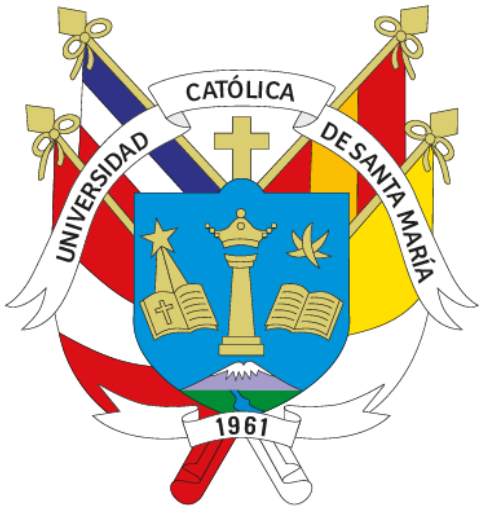
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

FACULTAD DE CIENCIAS FÍSICAS Y FORMALES

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



ANÁLISIS DE INFRAESTRUCTURA DE RED AUTODEMA - PROYECTO ESPECIAL MAJES-SIGUAS

AUTORES

Cusirramos Chiri, Santiago Jesús (2023601381)
Huamani Chuquimamani, Fabian Genaro (2023243831)
Rodríguez López, Elizabeth Camila (2023802962)
Yato Marroquin, Joaquín Mateo (2023405091)

Docente:
Karina Rosas Paredes

Curso:
Computación en Red II

AREQUIPA-PERÚ
2025

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. RESUMEN

Este documento presenta un análisis integral de la infraestructura de red de AUTODEMA (Autoridad Autónoma de Majes), entidad responsable del Proyecto Especial Majes-Siguas en Arequipa, Perú. El estudio evalúa la implementación del modelo OSI en la infraestructura, el cumplimiento de estándares de cableado estructurado y protocolos de enrutamiento.

Hallazgos Principales:

- Arquitectura modular funcional con 7 módulos interconectados mediante fibra óptica multimodo conforme a IEEE 802.3z
- Centro de datos operativo con servidores críticos implementando stack TCP/IP completo
- Conectividad robusta con enlaces dedicados de 200 Mbps y respaldo de 1 Gbps

Problemas Críticos Identificados:

- Ausencia total de segmentación VLAN (Capa 2 OSI) comprometiendo dominios de broadcast
- Gestión mediante protocolos de capa de aplicación inseguros (Telnet/HTTP)
- Incumplimiento del Código Eléctrico Nacional del Perú en sistemas de puesta a tierra
- Configuración híbrida de enrutamiento: estático para interconexión de redes, DHCP para asignación dinámica
- Infraestructura de cableado estructurado con desviaciones de estándar TIA/EIA-568

Impacto Operacional:
La infraestructura actual presenta riesgos significativos en las capas de red y aplicación del modelo OSI, comprometiendo la continuidad operativa de los servicios que sustentan la gestión de recursos hídricos para aproximadamente 50,000 habitantes beneficiarios del proyecto.

2. ABSTRACT

This document presents a comprehensive analysis of the network infrastructure of AUTODEMA (Autonomous Authority of Majes), the entity responsible for the Majes-Siguas Special Project in Arequipa, Peru. The study evaluates the implementation of the OSI model, compliance with structured cabling standards, and routing protocols. Key findings include a functional modular architecture with seven interconnected modules using multimode fiber optics (IEEE 802.3z), an operational data center with critical servers, and robust connectivity with dedicated 200 Mbps links and 1 Gbps backup. Critical issues identified include the absence of VLAN segmentation, insecure management protocols (Telnet/HTTP), and deviations from TIA/EIA-568 cabling standards. The proposed improvements focus on enhancing security, redundancy, and performance through VLAN implementation, encrypted protocols, and infrastructure upgrades.

3. PALABRAS CLAVE

ISO 27001, CIS Controls, VLAN segmentation, network security, structured cabling, OSI model, routing protocols, infrastructure optimization.

4. INTRODUCCION

La infraestructura de red constituye el pilar fundamental de las operaciones tecnológicas en organizaciones modernas. En el caso de AUTODEMA, la correcta gestión de recursos hídricos depende directamente de la eficiencia, estabilidad y seguridad de su red. La necesidad de garantizar la continuidad operativa y prevenir riesgos asociados a fallos de conectividad o seguridad impulsa el presente estudio.

4.1 Contexto y Justificación

AUTODEMA gestiona un sistema de información distribuido en siete módulos interconectados. Su correcta operación permite planificar, controlar y supervisar obras hídricas, así como coordinar esfuerzos interinstitucionales. El crecimiento de amenazas informáticas y la evolución de los requisitos normativos justifican un diagnóstico integral de su red.

4.2 Problemática Identificada

Durante el relevamiento se identificaron vulnerabilidades lógicas y físicas: falta de segmentación VLAN, uso de protocolos inseguros, deterioro del cableado estructurado, ausencia de redundancia, deficiencias en la puesta a tierra y una documentación técnica incompleta.

5. OBJETIVOS

En el marco de la modernización de infraestructuras críticas, este proyecto tiene como objetivo principal realizar un análisis integral de la red de AUTODEMA para diagnosticar vulnerabilidades operacionales y de seguridad, con el fin de diseñar un plan de optimización que garantice un sistema robusto, escalable y protegido contra amenazas internas y externas. Para ello, se empleará una metodología basada en estándares internacionales (ISO 27001, CIS Controls) que combine evaluaciones técnicas exhaustivas con enfoques preventivos y correctivos.

A nivel específico, la investigación se articulará en cuatro dimensiones clave: (1) documentación detallada de la topología actual, incluyendo componentes activos, pasivos y flujos de datos; (2) auditoría de seguridad para detectar fallos en segmentación, autenticación y sistemas de monitoreo; (3) inspección de riesgos físicos en cableado, energía y condiciones ambientales; y (4) desarrollo de propuestas técnicas priorizadas, como implementación de VLANs, protocolos cifrados (Ej. IPsec) y arquitecturas redundantes, alineadas a las mejores prácticas del sector.

6. METODOLOGIA Y ALCANCE

La metodología aplicada en el análisis de la infraestructura de red de AUTODEMA se fundamentó en un enfoque técnico integral que combinó observación directa, análisis documental y entrevistas estructuradas. Se realizaron inspecciones visuales in situ en cada módulo operativo, evaluando el estado del cableado estructurado, la disposición y organización de gabinetes, la funcionalidad de los sistemas de puesta a tierra y la instalación de dispositivos inalámbricos. Estas visitas permitieron validar la correspondencia entre la infraestructura física y la topología lógica declarada.

De forma paralela, se revisaron configuraciones de switches y puntos de acceso, con especial atención en parámetros de seguridad, segmentación de red (VLAN), protocolos de gestión (Telnet, SSH, SNMP), direccionamiento IP y servicios DHCP. Este análisis técnico se complementó con entrevistas al personal de TI de AUTODEMA, lo que permitió entender las políticas operativas vigentes, rutinas de mantenimiento, flujos de comunicación interna y restricciones presupuestales que condicionan las decisiones tecnológicas.

El alcance del estudio se delimitó a los siete módulos principales que componen la red institucional de AUTODEMA, incluyendo su Centro de Datos. Se orientó hacia la identificación de vulnerabilidades físicas y lógicas, con base en estándares internacionales como ANSI/TIA-568 para el diseño y despliegue del cableado estructurado, ANSI/TIA-606 para el etiquetado e inventario de infraestructura, y buenas prácticas de seguridad recogidas en normativas como ISO/IEC 27001 y CIS Controls v8.

La finalidad de esta metodología es generar un diagnóstico técnico detallado y documentado que sustente una propuesta de mejora integral. Esta propuesta estará orientada a subsanar las deficiencias identificadas, garantizar la continuidad operativa, optimizar el desempeño de la red y fortalecer la postura de ciberseguridad de la organización, en consonancia con las exigencias actuales de resiliencia digital y sostenibilidad institucional.

7. AUTODEMA: AUTORIDAD AUTÓNOMA DE MAJES

AUTODEMA (Autoridad Autónoma de Majes) es el organismo responsable de gestionar, ejecutar y supervisar el **Proyecto Especial Majes-Siguas (PEMS)**. Este proyecto transforma los desiertos del sur del Perú en áreas agrícolas productivas, garantizando la disponibilidad y el uso sostenible del recurso hídrico en la región de Arequipa.

7.1 Contexto Geográfico e Hídrico

Perú cuenta con una geografía rica y diversa gracias a su ubicación entre el Océano Pacífico y la Cordillera de los Andes. Esta configuración ha permitido el desarrollo de tres regiones naturales costa, sierra y selva y una compleja red hidrográfica:

- **Ríos** que desembocan en el Atlántico y el Pacífico, pasando por fértiles valles interandinos.
- **Presencia de nevados** que conservan recursos hídricos por siglos.
- La **escasez de tierras agrícolas en el sur** motivó el desarrollo de grandes proyectos de irrigación.

7.2 Origen del Proyecto Majes-Siguas

- En **1920**, el gobierno peruano encargó estudios al ingeniero Carlos Sutton para el uso del río Colca.
- En **1966**, Electroconsult (Italia) elaboró el estudio de factibilidad para Majes.
- La ejecución del proyecto se formaliza en **1971** bajo el gobierno de Juan Velasco Alvarado, con apoyo de empresas de Suecia, Canadá, Sudáfrica, entre otros.

7.3 Obras Hidráulicas Principales

7.3.1 Presa Condoroma

- Ubicada a **4,158 m s.n.m.**, es una de las más altas del mundo.
- Altura: **100 m**, base: **450 m**.
- Capacidad máxima: **285 millones m³**.
- Estructura: Enrocado, arcilla y grava.
- Desembalse a través de un vertedero de **75 m de ancho**.

7.3.2 Infraestructura de Conducción

- **Bocatoma de Tuti**: regula y eleva el nivel del agua.
- **Canal y túneles** recorren más de **100 km** hasta las pampas de Majes.
- **Túnel terminal de 15 km** supera montañas de 5,000 m.
- **Presa de Paltiture y bocatoma** derivan aguas hacia zonas agrícolas.
- **Desarenadores** eliminan sólidos antes del riego.

7.4 Transformación Agraria y Productiva

- Se adjudicaron parcelas de **5 ha a 590 colonos en 1982**.
- Cultivo inicial: **alfalfa**, que facilitó la formación de cuencas lecheras.
- **Reconversión productiva** hacia cultivos de agroexportación como alcachofas y arándanos.
- Introducción de tecnologías como **riego por goteo automatizado**, que mejora el uso del agua y permite fertilización programada.

7.5 Impacto Regional

- El distrito de Majes es uno de los de **mayor crecimiento poblacional** en el país.
- AUTODEMA promueve:
    - **Seguridad hídrica sostenible** para Arequipa.
    - **Cultura del uso racional del agua**.
    - **Inversión privada y reconversión productiva**.
    - Desarrollo de marcas y productos agroindustriales como **quesos, yogures y uvas sin pepa**.

8. TOPOLOGÍA Y BW – LAN – WAN

AUTODEMA, tiene una topología clara y fácil de entender, donde se ve una distribución uniforme.

