que poseen las mismas características, se recomienda el software *Nagios* por su facilidad de administración e interfaz gráfica mejorada.

### 3.4.10. DIAGRAMA DE RED

El diagrama de red planteado se muestra en la Figura 3-4:

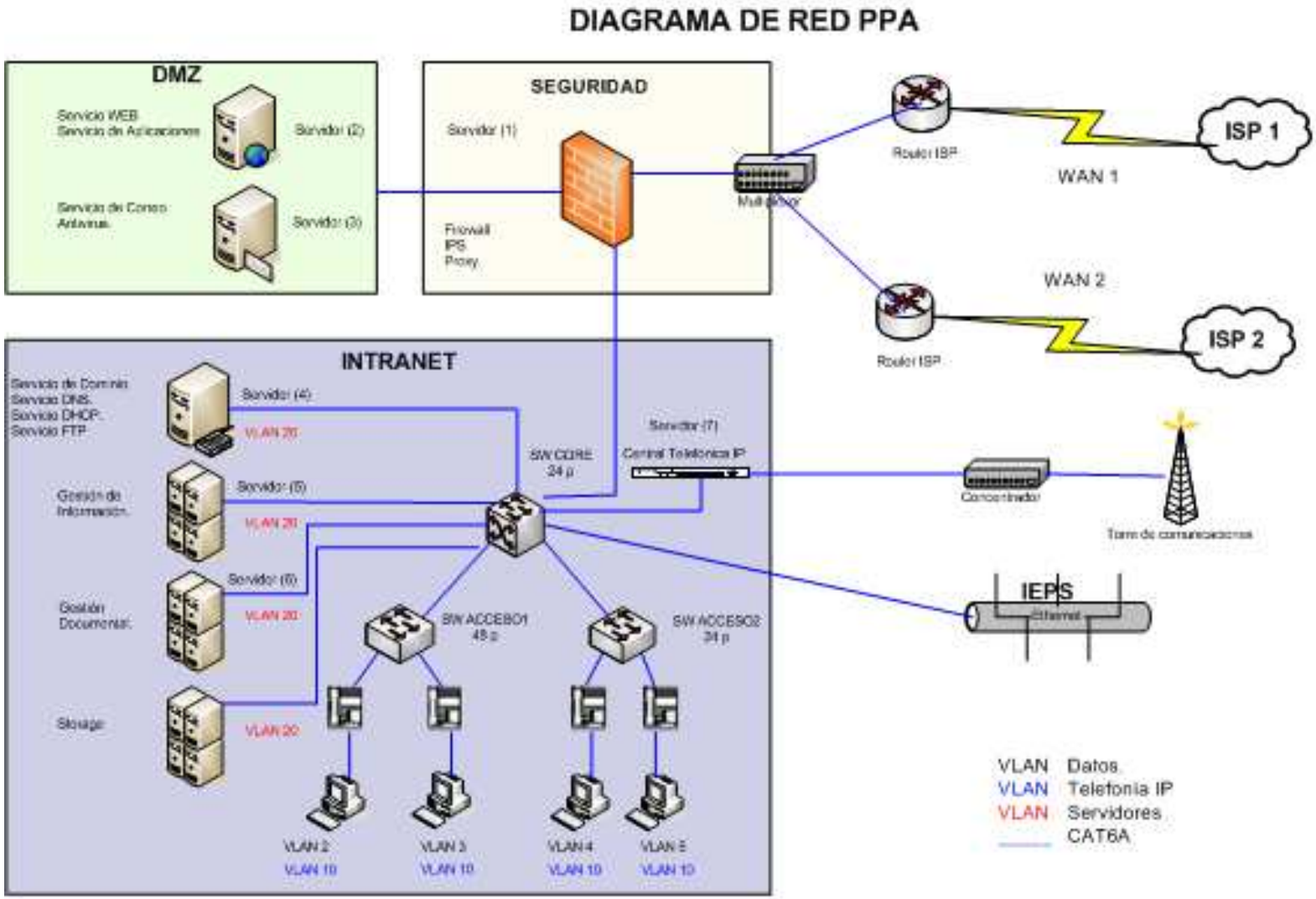



**Figura 3-4 Diagrama de Red**

# CAPÍTULO IV

# 4. IMPLEMENTACION DEL SISTEMA DE CABLEADO ESTRUCTURADO Y PRUEBAS DE LA INFRAESTRUCTURA DE RED

## 4.1. INTRODUCCIÓN

Luego de realizado el diseño de la infraestructura de comunicaciones del PPA se procede a realizar las pruebas de la misma mediante la implementación del Sistema de Cableado Estructurado, pruebas de la configuración del sistema de conectividad y el prototipo de los servicios a implementar en la infraestructura de red.

El Sistema de Cableado Estructurado se implementará con el oferente que cumpla con los requisitos técnicos, administrativos y presupuestarios dados por el PPA.

## 4.2. IMPLEMENTACIÓN DEL SCE

Luego de elegido el tipo y categoría del cable, así como la cantidad aproximada del material a utilizar se procede a la implementación del Sistema de Cableado Estructurado el cual se lo realizará en tres fases; fase de preparación, fase de recorte y fase de finalización.

### 4.2.1. FASE DE PREPARACIÓN

En la fase de preparación se realizará un reconocimiento de las nuevas instalaciones del PPA, se verificará las herramientas a utilizar, se instalará toda la ductería y cables en paredes, techo y conductos verticales.

Como primer paso se realiza el reconocimiento de las nuevas instalaciones del PPA y la verificación de los requerimientos técnicos exigidos por el PPA. El certificado de visita técnica extendida por el PPA al oferente ganador se encuentra en el Anexo 4.1.

La Figura 4-1 muestra el estado de las instalaciones del PPA en el momento de la verificación.

**Figura 4-1 Verificación de las nuevas instalaciones del PPA**

Al tratarse de instalaciones antiguas en proceso de remodelación se procura que la gran mayoría del cableado vaya empotrada en pared y conocer de antemano el lugar de las áreas de trabajo para la ubicación de los puntos de red.

#### 4.2.1.1. Materiales y equipo asignado al proyecto

El material asignado al proyecto es el siguiente:

- El cable a utilizar es 10G F/UTP Categoría 6A LSZH de la marca AMP Netconnect que cumple el desempeño del estándar ANSI/TIA/EIA 568 C. Las especificaciones técnicas se encuentran en el Anexo 4.2.
- El resto de materiales calculados en la fase de diseño deberán ser de la marca AMP Netconnect que cumple el desempeño del estándar ANSI/TIA/EIA 568 C. Los productos del SCE utilizados se encuentran en el Anexo 4.2.

El equipo asignado al proyecto es el siguiente:

- Certificadora
- Taladro
- Lantester
- Pinza amperimétrica

- Impresora de etiquetas
- Seguidor de señal
- Juego de radio de comunicaciones

La marca, modelo y estado de cada uno de los equipos son descritos por el oferente en el Anexo 4.2.

#### 4.2.1.2. Instalación en techo falso

La Figura 4-2 muestra la canalización tipo escalerilla utilizada para distribuir el cable desde el cuarto de equipos al área de trabajo, la cual será sujetada al techo, tendrá 20 centímetros de ancho que permitan el peinado apropiado del cable y recorrerá toda la instalación de acuerdo al plano diseñado. Para evitar interferencias electromagnéticas la canaleta de datos debe mantenerse separada de la canaleta de cables eléctricos.

**Figura 4-2 Canaleta de Datos y Canaleta Eléctrica**

Los aspectos a tomar en cuenta durante el tendido del cable son:

- Los ductos no deberán llenarse a más del 40% de su capacidad y el tendido del cable no sobrepasará los 90 metros en el enlace permanente.
- Los cables serán fijados en grupos mediante abrazaderas colocadas a intervalos de máximo 4 metros sin apretarlos, evitando que el cable se comprima.
- Al desenrollar el cable se procurará no cortarlo demasiado justo evitando excesivas torsiones.

- El peinado de los cables se lo realizará de forma ordenada (Figura 4-3).

**Figura 4-3 Sujeción y peinado del cable**

- Se cuidará que se cumpla con el radio de curvatura para cable categoría 6A (mínimos 4 veces el diámetro exterior del cable UTP). La Figura 4-4 muestra el radio de curvatura del cable.

**Figura 4-4 Radio de curvatura del cable**

- Cuidar al cable de posibles torsiones por objetos pesados, en el caso que el cable se encuentre deteriorado no se lo debe reparar, se lo debe reemplazar.
- Limitar el destrenzado de los conductores a 13 milímetros como máximo para evitar diafonía.
- De la canaleta principal hacia cada una de las áreas de trabajo deberán ser conducidas con tubería EMT (Figura 4-5).

**Figura 4-5 Tubería EMT hacia área de trabajo**

- Se hará uso de cajas de paso para la derivación de los cables hacia las distintas áreas de trabajo que faciliten la administración del cableado para posibles cambios y ampliaciones futuras (Figura 4-6).

**Figura 4-6 Caja de paso: Derivación hacia áreas de trabajo**

- Se deberá prever la acometida del servicio de Internet, televisión por cable y otros servicios futuros. Para tal efecto de dejará una tubería EMT que ingrese al PPA por medio de postería y llegue al cuarto de equipos (Figura 4-7).

**Figura 4-7 Acometida para futuros servicios**

#### 4.2.1.3. Bajantes

En las bajantes hacia las estaciones de trabajo se procurará que en su gran mayoría sean empotradas en pared (Figura 4-8).

Los aspectos tomados en cuenta durante el tendido del cable son:

- Se debe cuidar no sobrepasar el radio de curvatura y el cable debe bajar por medio de un ducto hasta el área de trabajo.

**Figura 4-8 Bajantes por pared**

- Las bajantes que van a través de la panelería deberán ir por ductos separados de los cables de energía eléctrica regulada o a su vez los cables de energía bajarán a través de tubería BX que eviten interferencia electromagnética en los cables de datos UTP (Figura 4-9).

**Figura 4-9 Bajante por panelería**

#### 4.2.1.4. Cuarto de Equipos

El cuarto de equipos será dividido por paredes de hormigón y no contará con techo falso, en este lugar se concentrará todo el SCE en una topología tipo estrella y de igual manera se deberá cuidar radio de curvatura del cable y su tensión (Figura 4-10).

**Figura 4-10 Cuarto de Equipos**

- En el cuarto de equipos también se deberá cuidar que los cables de datos no se junten con los cables de energía regulada por efectos de interferencias electromagnéticas (Figura 4-11).

**Figura 4-11 Canaleta de datos y eléctrica en cuarto de equipos**

#### 4.2.1.5. Área de trabajo

En el área de trabajo se colocará un punto de red y dos toma corrientes (normal y regulado respectivamente).

La ubicación de los puntos de red se los ubicará de preferencia en la pared, de los contrario se ubicarán en la parte inferior de los paneles, los cuales deberán tener ductos separados para los cables de datos y de energía eléctrica (Figura 4-12).

Los aspectos tomados en cuenta en el área de trabajo son:

- Se deberá prever una longitud de 30 centímetros de holgura para llegar al jack para posibles cambios.
- El cableado llegará a las estaciones de trabajo a través de las columnas de la panelería, la cual deberá tener adaptado dos ductos, uno para datos y otro para energía eléctrica regulada.

**Figura 4-12 Ductos de panelería**

Para montar un jack RJ-45 se debe tomar en consideración lo siguiente:

- Los jacks ubicados en pared deberán estar de 30 a 45 centímetros sobre el nivel del piso (Figura 4-13).

**Figura 4-13 Punto de red, energía eléctrica normal y regulada**

- Los jacks ubicados en los paneles deberán colocarse en la parte inferior del mismo por donde recorre el cable (Figura 4-14).

**Figura 4-14 Ubicación de cajas dexon para punto de red y energía eléctrica regulada**

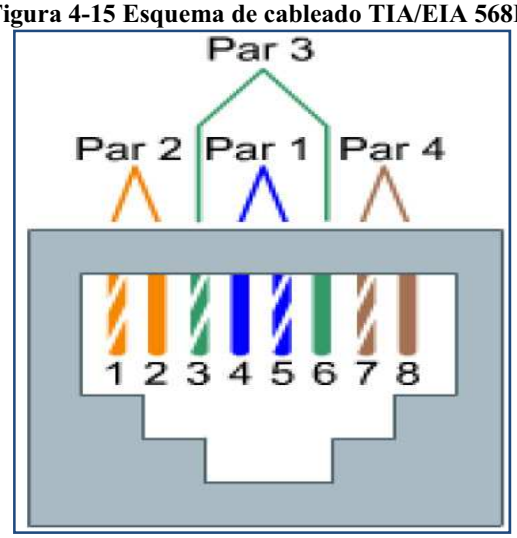
### 4.2.2. FASE DE RECORTE

En la fase de recorte se realizará la terminación de los hilos y se verificará la administración de los cables. En esta fase se cuidará que se haya dejado cable sobrante en ambos extremos del cable que faciliten cambios posteriores.

#### 4.2.2.1. Terminación de los cables de datos

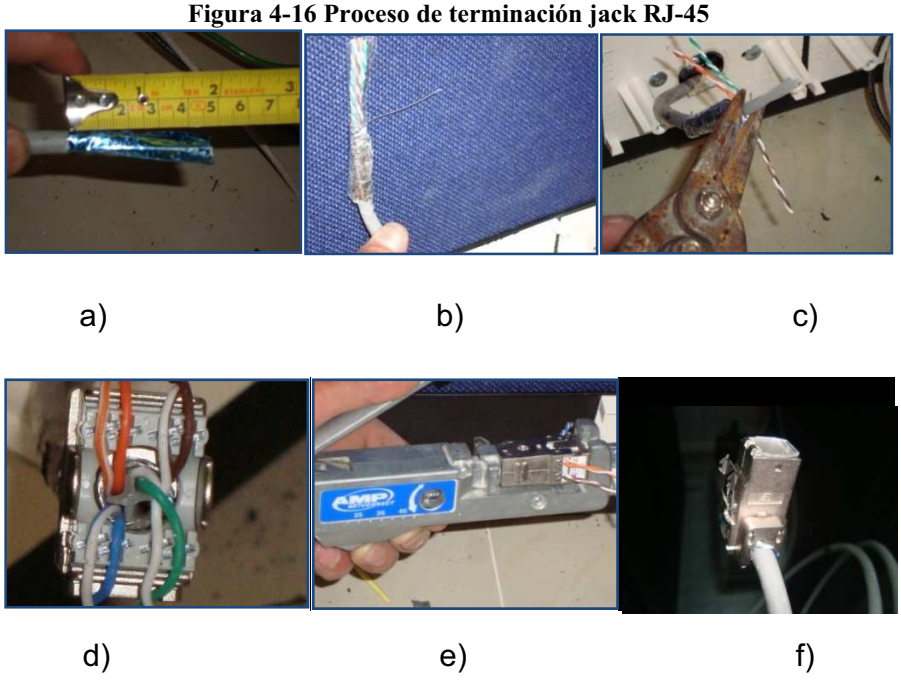
El esquema de cableado a utilizar será T568B, cuya asignación de pines se muestra en la Figura 4-15.

**Figura 4-15 Esquema de cableado TIA/EIA 568B**



- Se deberá cuidar que el jack esté conectado correctamente, de lo contrario no habrá comunicación entre los dos extremos. El proceso de parcheo deberá seguir los siguientes pasos (Figura 4-16):
    a. Cortar la chaqueta alrededor de 4 a 5 centímetros.
    b. Aislar el blindaje de aluminio y el conductor de tierra para hacer contacto con la carcasa del jack.
    c. Cortar el elemento central de refuerzo.
    d. Ubicar los cables en el jack según el código de colores del esquema T568B
    e. Utilizar la herramienta de AMP Netconnect para conectorizar los 4 pares del cable, la cual al mismo tiempo corta el excedente de cable.
    f. Finalmente se tiene armada la conexión T568B.

**Figura 4-16 Proceso de terminación jack RJ-45**




a) b) c)

d) e) f)

#### 4.2.2.2. Terminación de face plate

Se deberá cuidar que el jack esté conectado correctamente al face plate. El face plate tendrá cabida para un segundo punto de red para posibles ampliaciones (Figura 4-17).

**Figura 4-17 Conexión del jack al face plate**

La Figura 4-18 muestra el área de trabajo, la cual deberá contar con un punto de red, un punto de energía eléctrica normal y un punto de energía eléctrica regulada, identificadas cada una por colores.

**Figura 4-18 Salida de servicios al área de trabajo**


#### 4.2.2.3. Terminación en rack

En la Figura 4-19 se muestra las terminaciones en el extremo del rack, las cuales serán en un jack RJ-45 bajo el estándar T568B y conectado al path panel, se deberá cuidar constar con una reserva de cable de mínimo 1 metro por enlace.

**Figura 4-19 Terminaciones de cables en patch panel**

#### 4.2.2.4. Puesta a tierra

Se revisará que todo el SCE se encuentre aterrizado, esto incluye todas las canaletas y equipos del rack de comunicaciones.

En la Figura 420 se muestra la conexión a tierra de la canaleta de datos, mientras que en la Figura 4-21 se muestra la conexión a tierra del rack de comunicaciones.

**Figura 4-20 Conexión de la canaleta al sistema de puesta a tierra**

**Figura 4-21 Conexión del rack al sistema de puesta a tierra**

#### 4.2.2.5. Administración de cables

En la Figura 4-22 se observa la organización de los cables en el subsistema horizontal, el cual se lo realiza a través de la canaleta de datos, mientras que en el rack se lo realiza a través de organizadores, los cuales permiten la llegada ordenada de los cables al patch panel.

**Figura 4-22 Organización de cables en el rack**

#### 4.2.2.6. Etiquetado

Los cables deberán estar rotulados en ambos extremos para evitar confusión, TIA/EIA 606A específica que cada terminación de cable debe tener un identificador único.

La Figura 4-23 muestra el etiquetado en las terminaciones del área de trabajo, las cuales serán de la forma PP# - D# (Número de patch panel y número de punto de red).

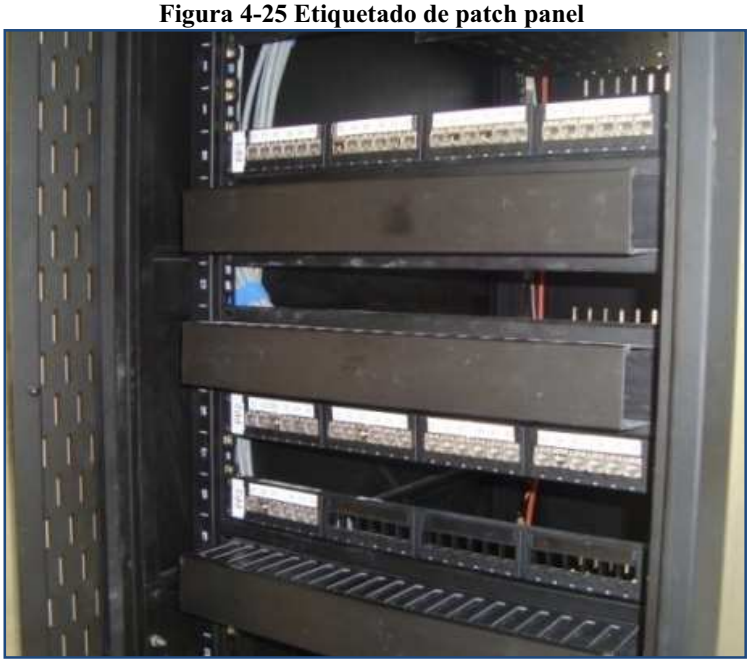
**Figura 4-23 Etiquetado en faceplate**


Las etiquetas serán realizadas con una máquina etiquetadora, no deberán ser hechas a mano o tinta degradable, las etiquetas serán de fácil lectura, con letras de molde (Figura 4-24).

**Figura 4-24 Etiquetado en Rack**

La correcta etiquetación en ambos extremos del cable permitirá una correcta administración del SCE, el punto de red en el face plate del área de trabajo deberá coincidir con el punto de red ubicado en el patch panel del rack.

**Figura 4-25 Etiquetado de patch panel**



### 4.2.3. FASE DE FINALIZACIÓN

En la fase de finalización se realizarán las pruebas de cables, diagnóstico de problemas y certificación de los puntos de red en el enlace permanente.

Una vez finalizada la instalación del enlace permanente se debe certificar el SCE mediante la comparación del rendimiento de transmisión del SCE con el estándar TIA/EIA 568 C.2 para cableado categoría 6A. La certificación demostrará y garantizará la calidad de los componentes y de la mano de obra.

La certificación del SCE se debe realizar con un analizador de cables que permita medir el rendimiento del cable y descubrir circuitos abiertos, cortocircuitos, pares divididos y otros problemas de cableado. Las pruebas de certificación se realizarán con equipos dedicados al la comprobación del cable categoría 6A los cuales deberán tener su respectiva certificación de calibración (Anexo 4.3).

