

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

**ESTUDIO Y DISEÑO DE UNA RED LAN CORPORATIVA DEL
MINISTERIO DEL AMBIENTE Y AGUA PARA EL MANEJO DE VOZ,
DATOS Y VIDEO, UTILIZANDO MECANISMOS DE SEGURIDAD Y
ALTA DISPONIBILIDAD.**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES**

KLEBER ROLANDO ANDRANGO CALUGUILLIN

DIRECTOR: Ing. CARLOS ALFONSO HERRERA MUÑOZ

Quito, junio 2022

AVAL

Certifico que el presente trabajo fue desarrollado por Kleber Rolando Andrango Caluguillin, bajo mi supervisión.

Ing. CARLOS ALFONSO HERRERA MUÑOZ
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo Kleber Rolando Andrango Caluguillin, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado 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 dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Kleber Rolando Andrango Caluguillin

DEDICATORIA

El Trabajo de Titulación va dedicado primeramente a Dios que siempre está presente en todo momento, dándome sabiduría, el ánimo y entendimiento para poder seguir adelante.

A mis padres José Andrango y Eloísa Caluguillin ya que me apoyaron en todo momento sin perder las esperanzas en mí, Papito José donde quieras que estés cuídate mucho y siempre pediré a Dios por ti y por la familia para que nos cuide y nos de Salud y vida.

A mis hermanos que de una u otra forma me ayudan en lo que necesite, tratando de sobrellevar y seguir adelante.

Kleber Andrango

AGRADECIMIENTO

Agradezco primeramente a Dios por la sabiduría, salud, entendimiento y vida cada día que pasa, también en aquellos momentos de soledad y tristeza siempre ha estado ahí.

Agradezco a los seres más queridos para mí: Eloísa Caluguillin y José Andrango con su sustento ilimitado en todo sentido, en la parte moral el cual me hace una persona mejor cada día.

Agradezco a mis hermanos por su apoyo en todo sentido, siempre ahí con sus buenos consejos para bien.

Agradezco a todos los ingenieros y en especial al Ingeniero Carlos Herrera que siempre estuvo ahí con su soporte, pauta y conocimiento para el cumplimiento del Trabajo de Titulación.

Finalmente, agradezco al Ministerio por su auspicio para el progreso del Trabajo de Titulación.

Kleber

ÍNDICE DE CONTENIDO

AVAL	I
DECLARACIÓN DE AUTORÍA	II
DEDICATORIA	III
AGRADECIMIENTO	IV
ÍNDICE DE CONTENIDO	V
RESUMEN.....	X
ABSTRACT.....	XI
1. INTRODUCCIÓN.....	1
1.1. OBJETIVOS	1
1.2. ALCANCE.....	1
1.3. MARCO TEÓRICO	2
1.3.1. PARÁMETROS EN UN SISTEMA CONFIABLE	3
1.3.2. SEGURIDAD EN REDES CORPORATIVAS	4
1.3.2.1. Amenazas y ataques	4
1.3.2.1.1. <i>Inminencias exteriores e interiores</i>	4
1.3.2.2. Sistemas de detección de intrusos (IDS)	5
1.3.2.3. Inseguridades permisibles en los servicios de la red	5
1.3.2.4. Comunicaciones indudables	6
1.3.3. ALTA DISPONIBILIDAD	6
1.3.3.1. Soluciones de alta disponibilidad	7
1.3.3.1.1. <i>Raid</i>	8
1.3.3.1.2. <i>Balanceo de carga</i>	9
1.3.3.1.3. <i>Entornos virtuales</i>	10
2. METODOLOGÍA.....	11
2.1. SITUACIÓN ACTUAL DE LA RED.....	11
2.2. MINISTERIO DEL AMBIENTE Y AGUA	11
2.2.1. MISIÓN DEL MINISTERIO DEL AMBIENTE Y AGUA.....	12

2.2.2.	VISIÓN DEL MINISTERIO DEL AMBIENTE Y AGUA.....	12
2.3.	DESCRIPCIÓN DE LA INFRAESTRUCTURA FÍSICA.....	13
2.4.	DESCRIPCIÓN ACTUAL DE LA RED	14
2.5.	ANÁLISIS DEL ESQUEMA ACTUAL DE LA RED	16
2.6.	EQUIPOS QUE CONFORMAN LA RED ACTUAL.....	16
2.6.1.	COMPONENTES PASIVOS DE LA RED	16
2.6.1.1.	Sistema de Cableado Estructurado (SCE) de la red actual.....	16
2.6.1.2.	Sistema de Puesta a Tierra de la red.....	18
2.6.2.	ESTUDIO DE LOS COMPONENTES PASIVOS.....	18
2.6.3.	ELEMENTOS ACTIVOS DE LA RED	18
2.6.4.	ESTUDIO DE LOS ELEMENTOS ACTIVOS	19
2.6.5.	SISTEMA DE TELEFONÍA ACTUAL	20
2.6.5.1.	Estudio del Sistema de Telefonía	21
2.6.6.	SISTEMA DE VIDEO ACTUAL.....	21
2.6.6.1.	Estudio del Sistema de Video	22
2.6.7.	RED INALÁMBRICA ACTUAL.....	22
2.6.7.1.	Estudio de la Red Inalámbrica.....	23
2.6.8.	SERVICIO DE INTERNET CONTRATADO ACTUALMENTE.....	23
2.6.8.1.	Estudio del Servicio de Internet	24
2.7.	DISEÑO DE LA RED LAN CORPORATIVA PARA EL MINISTERIO DEL AMBIENTE Y AGUA	24
2.7.1.	VISIÓN	24
2.7.2.	MODELO DE RED PROPUESTO	24
2.7.2.1.	Capa de Acceso	25
2.7.2.2.	Capa de Distribución	25
2.7.2.3.	Capa de Core	25
2.7.3.	TECNOLOGÍA DE RED A UTILIZAR.....	25
2.7.4.	TOPOLOGÍA DE RED PROPUESTA	26
2.7.5.	DISEÑO DE LA RED PASIVA PROPUESTA.....	28

2.7.5.1.	Diseño de la infraestructura de red para la institución.....	28
2.7.5.1.1.	<i>Repartición de los puntos de red</i>	28
2.7.5.2.	Diseño del sistema de cableado horizontal.....	29
2.7.5.2.1.	<i>Recorridos para el cableado horizontal</i>	31
2.7.5.2.2.	<i>Complementos para el cableado horizontal</i>	32
2.7.5.3.	Diseño del sistema de cableado vertical	34
2.7.5.4.	Diseño de la red de trabajo.....	35
2.7.5.5.	Diseño del cuarto de telecomunicaciones.....	35
2.7.5.5.1.	<i>Dimensionamiento de los racks</i>	35
2.7.5.5.2.	<i>Dimensionamiento del rack primordial</i>	40
2.7.5.6.	Diseño de la sala de equipos.....	41
2.7.5.7.	Gestión del Sistema de Cableado Estructurado para la red.....	41
2.7.5.7.1.	<i>Etiquetado para el cableado</i>	41
2.7.6.	DIMENSIONAMIENTO DE TRÁFICO.....	42
2.7.6.1.	Dimensionamiento del Tráfico Interno	42
2.7.6.1.1.	<i>Cómputo del ancho de banda en el Correo interno</i>	42
2.7.6.1.2.	<i>Cómputo del ancho de banda en el ingreso a la Base de datos</i>	43
2.7.6.1.3.	<i>Cómputo del ancho de banda en acceso a Video seguridad</i>	43
2.7.6.1.4.	<i>Cómputo del ancho de banda en acceso a Transferencia de archivos</i> 43	
2.7.6.1.5.	<i>Cómputo del ancho de banda para Videoconferencia</i>	44
2.7.6.1.6.	<i>Cómputo del ancho de banda para Voz sobre IP</i>	44
2.7.6.2.	Dimensionamiento del Tráfico Externo	48
2.7.6.2.1.	<i>Cómputo del ancho de banda en la Mensajería externa</i>	48
2.7.6.2.2.	<i>Cómputo del ancho de banda en el Acceso web</i>	48
2.7.6.2.3.	<i>Cómputo del ancho de banda en la Carga o Subida de archivos</i>	49
2.7.6.2.4.	<i>Cómputo del ancho de banda en la Descarga de archivos</i>	49
2.7.6.2.5.	<i>Proyección de la red LAN para 5 años</i>	50
2.7.7.	DISEÑO DE LA RED ACTIVA	51

2.7.7.1.	Características Técnicas mínimas de los dispositivos de la red.....	51
2.7.7.1.1.	<i>Switch de Acceso</i>	51
2.7.7.1.2.	<i>Switch de Distribución</i>	53
2.7.7.1.3.	<i>Switch de Core</i>	54
2.7.7.1.4.	<i>Firewall</i>	55
2.7.7.1.5.	<i>Servidores</i>	56
2.7.7.1.6.	<i>Cámaras de Video vigilancia</i>	56
2.7.7.1.7.	<i>Access Point</i>	57
2.7.7.1.8.	<i>Teléfono IP</i>	58
2.7.8.	DIRECCIONAMIENTO DE LA RED CORPORATIVA DEL MINISTERIO DEL AMBIENTE Y AGUA.....	59
2.7.8.1.	Zona Desmilitarizada	59
2.7.8.2.	Direccionamiento IP para la Red Corporativa	59
2.7.9.	MECANISMOS DE SEGURIDAD	60
2.7.9.1.	Configuración de reglas permitidas en el firewall	61
2.7.9.2.	Filtrado web.....	65
2.7.9.3.	Servicio de antivirus.....	65
2.7.9.4.	Observación de Tráfico en la red.....	66
2.7.10.	ALTA DISPONIBILIDAD DE LA RED.....	67
2.8.	PRESUPUESTO DE COSTOS PARA LA RED LAN CORPORATIVA	68
2.8.1.	COSTO DE LA RED PASIVA	68
2.8.2.	COSTO DE LA RED ACTIVA	68
2.8.2.1.	Comparación de Switches de Acceso.....	69
2.8.2.2.	Comparación de Switches de Distribución	69
2.8.2.3.	Comparación de Switches de Core.....	70
2.8.2.4.	Comparación de Cámaras de Video vigilancia.....	71
2.8.2.5.	Comparación de los Access Point	72
2.8.2.6.	Comparación de los Teléfonos IP	73
2.8.2.7.	Equipos Cisco ASA.....	74

2.8.2.8.	Garantía de Cisco.....	74
2.8.2.9.	Garantía de Huawei.....	75
2.8.2.10.	Garantía de Aruba	75
2.8.2.11.	Elección de los equipos de red y costo de la red activa	75
2.8.3.	COSTO DE LA RED LAN	76
2.9.	SIMULACIÓN DE LA RED LAN CORPORATIVA	76
2.9.1.	SOFTWARE DE SIMULACIÓN DE RED	76
2.9.1.1.	Cisco Packet Tracer	76
2.9.1.2.	Configuración básica de los switches y routers.....	77
2.9.2.	SIMULACIÓN DE LA RED.....	78
2.9.3.	SIMULACIÓN DE ACCESO A INTERNET USANDO EL FIREWALL CISCO ASA 82	
3.	RESULTADOS Y DISCUSIÓN	86
3.1.	PRUEBAS EN LA SIMULACIÓN DE LA RED.....	86
3.2.	PRUEBAS EN LA SIMULACIÓN DE ACCESO A INTERNET USANDO EL FIREWALL CISCO ASA.....	87
3.3.	ANÁLISIS DE RESULTADOS.....	88
4.	CONCLUSIONES Y RECOMENDACIONES	90
4.1.	CONCLUSIONES	90
4.2.	RECOMENDACIONES.....	91
5.	REFERENCIAS BIBLIOGRÁFICAS.....	92
	ANEXOS.....	95

RESUMEN

El Trabajo de titulación presenta el Estudio y diseño de una red LAN corporativa para el Ministerio del Ambiente y Agua en cuanto al manejo de los 3 servicios, utilizando mecanismos de seguridad y alta disponibilidad.

En el primer capítulo se describe los mecanismos de seguridad en redes LAN corporativas y alta disponibilidad.

El segundo capítulo describe el escenario actual de la red del Ministerio del Ambiente y Agua y en base a los requerimientos actuales se propone un diseño de una red LAN corporativa que incluye mecanismos de seguridad y alta disponibilidad.

También se presenta el presupuesto de los componentes de red y la simulación de algunos segmentos de la red LAN corporativa.

Se incluye los conceptos relacionados a los diferentes mecanismos de seguridad y alta disponibilidad para aplicar al diseño de esta red corporativa para así dar una solución a la situación actual del Ministerio del Ambiente y Agua.

En el tercer capítulo se realizan las pruebas de conectividad de las simulaciones para su validación, así como un análisis de resultados de la red corporativa diseñada verificando los objetivos propuestos.

El cuarto capítulo presenta las conclusiones y recomendaciones alcanzadas al realizar este Trabajo de titulación.

PALABRAS CLAVES: Seguridad, Alta disponibilidad, Servicio, Respaldo, Red corporativa.

ABSTRACT

The degree work presents the study and design of a corporate LAN network for the Ministry of the Environment and Water in terms of the management of the 3 services, using security mechanisms and high availability.

The first chapter describes security mechanisms in corporate LANs and high availability.

The second chapter describes the current scenario of the network of the Ministry of Environment and Water and based on the current requirements, a design of a corporate LAN network is proposed that includes security mechanisms and high availability.

The budget of the network components and the simulation of some segments of the corporate LAN network are also presented.

The concepts related to the different security and high availability mechanisms are included to apply to the design of this corporate network in order to provide a solution to the current situation of the Ministry of Environment and Water.

In the third chapter, the connectivity tests of the simulations are carried out for their validation, as well as an analysis of the results of the corporate network designed, verifying the proposed objectives.

The fourth chapter presents the conclusions and recommendations reached when carrying out this Degree Project.

KEYWORDS: Security, High availability, Service, Backup, Corporate network.

1. INTRODUCCIÓN

El Ministerio de Ambiente y la Secretaría del Agua son entidades independientes razón por la cual cada una de estas instituciones maneja su propia red de acuerdo a las políticas y leyes que rigen es estos organismos.

Actualmente por medio del decreto ejecutivo se fusionan estas dos instituciones en un solo denominado como Ministerio del Ambiente y Agua por la cual la red que manejan actualmente no se encuentra integrada en los 3 servicios.

En este capítulo se especifican los objetivos, alcance y marco teórico el cual se va a fundamentar para el desarrollo del Trabajo de Titulación.

Dentro del marco teórico se detalla los fundamentos de alta disponibilidad y mecanismos de seguridad para aplicar al diseño de la red LAN Corporativa.

1.1. OBJETIVOS

El objetivo general de este Proyecto Técnico es el Estudio y Diseño de una Red LAN Corporativa del Ministerio del Ambiente y Agua para el manejo de voz, datos y video, utilizando mecanismos de seguridad y alta disponibilidad.

Los objetivos específicos del Proyecto Técnico son:

- Recopilar la información de la situación actual de la red del Ministerio del Ambiente y Secretaría del Agua.
- Estudiar los principales mecanismos de seguridad y alta disponibilidad para la red LAN Corporativa del Ministerio del Ambiente y Secretaría del Agua.
- Diseñar la Red LAN Corporativa del Ministerio del Ambiente y Secretaría del Agua de acuerdo al decreto ejecutivo de fusión para manejo de voz, datos y video.
- Elaborar escenarios para simular en base a Packet Tracer determinados segmentos de la red diseñada.
- Determinar el presupuesto referencial de los costos para la implementación de la red diseñada.

1.2. ALCANCE

Este Trabajo de Titulación propone el Estudio y Diseño de una red LAN Corporativa para el Ministerio de Ambiente y Agua para el manejo de voz, datos y video utilizando mecanismos de seguridad y alta disponibilidad mediante el cumplimiento de cinco fases:

Fase 1: Se realizará la recopilación de la información de la situación actual de la red del Ministerio del Ambiente y Secretaría del Agua.

Fase 2: Se estudiará los principales mecanismos de seguridad de red y alta disponibilidad para una red LAN.

Fase 3: Se realizará el diseño de la Red Corporativa del Ministerio del Ambiente y Agua para el manejo de voz, datos y video.

Fase 4: Se realizará el presupuesto de Costos y Simulación de Segmentos de la Red del Ministerio del Ambiente y Secretaría del Agua.

Fase 5: Se realizará el análisis de Resultados de la Red LAN diseñada para el Ministerio del Ambiente y Secretaría del Agua.

No se contará con producto final demostrable, se presentará la simulación de algunos segmentos de la red propuesta (ver Figura 1.1).

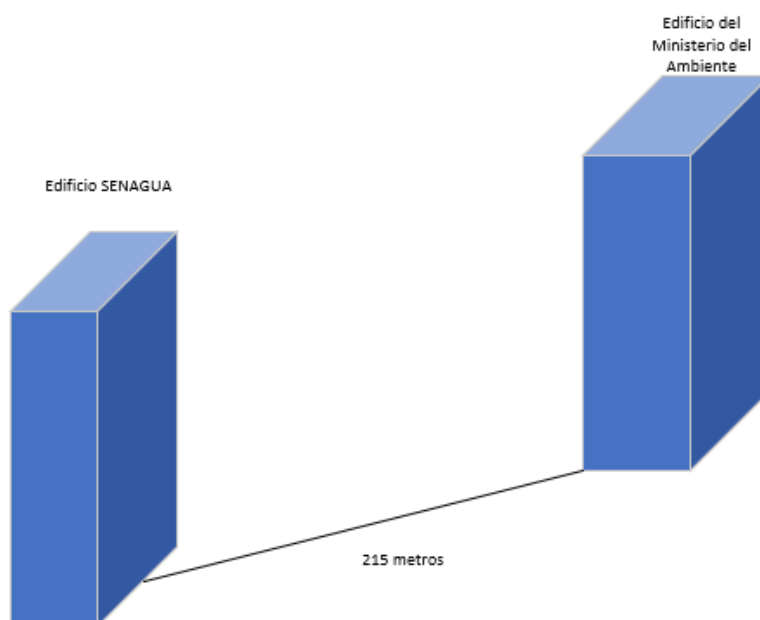


Figura 1.1. Edificios que se interconectarán a la Red.

1.3. MARCO TEÓRICO

La tecnología que se enfoca en las comunicaciones agrupadas, está en todos los ámbitos de la sociedad y siendo útiles en las actividades diarias. La seguridad informática tiene como objetivo el correcto funcionamiento de los cada uno de los componentes de la red de una organización o empresa, así como el correcto acceso a los mismos por personas autorizadas.

1.3.1. PARÁMETROS EN UN SISTEMA CONFIABLE [1]

La seguridad absoluta es imposible porque siempre existe un riesgo, por lo que la seguridad informática es una combinación de métodos enfocados a tener un alto nivel de seguridad en los sistemas en red.

Confiabilidad: Es la probabilidad de que un sistema tenga un comportamiento suficiente, por lo que se espera hablar más de sistemas confiables.

Un sistema confiable debe garantizar lo siguiente:

Confidencialidad: Es una condición de los mensajes, comunicaciones o datos que sólo una persona o sistema autorizado puede entender.

Integridad: Es la condición de un mensaje, comunicación o dato que permite verificar si existe manipulación del mensaje o dato.

Disponibilidad: Es la capacidad de un servicio, dato o sistema que los usuarios pueden utilizar en cualquier momento.

La información se puede recuperar para evitar pérdidas o bloqueos.

En términos generales, los tres aspectos mencionados deben estar presentes para tener seguridad.

Además de estos aspectos se debe mencionar otros conceptos fundamentales como la autenticación y el no repudio.

Autenticación: Autenticar la identidad del usuario ante el sistema a través de usuario y contraseña.

No repudio: Permite la intervención de todas las partes en la comunicación.

- **No repudio de origen:** El remitente no rechaza el envío, crea prueba de que el destinatario lo recibe.

- **No repudio de destino:** El receptor no puede negar que recibió el mensaje del remitente porque el remitente tiene constancia de la recepción del mensaje.

En general el repudio verifica la autenticidad durante la comunicación.

A este conjunto se denomina CIDAN (ver Figura 1.2).



Figura 1.2. Servicios de seguridad en forma jerárquica [1].

Como se puede ver en la figura la correspondencia de estos servicios de seguridad de manera jerárquica en la cual debe existir un nivel interior para poder aplicar el nivel exterior [1].

1.3.2. SEGURIDAD EN REDES CORPORATIVAS [1]

1.3.2.1. Amenazas y ataques

Los ataques e intrusiones a las redes son en general usuales y causan complicaciones en la disponibilidad de los servicios, pérdida de trabajo, información y dinero. Las iminencias se dividen de la siguiente forma:

Interrupción: Un servicio o dato se pierde en la comunicación y no está disponible.

Interceptación: Un componente sin autorización tiene accesibilidad al sistema.

Modificación: Además de tener acceso no permitido realiza modificaciones en el objeto o destruye un cambio que invalida.

Fabricación: Alteración del objeto original a uno similar para que al ser atacado sea difícil su detección.

En la práctica hay diferentes métodos de acometidas informáticos en la red como son:

Agresión de rechazo al servicio: O también denominado DoS que causa a un servicio de red sea inaccesible para usuarios autorizados provocando el consumo intenso de internet a través de la conectividad del cliente, sobrecargando los recursos del sistema usando botnet o red zombie pueden controlar gran cantidad de sistemas para saturar asaltos a los servidores.

Sniffing: Rastreo mediante monitoreo la cantidad de información que se envía por la red.

Man in the middle: El cual el atacante inspecciona la comunicación en los 2 sentidos, suplantando las identificaciones y recogiendo información bilateralmente.

Spoofing: Habilidad de Producción, negando la identidad o cumpliendo una falsa identidad.

Pharming: Técnica de Modificación en la cual explota las debilidades en los servidores DNS o en los dispositivos del usuario final, cambiando los valores del DNS con otro dominio de un dispositivo falso [1].

1.3.2.1.1. Inminencias exteriores e interiores

Las iminencias en cuanto a seguridad en las redes corporativas pueden ser de exteriores o interiores.

Inminencia exterior: Los atacadores están fuera de la red e ingresan interiormente a la red sin permiso. Los servidores o routers son atacados desde el exterior con la finalidad de ingresar a la red.

Inminencia interior: Ocurre cuando los atacadores ingresan sin permiso a la red e incluso son parte de la red interna. De manera que comprometen la seguridad, información y servicios de la institución.

Para esto mencionaremos soluciones de defensa de la seguridad en la red corporativa y disposición de medidas de defensa en los dispositivos de borde que son de mayor ataque recibido desde el exterior [1].

1.3.2.2. Sistemas de detección de intrusos (IDS)

Son instrumentos de protección que detectan acontecimientos presentes en un sistema en la indagación de sucesos inusuales que compliquen la seguridad de red. Buscan patrones de actividad sospechosa sobre la red y previenen o alerta de una actividad sospechosa. No detiene el ataque, pero aumentan la seguridad vigilando la cantidad de información que se envía o recibe por la red para hallar sucesos dudosos.

IDS (Intrusion Detection System): Es un programa de seguridad que detecta accesos no autorizados a un sistema.

Los tipos de IDS son:

HIDS (host IDS): Monitorea los eventos y cuida al servidor. Además, examina acciones con una buena exactitud estableciendo los procesos y usuarios que involucran una acción. Recopilan información del sistema para el estudio y búsqueda de sucesos inusuales.

NIDS (Net IDS): Cuida al sistema de red. Recoge y examina los datos buscando patrones de asalto. Manejan un dispositivo de red establecido en estado heterogéneo para proceder.

La arquitectura de un IDS está conformada de lo siguiente:

- El origen de recolección de información.
- Normas y filtros sobre antecedentes y pautas para descubrir rarezas.
- Dispositivo generador de informe o alarma, en unos casos es suficiente una alerta vía email o SMS.

Es recomendable ubicar los IDS en los extremos del cortafuego de borde en la red. De esta forma se posee datos precisos de las inminencias, con una correcta configuración del firewall que detenga inminencias. [1].

1.3.2.3. Inseguridades permisibles en los servicios de la red

TCP/IP es la arquitectura de protocolos más empleada en los computadores para conectarse a Internet. Se usan puertos o numeración lógica que se determina para asemejar las conexiones de red en los extremos del sistema de comunicación. Los puertos son específicos para cada servicio de red. El puerto 80 para el protocolo HTTP, el puerto 21 para transferencia de archivos FTP, etc.

Las diferentes aplicaciones y sistemas de red envían y recogen servicios por medio de los puertos. El análisis de puertos se realiza en:

- Una máquina local viendo los puertos y conexiones que quedan habilitados o el control de las aplicaciones sobre los puertos.
- Netstat es un comando que en tiempo real observa el cambio de las conexiones.
- Los firewalls son instrumentos de seguridad en contra de las inminencias exteriores.
- La administración de la red examina el estado de los puertos de un grupo de dispositivos.
- Nmap; de un conjunto de direcciones escanea puertos, aplicaciones y sistemas operativos.
- Los firewalls y proxys de borde realizan la filtración de puertos en conexiones tanto entrantes como salientes, de esta manera prometen protección [1].

1.3.2.4. Comunicaciones indudables [1]

Gran parte de las comunicaciones de red no manipulan cifrado como los protocolos HTTP, FTP o SMTP/POP. Hay protocolos que usan comunicaciones cifradas como SSH a través del puerto 22, tolerando protocolos de transferencia de archivos de manera segura como SFTP.

Existen 2 elecciones cifrando comunicaciones de diferente nivel como:

SSL y TLS: Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS), utilizan TCP y se establecen en una capa en los protocolos de aplicación. Se aprovecha a través de puertos como: HTTPS, FTPS, SMTP, POP3, etc.

IPSEC o Internet Protocol Security, es un conjunto de protocolos en la cual su finalidad es conservar las comunicaciones indudables y fiables, usando el protocolo IP y realizando la autenticación de los datos [1].

1.3.3. ALTA DISPONIBILIDAD [1]

Es el aforo de que los servicios, datos y aplicaciones de un sistema estén operativos y disponibles para los usuarios en todo momento y sin interrupciones ya que son críticos. Su objetivo es que se encuentre funcionando en todo momento sin dificultades. Tomando en cuenta 2 tipos de interrupciones:

- **Interrupciones previstas:** Sucede cuando se interrumpe el sistema para realizar cambios o mantenimientos del mismo.

- **Interrupciones imprevistas:** Sucede por acontecimientos no contemplados (apagón, errores del sistema, desastres naturales, etc.)

Para calcular la confiabilidad y disponibilidad de un sistema se utilizan las siguientes métricas:

- **MTTF (Mean Time to Failure):** Calcula el tiempo que pasa cuando un dispositivo falla.
- **MTTR (Mean Time to Recover):** Calcula el tiempo en el que la situación vuelve a la normalidad después del fallo.

Lo primordial será el decremento del MTTR y el incremento del MTTF para reducir el tiempo del servicio que no esté disponible.

Los niveles de disponibilidad varían en función del tiempo sin actividad anual aproximado.

Para lograr una disponibilidad del 99.999% se requiere de 5 minutos sin actividad de la red anual.

1.3.3.1. Soluciones de alta disponibilidad

Las redes de las empresas conviene que sean tolerantes a errores para alcanzar alta disponibilidad, la instalación de sistemas de respaldo de los dispositivos más decisivos para que el tiempo de inactividad sea lo mínimo posible.

Para sistemas que requieren una gran protección, se requieren:

- **Respaldo en equipos hardware**, facilitando la continuidad del servicio como por ejemplo servidores, fuentes de electricidad (ver Figura 1.3), generadores eléctricos.



Figura 1.3. Fuente de alimentación [1].

- **Respaldo, repartición y confiabilidad en administración de los datos.** Se certifica que los datos son recuperables, evitando su detrimento o asedio en cuanto a las inminencias. Los métodos manejados conforman:
 - o Sistemas de acopio RAID.
 - o Centro de procesamiento de información de acopio, certificando copias de seguridad en diferentes localizaciones.

- **Respaldo en las comunicaciones.** Actualmente la red entre las oficinas de la empresa está conectada al igual que los servicios deben estar activos. Si la red se encuentra con fallas, se opta por tener conexiones de red distintas en independientes. Como alternativa se utiliza el balanceo de carga.
- **Respaldo y repartición en el procesamiento de datos.** Mediante la utilización de sistemas de asociación de servidores o clustering para remontar la cabida en el proceso.
- **Configuración de servicios y aplicaciones y Administración Independiente.** Usando un entorno virtual el cual se refiere a servidores soportados dentro de una misma máquina [1].

1.3.3.1.1. Raid [1]

(Redundant Array of Independent Disks), almacena la información entre los diferentes discos duros con la finalidad de repetir o repartir los datos.

La repartición de la información es gestionada por:

- **Hardware:** Para la gestión de los discos, se usa un controlador RAID específico que puede ser una tarjeta integrada en la placa o de extensión independiente. Ofrece un mejor rendimiento en el reemplazo del disco mediante el cambio en caliente sin afectar al sistema.
- **Software:** La administración de los discos se realiza mediante el sistema operativo por medio del controlador del disco.
- **Híbridos:** Se basa en los 2 anteriores con la utilización de controladoras RAID hardware baratas o controladoras de disco sin RAID y el manejo de un programa de nivel inferior que cimienta RAID vigilado por BIOS.

Las configuraciones RAID más utilizadas son:

RAID 0 data striping: Reparte la información imparcialmente en los discos sin datos de equivalencia, facilitando el respaldo. Empleado con el fin de aumentar el rendimiento o la creación de grandes discos virtuales de pequeños discos físicos (ver Figura 1.4).

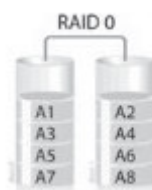


Figura 1.4. Distribución RAID 0 [1].

RAID 1 o data mirroring: Realiza una copia exacta de la información entre los discos. En el caso de fallo de un disco, se tiene otro disco con respaldo de la información similar aumentado así la confiabilidad. Los discos tienen la misma actitud de un solo disco en el modo de escritura (ver Figura 1.5).

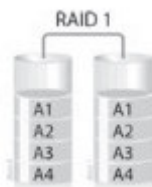


Figura 1.5. Distribución RAID 1 [1].

RAID 5 conjunto fraccionado y equivalencia repartida: Fracciona la información en bloques repartiendo los datos equivalentes en todos los discos. Aumentando los datos equivalentes en los diferentes discos, cuando empiezan a fallar, se puede recuperar la información a partir del contenido de los otros discos. RAID 5 es popular gracias a su bajo costo de redundancia (ver Figura 1.6).



Figura 1.6. Distribución RAID 5 [1].

Muchas controladoras pueden anidar niveles RAID, puede usarse como elemento básico en vez de otros discos físicos. Los RAID anidados se muestran acoplando en una cantidad los adecuados niveles RAID, usado sumando un +.

Al unir niveles de RAID se combina de tal manera que tenga respaldo a un RAID 0 que incremente utilidad por lo que es recomendable conservar como nivel alto al RAID 0 para la reconstrucción de menos discos en casos de fallos [1].

1.3.3.1.2. *Balaceo de carga*

Es un dispositivo que se conecta a la unión de servidores con la finalidad de determinar y distribuir las peticiones. Utiliza algoritmos como el Round Robin, en cuanto a la repartición balanceada de carga.

Reparten la carga y excluye las conexiones deficientes momentáneas entre la comunicación de un usuario con el servidor DNS. El balanceo de carga redirecciona las peticiones a un servidor DNS diferente que se ha establecido al equipo conectado del balance de carga.

Puede unificar 2 o más conexiones de red en una sola salida a Internet. Al usar un balanceador de carga se reparte la carga saliente hacia el Internet definiendo la cantidad de peticiones por línea [1].

1.3.3.1.3. Entornos virtuales

Se utiliza una aplicación instalada dentro de un dispositivo para ejecutar varios sistemas operativos dentro de un mismo terminal. Efectúa el enajenamiento de los medios del sistema, permitiendo la compartición y gestión dinámica de los medios del terminal a todas las máquinas virtuales dentro de un mismo equipo físico.

Los provechos de la virtualización son ahorro de costos y espacio, crecimiento flexible ya que es más fácil instalar servidores virtuales que servidores físicos, fácil administración desde una sola consola manejando los recursos de cada máquina virtual, disminución de tiempos de parada realizando copias de seguridad en menos tiempo como puede ser clonando la máquina mientras se realiza mantenimiento, gestión y balanceo de recursos [1].

2. METODOLOGÍA

2.1. SITUACIÓN ACTUAL DE LA RED

Para establecer el esquema de una red fusionada de voz, datos y video se debe efectuar un análisis previo de la red actual de la institución, para solventar los requerimientos.

Este capítulo está enfocado a determinar la situación actual de la institución, representando la construcción actual de este Ministerio y especificando las exigencias requeridas para el diseño de la red del Ministerio de Ambiente y Agua para gestionar los servicios como Transferencia de archivos, Telefonía IP, Video seguridad entre otros.

Dentro de la descripción de la infraestructura física se indica los elementos activos y pasivos con los que cuenta, así como la administración de la red que se mantiene dentro de las diferentes áreas.

Con el levantamiento de información se tendrá un enfoque más claro del estado actual de este Ministerio con el cual se podrá implementar el diseño de la red.

2.2. MINISTERIO DEL AMBIENTE Y AGUA [2]

Esta institución certifica un ambiente ecológico equilibrado, además de la conservación de la biodiversidad y del ambiente, se siembra al progreso. Además, reconoce a los recursos naturales como el agua, suelo y aire como vitales.

El día 4 de octubre de 1996, se forma esta institución conforme al Decreto Ejecutivo No 195 por el expresidente Abdalá Bucarán.

La Secretaría Nacional del Agua (SENAGUA) lleva y administra los procesos del agua a nivel nacional de un modo fusionado en los contornos de las cuencas hidrográficas

El día 15 de mayo del 2008, se forma esta institución conforme al Decreto Ejecutivo No 1088.

El día 4 de marzo del 2020, conforme al Decreto Ejecutivo No 1007, establece la unión de las dos instituciones, en una sola institución designada: Ministerio del Ambiente y Agua.

La institución se encuentra en la ciudad de Quito. La Figura 2.1 indica el mapa de donde se encuentran estas instituciones [2].

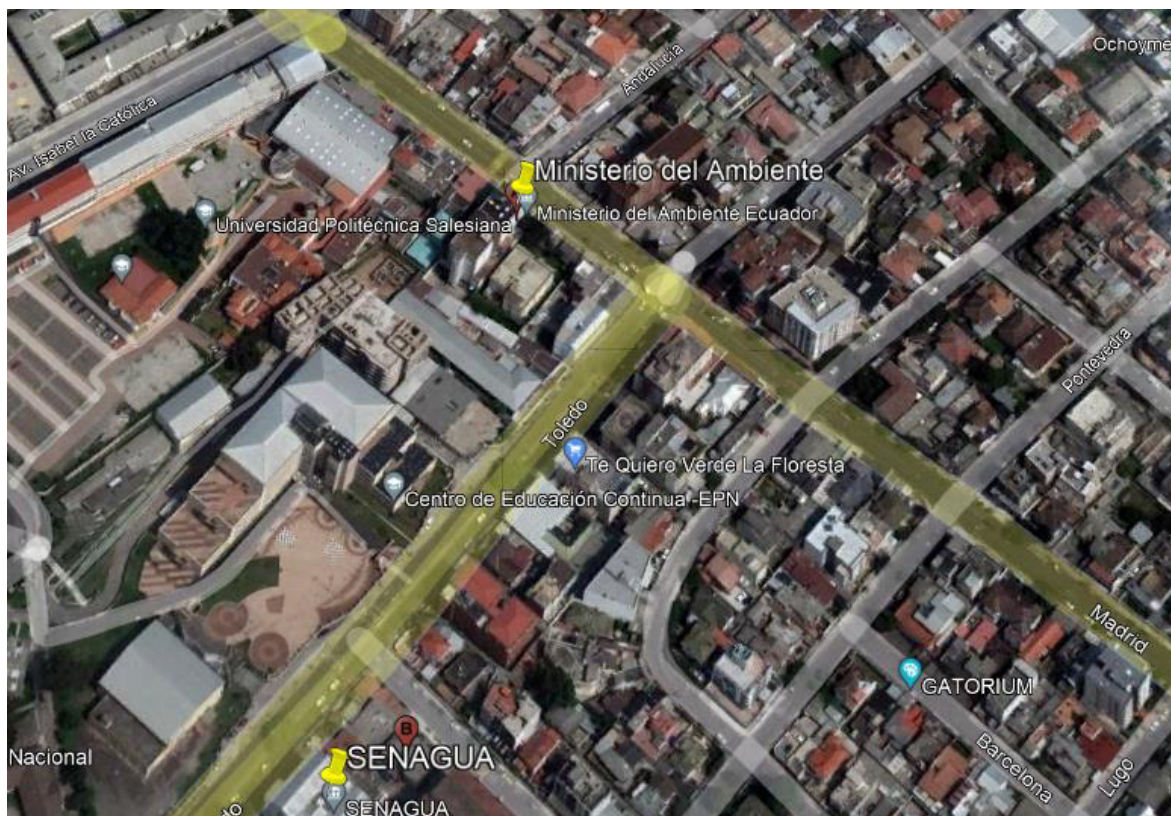


Figura 2.1. Mapa de la ubicación de los Edificios SENAGUA y Ministerio del Ambiente.

2.2.1. MISIÓN DEL MINISTERIO DEL AMBIENTE Y AGUA

Garantizar la calidad, conservación y sostenibilidad de los recursos naturales, mediante el ejercicio efectivo de la rectoría, planificación, regulación, control, coordinación y gestión ambiental y de los recursos hídricos, a través de la participación de organizaciones públicas, privadas, comunitarias y la ciudadanía, en el marco del respeto, integridad, responsabilidad y transparencia [3].

2.2.2. VISIÓN DEL MINISTERIO DEL AMBIENTE Y AGUA

Al 2025, ser la institución que garantice la calidad de los servicios ecosistémicos, a través de procesos y servicios institucionales eficientes que impulsen la conservación, remediación y aprovechamiento de los recursos naturales [3].

2.3. DESCRIPCIÓN DE LA INFRAESTRUCTURA FÍSICA

Primero empezamos por describir la distribución física de los edificios que compone esta institución.

El Ministerio del Ambiente es un edificio de 7 pisos que consta de la siguiente manera:

Parqueadero: En el cual se encuentra la zona de estacionamiento de vehículos, una bodega automotriz y un cuarto de generador de emergencia.