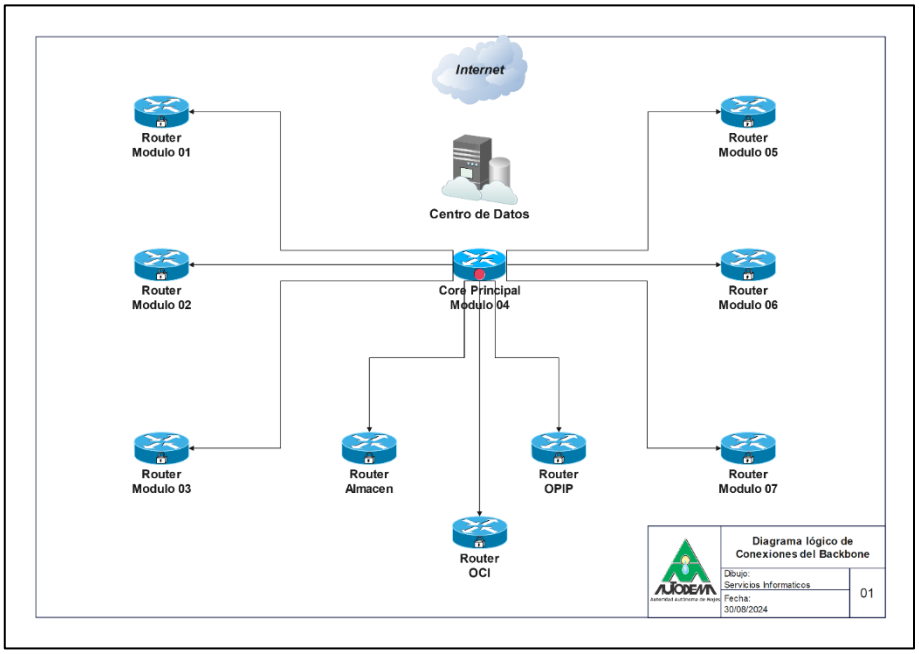


Ilustración 1: Topología física AUTODEMA

Referencia: Otorgado por AUTODEMA

Ancho de Banda (BW)

La infraestructura de red de AUTODEMA cuenta con un esquema de conectividad a Internet diseñado para garantizar disponibilidad y redundancia. A continuación, se detalla la distribución del ancho de banda:

Tabla 1: Ancho de banda

Tipo de Enlace	Velocidad	Uso Principal	Criticidad
Internet Dedicado	200 Mbps	Operaciones diarias y servicios	Alta
Enlace de Reserva	1 Gbps	Contingencia y alta disponibilidad	Critica
Respaldo	2 Gbps	Contingencia y alta disponibilidad	Critica

- La conexión principal de **200 Mbps** es suficiente para las operaciones actuales, pero podría verse limitada en escenarios de crecimiento o ataques DDoS.
- El enlace de reserva de **1 Gbps** no está optimizado para uso simultáneo; se recomienda balancear cargas entre ambos proveedores.

Sala de servidores

Su sala de servidores posee diversos dispositivos que los ayuda a organizar y tener respaldo de sus diversos documentos y archivos.

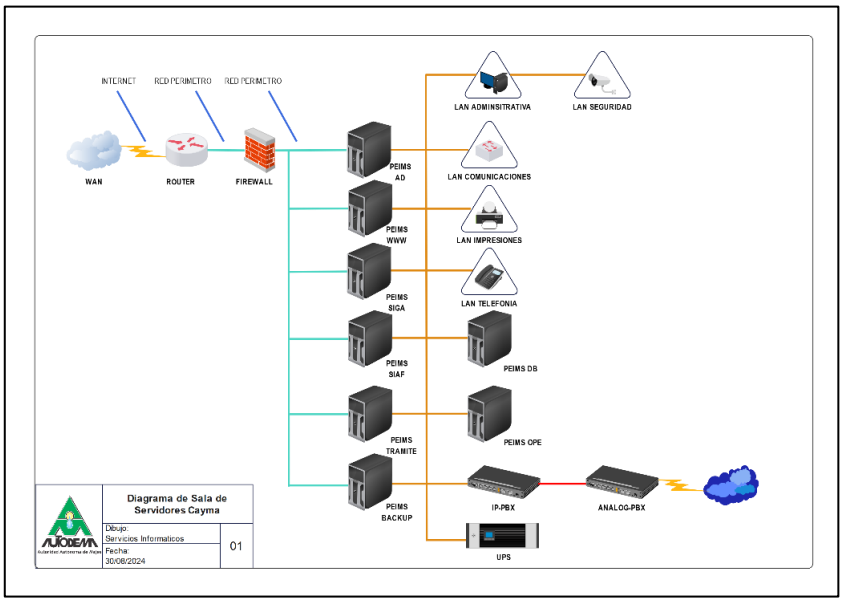


Ilustración 2: Sala de servidores

Referencia: Otorgado por AUTODEMA

Seguridad de la red de datos

La seguridad de la red es un tema muy importante para tratar, por lo que AUTODEMA, lo tiene presente y su seguridad de datos se vista de la siguiente manera.

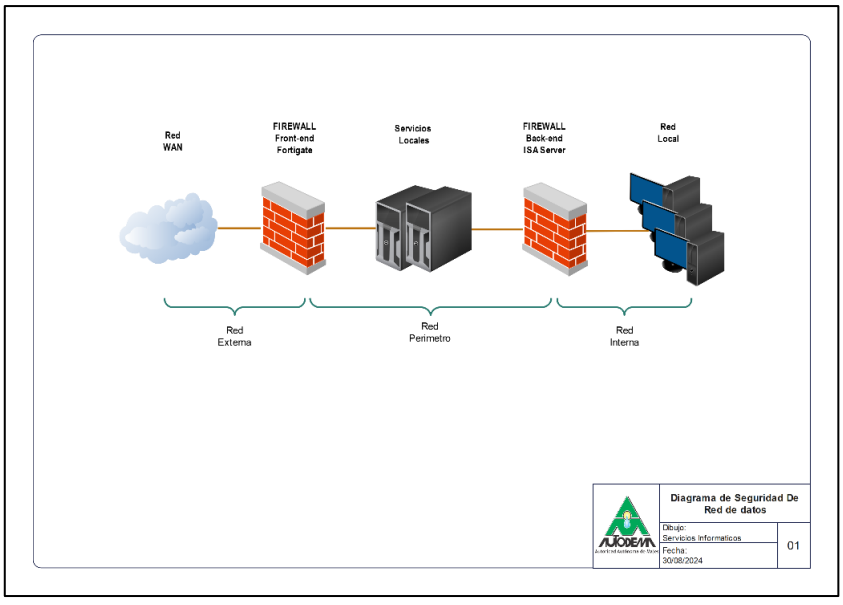


Ilustración 3: Seguridad de la red

Referencia: Otorgado por AUTODEMA

Teléfono IPs

La comunicación en las instalaciones es de debida importancia, por la arquitectura de la sede, por ende, maneja una distribución de telefonía por IP.

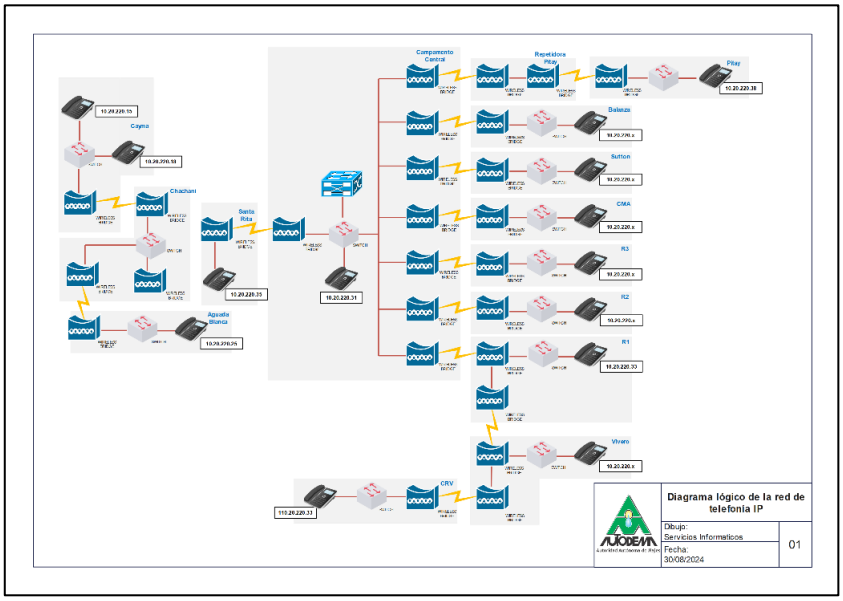


Ilustración 4: teléfonos IPs

Referencia: Otorgado por AUTODEMA

Cámaras

Además, de la seguridad de datos, se tiene que tener en cuenta la seguridad de la instalación y de sus trabajadores, por ende, AUTODEMA cuenta con una distribución de cámaras por toda su sede.

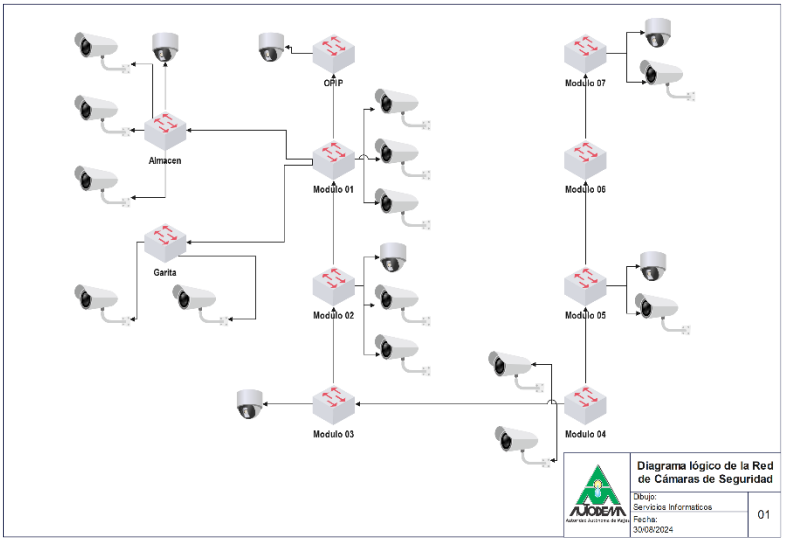


Ilustración 5: Cámaras

Referencia: Otorgado por AUTODEMA

9. MODELO OSI Y TECNOLOGIAS IMPLEMENTADAS

- **Capa Física:** Fibra óptica multimodo (IEEE 802.3z) como backbone, cableado estructurado UTP Cat6 (TIA/EIA-568-C.2), cajas de paso, patch panels, conectores SC y RJ-45.

- **Capa de Enlace:** Switches Ethernet (IEEE 802.3), mayoritariamente sin configuración de VLANs. Protocolos como STP habilitado por defecto, sin personalización de prioridades.

- **Capa de Red:** Direccionamiento IPv4 con esquemas /24. Enrutamiento estático. DHCPv4 activo. No se usa VLSM ni DHCPv6. Sin enrutamiento inter-VLAN.

- **Capa de Transporte:** Uso de TCP/UDP.

- **Capas Altas:** HTTP, Telnet, FTP y otros servicios sin cifrado. Se recomienda migrar a HTTPS, SSH y SNMPv3.

10. NORMATIVAS NACIONES, INTERNACIONALES Y ESTÁNDARES

- **IEEE 802.3:** Ethernet.

- **IEEE 802.1Q:** VLAN tagging.

- **IEEE 802.1D / 802.1w:** STP/RSTP.

- **IEEE 802.1X:** Autenticación de puerto.

- **ANSI/TIA-568-C.2:** Cableado Cat6.

- **TIA/EIA-606:** Etiquetado de cableado.

- **TIA-942:** Infraestructura de centros de datos.

- **Código Nacional de Electricidad del Perú (CNE-U):** Seguridad eléctrica.

- **ITINTEC 200.002:** Sistema de puesta a tierra.

11. EL MARCO DE DISTRIBUCIÓN PRINCIPAL (MDF) Y EL MARCO DE DISTRIBUCIÓN INTERMEDIO (IDF)

El marco de distribución principal (MDF) y el marco de distribución intermedio (IDF) son elementos clave en la infraestructura de red de AUTODEMA. El MDF, ubicado en el Centro de Datos del Módulo 4, actúa como el núcleo central que conecta y gestiona toda la red. Los IDF, localizados en los demás módulos, sirven como puntos de conexión secundarios que distribuyen la señal de red a los dispositivos finales, permitiendo una gestión eficiente, organizada y escalable de la red.