#### 4.2.3.1. Equipo analizador de cable

Los equipos utilizados para la certificación del SCE son:

**Analizador de cable Fluke Networks DTX-1800**

- Mide el rendimiento de 10 Gigabit Ethernet y Alien Crosstalk (ANEXT, AFEXT) a una frecuencia de 500 MHz.
- Analiza cables de par trenzado con o sin blindaje (STP, FTP, SSTP y UTP).
- TIA categoría 3, 4, 5, 5E, 6 y 6A
- Cumple el estándar de prueba TIA categoría 6A según ANSI/TIA-568-C.2 (solo 6A DTX-1800).
- Comprobación automática bidireccional completa de enlaces categoría 6A e ISO/IEC clase F en 22 segundos.
- Parámetros de comprobación
    - Longitud
    - Retardo de propagación
    - Diferencia de retardo
    - Resistencia de bucle CC
    - Pérdidas de inserción (atenuación)
    - Pérdida de Retorno (RL)
    - NEXT
    - Radio de atenuación (ACR)

**Figura 4-26 Analizador de cables DTX-1800**

Las especificaciones técnicas del analizador DTX (Figura 4-26) se encuentra en el Anexo 4.4

**Adaptador de enlace permanente DTX-PLA002 para categoría 6A**

- El equipo soporta varias categorías de cables UTP, cuyo análisis depende del adaptador utilizado. El adaptador para cable categoría 6A es el DTX-PLA002 (Figura 4-27).
- Tipo de conector y duración de los adaptadores de enlace permanente categoría 6A/clase $E_A$: cable con y sin blindaje, TIA categoría 3, 4, 5, 5e, 6, 6A y enlace permanente clase C, D, E y $E_A$ ISO/IEC.
- El adaptador de enlace permanente deberán ser totalmente transparentes a las mediciones.

**Figura 4-27 Adaptador de enlace permanente DTX-PLA002**


#### 4.2.3.2. Proceso de Certificación

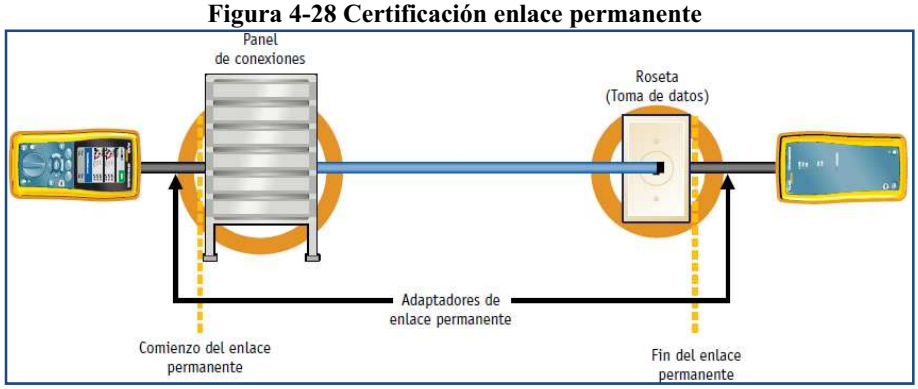
El proceso de certificación conlleva la selección del estándar de comprobación (estándar T568), el modo de enlace (permanente), el tipo de cable (categoría 6A) y la frecuencia de operación (500MHz). Así como la comprobación de la calibración de los instrumentos, los cuales se calibran en fábrica y se verifican cada 12 meses.

Se ha elegido la certificación en modo de enlace permanente debido a que los patch cords tanto del área de trabajo como del rack cambian muchas veces durante la vida útil del enlace permanente.

El proceso de comprobación del enlace permanente se observa en la Figura 4-28.

- Se coloca al analizador en el extremo del cable localizado en el patch panel del rack mientras que el otro extremo se ubica el analizador remoto.

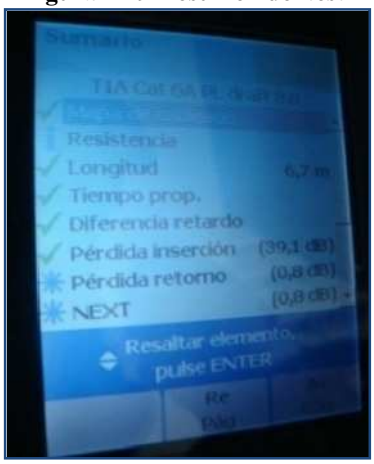
**Figura 4-28 Certificación enlace permanente**




- Al realizar el test, el analizador muestra los siguientes datos:
  - Mapa del cableado según el estándar T568B
  - Longitud de cada uno de los pares del cable
  - Tiempo de propagación
  - Diferencia de retardo
  - Pérdida de inserción

Y finalmente en la Figura 4-29 se muestra el resumen del test, el cual es guardado y almacenado en el equipo para su posterior traspaso a un computador donde se encuentra el software para la generación de informes.

**Figura 4-29 Resumen del test**



En el caso de que falle la certificación, este mostrará en pantalla su causa (Figura 4-30). Un error por falla del cableado es el que se muestra en la siguiente y figura, el cual deberá ser solucionado a través de su correcta ubicación de cables de acuerdo al estándar T568B, en el caso que el cable presente fallas de atenuación, retardo u otro defecto que merme su rendimiento el cable deberá ser revisado.

**Figura 4-30 Falla de certificación**


#### 4.2.3.3. Análisis de resultados

El análisis de los resultados se realizará tomando como ejemplo los resultados obtenidos del enlace permanente PP1-D01 (Anexo 4.3).

Los resultados de tiempo de propagación, diferencia de retardo y pérdida de inserción serán certificados solamente si sus resultados cumplen o exceden los requerimientos de la categoría 6A según el estándar ANSI/TIA/EIA 568 B.2-10 y ANSI/TIA-568-C.2.

**Tabla[44] 4-1 Características de desempeño del SCE categoría 6A de ANSI/TIA/EIA 568 B.2-10**

| Frecuencia (MHz) | IL Máximo (dB/100 m) | NEXT Mínimo (dB) | PSNEXT Mínimo (dB) | ELFEXT Mínimo (dB) | PSELFEXT Mínimo (dB) | Retardo Máximo (ns/100 m) | RL Mínimo (dB) | Impedancia Característica (Ω) | ACR Mínimo (dB) |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 3.7 | 65.3 | 63.3 | 55.8 | 52.8 | 552 | 23.0 | 100 ± 15 | 61.0 |
| 8 | 5.2 | 60.8 | 58.8 | 49.7 | 46.7 | 547 | 24.5 | 100 ± 15 | 55.0 |
| 10 | 5.9 | 59.3 | 57.3 | 47.8 | 44.8 | 545 | 25.0 | 100 ± 15 | 53.0 |
| 16 | 7.4 | 56.2 | 54.2 | 43.7 | 40.7 | 543 | 25.0 | 100 ± 15 | 49.0 |
| 20 | 8.3 | 54.8 | 52.8 | 41.8 | 38.8 | 542 | 25.0 | 100 ± 15 | 46.0 |
| 25 | 9.3 | 53.3 | 51.3 | 39.8 | 36.8 | 541 | 24.3 | 100 ± 15 | 44.0 |
| 31.25 | 10.4 | 51.9 | 49.9 | 37.9 | 34.9 | 540 | 23.6 | 100 ± 15 | 41.0 |
| 62.5 | 14.9 | 47.4 | 45.4 | 31.9 | 28.9 | 539 | 21.5 | 100 ± 15 | 32.0 |
| 100 | 19.0 | 44.3 | 42.3 | 27.8 | 24.8 | 538 | 20.1 | 100 ± 15 | 24.0 |
| 150 | 23.6 | 41.7 | 39.7 | 24.3 | 21.3 | 537 | 18.9 | 100 ± 15 | 16.8 |
| 200 | 27.5 | 39.8 | 37.8 | 21.8 | 18.8 | 537 | 18.0 | 100 ± 15 | 10.6 |
| 250 | 31.0 | 38.3 | 36.3 | 19.8 | 16.8 | 536 | 17.3 | 100 ± 15 | 5.3 |
| 300 | 34.2 | 37.1 | 35.1 | 18.3 | 15.3 | 536 | 16.8 | 100 ± 15 | – |
| 500 | 45.3 | 33.8 | 31.8 | 13.8 | 10.8 | 536 | 15.2 | 100 ± 15 | – |

[44] Tabla tomada de: http://www.ampnetconnect.com/documents/Cable_FTP_C6A_LSZH_1859218-X_Rev_E.pdf

El análisis de los datos obtenidos de la certificación se realiza a través de una prueba de margen y de peor valor.

La prueba de margen consiste en efectuar la diferencia entre el valor medido y el valor de límite aplicable. En este caso los valores de rendimiento medidos son comparados con el valor de rendimiento límite en el rango de frecuencia de 500MHz del cable categoría 6A mostrado en la Tabla 4.1. Si el margen más bajo encontrado es positivo la certificación “PASA”, si el margen es negativo la certificación “FALLA” y si el margen es cero el valor medido será igual al valor límite. Si margen analizado es alto quiere decir que es un resultado de comprobación muy bueno mientras que un margen muy cercano al límite se lo conoce como resultado de comprobación marginal en cuyo caso se debe generar información de diagnóstico para localizar el problema, corregirlo y conseguir un enlace de buen rendimiento.

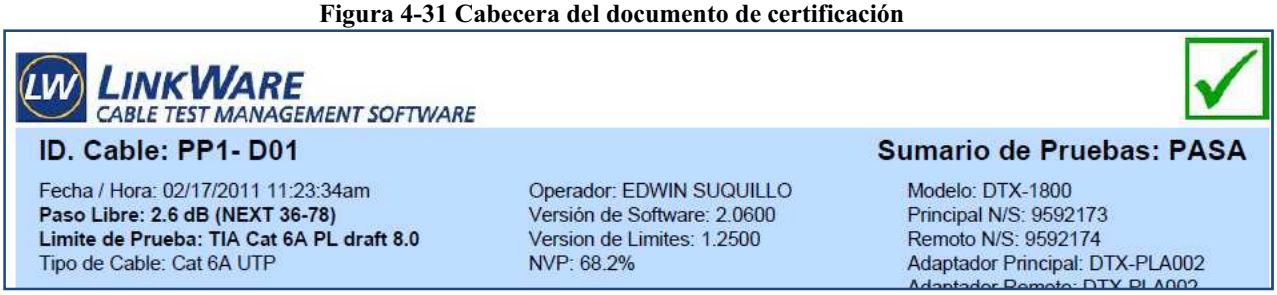
La prueba del peor valor en un principio no toma como referencia los límites de rendimiento del cable, únicamente toma el peor valor en el rango de frecuencia respectivo. Luego de encontrado el peor valor se procede a comparar con el límite de rendimiento a dicha frecuencia y se encuentra el margen de peor valor.

En las pruebas de certificación del anexo digital 4 se puede observar que los valores no siempre son tomados en los mismos pares de cables, ya que la prueba se realiza sobre todos los pares y se toma como referencia al par de más bajo rendimiento. Además se toma los valores en los dos extremos (“MAIN”, “SR”) del enlace permanente para compararlos y tomar la peor medida, no siempre son los mismos debido al margen de error del equipo.

La prueba de margen y de peor valor son utilizados para la certificación, los dos valores pueden ser el mismo y en el mismo par, sin embargo la prueba de margen no puede ser nunca mayor que la prueba del peor valor, por lo que los proveedores de cable y el cliente se interesan más en el valor de la prueba de margen.

La Figura 4-31 muestra parte de los resultados de la certificación del enlace permanente PP1-D01 (Anexo 4.5) en la que se describen los siguientes resultados:

**Figura 4-31 Cabecera del documento de certificación**




Donde:

- El Paso Libre o Headroom es 2.6 dB (NEXT 36-78) que es el margen obtenido de la diferencia del NEXT.
- Se especifica que el límite de prueba es realizado en relación con los límites de rendimiento del cable UTP categoría 6A.
- Se especifica el NVP en 68.2% (Velocidad Nominal de Propagación) la cual relaciona la velocidad de propagación del cable con la velocidad de la luz, la cual es utilizada por el equipo para encontrar la distancia a la cual se encuentra una falla.
- Se especifica el operador, versión del software y el modelo del equipo analizador.

En la Figura 4-32 se muestra los resultados del mapa de cableado y rendimiento.

**Figura 4-32 Documento: Mapa de cableado y rendimiento**


Donde:

- El primer parámetro es el mapa del cableado según el estándar elegido (T568 B) donde se prueba la continuidad del cable. Las causas posibles de falla del cableado se muestran Tabla 4-2.

**Tabla[45] 4-2 Posibles fallas del mapa de cableado**

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Abierto | • Cables rotos por tensiones en las conexiones<br>• Cables unidos a una conexión equivocada<br>• El cable no está fijado correctamente y no hace contacto en el IDC<br>• Conector dañado<br>• Cortes o ruptura en el cable<br>• Cables conectados a pines incorrectos en el conector o bloque de conexión<br>• Cable específico de la aplicación (por ej. Ethernet que utilice sólo 12/36) |
| Cortocircuito | • Terminación incorrecta del conector<br>• Conector dañado<br>• Material conductor pegado entre los pines de una conexión<br>• Cable dañado<br>• Cable *específico de la aplicación (por ej. en la automatización de la fábrica)* |
| Par invertido alineado | • Cables conectados a pines incorrectos en el conector o bloque de conexión |
| Par cruzado | • Cables conectados a pines incorrectos en el conector o bloque de conexión<br>• Mezcla de estándares de cableado 568A y 568B (12 y 36 cruzados)<br>• Se han utilizado cables cruzados (12 y 36 cruzados) |

- Luego se especifica la longitud del cable (26.6 metros), el cual no debe sobrepasar los 90 metros. Las posibles causas de falla en la longitud del cable se muestran en la Tabla 4-3.

**Tabla 4-3 Posibles fallas de la longitud del cable**

***Longitud***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| La longitud excede los límites | • Cable demasiado largo: *compruebe si hay bucles de servicio enrollados y, si los hay, deshágalos*<br>• La NVP está mal configurada |
| La longitud resultante es menor que la conocida | • Rotura en una zona intermedia del cable |
| Uno o más pares son sensiblemente más cortos | • Cable dañado<br>• Mala conexión |

[45] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

- Se especifica el tiempo de propagación (139 nano segundos) que es el tiempo que la señal demora llegar al extremo distante, el cual no debe pasar los 496 nanosegundos.
- Se especifica la diferencia de retardo (9 nanosegundos), el cual no puede pasar de los 44 ns. Las posibles causas de falla se detallan en la Tabla 4-4.

**Tabla[46] 4-4 Posibles causas de falla de los retardos**

***Retardos/Diferencia***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Límites excedidos | • Cable demasiado largo: *retardo de propagación*<br>• El cable usa distintos materiales aislantes en los diferentes pares: *diferencia de retardos* |

- Se especifica la resistencia del cable (3.9 ohmios) la cual no puede pasar de los 100 +/- 15% 0hmios. Las posibles causas de falla se muestran en la Tabla 4-5.

**Tabla 4-5 Posibles causas de falla de la resistencia**

***Resistencia***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Falla *falla o *pasa | • Longitud excesiva del cable<br>• Conexión en mal estado debido a contactos oxidados<br>• Conexión en mal estado debido a conductores conectados de forma superficial<br>• Cable de calibre inferior<br>• Tipo de latiguillo incorrecto |

- Se especifica el margen de pérdida de inserción o atenuación (31.5 dB) que constituye la disminución de potencia que sufre la señal al propagarse por el cable.
- Se especifica la frecuencia de operación (500MHz).
- Se especifica el límite de perdida de inserción a dicha frecuencia (43.8 dB). Las posibles causas de falla se muestran en la Tabla 4-6.

[46] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

**Tabla[47] 4-6 Posibles causas de la atenuación**

***Pérdidas de inserción (atenuación)***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Límites excedidos | • Longitud excesiva<br>• Cables de conexión no trenzados o de calidad deficiente<br>• Conexiones de alta impedancia: *utilice técnicas en el dominio del tiempo para solucionar los problemas*<br>• Categoría de cable inadecuada: *por ej., categoría 3 en una aplicación de categoría 5e*<br>• Seleccionada una prueba automática incorrecta para el cableado que se comprueba |

Seguidamente se muestran los siguientes datos:

- **NEXT (*Near End Crosstalk*) Y PS NEXT (*Power Sum NEXT*)**

Como se mencionó, se tomarán en cuenta los valores de margen de peor caso en el extremo principal y en el extremo remoto.

En la Figura 4-33 del enlace analizado (PP1-D01) se observa que los peores pares en NEXT en el extremo principal son el 3-6 y 4-5 con una margen de 3.7 dB a una frecuencia de 473 MHz. Este margen es sumamente inferior a su límite de 27.4 dB.

Los peores pares en NEXT en el extremo remoto son el 3-6 y 7-8 con una margen de 2.6 dB a una frecuencia de 70.3 MHz, éste margen es sumamente inferior a su límite de 44.3 dB.

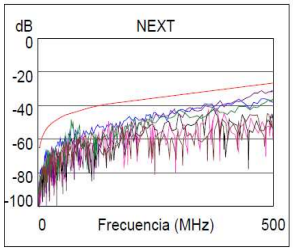
Con los datos obtenidos se concluye que el acoplamiento electromagnético entre los pares es adecuado, sin producir diafonía en enlace y por ende el paso de la prueba de certificación.

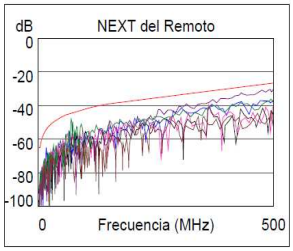
De la misma manera se analiza el PS NEXT el cual se diferencia del NEXT en que se mide la interferencia electromagnética producida por los tres pares sobre uno de los pares. En los protocolos de red se utilizan los cuatro pares, por lo cual ésta medida de rendimiento es tomada más muy en cuenta.

[47] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

**Figura 4-33 Documento: NEXT y PS NEXT**

| | Margen de Peor Caso | | Valor de Peor Valor | |
|---|---|---|---|---|
| **PASA** | MAIN | SR | MAIN | SR |
| Peor Par | 36-45 | 36-78 | 36-45 | 36-45 |
| **NEXT (dB)** | 3.7 | 2.6 | 3.7 | 3.2 |
| Frec. (MHz) | 473.0 | 70.3 | 473.0 | 489.0 |
| Límite (dB) | 27.4 | 44.3 | 27.4 | 27.0 |
| Peor Par | 36 | 36 | 36 | 36 |
| **PS NEXT (dB)** | 4.8 | 4.4 | 4.8 | 4.5 |
| Frec. (MHz) | 473.0 | 431.0 | 473.0 | 489.0 |
| Límite (dB) | 24.6 | 26.0 | 24.6 | 24.1 |




Las posibles causas de márgenes pequeños o negativos del NEXT y PS NEXT se describen en la Tabla 4-7.

**Tabla[48] 4-7 Posibles causas de NEXT**

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Falla *falla o *pasa | • Trenzado deficiente en los puntos de conexión<br>• La conexión (ajuste) macho-hembra no es demasiado buena (aplicaciones de categoría 6/Clase E)<br>• Adaptador de enlace incorrecto (adaptador de categoría 5 para enlaces de categoría 6)<br>• Latiguillos de calidad deficiente<br>• Conectores defectuosos<br>• Cable defectuoso<br>• Pares divididos<br>• Uso inadecuado de los acopladores<br>• Compresión excesiva provocada por bridas de plástico<br>• Fuente de ruido excesiva, adyacente a la medición |
| Resultado Pasa inesperado | • Los nudos o torceduuras no siempre causan fallos de NEXT, sobre todo en un cable en buen estado y alejado de los extremos del enlace<br>• Seleccionada una prueba automática incorrecta (por ej., un enlace de categoría 6 probado por error con los límites de la categoría 5)<br>• "Falla" a baja frecuencia en el gráfico NEXT, pero pasa el límite general de aceptación. Cuando se utilizan los estándares ISO/IEC, la llamada "regla de los 4 dB" indica que los resultados NEXT medidos con una pérdida de inserción menor de 4 dB no pueden dar como resultado un Falla. |

- **ACR-F (Attenuation to Crosstalk Ratio) Y PS ACR-F (Power Sum ACR)**

El valor de ACR-F (*Attenuation to Crosstalk Ratio*) proporciona une medida de la calidad de la señal frente al ruido debido a que se define como la relación entre la señal

[48] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

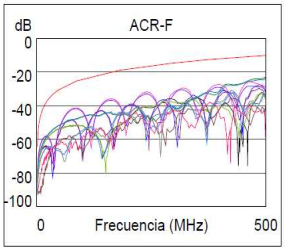
de entrada útil y el nivel de señal interferente, por lo que espera valores de ACR altos con respecto a su límite.

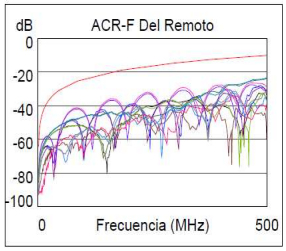
En la Figura 4-34 se observa que el peor par en el emisor (3-6 y 4-5) tiene un ACR de 13 dB que sobrepasa el valor mínimo de 10.3 dB a 497 MHz, y en el receptor se tiene un ACR-F de 13.4 dB el cual también sobrepasa a su valor mínimo de 10.2 dB a 498 MHz, lo cual quiere decir que el ruido no causará pérdida de información.

El PS ACR-F es la suma de los efectos individuales ACR de cada par de cables.