Planta baja: En el cual se encuentra ubicado la Cafetería, Consultorio Médico, Secretaría General, Sala de espera, Información, Archivo, Secretaría, Control CCTV, Auditoría interna, dirección, Proyectos de Calidad Ambiental, Atención al público, Salón de usos múltiples y Mantenimiento de Administración Financiera.

Primera planta alta: En el cual se encuentra ubicado el cuarto del Director, Subsecretario, Control de Calidad, Subsecretaria, Cambio Climático de Calidad Ambiental, Secretaría, Control Ambiental, Archivo mecánico, Sala de reuniones, Asesor y Archivo mecánico.

Segunda planta alta: En la cual se encuentra ubicado el cuarto de Prevención de Contaminación de Calidad Ambiental, Gestión Ambiental, Director, Archivo mecánico, Secretaría, Procesal, Cafetería y Sala de Reuniones.

Tercera planta alta: En el cual se encuentra ubicado el cuarto de Dirección Financiera, Proyecto de Reparación Ambiental y Social Jurídico Administrativo, Director, Taller, Secretaría, Taller, Servidores, Sala de Sesiones, Contabilidad y Seguimiento, Plotter, Coordinador, Área Técnica y Calidad Ambiental.

Cuarta planta alta: En el cual se encuentra ubicado el cuarto de Patrimonio Natural Biodiversidad, Archivo mecánico de biodiversidad, Director, Subsecretario, Secretaría, Asesor, Archivo mecánico forestal, Cafetería y Sala de Espera.

Quinta planta alta: En el cual se encuentra ubicado el cuarto de Dirección Administrativa, Director, Secretaría, Director de Recursos Humanos, Director Financiero, Tesorería, Recursos Humanos, Desarrollo Institucional, Suministros, Archivo mecánico Administrativo y Recaudaciones.

Sexta planta alta: En el cual se encuentra ubicado el cuarto de Investigación, Información, Director, Secretaría, Cafetería, Impresión/copiado, Educación Ambiental, Subsecretaria, Asesor, Director Planificación - Políticas, Archivo mecánico y Archivo del Subsecretario.

Séptima planta alta: En el cual se encuentra ubicado el cuarto del Despacho del Viceministro, Secretaría, Sala de espera, Salón del Gabinete ("Verde") Sala interactiva, Despacho de Ministro, Asesor Ministro, Archivo y Antesala.

Terraza: En la cual se encuentra ubicado los cuartos de máquinas.

La Secretaría del Agua es un edificio de 5 pisos que consta de la siguiente manera:

En la parte del fondo se encuentra:

Subsuelo: En el cual se encuentra el cuarto de materiales de limpieza y de bombas, DH Esmeraldas y Asesor.

Primera planta baja: en el cual se encuentra el Centro de Datos, DTIC, Documentación y Archivo y Recepción de Documentos.

Segunda planta baja: En el cual se encuentra la Dirección de Comunicación Social, Bodega y Área Jurídica.

Tercera planta baja: En el cual se encuentra la Subdirección de Riego y Drenaje, Sistemas de Información.

Cuarta planta baja: En el cual se encuentra la Subdirección del Agua Potable y Saneamiento.

Quinta planta baja: En el cual se encuentra la Dirección de Talento Humano, Coordinación General Administrativa y la Dirección Administrativa.

Como extensión del edificio, en la parte de adelante se encuentra:

Planta baja: En el cual se encuentra el Salón Auditorio, Vestidores, Centro de atención al ciudadano.

Primera planta alta: En el cual se encuentra el Secretario Nacional, Oficina del Subsecretario, Articulación territorial Porcelanato, Porcelanato y Cocina.

Segunda planta alta: En el cual se encuentra la Subsecretaria Nacional, Plan Nacional del Agua, Dirección Técnica, Subsecretaria Técnica y Dirección Administrativa de Recursos Humanos.

Tercera planta alta: En el cual se encuentra la Dirección Política de Servicios de Agua Potable y Saneamiento y Auditoría.

Cuarta planta alta: En el cual se encuentra la Coordinación General de Planificación, Dirección Financiera y Archivo.

Quinta planta alta: En el cual se encuentra la Cafetería, Oficinas y Salón.

2.4. DESCRIPCIÓN ACTUAL DE LA RED

La red actualmente no se encuentra unificada entre los 2 edificios debido a que se manejaban como redes independientes tanto el Ministerio de Ambiente como la Secretaría del Agua, por lo que mediante el decreto ejecutivo de fusión estas instituciones deben integrarse en uno solo.

Estas redes fueron creadas según especificaciones de la época y en base a las necesidades de cada Institución. Cada edificio maneja una red diferente debido a que eran instituciones independientes.

La Red del Ministerio del Ambiente conserva un datacenter que cuenta con climatización (dos aires acondicionados en redundancia), energía regulada UPS 40KVA y redundancia del UPS, sistema contra incendio y sistema de monitoreo; adicional se realiza mantenimientos preventivos y correctivos sobre el equipamiento (ver Figura 2.2) [4].

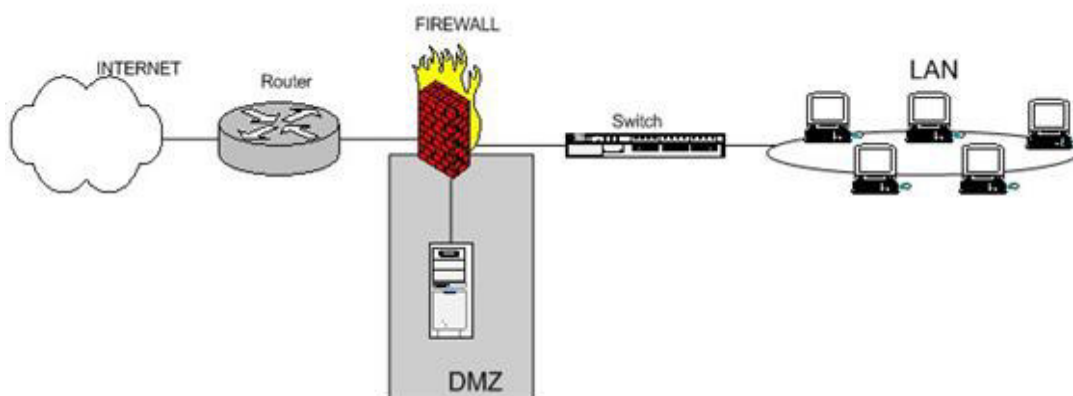


Figura 2.2. Red Actual del MAE [5].

La red del SENAGUA mantiene dos datacenters, uno contratado a CNT y otro que servía como respaldo y en su propia red no dispone de redundancia tanto en la capa de Core y distribución.

Cuentan con un switch Core PALOALTO y no cuenta con garantía, servicio técnico, respaldo, los demás switches de distribución están en cada uno de los pisos. En el cuarto de datos se encuentran 2 switches de distribución que son del subsuelo y primera planta baja. Solo el cuarto de equipos principal y el último piso son cuartos independientes de telecomunicaciones. Los demás equipos de los demás pisos se encuentran en racks abiertos sin un cuarto específico.

Tiene 2 firewalls uno activo y otro por redundancia para validar el tráfico como seguridad perimetral (ver Figura 2.3).

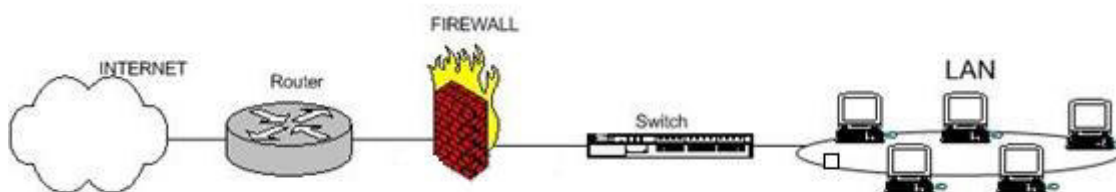


Figura 2.3. Red Actual del SENAGUA [5].

2.5. ANÁLISIS DEL ESQUEMA ACTUAL DE LA RED

Las redes de cada institución son creadas de manera independiente.

La Red del Ministerio del Ambiente utiliza puertos Fast Ethernet y cable UTP categoría 6A.

Las topologías son de tipo estrella jerárquica independientes, por lo que se requiere el manejo de una topología que unifique las infraestructuras independientes en una sola red.

En la actualidad se manejan estas 2 instituciones como redes independientes, por lo se va a proponer un esquema de Red Corporativa que unifiquen las anteriores instituciones, permitiendo así una buena gestión de los recursos y certificando una administración eficiente, de alta disponibilidad y seguridad [6].

2.6. EQUIPOS QUE CONFORMAN LA RED ACTUAL

Para la realización de un diseño de red de comunicaciones se requiere saber de los equipos con los que cuenta el Ministerio actualmente, es decir si los elementos y equipos están en funcionamiento o es necesario el reemplazo de otro equipo.

A continuación, se describen los equipos de conectividad, entre otros con los que cuenta las dos instituciones.

2.6.1. COMPONENTES PASIVOS DE LA RED

Son los que permiten la conexión en una red de datos es decir solo transmiten señales.

Dentro de los componentes pasivos de la red tenemos la estructuración de cables y sus elementos que lo conforman como son: armarios, tomas, cables, ductos, canaletas, etc. [7].

2.6.1.1. Sistema de Cableado Estructurado (SCE) de la red actual [8]

La red del Ministerio del Medio Ambiente cuenta con un backbone de Fibra Óptica de 6 hilos multimodo 62.5/125 um con chaqueta reforzada para ductos.

Dispone además de MDF y de SDFs por piso, en el 7mo piso solo se encuentra un armario abatible de pared de 12 unidades. Cada rack tiene organizadores verticales.

El Sistema de cableado estructurado conforman los elementos que cumplen con el estándar TIA/EIA 568B.2-10 para categoría 6A.

Debido a que han existido cambios de ubicación y movimiento de puesto de trabajos, se presentan daños en etiquetados de cables de red y daños físicos en cableado. En la Figura 2.4 se muestra el cableado del rack principal del Ministerio de Ambiente.



Figura 2.4. Cableado del rack principal del Ministerio del Ambiente.

La red del SENAGUA con backbone de fibra óptica al igual que la red del Ministerio del Ambiente.

El sistema de cableado estructurado utiliza un cableado categoría 5e. El estado del cableado de la red de la Secretaría del Agua en la cual se puede observar que se tiene un cableado desorganizado (ver Figura 2.5).

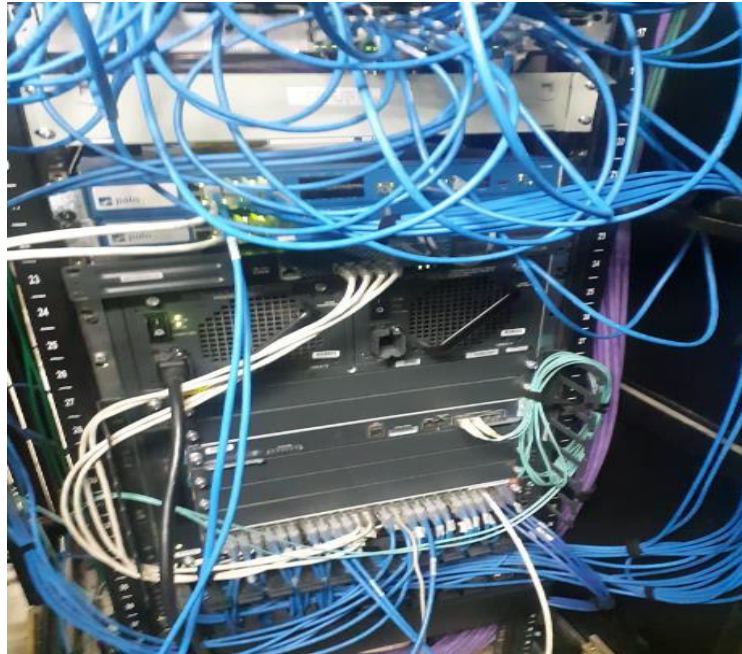


Figura 2.5. Cableado del rack principal del SENAGUA.

2.6.1.2. Sistema de Puesta a Tierra de la red

El sistema efectuado en esta red es de tipo mallado mediante el establecimiento de las representaciones del estándar TIA/EIA-607, debido a que cubre toda la instrumentación mecánica incluido el cuarto de telecomunicaciones.

Este sistema a tierra está realizado adecuadamente para la conexión de los diferentes dispositivos de red y con las protecciones requeridas.

2.6.2. ESTUDIO DE LOS COMPONENTES PASIVOS

Los componentes que conforman la red del Ministerio del Ambiente si están en buenas condiciones y fueron levantados con las respectivas normas anteriormente mencionadas, las instalaciones están en buenas condiciones en este caso no habrá una caída de la red por lo cual se sigue manteniendo.

Por lo cual los elementos de la red del Ministerio del Ambiente pueden ser reutilizados en el diseño casi en su totalidad.

2.6.3. ELEMENTOS ACTIVOS DE LA RED

Son elementos electrónicos que distribuyen información a la red como: concentradores switches, router, etc.

Las 2 instituciones antes mencionadas tienen redes LAN separadas e independientes.

En la red del Ministerio del Ambiente, el switch de Core no cuenta con redundancia, pero tiene garantía y soporte del fabricante por 3 años, incluye reemplazos del mismo, cambio de partes y piezas en caso de daños.

Pero ya paso 10 años desde su implementación y corre el riesgo de que la red falle y se pierda gran cantidad de información.

La red del SENAGUA no dispone de redundancia tanto en la capa de Core y distribución por lo cual puede estar en riesgo de que falle la red y se pierda información al igual que la red anterior.

Estos aspectos hay que considerar para el diseño de la red en cuanto a redundancia de equipos sobre todo en las capas de la red que son más críticas y afecten el rendimiento de la red.

La Tabla 2.1 presenta un listado de los equipos activos más importantes de la red.

Tabla 2.1. Lista de los principales dispositivos activos de la red del Ministerio del Ambiente

CANTIDAD	EQUIPO	MODELO
24	Switch	WS-C2960S-24TS-L
2	Switch	WS-C2960X-48TS-L
14	Switch	WS-C3560X-24T-S
1	Switch de Core	C6807-XL-S2T-BUN
1	Wireless LAN controller	AIR-CT5508-K9
19	Access point	AIR-CAP2702E-A-K9
1	Access points	AIR-CAP2602I-A-K27
1	Modular switch	C6807-XL (M8572)
2	Firewall	ASA 5525-X
2	Equipos para el control de los accesos a la red	Identity Services Engine (ISE) C6807-XL-S2T-BUN

2.6.4. ESTUDIO DE LOS ELEMENTOS ACTIVOS

Se determina que los equipos activos de la red funcionan de manera correcta sin embargo los switches ya no tienen garantía es decir que ante cualquier fallo de estos equipos no tendrán soporte técnico por lo cual peligra la red a que falle o no puede estar disponible en

cualquier momento. Por lo cual estos equipos deben tener redundancia para lo cual se tomará en cuenta en el diseño de la red.

2.6.5. SISTEMA DE TELEFONÍA ACTUAL

La red del Ministerio del Ambiente cuenta con el OmniPCX Enterprise es un PBX con una construcción IP.

Los principales elementos del OmniPCX Enterprise son:

- Un Call Server, CPU del sistema,
- Un (o más) Media Gateway que tolera dispositivos de telefonía clásica:
- Teléfonos Digitales (o UA) o Analógicos,
- Líneas públicas o privadas,
- Teléfonos móviles DECT,
- Guías vocales,
- Compresores para la comunicación entre telefonía clásica y telefonía IP.
- Teléfonos Digitales (o UA) o Analógicos,
- Teléfonos IP (IP-Phones, Terminales H323/SIP),
- Teléfonos móviles DECT o Wireless.

El Call Server del OmniPCX Enterprise emplea el sistema operativo Linux. Guarda la información de configuración del PBX en una base de datos, en memorias los estados de cada componente (por ejemplo, si un teléfono tiene desvío).

Cada nuevo evento (una llamada entrante, ...) será transmitido del Call Server a la Media Gateway. Dependiendo del estado del teléfono, el Call Server decide las acciones a ejecutar. Por ejemplo: el caso del descolgado de un teléfono al estado de reposo, el Call Server emite un mensaje por el canal IP al Media Gateway para reproducir el tono de descolgado. La Media Gateway conecta la tonalidad con el teléfono.

Protocolos usados:

- Las comunicaciones de Voz IP: G711, G723 o G729,
- Las comunicaciones de Fax: T38. [7]

El sistema de telefonía que tiene SENAGUA es una central IP que funciona con un software libre Elastix en un servidor virtualizado, toda la telefonía va en el canal de datos con la Vlan de voz correspondiente. Cada teléfono IP (ver Figura 2.6) cuenta con su extensión. Cuentan con 104 extensiones activas, aquí se encuentran incluidos teléfonos de provincias y las del Ministerio del Ambiente.



Figura 2.6. Teléfono IP utilizado en el Sistema de Telefonía actual del SENAGUA.

2.6.5.1. Estudio del Sistema de Telefonía

Actualmente la central telefónica cuenta con la configuración de líneas analógicas y digitales E1 con el proveedor CNT por donde se realizan y se reciben llamadas al exterior. El sistema de Telefonía del Ministerio de Ambiente se encuentra sin garantía ni soporte técnico del fabricante desde el 31 de mayo del 2013 por lo tanto no es factible que el Departamento Tecnológico garantice la continuidad en el servicio de telefonía del edificio de Planta Central en caso de presentarse daños fortuitos en el hardware que requieran reposición de partes o piezas de la infraestructura telefónica o a su vez a nivel de software de administración.

Se requiere de garantía de los equipos que conforman para que este servicio se encuentre en funcionamiento o el cambio a un sistema de telefonía que brinde garantía y soporte técnico.

2.6.6. SISTEMA DE VIDEO ACTUAL

La red actual del Ministerio del Ambiente cuenta con el servicio de videoconferencia con una conexión de video conferencia interministerial y externas a través de un equipo Polycom o con el sistema de video conferencia Aetra que son los equipos estándares que todos los Organismos del Estado cuentan en vista de que esta dotación lo realizó la Presidencia de la República del Ecuador.

La red del SENAGUA cuenta con un servidor de video con sistema Operativo Windows 10, utilizan cámaras IP y software Vivotek. Se cuenta con 25 cámaras, pero ya cumplieron con su vida útil y pues fallan cuando existe corte eléctrico o una falla en el switch, ya que las cámaras se conectan desde los puertos del switch ya que utilizan PoE.

PoE (Power over Ethernet) suministra la corriente a los componentes activos de red por medio un cable de red [7].

Tiene una duración de 7 días la grabación de cada cámara y luego se reescribe el último registro. Fueron adquiridas en el 2015 y ya cumplieron su vida útil de 3 años y ya no tienen garantía o en el caso que falle por componentes internos.

2.6.6.1. Estudio del Sistema de Video

De acuerdo con el sistema de video que tiene la red actual del Ministerio del Ambiente y del SENAGUA, pues funciona correctamente pero tampoco se encuentra con garantía y en el caso de que fallen los equipos no están garantizados a un reemplazo.

Por lo que la solución sería reemplazo de cámaras tomando en cuenta compatibilidad con el sistema de video existente.

2.6.7. RED INALÁMBRICA ACTUAL

La red inalámbrica del Ministerio del Ambiente está administrada por el Wireless LAN controller Cisco (ver Figura 2.7) a todos los Access Point como se indica en la Figura 2.8 con sus respectivos perfiles como funcionarios, Autoridades.

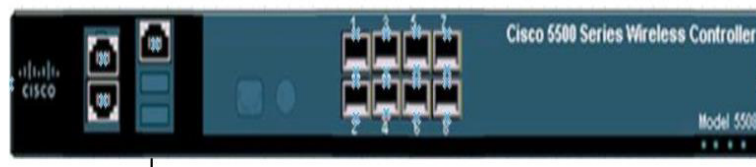


Figura 2.7. Controlador Inalámbrico CISCO.

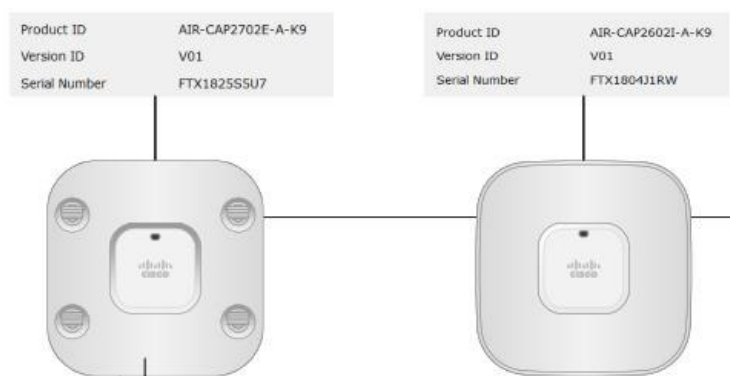


Figura 2.8. Modelos de AP utilizados actualmente en el Sistema Inalámbrico.

El diseño inalámbrico del Ministerio del Ambiente tiene los puntos de acceso del servicio autónomo en cada piso con un SSID común, por lo cual el tráfico sería manejado conjuntamente con el generado por el piso.

También el sistema opera en un ambiente VLAN, el tráfico de administración puede ser llevado bajo su propia VLAN inalámbrica repartiendo los puntos accesibles en modo controlado. De esta manera el tráfico puede ser mapeado a nivel de puntos de acceso y a nivel de control para direccionar el tráfico.

2.6.7.1. Estudio de la Red Inalámbrica

Actualmente estos equipos inalámbricos no cuentan con SMARNET (soporte y mantenimiento), por lo que estos equipos cumplieron con su vida útil de 3 años por lo que si fallan estos dispositivos inalámbricos pueden quedarse sin servicio de Internet lo cual es crítico en esta institución.

2.6.8. SERVICIO DE INTERNET CONTRATADO ACTUALMENTE

La red del Ministerio del Ambiente tiene interconexiones externas con CNT (internet y anillo de datos Gubernamental) mediante los servicios vigentes (ver Tabla 2.2).

Tabla 2.2. Lista de los principales servicios que provee CNT al Ministerio del Ambiente

TIPO DE SERVICIO	Datos
Ancho de Banda	10 Mbps
Redundancia	A nivel de Última Milla, según disponibilidad.
Disponibilidad del servicio	99.8%
Servicios adicionales SEGURIDAD DNS	Protección Perimetral basados en equipos UTM específicos para la Red Nacional Gubernamental. Servicio de DNS Zonas (Servidores internos dedicados para la Red Gubernamental).
TIPO DE SERVICIO	Internet
Ancho de Banda	80 Mbps
Redundancia	A nivel de Última Milla, según disponibilidad.
Disponibilidad del servicio	99.8%
Servicios adicionales SEGURIDAD DNS	Servicio de Canal Seguro "SCS" Servicio de DNS de Cache Corporativos, para navegación

CNT provee un canal de Internet de 20 Mbps de última milla a SENAGUA con disponibilidad de servicio del 99.8%.

2.6.8.1. Estudio del Servicio de Internet

Se mantiene la administración del servicio de enlaces e internet sin percances presentados, es recomendable dar seguimiento al proceso de firma y pago.

2.7. DISEÑO DE LA RED LAN CORPORATIVA PARA EL MINISTERIO DEL AMBIENTE Y AGUA

2.7.1. VISIÓN

La red unificada para esta institución, permitirá crear un sistema centralizado, seguro, con mecanismos de seguridad y alta disponibilidad. Con este procedimiento se completarán los servicios más manejados, con el fin de facilitar una comunicación interna dentro de los edificios, así como la comunicación entre edificios de manera eficiente y segura.

El Ministerio ha visto necesario describir con servicios de video para aumentar la seguridad de la institución en todos los pisos de los edificios.

2.7.2. MODELO DE RED PROPUESTO

Para el diseño de red LAN para esta institución Corporativa, utilizaremos el modelo jerárquico el cual permite implementar y administrar la red en forma eficiente.

El diseño jerárquico fracciona la red en capas autónomas, con funciones específicas dentro de la red. La referencia estructurada e instituida por el Fabricante Cisco concreta 3 capas: acceso, distribución y núcleo.

Utilizaremos redundancia en las capas de Distribución y Núcleo para tener alta disponibilidad de la red, así evitando cortes e interrupciones en la red (ver Figura 2.9) [8].

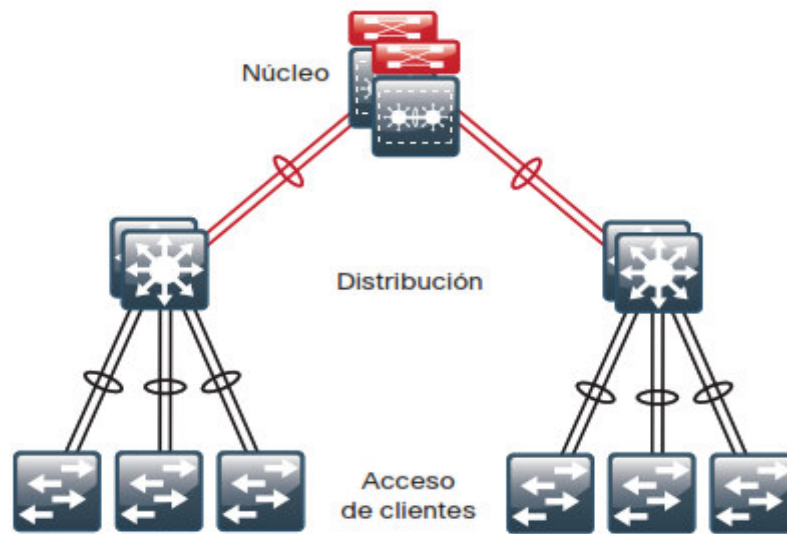


Figura 2.9. Diseño LAN en capas [8].

2.7.2.1. Capa de Acceso

Es aquella capa que facilita el ingreso de a la red a usuarios y grupos de trabajo. Ofrece conectividad tanto inalámbrica y cableada y tiene características y servicios para certificar seguridad y recuperabilidad para la red [9].

2.7.2.2. Capa de Distribución

Provee conectividad establecida en políticas y controla el límite entre las capas de acceso y de núcleo.

Sirve como punto de agregación para múltiples switches de la capa de acceso y aumenta la disponibilidad de red [9].

2.7.2.3. Capa de Core

Es la encargada para la interconexión entre los dispositivos de la capa inferior del modelo jerárquico y debe ser redundante y disponible para evitar interrupciones en la red.

Su función principal es conmutar tráfico a gran velocidad llevando información de manera confiable [9].

2.7.3. TECNOLOGÍA DE RED A UTILIZAR

Para el diseño de la Red LAN Corporativa para la institución se debe optar por una tecnología que soporte los servicios de transporte de datos, Telefonía IP, video, Navegación WEB, intercambio de archivos entre otros. Se va a considerar la cantidad real de usuarios que van a usar esta red.

El nombramiento de la tecnología de red está determinado también al dimensionamiento de tráfico que se envía por la red y en base a ello se elige la tecnología Gigabit Ethernet para el diseño, con la finalidad de solventar las necesidades presentes y progresos en el futuro que puede brindar el Ministerio del Ambiente y Agua.

La Tabla 2.3 indica las tecnologías Gigabit Ethernet efectivas y pertinentes tipos: velocidad de transmisión, tipo de cable y longitud de segmento.

Tabla 2.3. Tecnología Gigabit Ethernet

	NOMBRE	VELOCIDAD DE TRANSMISION	TIPO DE CABLE	LONGITUD DE SEGMENTO
GIGABIT ETHERNET	1000Base-T	1000 Mbps	Cable UTP	100 metros
	1000Base-X		Fibra Óptica	MMF: 500 metros SMF: 2 kilómetros
	1000Base-SX		Fibra Óptica Multimodo	500 metros
	1000Base-LX		Fibra Óptica Monomodo	2 kilómetros

2.7.4. TOPOLOGÍA DE RED PROPUESTA

La topología de red es la manera que están acoplados los dispositivos, estaciones de trabajo internamente en la red [13].

Se ha designado una topología tipo estrella. Se eligió esta topología tomando en cuenta la distribución de los equipos de interconexión, la ubicación actual de los edificios, aplicaciones que van a ser utilizados, escalabilidad, presupuesto y las respectivas representaciones de los estándares del Cableado Estructurado.

El MDF (Punto de distribución Principal) se ubicará en el Edificio del Ministerio del Ambiente y de ahí hacia todos los cuartos de telecomunicaciones que estarán por pisos en cada uno de los edificios.

Para el Cableado Estructurado, en los enlaces de acceso se manejará cable UTP categoría 6A y en los enlaces de backbone se manejará la fibra óptica multimodo, considerando la distancia entre las dos instituciones antes independientes, mejorando la utilidad de la red.

El esquema de red Corporativa diseñado, se revela los niveles jerárquicos de la red, los tipos de cable a usarse, el establecimiento de las áreas de telecomunicaciones, así como las primordiales unidades de red.

Significativamente, se debe también considerar la distancia entre los diferentes edificios que componen este nuevo Ministerio y en el cual el MDF ubicado en el edificio del Ministerio del Ambiente donde estará el cuarto principal de equipos el cual se detallará más adelante. En la Figura 2.11 se muestran la distancia entre los 2 edificios.

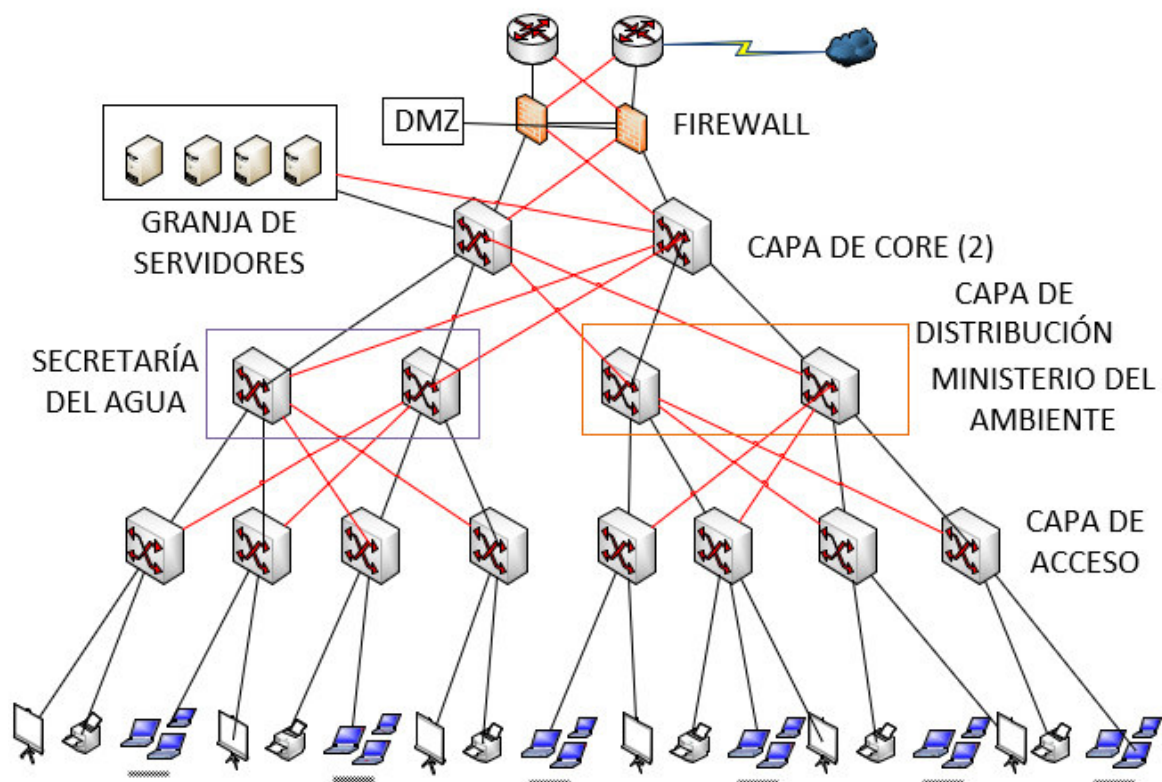


Figura 2.10. Esquema de red diseñado.

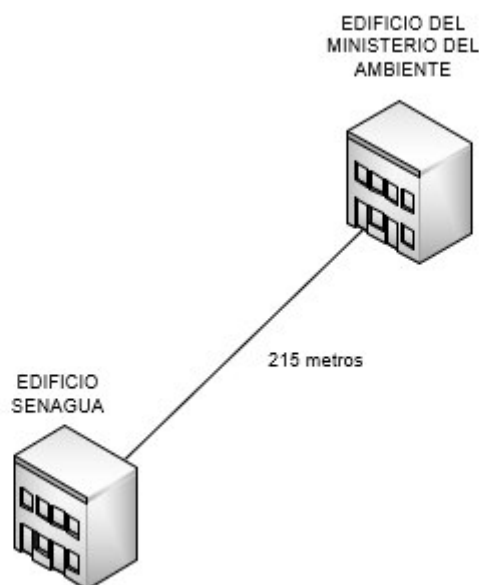


Figura 2.11. Distancia al área de dispositivos.

2.7.5. DISEÑO DE LA RED PASIVA PROPUESTA

Constituye la distribución que va a tener esta red, es decir todos los dispositivos que actúan en la transmisión de datos sin modificación y que son obligatorios para la transmisión.

2.7.5.1. Diseño de la infraestructura de red para la institución

El Ministerio del Ambiente y Agua necesita un diseño de una infraestructura de red que permita solventar los requerimientos actuales a la Red a diseñar, para esto se debe tomar en cuenta los puntos de red y la localización dentro del Ministerio del Ambiente y Agua.

2.7.5.1.1. Repartición de los puntos de red

En cada piso de los Edificios de las dos instituciones, tendrán un cuarto de Telecomunicaciones y el área de dispositivos principal se encontrará en el tercer piso del edificio del Ministerio del Ambiente, los cuales brindarán el servicio dentro de cada piso, efectuando la distancia máxima permitida del cableado horizontal que son 90 metros según la norma EIA/TIA 568-C [14].

Iniciando con el diseño del SCE se establece los puntos de red dentro de cada edificio, localización, así como su ocupación, también como consideración del diseño se tendrá en cuenta la escalabilidad de un 20 % dentro de cada edificio para un cableado a futuro de 10 años sin tener que realizar cambios.

La Tabla 2.4 indica el repartimiento de los puntos de los servicios requeridos para el edificio del Ministerio del Ambiente.

Tabla 2.4. Distribución de los puntos de red para el edificio del Ministerio del Ambiente

DISTRIBUCIÓN DE PUNTOS- EDIFICIO DEL MINISTERIO DEL AMBIENTE							
Piso	Datos	Voz	Video	AP	Pedidos	Extras	Instalados
Subsuelo	1	1	10	2	14	7	21
Planta Baja	32	24	18	2	76	33	109
1era Planta Alta	65	64	18	2	149	32	181
2da Planta Alta	57	57	14	2	130	30	160
3era Planta Alta	40	40	16	2	98	25	123
4ta Planta Alta	38	40	14	2	94	26	120
5ta Planta Alta	38	42	16	2	98	28	126
6ta Planta Alta	42	45	20	2	109	30	139
7ma Planta Alta	22	27	15	2	66	22	88
Terraza	2	2	4	0	8	5	13
Total	337	342	145	18	842	238	1080
Escalabilidad	22,04%						

La Tabla 2.5 indica el repartimiento de los puntos de los servicios requeridos para el edificio de la Secretaría del Agua.

Tabla 2.5. Distribución de los puntos de red para el edificio de la Secretaría del Agua

DISTRIBUCIÓN DE PUNTOS- EDIFICIO DEL SENAGUA							
Piso	Datos	Voz	Video	AP	Pedidos	Extras	Instalados
Subsuelo	25	24	5	1	55	16	71
Planta Baja	18	18	6	1	43	11	54
1era Planta Baja	29	26	6	1	62	20	82
1era Planta Alta	24	24	6	1	55	16	71
2da Planta Baja	25	24	5	1	55	17	72
2da Planta Alta	30	27	5	1	63	23	86
3era Planta Baja	34	34	3	1	72	20	92
3era Planta Alta	40	40	3	1	84	22	106
4ta Planta Baja	18	18	4	1	41	24	65
4ta Planta Alta	30	28	4	1	63	22	85
5ta Planta Baja	33	31	4	1	69	21	90
5ta Planta Alta	15	15	3	1	34	20	54
Total	321	309	54	12	696	232	928
Escalabilidad	25,00%						

2.7.5.2. Diseño del sistema de cableado horizontal

Va de acuerdo a la estructura física de los edificios que compone el Ministerio del Ambiente y Agua.

El Anexo A puntualiza la colocación de los puntos de los diferentes servicios en el croquis arquitectónico de la institución.

El diseño debe soportar aplicaciones que son necesarias en la institución como son: transferencia de datos, Telefonía IP, sistemas de video entre otros .La norma TIA/EIA 568-C establece el uso de cable UTP categoría 6A de 4 pares con los conectores RJ45 [14].

El estándar 568 C-2 define las características mecánicas, eléctricas y de transmisión del cable UTP categoría 6A.

El cable UTP 6A está relacionado con los cables UTP categoría 6 ,5 y 5e. Adquiere frecuencias de 500 MHz en cada par a una velocidad de 10 Gbps a 100 metros (ver Figura 2.12) [10].

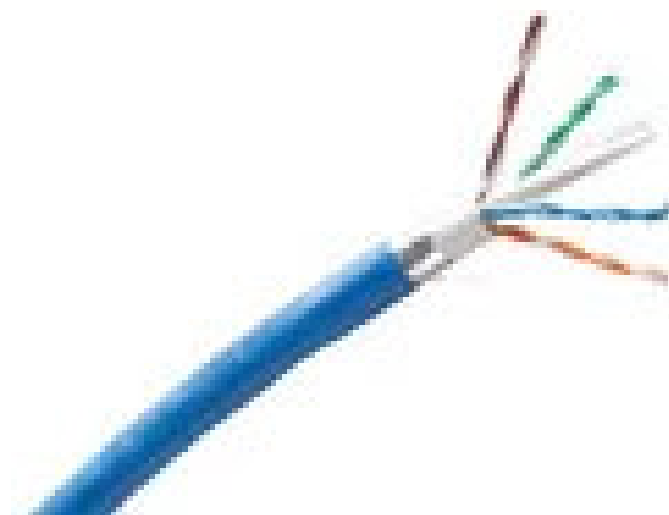


Figura 2.12. Cable UTP Categoría 6A [14]

En base a los planos arquitectónicos de los edificios se procede a realizar el cálculo de la longitud promedio del cable mediante la Ecuación 2.1.

$$L_{promedio}(m) = \frac{d_{min}(m)+d_{max}(m)}{2} * 1.2 + 2.5 \quad (2.1)$$

Donde:

d_{min} : es el trayecto al punto de red más contiguo.