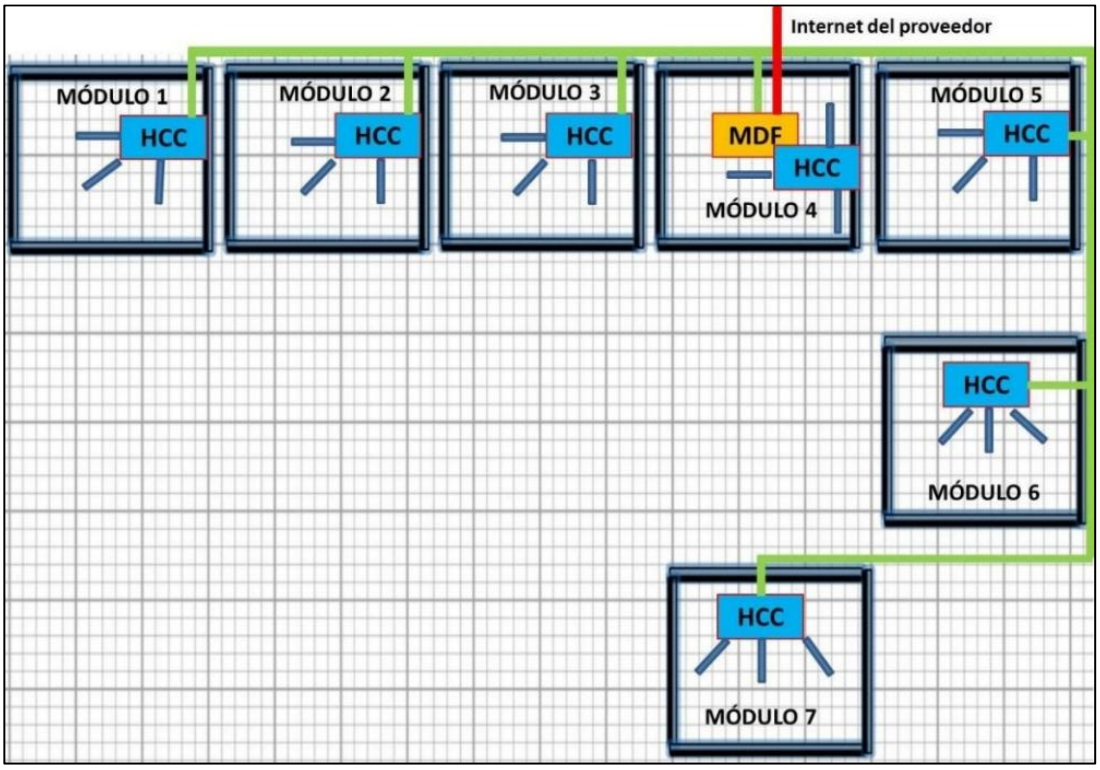


Ilustración 6: distribución principal e interna

Referencia: Realizado por los autores del documento

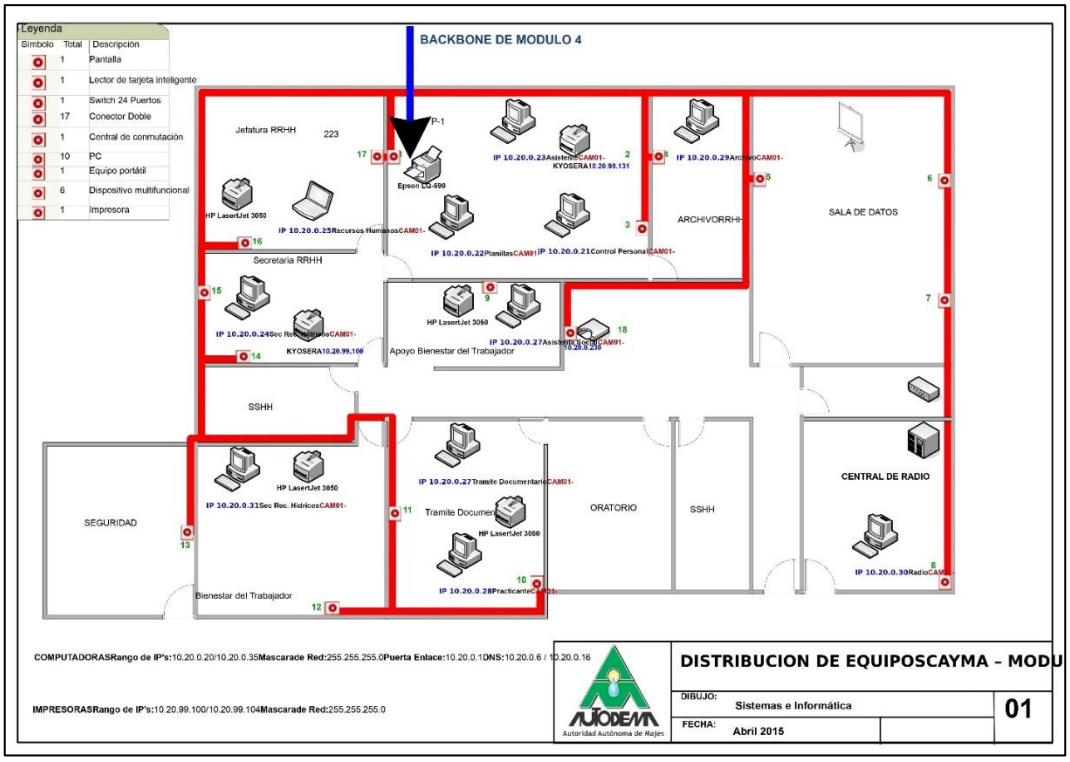


Ilustración 7: Modulo 1

Referencia: Otorgado por AUTODEMA

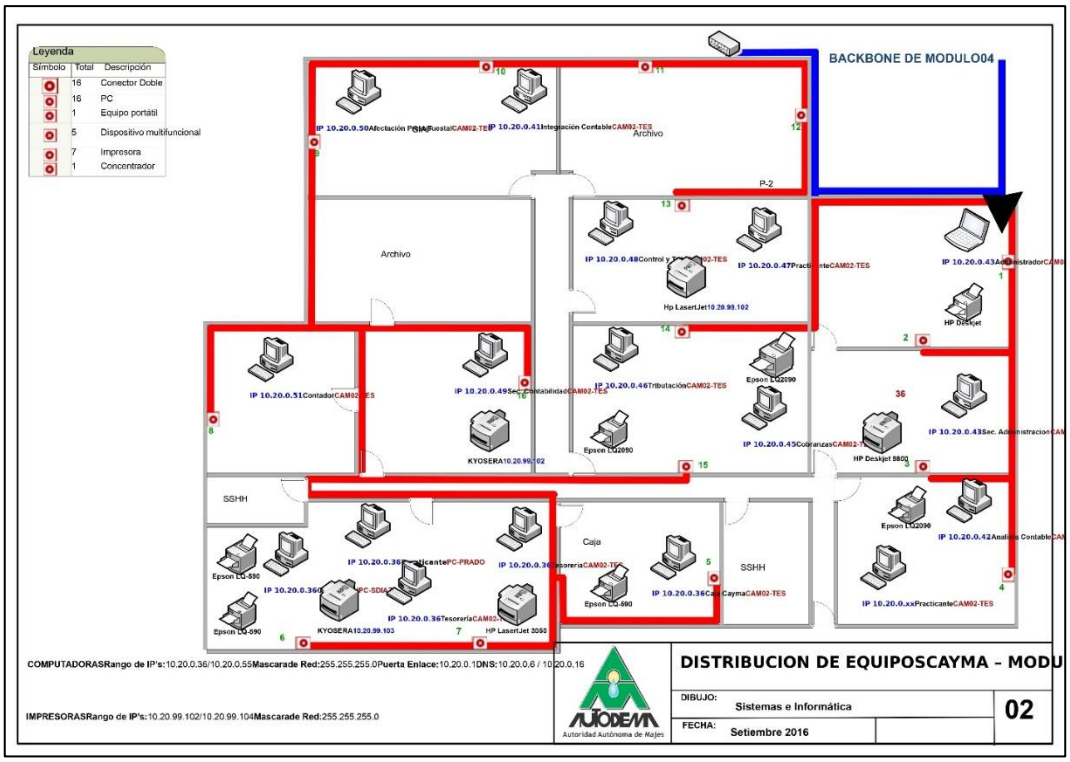


Ilustración 8: Modulo 2

Referencia: Otorgado por AUTODEMA

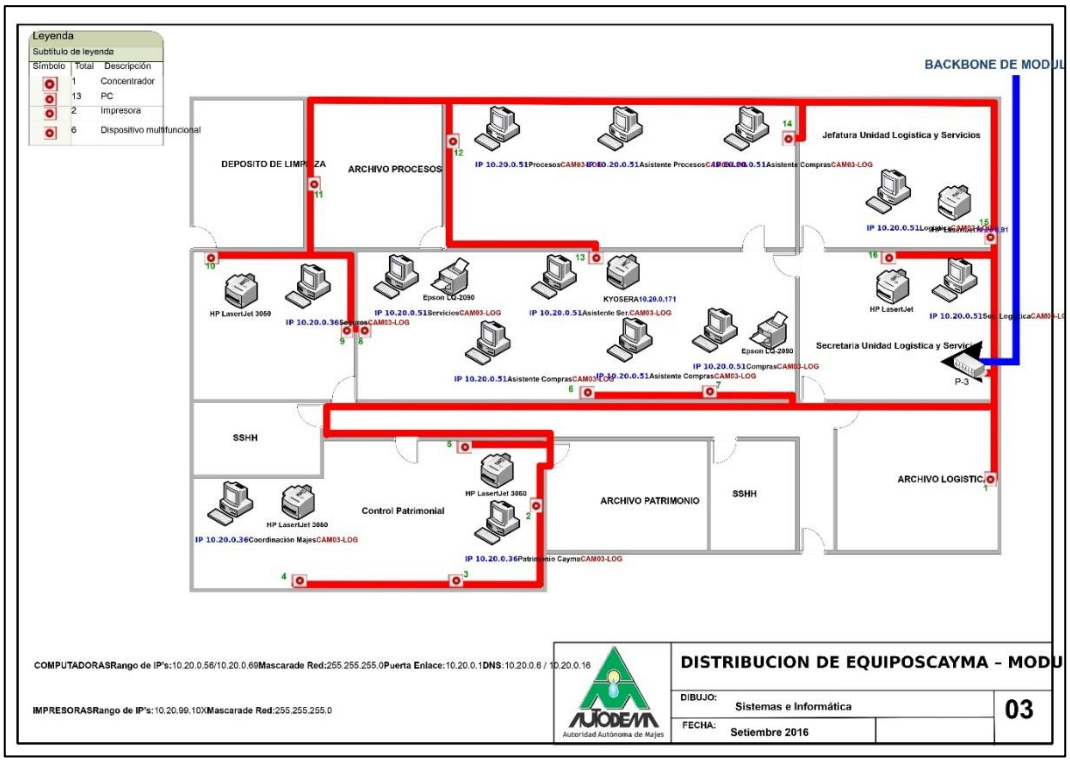


Ilustración 9: Modulo 3

Referencia: Otorgado por AUTODEMA

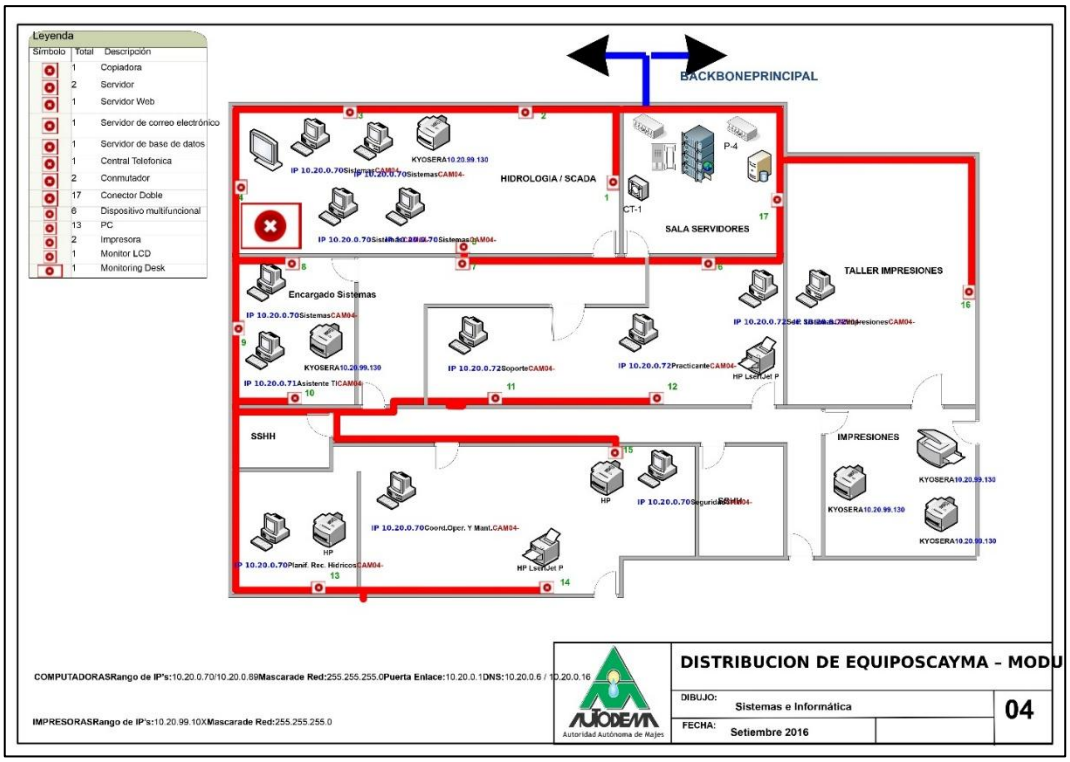


Ilustración 10: Modulo 4

Referencia: Otorgado por AUTODEMA

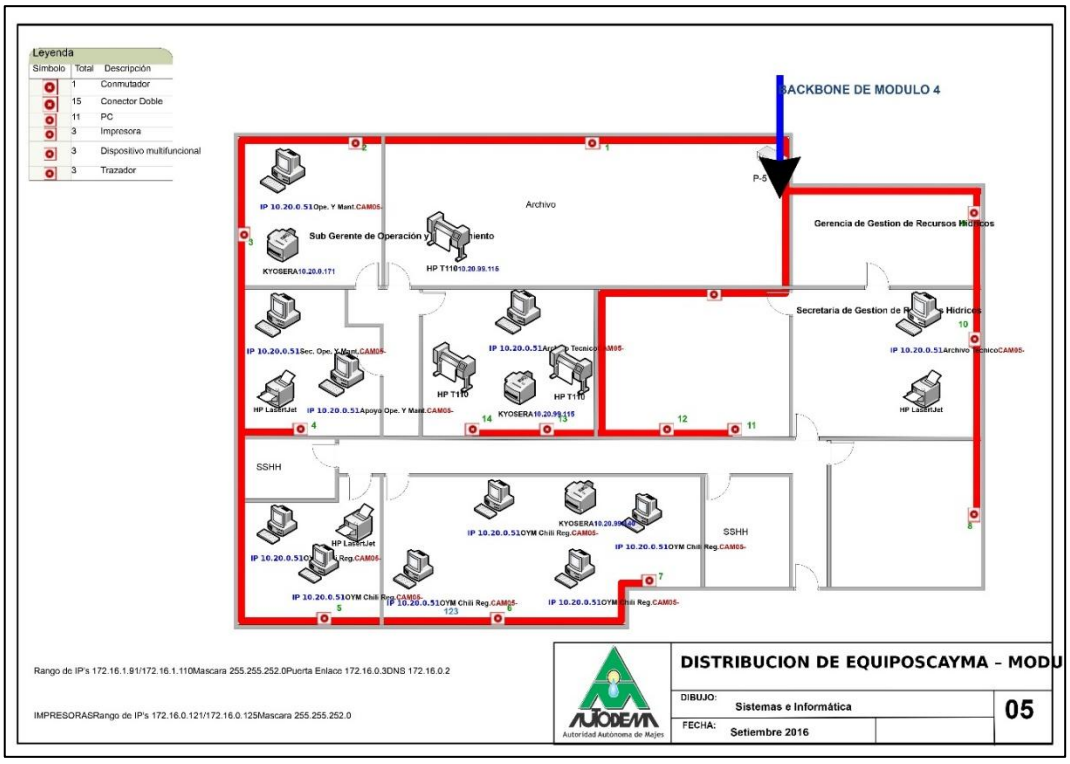


Ilustración 11: Modulo 5

Referencia: Otorgado por AUTODEMA

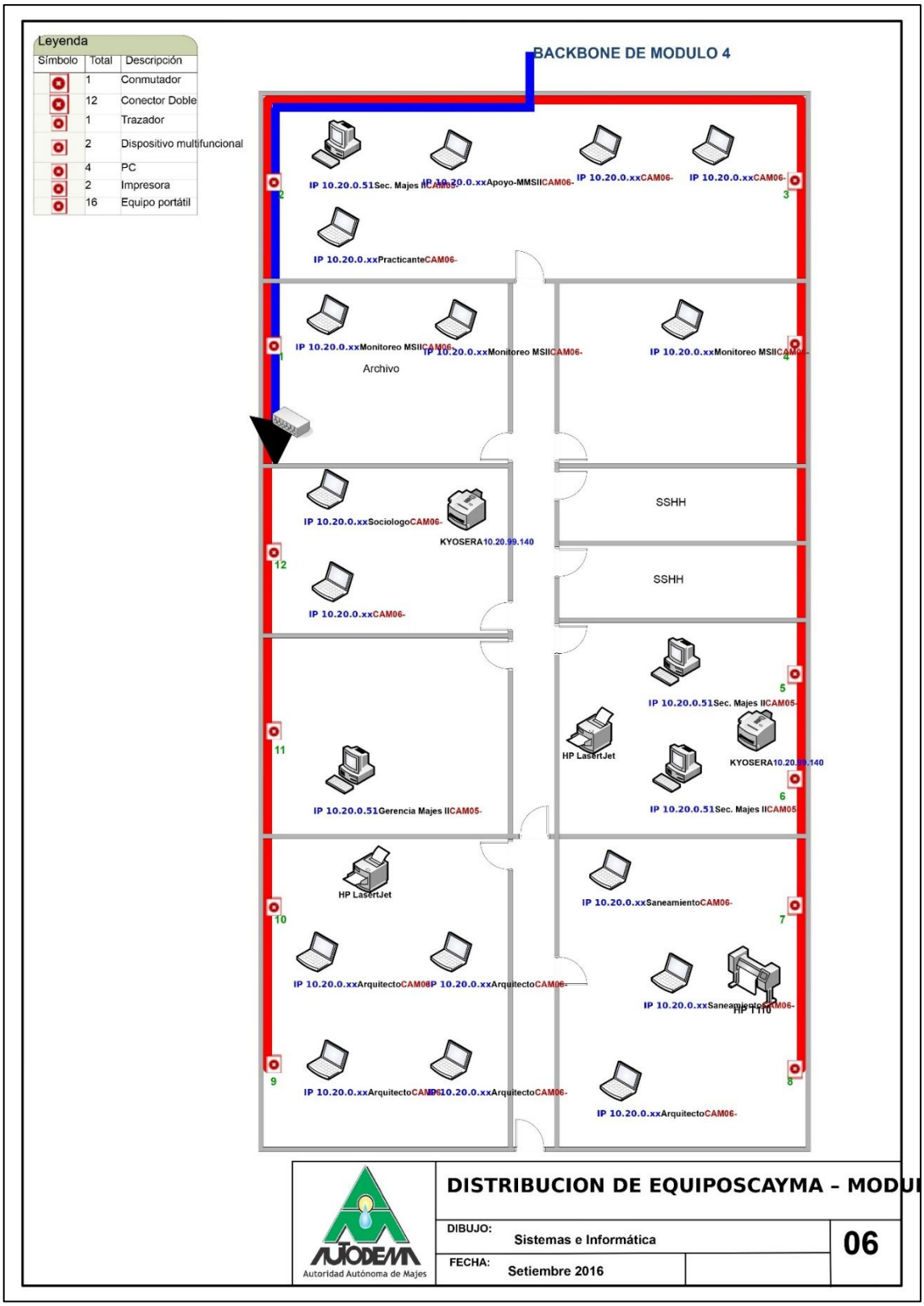


Ilustración 12: Modulo 6

Referencia: Otorgado por AUTODEMA

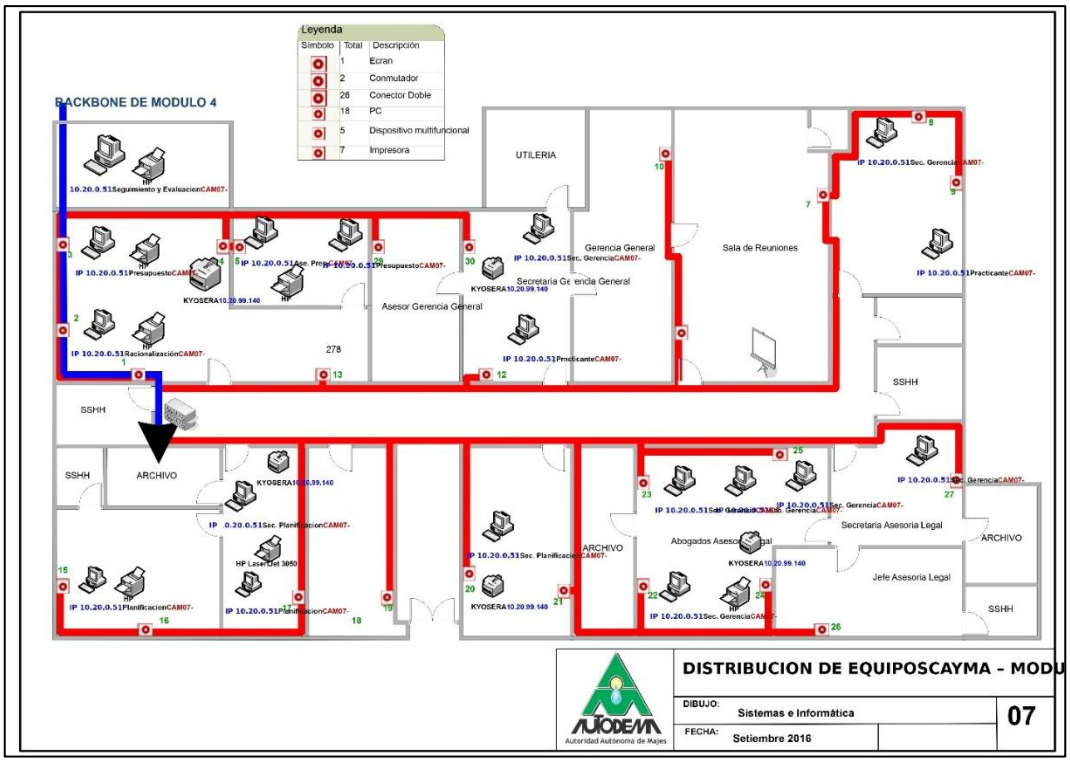


Ilustración 13: Modulo 7

Referencia: Otorgado por AUTODEMA

12. TABLA DE DISPOSITIVOS

12.1 Modulo 1

Tabla 2: Dispositivos intermedios Modulo 1

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch de acceso	HPE Aruba 2530 24G	24	Distribución LAN	Sin PoE
Switch MikroTik	CRS354-48P-4S+2Q+RM	48	Alimentación de dispositivos	Con PoE (para cámaras IP/VoIP)
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	2 unidades

Referencia: Otorgado por AUTODEMA