**Figura 4-34 Documento: ACR-F y PS ACR-F**

| PASA | MAIN | SR | MAIN | SR |
|---|---|---|---|---|
| Peor Par | 36-45 | 36-45 | 36-45 | 36-45 |
| **ACR-F (dB)** | 13.0 | 13.4 | 13.0 | 13.4 |
| Frec. (MHz) | 497.0 | 498.0 | 498.0 | 498.0 |
| Límite (dB) | 10.3 | 10.2 | 10.2 | 10.2 |
| Peor Par | 45 | 36 | 45 | 36 |
| **PS ACR-F (dB)** | 14.3 | 15.4 | 14.6 | 15.4 |
| Frec. (MHz) | 467.0 | 495.0 | 497.0 | 495.0 |
| Límite (dB) | 7.8 | 7.3 | 7.3 | 7.3 |




Las posibles causas de márgenes bajo el nivel mínimo de ACR-F y PS ACR-F se detallan en la Tabla 4-8.

**Tabla[49] 4-8 Posibles causas de ACR-F y PS ACR-F**

***ACR-F y PS ACR-F (anteriormente: ELFEXT y PSELFEXT)***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Falla *falla o *pasa | • Regla general: solucione los problemas de NEXT primero. Así se corrigen, normalmente, los problemas de ACR-F (ELFEXT)<br>• Bucles de servicio con muchos enrollamientos apretados |

- **RL (Pérdida de Retorno)**

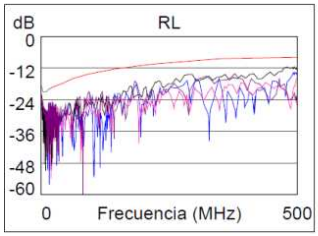
La pérdida de retorno es causada debido a la incorrecta adaptación de impedancias entre los componentes del enlace permanente.

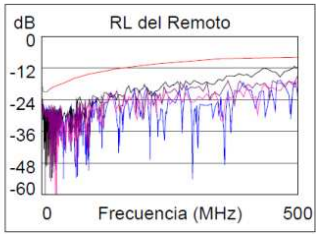
Los resultados obtenidos del análisis de la pérdida de retorno se muestran en la Figura 4-35.

[49] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

**Figura 4-35 Documento: Pérdida de retorno**

| PASA | MAIN | SR | MAIN | SR |
|---|---|---|---|---|
| Peor Par | 45 | 45 | 45 | 45 |
| RL (dB) | 3.3 | 3.4 | 3.3 | 3.4 |
| Frec. (MHz) | 477.0 | 493.0 | 477.0 | 493.0 |
| Límite (dB) | 8.0 | 8.0 | 8.0 | 8.0 |




Los factores que afectarían la discontinuidad y generarían una onda reflejada que haría disminuir las pérdidas de retorno dificultando la transmisión de los datos se detallan en la Tabla 4-9.

**Tabla[50] 4-9 Posibles causas de pérdida de retorno**

***Pérdida de retorno***

| Resultado de las comprobaciones | Posible causa del resultado |
|---|---|
| Falla *falla o *pasa | • La impedancia del latiguillo no es de 100 ohmios<br>• La manipulación incorrecta del latiguillo causa cambios en la impedancia<br>• Prácticas de instalación (destrenzado o deformaciones en el cable: *deben mantenerse, en lo posible, los trenzados originales para cada par*)<br>• Cantidad excesiva de cable atascado en la caja de la roseta<br>• Conector defectuoso<br>• La impedancia del cable no es uniforme<br>• El cable no es de 100 ohmios<br>• La impedancia no coincide en la unión entre los cables de conexión o latiguillos y el horizontal<br>• La conexión (ajuste) macho-hembra no es demasiado buena<br>• Se está utilizando un cable de 120 ohmios<br>• Bucles de servicio en el armario de telecomunicaciones<br>• Seleccionada una prueba automática incorrecta<br>• Adaptador de enlace defectuoso |
| Resultado Pasa inesperado | • Los nudos o deformaciones no siempre causan fallos de pérdida de retorno, sobre todo en un cable en buen estado y alejado de los extremos del enlace<br>• Seleccionada una prueba automática incorrecta (más fácil pasar los límites de RL)<br>• "Falla" a baja frecuencia en el gráfico RL, pero pasa el límite general de aceptación. Gracias a la "regla de los 3 dB", por la cual no pueden fallar los resultados de RL medidos con una pérdida de inserción menor de 3 dB |

En la certificación se muestran puntos certificados con la señal “PASA*” con un asterisco, lo cual nos permite conocer que dicho valor de rendimiento están dentro de

[50] Tablas tomadas de: http://www.abmrexel.es/img/descargas/pdf/pdf_desc_44.pdf

los límites de exactitud del instrumentos, es decir que el margen se acerca al límite, los cuales deberán ser revisados.

La Figura 4-36 muestra la fachada final con los puntos de red en las áreas de trabajo.

**Figura 4-36 Área de trabajo terminada**

## 4.3. PRUEBAS DE LA INFRAESTRUCTURA DE RED

En base a los requerimientos analizados en la etapa de diseño y al esquema de red propuesto se presentará la instalación, configuración y pruebas de los servicios requeridos por el PPA.

Los servicios instalados en la red serán:

- Servicio de DHCP
- Servicio de DNS
- Servidor de página Web
- Servidor FTP
- Servidor de correo electrónico
- Servidor de Base de Datos
- Servicio de Directorio
- Firewall

- Establecimiento de VPN
- Detección de virus y spam

El esquema de red presentado en el diseño se conforma con un *datacenter* de infraestructura y de un sistema de seguridad perimetral.

El data center de infraestructura constará con los servicios y servidores de comunicación necesarios para la conectividad de la Intranet, así como los servicios necesarios para el desarrollo de las actividades del PPA.

La seguridad perimetral será realizada a través del servicio de Firewall, NAT, IPS y *routing.*

### 4.3.1. INSTALACIÓN Y CONFIGURACIÓN DEL DATACENTER DE INFRAESTRUCTURA

La infraestructura de comunicaciones será configurada haciendo uso de Software Libre, el software ha utilizar en el data center de infraestructura será el analizado en la etapa de diseño, en la cual se analizó las diferentes opciones de software.

La infraestructura de comunicaciones será realizada a través de la distribución *ClearOS*, la cual se basa en *CentOS*. Esta distribución presenta la posibilidad de ser utilizada como servidor Gateway (puerta de enlace) y servidor de comunicaciones. Es una distribución orientada a PyMEs, lo cual se adapta a los requerimientos del PPA.

Para el *datacenter* de infraestructura se enfocará al *ClearOS* como servidor de comunicaciones, en el cual se tienen los siguientes servicios:

- Servidor LDAP con autenticación SAMBA como PDT (*Primary Domain Controller*).
- Servicio de DHCP y DNS a través de Dnsmasq
- Servidor de correo electrónico a través de Postfix, servicio de webmail a través de Horde.
- Servidor de Base de Datos a través de MySQL.

- Servidor FTP a través de Proftpd
- Servidor de impresión a través de Cups.
- Servidor Web a través de Apache Web Server

La instalación de la distribución ClearOS se encuentra en el Anexo 4.6.

#### 4.3.1.1. Servicio de Directorio

El servicio de directorio se lo implementará a través de OpenLDAP con autenticación SAMBA como PDT (*Primary Domain Controller*).

El servicio de directorio almacenará de forma jerárquica la información de los recursos de la red, usuarios, computadores, servicios y demás dispositivos periféricos. De esta forma la administración del acceso a equipos y servicios de la red será centralizado.

##### *4.3.1.1.1. Configuración*

Si bien el servicio de directorio se viene instalado en la distribución instalada, éste deberá ser configurado de acuerdo al dominio y estructura organizacional del PPA.

A través de la interfaz gráfica se configurará:

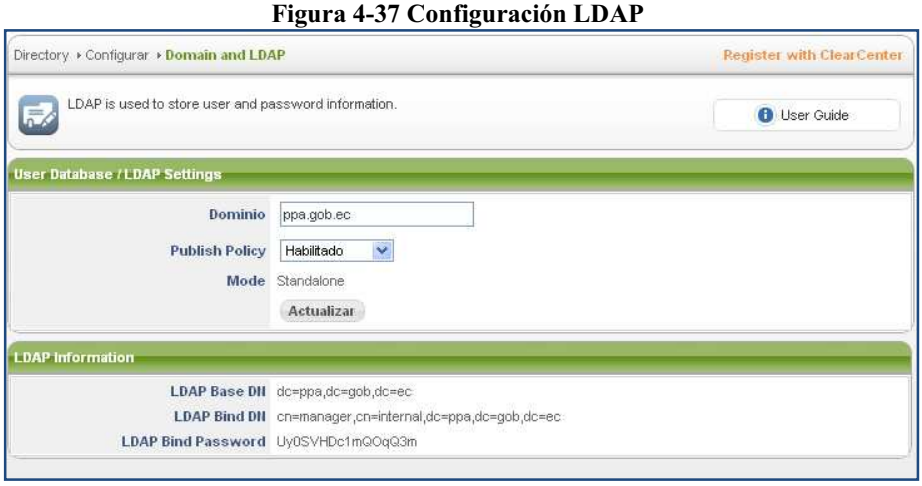
- EL dominio: ppa.gob.ec
- LDAP Base DN: dc=ppa, dc=gob, dc=ec
- LDAP Bind DN: cn=manager, cn=internal, dc=ppa, dc=gob, dc=ec

Donde Base DN (*Distinguished Name*) es el directorio base o raíz dentro del árbol y dc determina un componente del nombre de dominio.

Bind DN es la ubicación del administrador del directorio LDAP dentro de la clase person, además se especifica la contraseña creada.

La Figura 4-37 muestra la interfaz gráfica para la configuración LDAP.

**Figura 4-37 Configuración LDAP**




La Figura 4-38 muestra el archivo de configuración, el cual se encuentra en /etc/openldap/slapd.conf en el que se encuentran los esquemas (core, cosine, samba).

**Figura 4-38 Archivo de configuración OpenLDAP**

```
[root@server etc]# vi /etc/openldap/slapd.conf
# Global configuration directives
#---------------------------------------------------------

include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/rfc2307bis.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/rfc2739.schema
include /etc/openldap/schema/kolab2.schema
include /etc/openldap/schema/horde.schema
include /etc/openldap/schema/pcn.schema
include /etc/openldap/schema/samba.schema
include /etc/openldap/schema/ppolicy.schema
include /etc/openldap/schema/RADIUS-LDAPv3.schema

pidfile /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args

TLSCACertificateFile   /etc/openldap/cacerts/cert.pem
TLSCertificateFile     /etc/openldap/cacerts/cert.pem
TLSCertificateKeyFile  /etc/openldap/cacerts/key.pem

rootDSE /etc/openldap/rootDSE.ldif

defaultsearchbase "dc=ppa,dc=gob,dc=ec"

allow bind_v2

loglevel 0

sizelimit 10000

modulepath /usr/lib/openldap
moduleload accesslog.la
moduleload ppolicy.la
moduleload syncprov.la
```

Luego se verifica el funcionamiento del servicio mediante la instrucción:

*ldapsearch -h localhost –b "dc=ppa, dc=gob, dc=ec" –D "cn=manager, cn=internal, dc=ppa, dc=gob, dc=ec"-s base "objectclass=*" –x –w UyOS*

En la Figura 4-39 se observa la instrucción donde se busca todos los objetos del dominio con la cuenta del administrador y su contraseña.

**Figura 4-39 Comprobación de la configuración LDAP**

```
[root@server ~]# ldapsearch -h localhost -b "dc=ppa,dc=gob,dc=ec" -D "cn=manager
,cn=internal,dc=ppa,dc=gob,dc=ec" -s base "objectclass=*" -x -w UyOSVHDc1mQOqQ3m

# extended LDIF
#
# LDAPv3
# base <dc=ppa,dc=gob,dc=ec> with scope baseObject
# filter: objectclass=*
# requesting: ALL
#

# ppa.gob.ec
dn: dc=ppa,dc=gob,dc=ec
dc: ppa
objectClass: top
objectClass: domain

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
[root@server ~]#
```

Luego se debe ingresar la información acerca del dominio ppa.gob.ec y la organización para crear la configuración por defecto de seguridad. Estos datos son utilizados para hacer de nuestro servidor una Autoridad Certificadora internan para servicios de correo electrónico, web, etc.

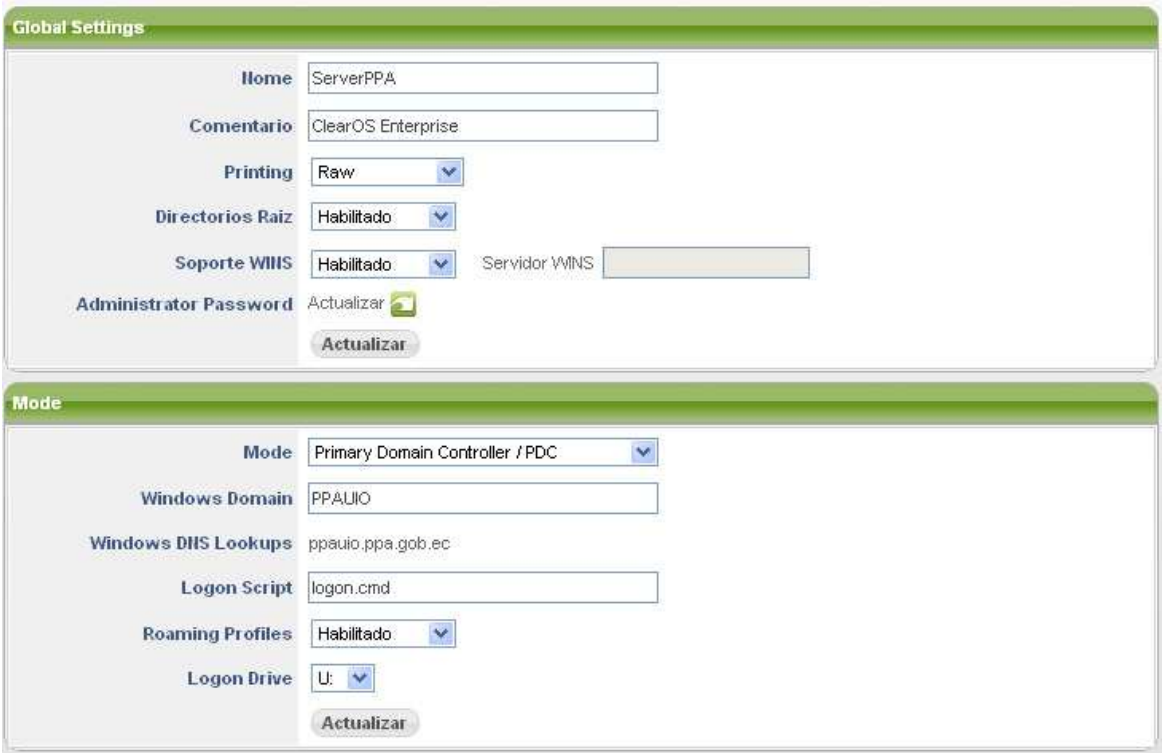
La Figura 4-40 muestra la interfaz gráfica para la configuración de los datos de la organización del PPA.

**Figura 4-40 Organización PPA**


En la Figura 4-41 se observa la configuración del servicio de autenticación con el servidor Linux y compartición de archivos con sistemas Windows. Aquí se realiza la configuración de Samba en donde se especifica:

- Se configura el nombre del servidor
- Se configura la opción de compartición de impresoras. Raw cuando los drives se instalarán en cada cliente y Point and Click cuando los drivers serán instalados desde el servidor.
- Se configura el uso de servidor WINS.
- Se configura la contraseña del usuario winadmin, la cual será usada en dominios Windows para adherir computadoras el dominio de ClearOS.
- Se configura el modo de red, en este caso será como PDC (Primary Domain Controller), donde se configurará el dominio Windows.

**Figura 4-41 Configuración para sistemas Windows**



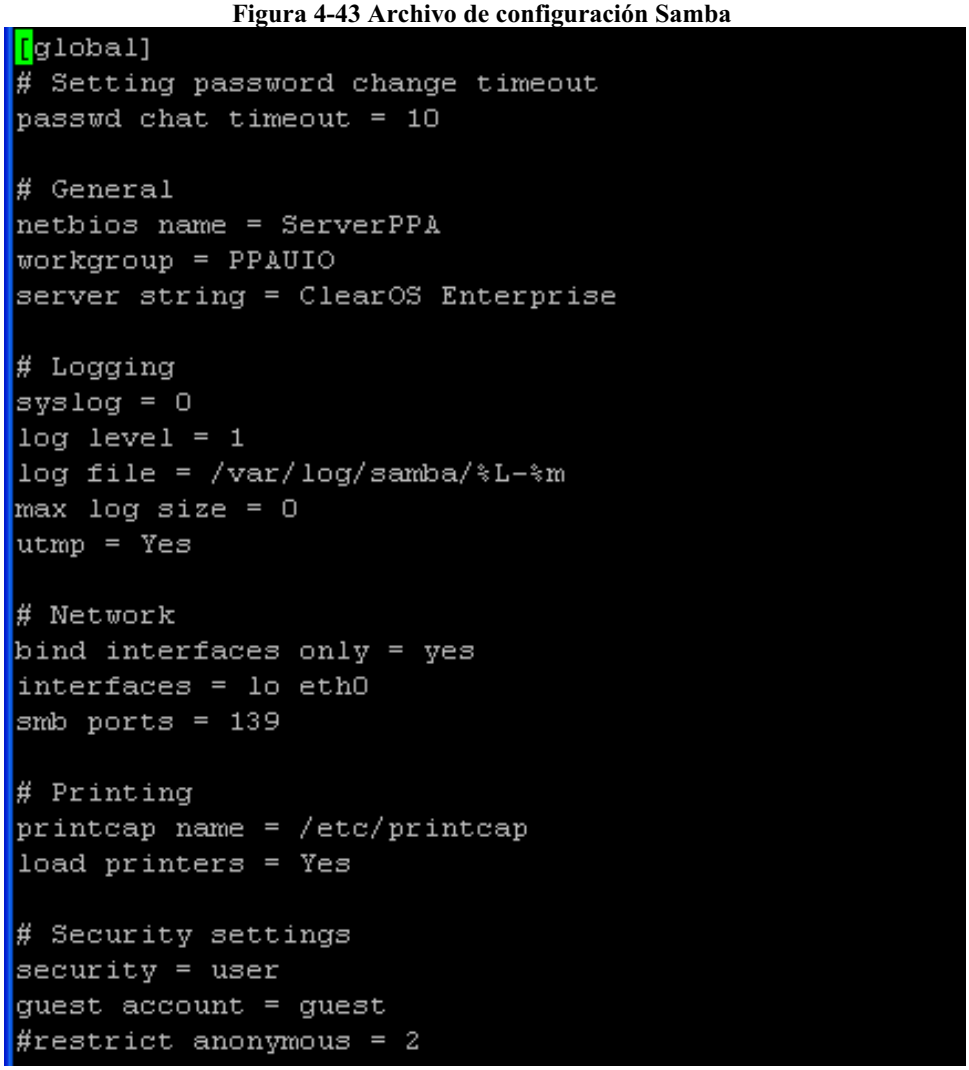

Finalmente se revisa la configuración por línea de comando del servicio smbd y sus archivos de configuración. En la Figura 4-42 se observa el archivo de configuración que le permite tener una conexión con OpenLDAP es */etc/samba/smb.ldap.conf*

**Figura 4-42 Samba – OpenLDAP**

```
# This file is automatically updated by ldapsync -- please do not edit.
passdb backend = ldapsam:ldap://127.0.0.1
ldap admin dn = cn=manager,cn=internal,dc=ppa,dc=gob,dc=ec
ldap group suffix = ou=Groups,ou=Accounts
ldap idmap suffix = ou=Idmap
ldap machine suffix = ou=Computers,ou=Accounts
ldap passwd sync = no
ldap suffix = dc=ppa,dc=gob,dc=ec
ldap user suffix = ou=Users,ou=Accounts
ldap connection timeout = 8
```

El archivo de configuración de samba deberá especificar el dominio a utilizar en sistemas Windows y la compartición de impresoras y archivos. El archivo de configuración es */etc/samba/smb.conf* (Figura 4-43).

**Figura 4-43 Archivo de configuración Samba**



```
[global]
# Setting password change timeout
passwd chat timeout = 10

# General
netbios name = ServerPPA
workgroup = PPAUIO
server string = ClearOS Enterprise

# Logging
syslog = 0
log level = 1
log file = /var/log/samba/%L-%m
max log size = 0
utmp = Yes

# Network
bind interfaces only = yes
interfaces = lo eth0
smb ports = 139

# Printing
printcap name = /etc/printcap
load printers = Yes

# Security settings
security = user
guest account = guest
#restrict anonymous = 2
```

*4.3.1.1.2. Pruebas*

Las pruebas del servicio de directorio se realizarán con cada uno de los servicios configurados, ya que podrán ser accedidos únicamente los usuarios registrados en el directorio y de acuerdo a sus permisos.

En primer lugar se procederá al ingreso de computadores Windows al dominio del PPA.

- El PPA cuenta con sus computadores con el sistema operativo Windows 7, En la Figura 4-44 se muestra los cambios necesarios en el Regedit para la adhesión de una PC Windows 7 al dominio en Linux.