$d_{máx}$: es la distancia al punto de red más lejano.

Además, se considera un 20% de margen de error y 2.5 metros de holgura.

Para el cálculo de numero de rollos se realiza el cálculo mediante la Ecuación 2.2.

$$Número\ de\ rollos = \frac{L_{promedio}(m)*Número\ de\ salidas}{305} \quad (2.2)$$

En las Tablas 2.6 y 2.7 se indican la cantidad de cable por piso de cada uno de los edificios que compone el Ministerio del Ambiente y Agua.

Tabla 2.6. Cantidad de rollos requeridos de cable UTP en el Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE					
PISOS	LMIN	LMAX	PUNTOS	L.PROMEDIO	NÚMERO DE ROLLOS
Subsuelo	1,64	68,54	21	44,608	4
Planta Baja	1,57	51,64	109	34,426	13
1era Planta Alta	1,44	66,2	181	43,084	26
2da Planta Alta	2,63	50,67	160	34,48	19
3era Planta Alta	2,8	35,24	123	25,324	11
4ta Planta Alta	2,6	50,06	120	34,096	14
5ta Planta Alta	3,03	38,85	126	27,628	12
6ta Planta Alta	2,73	39,03	139	27,556	13
7ma Planta Alta	2,82	44,63	88	30,97	9
Terraza	1	26,28	13	18,868	1
TOTAL					122

Tabla 2.7. Cantidad de rollos requeridos de cable UTP en el edificio del SENAGUA

EDIFICIO DEL SENAGUA					
PISOS	LMIN	LMAX	PUNTOS	L.PROMEDIO	CANTIDAD DE ROLLOS
Subsuelo	1,64	23,65	71	17,674	5
Planta Baja	0,86	36,77	54	25,078	5
1era Planta Baja	2,84	44,51	82	30,91	9
1era Planta Alta	0,89	31,9	71	22,174	6
2da Planta Baja	1,14	60,52	72	39,496	10
2da Planta Alta	0,96	35,45	86	24,346	7
3era Planta Baja	1,47	62,19	92	40,696	13
3era Planta Alta	1,09	40,65	106	27,544	10
4ta Planta Baja	0,76	48,73	65	32,194	7
4ta Planta Alta	1,41	46,73	85	31,384	9
5ta Planta Baja	1,9	64,39	90	42,274	13
5ta Planta Alta	1,67	36,57	54	25,444	5
TOTAL					99

2.7.5.2.1. *Recorridos para el cableado horizontal*

Para este diseño se utilizan tubos Conduit y escalerillas para el cableado horizontal como establece la norma 569A.

Para establecer la cantidad de cables que deberán pasar por un Conduit está establecida en tablas dependiendo del diámetro de la Fibra óptica al igual que para el cable UTP.

Como se puede ver en las Tablas 2.8 y 2.9 los valores tabulados de los Conduit dependiendo del diámetro de cable ya sea para Fibra óptica como para cable UTP respectivamente.

Tabla 2.8. Número de conduits en función al diámetro de la Fibra Óptica

Designación	Diámetro interior (mm)	Área interior total (mm ²)	Área disponible para conductores (mm ²)		
			Un conductor fr = 53%	Dos conductores fr = 31%	Más de dos conductores fr = 40%
16 (1/2)	15.8	196	103	60	78
21 (3/4)	20.9	344	181	106	137
27 (1)	26.6	557	294	172	222
35 (1-1/4)	35.1	965	513	299	387
41 (1-1/2)	40.9	1313	697	407	526
53 (2)	52.5	2165	1149	671	867
63 (2-1/2)	62.7	3089	1638	856	1236
78 (3)	77.9	4761	2523	1476	1904
91 (3-1/2)	90.1	6379	3385	1977	2555
103 (4)	102.3	8213	4349	2456	3282
129(5)	128.2	12907	6440	4001	5163
155 (6)	154.1	18639	9879	5778	7456

Tabla 2.9. Número de conduits en función al diámetro del cable UTP



Tamaño	Número de Cable o Alambres									
	Diámetro del cable en mm (in)									
Comercial	3.3 (.13)	4.6 (.18)	5.6 (.22)	6.1 (.24)	7.4 (.29)	7.9 (.31)	9.4 (.37)	13.5 (.53)	15.8 (.62)	17.8 (0.7)
1/2	1	1	0	0	0	0	0	0	0	0
3/4	6	5	4	3	2	2	1	0	0	0
1	8	8	7	6	3	3	2	1	0	0
1 1/4	16	14	12	10	6	4	3	1	1	1
1 1/2	20	18	16	15	7	6	4	2	1	1
2	30	26	22	20	14	12	7	4	3	2
2 1/2	45	40	36	30	17	14	12	6	3	3
3	70	60	50	40	20	20	17	7	6	6
3 1/2	-	-	-	-	-	-	22	12	7	6
4	-	-	-	-	-	-	30	14	12	7

2.7.5.2.2. Complementos para el cableado horizontal

De acuerdo con los datos y la repartición de puntos, se detalla un listado de componentes requeridos en el sistema de cableado horizontal.

Las Tablas 2.10 y 2.11 se indican los elementos necesarios y la cantidad por pisos en cada uno de los edificios que conforman el Ministerio de Ambiente.

Tabla 2.10. Lista de elementos para el cableado horizontal en el Ministerio del Ambiente

LISTA DE ELEMENTOS - EDIFICIO DEL MINISTERIO DEL AMBIENTE											
MATERIALES	Subsuelo	PB	1era PA	2da PA	3era PA	4ta PA	5ta PA	6ta PA	7ma PA	Terraza	TOTAL
Faceplate simple	19	61	151	50	79	38	48	53	44	9	552
Faceplate doble	1	24	15	55	22	41	39	43	22	2	264
Conduit 3/4" mt.	90	215	450	400	350	350	350	375	300	215	3095
Conduit 1" mt.	90	0	0	0	0	0	0	0	0	90	180
Escalerilla metálica	28	110	152	140	135	130	132	137	120	110	1194
Caja 20x20	34	0	0	0	0	0	0	0	0	34	68
Cajetín 20x10	10	42	100	85	70	70	75	80	60	40	632
Tapas 20x20	34	0	0	0	0	0	0	0	0	34	68
Rack abierto 12UR	1	0	0	0	0	0	0	0	0	1	2
Rack abierto 24UR	0	0	0	0	0	0	0	0	1	0	1
Rack abierto 42UR	0	1	1	1	2	1	1	1	0	0	8
Jack RJ-45 cat. 6A	20	160	60	165	140	140	130	135	120	30	1100
Patch Cords 1 mt.	25	74	20	30	20	20	25	25	20	5	264
Patch Cords 3 mts.	2	55	200	160	130	130	135	150	100	20	1082
Patch Panel cat. 6A	1	5	8	7	6	5	6	6	4	1	49
Organizador	3	7	10	9	8	7	8	8	6	3	69
Toma eléctrica	2	5	6	6	10	6	7	7	5	2	56
Otros (Tornillos, Tacos, Clavos, Alambre)	-	-	-	-	-	-	-	-	-	-	500

Tabla 2.11. Lista de elementos para el cableado horizontal en el edificio del SENAGUA

EDIFICIO DEL SENAGUA													
MATERIALES	Subsuelo	PB	1era PB	1era PA	2da PB	2da PA	3era PB	3era PA	4ta PB	4ta PA	5ta PB	5ta PA	TOTAL
Faceplate simple	21	18	24	21	22	32	24	28	27	13	30	20	280
Faceplate doble	25	18	29	25	25	27	34	39	19	36	30	17	324
Conduit 3/4" mt.	300	215	330	300	300	330	350	400	300	330	350	215	3720
Escalerilla metálica	120	90	135	120	125	138	140	165	120	137	140	90	1520
Cajetín 20x10	60	52	70	60	62	70	75	100	60	72	80	60	821
Jack RJ-45 cat. 6A	120	100	130	120	123	130	135	150	120	135	140	120	1523
Rack abierto 19UR	1	1	0	1	1	0	0	0	1	0	0	1	6
Rack abierto 24UR	0	0	1	0	0	1	1	0	0	1	1	0	5
Rack abierto 42UR	0	0	1	0	0	0	0	1	0	0	0	0	2
Patch Cords 1 mt.	20	15	20	20	22	20	25	25	20	20	25	20	252
Patch Cords 3 mts.	100	60	120	100	105	130	140	150	100	120	130	100	1355
Patch Panel cat. 6A	3	3	4	3	3	4	4	5	3	4	4	3	43
Organizador	5	5	6	5	5	6	6	7	5	6	6	5	67
Toma eléctrica	3	5	5	3	3	4	3	6	3	3	3	3	44
Otros (Tornillos, Tacos, Clavos, Alambre)	-	-	-	-	-	-	-	-	-	-	-	-	450

En el ANEXO A y B se muestran los planos de la distribución de puntos, así como el diseño de cableado horizontal dentro de cada uno de pisos de cada edificio que conforman el Ministerio. (Ver desde la Figura A.1 hasta la Figura B.12).

2.7.5.3. Diseño del sistema de cableado vertical

El sistema de cableado vertical para la institución es aquel que permite la interconexión de los edificios que anteriormente fueron instituciones independientes.

Debido a la distancia de separación de estos 2 edificios supera los 100 metros admitidos por el estándar se requiere el manejo de fibra óptica multimodo de 62.5/125 um, ya que en el cableado vertical alcanza una longitud máxima de 2000 metros.

Para la interconexión de los edificios se utilizará ductos subterráneos por donde será enviado la fibra óptica.

El uso de fibra óptica en este sistema es requerido por su gran manejo de ancho de banda y flexibilidad.

Para el establecimiento de fibra óptica en el sistema de cableado vertical, se requiere seguir las recomendaciones del estándar EIA/TIA 568C-3 [17].

Tomar en cuenta que la distancia entre los dos edificios que conforman la institución es 215 metros.

El ANEXO C indica el diagrama unifilar de la interconexión de los edificios de la institución. (Ver la Figura C.1).

El ANEXO D especifica el diagrama unifilar de cada uno de los edificios que compone la institución. (Ver las Figuras D.1 y D.2).

2.7.5.4. Diseño de la red de trabajo

El sitio de trabajo lo compone un PC o laptop, teléfono IP que están acoplados a un punto de red, se sitúa los faceplates dobles de los servicios que se localizan a 50 cm del suelo.

Los dispositivos de red se conectan a un punto de red usando patch cords RJ45 de categoría similar que la del cableado horizontal.

Los patch cords deben ser elaborados y certificados por el fabricante a fin de uso adentro del espacio laboral.

2.7.5.5. Diseño del cuarto de telecomunicaciones

El cuarto de telecomunicaciones es un espacio único interior al edificio en el cual se encuentran los equipos de telecomunicaciones. Estos cuartos se encuentran en cada piso, para mayor facilidad en el cableado del backbone. Dentro del cuarto de telecomunicaciones se instalarán racks dependientes del número de switch y patch panels por piso.

Todos los cuartos de telecomunicaciones deben converger en el área principal de equipos ubicada en la tercera planta alta del edificio del Ministerio del Ambiente.

Las especificaciones a considerar para un cuarto de telecomunicaciones son:

- Ser únicamente para equipos de telecomunicaciones.
- El rango de temperatura permitido es de 18 a 24 °C y humedad de 30 a 50%.
- La dimensión de la puerta abriéndola hacia afuera debe ser de 0.9m x 2.15m.

2.7.5.5.1. Dimensionamiento de los racks

Se debe conocer la cantidad de equipos que estarán dentro del mismo para escoger el tamaño de rack adecuado.

Las Tablas 2.12 y 2.13 muestran el número de equipos, así como la denominación de cada rack para cada piso de cada edificio.

Tabla 2.12. Lista de equipos y denominación del rack para el Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
PISO	NÚMERO DE RACK	SWITCHES DE 24 PUERTOS
Subsuelo	1	1
Planta Baja	2	5
1era Planta Alta	3	8
2da Planta Alta	4	7
3era Planta Alta	5	6
4ta Planta Alta	6	5
5ta Planta Alta	7	6
6ta Planta Alta	8	6
7ma Planta Alta	9	4
Terraza	10	1

Tabla 2.13. Lista de equipos y denominación del rack para el edificio del SENAGUA

EDIFICIO DE SENAGUA		
PISO	NÚMERO DE RACK	SWITCH DE 24 PUERTOS
Subsuelo	1	3
Planta Baja	2	3
1era Planta Baja	3	4
1era Planta Alta	4	3
2da Planta Baja	5	3
2da Planta Alta	6	4
3era Planta Baja	7	4
3era Planta Alta	8	5
4ta Planta Baja	9	3
4ta Planta Alta	10	4
5ta Planta Baja	11	4
5ta Planta Alta	12	3

A continuación, en las Tablas de la 2.14 a la 2.22 se detalla el dimensionamiento de los racks de acuerdo al número de equipos, aquí se tomarán en cuenta elementos como patch panels organizadores de cables, ventilación alimentación y UPS para cada rack.

Tabla 2.14. Dimensionamiento de los racks 1 y 10 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	1	1
Patch panel FO	1	1
Switch de 24 puertos	1	1
Organizador de cables	1	1
Patch panel de 24 puertos	1	1
Alimentación	1	1
UPS	2	2
Vacío	3	3
Total		12

Tabla 2.15. Dimensionamiento del rack 9 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	5	5
Patch panel FO	1	1
Switch de 24 puertos	4	4
Organizador de cables	4	4
Patch panel de 24 puertos	4	4
Alimentación	1	1
UPS	2	2
Vacío	2	2
Total		24

Tabla 2.16. Dimensionamiento de los racks 2 y 6 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	6	6
Patch panel FO	1	1
Switch de 24 puertos	5	5
Organizador de cables	5	5
Patch panel de 24 puertos	5	5
Alimentación	1	1
UPS	2	2
Vacío	16	16
Total		42

Tabla 2.17. Dimensionamiento de los racks 5,7,8 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	7	7
Patch panel FO	1	1
Switch de 24 puertos	6	6
Organizador de cables	6	6
Patch panel de 24 puertos	6	6
Alimentación	1	1
UPS	2	2
Vacío	12	12
Total		42

Tabla 2.18. Dimensionamiento del rack 4 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	8	8
Patch panel FO	1	1
Switch de 24 puertos	7	7
Organizador de cables	7	7
Patch panel de 24 puertos	7	7
Alimentación	1	1
UPS	2	2
Vacío	8	8
Total		42

Tabla 2.19. Dimensionamiento del rack 3 del edificio del Ministerio del Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	9	9
Patch panel FO	1	1
Switch de 24 puertos	8	8
Organizador de cables	8	8
Patch panel de 24 puertos	8	8
Alimentación	1	1
UPS	2	2
Vacío	4	4
Total		42

Tabla 2.20. Dimensionamiento de los racks 1,2,4,5,9 y 12 del edificio del SENAGUA

EDIFICIO DEL SENAGUA		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	4	4
Patch panel FO	1	1
Switch de 24 puertos	3	3
Organizador de cables	3	3
Patch panel de 24 puertos	3	3
Alimentación	1	1
UPS	2	2
Vacío	1	1
Total		19

Tabla 2.21. Dimensionamiento de los racks 3,6,7,10 y 11 del edificio del SENAGUA

EDIFICIO DEL SENAGUA		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	5	5
Patch panel FO	1	1
Switch de 24 puertos	4	4
Organizador de cables	4	4
Patch panel de 24 puertos	4	4
Alimentación	1	1
UPS	2	2
Vacío	2	2
Total		24

Tabla 2.22. Dimensionamiento del rack 8 del edificio del SENAGUA

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	6	6
Patch panel FO	1	1
Switch de 24 puertos	5	5
Organizador de cables	5	5
Patch panel de 24 puertos	5	5
Alimentación	1	1
UPS	2	2
Vacío	16	16
Total		42

2.7.5.5.2. *Dimensionamiento del rack primordial*

El rack primordial se localizará en la tercera planta alta del edificio del Ministerio del Ambiente ya que este cuarto almacenará una gran cantidad de equipos. La Tabla 2.23 indica la referencia de los equipos que estarán dentro del rack principal.

Tabla 2.23. Dimensionamiento del rack principal

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
Ventilador	1	1
Separación	7	8
Routers	2	2
Patch panel FO	1	1
Switch de 24 puertos	4	4
Organizador de cables	4	4
Patch panel de 24 puertos	4	4
Monitor	1 (2UR)	2
Servidor de video	2	2
Alimentación	2	2
UPS	2	2
Vacío	10	10
Total		42

Además de este rack se contará con racks exclusivos para servidores de almacenamiento de datos, respaldo de servidores y Telefonía IP.

En el ANEXO E y F se indican cada uno de los diagramas de rack para cada uno de los edificios del Ministerio del Ambiente. (Ver desde la Figura E.1 hasta la Figura F.12).

2.7.5.6. Diseño de la sala de equipos

Este sistema es estandarizado por la norma EIA/TIA 569. Los dispositivos y elementos a encontrarse son:

El armario de repartición principal (MDF), Servidores de almacenamiento de datos, Servidores de video, Centrales Telefónicas, etc.

Este subsistema debe cubrir lo siguiente:

- Debe estar conecto al enrutamiento vertical.
- Estar en una temperatura entre 18 a 27 grados centígrados.
- Tener un mínimo de 14 metros cuadrados de área.

2.7.5.7. Gestión del Sistema de Cableado Estructurado para la red

Está determinada por el estándar EIA/TIA 606-A para que la administración de la red sea más fácil, admitiendo escalabilidad y flexibilidad para el funcionamiento de la red de al menos 10 años. Es necesario contar con una certificación para la administración del cableado estructurado.

La Tabla 2.24 establece un código de color para que el etiquetado sea más fácil de identificar.

Tabla 2.24. Código de colores para la gestión del SCE

COLOR	DESCRIPCION
NARANJA	Conexión mayor
VERDE	Backbone del edificio del SENAGUA
PURPURA	Backbone del edificio del MAE
BLANCO	Backbone entre edificios
GRIS	Límite centrado de oficina
AZUL	Enlace de red en el usuario final
CAFÉ	Mantenimiento Auxiliar
AMARILLO	Sistema de Video
ROJO	Sistema Telefónico

2.7.5.7.1. Etiquetado para el cableado

Esta determinado en la norma EIA/TIA 606-A, el cual precisa el rotulado que se realiza en los extremos de los cables, faceplates y patch panels del cuarto de telecomunicaciones.

Para este diseño se basará en un etiquetado adhesivo con protección de plástico para evitar la manipulación directa de las manos sobre el impreso del rotulado.

El formato del etiquetado para la institución establecido (ver Figura 2.13).

U-R-ESP

Figura 2.13. Formato de etiquetado para el SCE

Donde:

U es la ubicación al cuarto de telecomunicaciones del edificio al que se encuentra ya sea M que se encuentra en el Ministerio del Ambiente o SA que se encuentra en el edificio del SENAGUA.

R es el número de rack al que corresponde.

E es el número de patch panel al que está conectado.

S es el tipo de servicio el cual puede ser: V de voz, D de datos, F de video, E de enlace

P es el número de puerto.

Por ejemplo, si se tiene una etiqueta SA-3-2F10, quiere decir que pertenece a un cuarto de telecomunicaciones del edificio del SENAGUA, que se encuentra en el rack 3, el servicio que brinda es de video y está acoplado al puerto 10.

Luego de esto se debe contratar una empresa que certifique la rotulación de los cables para que se cumpla los requisitos señalados en los estándares EIA/TIA.

2.7.6. DIMENSIONAMIENTO DE TRÁFICO

Para el dimensionamiento del tráfico se tomarán en cuenta los servicios que ofrece esta red, para eso se va a considerar el tráfico interno y externo.

2.7.6.1. Dimensionamiento del Tráfico Interno

El tráfico interno es la cantidad de información que se envía por la red LAN, su origen es un host y su destino es otro host de la misma red.

Para este tráfico se consideran los siguientes servicios:

Correo interno, Base de datos, Transferencia de archivos, Videoconferencia y VoIP.

2.7.6.1.1. Cómputo del ancho de banda en el Correo interno

Es el servicio de mensajería mediante correo electrónico que pasa por la red LAN y no requiere de salida al Internet y sirve para comunicar a las diferentes áreas administrativas de los 2 edificios de la institución.

En cuanto al cómputo aproximado de la cantidad de información para el correo electrónico interno se considera un número promedio de 50 correos que se envían en la hora pico y se establece un correo con archivos de texto adjuntos de 600 KB de promedio.

En la Ecuación 2.3 se indica el cálculo de este ancho de banda.

$$AB_{\text{CorreoInt}} = \frac{600 \text{ KB}}{1 \text{ correo}} * \frac{50 \text{ correos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 66,67 \frac{\text{Kbps}}{\text{usuario}} \quad (2.3)$$

2.7.6.1.2. *Cómputo del ancho de banda en el ingreso a la Base de datos*

Es la prestación de ingreso y visita a la base de datos, que cada usuario realiza desde su estación de trabajo. Para este servicio no se necesita una salida a internet ya que las consultas e ingresos son dentro de la LAN.

Para el cálculo aproximado de la cantidad de información para el ingreso la base de datos se considera un promedio de 30 consultas que se realizan en la hora pico y se establece un promedio de 400 KB por consulta, ya que por lo general se tiene información relevante y confidencial de texto de la institución que siempre es requerida. La Ecuación 2.4, indica la medición de este ancho de banda.

$$AB_{BD} = \frac{400 \text{ KB}}{1 \text{ consulta}} * \frac{30 \text{ consultas}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 26,67 \frac{\text{Kbps}}{\text{usuario}} \quad (2.4)$$

2.7.6.1.3. *Cómputo del ancho de banda en acceso a Video seguridad*

El tráfico de Video seguridad corresponde a toda la cantidad de información que se utiliza en las cámaras de seguridad las cuales son consideradas en el tráfico de la LAN. Cada edificio contara con un número determinado de cámaras de seguridad ubicadas en puntos específicos creando un circuito cerrado de video. Cada edificio tiene un tráfico diferente debido a que se tiene un número diferente de puntos en cada uno de los pisos.

Para el cómputo aproximado del de la cantidad de información interna de la Video vigilancia se considera un promedio de 50 accesos que se realizan en la hora pico y se establece un promedio de 1800 KB por acceso. Se consideran 50 acceso por hora, ya se usarán cámaras con detectores de movimiento ya que reducen el tráfico de la red. En la Ecuación 2.5 se indica el cálculo de este ancho de banda.

$$AB_{VS} = \frac{1800 \text{ KB}}{1 \text{ acceso}} * \frac{50 \text{ accesos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 200 \frac{\text{Kbps}}{\text{usuario}} \quad (2.5)$$

2.7.6.1.4. *Cómputo del ancho de banda en acceso a Transferencia de archivos*

Esta prestación corresponde al tráfico empleado al usar el protocolo FTP para el intercambio de archivos entre estaciones de trabajo dentro de la red LAN.

Para este servicio se considera un número promedio de 30 archivos que se envían en la hora pico y se establece un promedio de 2048 KB por archivo. En la Ecuación 2.6 se indica el cálculo de este ancho de banda.

$$AB_{TA} = \frac{2048 \text{ KB}}{1 \text{ archivo}} * \frac{30 \text{ archivos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 136,53 \frac{\text{Kbps}}{\text{usuario}} \quad (2.6)$$

2.7.6.1.5. Cómputo del ancho de banda para Videoconferencia

El ancho de banda de la Videoconferencia corresponde al tráfico que se tiene en la red con respecto a video enfocado a una videoconferencia entre puntos distantes de la red LAN. Este servicio es en tiempo real por lo que es necesario tomar las consideraciones necesarias para poder determinar el ancho de banda adecuado generado por este servicio. Se considera una videoconferencia de 1800 KB que corresponde a una imagen HD y se considera que en la hora pico se tiene una videoconferencia que se ocupará el 97% de la hora. En la Ecuación 2.7 se indica el cálculo de este ancho de banda.

$$AB_{VC} = \frac{1800 \text{ KB}}{1 \text{ acceso}} * \frac{50 \text{ accesos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 200 \frac{\text{Kbps}}{\text{usuario}} \quad (2.7)$$

2.7.6.1.6. Cómputo del ancho de banda para Voz sobre IP

Para el cálculo del ancho de banda para Voz sobre IP se realiza lo siguiente:

Se calcula el tamaño de la trama de voz considerando el CODEC para tener la dimensión se adiciona los encabezados de las capas 4,3 y 2, como se muestra en la Ecuación 2.8.

$$\text{Tamaño de trama} = \text{Payload} + \text{header4} + \text{header3} + \text{header 2} \quad (2.8)$$

Por ejemplo, se considera un códec G.729 en la cual las tramas poseen una amplitud de 20 bytes, se le suma los encabezados RTP, UDP e IP en total 40 bytes que se encapsula en la capa de enlace con PPP que es una trama de 6 bytes. En la Tabla 2.25 se indica los tamaños de los encabezados obteniendo la dimensión de la trama de voz.

Tabla 2.25. Dimensión de la trama de voz con PPP

Payload de voz	20 bytes
Cabecera RTP	8 bytes
Cabecera UDP	12 bytes
Cabecera IP	20 bytes
Encapsulamiento PPP	6 bytes
Tamaño total de la trama	66 bytes

Se realiza la compresión ya que se tienen enlaces de bajo ancho de banda para lo cual se realiza la compresión RTP el cual reduce los 40 bytes iniciales a 2 o 4 bytes como se indica en la Tabla 2.26.

Tabla 2.26. Dimensión de la trama de voz con PPP con compresión RTP

Payload de voz	20 bytes
Cabecera RTP/UDP/IP	2 bytes
Encapsulamiento PPP	6 bytes
Tamaño total de la trama	28 bytes

Este tamaño de trama de voz se debe transformar a bits de acuerdo a la Ecuación 2.9.

$$28 \text{ bytes} * \frac{8 \text{ bits}}{1 \text{ byte}} = 224 \frac{\text{bits}}{\text{trama}} \quad (2.9)$$

Para una llamada se debe multiplicar por el número de tramas generadas por segundo según el códec usado, en el caso del códec G.729 se generan 50 tramas por segundo.

La Ecuación 2.10 nos permite calcular este ancho de banda.

$$AB_{VoIP} = 224 \frac{\text{bits}}{\text{trama}} * \frac{50 \text{ tramas}}{\text{segundo}} = 11,2 \frac{\text{Kbps}}{\text{llamada}} \quad (2.10)$$

El ancho de banda en una implementación se multiplica el valor anterior obtenido por el número de llamadas concurrentes. En la Ecuación 2.11 se indica el cálculo de este ancho de banda.

$$AB_{VoIPreq} = 11,2 \frac{\text{Kbps}}{\text{llamada}} * 10 \text{ llamadas} = 112 \text{ Kbps} \quad (2.11)$$

Para encontrar el ancho de banda de VoIP de esta institución, se considera un códec G.729 y Encapsulamiento de capa 2: Ethernet.

El encapsulamiento Ethernet tiene los campos MAC destino, MAC origen, Tipo y FCS, en total son 18 bytes.

La Tabla 2.27 enseña el cálculo de la dimensión de la trama con las indicaciones antes mencionadas.

Tabla 2.27. Dimensión de la trama de VoIP utilizando Ethernet sin compresión RTP

Payload de voz	20 bytes
Cabecera RTP	8 bytes
Cabecera UTP	12 bytes
Cabecera IP	20 bytes
Encapsulamiento Ethernet	20 bytes
Tamaño total de la trama	78 bytes

Se encuentra la cantidad de bits por trama (ver Ecuación 2.12).

$$78 \text{ bytes} * \frac{8 \text{ bits}}{1 \text{ byte}} = 624 \frac{\text{bits}}{\text{trama}} \quad (2.12)$$

Se encuentra el ancho de banda multiplicando el valor anterior obtenido por la cantidad de tramas por segundo que son 50 del códec G.729. En la Ecuación 2.13 se indica el cálculo de este ancho de banda.

$$AB_{VoIP} = 624 \frac{\text{bits}}{\text{trama}} * \frac{50 \text{ tramas}}{\text{segundo}} = 31,2 \frac{\text{Kbps}}{\text{llamada}} \quad (2.13)$$

El índice de simultaneidad el cual revela el número de usuarios que usan los servicios al mismo tiempo. Para ello se determina la cantidad de usuarios que usan el servicio, luego se multiplica por el índice de simultaneidad y por la capacidad por usuario de cada servicio que se calculó anteriormente así obteniendo el ancho de banda interno.

Para el caso del servicio de Video seguridad, la cantidad de información por segundo obtenido es a partir de la cantidad de cámaras por la capacidad de transmisión de cada cámara.

En las Tablas 2.28, 2.29, 2.30 y 2.31 se indican la cantidad de usuarios con los respectivos índices de simultaneidad, así como la capacidad de transmisión total para este tráfico, para cada uno de los edificios que componen el Ministerio del Ambiente y Agua.

Tabla 2.28. Valores de Tráfico Interno de los servicios para el edificio del Ministerio del Ambiente

SERVICIOS	USUARIOS TOTALES	% IS	USUARIOS	CAPACIDAD POR USUARIO (Kbps)	CAPACIDAD TOTAL (Kbps)
Correo Interno	337	50	168,5	66,67	11233,895
Base de datos	200	70	140	36,67	5133,8
Transferencia de Archivos	250	50	125	136,53	17066,25
Videoconferencia	20	80	16	200	3200
VoIP	137	60	82,2	31,2	2564,64

Tabla 2.29. Valores de Tráfico Interno de Video seguridad para el Ministerio el Ambiente

SERVICIO	NÚMERO DE CÁMARAS	CAPACIDAD POR CÁMARA (Kbps)	CAPACIDAD (Kbps)
Video seguridad	80	750	60000
	65	400	26000

Tabla 2.30. Valores de Tráfico Interno de los servicios para el edificio del SENAGUA

SERVICIOS	USUARIOS TOTALES	% IS	USUARIOS	CAPACIDAD POR USUARIO (Kbps)	CAPACIDAD TOTAL (Kbps)
Correo Interno	200	60	120	66,67	8000,4
Base de datos	20	70	14	36,67	513,38
Transferencia de Archivos	250	80	200	136,53	27306
Videoconferencia	25	80	20	200	4000
VoIP	309	60	185,4	31,2	5784,48

Tabla 2.31. Valores de Tráfico Interno de Video seguridad para el edificio del SENAGUA

SERVICIO	NÚMERO DE CÁMARAS	CAPACIDAD POR CÁMARA (Kbps)	CAPACIDAD (Kbps)
Video seguridad	30	750	22500
	24	400	9600

En la Tabla 2.32 se indica el valor total obtenido del ancho de banda interno totales de los 2 edificios.

Tabla 2.32. Valor total del ancho de banda interno

AB INTERNO MAE	125198,585
AB INTERNO SENAGUA	77704,26
AB INTERNO TOTAL (Kbps)	202902,845

2.7.6.2. Dimensionamiento del Tráfico Externo

El tráfico externo es aquel que se origina en un host y saldrá al internet por la acometida donde se conecta al ISP.

Este tráfico se considera las siguientes aplicaciones:

Correo externo, Acceso Web, Carga de Archivos y Descarga de archivos.

2.7.6.2.1. Cómputo del ancho de banda en la Mensajería externa

El ancho de banda del correo electrónico corresponde al servicio de mensajería por correo electrónico que pasa por la red LAN y saldrá al Internet. Se utiliza para comunicarse con otras estaciones de otras redes externas.

Para el cálculo aproximado se considera un promedio de 30 correos que se envían en la hora pico además se establece un correo de 600 KB de promedio. En la Ecuación 2.14 se indica el cálculo de este ancho de banda.

$$AB_{\text{correoext}} = \frac{600 \text{ KB}}{1 \text{ correo}} * \frac{30 \text{ correos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 40 \frac{\text{Kbps}}{\text{usuario}} \quad (2.14)$$

2.7.6.2.2. Cómputo del ancho de banda en el Acceso web

La cantidad de información por segundo en el ingreso web se genera a una página web que esta fuera de la LAN y se necesita una salida a internet usando el protocolo http.

Para esto se considera que un sitio web posee como promedio 500 KB con la ayuda de la herramienta web GTmetrix que muestra el tamaño del sitio web mediante el ingreso de la URL de la misma. El número de accesos al sitio web es de 40 veces en la hora pico. En la Ecuación 2.15 se indica el cálculo de este ancho de banda.

$$AB_{\text{accesoweb}} = \frac{500 \text{ KB}}{1 \text{ acceso}} * \frac{40 \text{ accesos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 44,44 \frac{\text{Kbps}}{\text{usuario}} \quad (2.15)$$

2.7.6.2.3. Cómputo del ancho de banda en la Carga o Subida de archivos

El ancho de banda para subida de archivos corresponde al tráfico generado al subir información o archivos a páginas web que las almacenan.

Para este servicio se considera una carga de archivos de 2000KB y que se accede a este servicio 20 veces en una hora. En la Ecuación 2.16 se indica el cálculo de este ancho de banda.

$$AB_{cargarch} = \frac{2000 \text{ KB}}{1 \text{ acceso}} * \frac{20 \text{ accesos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 88,88 \frac{\text{Kbps}}{\text{usuario}} \quad (2.16)$$

2.7.6.2.4. Cómputo del ancho de banda en la Descarga de archivos

La cantidad de información por segundo para la descarga de archivos corresponde al tráfico generado al bajar información o archivos de internet.

Para este servicio se considera una descarga de archivos como promedio de 2000 KB y se accede a este servicio 15 veces en una hora. En la Ecuación 2.17 se indica el cálculo de este ancho de banda.

$$AB_{descargarch} = \frac{2000 \text{ KB}}{1 \text{ acceso}} * \frac{15 \text{ accesos}}{1 \text{ hora}} * \frac{1 \text{ hora}}{3600 \text{ s}} * \frac{8 \text{ bits}}{1 \text{ byte}} = 66,67 \frac{\text{Kbps}}{\text{usuario}} \quad (2.17)$$

Para el cómputo de la información se verifica el índice de simultaneidad, como se tomó en cuenta para el tráfico interno, así como las cantidades de ancho de banda calculados anteriormente para cada servicio obteniendo los resultados en las Tablas 2.33 y 2.34.

Tabla 2.33. Valores de Tráfico Externo de los servicios para el Ministerio del Ambiente

SERVICIOS	USUARIOS TOTALES	% IS	USUARIOS	CAPACIDAD POR USUARIO (Kbps)	CAPACIDAD TOTAL (Kbps)
Correo Externo	337	80	269,6	40	10784
Acceso web	200	70	140	44,44	6221,6
Carga de Archivos	150	80	120	88,88	10665,6
Descarga de archivos	160	50	80	66,67	5333,6

Tabla 2.34. Valores de Tráfico Externo de los servicios para el edificio del SENAGUA

SERVICIOS	USUARIOS TOTALES	% IS	USUARIOS	CAPACIDAD POR USUARIO (Kbps)	CAPACIDAD TOTAL (Kbps)
Correo Externo	321	60	192,6	40	7704
Acceso web	250	60	150	44,44	6666
Carga de Archivos	200	40	80	88,88	7110,4
Descarga de archivos	140	50	70	66,67	4666,9

En la Tabla 2.35 se indica el valor total obtenido del ancho de banda externo total de los 2 edificios.

Tabla 2.35. Valor total del ancho de banda externo

AB EXTERNO MAE	33004,8
AB EXTERNO SENAGUA	26147,3
AB EXTERNO TOTAL (Kbps)	59152,1

La capacidad total de la LAN obtenida se obtiene sumando los anchos de banda tanto interno como externo (ver Tabla 2.36).

Tabla 2.36. Valor total del ancho de banda

AB INTERNO	202902,845
AB EXTERNO	59152,1
AB TOTAL (Kbps)	262054,945

2.7.6.2.5. Proyección de la red LAN para 5 años

En la Tabla 2.37 se indica la proyección de la red a 5 años.

Tabla 2.37. Proyección de 5 años para la red LAN

Proyección de Escalabilidad para 5 años				
Año 1	Año 2	Año 3	Año 4	Año 5
262054,95	275157,69	288915,58	303361,36	318529,42

La capacidad total de la LAN es de 262054,945 Kbps, por lo cual se llega a la conclusión de escoger una red Gigabit Ethernet conmutada, ya que dentro de este diseño se considera una escalabilidad, se considera que la red va a crecer es de un 5% por el aumento de la utilización de los servicios a futuro. Se debe considerar el cambio de equipos activos de la

red por la falta de soporte y garantía en cuanto a repuestos y fallos ya que una vez cumplido su vida útil pueda ser que fallen estos equipos dejando que la red falle y no se tenga alta disponibilidad.

2.7.7. DISEÑO DE LA RED ACTIVA

El diseño de la red para el manejo de voz, datos y video para el Ministerio del Ambiente y Agua se establece en una estructura de capas de red de 3 niveles que son Acceso, Distribución y Core.

La capa de acceso provee el ingreso a la red a los equipos del usuario final. Estos equipos están acoplados a un switch de acceso y se conectan a los switches de distribución en el manejo de datos.

La capa de distribución realiza listas de control de acceso, manejo de seguridad entre otras. Esta capa se comunica con la capa de core para estar siempre disponible.

La capa de core realiza tareas como conmutación y enrutamiento entre VLANs, etc.

Se pueden encontrar switches multicapa que pueden realizar ciertas funciones básicas de un router, centrales telefónicas, etc.

2.7.7.1. Características Técnicas mínimas de los dispositivos de la red

Para la elección de dispositivos se debe tomar en cuenta ciertas funciones como facilidad para la administración, mecanismos de seguridad, calidad de servicio, etc.

Los equipos deben ofrecer las facilidades para ser administrados remotamente. También debe tolerar los protocolos de autenticación y ocultación de la información, SNMP, RMON y SSH.

Los dispositivos se comprometen a ajustarse a las innovaciones futuras de la red.