Muestra los equipos que conectan otros dispositivos en la red del módulo 1: switches y puntos de acceso Wi-Fi.

Tabla 3: Dispositivos finales Modulo 1

Cantidad Total	Dispositivos del Modulo
1	Pantalla
1	Lector de Tarjeta inteligente
17	Conector Doble
1	Central de conmutación
10	PC
1	Dispositivo portátil
6	Dispositivo multifuncional
1	Impresora

Referencia: Otorgado por AUTODEMA

Lista los equipos usados por los usuarios finales como computadoras, impresoras y teléfonos.

12.2 Modulo 2

Tabla 4: Dispositivos intermedios Modulo 2

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch HP	ProCurve 24-port	24	Distribución LAN	Único switch de 24 puertos
Switch Microtip	CRS354-48P-4S+2Q+RM	48	Alimentación de dispositivos	Puerto A (PoE) / Puerto B (no PoE)
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	2 unidades

Referencia: Otorgado por AUTODEMA

Detalla los equipos que gestionan la red dentro del módulo 2, incluyendo un switch HP y uno MikroTik.

Tabla 5: Dispositivos finales Modulo 2

Cantidad Total	Dispositivos del Modulo
16	Conector Doble
16	PC
1	Equipo portátil
5	Dispositivo multifuncional
7	Impresora
1	Concentrador

Referencia: Otorgado por AUTODEMA

Incluye las computadoras, impresoras y otros dispositivos utilizados directamente por el personal.