**Figura 4-44 Cambio en el Regedit de Windows 7**

```
HKLM\System\CCS\Services\LanmanWorkstation\Parameters

DWORD  DomainCompatibilityMode = 1

DWORD  DNSNameResolutionRequired = 0
```

En los computadores se configura el dominio al cual va a ser parte el equipo (Figura 4-45), en cuyo proceso se pedirá el nombre de usuario y contraseña del administrador Windows. Una vez unida la computadora al dominio, ésta se la podrá asignar a usuarios registrados en el directorio.

**Figura 4-45 Configuración del dominio en Windows 7**

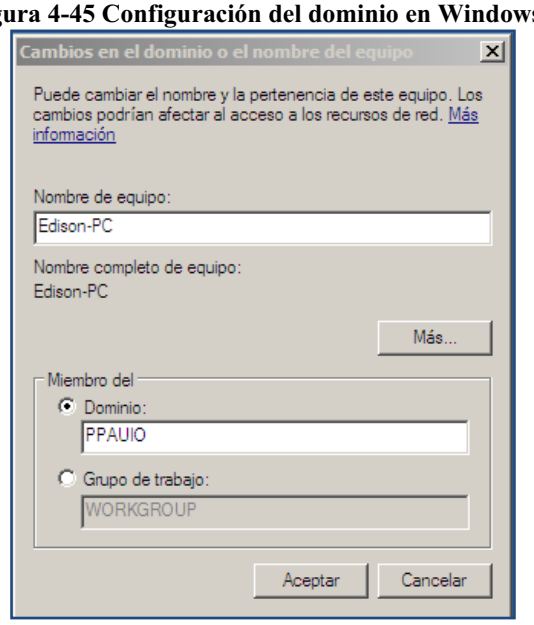
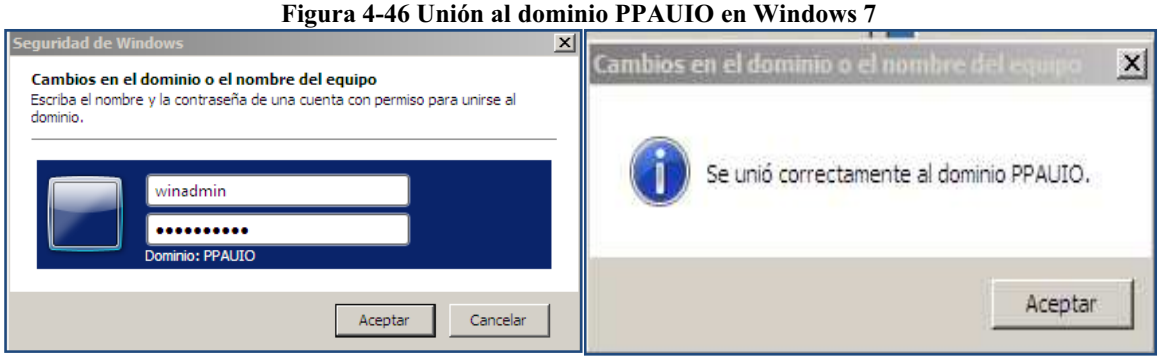
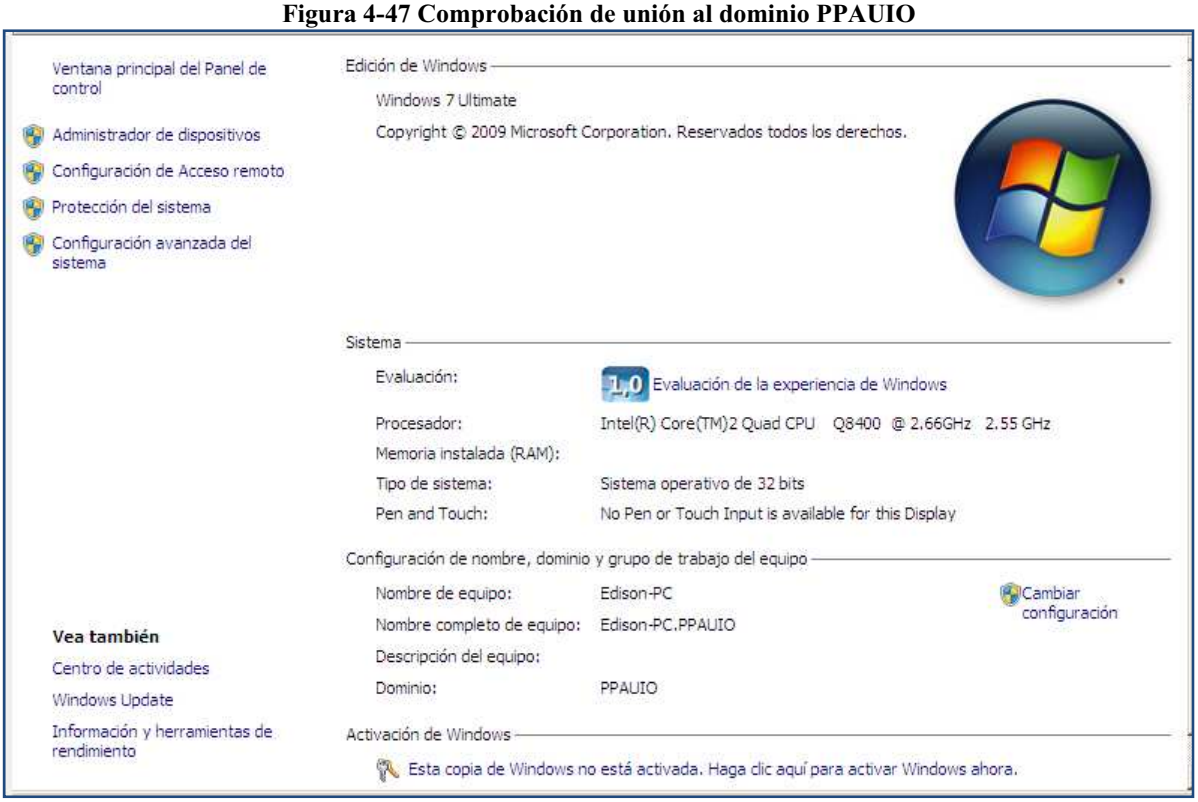



**Figura 4-46 Unión al dominio PPAUIO en Windows 7**



La Figura 4-47 se muestra la comprobación de la unión al dominio PPAUIO de una computadora del PPA.

**Figura 4-47 Comprobación de unión al dominio PPAUIO**




#### 4.3.1.2. Servidor DHCP y DNS

El servicio de DHCP será configurado para la asignación dinámica de direcciones red a computadores y portátiles, mientras que a servidores y equipos de conectividad se les asignará direcciones estáticas.

##### *4.3.1.2.1. Configuración*

El servicio de DHCP será configurado como autoritativo, el cual será el servidor maestro en el caso de existir otro servicio de DHCP, además asignará direcciones IP a equipos que no se encuentren necesariamente en el dominio, como es el caso de laptops de visitantes.

En la Figura 4-8 se observa la interfaz de configuración del servidor de DHCP, el cual entregará la dirección IP, máscara de red, puerta de enlace, DNS primario, DNS secundario.

**Figura 4-48 Configuración del servicio de DHCP**


En la Figura 4-49 se muestra el archivo de configuración del servicio de DHCP, el cual se encuentra en /etc/dnsmasq/dhcp.conf

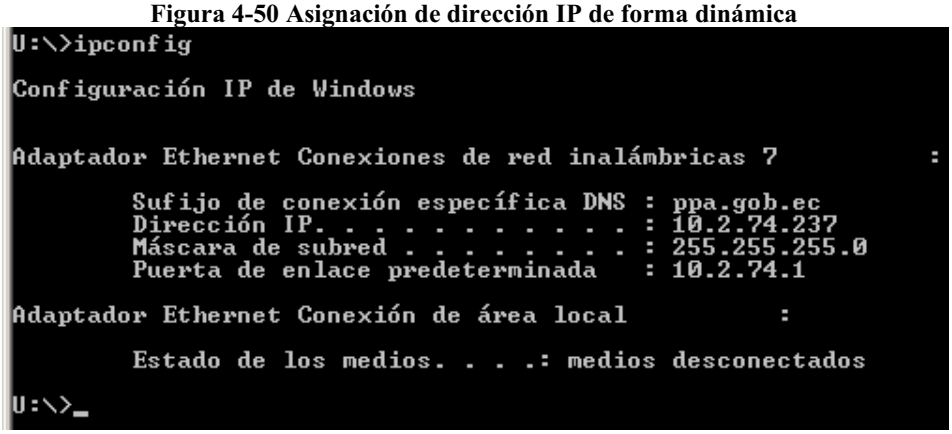
**Figura 4-49 Configuración DHCP**

```
dhcp-option=eth0,1,255.255.255.0
dhcp-option=eth0,28,10.2.74.255
dhcp-option=eth0,3,10.2.74.1
dhcp-option=eth0,6,10.2.70.11
dhcp-range=eth0,10.2.74.100,10.2.74.254,24h
read-ethers
```

*4.3.1.2.2. Pruebas*

En la Figura 4-50 se muestra la conexión de una portátil de forma inalámbrica a través de DHCP a la red LAN.

**Figura 4-50 Asignación de dirección IP de forma dinámica**



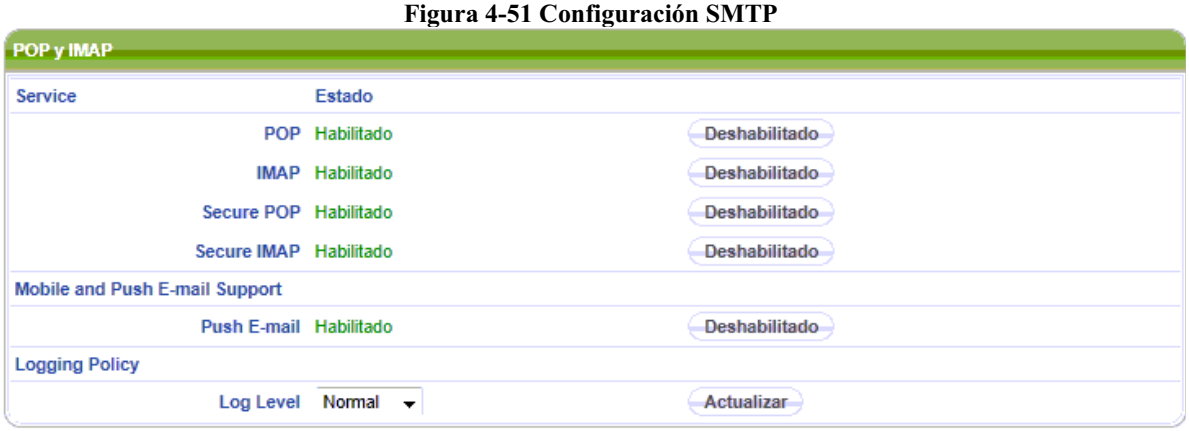

#### 4.3.1.3. Servidor de correo electrónico y Webmail

El servidor de correo electrónico se instala en la distribución ClearOS a través de Postfix, de la misma manera se instala el servicio de Webmail a través de Horde, los cuales son Software Libre. El servicio de correo electrónico además deberá estar resguardado ante virus, spam y demás amenazas electrónicas.

##### *4.3.1.3.1. Configuración*

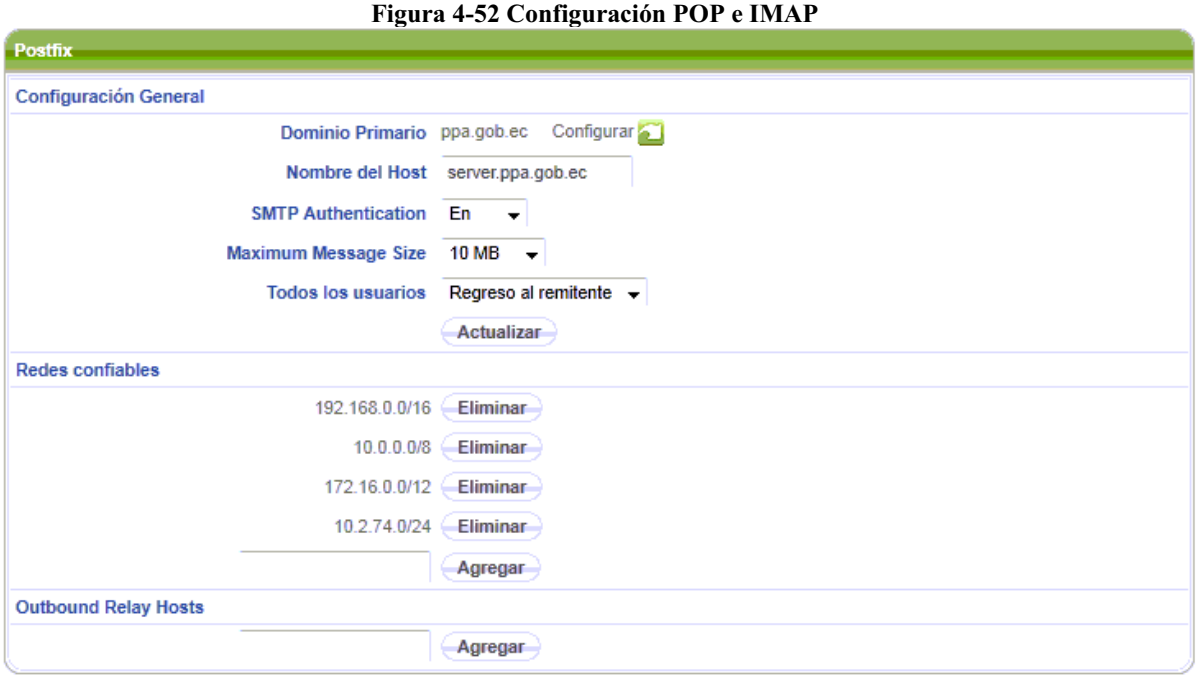
La Figura 4-51 se muestra la configuración del servidor SMTP, en el cual se configurará el dominio de la red, nombre de host, tipo de autenticación y el tamaño máximo del correo. Se especificará las redes LAN confiables que harán uso del servicio.

**Figura 4-51 Configuración SMTP**



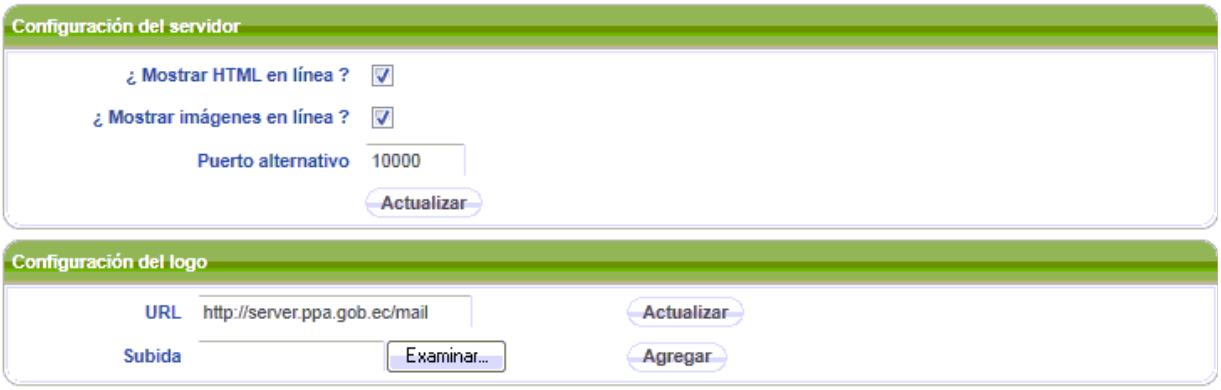

La Figura 4-52 muestra la configuración del servicio de entrega de correo electrónico donde se tiene la posibilidad de configurar tanto POP e IMAP a través de Dovecot.

**Figura 4-52 Configuración POP e IMAP**




La Figura 4-53 muestra la configuración del servicio de Webmail, donde se configura con Horde el puerto por el cual escuchará el servidor y su URL.

**Figura 4-53 Configuración Webmail**

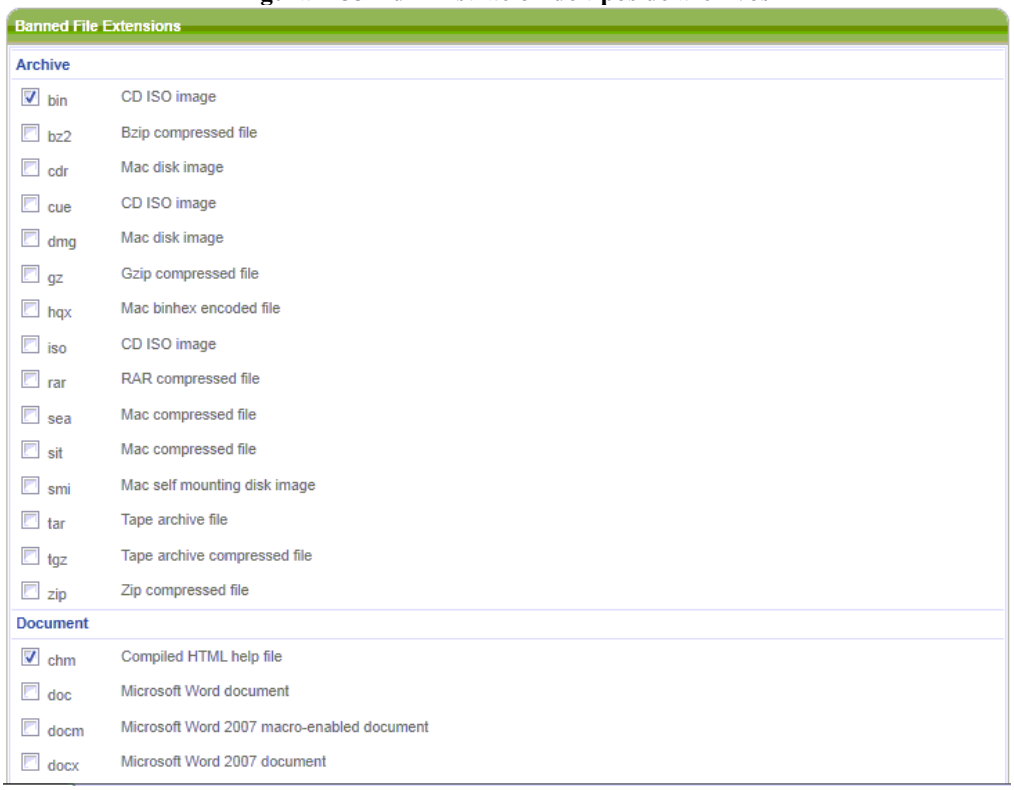



Además se tiene la posibilidad de configurar alias para usuarios o grupos de usuarios.

El servidor será configurado para el chequeo de virus y de archivos con formatos no permitidos, de acuerdo a las políticas del PPA.

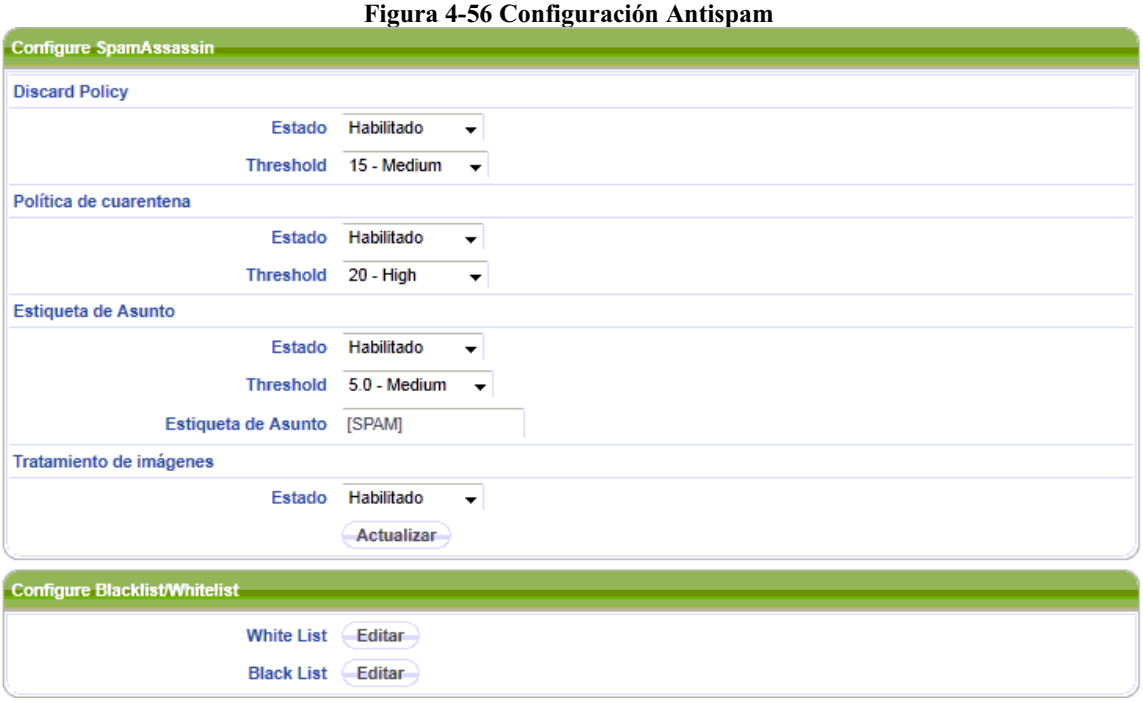
**Figura 4-54 Políticas de detección de virus**


**Figura 4-55 Administración de tipos de archivos**




La Figura 4-56 muestra la configuración del servicio de *Antispam*, el cual es configurado a través de *SpamAssassin*, donde se configura las políticas de cuándo considerar a un número de archivos como *spam*, y se configura políticas de cuarentena. Además se tiene la posibilidad de la creación de listas blancas y negras, las cuales se configurarán de acuerdo requerimientos del PPA.