Debe contar con protocolos IEEE 802.1x y IEEE 802.1p, soporte para VLANs, vigilancia de puertos empleando direcciones MAC, distribución de Listas de Control de Acceso.

Es preciso contar las características requeridas de los dispositivos necesarios para la red.

2.7.7.1.1. Switch de Acceso

El Ministerio del Ambiente y Agua tiene 2008 puntos por lo que se requiere un total de 92 switches de acceso quedando con un total de 200 puertos libres para futuras expansiones.

Se debe tomar en cuenta la velocidad de backplane, en el que se considera la cifra de puertos empleados paralelamente en la hora pico interno a cada edificio.

La Ecuación 2.18 muestra el cálculo de la velocidad de backplane.

$$V_{backplane} = \text{Numero de puertos utilizados simultaneamente} * 100\text{Mbps} * 2 \quad (2.18)$$

La hora pico es de 11am a 12pm y que 18 de los 24 puertos son usados al mismo tiempo. La Ecuación 2.19 indica el cómputo de la rapidez del backplane.

$$V_{backplane} = \{(18 * 100\text{Mbps}) + (1 * 1000)\} * 2 = 5.6 \text{ Gbps} \quad (2.19)$$

Tomando en cuenta lo anterior se describe en la Tabla 2.38 las especificaciones necesarias para los switches de acceso.

Tabla 2.38. Especificaciones requeridas en el Switch de capa de Acceso

Switch de Acceso	
Parámetro	Especificaciones
Puertos Ethernet	24 puertos 10/100 Mbps
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps
Capa	2
Backplane	6 Gbps
Throughput	6 Mpps
Administración de VLANs	Si
Calidad de Servicio	Si
Estándares	IEEE 802.1d
	IEEE 802.1p
	IEEE 802.1q
	IEEE 802.1x
	IEEE 802.1w
	IEEE 802.3u
	IEEE 802.3x
IEEE 802.3af	
Protocolo	SNMP ¹ , Telnet ² ,
Administración	GUI, SNMP, Telnet, CLI, RMON ³

Las Tablas 2.39 y 2.40 indican la cantidad de switches de acceso necesarios por edificios.

¹ **SNMP** (Simple Network Management Protocol): Protocolo de capa aplicación fundamentado en IP más utilizado en la gestión de redes.

² **Telnet** (Telecommunication Network): Protocolo de capa de red TCP/IP, proporciona el manejo de equipos mediante acceso remoto.

³ **RMON** (Remote Network Monitoring): Concede el intercambio de datos de monitoreo en la red entre monitores de red y sistemas de consola.

Tabla 2.39. Número de switches de acceso para el edificio del Ministerio el Ambiente

EDIFICIO DEL MINISTERIO DEL AMBIENTE		
PISO	NÚMERO DE PUERTOS	NÚMERO DE SWITCHES
Subsuelo	21	1
Planta Baja	109	5
1era Planta Alta	181	8
2da Planta Alta	160	7
3era Planta Alta	123	6
4ta Planta Alta	120	5
5ta Planta Alta	126	6
6ta Planta Alta	139	6
7ma Planta Alta	88	4
Terraza	13	1

Tabla 2.40. Número de switches de acceso para el edificio del SENAGUA

EDIFICIO DE SENAGUA		
PISO	NÚMERO DE PUERTOS	NÚMERO DE SWITCHES
Subsuelo	71	3
Planta Baja	54	3
1era Planta Baja	82	4
1era Planta Alta	71	3
2da Planta Baja	72	3
2da Planta Alta	86	4
3era Planta Baja	92	4
3era Planta Alta	106	5
4ta Planta Baja	65	3
4ta Planta Alta	85	4
5ta Planta Baja	90	4
5ta Planta Alta	54	3

En base a la información anterior se tiene en total de 200 puertos libres que pueden usar los nuevos usuarios que deseen utilizar la red, estableciendo un 20% de escalabilidad.

2.7.7.1.2. *Switch de Distribución*

El switch de distribución deben cumplir características como conmutación entre VLANs, diferenciación de servicios, listas ACL, etc.

Para este diseño de red se consideran 5 switches de distribución que se conectan a los switch de acceso y 5 para redundancia a la red y tener una red de alta disponibilidad, que en total se tiene 10 switches de 24 puertos. Los switches de distribución están repartidos

de la siguiente forma: 4 switches incluidos los de redundancia para el edificio del SENAGUA y 6 switches de distribución para el edificio del Ministerio del Ambiente.

Los switches de distribución deben contar con las especificaciones de la Tabla 2.41.

Tabla 2.41. Especificaciones mínimas para el Switch de Distribución

Switch de Distribución	
Parámetro	Especificaciones
Puertos Ethernet	24 puertos 10/100/1000 Mbps
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps
Capa	2/3
Backplane	20 Gbps
Throughput	6 Mpps
Seguridad	soporte de ACL
Manejo de VLANs	Si
Entrada de direcciones MAC	8000
Estándares IEEE	802.1d
	802.1p
	802.1q
	802.1x
	802.1w
	802.3u
	802.3x
802.3af	
Protocolo	IP ⁴ , IPv6, OSPF ⁵ , RIPv2 ⁶ , BGP ⁷ , DHCP ⁸
Administración	GUI, SNMP, Telnet, CLI

2.7.7.1.3. Switch de Core

Tienen alta capacidad de envío de paquetes hacia el exterior de la Red. Estos dispositivos deben tener alta disponibilidad y adaptarse a cambios de la Red.

Las especificaciones mínimas para el Switch de Core se revelan en la Tabla 2.42.

⁴ **IP** (Internet Protocol): Protocolo consciente en la expedición y enrutamiento de los paquetes entre los equipos de usuario final.

⁵ **OSPF** (Open Shortest Path First): Protocolo de enrutamiento de estado de enlace, robusto y escalable.

⁶ **RIPv2** (Routing Information Protocol): Protocolo de enrutamiento por vector distancia que soporta subredes, CIDR Y VLSM.

⁷ **BGP** (Border Gateway Protocol): Protocolo de puerta de enlace exterior que permuta los datos de dirección en los sistemas autónomos.

⁸ **DHCP** (Dynamic Host Configuration Protocol): Protocolo que asigna dinámicamente direcciones IP en cada dispositivo de la red.

Tabla 2.42. Especificaciones mínimas para el Switch de Core

Switch de Core	
Parámetro	Características
Puertos Ethernet	24 puertos 10/100/1000 Mbps
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps
Capa	2 y 3
Backplane	80 Gbps
Throughput	6 Mpps
Seguridad	soporte de ACL
Entrada de direcciones MAC	20000
Estándares IEEE	802.1d
	802.1p
	802.1q
	802.1x
	802.1w
	802.3u
	802.3x
802.3af	
Protocolos	IP, IPv6, OSPF, RIPv2, BGP, DHCP
Administración	GUI, SNMP, Telnet, CLI

2.7.7.1.4. Firewall

Para la elección del Firewall se debe tener en cuenta las siguientes especificaciones de acuerdo a la Tabla 2.43.

Tabla 2.43. Especificaciones mínimas para el Firewall

Firewall	
Stateful Inspection Throughput ⁹	450 Mbps
IPS Throughput ¹⁰	225 Mbps
3DES/AES VPN Throughput ¹¹	225 Mbps
Usuarios/Nodos	Ilimitado
IPsec VPN Peers	750
Conexiones Concurrentes	280000
VLANs	150
Alta disponibilidad	Activo
Puertos Seriales	1 RJ-45
Puerto de Administración	1 GE
Puertos de I/O Integrados	4 GE +1 FE
Memoria	2 GB

⁹ Rendimiento medido con tráfico UDP en condiciones ideales.

¹⁰ El tráfico de firewall que no pasa por el servicio IPS puede tener un mayor rendimiento.

¹¹ El rendimiento de VPN y el conteo de sesiones dependen de la configuración del dispositivo ASA y los patrones de tráfico de VPN. Estos elementos deben tenerse en cuenta como parte de su planificación de capacidad.

2.7.7.1.5. Servidores

Los servidores deben ser tolerantes a fallas, permitir aumento de capacidad de usuarios y de alto rendimiento y fácil administración.

- Ser tolerantes a fallas.
- Aumento de capacidad de usuarios.
- Alto rendimiento y de fácil administración.

El servidor de datos debe disponer de gran almacenamiento, memoria RAM y garantía en cuanto al soporte técnico.

El servidor de correo más utilizado es zimbra bajo el Sistema operativo Linux en cuanto a flexibilidad, fácil administración y de alta fiabilidad. Actualmente es con el que cuenta el Ministerio del Ambiente.

El servidor DHCP estipula las direcciones IP automáticamente instalado bajo Linux.

La función del Servidor de Llamadas IP es realizar llamadas y crear extensiones a los usuarios. Actualmente se cuenta con el Servidor

OmniPCX Enterprise que usa el sistema operativo Linux dentro de la red del Ministerio del Ambiente.

Entre sus características se encuentran las siguientes:

- Gestión eficiente de llamadas.
- Conectividad híbrida: IP, SIP¹², WLAN, IP-DECT, DECT, digital, analógica.
- Maneja un software propio del fabricante para la administración de la Telefonía IP.
- Alta disponibilidad y escalabilidad [11].

2.7.7.1.6. Cámaras de Video vigilancia

Estas cámaras deben cumplir con las características mínimas (ver Tabla 2.44).

¹² **SIP** (*Session Initiation Protocol*): Protocolo de capa aplicación que establece, modifica y termina sesiones multimedia.

Tabla 2.44. Especificaciones mínimas en las cámaras empleadas en Video vigilancia

Cámaras de Video vigilancia	
Parámetro	Características
Resolución	640 x 480
Tipo de compresión	H.264 ¹³
Iluminación	min 1 lux ¹⁴
Visibilidad nocturna	Si
Ángulo de visión	350 grados
Sensor de imagen	Si
Calidad de servicio	Si
Seguridad	Si
Estándares IEEE	802.3i
	802.3u
	802.3af
Protocolo	IPv4, IPv6, TCP ¹⁵ , UDP ¹⁶ , FTP ¹⁷ , HTTP ¹⁸ , DHCP, RTP ¹⁹ /RTCP ²⁰ , SNMP
Administración	Software libre

2.7.7.1.7. Access Point

Las especificaciones mínimas de estos equipos se establecen de acuerdo a los requerimientos de la institución y también se basa en las especificaciones de los equipos con los que actualmente cuenta la institución.

Estos APs deben cumplir con las especificaciones mínimas (ver Tabla 2.45).

¹³ **H.264:** Es un códec de video más reciente estandarizado por la UIT y usado como perfil de compresión de video.

¹⁴ **Lux:** Unidad de iluminancia, su función es determinar la porción de luz proyectada en la superficie.

¹⁵ **TCP (Transmission Control Protocol):** Es un protocolo verídico y orientado a la conexión, que brinda un medio sin errores para emitir la información.

¹⁶ **UDP (User Datagram Protocol):** Protocolo de transporte no orientado a conexión que intercambia datagramas (fragmento de paquete), sin acuse de recibo ni entrega garantizada.

¹⁷ **FTP (File Transfer Protocol):** Protocolo de red de transferencia de archivos en los sistemas unidos a una red TCP.

¹⁸ **HTTP (Hypertext Transfer Protocol):** Protocolo que transfiere datos entre los usuarios WEB y los servidores HTTP.

¹⁹ **RTP (Real-Time Transport Protocol):** Protocolo que admite a los receptores compensar el jitter (retardo variable) y detectar paquetes que arriben en desorden.

²⁰ **RTCP (RTP Control Protocol):** Es un protocolo utilizado con RTP que transporta datos de retroalimentación en cuanto a la calidad de transmisión.

Tabla 2.45. Especificaciones mínimas para el Access Point

Access Point	
Parámetro	Características
Frecuencia	2,4 GHz
Número de canales a 20 MHz	3
Rango	100 metros
No de puntos de acceso	64
Puertos Ethernet 10/100 base TX	2
Calidad de servicio	Si
Estándares IEEE	802.11 b/g/n
	802.3u
	802.1p
Seguridad	WPA2 ²¹ , TKIP ²² , AES ²³
Administración	CLI, Telnet

2.7.7.1.8. Teléfono IP

Para la elección del Teléfono IP se debe tener en cuenta las siguientes especificaciones de acuerdo a la Tabla 2.46.

Tabla 2.46. Especificaciones mínimas para el Teléfono IP

Teléfono IP	
Parámetro	Especificaciones
Puertos	2 puertos RJ45 10/100Mbps
Interfaces FXO	24
Códec de voz	G.711, G729
Anular resonancia	Si
Eliminación de sigilo	Si
Manejo de VLANs	Si
Estándares IEEE	802.1p
	802.1q
	802.3af
Protocolos	SNMPv1, SNMPv2, SNMPv3, Telnet, SIP, H.323 ²⁴ , MPLS ²⁵
Administración	GUI, SNMP, TELNET, CLI, RMON

²¹ **WPA2** (Wi-Fi Protect Access 2): Sistema de defensa de los sistemas inalámbricos empleando el algoritmo de cifrado AES.

²² **TKIP** (Temporal Key Integrity Protocol): Protocolo de seguridad que incluye mecanismos de seguridad del estándar 802.11 i para mejorar el cifrado de datos.

²³ **AES** (Advanced Encryption Standard): Sistema de ocultación de información por bloques.

²⁴ **H.323**: Es un protocolo parecido a SIP y se puede utilizar con paquetes IP.

²⁵ **MPLS** (Multiprotocol Label Switching): Arquitectura que proporciona un nombramiento eficiente, enrutamiento, expedición y conmutación de cantidad de información por la red.

2.7.8. DIRECCIONAMIENTO DE LA RED CORPORATIVA DEL MINISTERIO DEL AMBIENTE Y AGUA

2.7.8.1. Zona Desmilitarizada

Es una red apartada y localizada internamente en la red de la empresa. En la que aparecen los servidores web y mensajería. La DMZ impide las conexiones hacia la red local debido a que servidores pueden ser atacados desde Internet. La DMZ protegen los servidores de los ataques al bloquear conexiones (ver Figura 2.14) [12].

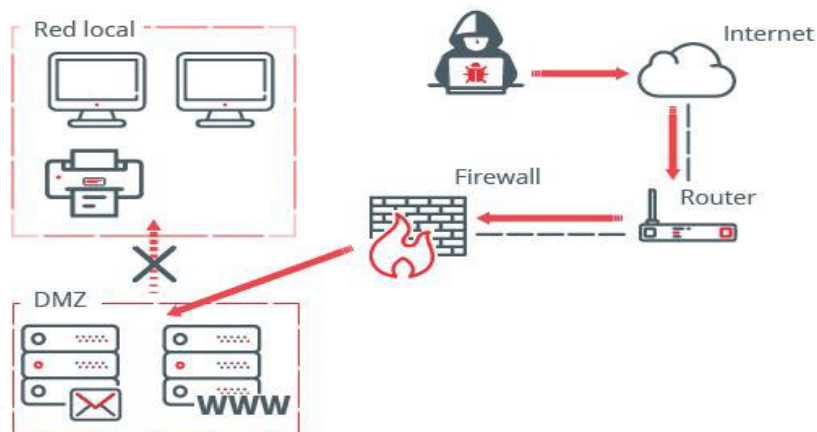


Figura 2.14. Zona desmilitarizada DMZ [12].

2.7.8.2. Direccionamiento IP para la Red Corporativa

Para la asignación de VLANs se consideró las funciones de cada departamento de cada uno de los edificios que compone el Ministerio, se llegó a fijar 26 VLANs. Además, se considera un direccionamiento de Subneteo partiendo de una dirección de red de clase B usando los 8 bits del último octeto para la creación de subredes y dejando los 8 bits restantes para los hosts. Se consideró VLSM dejando cantidad de direcciones de host necesarias en caso de un futuro crecimiento de la red (ver Figura 2.15).

Dirección Red	Dirección IP	Máscara de Red	Broadcast
	172.16.0.0	255.255.0.0	172.16.255.255
Bits Para Subred	8		
Subredes Necesitadas	25		
Subredes Totales	256		
Subredes Útiles	254		

VLAN	Dirección Subred	Máscara de Subred	Primera Dirección Válida	Última Dirección Válida	Broadcast
Recepción	172.16.1.0	255.255.255.0	172.16.1.1	172.16.1.254	172.16.1.255
Oficina	172.16.2.0	255.255.255.0	172.16.2.1	172.16.2.254	172.16.2.255
Subsecretaría	172.16.3.0	255.255.255.0	172.16.3.1	172.16.3.254	172.16.3.255
Dirección	172.16.4.0	255.255.255.0	172.16.4.1	172.16.4.254	172.16.4.255
Coordinación	172.16.5.0	255.255.255.0	172.16.5.1	172.16.5.254	172.16.5.255
Jurídico	172.16.6.0	255.255.255.0	172.16.6.1	172.16.6.254	172.16.6.255
Despacho Ministro	172.16.7.0	255.255.255.0	172.16.7.1	172.16.7.254	172.16.7.255
Despacho Viceministro	172.16.8.0	255.255.255.0	172.16.8.1	172.16.8.254	172.16.8.255
Secretaría	172.16.9.0	255.255.255.0	172.16.9.1	172.16.9.254	172.16.9.255
Auditoría	172.16.10.0	255.255.255.0	172.16.10.1	172.16.10.254	172.16.10.255
Proyecto	172.16.11.0	255.255.255.0	172.16.11.1	172.16.11.254	172.16.11.255
Financiera	172.16.12.0	255.255.255.0	172.16.12.1	172.16.12.254	172.16.12.255
Gestión	172.16.13.0	255.255.255.0	172.16.13.1	172.16.13.254	172.16.13.255
Contabilidad	172.16.14.0	255.255.255.0	172.16.14.1	172.16.14.254	172.16.14.255
Área Técnica	172.16.15.0	255.255.255.0	172.16.15.1	172.16.15.254	172.16.15.255
Asesoría	172.16.16.0	255.255.255.0	172.16.16.1	172.16.16.254	172.16.16.255
Administración	172.16.17.0	255.255.255.0	172.16.17.1	172.16.17.254	172.16.17.255
Producción	172.16.18.0	255.255.255.0	172.16.18.1	172.16.18.254	172.16.18.255
Pre-producción	172.16.19.0	255.255.255.0	172.16.19.1	172.16.19.254	172.16.19.255
Recaudación	172.16.20.0	255.255.255.0	172.16.20.1	172.16.20.254	172.16.20.255
Impresión	172.16.21.0	255.255.255.0	172.16.21.1	172.16.21.254	172.16.21.255
Atención al Público	172.16.22.0	255.255.255.0	172.16.22.1	172.16.22.254	172.16.22.255
Inalámbrico	172.16.23.0	255.255.255.0	172.16.23.1	172.16.23.254	172.16.23.255
Telefonía MAE	172.16.24.0	255.255.255.0	172.16.24.1	172.16.24.254	172.16.24.255
Telefonía SENAGUA	172.16.25.0	255.255.255.0	172.16.25.1	172.16.25.254	172.16.25.255
Video seguridad	172.16.26.0	255.255.255.0	172.16.26.1	172.16.26.254	172.16.26.255

Figura 2.15. Direccionamiento IP para la Red.

2.7.9. MECANISMOS DE SEGURIDAD

La red de la institución, maneja ciertas reglas de seguridad manejadas en el firewall Cisco ASA. El resumen de reglas permitidas (ver Figura 2.16).

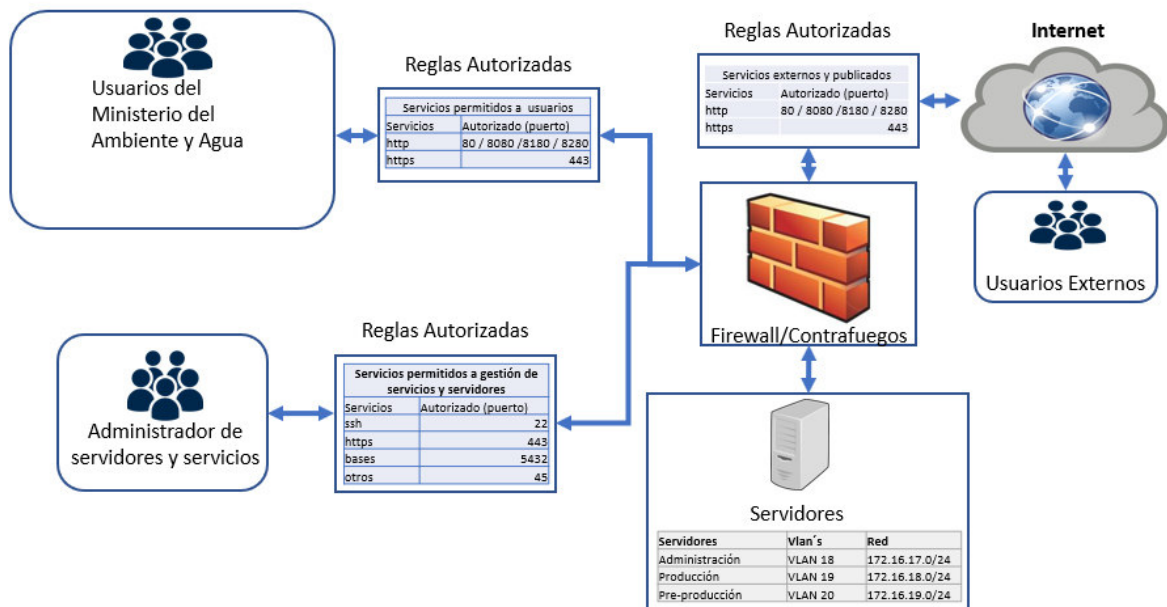


Figura 2.16. Reglas Autorizadas a cada grupo de usuarios en la Red.

Se maneja un perfil para cada uno de los grupos de usuarios en los cuales se establecen reglas específicas de acceso a un conjunto específico de servicios.

Para los servicios http y https pueden ingresar los Usuarios de la institución, como una lista de acceso por medio de las VLANs en su perfil específico.

Los Administradores de servidores tienen un perfil de acceso a los servicios de ssh, https, bases y otros.

Los usuarios externos son creados como una lista de acceso y dentro de un perfil para que el firewall permita el acceso http, https mediante los respectivos puertos.

Se dispone de 2 firewall Cisco Asa el uno que está Activo y el otro en Modo espera y se conmutan para que trabajen por turnos cada cierto tiempo. El estado del firewall se puede ver en la Figura 2.17.

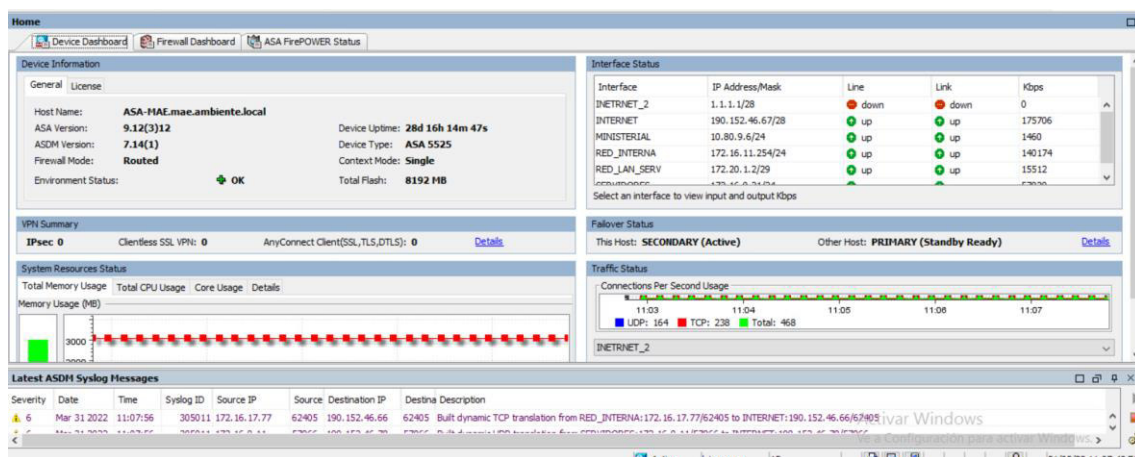


Figura 2.17. Interfaz del Firewall Cisco ASA.

La interfaz gráfica de la configuración del firewall nos indica el estado actual de las interfaces, así como el estado del tráfico de la red y el estado del manejo de los medios del sistema como memoria, uso de CPU.

2.7.9.1. Configuración de reglas permitidas en el firewall

La regla para la prueba de conectividad hacia el Internet (ver Figura 2.18).

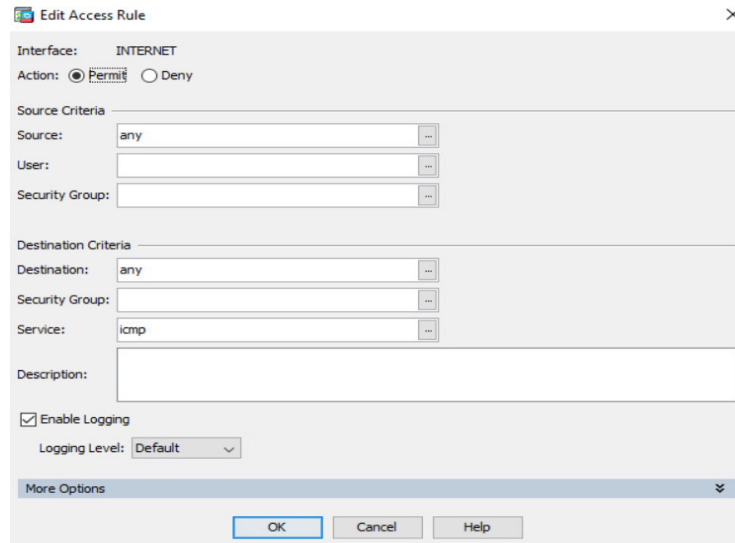


Figura 2.18. Regla de acceso hacia Internet mediante ICMP.

Esta regla nos indica que todo lo que sale desde esta interface hacia afuera pueda hacer ping mediante ICMP²⁶.

La regla para realizar el trazado de una ruta desde esta interface hacia el Internet (ver Figura 2.19).

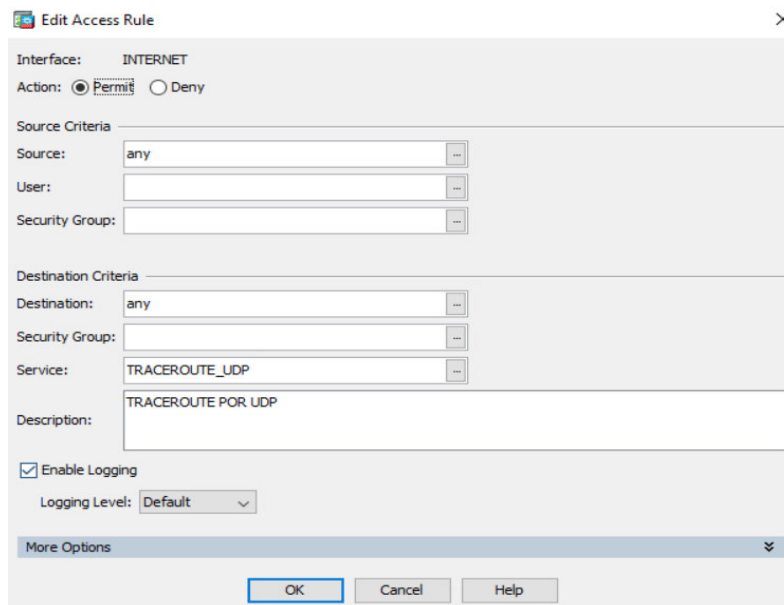


Figura 2.19. Regla de acceso hacia Internet usando Traceroute.

Estas reglas son usadas para pruebas de conectividad de equipos y se aplican tanto en la red Interna como a nivel de servidores para el acceso a Internet.

²⁶ **ICMP** (*Internet Control Message Protocol*): Protocolo en la capa de red, utilizado como mecanismo para la expedición de mensajes de control y error por la red.

Existen reglas de dominio externo las cuales se crean el firewall para el acceso a servidor previo la consulta del DNS (ver Figura 2.20).

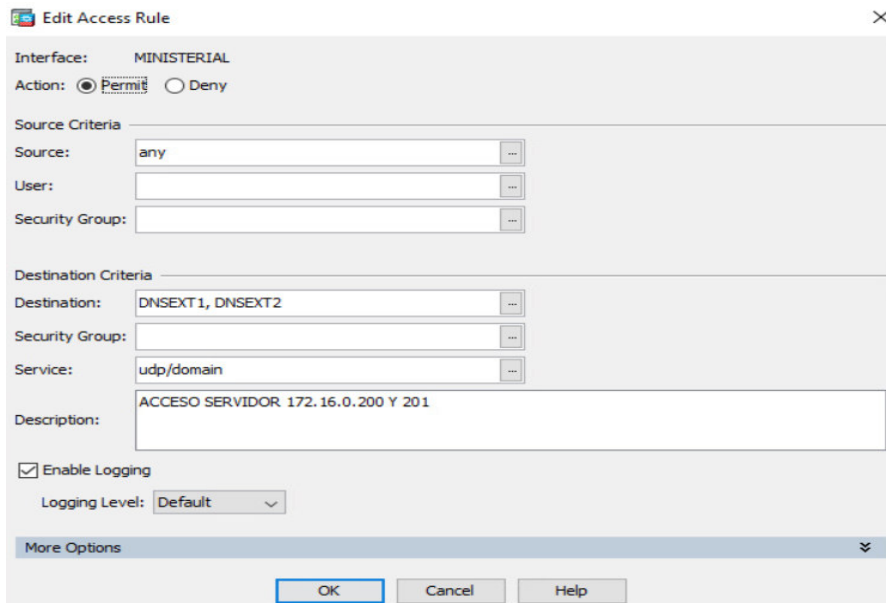


Figura 2.20. Regla para acceso al Servidor previo consulta del DNS.

Las reglas para un servicio específico en el cual un usuario desea acceder. Primero se debe tomar en cuenta en que lista de acceso se encuentra para poder darle permiso.

La regla que se indica en la Figura 2.21 es una regla de acceso a ANT.

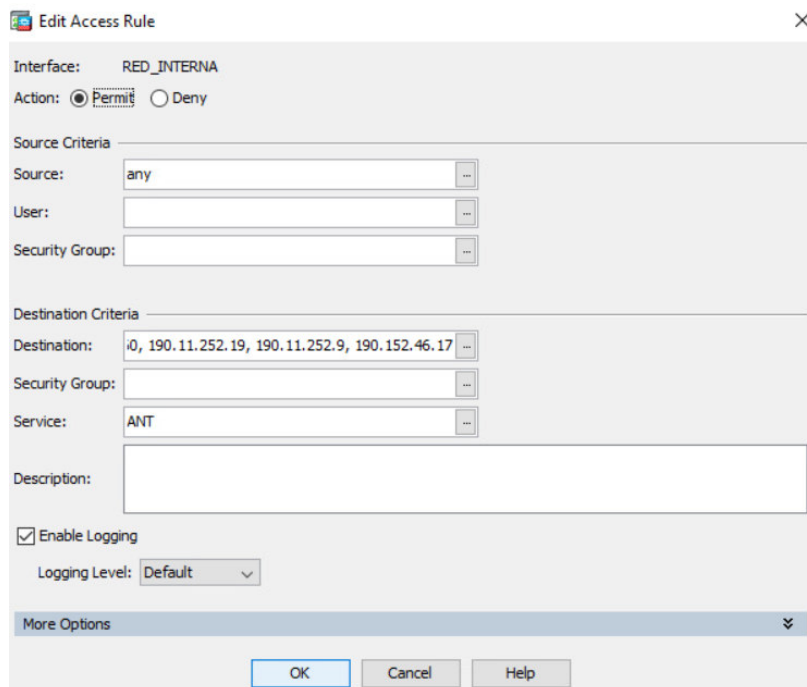


Figura 2.21. Regla de ingreso a los clientes de la red Interna hacia ANT.

La ANT no tiene dominio específico, pero manejan direcciones IP públicas. Como el firewall maneja direcciones IP y no dominios, se crea esta regla en el firewall para que los clientes de la Red Interna accedan hacia ANT.

Antes de acceder a un servicio básico, a los clientes se les asigna un dominio y un puerto específico y solo a direcciones IP específicas como se indican en la Figuras 2.22 y 2.23.

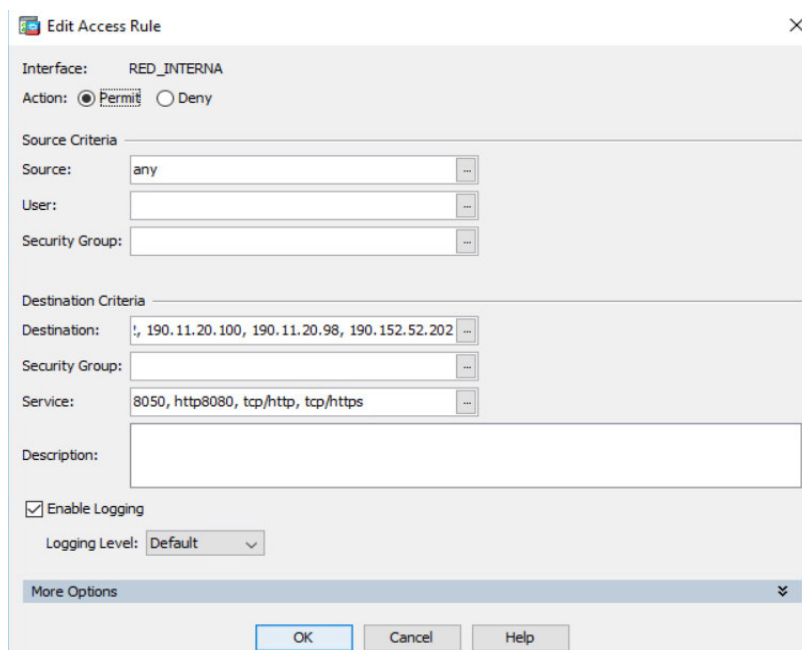


Figura 2.22. Regla de ingreso de los clientes a los servicios específicos de la Red.

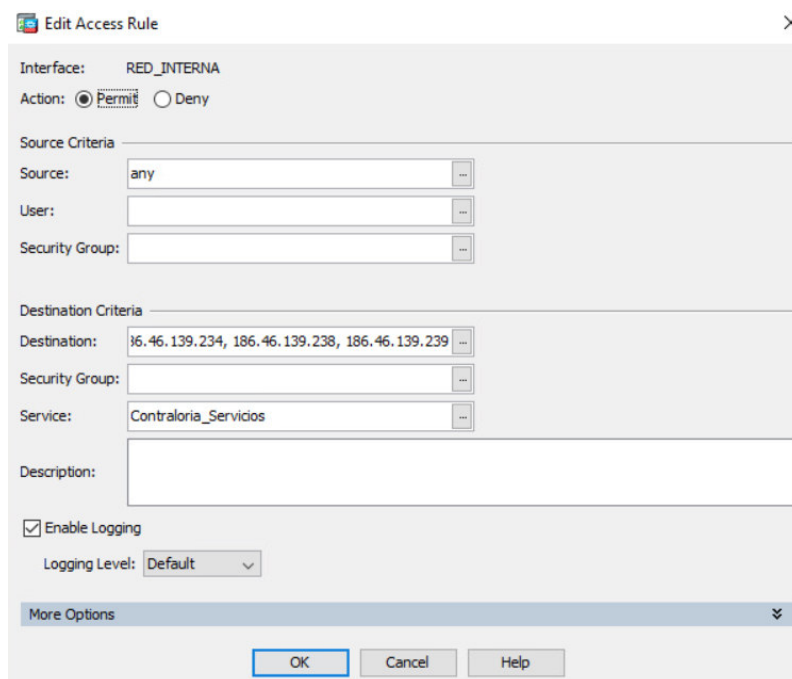
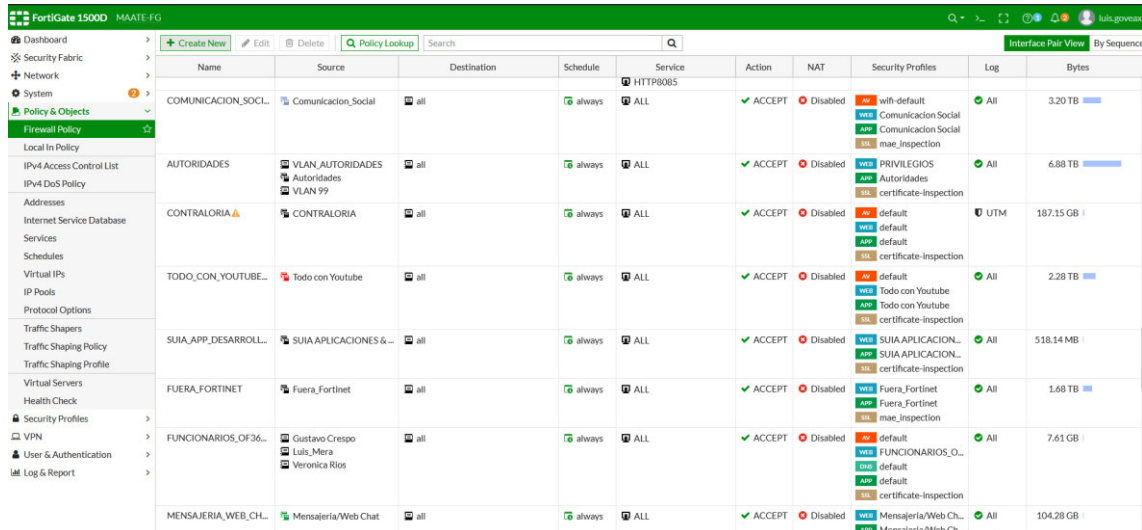


Figura 2.23. Regla de ingreso de los clientes a los servicios de la Contraloría.

2.7.9.2. Filtrado web

Para ello se dispone de un equipo Fortigate 1500, el cual también se establece reglas para permitir el acceso y denegación de páginas web.

Las reglas se basan por tipos de navegación, un usuario normal cae dentro de una regla normal con diferentes permisos (ver Figura 2.24).