12.3 Modulo 3

Tabla 6: Dispositivos intermedios Modulo 3

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch HP	ProCurve 48-port	48	Distribución LAN	Sin configuración avanzada
Switch Microtip	CRS354-48P-4S+2Q+RM	48	Conectividad inalámbrica	Soporta APs Wi-Fi
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	1 unidad

Referencia: Otorgado por AUTODEMA

Muestra los switches y puntos de acceso que forman parte de la infraestructura de red del módulo.

Tabla 7: Dispositivos finales Modulo 3

Cantidad Total	Dispositivos del Modulo
1	Concentrador
13	PC
2	Impresora
6	Dispositivo multifuncional

Referencia: Otorgado por AUTODEMA

Lista los dispositivos usados por los usuarios, como computadoras e impresoras.

12.4 Modulo 4

Tabla 8: Dispositivos intermedios Modulo 4

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Servidores	HPE ProLiant DL380	N/A	Hosting de servicios críticos	DNS, DHCP, Correo, IoT
Firewall	FortiGate 100F	N/A	Seguridad perimetral	Único control de acceso
Switch HP (x2)	ProCurve 48-port	48 c/u	Core de red	Backbone redundante
Switch Microtip (x2)	CRS354-48P-4S+2Q+RM	48 c/u	Conexión a módulos	Redundancia en fibra óptica
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	2 unidades
UPS	APC Smart-UPS RT	N/A	Respaldo eléctrico inmediato	Activo durante cortes de luz
Grupo Electrógeno	Caterpillar	N/A	Generador de energía externa	Recarga el UPS fuera del módulo

Referencia: Otorgado por AUTODEMA

Incluye servidores, firewalls, switches y sistemas de respaldo energético del centro de datos.

Tabla 9: Dispositivos finales Modulo 4

Cantidad Total	Dispositivos del Modulo
1	Copiadora
2	Servidor
1	Servidor WEB
1	Servidor de correo electrónico
1	Servidor de base de datos
1	Central Telefónica
2	Conmutador
17	Conector Doble
6	Dispositivo multifuncional
13	PC
2	Impresora
1	Monitor LCD
1	Monitoring Desk

Referencia: Otorgado por AUTODEMA

Muestra los equipos terminales como servidores web, PCs y monitores.

12.5 Modulo 5

Tabla 10: Dispositivos intermedios Modulo 5

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch HP	ProCurve 48-port	48	Distribución LAN	Sin PoE
Switch Microtip	CRS354-48P-4S+2Q+RM	48	Dispositivos IoT	Alimenta sensores/equipos
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	1 unidad

Referencia: Otorgado por AUTODEMA

Detalla los switches y puntos de acceso del módulo 5.

Tabla 11: Dispositivos finales Modulo 5

Cantidad Total	Dispositivos del Modulo
1	Conmutador
15	Conector Doble
11	PC
3	Impresora
3	Dispositivo multifuncional
3	Trazador

Referencia: Otorgado por AUTODEMA

Incluye computadoras, impresoras y trazadores usados en este módulo.

12.6 Modulo 6

Tabla 12: Dispositivos intermedios Modulo 6

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch HP	ProCurve 48-port	48	Distribución LAN	Conexión a backbone
Switch Microtip	CRS354-48P-4S+2Q+RM	48	Telefonía IP	Soporta VoIP
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	1 unidad

Referencia: Otorgado por AUTODEMA

Muestra los switches y puntos de acceso que forman parte de la infraestructura del módulo.

Tabla 13: Dispositivos finales Modulo 6

Cantidad Total	Dispositivos del Modulo
1	Conmutador
12	Conector Doble
1	Trazador
2	Dispositivo Multifuncional
4	PC
2	Impresora
16	Equipo portátil

Referencia: Otorgado por AUTODEMA

Lista los equipos usados por los usuarios, como laptops, impresoras y dispositivos móviles.

12.7 Modulo 7

Tabla 14: Dispositivos intermedios Modulo 7

Dispositivo	Marca/Modelo	Puertos	Función Principal	Observaciones
Switch HP	ProCurve 48-port	48	Distribución LAN	Terminal de red
Switch Microtip	CRS354-48P-4S+2Q+RM	48	CCTV	Alimenta cámaras de seguridad
Access Point	Ubiquiti UniFi UAP-AC-LR	N/A	Cobertura Wi-Fi	1 unidad

Referencia: Otorgado por AUTODEMA

Detalla los switches y puntos de acceso del módulo 7.

Tabla 15: Dispositivos finales Modulo 7

Cantidad Total	Dispositivos del Modulo
1	Ecran
2	Conmutador
26	Conectador Doble
18	PC
5	Dispositivo Multifuncional
7	Impresora

Referencia: Otorgado por AUTODEMA

Incluye computadoras, impresoras y dispositivos multifuncionales utilizados en este módulo.

12.8 Tablas generales

Tabla 16: Dispositivos intermedios AUTODEMA

Dispositivo	Ubicación	Cantidad Total	Función	Marca / Modelo
Switch Core (Módulo 4)	Centro de Datos	2 (HP) + 2 (MikroTik)	Core de red y redundancia	HP ProCurve / MikroTik CRS354
Switch Acceso	Módulos 1–7	7 (HP) + 7 (MikroTik)	Distribución LAN, PoE para VoIP, CCTV	HP ProCurve / MikroTik CRS354
Access Points	Módulos 1–7	10 aprox.	Cobertura Wi-Fi corporativa	Ubiquiti UniFi UAP-AC-LR
Servidores	Centro de Datos	4	DNS, DHCP, Correo, IoT	HPE ProLiant DL380
Firewall	Centro de Datos	1	Seguridad perimetral	FortiGate 100F
UPS	Centro de Datos	1	Respaldo eléctrico inmediato	APC Smart-UPS RT
Grupo Electrógeno	Exterior (CDP)	1	Generador externo para recarga UPS	Caterpillar / Generac (referencia)
Gabinetes Rack	Cada módulo	7	Organización cableado y equipos	Rack 42U

Referencia: Otorgado por AUTODEMA

Resume todos los equipos de red principales de toda la infraestructura de AUTODEMA.

Tabla 17: Dispositivos finales AUTODEMA

Cantidad Total	Dispositivo
1	Pantalla
1	Lector de Tarjeta Inteligente
116	Conector Doble
8	Conmutador / Central
96	PC
18	Dispositivo Portátil
33	Dispositivo Multifuncional
20	Impresora

1	Copiadora
5	Servidores (WEB, Correo, BD, etc.)
1	Monitor LCD
1	Monitoring Desk
2	Concentrador
1	Ecran
4	Trazador

Referencia: Otorgado por AUTODEMA

Muestra la cantidad total de dispositivos usados por los usuarios en toda la organización.

13. ANÁLISIS DE RED - AUTODEMA

13.1 TABLAS POR SUBRED IDENTIFICADA

SUBRED 10.20.0.0/24 (Red Principal)

Tabla 18: Subred Principal

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.23	Asistente CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.29	Archivo CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.21	Control Personal CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.22	Planilla CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.23	Recursos Humanos CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.27	Tramite Documentario CAM01	Workstation	SSHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.28	Practicante CAM01	Workstation	SSHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.31	Sec. Recursos Humanos CAM01	Workstation	RRHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.30	Radio CAM01	Central Radio	Centro Datos	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

Muestra direcciones IP asignadas a equipos clave en la red principal.

SUBRED 10.20.0.0/24 (Continuación - Oficinas Administrativas)

Tabla 19: Subred Oficinas Administrativas

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.50	Afectación Predial CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.41	Integración Contable CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.48	Control Patrimonial CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.47	Practicante CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.46	Tributación CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.45	Cobranzas CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.43	Administración CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.42	Análisis Contable CAM01	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

Direcciones IP usadas en oficinas administrativas.

SUBRED 10.20.0.0/24 (CAM03 - Logística y Servicios)

Tabla 20: Subred Logística y Servicios

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.51	Procesos CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Asistente Procesos CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Asistente Compras CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Logística CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Servicios CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Compras CAM03	Workstation	Logística	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.36	Coordinación Majes CAM03	Workstation	SSHH	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.36	Patrimonio Cayma CAM03	Workstation	SSHH	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

IPs dedicadas al área de logística y servicios.

SUBRED 10.20.0.0/24 (CAM04 - Sistemas)

Tabla 21: Subred Sistema

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.70	Sistemas CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.70	Sistemas CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.70	Encargado Sistemas CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.71	Asistente TICAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.72	Soporte CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.72	Practicante CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.70	Coord.Oper. Y Mant. CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.70	Planif. Rec. Hídricos CAM04	Workstation	Sala Servidores	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

Direcciones para equipos del departamento de sistemas.

SUBRED 172.16.0.0/24 (Red Secundaria - CAM05)

Tabla 22: Subred Red Secundaria

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
172.16.0.51	Operación Y Mant. CAM05	Workstation	Oficina	255.255.255.0	172.16.0.1	172.16.0.0
172.16.0.51	Sec. Operación Y Mant. CAM05	Workstation	Oficina	255.255.255.0	172.16.0.1	172.16.0.0
172.16.0.51	Apoyo Operación Y Mant. CAM05	Workstation	Oficina	255.255.255.0	172.16.0.1	172.16.0.0
172.16.0.51	Archivo Técnico CAM05	Workstation	Oficina	255.255.255.0	172.16.0.1	172.16.0.0
172.16.0.51	OYM Chili Reg CAM05	Workstation	SSHH	255.255.255.0	172.16.0.1	172.16.0.0
172.16.0.51	OYM Chili Reg CAM05	Workstation	SSHH	255.255.255.0	172.16.0.1	172.16.0.0

Referencia: Otorgado por AUTODEMA

IPs usadas en una red secundaria, principalmente para operaciones y mantenimiento.

SUBRED 10.20.0.0/24 (CAM06 - Arquitectura y Monitoreo)

Tabla 23: Subred Arquitectura y Monitoreo

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.x	Sec. Majes IICAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Apoyo MMSIIICAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Practicante CAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Monitoreo MSIICAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Sociología CAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Gerencia Majes IICAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Sec. Majes IICAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Saneamiento CAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.x	Arquitecto CAM06	Workstation	Oficina	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

Direcciones asignadas al área de arquitectura y monitoreo.

SUBRED 10.20.0.0/24 (CAM07 - Gerencia General)

Tabla 24: Subred Gerencia General

IP	Dispositivo/Usuario	Función	Ubicación	Máscara	Gateway	IP Red
10.20.0.51	Seguimiento y Evaluación CAM07	Workstation	Gerencia	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Racionalización CAM07	Workstation	Gerencia	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Asec. Presupuesto CAM07	Workstation	Gerencia	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Presupuesto CAM07	Workstation	Gerencia	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Sec. Gerencia CAM07	Workstation	Gerencia	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Gerencia CAM07	Workstation	Gerencia General	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Practicante CAM07	Workstation	Sala Reuniones	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Sec. Planificación CAM07	Workstation	Archivo	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Planificación CAM07	Workstation	Archivo	255.255.255.0	10.20.0.1	10.20.0.0
10.20.0.51	Sec. Gerencia CAM07	Workstation	Asesoría Legal	255.255.255.0	10.20.0.1	10.20.0.0

Referencia: Otorgado por AUTODEMA

IPs dedicadas a la gerencia general.

13.2 TABLAS POR MÓDULO/PLANO

MÓDULO 01 - CENTRO DE DATOS Y RRHH (Abril 2015)

Tabla 25: Direcciones IPs Modulo 1

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
Switch 24 Puertos	-	Core de Red	Centro Datos	Activo
Epson LQ-590	-	Impresora	Secretaría RRHH	Activo
HP LaserJet 3050	-	Multifuncional	Jefatura RRHH	Activo
KYOSERA	10.20.0.23	Asistente CAM01	RRHH	Activo
KYOSERA	10.20.0.29	Archivo CAM01	RRHH	Activo
PC	10.20.0.21	Control Personal CAM01	RRHH	Activo
PC	10.20.0.22	Planilla CAM01	RRHH	Activo
PC	10.20.0.31	Recursos Humanos CAM01	RRHH	Activo
HP LaserJet 3050	-	Multifuncional	Tramite Documentario	Activo
PC	10.20.0.27	Tramite Documentario CAM01	SSHH	Activo
PC	10.20.0.28	Practicante CAM01	SSHH	Activo
PC	10.20.0.30	Radio CAM01	Central Radio	Activo

Referencia: Otorgado por AUTODEMA

Asignación de IPs a dispositivos del Módulo 1.