**Figura 4-56 Configuración Antispam**




#### *4.3.1.3.2. Pruebas*

Una vez configurado el servicio de correo electrónico es necesario la revisión del estado de los servicio a través de línea de comandos. La Figura 4-57 muestra el archivo de configuración de *Postfix* "*/etc/postfix/main.cf*" en donde deberá encontrarse configurado el nombre de host, dominio y la red LAN.

**Figura 4-57 Archivo de configuración Postfix**

```
key.pem            postgrey_whitelist_clients
[root@server postfix]# vi main.cf

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
#mydomain = domain.tld
mydomain = ppa.gob.ec

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
#
# For the sake of consistency between sender and recipient addresses,
# myorigin also specifies the default domain name that is appended
# to recipient addresses that have no @domain part.
#
#myorigin = $myhostname
#myorigin = $mydomain
myorigin = $mydomain
```

La Figura 4-58 muestra las pruebas del servicio entre el cliente de correo Outlook y Webmail, se utilizará dos cuentas de usuarios registrados en el directorio.

**Figura 4-58 Correo: Envío de correo electrónico**

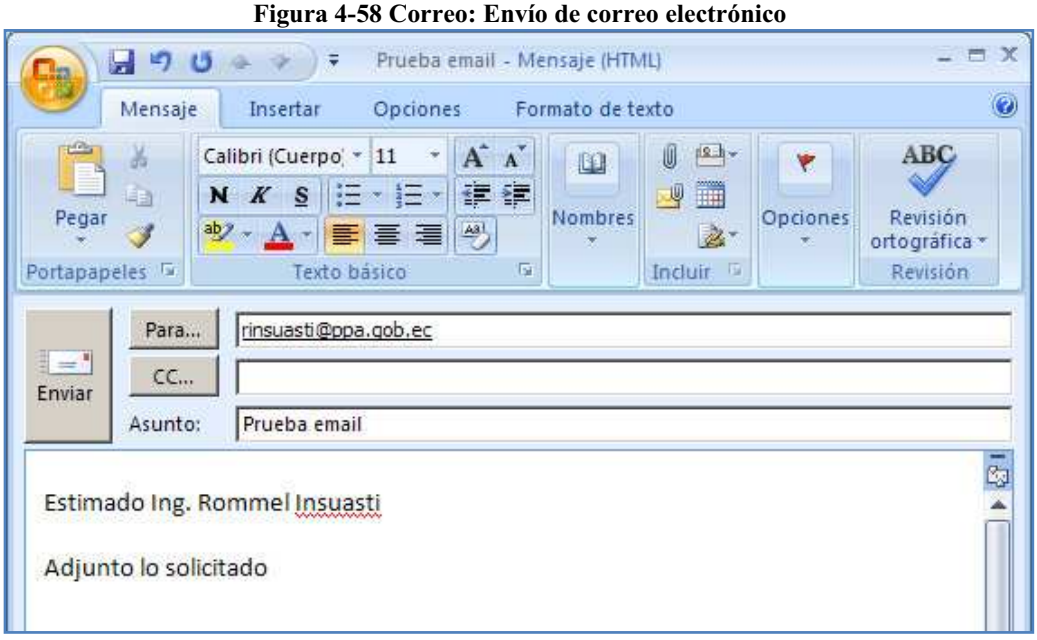
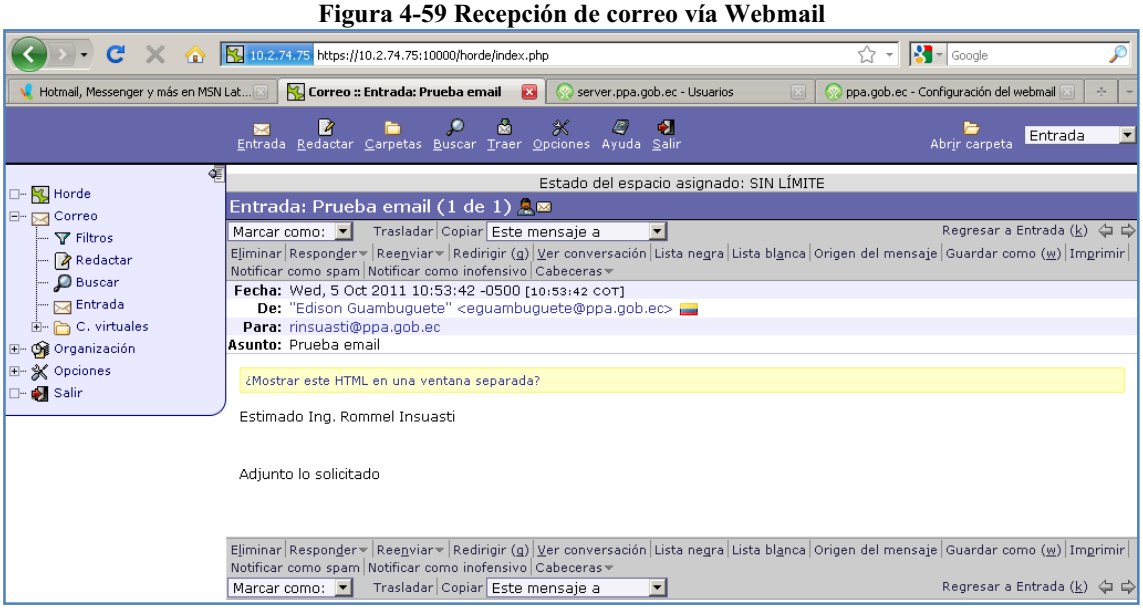


**Figura 4-59 Recepción de correo vía Webmail**



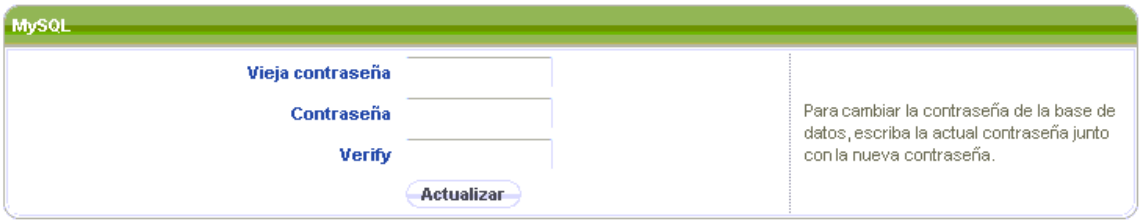

#### 4.3.1.4. Servidor de Base de Datos

La distribución ClearOS permite la instalación del servicio de Base de Datos a través de MySQL.

##### *4.3.1.4.1. Configuración*

La distribución ClearOS permite la instalación del servicio de Base de Datos a través de MySQL.

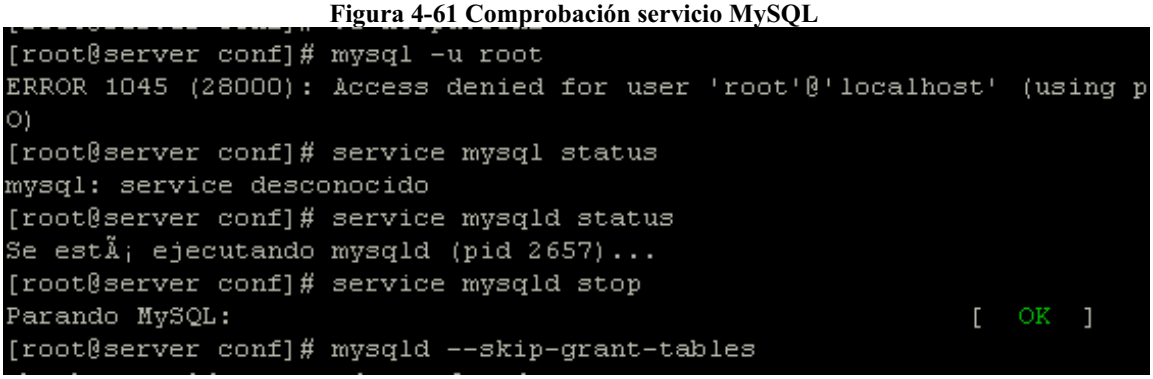
**Figura 4-60 Configuración contraseña MySQL**




##### *4.3.1.4.2. Pruebas*

La Figura 4-61 muestra el estado del servicio "mysqld service status" y se verifica el cambio de usuario y contraseña, ya que con el usuario "*root*" ya no es posible el ingreso a la base de datos.

**Figura 4-61 Comprobación servicio MySQL**




#### 4.3.1.5. Servidor FTP

El servicio de FTP permitirá la compartición de archivos en el PPA, el cual suplirá a los archivos compartidos en Windows con los que actualmente trabajan sus funcionarios. El acceso al servicio FTP será controlado desde el servicio de directorio.

##### *4.3.1.5.1. Configuración*

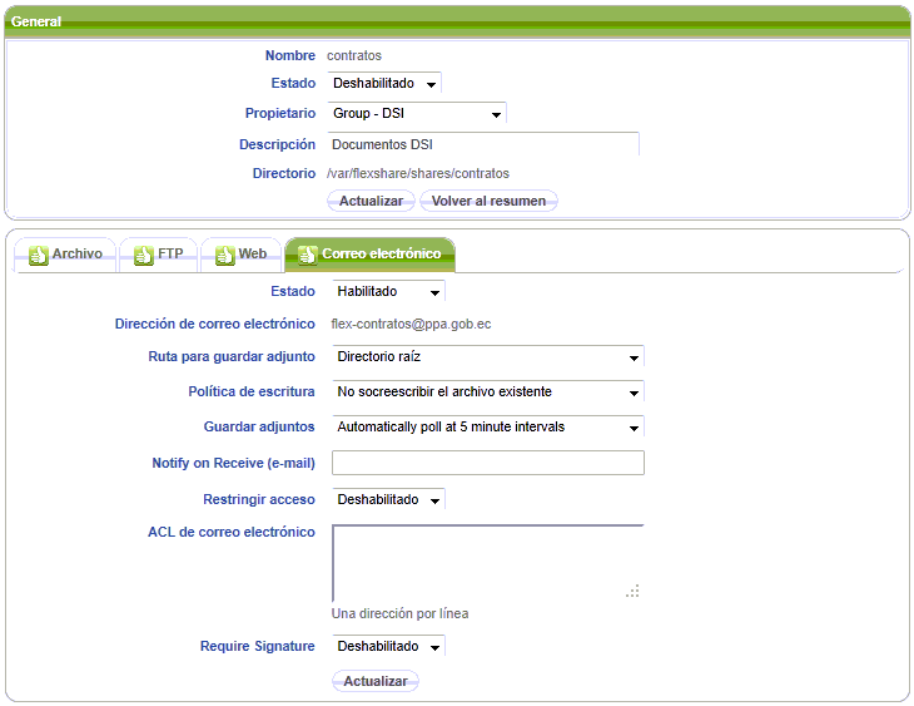
El servicio de FTP permitirá la compartición de archivos en el PPA, el cual suplirá a los archivos compartidos en Windows con los que actualmente trabajan sus funcionarios. El acceso al servicio FTP será controlado desde el servicio de directorio. El servicio de FTP será realizado a través de *Flexshares* que son archivos de colaboración seguros los cuales son accedidos vía Web, FTP, Archivos compartidos o vía email.

La Figura 4-62 muestra la interfaz gráfica para la configuración de las instancias máximas del servicio, el nombre del servidor y el puerto por el cual va a escuchar las peticiones FTP.

**Figura 4-62 Configuración servicio FTP**


La Figura 4-63 muestra la configuración de los archivos compartidos FTP.

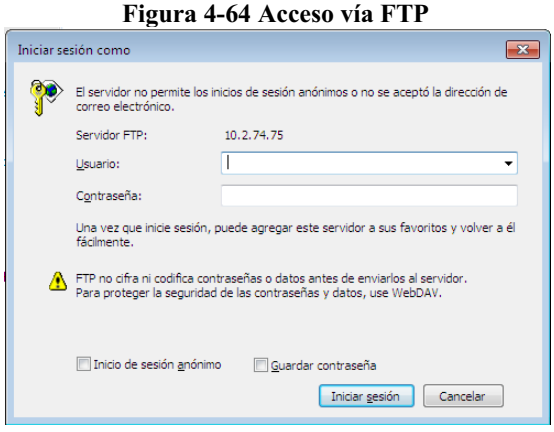
**Figura 4-63 Configuración de archivos compartidos**




#### *4.3.1.5.2. Pruebas*

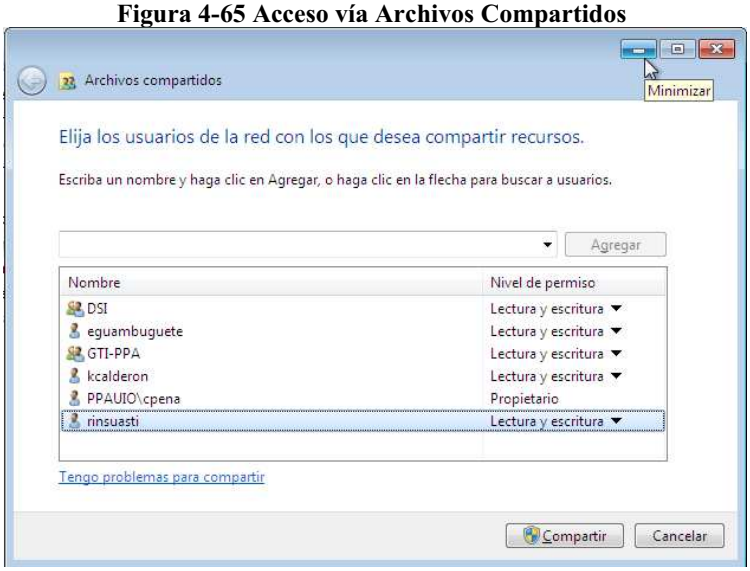
A los archivos flexshare se tendrá acceso desde clientes FTP, siempre y cuando se les haya dado los permisos respectivos de ingreso y se encuentren registrados en el directorio (Figura 4-64).

**Figura 4-64 Acceso vía FTP**



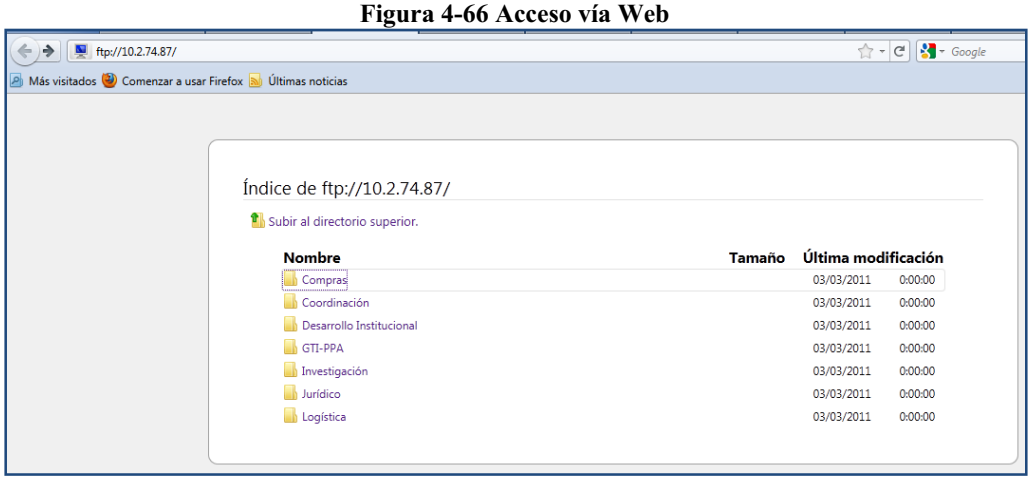

EN la Figura 4-65 se observa el acceso a través de archivos compartidos en donde se podrá compartir archivos entre los usuarios del dominio (PPAUIO).

**Figura 4-65 Acceso vía Archivos Compartidos**




En la Figura 4-66 se muestra el acceso a través de archivos compartidos vía web.

**Figura 4-66 Acceso vía Web**




A través de línea de comandos se puede observar que los archivos compartidos se encuentran en */var/flexshare/shares/configuración*.

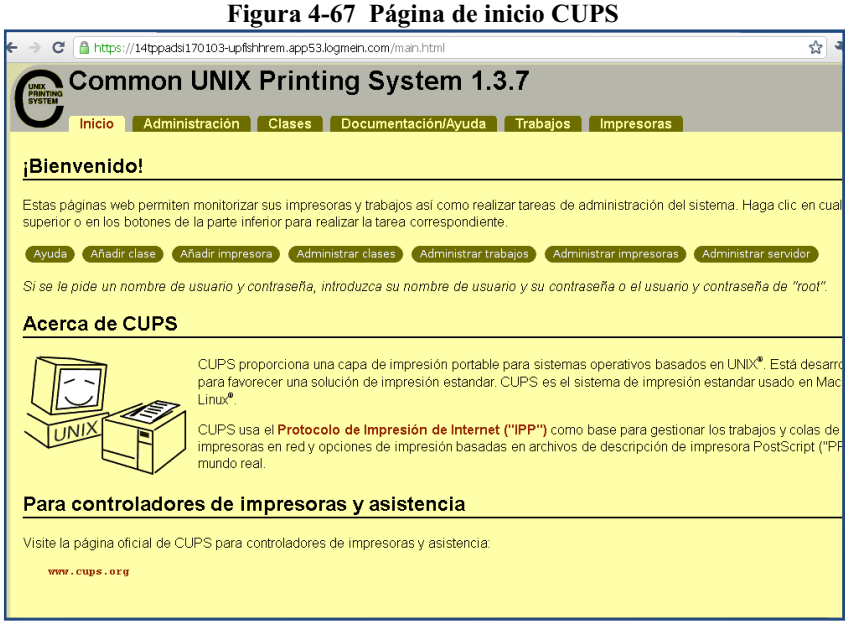
#### 4.3.1.6. Servidor de impresión

El servicio de impresión será configurado a través de CUPS (Sistema de Impresión Común de Unix), el cual permitirá compartir impresoras en la red del PPA. Además se contará con una administración centralizada de dichos dispositivos

#### *4.3.1.6.1. Configuración*

La Figura 4-67 muestra la interfaz gráfica desde dónde se realiza tanto la configuración como la administración del sistema vía Web. Cups convierte el host donde se ejecute como servidor de impresión, es decir que las los usuarios del dominio envían sus documentos a imprimir como requerimiento al servidor y éste es el que procesa la petición y lo envía a la impresora respectiva.

**Figura 4-67 Página de inicio CUPS**

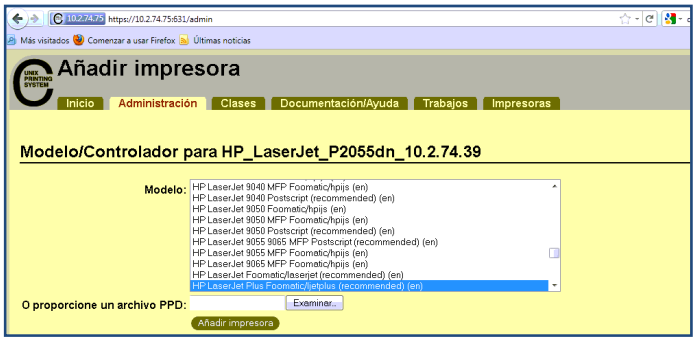



La Figura 4-68 muestra las impresoras conectadas al servidor e impresoras remotas, las cuales son añadidas al sistema junto a su controlador para ser administradas.

**Figura 4-68 Impresoras disponibles**


La Figura 4-69 muestra los controladores añadidos al sistema.

**Figura 4-69 Controladores de Impresoras**




#### *4.3.1.6.2. Pruebas*

El administrador del sistema tendrá la opción de gestionar el uso de las respectivas impresoras pudiendo detenerlas, rechazar trabajos, gestionar a los usuarios permitidos, etc. La Figura 4-70 muestra una impresora añadida al sistema.

**Figura 4-70 Impresora registrada en el sistema**


**Figura 4-71 Impresiones realizadas**

#### 4.3.1.7. Servidor Web

El servidor web será configurado a través de Apache web server, en el cual se encontrará la página web del PPA, la cual será la imagen del Programa ante el mundo, en la actualidad es únicamente informativa, por lo cual GTI-PPA se encuentra diseñando una página en la cual se pueda realizar consultas de los diferentes procesos de comprar de acuerno a la ley de transparencia.

##### *4.3.1.7.1. Configuración*

El servicio de página web deberá ser seguro a través de SSL/TLS, además de tener instalado y soporte para PHP y MySQL.