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
COMUNICACION_SOCL...	Comunicacion_Social	all	always	ALL	ACCEPT	Disabled	with-default Communication Social Communication Social mae_Inspection	All	3.20 TB
AUTORIDADES	VLAN_AUTORIDADES Autoridades VLAN 99	all	always	ALL	ACCEPT	Disabled	PRIVILEGIOS Autoridades certificate-inspection	All	6.88 TB
CONTRALORIA	CONTRALORIA	all	always	ALL	ACCEPT	Disabled	default default certificate-inspection	UTM	187.15 GB
TODO_CON_YOUTUBE...	Todo con Youtube	all	always	ALL	ACCEPT	Disabled	default Todo con Youtube Todo con Youtube certificate-inspection	All	2.28 TB
SUIA_APP_DESARROLL...	SUIA APLICACIONES & ...	all	always	ALL	ACCEPT	Disabled	SUIA APLICACION... SUIA APLICACION... certificate-inspection	All	518.14 MB
FUERA_FORTINET	Fuera_Fortinet	all	always	ALL	ACCEPT	Disabled	Fuera_Fortinet Fuera_Fortinet mae_Inspection	All	1.68 TB
FUNCIONARIOS_OF36...	Gustavo Crespo Luis Mera Veronica Rios	all	always	ALL	ACCEPT	Disabled	default FUNCIONARIOS_O... default default certificate-inspection	All	7.61 GB
MENSAJERIA_WEB_CHL...	Mensajeria/Web Chat	all	always	ALL	ACCEPT	Disabled	Mensajeria/Web_CH... Mensajeria/Web_CH...	All	104.28 GB

Figura 2.24. Configuración de reglas de Filtrado Web.

2.7.9.3. Servicio de antivirus

A cada usuario se instala un agente y se la conecta a una consola, la cual le proporciona una licencia al agente y cada computador es registrado en la consola. La consola automáticamente proporciona el instalador al computador o el agente es instalado de manera manual. La licencia solo tiene validez si el agente es registrado por la consola. Se tiene una licencia comercial para 1500 equipos actualmente (ver Figura 2.25).



Figura 2.25. Software Antivirus Kaspersky Endpoint Security.

2.7.9.4. Observación de Tráfico en la red

Se utiliza el software PRTG Network Monitor en cuanto a la vigilancia de tráfico en la red desde diferentes localizaciones mediante interfaz gráfica. Utiliza protocolos como SNMP, contadores de rendimiento y SSH, además muestra notificaciones y alertas del tráfico (ver Figura 2.26) [13].

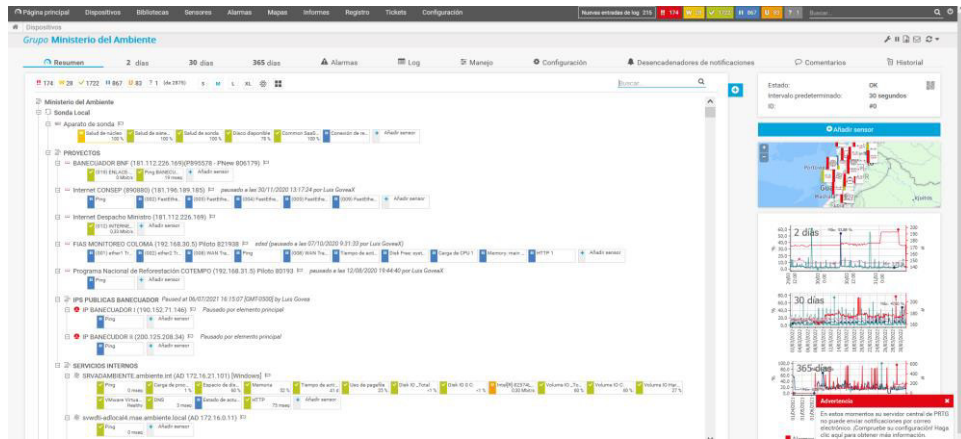


Figura 2.26. PTRG Network Monitor.

Se utiliza también para verificar el estado de los dispositivos e interfaces que se encuentran dentro de la red (ver Figura 2.27).

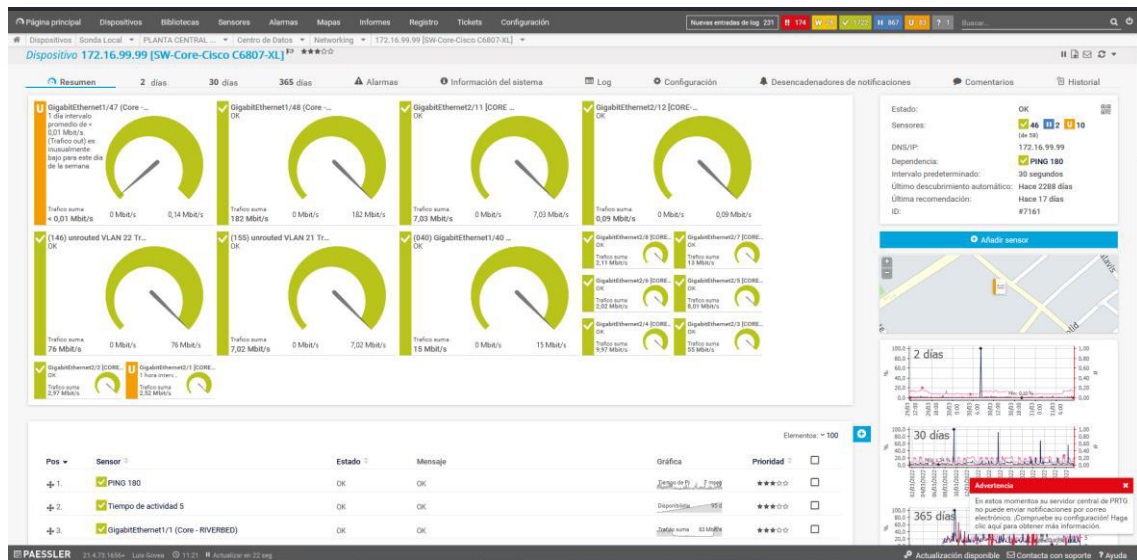


Figura 2.27. Estado de las Interfaces del Switch Core.

2.7.10. ALTA DISPONIBILIDAD DE LA RED

El diseño propuesto para la red de esta institución en cuanto a alta disponibilidad, tiene redundancia a nivel físico en enlaces redundantes, backbone y en equipos dentro de las capas más críticas como son la de distribución y core, a nivel de firewall se tiene redundancia. A nivel lógico también se tiene redundancia en cuanto al uso de protocolos como de agregación de enlace en los enlaces troncales. El diseño final se puede ver en la Figura 2.28.

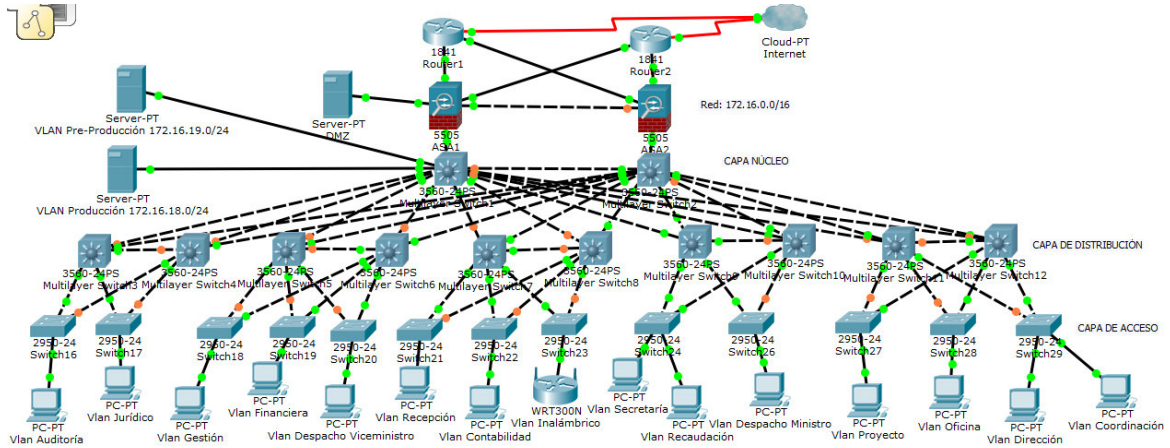


Figura 2.28. Diseño final de red propuesto.

2.8. PRESUPUESTO DE COSTOS PARA LA RED LAN CORPORATIVA

Se fija el costo de la red diseñada para la red LAN Corporativa para la institución, en base a los requerimientos del capítulo anteriormente descritos.

2.8.1. COSTO DE LA RED PASIVA

Como se determinó en el numeral 2.7.5.2.2, los elementos y accesorios de la red pasiva para la red de la institución, se va tomar en cuenta todos esos elementos para determinar el costo general de la Red Pasiva partir de la información anterior descrita. Para ello se muestra en la Tabla 2.47, las cantidades totales de cada elemento de la Red pasiva, así como su respectivo valor para así hallar el costo.

Tabla 2.47. Lista de Elementos de la Red Pasiva

LISTA DE ELEMENTOS PARA LA RED DEL MINISTERIO			
MATERIALES	CANTIDA D	P. Unitario (USD)	SUBTOTAL (USD)
Rollos de Cable UTP Categoría 6A	221	\$340	\$75140
Rollos de Fibra Óptica OM3	2	\$20449	\$40898
Faceplate simple	832	\$1,2	\$998,4
Faceplate doble	588	\$1,2	\$705,6
Conduit 3/4" mt.	6815	\$2	\$17037,5
Conduit 1" mt.	180	\$3	\$540
Escalerilla metálica	2714	\$3,7	\$10041,8
Caja 20x20 cajetín 20x10	68	\$0,5	\$34
Tapas 20x20	1453	\$2	\$2906
Jack RJ-45 cat. 6A	68	\$1	\$68
Rack abierto 12UR	2623	\$5,5	\$14426,5
Rack abierto 19UR	2	\$134,61	\$269,22
Rack abierto 19UR	6	\$174,57	\$1047,42
Rack abierto 24UR	6	\$182,29	\$1093,74
Rack abierto 42UR	10	\$196,26	\$1962,6
Patch Cords 1 mt.	516	\$2	\$1032
Patch Cords 3 mt.	2437	\$2,5	\$6092,5
Patch Panel de Fibra Óptica	23	\$102	\$2346
Patch Panel cat. 6A	92	\$12	\$1104
Organizador	136	\$8	\$1088
Toma eléctrica	99	\$15	\$1485
Otros (Tornillos, Tacos, Clavos, Alambre)	950	\$1	\$950
		SUBTOTAL (USD)	\$181266,28
		IVA (USD)	\$21751,9536
		TOTAL (USD)	\$203018,2336

2.8.2. COSTO DE LA RED ACTIVA

En la elección de los equipos de la red Activa se tomó en consideración algunas modelos y marcas de equipos, así como la verificación de las especificaciones mínimas que se

corresponden a considerar y que se especificó en el numeral 2.7.7.1. Para ello se consideró 3 marcas de fabricantes como Cisco, Huawei y Aruba.

2.8.2.1. Comparación de Switches de Acceso

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.1, se compara con las 3 marcas de equipos que se ha escogido para la comparación y su posterior elección (ver Tabla 2.48).

Tabla 2.48. Cuadro comparativo de los Switch de Acceso

Switch de acceso				
Marca		CISCO	HUAWEI	ARUBA
Modelo		C9200L-24P-4G-E	S2700-26TP-PWR-EI	2930F (JL259A)
Puertos Ethernet	24 puertos 10/100 Mbps	24 puertos 10/100/1000 Mbps	24 puertos 100 Mbps	24 puertos 10/100/1000 Mbps
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps	4 puertos Gigabit Ethernet de 1GE	2 puertos 10/100/1000 Mbps	4 puertos Gigabit Ethernet de 1GE
Capa	2	2	2	2
Backplane	6 Gbps	56 Gbps	32 Gbps	56 Gbps
Throughput	6 Mpps	41.66 Mpps	28 Mpps	41.77 Mpps
Administración de VLANs	Si	Si	Si	Si
QoS	Si	Si	Si	Si
Estándares IEEE	802.1d	Si	Si	Si
	802.1p			
	802.1q			
	802.1x			
	802.1w			
	802.3u			
	802.3af			
Protocolos	SNMP, Telnet	Si	Si	Si
Administración	GUI, SNMP, Telnet, CLI, RMON	Si	Si	Si
Costo (USD)		\$2.645,83	\$772,00	\$1.658,00

2.8.2.2. Comparación de Switches de Distribución

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.2, se compara con las 3 marcas de equipos que se ha escogido para la comparación y su posterior elección (ver Tabla 2.49).

Tabla 2.49. Cuadro comparativo de los Switch de Distribución

Switch de Distribución				
Marca		CISCO	HUAWEI	ARUBA
Modelo		C9200-24P-4X-E	S5731-H24P4XC	Aruba 6200F
Puertos Ethernet	24 puertos 10/100/1000 Mbps	Si	Si	Si
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps	4 puertos Gigabit Ethernet de 1GE	4 puertos Gigabit Ethernet de 10GE	4 puertos Gigabit Ethernet de 10GE
Capa	2 y 3	2 y 3	2 y 3	2 y 3
Backplane	20 Gbps	128 Gbps	288 Gbps	128 Gbps
Throughput	6 Mpps	95.23 Mpps	200 Mpps	95.2 Mpps
Seguridad	soporte de ACL	Si	Si	Si
Manejo de VLANs	Si	Si	Si	Si
Entrada de direcciones MAC	8000	32000	16000	16000
Estándares IEEE	802.1d	Si	Si	Si
	802.1p			
	802.1q			
	802.1x			
	802.1w			
	802.3u			
	802.3af			
Protocolos	IPv4, IPv6, OSPF, RIPv2, BGP, DHCP	Si	Si	Si
Administración	GUI, SNMP, Telnet, CLI	Si	Si	Si
Costo (USD)		\$4.129,39	\$2.452,00	\$2.106,00

2.8.2.3. Comparación de Switches de Core

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.3, se compara con las 3 marcas de equipos que se ha escogido para la comparación y su posterior elección como (ver Tabla 2.50).

Tabla 2.50. Cuadro comparativo de los Switch de Core

Switch de Core				
Marca		CISCO	HUAWEI	ARUBA
Modelo		C9500-24Y4C-A	S7703	6300M
Puertos Ethernet	24 puertos 10/100/1000 Mbps	Si	Si	Si
Puertos Uplink	2 puertos Gigabit Ethernet 10/100/1000 Mbps	Si	Si	Si
Capa	2 y 3	Si	Si	Si
Backplane	80 Gbps	2 Tbps	1.92 Tbps	880 Gbps
Throughput	6 Mpps	1 Bpps	1440 Mpps	654 Mpps
Seguridad	soporte de ACL	Si	Si	Si
Entrada de direcciones MAC	20000			
Estándares IEEE	802.1d	Si	Si	Si
	802.1p			
	802.1q			
	802.1x			
	802.1w			
	802.3u			
	802.3x			
802.3af				
Protocolo	IP, IPv6, OSPF, RIPv2, BGP, DHCP	Si	Si	Si
Gestión	GUI, SNMP, Telnet, CLI	Si	Si	Si
Costo (USD)		\$30.000,00	\$8.400,00	\$8.190,00

2.8.2.4. Comparación de Cámaras de Video vigilancia

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.6, se compara con las 2 marcas de equipos que se ha escogido para la comparación y su posterior elección (ver Tabla 2.51).

Tabla 2.51. Cuadro comparativo de los Cámaras de Video vigilancia

Cámaras de Video vigilancia			
Marca		HILOOK BY HIKVISION	D-Link
Modelo		PTZ-N4215I-DE	DCS-4614EK
Resolución	640 x 480	1920 x 1080	2592 x 1520
Tipo de compresión	H.264	H.265	H.265
Iluminación	min 1 lux	Si	Si
Visibilidad nocturna	Si	Si	Si
Angulo de visión	350 grados	Si	Si
Sensor de imagen	Si	Si	Si
Calidad de servicio	Si	Si	Si
Seguridad	Si	Si	Si
Estándares IEEE	802.3i	Si	Si
	802.3u		
	802.3af		
Protocolos	IP, IPv6, TCP, UDP, FTP, HTTP, DHCP, RTP/RTCP, SNMP	Si	Si
Administración	Software libre	Si	Propio del Fabricante
Costo (USD)		\$353,97	\$210,83

2.8.2.5. Comparación de los Access Point

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.7, se compara con las 2 marcas de equipos que se ha escogido para la comparación y su posterior elección (ver Tabla 2.52).

Tabla 2.52. Cuadro comparativo de los Access Point

Access Point			
Marca		CISCO	HUAWEI
Modelo		AIR-AP2802E-A-K9	AirEngine 5761-21
Frecuencia	2,4 GHz	Si	Si
Número de canales a 20 MHz	3	Si	Si
Rango	100 metros	Si	Si
No de puntos de acceso	64	Si	Si
Puertos Ethernet 10/100 base TX	2	Si	Si
Calidad de servicio	Si	Si	Si
Estándares IEEE	802.11 b/g/n	Si	Si
	802.3u		
	802.1p		
Seguridad	WPA, WPA2, TKIP, AES	WPA2-PSK	WPA2-PSK, WPA2-802,1X
Administración	CLI, Telnet	Si	Si
Costo (USD)		\$2.215,28	\$486,09

2.8.2.6. Comparación de los Teléfonos IP

Tomando en cuenta las características técnicas mencionadas en el numeral 2.7.7.1.8, se compara con las 2 marcas de equipos que se ha escogido para la comparación y su posterior elección (ver Tabla 2.53).

Tabla 2.53. Cuadro comparativo de los Teléfonos IP

Teléfono IP			
Marca		Grandstream	Cisco
Modelo		Grp2615	Cisco IP Phone 8851
Puertos	2 puertos RJ45 10/100Mbps	si	Si
Interfaces FXO	24	si	Si
Códec de voz	G.711, G729	si	Si
Anulación de resonancia	Si	si	Si
Eliminación de sigilo	Si	si	Si
Administración de VLANs	Si	si	Si
Estándares IEEE	802.1p	si	Si
	802.1q		
	802.3af		
Protocolo	SNMPv1, SNMPv2c, SNMPv3, Telnet, SIP, H.323, MPLS	si	Si
Administración	GUI, SNMP, RMON TELNET, CLI	si	Si
Costo (USD)		\$164,00	\$713,55

2.8.2.7. Equipos Cisco ASA

Se dispone de 2 equipos Firewall Cisco ASA 5525-X para la Red de la institución, una en modo activo y otra como respaldo en caso de que la primera falle por redundancia. Los costos de estos equipos no son tomados en cuenta para el presupuesto ya que se encuentran disponibles (ver Tabla 2.54).

Tabla 2.54. Especificaciones del Firewall Cisco ASA 5525-X

Firewall	
Marca	Cisco ASA
Modelo	5525-X
Stateful Inspection Throughput	2 Gbps
IPS Throughput	600 Mbps
3DES/AES VPN Throughput	300 Mbps
Usuarios/Nodos	Ilimitado
IPsec VPN Peers	750
Conexiones Concurrentes	500000
VLANs	150
Alta disponibilidad	Activo/En espera
Puertos Seriales	1 RJ-45
Puerto de Administración	1 GE
Puertos de I/O Integrados	8 GE
Memoria	8 GB

A más de cumplir de las características técnicas también se debe tomar en cuenta la garantía que ofrecen los Fabricantes a sus equipos en especial de los switches con lo cual se describe a continuación.

2.8.2.8. Garantía de Cisco

Cisco ofrece 5 años de garantía en sus equipos a partir de la fecha de envío del cliente. Durante este periodo en el caso de fallas de algún equipo, el fabricante envía un reemplazo del equipo en un periodo de 10 días hábiles como máximo. La garantía cubre si equipo tiene fallas internamente y no por una mala manipulación o caída de los equipos.

Cisco proporciona soporte técnico en las 8 horas hábiles, los 5 días de la semana en cuanto a diagnóstico y configuración de los dispositivos de conectividad. Una vez concluido esta garantía Cisco ofrece el servicio de SMARNET para renovar la garantía y seguirse manteniendo con soporte técnico además que esto ofrece herramientas e incluye un curso de capacitación personal para el correcto manejo de los dispositivos [20].

2.8.2.9. Garantía de Huawei

Huawei ofrece una garantía de 3 años con el usuario o la entidad que adquirió el equipo. La garantía empieza a partir de los 90 días de la fecha de envío o cuando Huawei recibe la solicitud. En caso de hardware Huawei garantiza el buen funcionamiento de sus equipos y en caso de reemplazo de equipos será cambiado por un nuevo o similar.

En caso de software Huawei ofrece una garantía limitada de 90 días [13].

2.8.2.10. Garantía de Aruba

Depende de los equipos de conectividad que se haya escogido en el caso de los switches. Para los usuarios que hayan adquirido estos equipos después del 1 de noviembre del 2019 tienen garantía de 5 años en cuanto a reemplazo de piezas o cambios de equipos siempre y cuando se presente un comprobante de compra para recibir la garantía. Circunscribe actualizaciones durante un año y corrección de vulnerabilidades de 3 años después de la terminación de la venta [14].

2.8.2.11. Elección de los equipos de red y costo de la red activa

Una vez que se ha realizado la comparación de las marcas de los equipos y también de la garantía que ofrecen los fabricantes se elige para este diseño los switches de marca CISCO debido a que ofrecen garantía de más tiempo y soporte técnico. En cuanto a cámaras de seguridad se elige la marca DLINK, en Access point se elige de Cisco y de Teléfonos IP se elige la marca Grandstream. Cabe recalcar que no se toma en cuenta la PBX y los servidores y otros equipos ya que son equipos que están en buen funcionamiento y no requieren cambios. Solo se realizará el presupuesto de los equipos activos que realmente necesitan un cambio.

Se enlista los componentes activos de la red con su respectivo costo y al final se determina el costo final para la red activa (ver Tabla 2.55).

Tabla 2.55. Lista de elementos para la Red Activa

LISTA DE EQUIPOS			
EQUIPOS	CANTIDAD	P. Unitario (USD)	SUBTOTAL (USD)
Switch de Acceso	92	\$2645,83	\$243416,36
Switch de Distribución	10	\$4139,29	\$41392,9
Switch de Core	2	\$30000	\$60000
Cámaras de Video vigilancia	199	\$210,83	\$41955,17
Access Point	30	\$2215,28	\$66458,4
Teléfono IP	651	\$164	\$106764
		SUBTOTAL (USD)	\$559986,83
		IVA (USD)	\$67198,4196
		TOTAL (USD)	\$627185,2496

2.8.3. COSTO DE LA RED LAN

Para comprobar este costo se deben sumar los valores totales de la Red Pasiva como de la Red Pasiva. A esto se debe añadir el costo del contrato del internet vigente para la Red con CNT en cual se particulariza (ver Tabla 2.56).

Tabla 2.56. Costo total de la red LAN Corporativa

Precio de los componentes pasivos de la Red (USD)	\$203.018,23
Precio de los componentes activos de la Red (USD)	\$627.185,25
Contrato de Internet	\$19.989,00
Costo Total de la Red LAN (USD)	\$850.192,48

El Costo total de la Red LAN Corporativa para el Ministerio es de 850192,48 dólares.

2.9. SIMULACIÓN DE LA RED LAN CORPORATIVA

2.9.1. SOFTWARE DE SIMULACIÓN DE RED

Para la simulación de la Red Corporativa de la institución, se utiliza el programa Cisco Packet Tracer el cual nos permite simular redes, a continuación, se indica el funcionamiento del programa.

2.9.1.1. Cisco Packet Tracer

Programa desarrollado por Cisco con el fin de simular redes y ciberseguridad a través de línea de comandos y también con interfaz gráfica (ver Figura 2.29) [15].

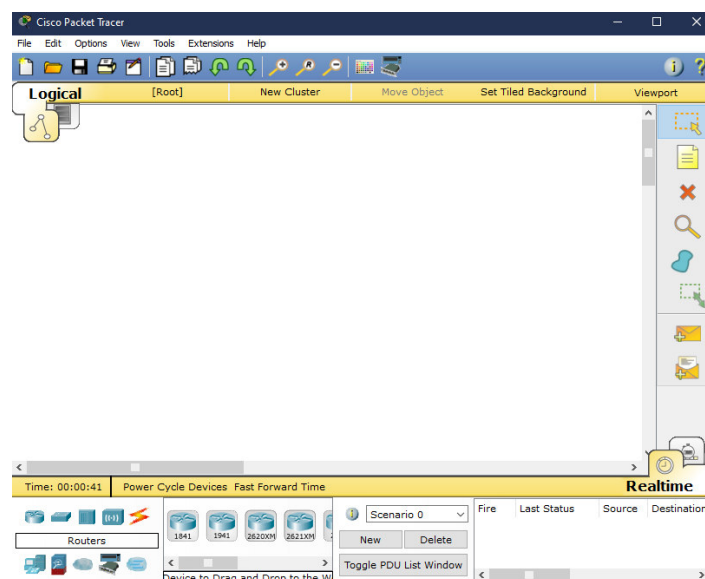


Figura 2.29. Programa Cisco Packet Tracer.

Para empezar la simulación se deben arrastrar los respectivos elementos de la red en la ventana, basándose en una topología de red y luego se realizan las configuraciones que se detallan a continuación.

2.9.1.2. Configuración básica de los switches y routers

Para ello movemos los elementos como los switches y routers al área de simulación y entramos al CLI a empezar la edición de la configuración básica (ver Figura 2.30).

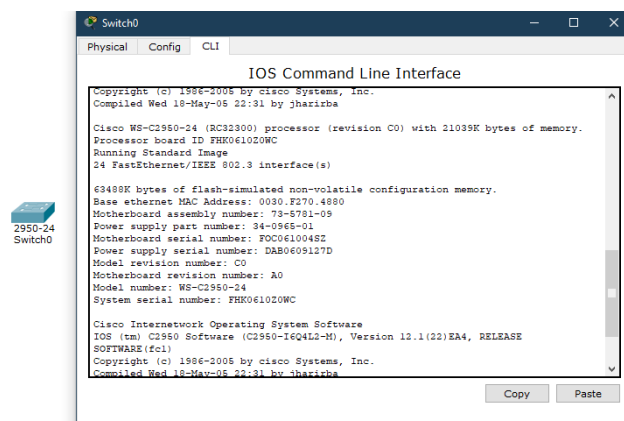
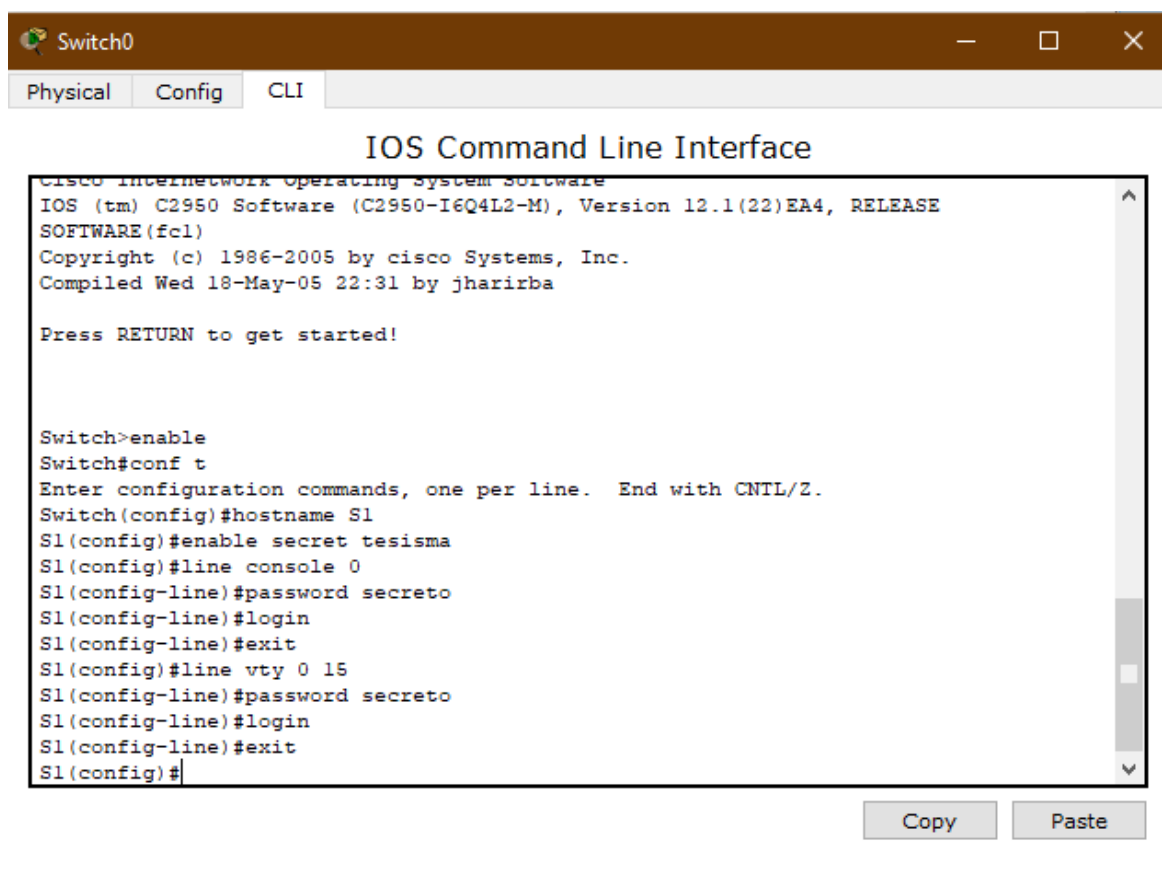


Figura 2.30. Ingreso al CLI del switch.

El Comando 2.1 muestra la configuración básica del switch.



Comando 2.1. Configuración básica del switch mediante CLI

Se activa el modo privilegiado EXEC con el comando enable y con el comando configure terminal (conf t) se accede al modo de configuración global.

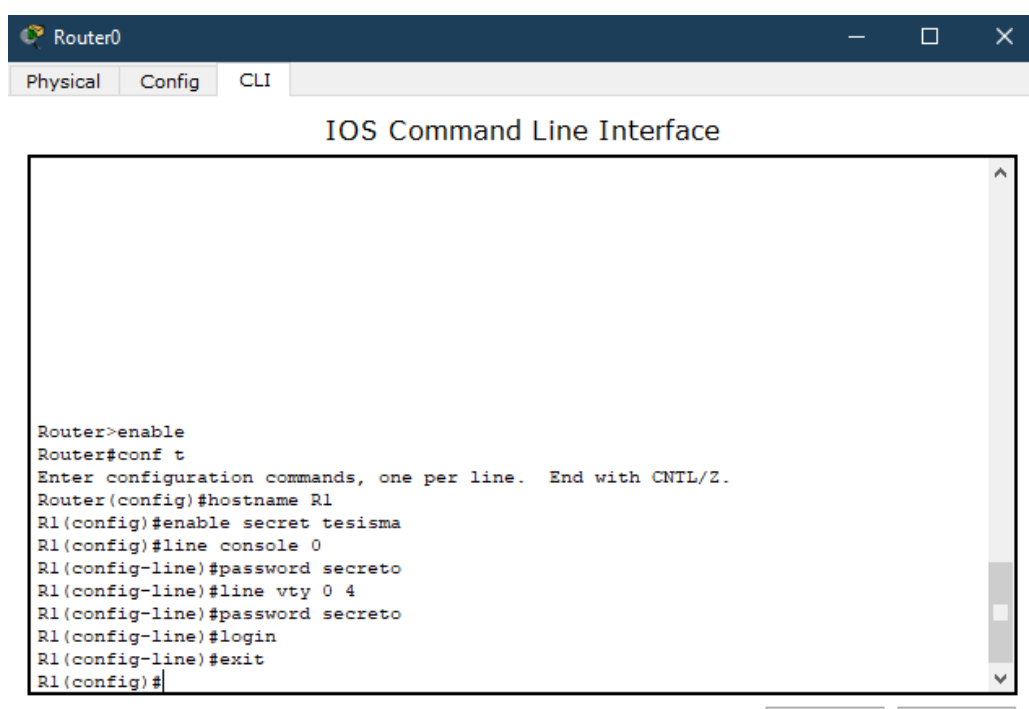
Enable secret (password codifica una contraseña en forma segura, el cual se le ha designado password tesisma.

Line console 0 admite el ingreso de contraseña a la línea de consola y restringe el ingreso.

Line vty indica el número de usuarios conectados remotamente en el equipo y permite el ingreso mediante contraseña.

Así mismo para el router se realiza la misma configuración similar a la del switch.

El Comando 2.2 muestra las configuraciones básicas del router.



```
Router0
Physical Config CLI
IOS Command Line Interface

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret tesisma
R1(config)#line console 0
R1(config-line)#password secreto
R1(config-line)#line vty 0 4
R1(config-line)#password secreto
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Comando 2.2. Configuraciones básicas del router mediante CLI

2.9.2. SIMULACIÓN DE LA RED

Se realiza la simulación de las 3 VLANs de la Red siguiendo el esquema del direccionamiento IP del numeral 3.8.2 (ver Figura 2.31).

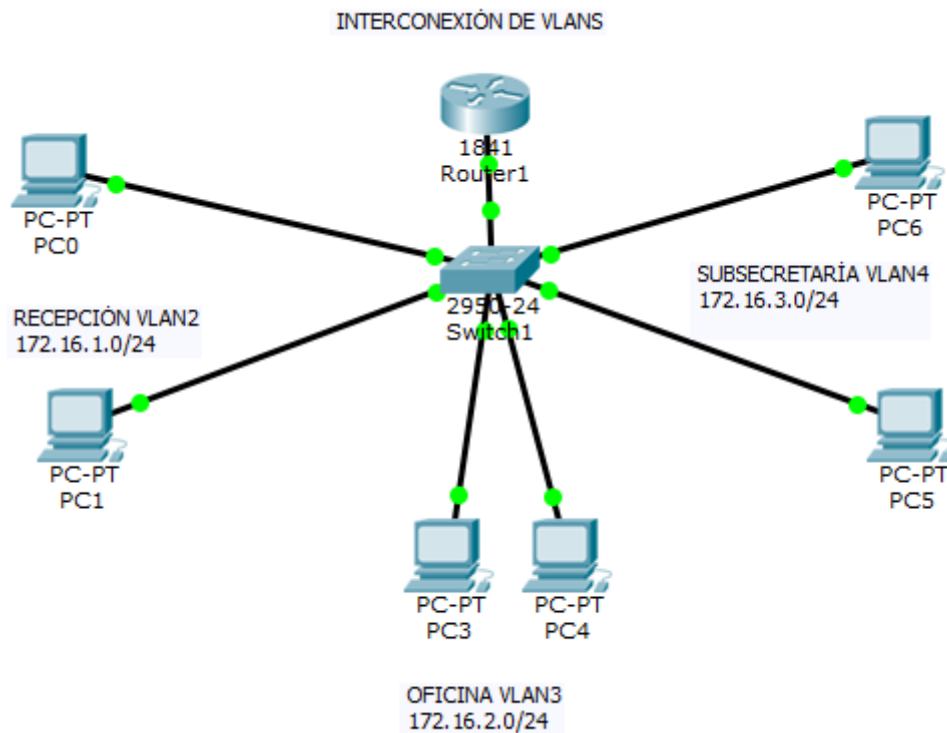


Figura 2.31. Esquema de la red a simular.

Primero se realiza las configuraciones básicas en el switch y router con los comandos mencionados anteriormente en el numeral 4.2.1.2.

Luego se crea las vlans con su nombre con los comandos vlan y name respectivamente.

Se ingresa al rango de interfaces correspondientes y con el comando switchport access vlan 2 se le da acceso a la vlan correspondiente (ver Comando 2.3).

```
S1(config)#vlan 2
S1(config-vlan)#name RECEPCION
S1(config-vlan)#exit
S1(config)#interface range fa0/2-3
S1(config-if-range)#switchport access vlan 2
S1(config-if-range)#exit
S1(config)#vlan 3
S1(config-vlan)#name OFICINA
S1(config-vlan)#exit
S1(config)#interface range fa0/4-5
S1(config-if-range)#switchport access vlan 3
S1(config-if-range)#exit
S1(config)#vlan 4
S1(config-vlan)#name SUBSECRETARIA
S1(config-vlan)#exit
S1(config)#interface range fa0/6-7
S1(config-if-range)#switchport access vlan 4
S1(config-if-range)#exit
S1(config)#
```

Comando 2.3. Creación de VLANs y asignación de interfaces

El comando show vlan brief indica las vlans creadas (ver Comando 2.4).

```
S1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
2 RECEPCION	active	Fa0/2, Fa0/3
3 OFICINA	active	Fa0/4, Fa0/5
4 SUBSECRETARIA	active	Fa0/6, Fa0/7
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
S1#
```

Comando 2.4. Directorio de VLANs creadas

Se ingresa a la interfaz del switch que está conectada con el router y se cambia a modo troncal con el comando switchport mode trunk (ver Comando 2.5).

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Comando 2.5. Configuración del enlace troncal en la interfaz del switch

Se habilita la interfaz del router que está conectada al switch con el comando no shutdown (ver Comando 2.6).

```
R1(config)#interface fa0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Comando 2.6. Habilitación del interfaz del router

Se verifica los enlaces troncales en el switch S1 (ver Comando 2.7).

```

S1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,2,3,4

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,2,3,4

```

Comando 2.7. Lista de enlaces troncales

Se configuran las subinterfaces y se establece el encapsulamiento del enlace troncal, se asocia la vlan con la subinterfaz y se pone una dirección IP que va a ser las direcciones de puerta de enlace para su correspondiente vlan (ver Comandos 2.8, 2.9).

```

R1(config)#interface fa0/0.2
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state
to up

R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 172.16.1.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fa0/0.3
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state
to up

R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 172.16.2.1 255.255.255.0
R1(config-subif)#exit

```

Comando 2.8. Distribución de 3 subinterfaces y encapsulamiento en el router

```

R1(config)#interface fa0/0.4
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state
to up

R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#ip address 172.16.3.1 255.255.255.0
R1(config-subif)#exit
R1(config)#

```

Comando 2.9. Configuración de la cuarta subinterfaz y encapsulamiento en el router

Finalmente, se le asigna la respectiva dirección IP cada PC correspondiente junto a su máscara de red y respectiva puerta de enlace (ver Figura 2.32).