MÓDULO 02 - OFICINAS ADMINISTRATIVAS (septiembre 2016)

Tabla 26: Direcciones IPs Modulo 2

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
PC	10.20.0.50	Afectación Predial CAM01	Archivo	Activo
PC	10.20.0.41	Integración Contable CAM01	Archivo	Activo
KYOSERA	10.20.0.48	Control Patrimonial CAM01	Archivo	Activo
PC	10.20.0.47	Practicante CAM01	Oficina	Activo
Epson LQ-590	-	Impresora	Oficina	Activo
PC	10.20.0.46	Tributación CAM01	Oficina	Activo
PC	10.20.0.45	Cobranzas CAM01	Oficina	Activo
HP DeskJet 5800	-	Impresora	Oficina	Activo
PC	10.20.0.43	Administración CAM01	Oficina	Activo
Epson LQ-590	-	Impresora	SSHH	Activo
PC	10.20.0.42	Análisis Contable CAM01	SSHH	Activo
KYOSERA	10.20.0.36	Alcantarillado CAM01	SSHH	Activo
HP LaserJet 3050	-	Multifuncional	SSHH	Activo

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
PC	10.20.0.36	Tesorería CAM01	SSHH	Activo
Epson LQ-590	-	Impresora	Caja	Activo
PC	10.20.0.36	Cayma CAM01	Caja	Activo

Referencia: Otorgado por AUTODEMA

IPs asignadas en el Módulo 2.

MÓDULO 03 - LOGÍSTICA Y SERVICIOS (septiembre 2016)

Tabla 27: Direcciones IPs Modulo 3

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
PC	10.20.0.51	Procesos CAM03	Jefatura ULS	Activo
PC	10.20.0.51	Asistente Procesos CAM03	Jefatura ULS	Activo
PC	10.20.0.51	Asistente Compras CAM03	Jefatura ULS	Activo
PC	10.20.0.51	Logística CAM03	Secretaría ULS	Activo
HP LaserJet	-	Impresora	Secretaría ULS	Activo
PC	10.20.0.51	Servicios CAM03	Archivo Procesos	Activo
Epson LQ-2090	-	Impresora	Archivo Procesos	Activo
KYOSERA	10.20.0.51	Asistente Servicios CAM03	Archivo Procesos	Activo
PC	10.20.0.51	Compras CAM03	Archivo Procesos	Activo
HP LaserJet 3050	-	Multifuncional	Control Patrimonial	Activo
PC	10.20.0.36	Coordinación Majes CAM03	SSHH	Activo
HP LaserJet 3050	-	Multifuncional	SSHH	Activo
PC	10.20.0.36	Patrimonio Cayma CAM03	SSHH	Activo

Referencia: Otorgado por AUTODEMA

Direcciones IP en el Módulo 3.

MÓDULO 04 - CENTRO DE DATOS Y SISTEMAS (septiembre 2016)

Tabla 28: Direcciones IPs Modulo 4

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
Copiadora	-	Multifuncional	Hidrología/SCADA	Activo
Servidor	-	Base de Datos	Sala Servidores	Activo
Servidor Web	-	Web Server	Sala Servidores	Activo
Servidor	-	Mail Server	Sala Servidores	Activo
Central Telefónica	-	Telefonía	Sala Servidores	Activo
Conmutador	-	Core Switch	Sala Servidores	Activo
KYOSERA	10.20.0.70	Sistemas CAM04	Hidrología/SCADA	Activo
PC	10.20.0.70	Sistemas CAM04	Encargado Sistemas	Activo

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
PC	10.20.0.71	Asistente TICAM04	Encargado Sistemas	Activo
KYOSERA	10.20.0.72	Soporte CAM04	Taller Impresiones	Activo
PC	10.20.0.72	Practicante CAM04	Taller Impresiones	Activo
HP LaserJet P	-	Impresora	Taller Impresiones	Activo
PC	10.20.0.70	Coord.Oper. Y Mant. CAM04	SSHH	Activo
HP	-	Multifuncional	SSHH	Activo
PC	10.20.0.70	Segundo Soporte CAM04	SSHH	Activo
PC	10.20.0.70	Planif. Rec. Hídricos CAM04	SSHH	Activo
HP LaserJet P	-	Impresora	SSHH	Activo
KYOSERA	10.20.0.89	Core Switch	Impresiones	Activo

Referencia: Otorgado por AUTODEMA

IPs asignadas a dispositivos del Centro de Datos y Sistemas.

MÓDULO 05 - OPERACIÓN Y MANTENIMIENTO (septiembre 2016)

Tabla 29: Direcciones IPs Modulo 5

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
Conmutador	-	Network Switch	Backbone	Activo
PC	172.16.0.51	Operación Y Mant. CAM05	Archivo	Activo
KYOSERA	172.16.0.51	Sub Gerente Operación	Oficina	Activo
HP T1010	172.16.0.51	Plotter Técnico	Oficina	Activo
PC	172.16.0.51	Sec. Operación Y Mant. CAM05	Oficina	Activo
PC	172.16.0.51	Apoyo Operación Y Mant. CAM05	Oficina	Activo
HP T1010	-	Plotter	Oficina	Activo
HP LaserJet	-	Impresora	Oficina	Activo
KYOSERA	172.16.0.51	Archivo Técnico CAM05	Gerencia Recursos Hídricos	Activo
HP LaserJet	-	Impresora	Secretaría Recursos Hídricos	Activo
PC	172.16.0.51	OYM Chili Reg CAM05	SSHH	Activo
KYOSERA	172.16.0.51	OYM Chili Reg CAM05	SSHH	Activo
PC	172.16.0.51	OYM Chili Reg CAM05	SSHH	Activo

Referencia: Otorgado por AUTODEMA

IPs usadas en el Módulo 5.

MÓDULO 06 - ARQUITECTURA Y MONITOREO (septiembre 2016)

Tabla 30: Direcciones IPs Modulo 6

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
Conmutador	-	Network Switch	Backbone	Activo
PC	10.20.0.x	Sec. Majes IICAM06	Oficina Superior	Activo
Laptop	10.20.0.x	Apoyo MMSIIICAM06	Oficina Superior	Activo
Laptop	10.20.0.x	Practicante CAM06	Oficina Superior	Activo
Laptop	10.20.0.x	Monitoreo MSIICAM06	Archivo	Activo
Laptop	10.20.0.x	Sociología CAM06	Archivo	Activo
KYOSERA	10.20.0.89	Core Switch	Archivo	Activo
PC	10.20.0.51	Gerencia Majes IICAM06	Oficina Inferior	Activo
HP LaserJet	-	Impresora	Oficina Inferior	Activo
PC	10.20.0.51	Sec. Majes IICAM06	Oficina Inferior	Activo
KYOSERA	10.20.0.89	Multifuncional	Oficina Inferior	Activo
Laptop	10.20.0.x	Saneamiento CAM06	Oficina Inferior	Activo
Laptop	10.20.0.x	Arquitecto CAM06	Oficina Inferior	Activo
Plotter HP	-	Plotter	Oficina Inferior	Activo

Referencia: Otorgado por AUTODEMA

Asignación de IPs al Módulo 6.

MÓDULO 07 - GERENCIA GENERAL (septiembre 2016)

Tabla 31: Direcciones IPs Modulo 7

Dispositivo	IP	Usuario/Función	Ubicación Específica	Estado
PC	10.20.0.51	Seguimiento y Evaluación CAM07	Oficina Superior	Activo
Laptop	10.20.0.51	Racionalización CAM07	Oficina Superior	Activo
PC	10.20.0.51	Asec. Presupuesto CAM07	Oficina Superior	Activo
Laptop	10.20.0.51	Presupuesto CAM07	Oficina Superior	Activo
KYOSERA	10.20.0.89	Multifuncional	Gerencia General	Activo
PC	10.20.0.51	Sec. Gerencia CAM07	Utilería	Activo
PC	10.20.0.51	Gerencia CAM07	Gerencia General	Activo
PC	10.20.0.51	Practicante CAM07	Sala Reuniones	Activo
KYOSERA	10.20.0.89	Multifuncional	Archivo Inferior	Activo
PC	10.20.0.51	Sec. Planificación CAM07	Archivo Inferior	Activo
HP LaserJet 3050	-	Multifuncional	Archivo Inferior	Activo
Laptop	10.20.0.51	Planificación CAM07	Archivo Inferior	Activo
KYOSERA	10.20.0.89	Multifuncional	Asesoría Legal	Activo
PC	10.20.0.51	Sec. Gerencia CAM07	Asesoría Legal	Activo

Referencia: Otorgado por AUTODEMA

13.3 TABLAS POR MÓDULO/PLANO

RANGO PRINCIPAL: 10.20.0.0/20 (10.20.0.1 - 10.20.15.254)

Tabla 32: Rangos IPs Principales

Subred	Rango Inicio	Rango Fin	Total IPs	Uso Actual	Disponibles	Observaciones
10.20.0.0/24	10.20.0.1	10.20.0.254	254	~120 IPs	~134 IPs	Red principal - Mayoría de equipos administrativos y operativos
10.20.1.0/24	10.20.1.1	10.20.1.254	254	0 IPs	254 IPs	Completamente disponible para expansión
10.20.2.0/24	10.20.2.1	10.20.2.254	254	0 IPs	254 IPs	Completamente disponible para expansión
10.20.3.0/24	10.20.3.1	10.20.3.254	254	0 IPs	254 IPs	Completamente disponible para expansión
10.20.4.0/24	10.20.4.1	10.20.4.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.5.0/24	10.20.5.1	10.20.5.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.6.0/24	10.20.6.1	10.20.6.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.7.0/24	10.20.7.1	10.20.7.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.8.0/24	10.20.8.1	10.20.8.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.9.0/24	10.20.9.1	10.20.9.254	254	~15 IPs	~239 IPs	Red para impresoras y periféricos
10.20.10.0/24	10.20.10.1	10.20.10.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.11.0/24	10.20.11.1	10.20.11.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.12.0/24	10.20.12.1	10.20.12.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.13.0/24	10.20.13.1	10.20.13.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.14.0/24	10.20.14.1	10.20.14.254	254	0 IPs	254 IPs	Disponible para expansión
10.20.15.0/24	10.20.15.1	10.20.15.254	254	0 IPs	254 IPs	Disponible para expansión

Referencia: Otorgado por AUTODEMA

Muestra los rangos de direcciones IP disponibles y su uso actual en la red principal.
RANGO SECUNDARIO: 172.16.0.0/24 (172.16.0.1 - 172.16.0.254)

Tabla 33: Rangos IPs Secundarias

Subred	Rango Inicio	Rango Fin	Total IPs	Uso Actual	Disponibles	Observaciones
172.16.0.0/24	172.16.0.1	172.16.0.254	254	~18 IPs	~236 IPs	Red específica para área de Operación y Mantenimiento

Referencia: Otorgado por AUTODEMA

Indica los rangos de IP usados en redes secundarias.

RESUMEN

Tabla 34: Resumen de IPs AUTODEMA

Aspecto	Valor
Total IPs Disponibles	4,318 IPs
Total IPs Utilizadas	~153 IPs
Total IPs Libres	~4,165 IPs
Porcentaje de Utilización	~3.5%
Capacidad de Crecimiento	2,725%

Referencia: Otorgado por AUTODEMA

Resume cuántas IPs se están usando y cuántas quedan disponibles

13.4 CONSOLIDACIÓN DE DISPOSITIVOS POR TIPO - BACKBONE MÓDULO 4

RESUMEN EJECUTIVO DE DISPOSITIVOS

Tabla 35: Resumen Dispositivos Modulo 4

Tipo de Dispositivo	Cantidad Total	Porcentaje	Observaciones
PC/Computadoras	86	54.8%	Dispositivo predominante
Conectores Doble	29	18.5%	Infraestructura de conectividad
Impresoras	15	9.6%	Distribución por áreas
Dispositivos Multifuncional	11	7.0%	Equipos híbridos
Equipos Portátiles	16	10.2%	Laptops y móviles

Referencia: Otorgado por AUTODEMA

Muestra la cantidad y tipos de dispositivos en el Módulo 4.