La Figura 4-72 muestra la habilitación de SSL para el servicio de página web, así como la configuración de host virtual.

**Figura 4-72 Configuración Página Web**


##### *4.3.1.7.2. Pruebas*

La Figura 4-73 muestra el archivo de configuración de del servicio http, el mismo que se encuentra en */etc/httpd/conf/httpd.conf* donde direcciona a la página web a */var/www/html*. La página web del PPA se encontrará ubicada en */ppaweb* por lo cual el archivo será modificado para su respectiva ubicación.

**Figura 4-73 Archivo de configuración http**

```
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#

#DocumentRoot "/var/www/html"
DocumentRoot "/ppaweb"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
<Directory />
    Options FollowSymLinks
    AllowOverride None
```

**Figura 4-74 Página web en el servidor 10.2.74.75**

### 4.3.2. INSTALACIÓN Y CONFIGURACIÓN DE LA SEGURIDAD PERIMETRAL

La seguridad perimetral de la infraestructura de red del PPA se la realizará a través del UTM Cisco SA 540 de la línea Small Business.

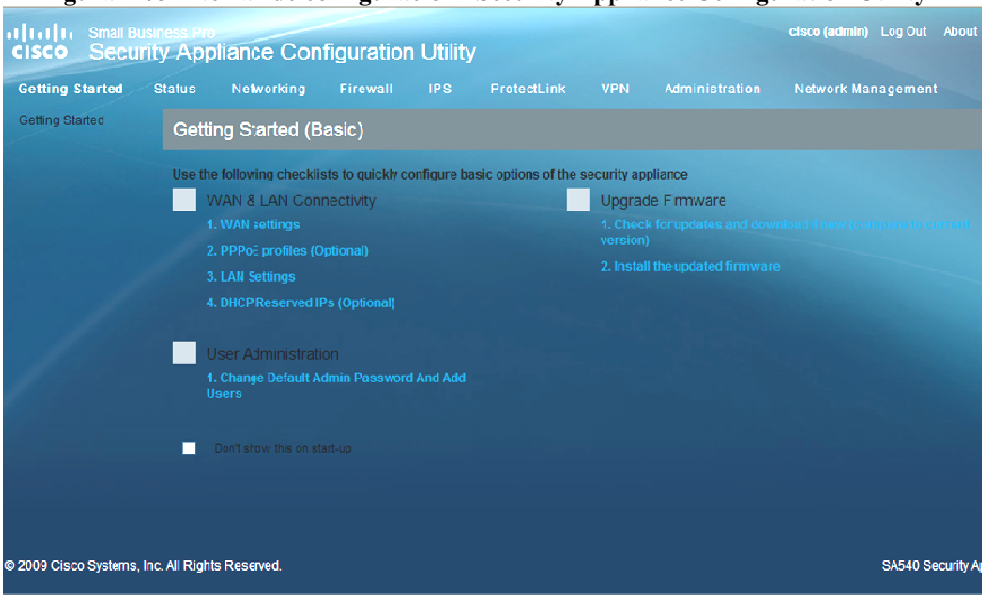
Las funciones del UTM Cisco SA 540 son:

- Firewall
- Sistema de Prevención de Intrusiones
- Capacidad de doble conexión WAN
- Protección contra virus, software espía, correos electrónicos no deseados y suplantaciones de identidad.
- Filtrado de contenido web y filtrado URL
- VPN con SSL para acceso remoto seguro

#### *4.3.2.1.1. Configuración*

La Figura 4-75 muestra la interfaz de configuración y administración del UTM, la cual se la realiza vía web a través de la aplicación integrada ¨*Security Appliance Configuration Utility*¨.

**Figura 4-75 Interfaz de configuración "Security Appliance Configuration Utility"**



En primer lugar de deberá cambiar la configuración de nombre de usuario y contraseña del equipo. El proceso de configuración de la seguridad perimetral es el siguiente.

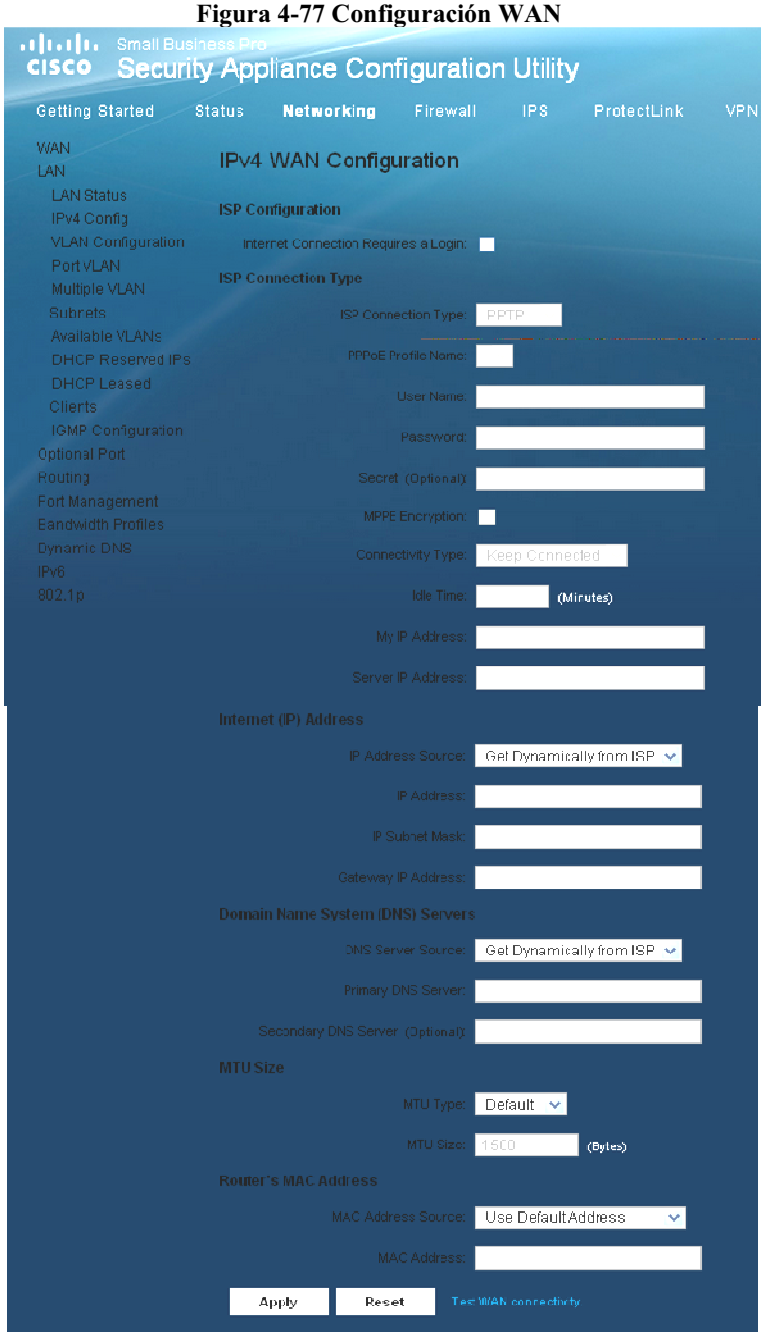
- Configuración LAN.- la dirección IP configurada en el extremo LAN será el Gateway de la red del PPA, la cual será configurada de forma estática. El equipo tiene la posibilidad de trabajar como servidor DHCP, la cual no será habilitada debido a que dicho servicio ya fue previsto en el servidor de comunicaciones (Figura 4-76).

**Figura 4-76 Configuración del Gateway LAN**


- Configuración WAN.- la configuración del enlace WAN dependerá en gran parte del tipo de conexión con el ISP, se deberá especificar si la conexión es PPTP, PPPoE o L2TP en cuyo caso se deberá ingresar el nombre de usuario y contraseña (Figura 4-77).

  En este caso se configurará para que el direccionamiento IP (dirección IP, máscara de red, Gateway y DNS) sea asignado por el DHCP de forma dinámica.

**Figura 4-77 Configuración WAN**




- Redundancia WAN.- el requerimiento de enlace redundante a Internet se lo realizará configurando el puerto opcional del equipo, al cual también se lo puede utilizar como DMZ (Figura 4-78).

**Figura 4-78 Configuración enlace redundante a Internet**


- Configuración NAT (*Network Address Traslation*).- que permita la conexión a Internet a través de una dirección IP pública (Figura 4-79).

**Figura 4-79 Configuración NAT**

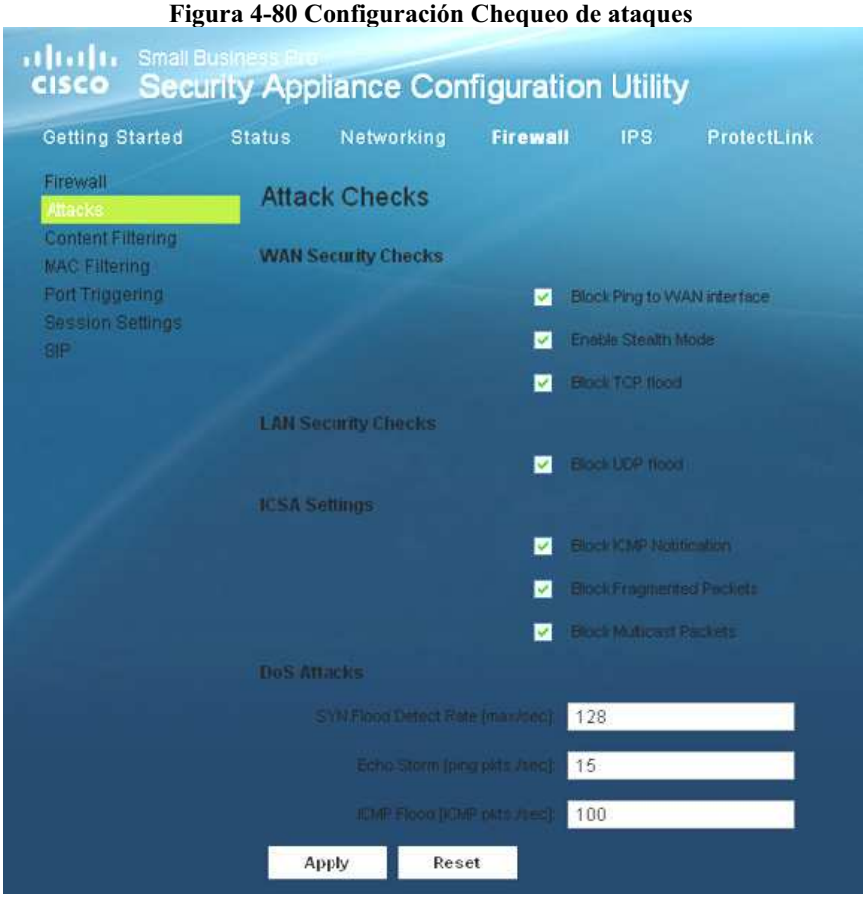

- Las reglas de firewall deberán ser realizadas de acuerdo al análisis de riesgo de la información realizada en el diseño, las cuales deberán ser proporcionadas por GTI-PPA.

  Se configurará el tipo de ataques que se deberán evitar (Figura 4-80).

  - Bloqueo de ping a la interfaz WAN que prevendrán ataques de descubrimiento de red a través de ICMP Echo request.
  - Se evitará que la interfaz WAN sea susceptible a escaneo de puertos habilitando el Modo Invisible que eviten el descubrimiento de la red.

- Se descartará paquetes TCP inválidos que protejan a la red de ataques “SYN flood” que consiste en el envío sucesivo de requerimientos de sincronización a la interfaz de red.
- Se verificará que el equipo de seguridad tenga la certificación “ICSA Firewall” de ICSA Labs, la cual se encarga de realizar pruebas de productos de seguridad informática y establece normas de seguridad de antivirus, firewalls y productos de protección contra espías.
- Se configurará el número máximo de paquetes de sincronización “SYN” por segundo que permita determinar que un ataque “*SYN Flood*” está ocurriendo, además se configurará el número máximo de pings y paquetes ICMP por segundo que determine que un ataque “*Echo storm*” o “*ICMP Flood*” está ocurriendo.

**Figura 4-80 Configuración Chequeo de ataques**



- Las opciones de filtro de contenido web y filtro URL serán configuradas de acuerdo a los requerimientos del Programa, los cuales serán proporcionados por GTI-PPA (Figura 4-81).

**Figura 4-81 Filtro URL**


- Se configurará VPNs que permitan tener acceso remoto a los recursos de la red según las políticas y permisos dados por GTI-PPA.

  El equipo de seguridad permite la configuración de los siguientes escenarios de VPN:

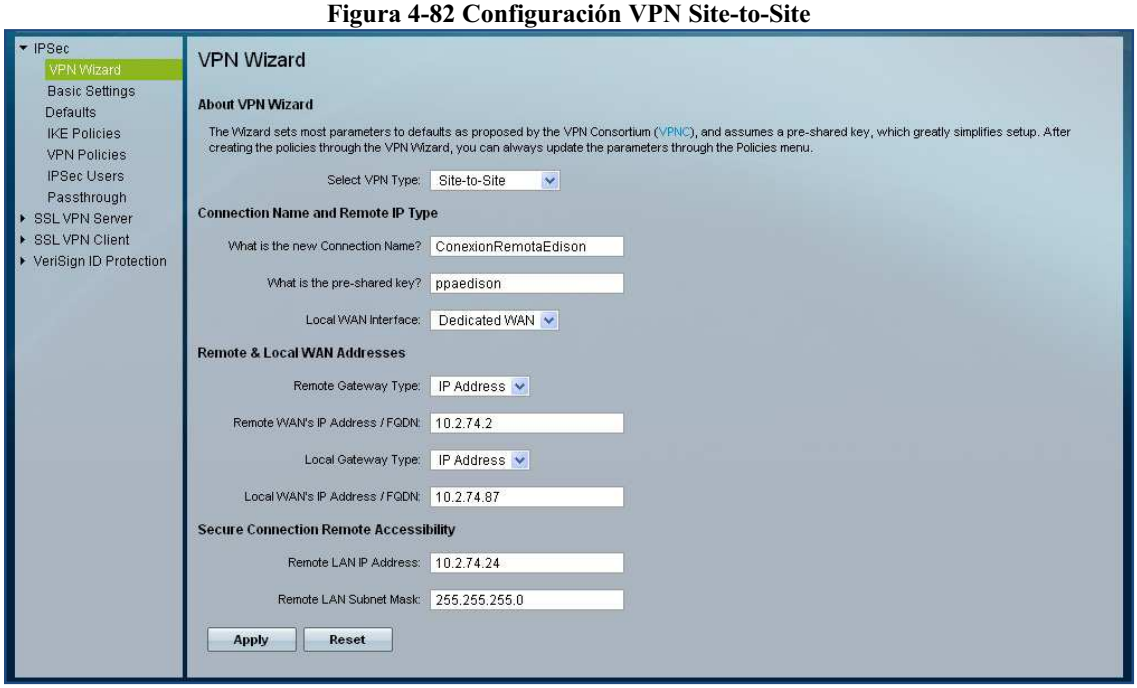
  **Site-to-Site VPN**.- en el cual la VPN conecta dos routers y garantiza la seguridad del tráfico entre los dos sitios físicamente separados.

  **Acceso Remoto con IPSec VPN**.- en el cual el usuario remoto usa un cliente VPN para acceder a la red.

  **Acceso Remoto vía Web**.- en el cual el usuario remoto usa un navegador web para iniciar un túnel VPN y acceder a los servicios de la red.

La Figura 4-82 muestra la configuración de un enlace VPN Site-to-Site

**Figura 4-82 Configuración VPN Site-to-Site**




#### *4.3.2.1.2. Pruebas*

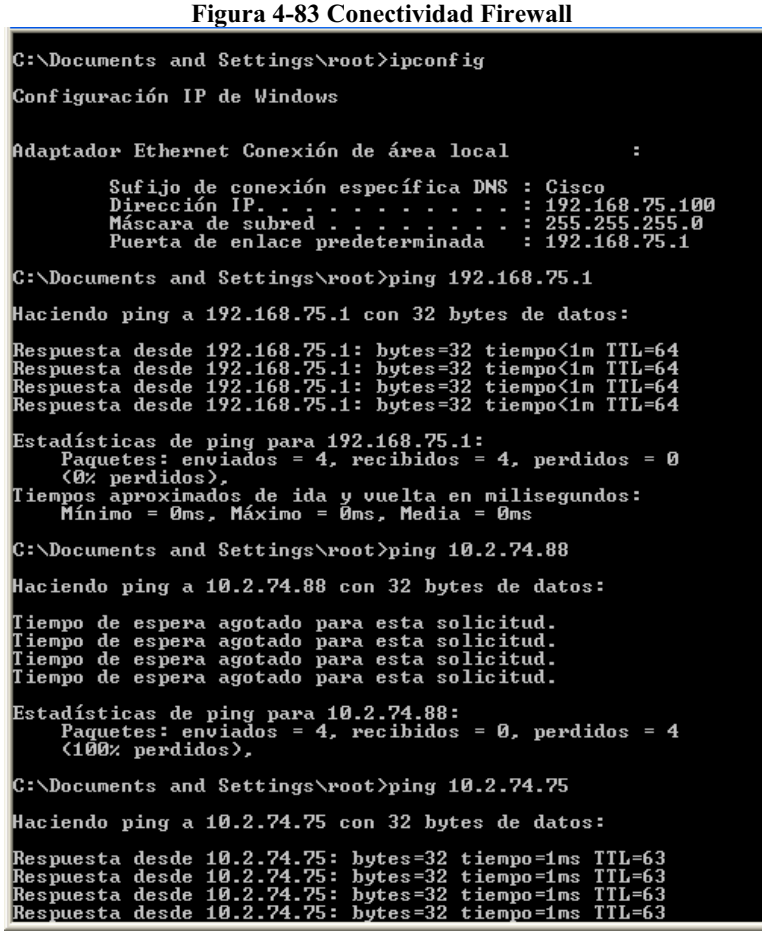
Las pruebas de sistema de seguridad perimetral se lo realizó en un ambiente de pruebas en el cual el direccionamiento IP es el siguiente:

- Red LAN :192.168.75.0/24; Gateway: 192.168.75.1
- Red WAN: 10.2.74.0/24

La Figura 4-83 muestra el acceso a la red local desde la red WAN:

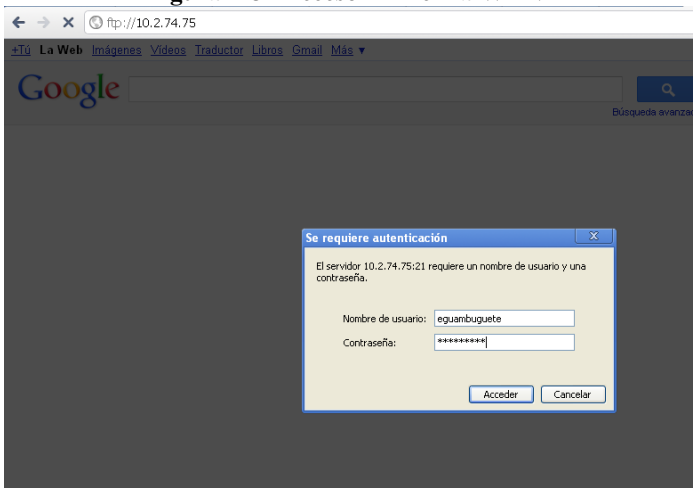
- La dirección IP de un usuario LAN (192.168.75.100).
- El ping al Gateway (192.168.75.1)
- El ping a la interfaz WAN del firewall (10.2.74.75)
- El ping al extremo de la WAN (10.2.74.75).

**Figura 4-83 Conectividad Firewall**



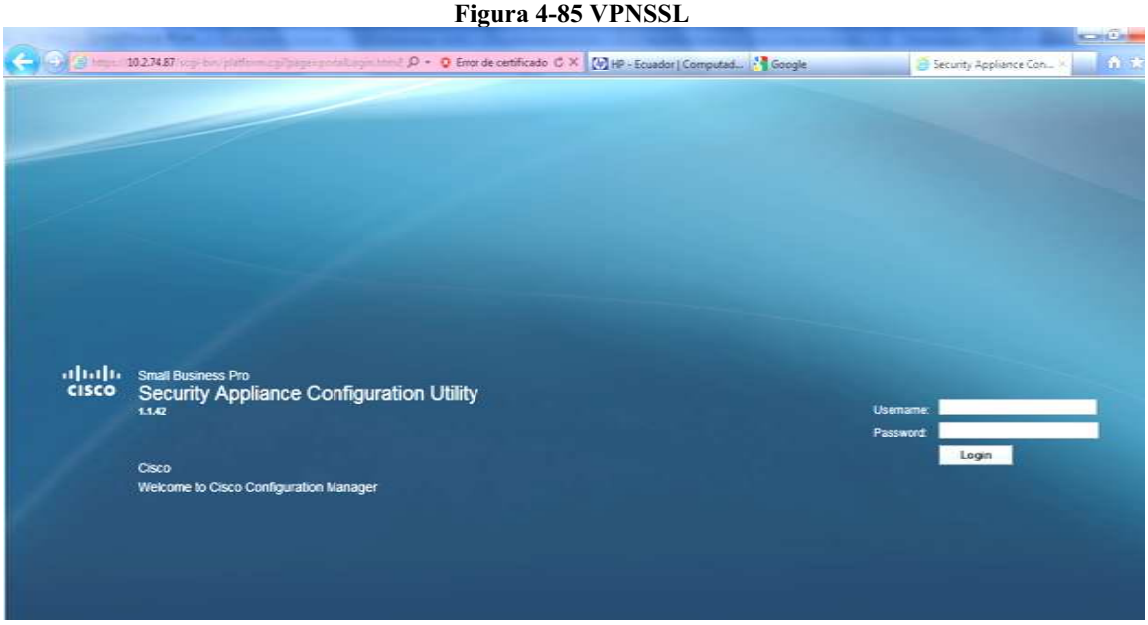

La Figura 4-84 muestra el acceso ftp desde la red LAN al servidor 10.2.74.75 ubicado en la WAN.