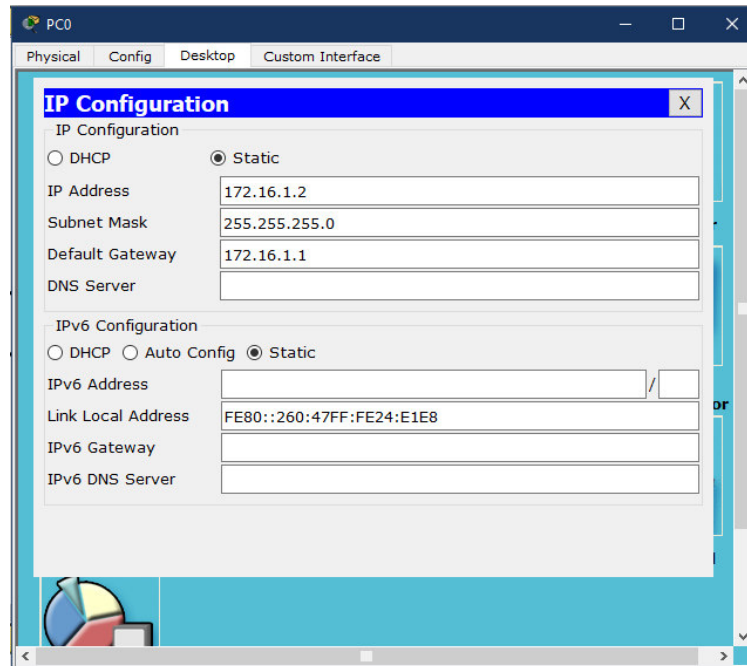


Figura 2.32. Configuración IP en la PC.

2.9.3. SIMULACIÓN DE ACCESO A INTERNET USANDO EL FIREWALL CISCO ASA

La configuración del firewall se realizó mediante consola desde una PC.

Para esta simulación se emplea el siguiente esquema de red (ver Figura 2.33).

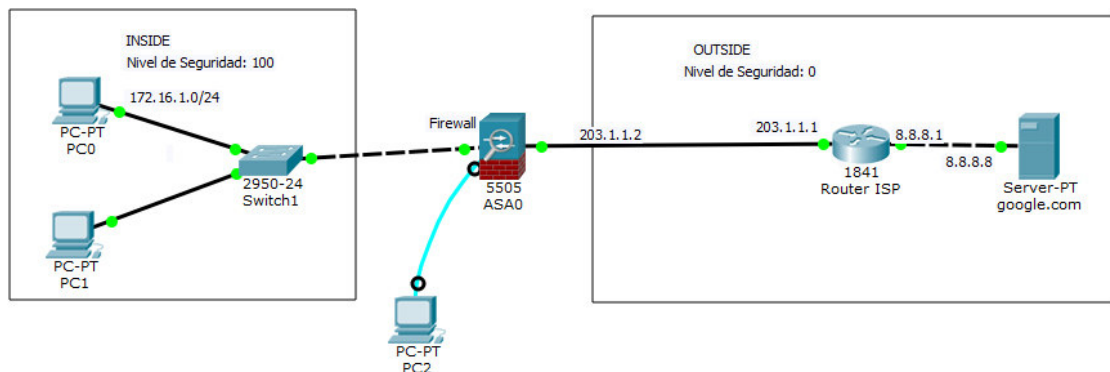


Figura 2.33. Acceso a Internet mediante el uso del Firewall.

Primero se verifica la configuración que trae por defecto el firewall con el comando `show running-config`. El Comando 2.11 indica que se encuentran por defecto 2 interfaces una inside y otra outside con sus respectivas direcciones IP y nivel de seguridad.

```

Terminal
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!

```

Comando 2.11. Configuración por defecto del Firewall Cisco ASA

Se quitan las direcciones IP de las interfaces mediante los comandos que se indican en el Comando 2.12.

```

ciscoasa(config)#interface vlan1
ciscoasa(config-if)#no ip address
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
ciscoasa(config-if)#exit
ciscoasa(config)#no dh
% Incomplete command.
ciscoasa(config)#no dhcpd address ?

configure mode commands/options:
WORD IP address[es], <ipl>[-<ip2>]
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside
Interface inside ip address or netmask not valid (0.0.0.0/255.255.255.255)
ciscoasa(config)#end

```

Comando 2.12. Eliminación de direcciones IP en las interfaces

Se verifica el cambio de configuración con el comando show running- config (ver Comando 2.13).

```

interface Vlan1
 nameif inside
 security-level 100
 no ip address
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp

```

Comando 2.13. Verificación de la configuración de las interfaces

Se configura cada interface con los respectivos niveles de seguridad (ver Comando 2.14).

```

ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#int e0/1
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit

```

```

ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 203.1.1.2 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#exit
ciscoasa(config)#

```

Comando 2.14. Disposición de las interfaces.

Al router ISP se añaden las respectivas direcciones IP en la interface correspondiente (ver Comando 2.15).

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int f0/0
ISP(config-if)#ip address 203.1.1.1 255.255.255.0
ISP(config-if)#no shutdown
ISP(config-if)#int f0/1
ISP(config-if)#ip address 8.8.8.1 255.255.255.0
ISP(config-if)#no shutdown
ISP(config-if)#exit

```

Comando 2.15. Configuración del Router ISP

Se configura el servidor DNS y DHCP en el Firewall Cisco ASA y se verifica la configuración con el comando show running-config (ver Comando 2.16).

```

ciscoasa(config)#dhcpd address 172.16.1.5-172.16.1.6 inside
ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside
ciscoasa(config)#end

-
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 172.16.1.5-172.16.1.6 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd enable inside
!
dhcpd auto_config outside
-

```

Comando 2.16. Configuración de los Servidores DHCP y DNS

Se configura una ruta por defecto en el firewall y una ruta dinámica en el router (ver Comando 2.17).

```

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.1.1.1

ISP(config)#router ospf 1
ISP(config-router)#network 203.1.1.0 0.0.0.255 area 0
ISP(config-router)#network 8.8.8.0 0.0.0.255 area 0

```

Comando 2.17. Creación de rutas

Se crean objetos de red y se habilita NAT (ver Comando 2.18).

```
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
```

Comando 2.18. Creación de objeto de red y habilitación de NAT

Se crean listas de acceso y un acceso de grupo para que la red tenga salida hacia Internet (ver Comando 2.19).

```
ciscoasa(config)#access-list in_to_internet extended permit tcp any any
ciscoasa(config)#access-list in_to_internet extended permit icmp any any
ciscoasa(config)#access-group in_to_internet in interface outside
```

Comando 2.19. Creación de listas de acceso

También se verifica el NAT con los comandos que se indican en el Comando 2.20.

```
ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s -
static, T - twice, N - net-to-net
ICMP PAT from inside:172.16.1.5/3 to outside:203.1.1.2/14259 flags i idle
00:00:08, timeout 0:00:30

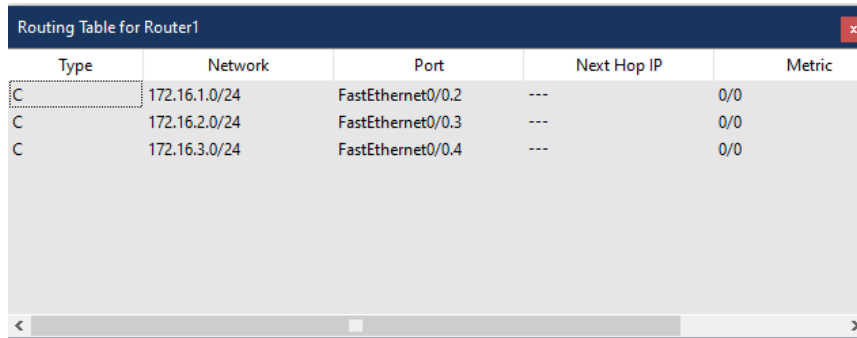
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic LAN interface
  translate_hits = 183, untranslate_hits = 182
```

Comando 2.20. Verificación del NAT

3. RESULTADOS Y DISCUSIÓN

3.1. PRUEBAS EN LA SIMULACIÓN DE LA RED

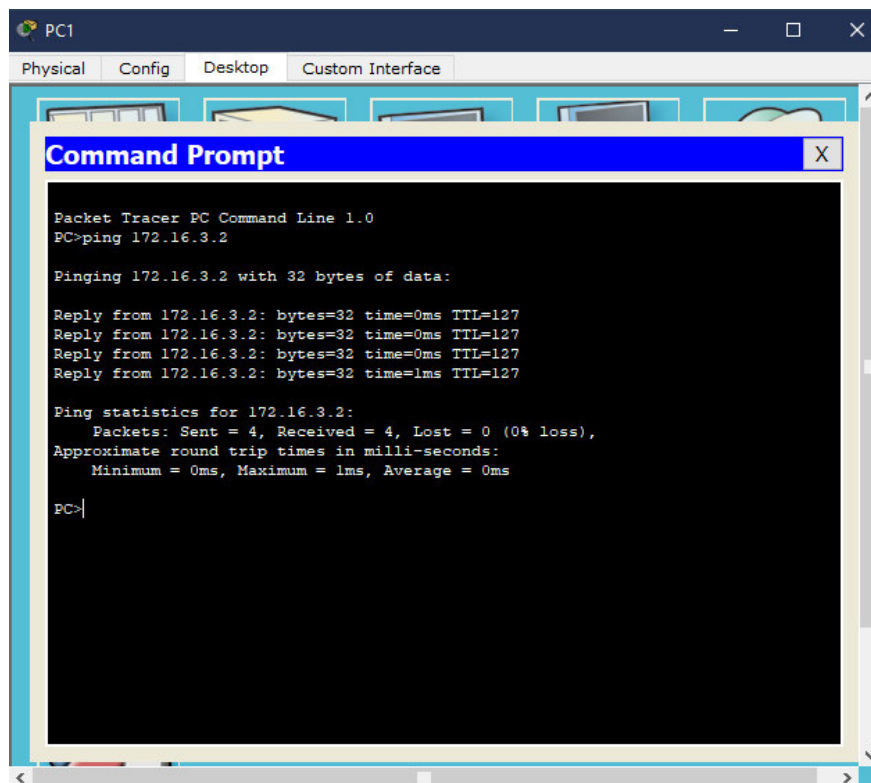
Una vez configurado la simulación de la red del numeral 2.9.2, se puede verificar la tabla de enrutamiento (ver Figura 3.1).



Type	Network	Port	Next Hop IP	Metric
C	172.16.1.0/24	FastEthernet0/0.2	---	0/0
C	172.16.2.0/24	FastEthernet0/0.3	---	0/0
C	172.16.3.0/24	FastEthernet0/0.4	---	0/0

Figura 3.1. Tabla de enrutamiento del router.

Se realiza la prueba de verificación con el comando ping de la PC1 de VLAN Recepción a la PC 5 de VLAN Subsecretaría (ver Figura 3.2).



```
Packet Tracer PC Command Line 1.0
PC>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time=0ms TTL=127
Reply from 172.16.3.2: bytes=32 time=0ms TTL=127
Reply from 172.16.3.2: bytes=32 time=0ms TTL=127
Reply from 172.16.3.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Figura 3.2. Prueba de conectividad

3.2. PRUEBAS EN LA SIMULACIÓN DE ACCESO A INTERNET USANDO EL FIREWALL CISCO ASA

Una vez configurado la simulación del numeral 2.9.3 , dentro del terminal del Servidor se realizan las pruebas de conectividad utilizando el comando PING hacia la puerta de enlace y salida de la interfaz de router (ver Figura 3.3).

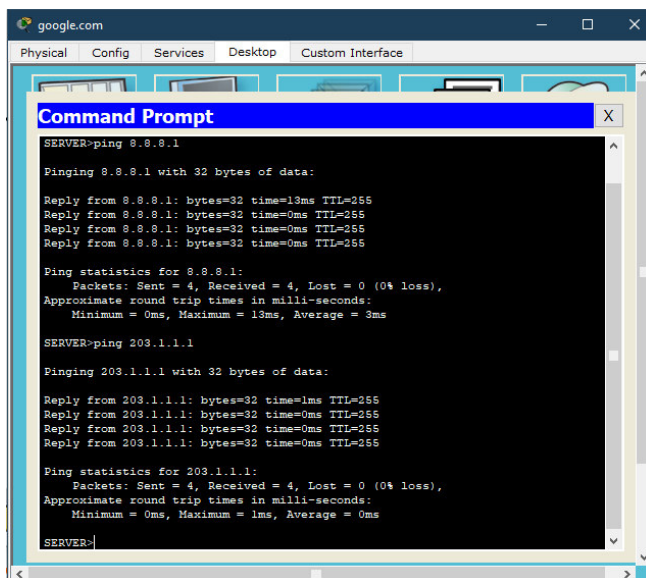


Figura 3.3. Prueba de conectividad del Servidor a la puerta de enlace

Se habilita el DHCP en cada una de las PCs de la red interna y se comprueba que tenga asignada una dirección IP automática y también se verifica la conectividad con la puerta de enlace (ver Figura 3.4).

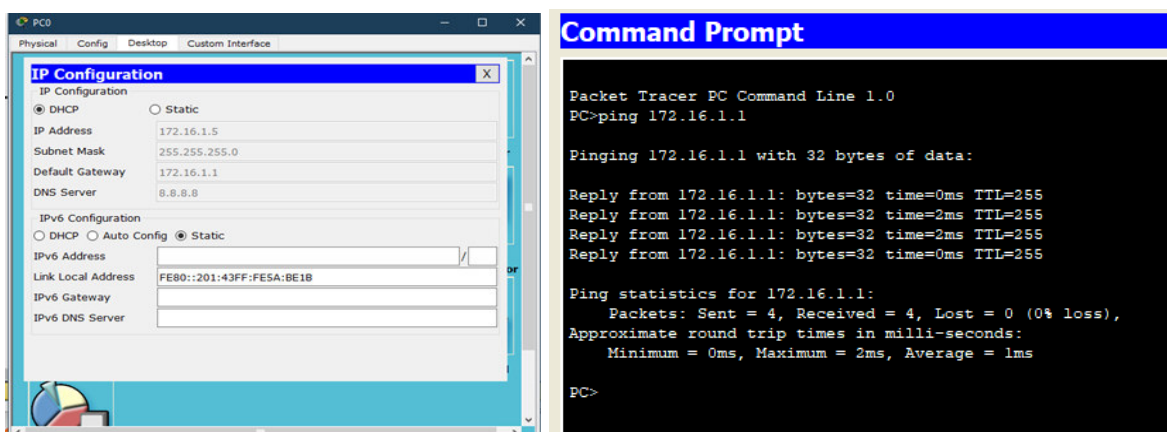


Figura 3.4. Verificación de los Servidores DHCP y DNS en los PCs

Se verifica la conectividad desde la red interna hacia el servidor DNS (ver Figura 3.5).

```

PC>ping -t 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=0ms TTL=126
Reply from 8.8.8.8: bytes=32 time=16ms TTL=126
Reply from 8.8.8.8: bytes=32 time=0ms TTL=126
Reply from 8.8.8.8: bytes=32 time=0ms TTL=126
Reply from 8.8.8.8: bytes=32 time=4ms TTL=126
    
```

Figura 3.5. Prueba de conectividad hacia el Servidor DNS.

3.3. ANÁLISIS DE RESULTADOS

A continuación, se muestra el diagrama de red diseñado propuesto (ver Figura 3.6).

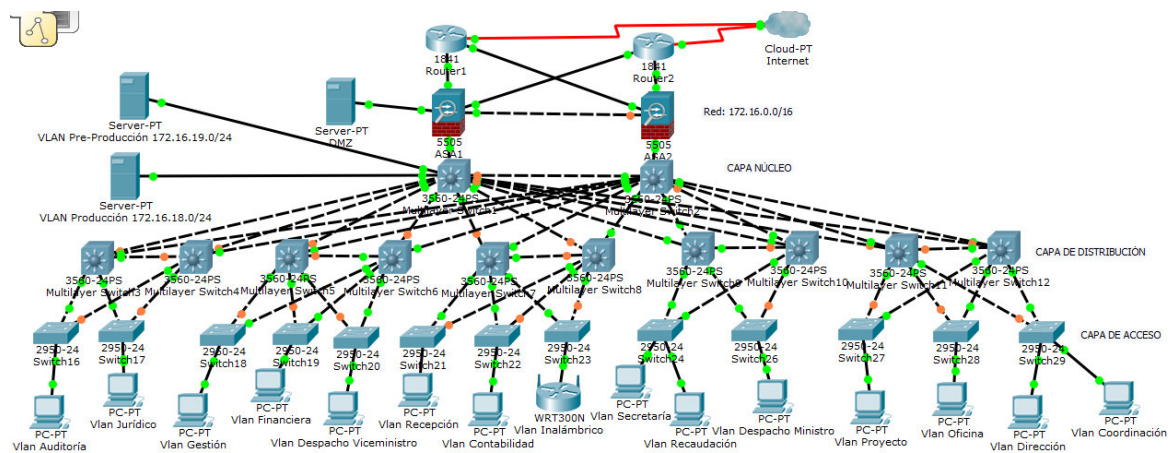


Figura 3.6. Red propuesta final.

; en el cual se indica el modelo jerárquico diseñado de 3 capas y además se añadió redundancia en las capas más críticas que son de distribución y núcleo para que tenga alta disponibilidad. Además, cuenta con una zona desmilitarizada DMZ para prevención de ataques externos de Internet en contra de los servidores de mensajería, DNS y navegación en cuanto a seguridad.

El costo de la Red diseñada representa el cambio que se debe hacer, sin embargo, todo depende de las políticas del Ministerio ya que también depende de eso.

El manejo de presupuesto es vital para un cambio en cuanto a una infraestructura de red. El Ministerio tiene la libertad de elegir los equipos para el cambio tomando en cuenta las especificaciones técnicas mínimas que se requiere.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- El estudio del escenario actual del Ministerio enfoca claramente la red que manejan, así como los requerimientos actuales que necesitan para poder dar solución o alternativas en cuanto a cambios de equipos o un diseño integrado de la red.
- Gracias a este análisis se logró obtener información acerca de todos los equipos de conectividad con los que cuenta para poder verificar las condiciones que se encuentran y poder dar solución.
- Se realizó el diseño jerárquico e integrado en una misma red para el Ministerio, así como el manejo de un cuarto de equipos y de telecomunicaciones centralizado.
- Se consideró una escalabilidad del 20% para los puntos de red en el caso de que la red crezca a futuro y también considerando una vida útil de la red de 10 años por el sistema del cableado estructurado sin cambios.
- Se añadió redundancia en la red en cuanto equipos de conectividad dentro de las capas más críticas para tener alta disponibilidad y además se estableció una DMZ para la prevención de ataques externos de otras redes hacia nuestra red interna incluyendo los servidores.
- Se estableció un presupuesto de la red en base al diseño realizado, tomando en cuenta los equipos activos de la red a ser cambiados y también especificando características técnicas a tomar en cuenta.
- Se dividió a la red en subredes en función de áreas de trabajo de cada uno de los edificios que conforman el Ministerio, usando VLSM tomando en cuenta el crecimiento a futuro, sin desperdiciar direcciones.
- Se realizó una simulación la cual nos permite interactuar con varias VLANs dentro de la misma red permitiendo la comunicación de los dispositivos sin importar su ubicación física de la red sino en la parte lógica.
- Se determinó un fabricante para el establecimiento de los equipos de la red activa que fue CISCO debido a su tiempo de garantía y soporte técnico en cuanto a la configuración y manejo adecuado de los equipos mediante un curso presencial para los administradores de la red.
- Se estableció mecanismos de seguridad a través de políticas y reglas para el acceso de servicios a grupos de usuarios mediante listas de acceso y perfiles y también hacia servicios específicos.

4.2. RECOMENDACIONES

- Al diseño de la red LAN se requiere considerar las áreas y espacios del edificio por donde se debe realizar el cableado sin afectar la infraestructura física del mismo
- Se deben tomar en cuenta las aplicaciones futuras que necesitaran mayor consumo de recursos de red por lo cual se debe proyectar la red LAN a futuro para evitar cambios constantes en la red en periodos cortos de tiempo.
- No se debe sobredimensionar la red, siempre se debe tomar en cuenta un grado de crecimiento a futuro de la red.
- Se debe tomar en cuenta el escenario en el cual se diseña la Red en cuanto a servicios que va a prometer la red.
- Mantener un alto nivel de seguridad en cuanto a la información más crítica que tenga la institución o empresa mediante el uso de Firewalls en redundancia y DMZ, para proteger información confidencial de ataques externos provenientes de Internet.
- Tomar en cuenta la vigencia de la licencia de los equipos de seguridad de la red ya que, si estos equipos fallan, puede la red estar expuesta a ataques, incluso el robo de información confidencial de la empresa o institución.
- Utilizar estándares y protocolos de la red de organismos de las Telecomunicaciones como la ITU, EIA, IEEE entre otros que se encuentren vigentes y no descontinuados.
- Para el dimensionamiento de la cantidad de información que transita por la red se debe tomar los valores promedio de acuerdo al grado de utilización del servicio de cada empresa o institución que generalmente se toma dentro hora crítica, es decir la hora donde más usuarios acceden a ese servicio.
- El uso de VLSM en la creación de subredes nos permite utilizar eficientemente el uso de direcciones IP sin desperdiciar de acuerdo a la cantidad de clientes que se tiene por subred.
- Se debe elegir los equipos de conectividad de acuerdo a los beneficios que se puede obtener y no solo por ahorro de dinero, el elegir un equipo correctamente puede brindar mayores beneficios de uso y de administración.
- Se debe tomar en cuenta la compatibilidad de los equipos con la infraestructura de red actual ya que el avance de la tecnología avanza y con el pasar del tiempo, los equipos nuevos funcionan con nuevos estándares y protocolos que no se los puede admitir dentro de la red.

5. REFERENCIAS BIBLIOGRÁFICAS

- [1] J. C. Santos, "SEGURIDAD Y ALTA DISPONIBILIDAD," España: RA-MA S.A, 2014.
- [2] A. Martínez, "El Ministerio del Ambiente y el Agua en Ecuador," 2022. [En línea]. Available: <https://www.iagua.es/blogs/andres-martinez-moscoso/ministerio-ambiente-y-agua-ecuador>. [Último acceso: 14 Enero 2022].
- [3] A. y. T. E. Ministerio del Ambiente, "Misión / Visión / Valores," 2022. [En línea]. Available: <https://www.ambiente.gob.ec/valores-mision-vision/>. [Último acceso: 14 Enero 2022].
- [4] M. d. Ambiente, "Historia de Creación," [En línea]. Available: <https://www.ambiente.gob.ec/wp-content/uploads/downloads/2012/07/Historia-de-Creacion.pdf>. [Último acceso: 14 Enero 2022].
- [5] V. Ponce, "Ministerio del Ambiente,» Quito.
- [6] J. Padilla, "Diseño de redes corporativas," [En línea]. Available: <http://jpadilla.docentes.upbbga.edu.co/Telematica/Diseno%20de%20redes%20Corporativas.pdf>. [Último acceso: 25 Enero 2022].
- [7] D. Pineda, "Dispositivos pasivos de una red de cableado estructurado," [En línea]. Available: <https://es.calameo.com/read/006488598e4de41e475c7>. [Último acceso: 15 Abril 2022].
- [8] J. Muñoz, "Planificación y Administración de Redes," 2017. [En línea]. Available: <https://planificacionadministracionredes.readthedocs.io/es/latest/Tema04/>. [Último acceso: 12 Abril 2022].
- [9] Alcatel Lucent Enterprise, "OmniPCX Enterprise Communication Server," 2022. [En línea]. Available: <https://www.al-enterprise.com/en/products/platforms/omnipcx-enterprise-communication-server>. [Último acceso: 25 Febrero 2022].
- [10] TecnoSeguro, "PoE," [En línea]. Available: <https://www.tecnoseguro.com/faqs/electronica/que-es-poe>. [Último acceso: 18 Febrero 2022].
- [11] Cisco, "Campus-Resumen de diseño," Abril 2014. [En línea]. Available: <https://www.cisco.com › dam › assets › pdfs › en-...> [Último acceso: 2 Febrero 2022].

[12 CCNA, "Diseño Jerárquico de Redes," [En línea]. Available:
] <https://ccnadesdecero.es/disenio-jerarquico-de-redes/>. [Último acceso: 6 Febrero 2022].

[13 Aruba Networks, "¿Qué es la topología de red?," [En línea]. Available:
] <https://www.arubanetworks.com/es/faq/que-es-la-topologia-de-red/>. [Último acceso: 14 Abril 2022].

[14 F. González, "Sistema de Cableado Estructurado," 2013.

]

[15 E. CABLES, "Cable Cat. 5E, Cat 6, Cat 6A y Cat 7," [En línea]. Available:
] <https://www.elandcables.com/es/cables/lan-cat-5e-6-6a-cable>. [Último acceso: 23 Febrero 2022].

[16 S. C. C. I. Development, "Categoría 6A, 4 pares, cable de Lan de cobre de F/UTP que
] protege el cable del establecimiento de una red 1000 pies en caja de tirón," [En línea]. Available: <http://spanish.copperconductorcable.com/sale-9936724-category-6a-4-pair-f-utp-copper-lan-cable-shielding-networking-cable-1000-ft-in-pull-box.html>. [Último acceso: 23 Febrero 2022].

[17 C. C. Systems, "Información Técnica," [En línea]. Available:
] <https://www.corning.com/catalog/coc/documents/white-papers/LAN-1135-SL.pdf>. [Último acceso: 15 Abril 2022].

[18 INCIBE, "Qué es una DMZ y cómo te puede ayudar a proteger tu empresa," 19
] Septiembre 2019. [En línea]. Available: <https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>. [Último acceso: 2 Marzo 2021].

[19 Paessler AG, "PRTG NETWORK MONITOR," 2022. [En línea]. Available:
] <https://www.paessler.com/es/prtg>. [Último acceso: 27 Marzo 2022].

[20 Cisco, "Servicio Cisco SMARTnet,» [En línea]. Available:
] https://www.cisco.com/c/dam/global/es_mx/assets/pdfs/services_at_a_glance_smartnet.pdf. [Último acceso: 28 Febrero 2022].

[21 Huawei, "Enterprise Warranty Policy," [En línea]. Available:
] <https://support.huawei.com/enterprise/en/warranty/ENEWS1000006975>. [Último acceso: 26 Febrero 2022].

[22 Aruba a Hewlett Packard Enterprise , "ARUBA WARRANTY AND SUPPORT
] SUMMARY 22.2," [En línea]. Available:

<https://www.arubanetworks.com/assets/support/warranty-summary.pdf>. [Último acceso: 28 Febrero 2022].

[23 Cisco, “Cisco Packet Tracer,” [En línea]. Available:] <https://www.netacad.com/es/courses/packet-tracer>. [Último acceso: 1 Marzo 2022].

ANEXOS

ANEXO A. PLANOS DE DISTRIBUCIÓN DE PUNTOS EN EL EDIFICIO DEL MINISTERIO DEL AMBIENTE.

ANEXO B. PLANOS DE DISTRIBUCIÓN DE PUNTOS EN EL EDIFICIO DE LA SECRETARÍA DEL AGUA.

ANEXO C. DIAGRAMA UNIFILAR DE LA INTERCONEXIÓN DE LOS EDIFICIOS DEL MINISTERIO DEL AMBIENTE Y AGUA.

ANEXO D. DIAGRAMA UNIFILAR DE LOS EDIFICIOS DEL MINISTERIO DEL AMBIENTE Y AGUA.

ANEXO E. DIAGRAMAS DE RACK EN EL EDIFICIO DE MINISTERIO DEL AMBIENTE.

ANEXO F. DIAGRAMAS DE RACK EN EL EDIFICIO DE LA SECRETARÍA DEL AGUA.

A. ANEXO A: PLANOS DE DISTRIBUCIÓN DE PUNTOS EN EL EDIFICIO DEL MINISTERIO DEL AMBIENTE.

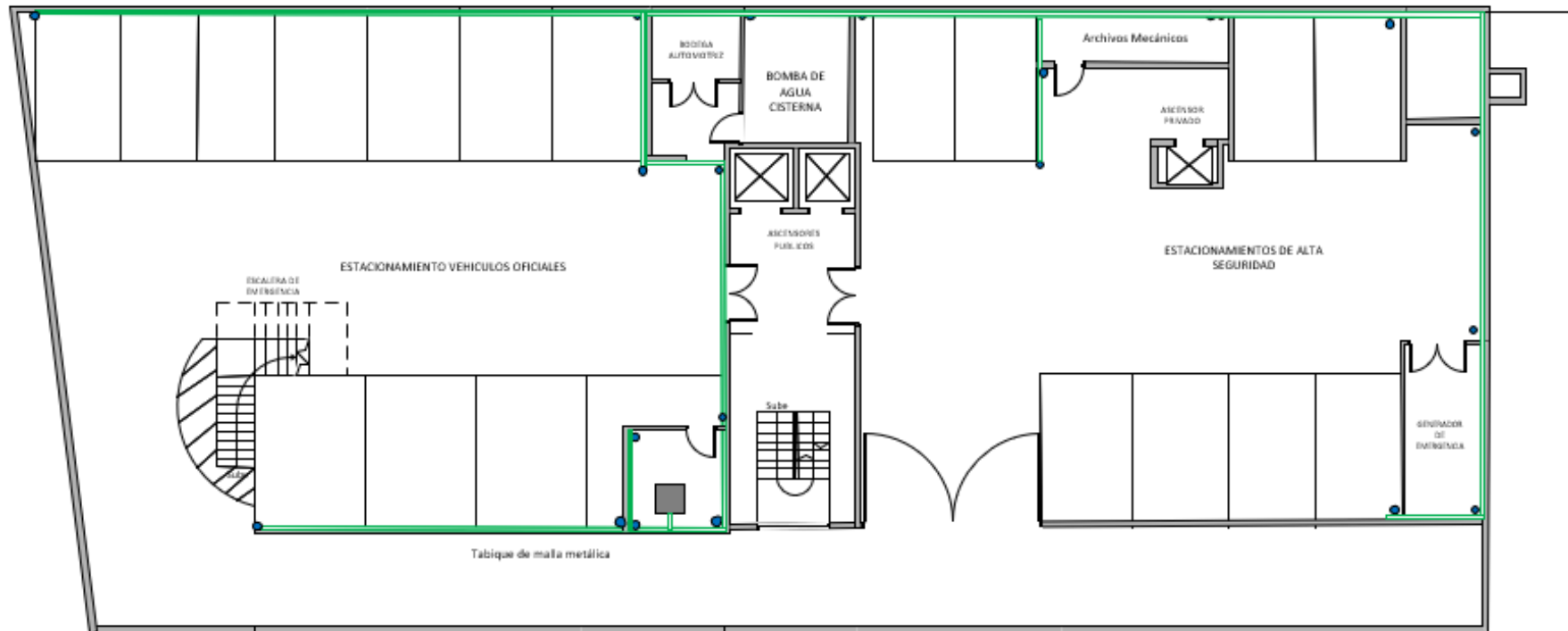


Figura A.1. Plano de distribución de puntos del Subsuelo del Edificio del Ministerio del Ambiente.

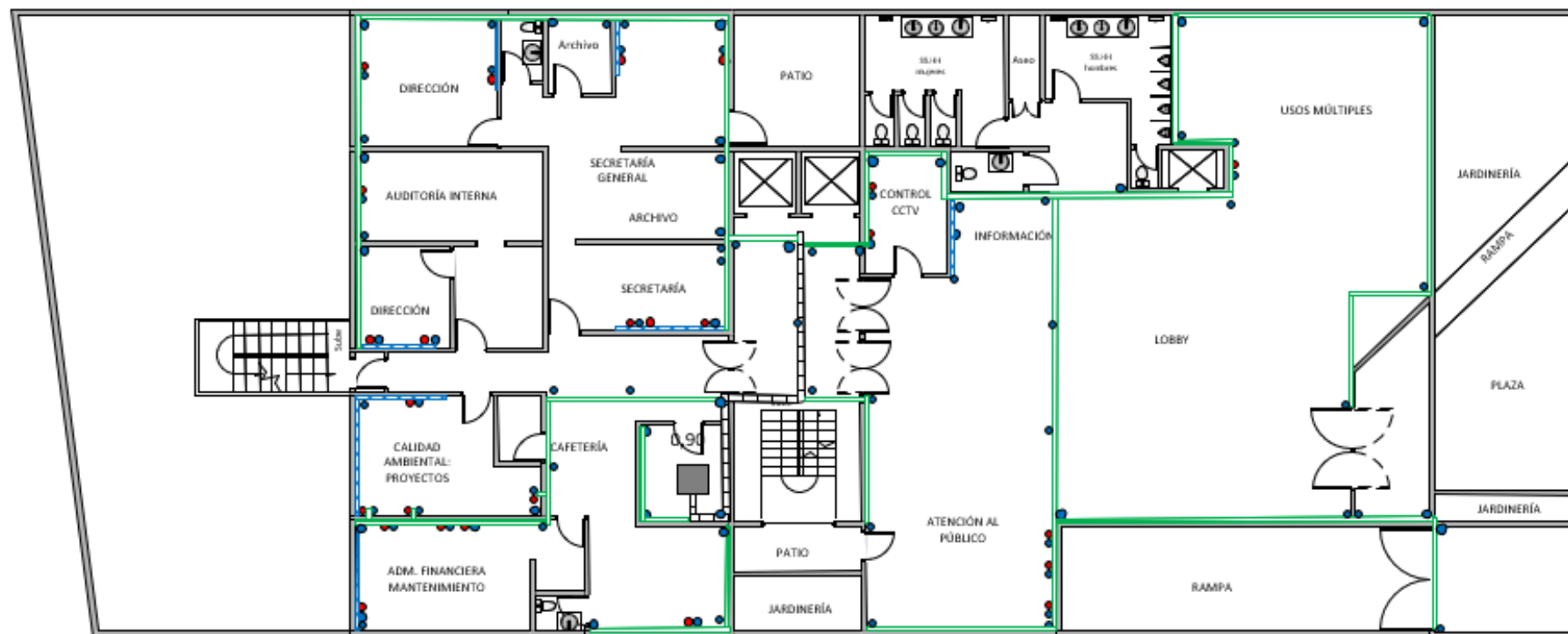


Figura A.2. Plano de distribución de puntos de la Planta Baja del Edificio del Ministerio del Ambiente.

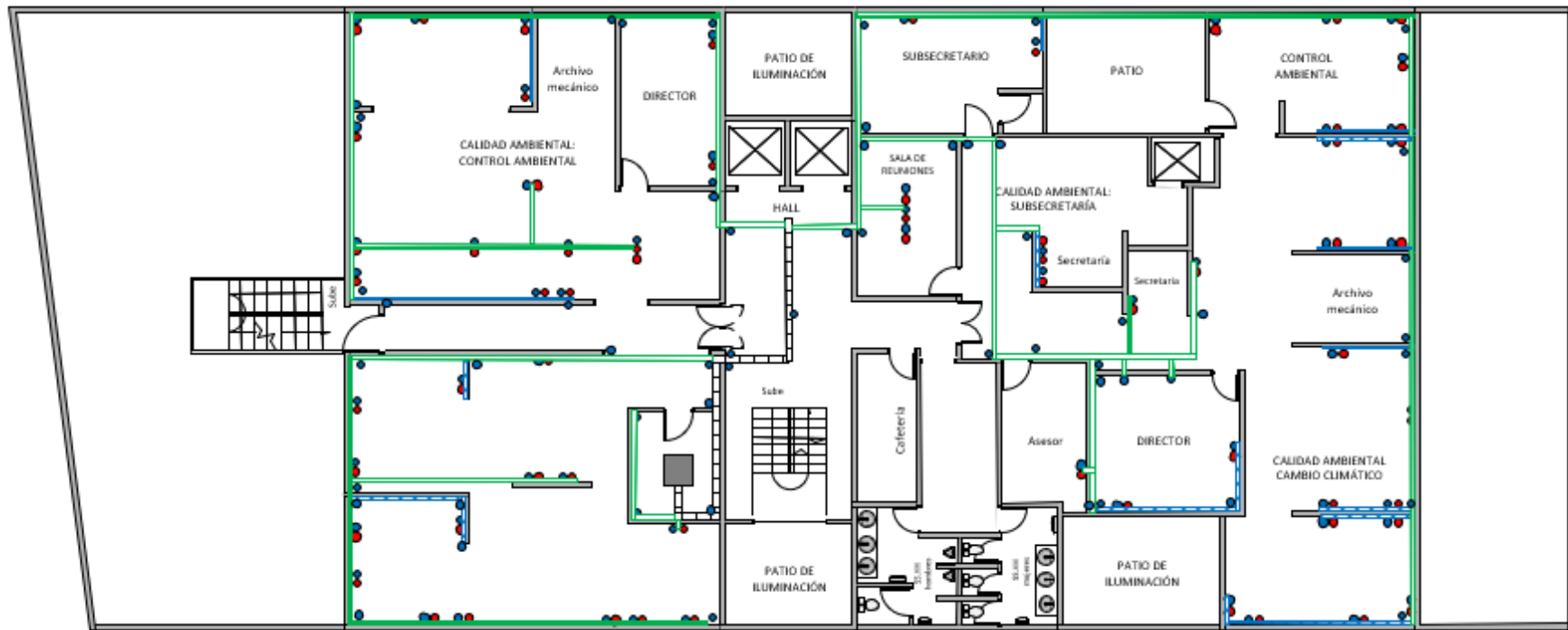


Figura A.3. Plano de distribución de puntos de la primera Planta Alta del Edificio del Ministerio del Ambiente.