DETALLE POR TIPO DE DISPOSITIVO

1. COMPUTADORAS (86 unidades)

Tabla 36: Detalles Dispositivos

Ubicación Principal	Cantidad	IP Ejemplo	Función
Oficinas Administrativas	35	10.20.0.23	Trabajo administrativo
Área Operativa	28	10.20.0.51	Control y monitoreo
Área Técnica	15	172.16.0.51	Gestión técnica
Salas de Reuniones	8	10.20.0.91	Presentaciones

Referencia: Otorgado por AUTODEMA

Desglose de computadoras por ubicación y función.

2. INFRAESTRUCTURA DE RED (33 unidades)

Switches Core

Tabla 37: Infraestructura de Red

Modelo	Cantidad	Ubicación	Función	IP
HP ProCurve	2	Centro de Datos	Core principal	N/A
MikroTik CRS354	2	Centro de Datos	Core redundante	N/A
KyoSera (Switch)	8	Distribuido	Acceso	10.20.99.xxx
HP LaserJet 3050	4	Distribuido	Switching local	N/A

Referencia: Otorgado por AUTODEMA

Detalla los modelos y funciones de los switches.

Conectores y Cableado

Tabla 38: Conectores y Cableados

Tipo	Cantidad	Distribución
Conectores Doble	29	Todas las áreas
Trazadores	3	Área técnica
Conmutadores	2	Centro de datos

Referencia: Otorgado por AUTODEMA

3. IMPRESORAS Y PERIFÉRICOS (15 unidades)
Por Marca y Modelo

Tabla 39: Impresores y Periféricos

Marca/Modelo	Cantidad	Rango IP	Ubicación Típica
Epson LX-300	4	10.20.0.xxx	Oficinas
HP LaserJet 3050	6	10.20.99.xxx	Distribuidas
HP LaserJet P	3	10.20.0.xxx	Áreas específicas
KyoSera	2	10.20.99.xxx	Áreas administrativas

Referencia: Otorgado por AUTODEMA

Tipos de impresoras y su ubicación típica.

4. DISPOSITIVOS MULTIFUNCIONALES (11 unidades)

Tabla 40: Dispositivos Multifuncionales

Función	Cantidad	Rango IP	Observaciones
Escáner/Impresora	6	10.20.0.xxx	Oficinas principales
Fax/Impresora	3	10.20.0.xxx	Comunicaciones
Copiadora/Red	2	10.20.99.xxx	Áreas centrales

Referencia: Otorgado por AUTODEMA

Funciones y cantidad de equipos multifuncionales.

5. EQUIPOS PORTÁTILES (16 unidades)

Tabla 41: Equipos Portátiles

Tipo	Cantidad	Asignación	Red
Laptops Ejecutivas	8	Personal directivo	10.20.0.xxx
Laptops Técnicas	5	Personal técnico	172.16.0.xxx
Tablets	3	Presentaciones	10.20.0.xxx

Referencia: Otorgado por AUTODEMA

Cantidad y tipo de laptops y tablets.

ANÁLISIS DE MARCAS Y MODELOS
Predominancia por Marca

Tabla 42: Marcas y Modelos

Marca	Dispositivos	Porcentaje	Tipo Principal
HP	15	23.1%	Impresoras/Switches
Epson	8	12.3%	Impresoras
KyoSera	12	18.5%	Multifuncionales/Switches
MikroTik	2	3.1%	Switches Core
Genérico/PC	28	43.1%	Computadoras

Referencia: Otorgado por AUTODEMA

Resumen de marcas predominantes en la infraestructura.

14. PROBLEMAS IDENTIFICADOS

La infraestructura de red de AUTODEMA presenta una serie de desafíos complejos que comprometen su eficiencia, seguridad y escalabilidad. Durante la evaluación preliminar, se identificaron problemáticas críticas, incluyendo la **ausencia total de segmentación mediante VLANs**. Esto crea un entorno de red plano donde cualquier brecha de seguridad puede propagarse sin restricciones a través de todos los módulos interconectados.

14.1 Vulnerabilidades de Seguridad Críticas.

14.1.1 Ausencia de Segmentación de Red

La **ausencia total de segmentación mediante VLANs** representa el riesgo más significativo identificado. Esta condición crea un entorno de red completamente plano donde cualquier brecha de seguridad puede propagarse sin restricciones a través de todos los módulos interconectados, comprometiendo la integridad de toda la infraestructura organizacional.

14.1.2 Protocolos de Gestión Inseguros

La gestión de equipos de red mediante protocolos inseguros como **Telnet y HTTP** expone credenciales administrativas críticas durante la transmisión. Esta práctica representa una vulnerabilidad de alto riesgo que facilita el acceso no autorizado a la infraestructura de red.

14.2 Deficiencias de Infraestructura Física.

14.2.1 Deterioro del Cableado Estructurado

La infraestructura física evidencia un **deterioro significativo en el cableado de fibra óptica**, afectando la confiabilidad y rendimiento de las comunicaciones entre módulos. Esta degradación compromete la continuidad operativa y requiere intervención correctiva inmediata.

14.2.2 Sistemas de Protección Eléctrica Deficientes

La **ausencia de sistemas de puesta a tierra** en seis de los siete módulos constituye una deficiencia crítica que expone tanto los equipos tecnológicos como al personal a riesgos eléctricos. Esta condición viola estándares de seguridad y puede ocasionar daños materiales significativos.

14.3 Impacto Operacional

La combinación de vulnerabilidades lógicas y físicas identificadas crea un **escenario de riesgo elevado** que compromete:

- **Continuidad del servicio**: Vulnerabilidad ante fallos en cascada
- **Integridad de datos**: Exposición a accesos no autorizados
- **Escalabilidad**: Limitaciones para crecimiento futuro
- **Cumplimiento normativo**: Incumplimiento de estándares de seguridad

Esta evaluación confirma la necesidad de una **intervención inmediata y planificada** para mitigar los riesgos identificados y establecer una base sólida para el crecimiento futuro de la infraestructura tecnológica de AUTODEMA.

15. DISPOSITIVOS UBICADOS EN LA RED.

15.1 Centro de Datos

El Centro de Datos es el núcleo principal de la infraestructura tecnológica de AUTODEMA, ubicado en el Módulo 4, y actúa como el corazón de toda la red institucional. Este espacio alberga los dispositivos más críticos que soportan los servicios esenciales para el funcionamiento de la organización.

Ilustración 14: Gabinete del servidor

Referencia: Foto tomada por los autores del documento

HPE LAMERICA: HPE (Hewlett Packard Enterprise) en Latinoamérica (LAMERICA) ofrece una gama de soluciones y servicios diseñados para transformar la gestión de TI desde el extremo hasta la nube.

Ilustración 15: HPE LAMERICA

Referencia: Imagen tomada de internet

Ilustración 16: HPE LAMERICA AUTODEMA

Referencia: Foto tomada por los autores del documento

Gabinete del Router Distribucion: La funcion principal de esto es desibuir la red a lo largo de AUTODEMA, distribuyendo la red.

Ilustración 17: Gabinete de la sala de servidores

Referencia: Foto tomada por los autores del documento

Access Point: Brinda una linea de internet para cada módulo a fin de evitar la saturación de red.

Ilustración 18: Access Point

Referencia: Foto tomada por los autores del documento

15.2 Zona de UPS

La Zona de UPS (Uninterruptible Power Supply) es un componente crítico dentro de la infraestructura tecnológica de AUTODEMA, especialmente en el Centro de Datos del Módulo 4. Esta zona asegura la continuidad del suministro eléctrico a los equipos sensibles, como servidores, switches y firewalls, incluso en caso de fallos o interrupciones en la red eléctrica principal.

Ilustración 19: UPS

Referencia: Foto tomada por los autores del documento

Ilustración 20: Transformador de almacenamiento

Referencia: Foto tomada por los autores del documento

Ilustración 21: conexión de energía sala de servidores

Referencia: Foto tomada por los autores del documento

16. INFRAESTRUCTURA DE SERVIDORES DE AUTODEMA

16.1 Descripción General

Según el Ingeniero responsable, la infraestructura de servidores de AUTODEMA ha sido diseñada para soportar una variedad de servicios críticos, incluyendo funcionalidades de correo electrónico, Internet de las Cosas (IoT) y un robusto sistema de almacenamiento.

16.2 Servicios Implementados

La infraestructura de servidores de AUTODEMA habilita los siguientes servicios clave:

- **Bases de Datos:** Ofrece almacenamiento centralizado para la información más crítica de la organización.
- **Correo Electrónico:** Cuenta con servidores POP3, IMAP y SMTP para asegurar una mensajería fluida y confiable
- **Web y Aplicaciones:** Proporciona servidores HTTP y FTP para alojar servicios web y facilitar la transferencia de archivos.

16.3 Red y Comunicaciones

- **DHCP:** Gestiona la asignación dinámica de direcciones IP.
- **DNS:** Se encarga de la resolución de nombres de dominio.
- **Radius y AAA:** Permite la autenticación, autorización y contabilidad de usuarios para un acceso seguro.
- **TFTP:** Facilita la transferencia de archivos para la configuración de dispositivos de red.
- **Telecomunicaciones:** Se integra con proveedores de servicios de internet (ISSP) como Claro, Movistar y Entel para garantizar la conectividad externa.
- **IoT:** Brinda soporte fundamental para la creciente red de dispositivos del Internet de las Cosas.
- **Seguridad:** Incorpora firewalls para proporcionar protección perimetral.

16.4 Configuración y Recursos

Los servidores de AUTODEMA están configurados con los siguientes recursos esenciales:

- Almacenamiento: Cuentan con discos de 3 TB dedicados a datos y aplicaciones.
- Enrutamiento: Utilizan enrutamiento estático para una gestión eficiente del tráfico de red.
- Redes: Implementan los protocolos TCP/IP para todas las comunicaciones.

16.5 Consideraciones Técnicas

Es importante destacar los siguientes puntos técnicos sobre la infraestructura de servidores:

Aunque los servidores operan con un firewall, se recomienda una evaluación exhaustiva para determinar y aplicar medidas de seguridad adicionales.

Esta infraestructura es vital, ya que soporta tanto las redes de telecomunicaciones como los servicios críticos necesarios para la operación diaria de AUTODEMA.

17. SEGURIDAD

La infraestructura de red de AUTODEMA presenta **vulnerabilidades críticas** tanto en la **seguridad física** como **lógica**. Esto incrementa significativamente los riesgos de ataques cibernéticos, interrupciones operativas y acceso no autorizado.

1. Seguridad Física
Estado Actual:

- **Cableado y Gabinetes:**
  - El cableado de fibra óptica está en mal estado, con empalmes deficientes y conectores deteriorados.
  - Los gabinetes, particularmente en el Módulo 3, están desorganizados.
  - Hay una falta de etiquetado en los patch panels.

- **Energía y Tierra:**
  - Solo el servidor principal cuenta con tres pozos a tierra; los demás módulos carecen de este sistema.
  - Existe un grupo electrógeno de respaldo (gasolina), pero no hay UPS en todos los módulos.

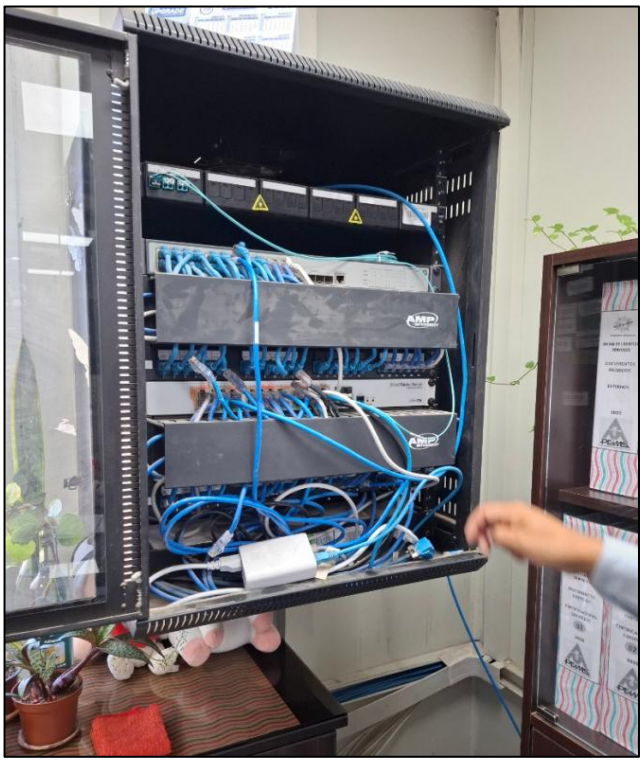


Ilustración 22: Gabinete modulo 2

Referencia: Foto tomada por los autores del documento

Riesgos:

- Interrupción de servicios debido a fallas eléctricas o daños en el cableado.
- Acceso físico no autorizado a gabinetes críticos (por ejemplo, el centro de datos).