**Figura 4-84 Acceso FTP en la WAN**



La Figura 4-85 muestra una VPN SSL que permite el acceso remoto a un servicio de la red a través de un navegador web, en este caso el servicio es la administración remota del UTM a través de su interfaz WAN (10.2.74.87).

**Figura 4-85 VPNSSL**



# CAPÍTULO V

# 5. COSTO REFERENCIAL DE LA SOLUCIÓN

## 5.1. INTRODUCCIÓN

Uno de los aspectos sumamente importantes a la hora de implementar un proyecto TIC es saber el costo de la solución que permita planificar los gastos respectivos al área financiera.

Luego de realizado el diseño de la infraestructura de red convergente de voz, datos y video se realizará el costo referencial de la solución de acuerdo a los equipos y servicios elegidos en el diseño.

Los costos de cada uno de los equipos, servicios, aplicaciones con sus respectivas garantías y soporte técnico serán divididos en costos recurrentes y no recurrentes que permitan conocer el gasto inicial que deberá realizar el PPA para la puesta en marcha de la infraestructura de red, así como del costo que conlleva el mantenimiento y soporte de los mismos.

## 5.2. COSTO REFERENCIAL

El costo referencial de la solución viene dado por los costos de diseño, implementación, monitoreo y mantenimiento y de los diferentes sistemas de la infraestructura de comunicaciones, los cuales en conjunto determinarán el costo total de la solución.

### 5.2.1. SISTEMA DE CABLEADO ESTRUCTURADO

Si bien el SCE se base en normas y estándares es necesaria la instalación de todo el sistema mediante una sola marca, debido principalmente a las garantías que debe extender el oferente por parte de la marca del cableado. Se entregará una sola garantía para todo el SCE no para cada elemento.

El ser un SCE monomarca no impide realizar futuros cambios, adiciones o modificaciones del sistema con otra marca, siempre y cuando cumpla con las respectivas normas de cableado estructurado.

La contratación del proyecto de implementación del SCE se lo realizó a través del INCOP en un proceso de mínima cuantía, en el cual participan aquellas empresas que cumplan con los requerimientos técnicos, administrativos y presupuestarios exigidos por la empresa contratante, en este caso el PPA

En los procesos de mínima cuantía se debe realizar los pliegos con los requerimientos técnicos a exigir y el presupuesto de la institución para el proyecto. El presupuesto para el proyecto del SCE se lo realizó en base a cotizaciones realizadas por varias empresas, entre las cuales se encuentran las participantes (Anexo 5.1).

Los costos referenciales de los diferentes materiales, equipos, mano de obra y certificación del Sistema de Cableado Estructura se detallan en la Tabla 5-1 y 5-2.

**Tabla 5-1 Costos: Punto de cableado estructurado**

| PUNTO DE CABLEADO ESTRUCTURADO | | | | |
|---|---|---|---|---|
| **DESCRIPCION** | **UNIDAD** | **CANTIDAD** | **VALOR UNITARIO** | **VALOR TOTAL** |
| Cable UTP categoría 6A | metros | 21.12 | 2.00 | 42.20 |
| Tubería EMT metálica sobre techo falso | metros | 25 | 2.00 | 50.00 |
| Canaleta plástica | metros | 2 | 1.50 | 3.00 |
| Cajetín Rectangular | unidad | 1 | 4.00 | 4.00 |
| Face plate | unidad | 1 | 3.00 | 3.00 |
| Jack categoría 6A | unidad | 1 | 11.00 | 11.00 |
| Patch cord categoría 6A de 3 pies | unidad | 1 | 8.00 | 8.00 |
| Patch cord categoría 6A de 7 pies | unidad | 1 | 15.00 | 15.00 |
| Certificación | unidad | 1 | 7.00 | 7.00 |
| Mano de obra | unidad | 1 | 15.00 | 15.00 |
| Misceláneos (tacos, tornillos, accesorios de canaletas) | global | 1 | 5.00 | 5.00 |
| | | | **TOTAL** | **163.24** |

**Tabla 5-2 Costos: Sistema de Cableado Estructurado**

| TOTAL CABLEADO ESTRUCTURADO | | | | |
|---|---|---|---|---|
| | | | | |
| **DESCRIPCION** | **UNIDAD** | **CANTIDAD** | **PRECIO UNITARIO** | **PRECIO FINAL** |
| Puntos de red CAT 6A UTP material, mano de obra, Certificación | punto | 54 | 163.20 | 8815.00 |
| Rack sala de equipos (equipado de acuerdo a especificaciones técnicas, normas y estándares vigentes) | unidad | 1 | 2,000.00 | 2000.00 |
| Cableado vertical | unidad | 1 | 300.00 | 300.00 |
| Acometida de E1 Telefonía y E1 Internet del tablero principal del edificio al rack piso 4 | metros | 80 | 12.00 | 960.00 |
| | | | **SUBTOTAL** | **12075.00** |
| | | | **IVA** | **1449.00** |
| | | | **TOTAL** | **13524.00** |

De las empresas participantes, las que cumplían todos los requerimientos técnicos, administrativos y presupuestarios fueron “COMERCIO & INGENIERIA CIA. LTDA” y “H4 INGENIERÍA ELÉCTRICA”. La contratación por mínima cuantía establece que en el caso de haber un empate técnico se debe hacer la elección a través de sorteo, de cuyo proceso la empresa favorecida fue “COMERCIO & INGENIERÍA CIA. LTDA”, la cual trabaja con la marca AMP NETCONNECT de TYCO ELECTRONICS LTDA.

Cabe mencionar que en los pliegos no se especificó la marca de ninguno de los elementos del SCE, ya que es prohibido por la ley y no es una característica para la elección de la empresa ganadora.

El Sistema de Cableado Estructurado tendrá un costo de alrededor de 12000 dólares americanos, en el que incluirán garantías de productos, mano de obra. Este presupuesto fue aceptado y justificado por “COMERCIO & INGENIERIA CIA. LTDA”.

La solución completa del SCE tiene una garantía extendida de 25 años sobre los productos manufacturados por AMP NETCONNECT ofrecidos a través de su canal integrador Comercio & Ingeniería Cía. Ltda (Anexo 5.2).

Comercio & Ingeniería Cía. Ltda. garantiza por 3 años la mano de obra y dirección técnica utilizada para la ejecución con personal con experiencia en proyectos similares y capacitados en la marca AMP NETCONNECT (Anexo 5.2).

EL costo total de la solución incluye el servicio de soporte técnico y mantenimiento correctivo del SCE por un período de 3 años, donde el tiempo de respuesta será en el esquema 8x5x2 (8 horas laborables, 5 días de la semana, 2 horas de respuesta).

Las garantías de productos, mano de obra y soporte técnico no cubrirán daños ocasionados por desastres naturales, incendios e inundaciones.

En el diseño se estableció la utilización de un sistema ininterrumpido de de energía (UPS) cuya potencia de salida debe ser de 15 KVA. El UPS fue cotizado por “PC.Networks” los cuales cotizaron dos de 20 KVA y uno de 15 KVA (Anexo 5.3).

De la propuesta ofrecida por Pc.Networks se eligió el USP de 15 KVA. El costo del UPS se detalla en la Tabla 5-3.

**Tabla 5-3 Cotos: UPS**

| PRESUPUESTO: UPS | | | | |
|---|---|---|---|---|
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| UPS DELTA 100 SERIES 15KVA Tecnologia ON LINE | Sistema: Ininterrumpido SAI-UPS<br>Tecnologia: True On Line Doble Conversion Onda senoidal pura<br>Potencia: 2-15KVA<br>Tiempo de Autonomia: 10 minutos | 1 | 8500.00 | 8500.00 |
| | | | **SUBTOTAL** | 8500.00 |
| | | | **IVA** | 1020.00 |
| | | | **TOTAL** | **9520.00** |

El UPS de 15 KVA tendrá un costo aproximado de 8500 dólares americanos.

### 5.2.2. RED LAN

El diseño de la red LAN se la realizó a través del modelo jerárquico core, distribución y núcleo, bajo los cuales se eligió equipos de conectividad de acuerdo a las necesidades del PPA.

Para la evaluación de costos se ha requerido la cotización de dos empresas dedicadas al área de *networking partners*[51] de Cisco (Megasupply y Adexus). Al comparar ambas cotizaciones se puede observar que los precios de Adexus son algo elevados debido a su experiencia que la respalda y al soporte de 24x7x4 que brindan mientras que Megasupply ofrece los mismos equipos con soporte 8x5xNBD el cual es suficiente para la puesta en marcha de la infraestructura de red del PPA.

Para la puesta en marcha de la red del PPA se optará por los equipos ofrecidos por Megasupply cuyo soporte deberá ser revisado de forma periódica según la infraestructura de red vaya creciendo y los procesos sean más críticos.

Los costos referenciales de dichos equipos se muestran en la Tabla 5-4.

**Tabla 5-4 Costos: Equipos de Conectividad**

| PRESUPUESTO: EQUIPOS DE CONECTIVIDAD | | | | |
|---|---|---|---|---|
| SWITCHES | | | | |
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| **Switch de Núcleo** | | | | |
| WS-C3560G-24TS-S | Catalyst 3560 24 10/100/1000T + 4 SFP + IPB Image | 1 | 3867.97 | 3867.97 |
| CON-SNT-3560GTS | SMARTNET 8X5XNBD Cat 3560 24 10/100/1000T + 4 SFP St | 1 | 294.59 | 294.59 |
| **Switch de Acceso** | | | | |
| WS-C2960S-24PS-L | Catalyst 2960S 24 GigE PoE 370W, 4 x SFP LAN Base | 1 | 3222.63 | 3222.63 |
| CON-SNT-2960S2PS | SMARTNET 8X5XNBD Catalyst 2960S Stack | 1 | 286.65 | 286.65 |
| WS-C2960S-48FPS-L | Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base | 1 | 6045.97 | 6045.97 |
| CON-SNT-2960S4FS | SMARTNET 8X5XNBD Cat 2960S Stk48 GigE PoE 740W,4xSFP | 1 | 286.65 | 286.65 |

[51] Distribuidor autorizado de Cisco en Ecuador.

Continúa

| | | | | |
|---|---|---|---|---|
| | Base | | | |
| **Servicios** | | | | |
| Configuración | Instalación y configuración de los Equipos | 1 | 2000.00 | 2000.00 |
| Capacitación | Transferencia de conocimientos (4 horas) | 1 | 160.00 | 160.00 |
| Soporte Técnico | Paquete de 30 horas de Soporte Técnico por un año | 1 | 900.00 | 900.00 |
| | | | **SUBTOTAL** | 17064.46 |
| | | | **IVA** | 2047.74 |
| | | | **TOTAL** | **19112.20** |

El sistema de conectividad tendrá un costo de alrededor de 17000 dólares americanos, en el cual se incluye la configuración, capacitación, transferencia de conocimientos y soporte técnico de 30 horas por un año.

Los equipos de conectividad de Cisco presentados cuentan con el servicio Cisco SMARTnet 8x5xNBD (*Next Business Day*) el cual da al PPA acceso al servicio de soporte técnico por parte de profesionales expertos en la marca, da la opción de reemplazo del equipo al siguiente día hábil en caso de fallas, acceso a la base de conocimientos, recursos y herramientas de la página "www.cisco.com" y actualizaciones continuas.

### 5.2.3. RED INALÁMBRICA

El equipo inalámbrico con los requisitos mencionados en el diseño de la red ha sido cotizado por la empresa Megasupply (Anexo 5.3). El costo referencial se detalla en la Tabla 5-5.

**Tabla 5-5 Costos: Access Point**

| PRESUPUESTO: ACCESS POINT | | | | |
|---|---|---|---|---|
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| AP541N-A-K9 | Cisco Small Business Pro AP 541N Wireless Access Point - Wireless access point - 802.11 a/b/g/n (draft 2.0) - external | 2 | 489.21 | 978.42 |

Continúa

| | | |
|---|---|---|
| | **SUBTOTAL** | 978.42 |
| | **IVA** | 117.41 |
| | **TOTAL** | **1095.83** |

La red inalámbrica tendrá un costo de alrededor de 980 dólares americanos.

### 5.2.4. SERVIDOR DE COMUNICACIONES

El servidor elegido en la fase de diseño fue el HP Proliant DL320 cuya serie tiene 3 modelos, las cuales difieren principalmente del número de núcleos del procesador y la memoria cache. El servidor elegido fue el HP ProLiant DL320 G6 L5609.

La Tabla 5-6 muestra los precios de cada uno de los modelos de la serie HP ProLiant DL320. Los precios mostrados se encuentran en la página oficial de HP para Latinoamérica.

**Tabla 5-6[52] Costos (EEUU): Servidor HP ProLiant 320**

| **MODELOS DE LA SERIE HP PROLIANT DL320 G6 SERVER** | | | |
|---|---|---|---|
| **Número de Parte** | 593493-001 | 638328-001 | 593498-001 |
| **Precio** | **$ 1,395.00** | **$ 1,395.00** | **$ 1,785.00** |
| **Descripción** | HP ProLiant DL320 G6 E5503 (1P) | HP ProLiant DL320 G6 E5603 | HP ProLiant DL320 G6 L5609 |
| **Procesador** | Intel® Xeon® E5503 (2 core, 2.00 GHz, 4MB L3, 80W) | Intel® Xeon® E5603 (4 core, 1.60 GHz, 4MB L3, 80W) | Intel® Xeon® L5609 (4 core, 1.16 GHz, 12MB L3, 40W) |
| **Network Controller** | 1 | 1 | 1 |
| **N de procesadores** | 4 GB | 4 GB | 4 GB |
| **Slot memoria** | 9 DIMM slots | 9 DIMM slots | 9 DIMM slots |
| **Tarjeta de red** | (1) 1GbE NC326i 2 Ports | (1) 1GbE NC326i 2 Ports | (1) 1GbE NC326i 2 Ports |
| **Controlador de red** | (1) Smart Array B110i SATA RAID | (1) Smart Array B110i SATA RAID | (1) Smart Array B110i SATA RAID |
| **Power Supply** | (1) 400 Watt Auto-sensing, PFC, CE Mark Compliant | (1) 400 Watt Auto-sensing, PFC, CE Mark Compliant | (1) 500 Watt PFC, CE Mark Compliant |
| **Software de Administración** | Insight Control (Optional) | Insight Control (Optional) | Insight Control (Optional) |

[52] Precios tomados de: http://h10010.www1.hp.com/wwpc/us/en/sm/WF25a/15351-15351-3328412-241644-241475-3929672.html

Los precios mostrados en la tabla anterior nos permitirán tener una referencia del precio al que deberán cotizarse en Ecuador.

El servidor cotizado por TecnoMega (Anexo 5.3) junto con los servicios de instalación de hardware y soporte por tres años es el que muestra la Tabla 5-7.

**Tabla 5-7 Costos: Servidor y paquete de cuidado HP**

| PRESUPUESTO: SERVIDOR HP ProLiant DL320 | | | | |
|---|---|---|---|---|
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| HP ProLiant DL320 593498-001 | Servidor DL320G6 L5609 QUAD-CORE (1) Intel® Xeon® Processor E5640 (1.16 GHz, 12MB L3 Cache,40 Watts, DDR3-1066, HT Turbo 1/1/2/2) | 1 | 2081.00 | 2081.00 |
| Paquete de cuidado HP | Servicio de Instalación de hardware | 1 | 134.00 | 134.00 |
| | Soporte Hardware 4-Hour, 24x7 Onsite por 3 años | 1 | 386.00 | 386.00 |
| | | | **SUBTOTAL** | **2601.00** |
| | | | **IVA** | **312.12** |
| | | | **TOTAL** | **2913.12** |

El servidor de comunicaciones tendrá un costo aproximado de 2600 dólares americanos, en cuyo costo incluye un paquete de cuidado HP que consta con servicio de instalación de harware y soporte del mismo por tres años en la forma 24x7x4.

### 5.2.5. EQUIPO DE SEGURIDAD

El equipo de seguridad perimetral escogido fue el SA 540 de cisco, el precio del equipo, configuración, así como sus licencias de IPS y Antivirus fueron cotizados por la empresa Megasupply S.A. (Anexo 5.3).

La Tabla 5-8 muestra el costo referencial del UTM SA 540 de Cisco

**Tabla 5-8 Costos: UMT Cisco SA 540**

| PRESUPUESTO: UTM | | | | |
|---|---|---|---|---|
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| SA540-GW100BUN3-K9 | Cisco Small Business Pro SA 540 - Security appliance - 8 ports - Ethernet, Fast Ethernet, Gigabit Ethernet - 1U - with Cisco IPS and ProtectLink Gateway 100 Licenses, 3 years | 1 | 2182.99 | 2182.99 |
| | El equipo incluye el servicio Cisco Small Business Pro Service | | | |
| | | | **SUBTOTAL** | 2182.99 |
| | | | **IVA** | 261.96 |
| | | | **TOTAL** | **2444.95** |

El equipo de seguridad perimetral UTM tendrá un costo aproximado de 2200 dólares americanos. El precio del UTM SA 540 incluye 100 licencias IPS y ProtectLink Gateway por tres años, además incluye el servicio *Cisco Small Business Pro Service* el cual permite el acceso a actualizaciones del software y reemplazo de hardware de la forma NBD (Next Business Day) cuando sea necesario.

### 5.2.6. TELEFONÍA IP

La telefonía IP a implementar será a través de software libre haciendo uso del software Asterisk, el cual cuenta con licencia GPL. Para el cálculo de la telefonía IP se evaluará el costo del servidor, configuración del servicio y teléfonos IP.

El servidor ha sido elegido de acuerdo a los requerimientos técnicos analizados en el diseño, la tarjeta de red deberá soportar las 6 troncales telefónicas analizadas en el tráfico de telefonía IP, por lo que se necesitará una tarjeta de 8 puertos.

El costo referencial del servidor ha sido cotizado por parte de la empresa TecnoMega, mientras que los teléfonos IP han sido cotizados a través de tiendas en Internet (ebay) donde ha sido considerado el costo del envío al Ecuador (Anexo 5.3).

La Tabla 5-9 muestra la cotización referencial del servicio de telefonía IP.

**Tabla 5-9 Costos: Telefonía IP**

| PRESUPUESTO: TELÉFONOS IP | | | | |
|---|---|---|---|---|
| **ÍTEM** | **DESCRIPCIÓN** | **CANTIDAD** | **VALOR UNITARIO ($)** | **VALOR TOTAL ($)** |
| SERVIDOR | HP Servidor DL120G6 (1)Quad-Core Intel® Xeon® Processor X3430 (2.40 GHz, 8M, Cache, DDR3)/ 2 GB RAM(1X2GB) | 1 | 1194.00 | 1194.00 |
| | Paquete de cuidado HP | 1 | 202.00 | 202.00 |
| TARJETA FXO | 1TDM808EF 8 port modular analog PCI 3.3/5.0V card with 8 Trunk interfaces | 1 | 924.00 | 924.00 |
| | | | **SUBTOTAL** | **2320.00** |
| TELÉFONO SIMPLES | Teléfono IP HP JC506A 3501 | 23 | 300.00 | 6900.00 |
| | Envío a Ecuador | 23 | 56.20 | 1292.60 |
| TELÉFONO PARA DIRECTORES | Teléfono IP HP JC508A 3503 | 7 | 400.00 | 2800.00 |
| | Envío a Ecuador | 7 | 56.20 | 393.40 |
| | | | **SUBTOTAL** | **11386.00** |
| CONFIGURACIÓN | Configuración Central IP | 1 | 1000.00 | 1000.00 |
| | Configuración Teléfonos IP | 30 | 15.00 | 450.00 |
| | | | **SUBTOTAL** | **1450.00** |
| | | | **TOTAL** | **15156.00** |

El costo total de implementación del servicio de telefonía IP será de aproximadamente 15200 dólares americanos.

### 5.2.7. CONFIGURACIÓN DE SERVIDOR DE COMUNICACIONES

La configuración del equipo de comunicaciones incluirá la instalación de los servicios Intranet mencionados en el capítulo 3, los cuales satisfacen los requerimientos para la red del PPA.

El costo total de la solución (CTS) considera 3 componentes:

$$CTS^{53} = CTI + CTA + CTC$$

Dónde:

- CTI = Costo Total de la Implementación
- CTA = Costo Total Administrativo
- CTC = Costo Total de Capacitación

Para el cálculo de costos de CTA y CTC se considerará 3 años de funcionamiento del sistema.