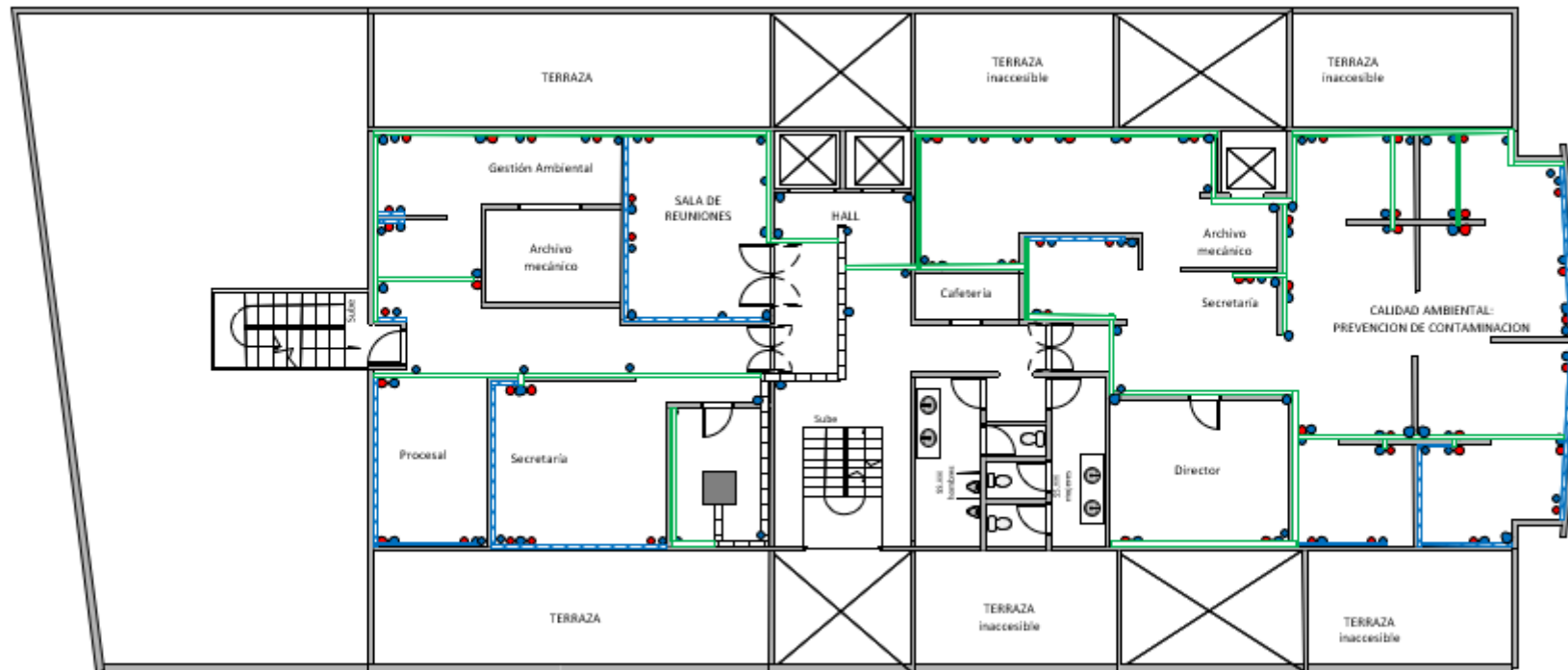


Figura A.4. Plano de distribución de puntos de la segunda Planta Alta del Edificio del Ministerio del Ambiente.

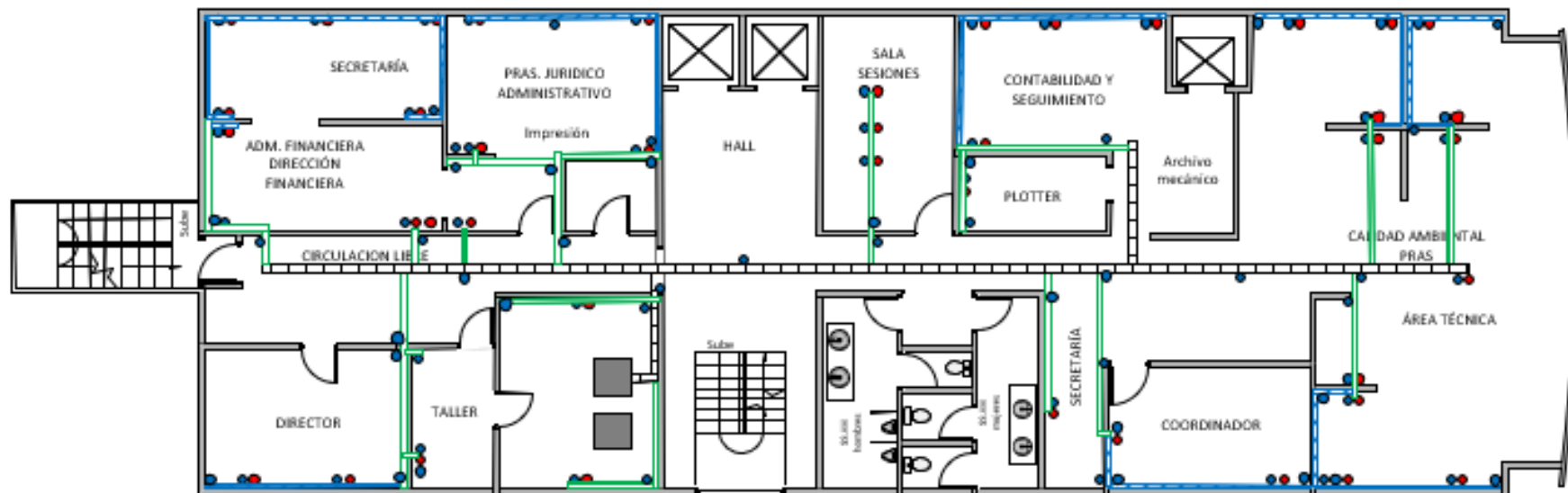


Figura A.5. Plano de distribución de puntos de la tercera Planta Alta del Edificio del Ministerio del Ambiente.

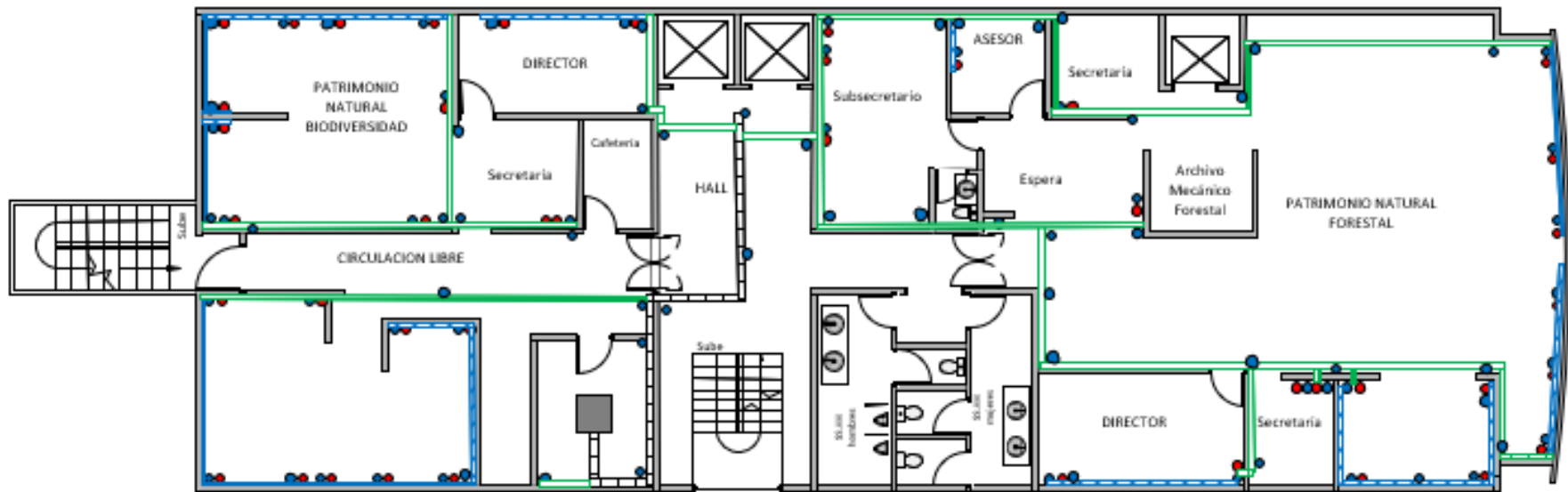


Figura A.6. Plano de distribución de puntos de la cuarta Planta Alta del Edificio del Ministerio del Ambiente.

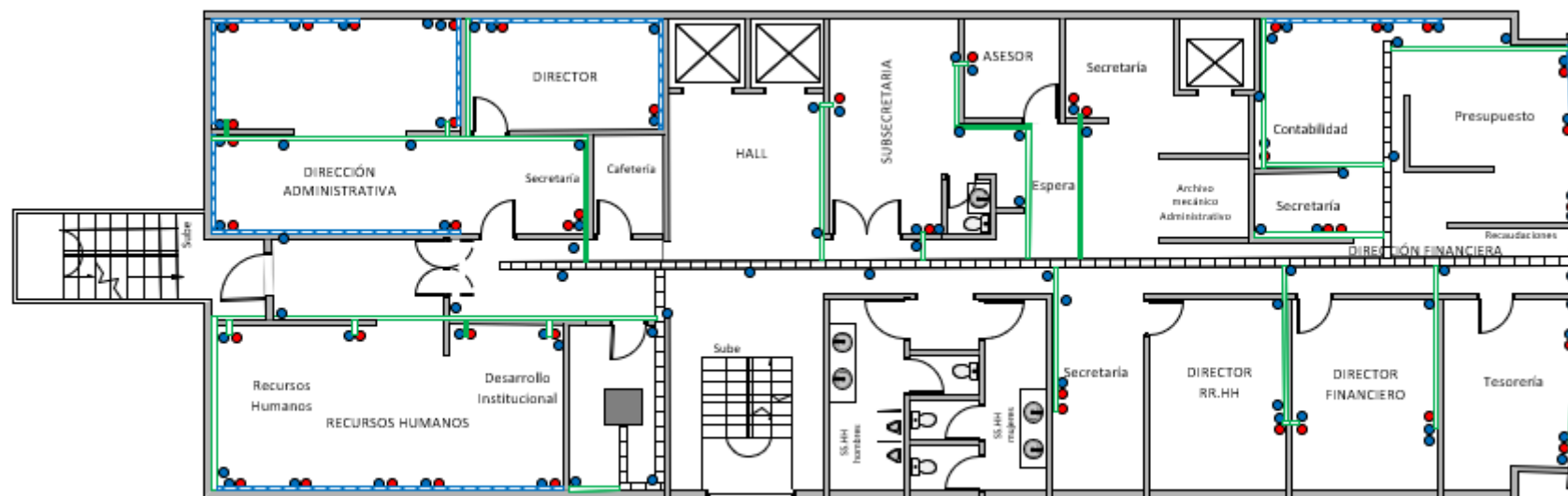


Figura A.7. Plano de distribución de puntos de la quinta Planta Alta del Edificio del Ministerio del Ambiente.

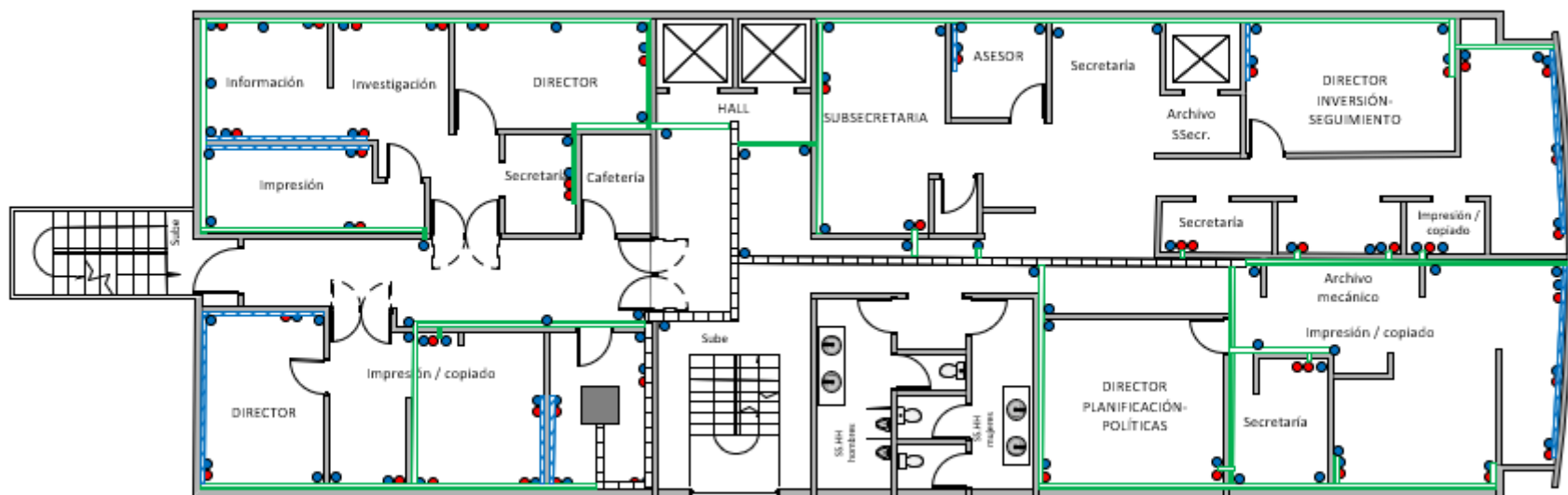


Figura A.8. Plano de distribución de puntos de la sexta Planta Alta del Edificio del Ministerio del Ambiente.

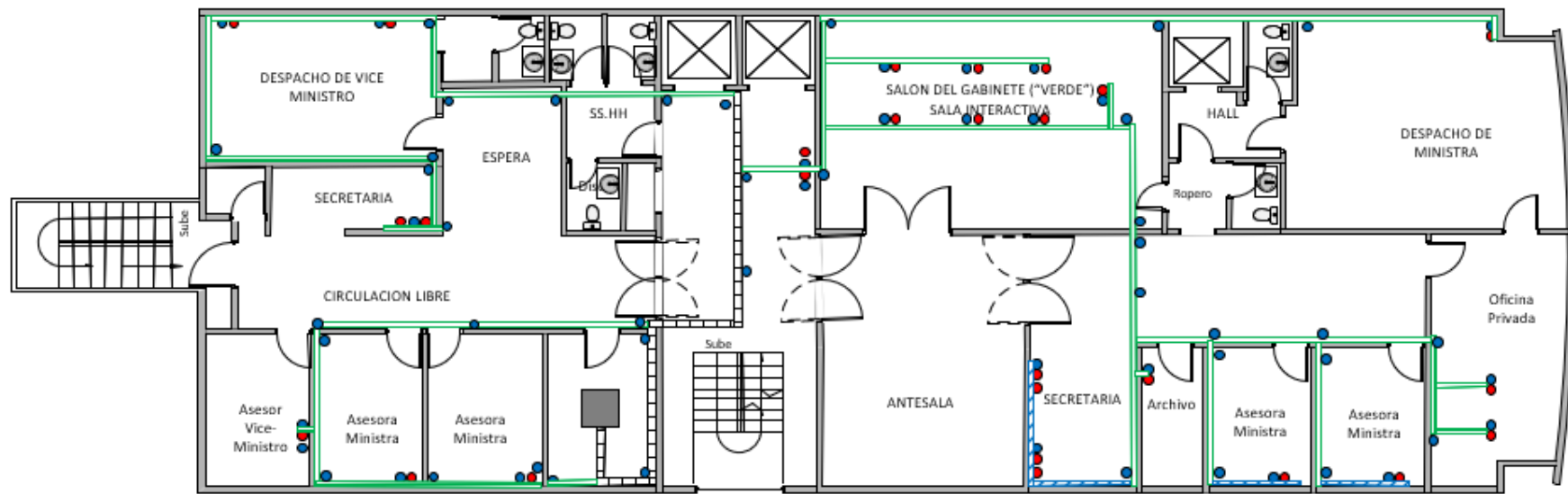


Figura A.9. Plano de distribución de puntos de la séptima Planta Alta del Edificio del Ministerio del Ambiente.

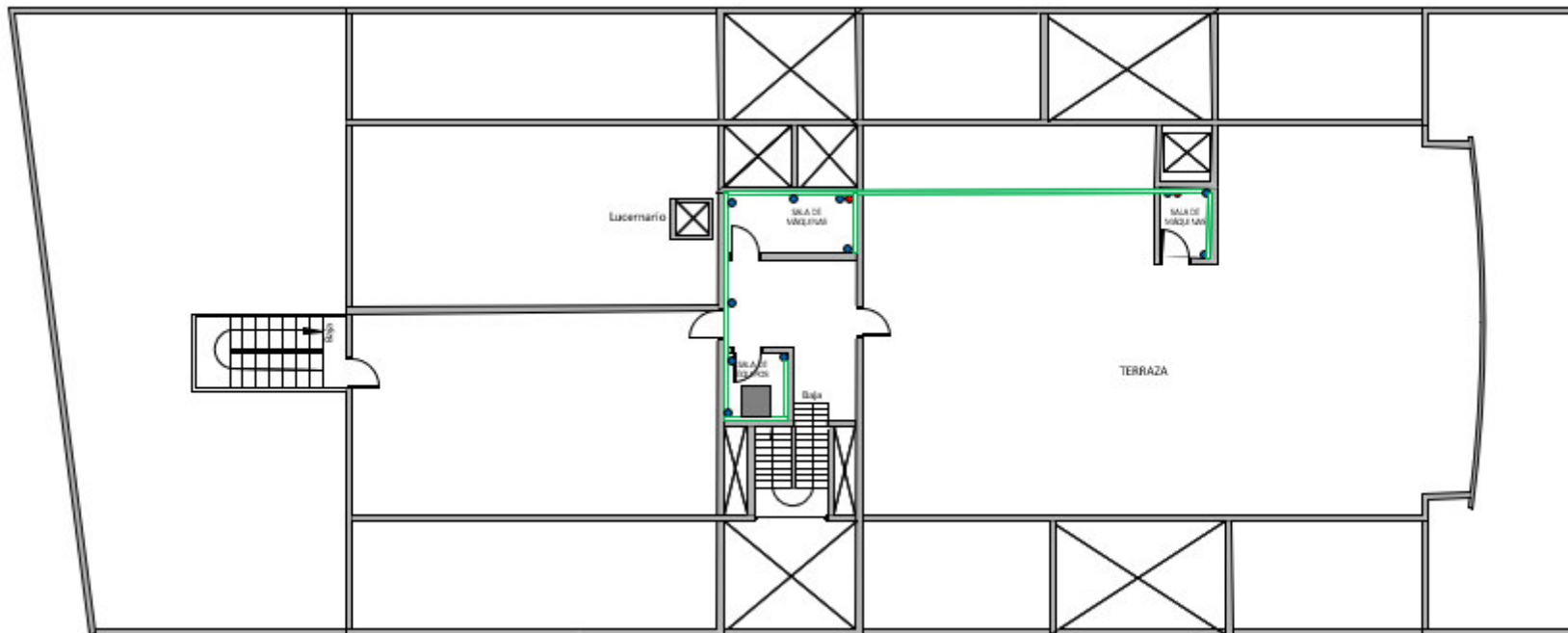


Figura A.10. Plano de distribución de puntos de la Terraza del Edificio del Ministerio del Ambiente.

B. ANEXO B: PLANOS DE DISTRIBUCIÓN DE PUNTOS EN EL EDIFICIO DE LA SECRETARÍA DEL AGUA.

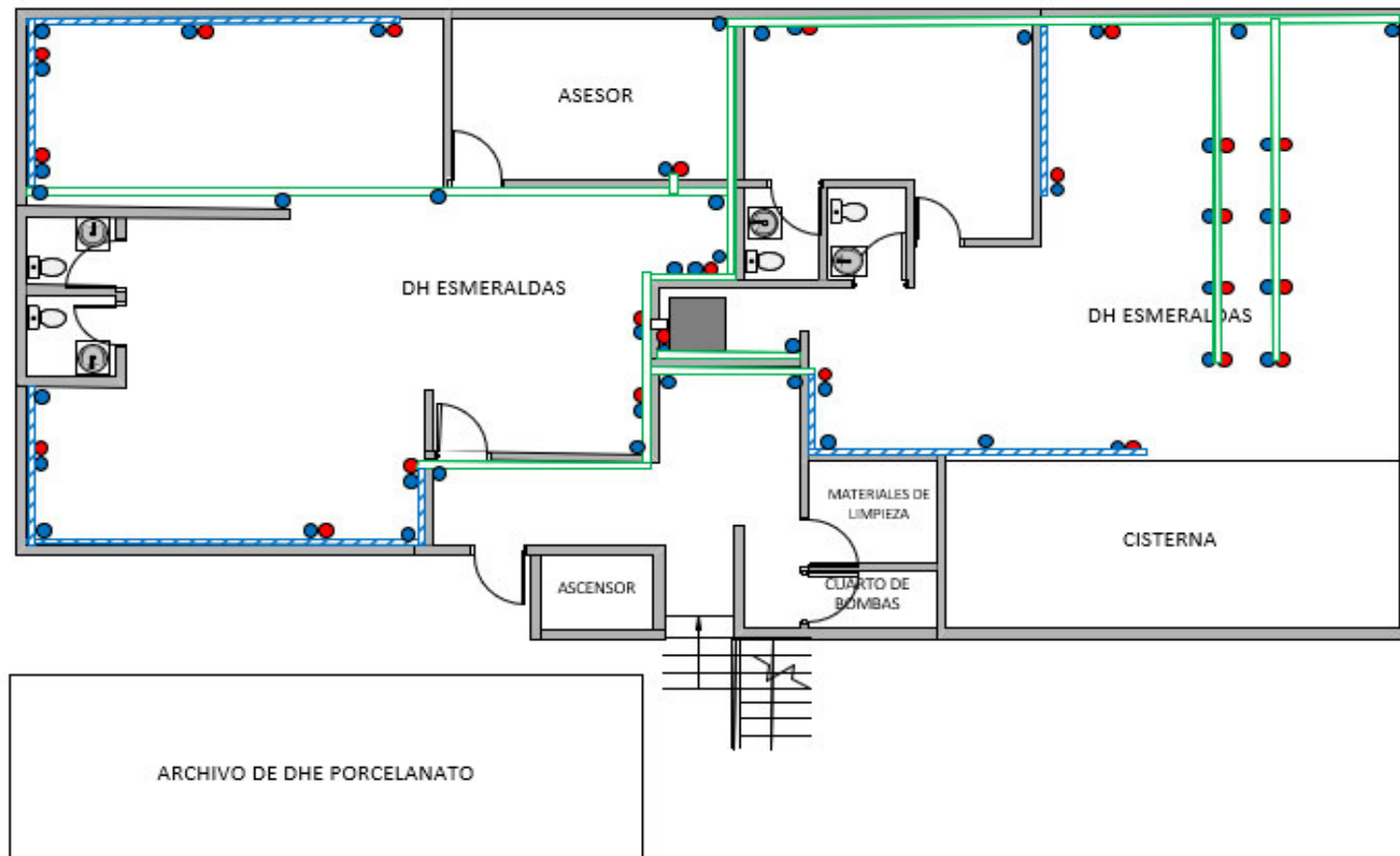


Figura B.1. Plano de distribución de puntos del Subsuelo del Edificio de la Secretaría del Agua.

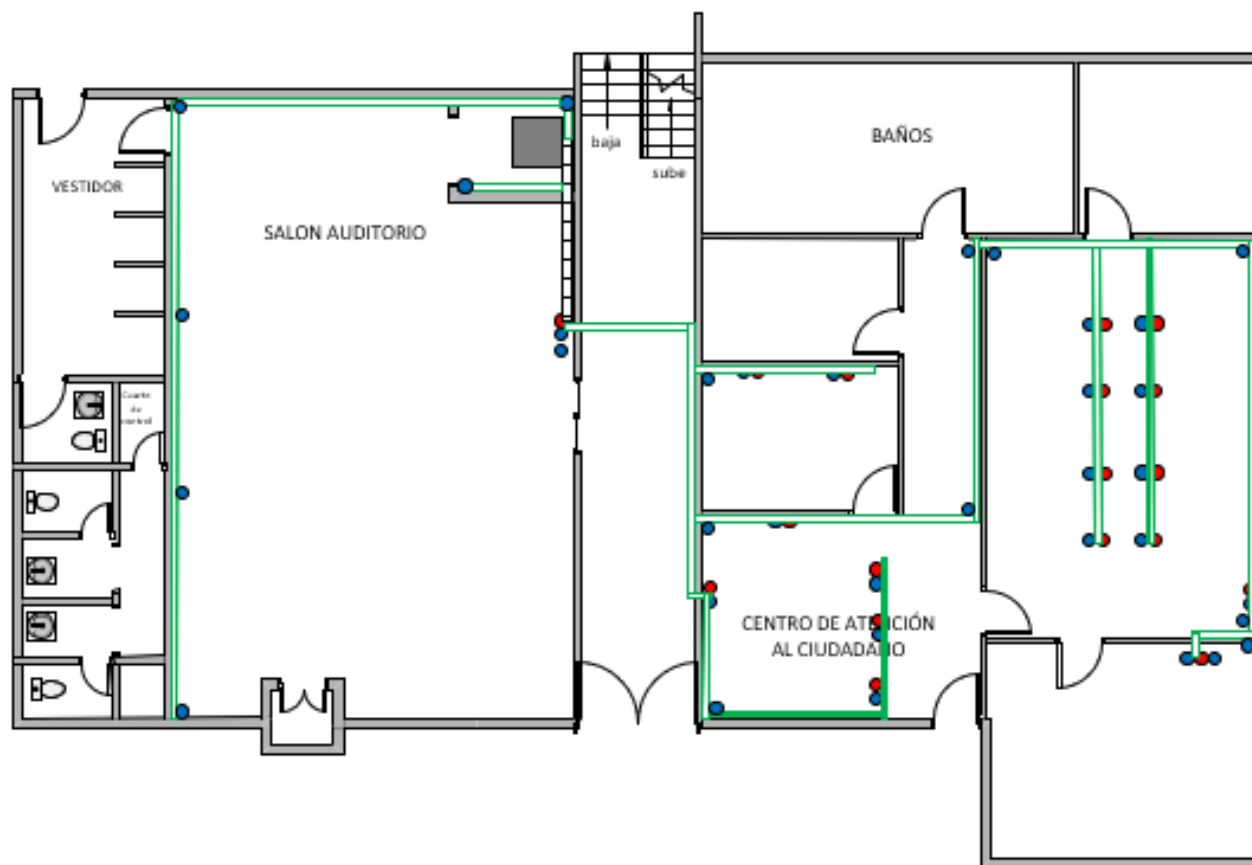


Figura B.2. Plano de distribución de puntos de la Planta Baja del Edificio de la Secretaría del Agua.

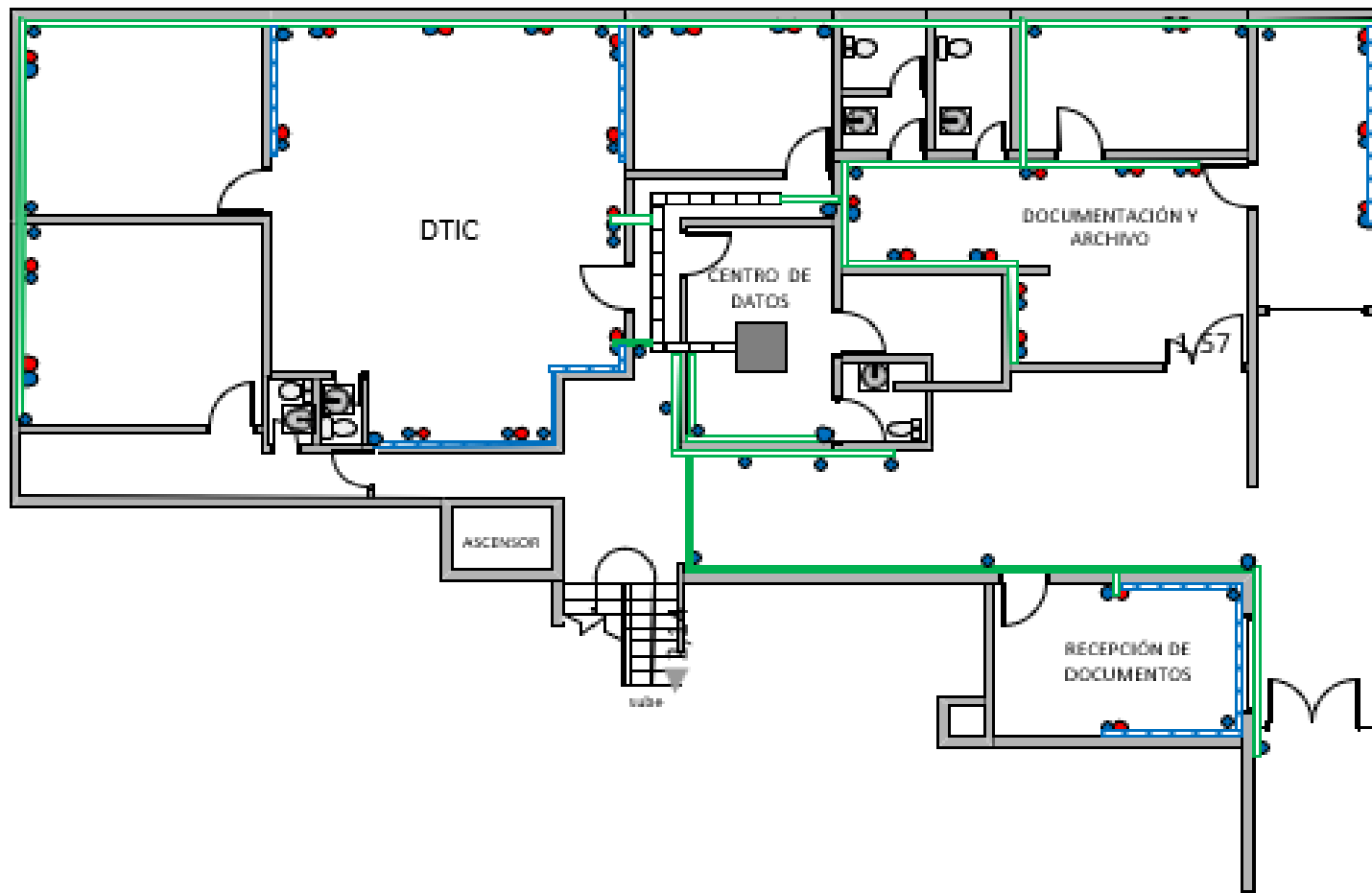


Figura B.3. Plano de distribución de puntos de la primera Planta Baja del Edificio de la Secretaría del Agua.

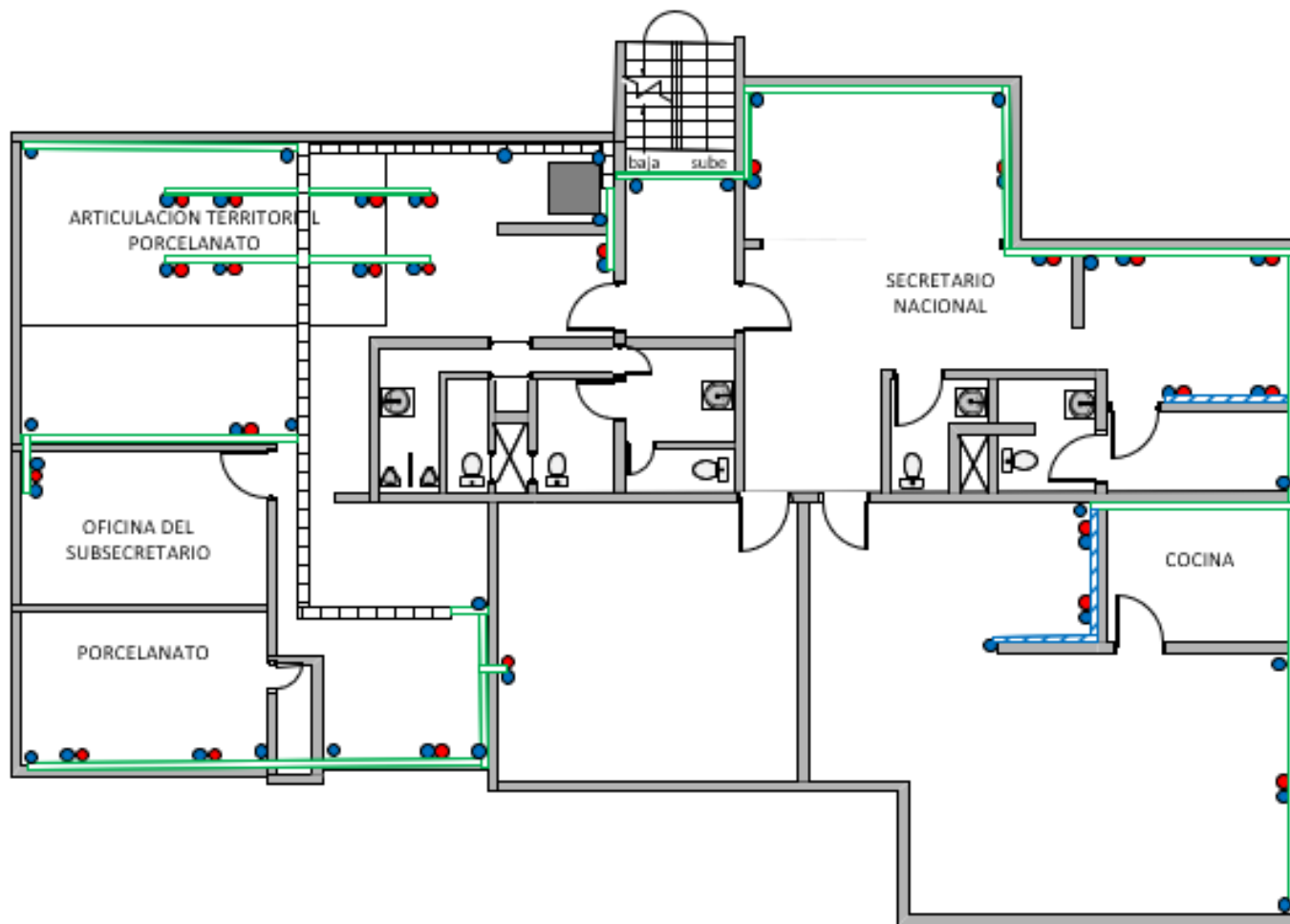


Figura B.4. Plano de distribución de puntos de la primera Planta Alta del Edificio de la Secretaría del Agua.

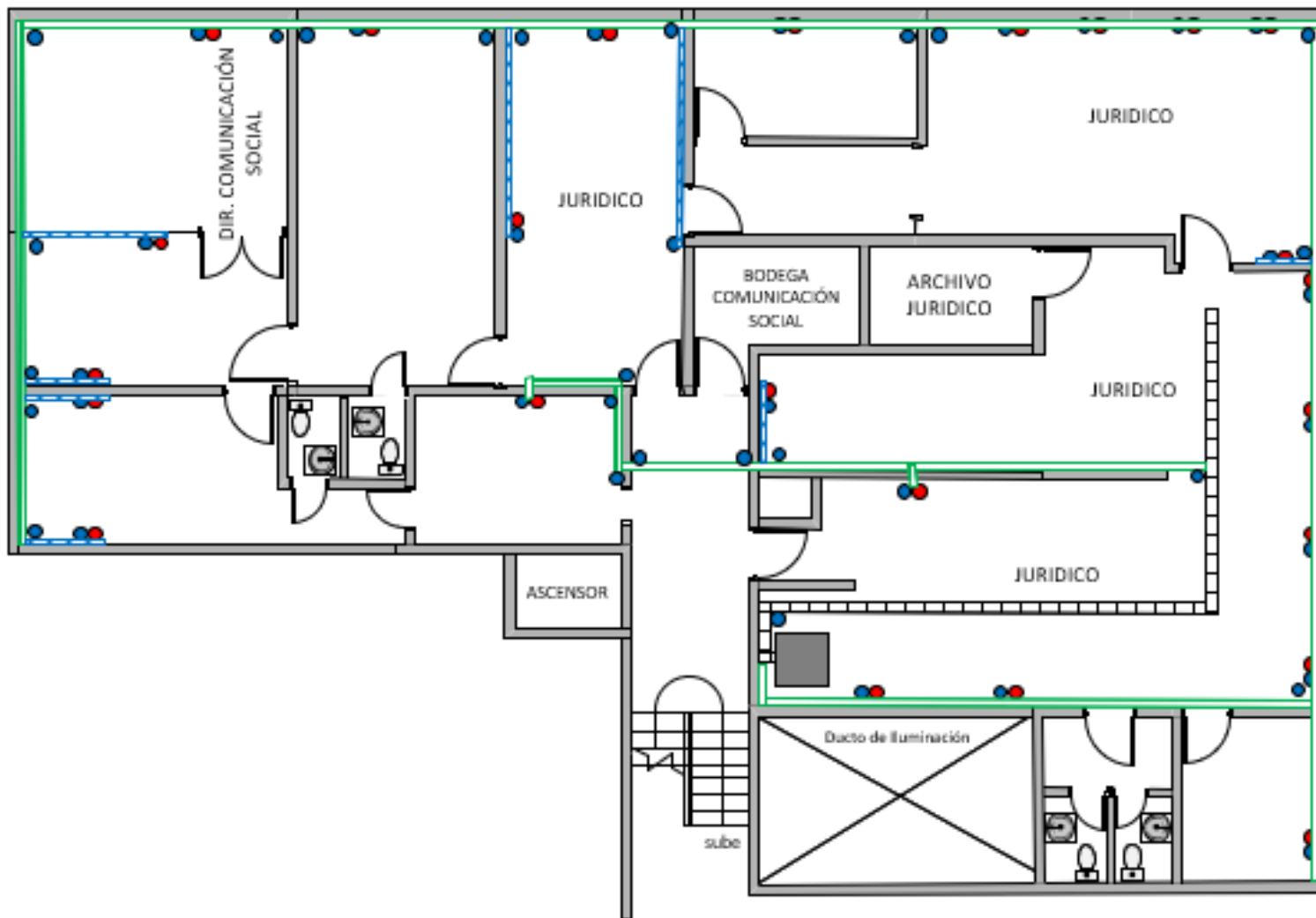


Figura B.5. Plano de distribución de puntos de la segunda Planta Baja del Edificio de la Secretaría del Agua.