El costo de implementación (CTI) considerará el costo de licencias del software, costo de instalación, configuración, adaptación, adicionales de hardware y software y el costo de migración de ser necesario.

El costo total administrativo (CTA) incluirá costos de actualización de software y hardware, costos del recurso humano, costo promedio anual de un ingeniero administrador, operador y de soporte de ser el caso.

El costo total de capacitación (CTC) incluirá el costo promedio anual para la capacitación continua del personal (técnico y usuarios).

La Tabla 5-10 muestra el costo de instalación, mantenimiento y soporte por los próximos 3 años del software a instalar los cuales han sido considerados de acuerdo al mercado actual.

**Tabla 5-10 Costos: Configuración y mantenimiento del servidor de comunicaciones**

| CONFIGURACIÓN: SERVIDOR DE COMUNICACIONES | | | |
|---|---|---|---|
| **Descripción** | | **Valor** | **Observación** |
| **CTI** | 1 Licencia servidor solución de colaboración | 0 | Licencia GPL |
| | 30 Licencias cliente solución de colaboración | 0 | Licencia GPL |
| | Instalación y configuración | **800** | |
| | Hardware e infraestructura adicional | 0 | No aplica |
| | 1 Licencia servidor de sistema operativo red | 0 | Licencia GPL |

Continúa

[53] Método tomado de: http://www.informatica.gob.ec/index.php/software-libre/costo-total-de-la-solucion/

| | | | | |
|---|---|---|---|---|
| | 30 Licencias cliente de sistema operativo | 0 | | Licencia GPL |
| | 30 Licencias cliente acceso a red | 0 | | Licencia GPL |
| | Software adicional | 0 | | **No aplica** |
| | Migración e Integración | **700** | | Integración con sistemas Windows |
| | **SUBTOTAL CTI** | **1500** | | |
| **CTA** | Actualización y mantenimiento de hardware | **0** | | No aplica, tomado en cuenta en la adquisición del servidor |
| | Actualización y soporte de software en 3 años | 3000 | | 1000 dólares cada año |
| | Costo promedio anual de un ingeniero administrador | 14400 | 10800 | Tomando como referencia 1200 dólares mensuales |
| | Número de Ingenieros | 1 | | |
| | Porcentaje del tiempo dedicado a la administración de la solución | 25% | | |
| | Número de años de la solución | 3 | | |
| | Costo promedio anual de un ingeniero de soporte | 9600 | 11520 | Tomando como referencia 1200 dólares mensuales |
| | Número de Ingenieros | 1 | | |
| | Porcentaje del tiempo dedicado a la operación de la solución | 40% | | |
| | Número de años de la solución | 3 | | |
| | **SUBTOTAL CTA** | **25320** | | |
| **CTC** | Costo de capacitación a un técnico por hora | 10 | 1200 | Se estima realizar 20 horas de capacitación anuales |
| | Numero de técnicos a capacitar | 2 | | |
| | Número de horas capacitación técnica | 20 | | |
| | Número de años de la solución | 3 | | |
| | **SUBTOTAL CTC** | **1200** | | |
| | **TOTAL CTS** | **28020** | | |

El costo del software a instalar tendrá un valor recurrente por 3 años de 28020 dólares americanos.

### 5.2.8. SERVICIO DE INTERNET

El servicio de Internet deberá ser provisto por dos ISPs, los cuales provean al PPA de una capacidad de 768 Kbps cada uno. Los costos de los enlaces según los siguientes ISPs se muestran en la Tabla 5-11.

**Tabla 5-11 Costos: Enlaces a Internet[54]**

| PRESUPUESTO: ENLACES A INTERNET | | | | |
|---|---|---|---|---|
| Enlace dedicado (1:1) de 768 Kbps | | | | |
| **ISP** | **DESCRIPCIÓN** | **COSTO MENSUAL ($)** | **COSTO INSTALACIÓN ($)** | **COSTO ANUAL ($)** |
| TELCONET | Compartición 1: 1<br>Disponibilidad del 98%<br>Medio de transmisión: fibra óptica | 175.00 | 150.00 | 2250.00 |
| PUNTONET | Compartición 1: 1<br>Disponibilidad del 99.85%<br>Medio de transmisión: fibra óptica e inalámbrico | 143.00 | 0.00 | 1715.64 |
| SURATEL | Compartición 1: 1<br>Disponibilidad del 99.6%<br>Medio de transmisión: fibra óptica | 180.00 | 200.00 | 2360.00 |

Según los valores cotizados para el enlace de 768 Kbps se estimará como valor referencial el presupuesto dado por SURATEL. El costo referencial para la adquisición del enlace a Internet al constar con dos enlaces será de 4720 dólares en el primer año, en el que se incluye el costo de instalación.

### 5.2.9. COSTO TOTAL

El costo total de la solución estará dado por los costos recurrentes y no recurrentes en los que deberá incurrir el PPA para el total funcionamiento de sus actividades.

Los costos no recurrentes están dados por equipos y servicios que serán necesarios para poner en marcha la infraestructura de comunicaciones, mientras que los recurrentes serán aquellos que son necesarios para el mantenimiento y soporte de equipos y servicios.

La Tabla 5-12 muestra el resumen de los costos de equipos y servicios no recurrentes.

[54] Precios tomados del Anexo F de la Tesis realizada en Marzo del año en curso "DISEÑO DE LA RED DE TELEFONÍA IP Y SU INTEGRACIÓN CON LA RED DE DATOS PARA LA COMUNICACIÓN DE LA MATRIZ CON LAS SUCURSALES DE IMPORTADORA VEGA S.A" de la Ing. Diana Lovato y el Ing. Luis Cadena

**Tabla 5-12 Costos no recurrentes**

| COSTO REFERENCIAL DE LA SOLUCIÓN | | |
|---|---|---|
| COSTOS NO RECURRENTES | | |
| **SISTEMA** | **DESCRIPCIÓN** | **COSTO ($)** |
| SISTEMA DE CABLEADO ESTRUCTURADO | Cableado estructurado | 12000.00 |
| | Soporte y mantenimiento correctivo por 3 años | |
| | UPS | 8500.00 |
| RED LAN | Equipos de conectividad | 17065.00 |
| | Configuración | |
| | Soporte técnico y capacitación | |
| RED INALÁMBRICA | Equipos de conectividad | 979.00 |
| | Configuración | |
| | Soporte técnico y capacitación | |
| SERVIDOR | Servidor | 2600.00 |
| | Soporte y mantenimiento correctivo por 3 años | |
| SEGURIDAD PERIMETRAL | Equipos | 2183.00 |
| | Licencias por 3 años | |
| | Soporte por 3 años | |
| TELEFONÍA IP | Servidor y tarjeta FXO | 15156.00 |
| | Teléfonos IP | |
| | Configuración del sistema | |
| SERVICIOS | Configuración del servicios Intranet | 1500.00 |
| ENLACE INTERNET | Por un año | 4720.00 |
| | **SUBOTAL** | **64703.00** |
| | **IVA** | **7764.36** |
| | **TOTAL** | **72467.36** |

El PPA deberá disponer de alrededor de 64700 dólares americanos (sin incluir IVA) para la puesta en marcha de la infraestructura de comunicaciones.

Los gastos recurrentes en los que deberá incurrir el PPA están dados por el mantenimiento y administración de los servicios Intranet, del monitoreo y gestión de la red y su seguridad, para lo cual es necesario la contratación de un ingeniero de soporte

encargado de los temas mencionados y que trabaje en conjunto con el Director de GTI-PPA.

La Tabla 5-13 muestra los equipos y servicios recurrentes.

**Tabla 5-13 Costos recurrentes**

| COSTO REFERENCIAL DE LA SOLUCIÓN | | |
|---|---|---|
| COSTOS RECURRENTES | | |
| **SISTEMA** | **DESCRIPCIÓN** | **COSTO ($)** |
| MANTENIMIENTO SERVICIOS INTRANET | Actualización y soporte de software | 28000.00 |
| | Costo de capacitación continua por 3 años | |
| | Costo de administración | |
| INGENIERO DE SOPORTE | Sueldo (mensual 800 dólares) en 3 años | 28800.00 |
| | **SUBTOTAL** | **56800.00** |
| | **IVA** | **6816.00** |
| | **TOTAL** | **63616.00** |

El PPA deberá costear durante los próximos 3 años alrededor de 56800 dólares americanos para el mantenimiento del software instalados y de un administrador de red, sin tomar en cuenta la contratación de servicios de Internet a partir del segundo año.

No se calcula la contratación del servicio de Internet en los siguientes años, ya que depende del precio que fluctúa de año a año y de la capacidad requerida de acuerdo al crecimiento de la institución.

Para la adquisición de los equipos mencionados se debe tomar en cuenta que luego de realizada la compra los equipos tardan en llegar a Ecuador de 30 a 45 días.

# CAPÍTULO VI

# 6. CONCLUSIONES Y RECOMENDACIONES

El diseño de la infraestructura de comunicaciones de voz, datos y video para el Programa de Provisión de Alimentos cumple con los objetivos planteados, los cuales deberán ser monitoreados para el correcto funcionamiento de la infraestructura en el transcurso del tiempo.

## 6.1. CONCLUSIONES

- El constante e importante crecimiento que ha tenido el PPA desde sus inicios ha hecho que sea necesaria la reubicación de la institución a sus propias instalaciones, para lo cual es necesario constar con una completa infraestructura de comunicaciones de voz, datos y video que le permita realizar sus actividades de forma eficiente.

- La infraestructura de comunicaciones de voz, datos y video del PPA constará con una red de alta velocidad que le permita integrar aplicaciones y servicios multimedia actuales y futuras de forma escalable sin recurrir a cambios considerables en la red.

- El diseño de la infraestructura de red se basa en el análisis de la situación actual del PPA, del número de usuarios actuales y futuros de la red y del tráfico que generan los mismos de acuerdo a los servicios y aplicaciones que utilizan para desarrollar sus actividades, los cuales en conjunto permiten dimensionar los servicios y equipos a utilizar sin que lleguen a ser deficientes o por el contrario sobredimensionados.

- El diseño del Sistema de Cableado Estructurado proporciona una completa solución de conectividad basada en estándares que permita la libre elección de proveedores y soluciones. De acuerdo a los servicios, aplicaciones y tráfico que deberá soportar en la actualidad y en los próximos 10 años se ha establecido el uso de un Sistema de Cableado Estructurado categoría 6A que garantice un adecuado rendimiento y confiabilidad.

- La implementación del Sistema de Cableado Estructurado constará con un plan de acción que permita su desarrollo de forma ordenada y en coordinación con las obras civiles cumpliendo los estándares precisos. El plan de acción constará con una fase de preparación, fase de recorte y fase de finalización. La fase de preparación constará con una visita técnica, revisión de certificados de mano de obra y materiales, la fase de recorte constará con el tendido del cable, recorte y terminación del enlace permanente tanto en el área de trabajo como en el rack, la fase de finalización constará con el proceso de certificación del SCE.

- El diseño de la red LAN se basa en una red Gigabit Ethernet bajo un esquema jerárquico (acceso, distribución y núcleo) que maneje el tráfico de la red evitando la creación de cuellos de botella facilitando la administración y corrección de fallas del sistema, además de facilitar la escalabilidad y la elección de los diferentes equipos de conectividad.

- El esquema lógico de la red ha sido diseñado de acuerdo a la estructura organizacional del PPA. El esquema lógico esta basado en subredes para cada uno de los departamentos, *datacenter* y telefonía IP, a los cuales también se los ha divido a través de VLANs que permitan ofrecer mayor seguridad entre las subredes. El direccionamiento IP se basará en subredes que permitan una mejor administración de la red por parte de GTI-PPA y será proporcionado de forma dinámica a través del servicio de DHCP a excepción de servidores y equipos de conectividad.

- La red inalámbrica WLAN brindará conectividad tanto a funcionarios del PPA como a visitantes, mediante la cual tendrán acceso a los servicios y aplicaciones previamente establecidos por GTI-PPA. La red inalámbrica estará basada en el estándar IEEE 802.11 g, la cual satisface las necesidades de cobertura o usuarios simultáneos del PPA.

- Para el servicio de Telefonía IP se ha diseñado una infraestructura de red Gigabit Ethernet que soporte voz sobre IP a través de un SCE categoría 6A, a nivel lógico se ha asignado una subred y una VLAN exclusiva para telefonía IP, los equipos de conectividad permitirán la priorización de tráfico de voz y soportarán PoE para el suministro de energía a los teléfonos IP.

- El PPA al ser una institución gubernamental debe apegarse al mandado 1014 que impulsa el uso de Software Libre que brinde iguales o mejores prestaciones que el software propietario. Los servicios Intranet al igual que el servicio de Telefonía IP serán provisto por Software Libre que ha sido probado por otras instituciones, cuentan con instituciones que brindan soporte y cuya comunidad actualiza el software de forma permanente, dando soluciones a problemas de rendimiento y seguridad.

- Los servicios Intranet han sido implementados a través de Software Libre a través de la distribución "*ClearOS*" el cual es un software con licencia GPL que es desarrollado por "*Clear Fundation*".

- La Seguridad de la Información del PPA ha sido tratada de acuerdo de la criticidad de la misma. Se ha realizado un análisis de riesgo que nos permite conocer la información crítica del PPA, sin la cual se vería en riesgo la continuidad del Programa, así mismo se ha determinado sus amenazas y vulnerabilidades, las cuales en conjunto han permitido determinar el nivel de riesgo de los activos informáticos más importantes. En base a dicho análisis se

ha realizado las recomendaciones que permitan resguardar dicha información. Las recomendaciones realizadas se ha basado en la norma ISO 27002 las cuales ayudarán a eliminar o disminuir el riesgo del activo informático en cuestión.

- La seguridad perimetral de la infraestructura de comunicaciones del PPA ha sido provista a través de un equipo UTM (Unified Threat Management) que a más de funcionar como firewall ofrezca funciones de Antivirus, VPN, IPS, los cuales sean de fácil administración y configuración debido a que no se dispone por el momento de una partida presupuestaria para contratar al personal dedicado a la seguridad del PPA.

- Todo el equipamiento elegido para la infraestructura de comunicaciones del PPA ha sido dimensionada de acuerdo a requerimientos de tráfico, número de usuarios de red, protocolos estándares y de acuerdo al tamaño de la red, evitando sobredimensionar los equipos y haciendo el proyecto rentable, tomando en cuenta un tiempo de vida útil de alrededor de 5 años.

## 6.2. RECOMENDACIONES

- La adquisición tanto del equipamiento como de los servicios deben constar con SLA (Niveles de Acuerdo de Servicio) que garanticen la calidad del servicio suministrado en aspectos como tiempo de respuesta, disponibilidad, documentación, soporte, entre otras, las cuales permitan garantizar la continuidad de las operaciones del PPA.

- Los equipos de la infraestructura de comunicaciones deberán constar con las garantías del fabricante, del proveedor y del instalador de ser el caso, además se deberá tener en cuenta que muchas de las veces la entrega de los equipos no es inmediata, por lo cual en el plan de acción de deberá prever un tiempo de mínimo 30 días desde la firma del contrato.

- Si bien se ha diseñado una infraestructura de comunicaciones lo suficientemente administrable, es necesario contar con un ingeniero de soporte que se encuentre a cargo de la administración y gestión de la red, así como del soporte técnico a las diferentes áreas del PPA.

- Se deberá programar el mantenimiento preventivo de los equipos de conectividad, se recomienda realizarlo como mínimo dos veces al año en horarios no laborales.

- Se recomienda a GTI-PPA analizar las pruebas realizadas sobre los servicios instalados en el prototipo realizado a través de *ClearOS* para su posible puesta en marcha. Si bien se cuenta con el procedimiento realizado para la instalación y configuración de los diferentes servicios, es necesario realizar una bitácora sobre los servicios instalados que permita conocer los cambios y actualizaciones de software y hardware que se realizan con el transcurso del tiempo, teniendo siempre procedimientos de *rollback* en caso de fallas, así como de los respaldos respectivos.

- El análisis de riesgos y las recomendaciones realizadas para la seguridad de la información de los activos informáticos más importantes del PPA son la base para el establecimiento de políticas de seguridad, las cuales deberán ser planteadas por GTI-PPA de acuerdo a sus experiencias y necesidades y deberán contar con el respaldo del Coordinador Nacional junto con el departamento de Recursos Humanos.

- Debido a que la adquisición del equipamiento y servicios para la puesta en marcha de la infraestructura de comunicaciones dependerá de la partida presupuestaria del Programa y de cuánto sea asignado a la implementación de la infraestructura de comunicaciones, es necesario realizar un plan de acción que permita la adquisición de equipos y servicios de forma gradual.

  El plan de acción recomendado es:

  1. Implementación del Sistema de Cableado Estructurado.
  2. Adquisición de equipos de conectividad (Switches, UTM, Access Point).
  3. Adquisición de servidores de Telefonía IP y servidor de Comunicaciones.
  4. Contratación del servicio de Internet.
  5. Configuración de servidores.
  6. Implementación de políticas de seguridad.

  El mínimo de equipos y servicios informáticos con los que deberá contar para la puesta en marcha de sus actividades son:

  1. Sistema de Cableado Estructurado.
  2. Inicialmente se adquiriría únicamente los switches de acceso y el UTM para la seguridad perimetral.
  3. El deberá contratar por lo menos un enlace a Internet.
  4. La página Web y correo electrónico son servicios vitales, por lo cual en un principio se encontrarán alojados en un *hosting*.

# REFERENCIAS

## LIBROS Y FOLLETOS

[3] STALLINGS, William. Comunicaciones y Redes de Computadoras. Prentice Hall, Sexta Edición. 2000.

[4] TANENBAUM, Andrew. Redes de Computadoras. Pearson Educación, Tercera Edición. 1997.

[1] Ing. GONZÁLEZ, Fabio. Folleto de Cableado Estructurado, 2008.

[5] Ing. VINUEZA, Mónica. Follero de Redes de Área Local, 2008.

[6] Ing. HIDALGO, Pablo. Folleto de Redes TCP/IP, 2008.

[8] Msc. SINCHE, Soraya. Folleto de Redes LAN Inalámbricas, 2009.

## PROYECTOS DE TITULACIÓN

- Análisis e implementación de un prototipo de servidor virtualizado sobre una distribución de Linux para el uso en PyMEs. *Por Bonilla Suárez Jorge Javier y Carrasco Aguilar Daniel Santiago*, Escuela Politécnica Nacional, Escuela de Ingeniería, Febrero 2010.
- Diseño de la Intranet de la empresa MEGAREDES Cía. Ltda. *Por César Alfredo Trelles Segovia y Ricardo Patricio Vallejo Cifuentes,* Escuela Politécnica Nacional, Escuela de Ingeniería, Marzo 2009.
- Desarrollo de un sistema de telefonía IP distribuido mediante la implementación de un mecanismo de descubrimiento de rutas de llamadas, en base al sistema operativo Linux. *Por Rodríguez Hoyos Ana Fernanda*, Escuela Politécnica Nacional, Escuela de Ingeniería, Septiembre 2010.

- Reingeniería de la red LAN del Ilustre Municipio del Cantón Rumiñahui. *Por Perugachi Alvear Félix Tomás*, Escuela Politécnica Nacional, Escuela de Ingeniería, Junio 2010.
- Rediseño de la red de comunicaciones para la Universidad Estatal de Bolívar que soporte aplicaciones de voz, datos y videoconferencia. Por Cortez Quintana Darwin Roberto y López Barragán Jaime Eduardo, Escuela de Ingeniería, Octubre 2006.


## PÁGINAS WEB


[2] **Sistema de Cableado Estructurado**

- http://www.ampnetconnect.com/documents/Catalog_2010_CH01_XG_Cat6A_82164-1_20110104.pdf
- http://www.ampnetconnect.com/documents/TIA-568-C-CIM_Sept-08_Spanish.PDF
- http://www.anixter.com/AXECOM/AXEDocLib.nfs/0/D15LJKCH/$file/sec_13.pdf?openelement

[7] **Red LAN**

- http://docwiki.cisco.com/wiki/Ethernet_Technologies#10-Mbps_Ethernet-10Base-T
- http://voiplab.niu.edu.tw/IEEE/802.3/802.3an-2006.pdf

[9] **Telefonía IP**

- http://www.idris.com.ar/lairent/pdf/ART0001%20-%20Calculo%20de%20ancho%20de%20banda%20en%20VoIP,pdf
- https://www.camundanet.com/attachments/article/86/unificadas1.pdf Comunicaciones Unificadas con Elastix, Volumen 1

[11] **Servicios Intranet**

- http://www.informática.gob.ec/index.php/software-libre
- http://www.clearfundation.com
- http://httpd.apache.org
- http://www.cups.org
- http://www.thekelleys.org.uk/dnsmasq/doc.html
- http://www.mysql.com
- http://www.openldap.org
- http://www.postfix.org
- http://www.proftpd.org

[10] **Seguridad de la Información**

- http://www.imaginar.org/conquito/manual_tic.pdf
- http://arcert.gov.ar/webs/manual/manual_de _seguridad.pdf
- http://www.iso27001standard.com/en/services/iso-27001-documentation-toolkit#