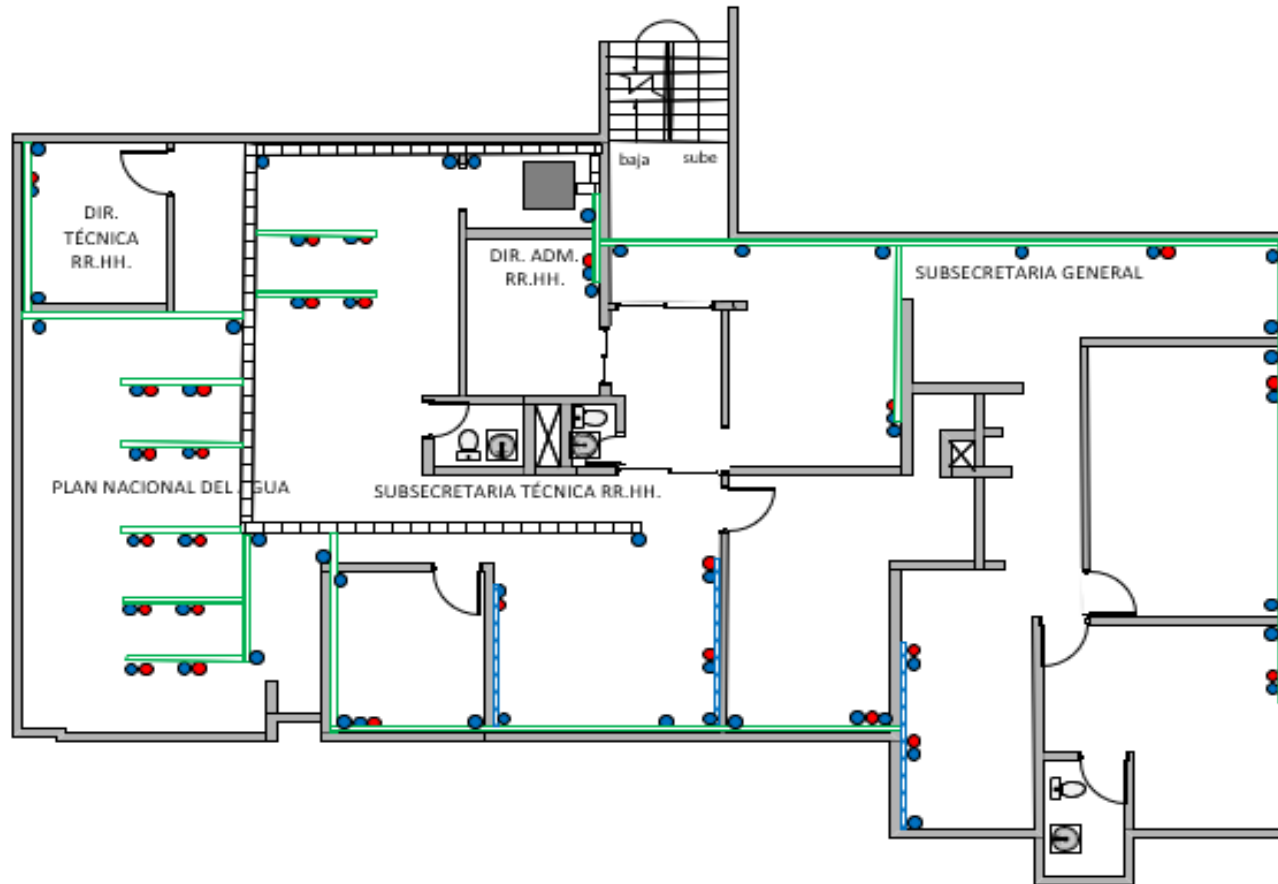


Figura B.6. Plano de distribución de puntos de la segunda Planta Alta del Edificio de la Secretaría del Agua.

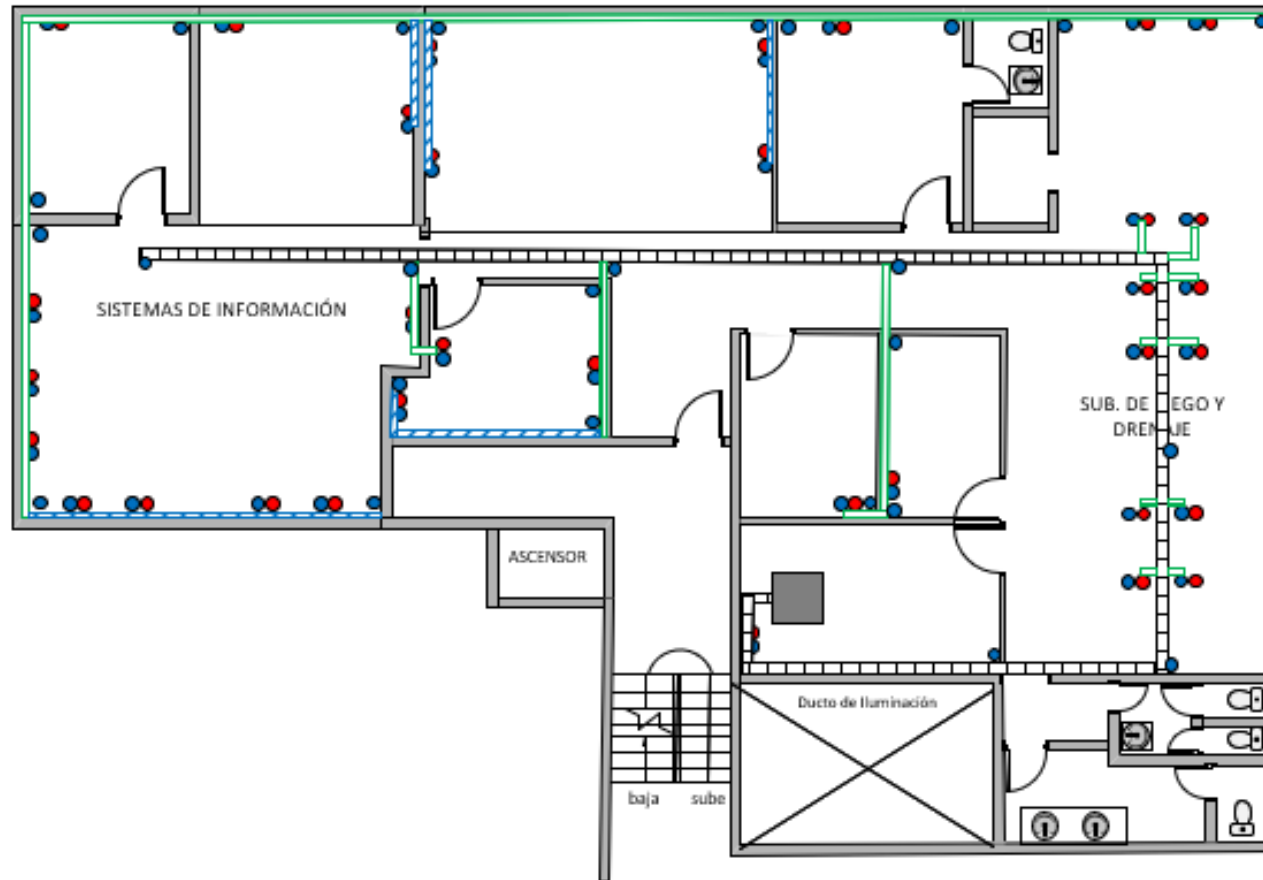


Figura B.7. Plano de distribución de puntos de la tercera Planta Baja del Edificio de la Secretaría del Agua.

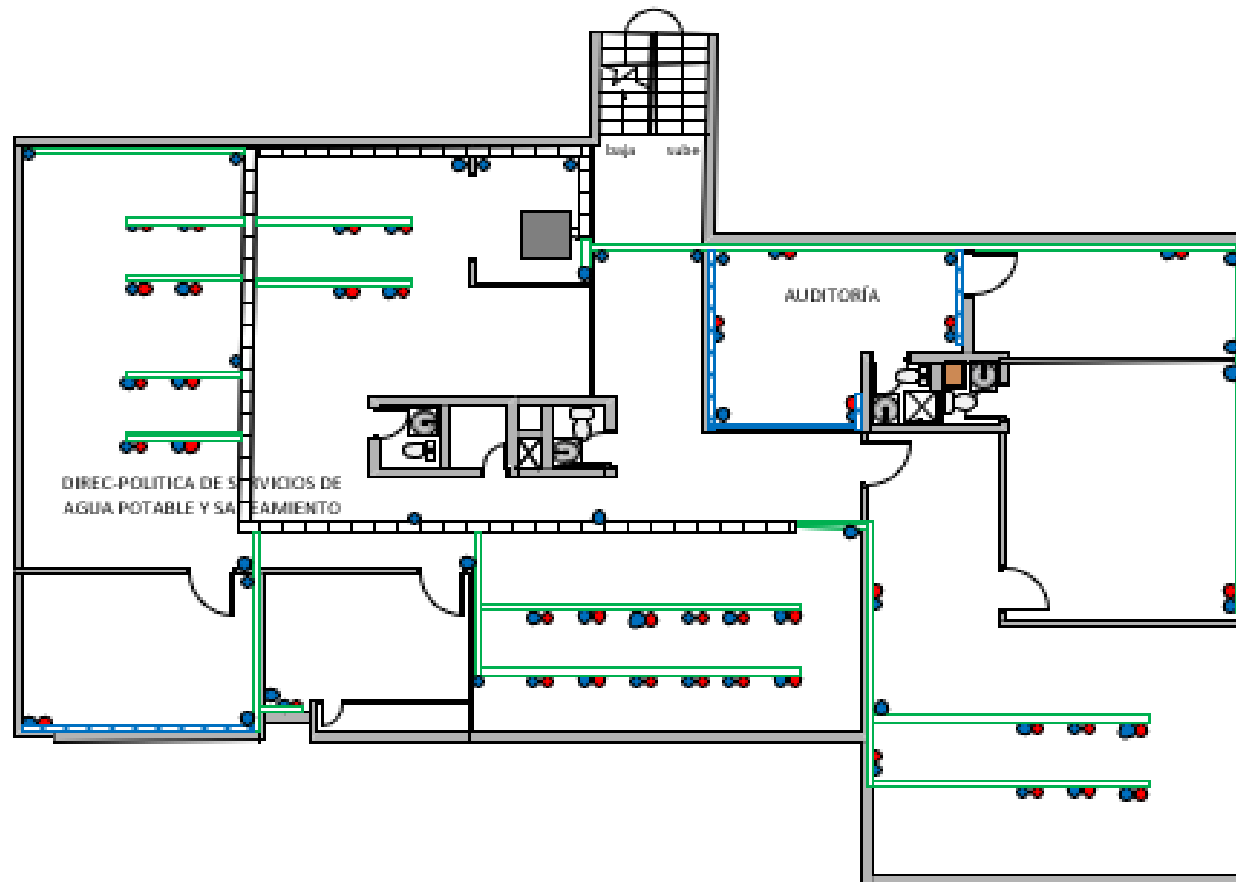


Figura B.8. Plano de distribución de puntos de la tercera Planta Alta del Edificio de la Secretaría del Agua.

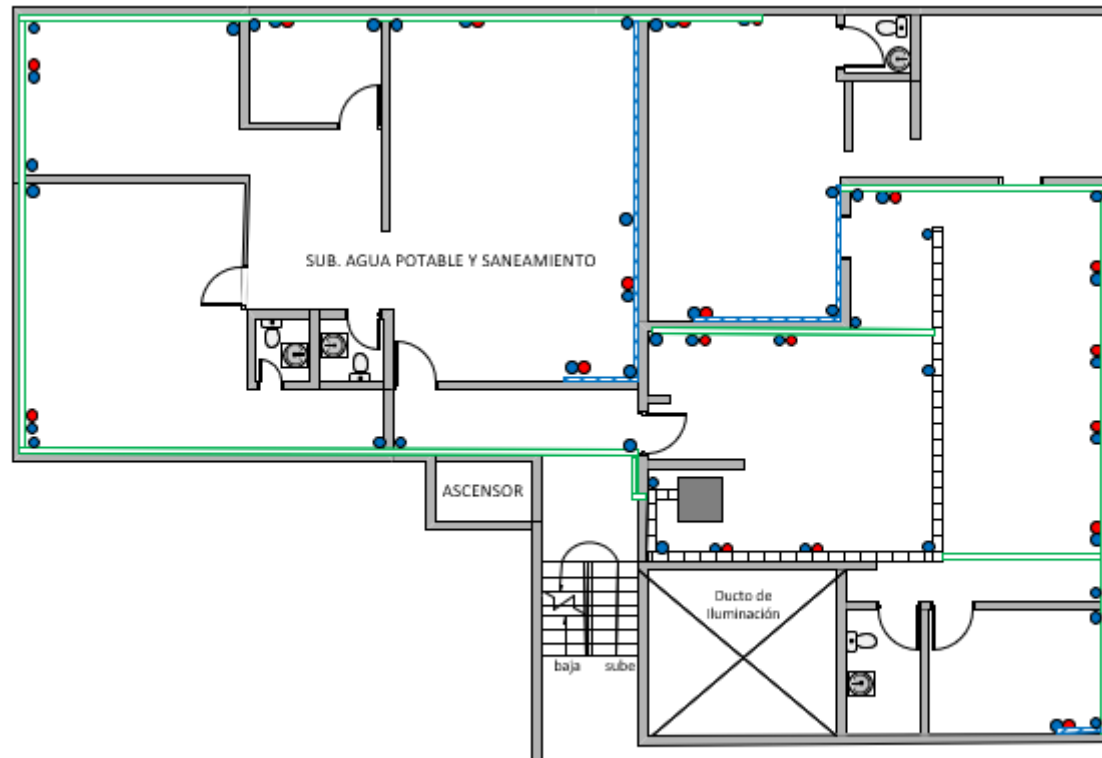


Figura B.9. Plano de distribución de puntos de la cuarta Planta Baja del Edificio de la Secretaría del Agua.

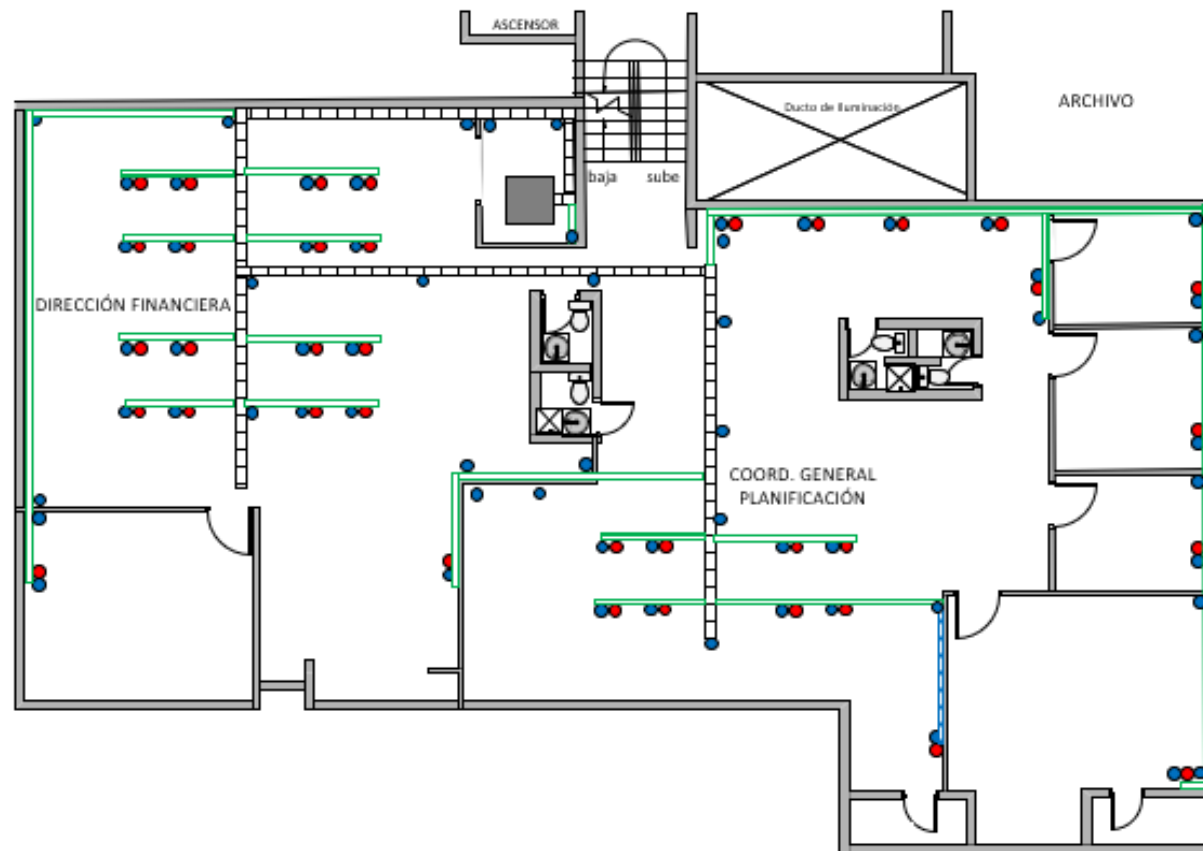


Figura B.10. Plano de distribución de puntos de la cuarta Planta Alta del Edificio de la Secretaría del Agua.

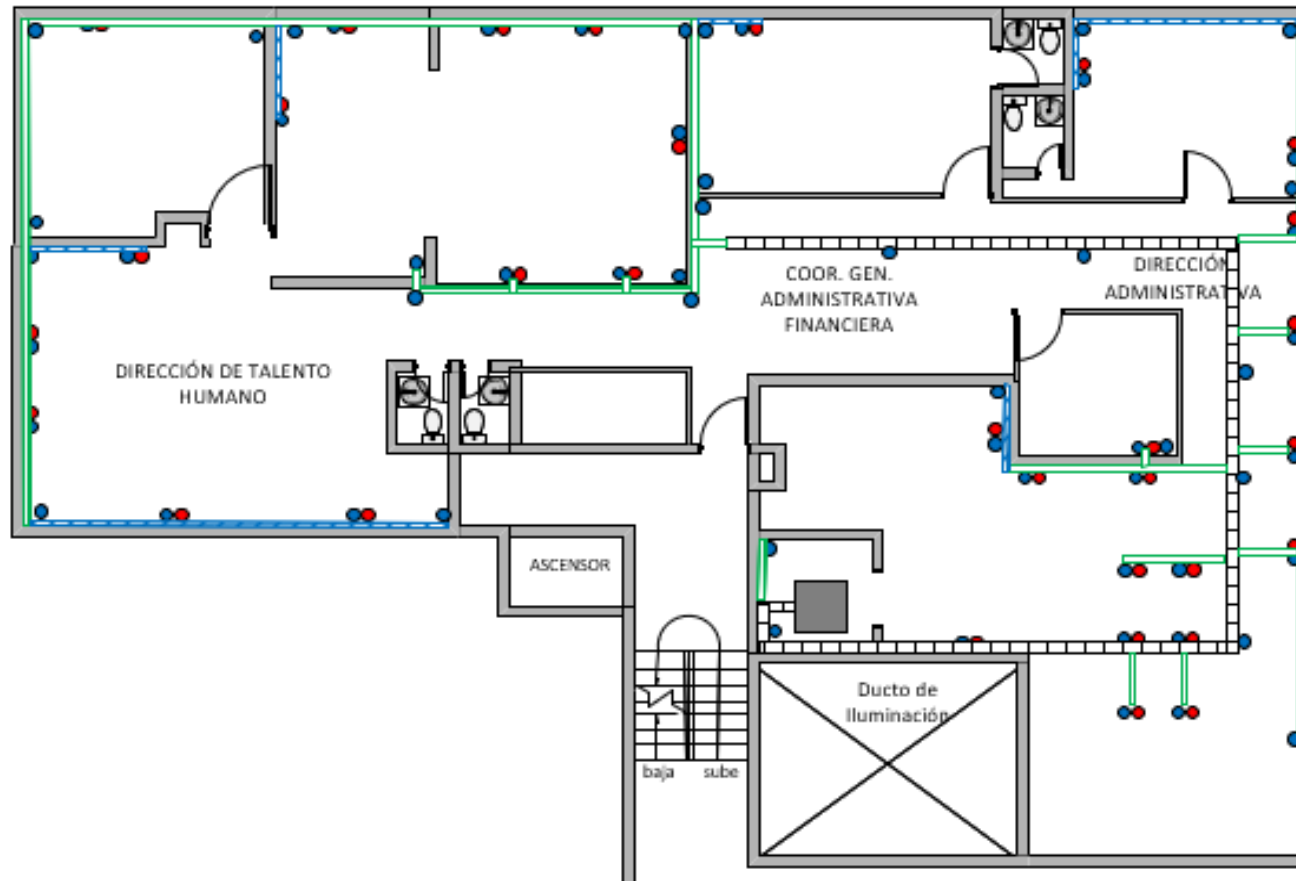


Figura B.11. Plano de distribución de puntos de la quinta Planta Baja del Edificio de la Secretaría del Agua.

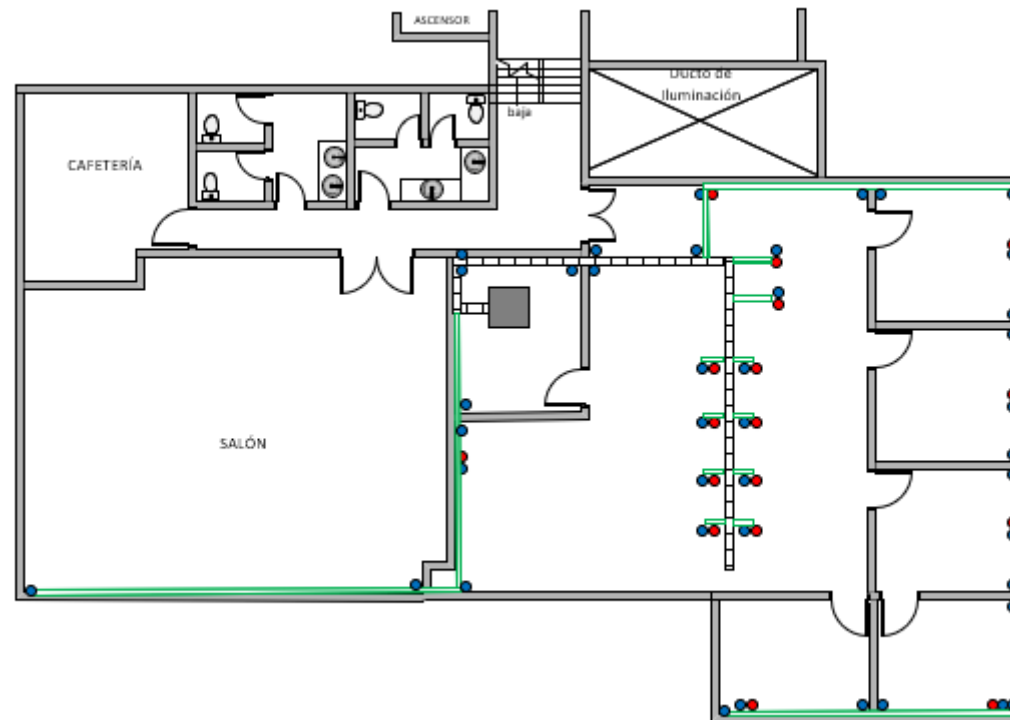


Figura B.12. Plano de distribución de puntos de la quinta Planta Alta del Edificio de la Secretaría del Agua.

C. ANEXO C: DIAGRAMA UNIFILAR DE LA INTERCONEXIÓN DE LOS EDIFICIOS DEL MINISTERIO DEL AMBIENTE Y AGUA.

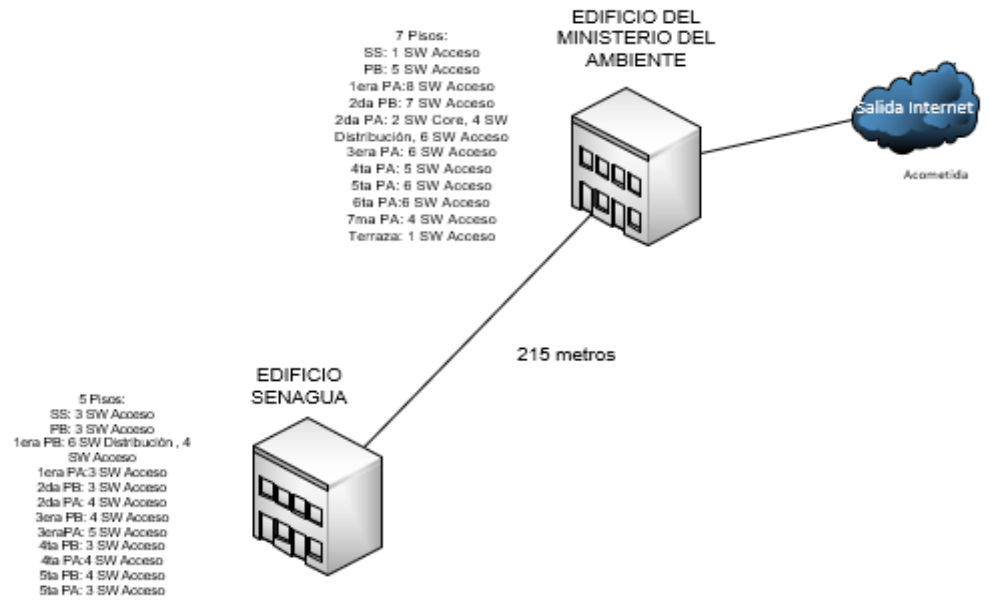


Figura C.1. Diagrama unifilar de la interconexión de los edificios del Ministerio del Ambiente y Agua.

D. ANEXO D: DIAGRAMA UNIFILAR DE LOS EDIFICIOS DEL MINISTERIO DEL AMBIENTE Y AGUA.

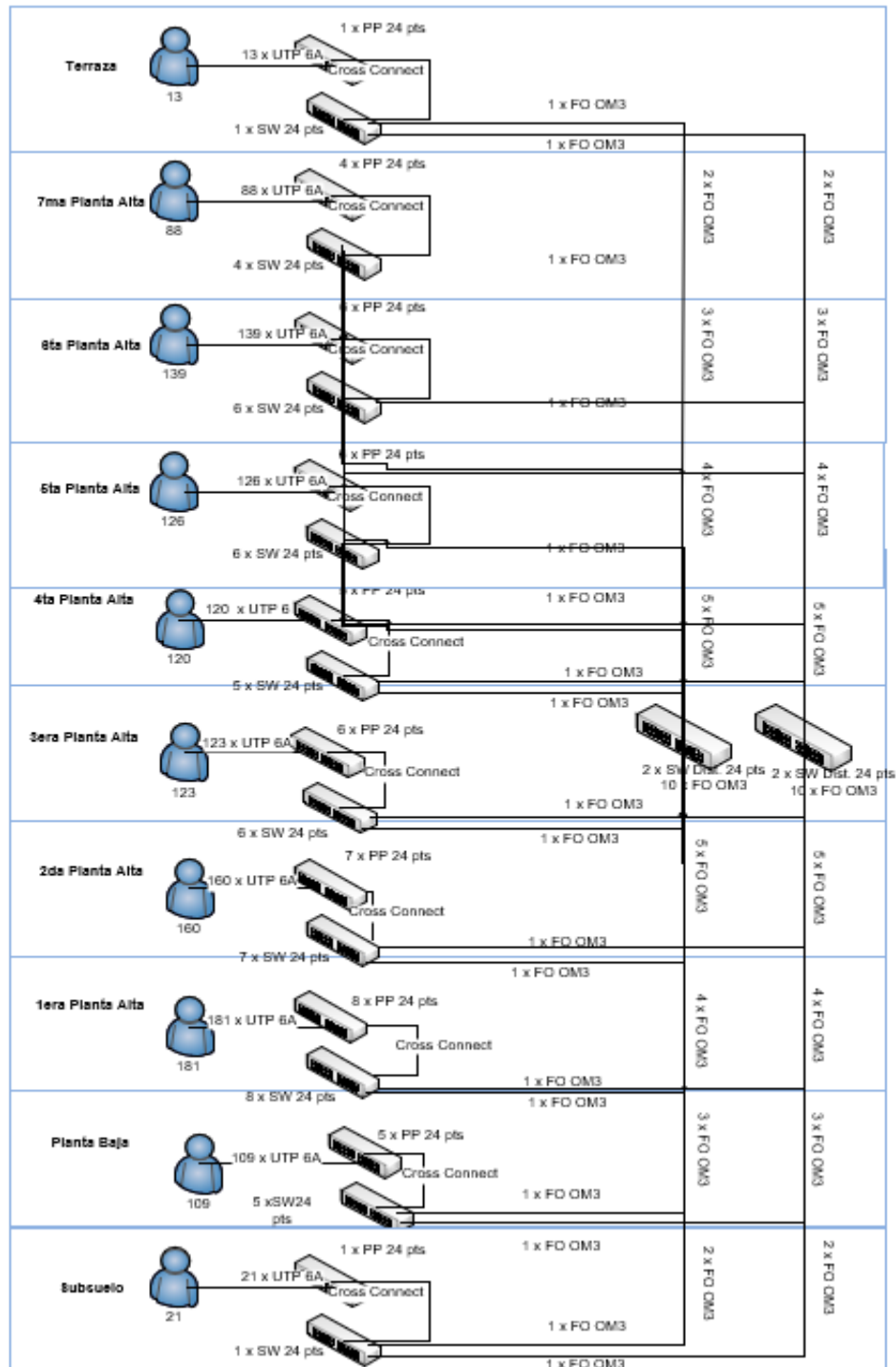


Figura D.1. Diagrama unifilar del edificio del Ministerio del Ambiente.

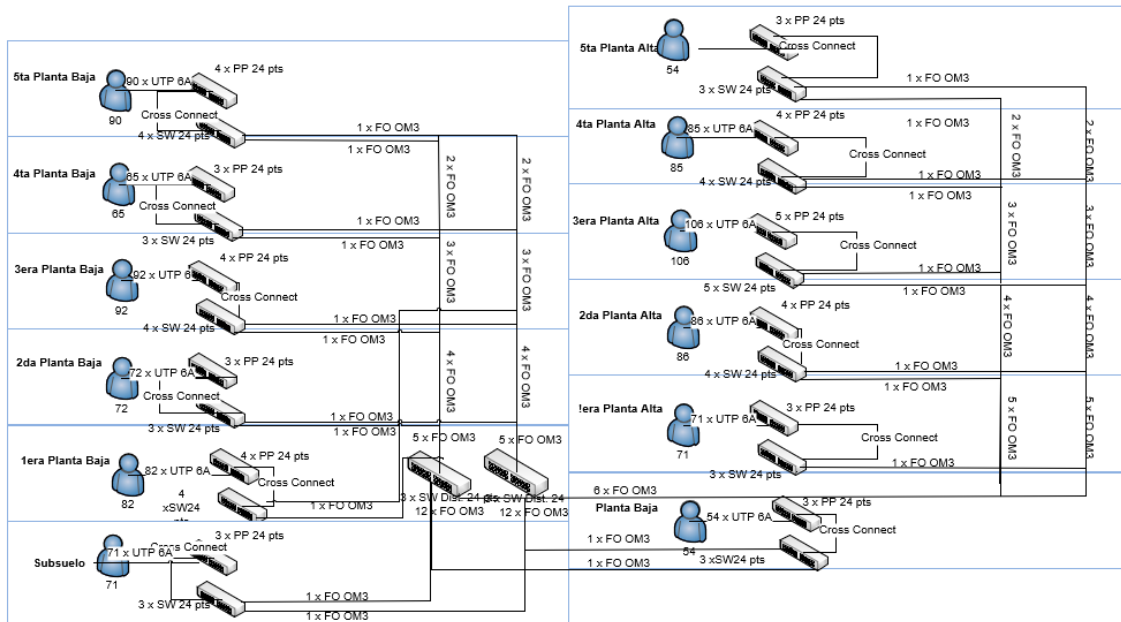


Figura D.2. Diagrama unifilar del edificio de la Secretaría del Agua.

E. ANEXO E: DIAGRAMAS DE RACK EN EL EDIFICIO DEL MINISTERIO DEL AMBIENTE.

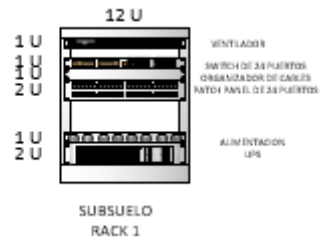


Figura E.1. Diagrama del rack 1 en el edificio del Ministerio del Ambiente.

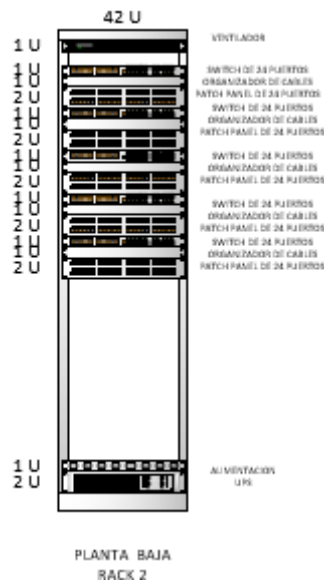


Figura E.2. Diagrama del rack 2 en el edificio del Ministerio del Ambiente.

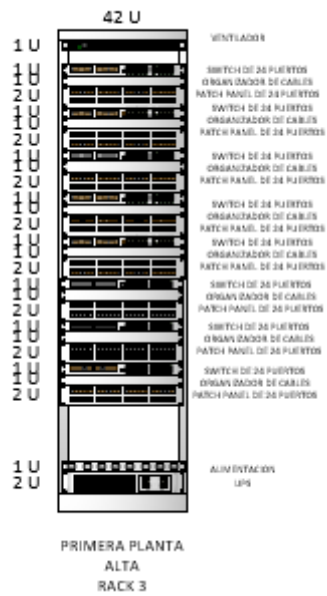


Figura E.3. Diagrama del rack 3 en el edificio del Ministerio del Ambiente.

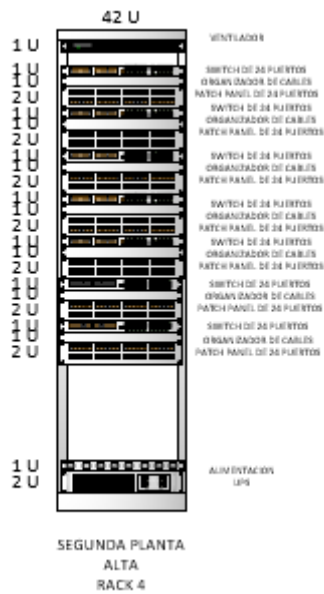


Figura E.4. Diagrama del rack 4 en el edificio del Ministerio del Ambiente.



Figura E.9. Diagrama del rack 9 en el edificio del Ministerio del Ambiente.

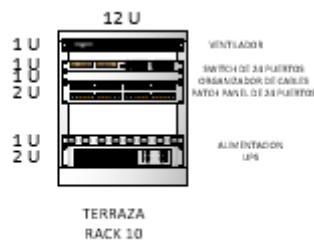


Figura E.10. Diagrama del rack 10 en el edificio del Ministerio del Ambiente.

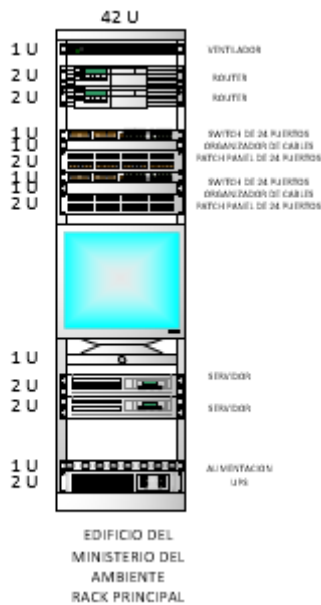


Figura E.11. Diagrama del rack principal en el edificio del Ministerio del Ambiente.

F. ANEXO F: DIAGRAMAS DE RACK EN EL EDIFICIO DE LA SECRETARÍA DEL AGUA.

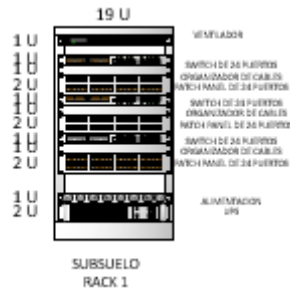


Figura F.1. Diagrama del rack 1 en el edificio de la Secretaría del Agua.

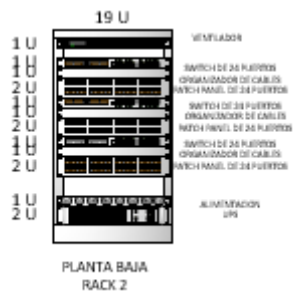


Figura F.2. Diagrama del rack 2 en el edificio de la Secretaría del Agua.

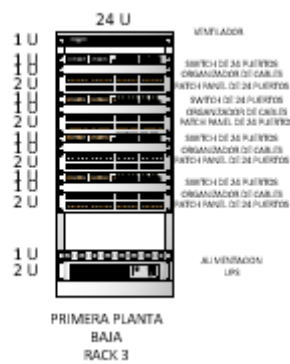


Figura F.3. Diagrama del rack 3 en el edificio de la Secretaría del Agua.

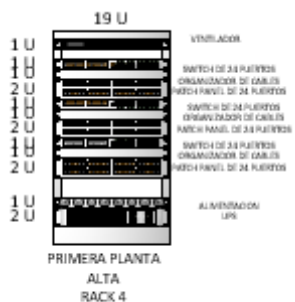


Figura F.4. Diagrama del rack 4 en el edificio de la Secretaría del Agua.



Figura F.5. Diagrama del rack 5 en el edificio de la Secretaría del Agua.



Figura F.6. Diagrama del rack 6 en el edificio de la Secretaría del Agua.

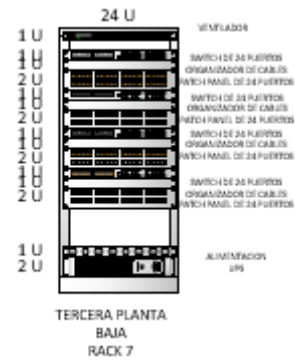


Figura F.7. Diagrama del rack 7 en el edificio de la Secretaría del Agua.

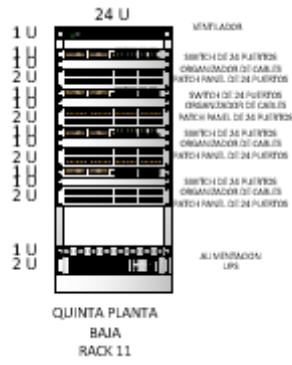


Figura F.11. Diagrama del rack 11 en el edificio de la Secretaría del Agua.

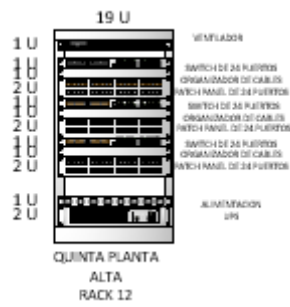


Figura F.12. Diagrama del rack 12 en el edificio de la Secretaría del Agua.

ORDEN DE EMPASTADO