Recomendaciones:

- Implementar puestas a tierra en todos los módulos.
- Reemplazar el cableado dañado y organizar los gabinetes con etiquetas claras.
- Instalar UPS en módulos clave para prevenir cortes de energía.

2. Seguridad Lógica.

Gestión de Red:

- Se utilizan protocolos inseguros (Telnet y HTTP) para administrar switches y routers.
- Hay una ausencia de SSH/HTTPS para conexiones cifradas.

Segmentación:

- No existen VLANs, lo que permite tráfico libre entre todos los dispositivos.
- Los switches operan como hubs, sin ninguna configuración de seguridad.

Protección Perimetral:

- Solo se cuenta con un firewall básico como única defensa efectiva.
- No se dispone de IDS/IPS para detectar intrusiones en tiempo real.

Riesgos:

- Interceptación de credenciales debido al uso de Telnet/HTTP.
- Propagación de malware facilitada por la falta de VLANs.
- Vulnerabilidad a ataques DDoS sin mitigación automática.

Recomendaciones:

- Migrar a SSH/HTTPS para una gestión remota segura.
- Implementar VLANs para aislar el tráfico (por ejemplo, administración, IoT, usuarios).
- Configurar port security, DHCP snooping y 802.1X en los switches.
- Desplegar un sistema IDS/IPS para un monitoreo proactivo de intrusiones.

3. Acceso Remoto y Autenticación
Estado Actual:

- VPN: Actualmente no existe una solución VPN para acceso remoto seguro.
- Autenticación: Se utilizan credenciales predeterminadas en algunos dispositivos.

Riesgos:

- Exposición de servicios internos a internet.
- Vulnerabilidad a ataques de fuerza bruta debido a contraseñas débiles.

Recomendaciones:

- Implementar una VPN corporativa (por ejemplo, OpenVPN o IPsec).
- Aplicar políticas de contraseñas complejas y configurar autenticación multifactor (MFA).

18. PROPUESTA

18.1 Asignación de Swtiches con SVI

Tabla 43: Asignación de Switches con SVI

Modulo	Switch con SVI	Observación
M1	PRINCIPAL	SVI en SW principal
M2	PRINCIPAL	SVI en SW principal
M3	PRINCIPAL	SVI en SW principal
M4	PRINCIPAL	SVI en SW principal
M5	PRINCIPAL	SVI en SW principal
M6	PRINCIPAL	SVI en SW principal
M7	PRINCIPAL	SVI en SW principal
Almacen	M4	Acceso local en M4
OCI	M4	Acceso local en M4
OPIP	M4	Acceso local en M4

Referencia: Otorgado por AUTODEMA

18.2 Tabla de direccionamiento

Tabla 44: Tabla de direccionamiento

Modulo	Switch central	Interfaz (Central ↔ Modulo)
M1	PRINCIPAL	Gi1/0/1 (PRINCIPAL) ↔ Gi1/0/1 (M1)
M2	PRINCIPAL	Gi1/0/2 (PRINCIPAL) ↔ Gi1/0/1 (M2)
M3	PRINCIPAL	Gi1/0/3 (PRINCIPAL) ↔ Gi1/0/1 (M3)
M4	PRINCIPAL	Gi1/0/5 (PRINCIPAL) ↔ Gi1/0/1 (M4)
M5	PRINCIPAL	Gi1/0/3 (PRINCIPAL) ↔ Gi1/0/1 (M5)
M6	PRINCIPAL	Gi1/0/4 (PRINCIPAL) ↔ Gi1/0/1 (M6)
M7	PRINCIPAL	Gi1/0/2 (PRINCIPAL) ↔ Gi1/0/1 (M7)
Almacen	M4	Gi1/0/3 (M4) ↔ Gi1/0/1 (ALMACÉN)
OCI	M4	Gi1/0/4 (M4) ↔ Gi1/0/1 (OCI)
OPIP	M4	Gi1/0/5 (M4) ↔ Gi1/0/1 (OPIP)

Referencia: Otorgado por AUTODEMA

18.3 Tabla de direcciones IPs

Tabla 45: Tabla de direcciones IPs

Módulo	VLAN	Red /25	Gateway HSRP
MOD1	10	172.16.0.0/25	172.16.0.1
MOD2	20	172.16.0.128/25	172.16.0.129
MOD3	30	172.16.1.0/25	172.16.1.1
MOD4	40	172.16.1.128/25	172.16.1.129
MOD5	50	172.16.2.0/25	172.16.2.1
MOD6	60	172.16.2.128/25	172.16.2.129
MOD7	70	172.16.3.0/25	172.16.3.1
ALMACEN	80	172.16.3.128/25	172.16.3.129
OCI	90	172.16.4.0/25	172.16.4.1
OPIP	100	172.16.4.128/25	172.16.4.129
Servidor	105	172.16.5.0/28	172.16.5.254
ASA	33	172.16.33.0/30	172.16.33.1

Referencia: Otorgado por AUTODEMA

18.4 Topología

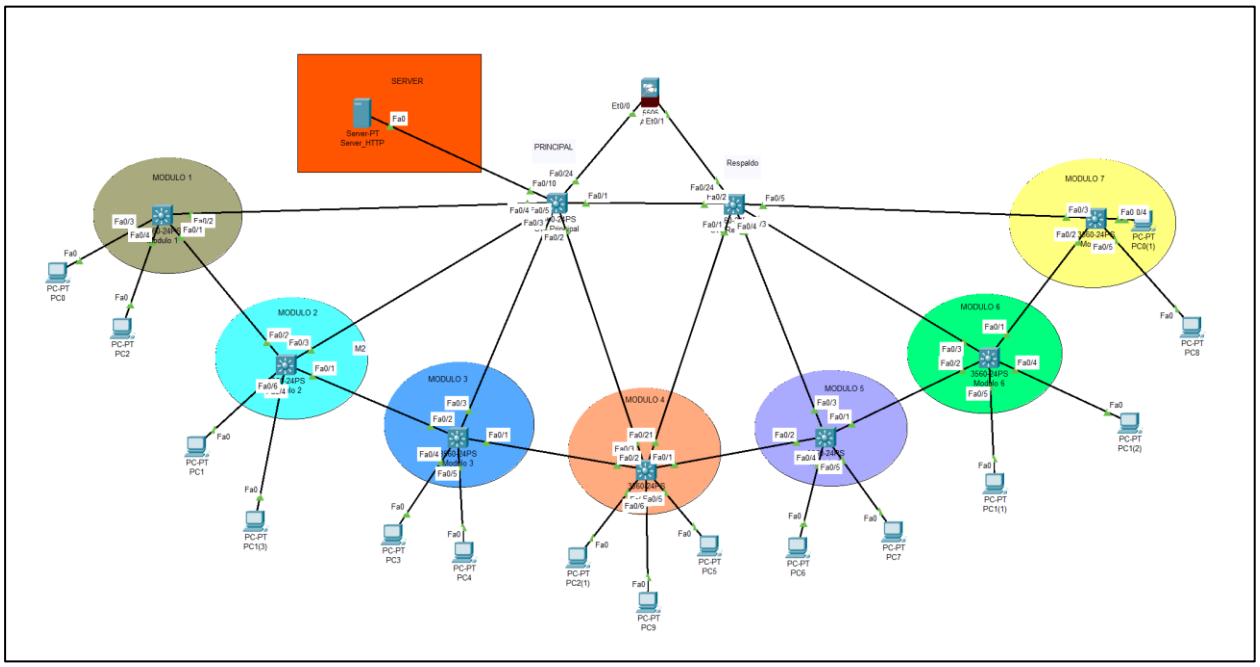


Ilustración 23: Topología física de la Propuesta

Referencia: Realizada por los autores del documento

19. CONFIGURACIÓN PROPUESTA

19.1 TOPOLOGÍA Y COMPONENTES

1. Dispositivos principales:

- Switch Principal (Layer 3) - Router de distribución principal
- Switch Respaldo (Layer 3) - Redundancia con HSRP
- Firewall ASA 5505 - Seguridad perimetral y NAT
- Servidor - IP: 172.16.5.2

2. Módulos de acceso (Layer 2):

- MOD1, MOD2, MOD3, MOD4, MOD5, MOD6, MOD7
- ALMACEN, OCI, OPIP

19.2 CONFIGURACIONES PROPUESTAS

1. Protocolos de Alta Disponibilidad

1.1.HSRP (Hot Standby Router Protocol)

- Switch Principal: Prioridad 110 (Activo)
- Switch Respaldo: Prioridad 100 (Standby)
- Gateway virtual compartido en todas las VLANs
- Preempt habilitado para failover automático

1.2.STP (Spanning Tree Protocol)

- Principal: Root bridge primario (Prioridad 4096)
- Respaldo: Root bridge secundario (Prioridad 8192)
- Prevención de bucles en topología redundante

2. Servicios de Red Implementados

2.1.HTTP/HTTPS

- Servidor web interno en 172.16.5.2
- Acceso desde todas las VLANs internas
- Navegación web externa via NAT

2.2.FTP (File Transfer Protocol)

- Servidor FTP en servidor principal
- Transferencia de archivos entre departamentos
- Acceso controlado por VLANs

2.3.DNS (Domain Name System)

- DNS primario: 8.8.8.8 (Google)
- DNS secundario configurado en servidor local
- Resolución de nombres para navegación

2.4.POP3/SMTP (Correo Electrónico)

- Servidor de correo en 172.16.5.2
- POP3 para recepción de mensajes
- SMTP para envío de correos
- Configuración por departamentos

3. Conectividad y Routing

3.1.NAT (Network Address Translation)

- Configuración: nat (inside,outside) dynamic interface
- Traducción automática de IPs privadas
- Acceso a Internet para todos los usuarios

3.2.Rutas Estáticas

- Ruta a DNS Google: 8.8.8.8 via 172.16.33.1
- Ruta a servicios Google: 142.250.0.0/16
- Default route hacia Internet via ASA

4. Servicios de Mensajería

4.1.Instant Messaging

- Chat interno entre departamentos
- Servidor de mensajería en VLAN servidor
- Comunicación en tiempo real

4.2.DHCP (Opcional)

- Asignación automática de IPs por VLAN
- Reservas para dispositivos críticos
- Configuración centralizada

5. Protocolos de Seguridad

5.1.ACLs en Firewall

- Traffic inside → outside: PERMITIDO
- Traffic outside → inside: DENEGADO (por defecto)
- Protección contra amenazas externas

5.2.VLANs y Segmentación

- Aislamiento de tráfico por departamentos
- Control de broadcast domains
- Políticas de acceso diferenciadas

19.3 SEGURIDAD BÁSICA

1. Contraseñas estándar en todos los dispositivos:

- Enable secret: cisco
- Console password: red
- VTY password: red

2. Firewall ASA:

- Interface inside: Nivel de seguridad 100
- Interface outside: Nivel de seguridad 0
- ACL permitiendo tráfico saliente

19.4 CONECTIVIDAD

1. Switches de Acceso

- Puertos troncales: FastEthernet0/1, 0/2 y 0/3
- Encapsulación: 802.1Q

2. Rutas estáticas

- DNS servicios: ip route 8.8.8.8 255.255.255.255 172.16.33.1
- Google services: ip route 142.250.0.0 255.255.0.0 172.16.33.1

19.5 VENTAJAS DE LA IMPLEMENTACIÓN

Beneficios Operacionales

- Alta Disponibilidad: Sin interrupciones por falla de equipos
- Escalabilidad: Fácil adición de nuevos módulos/usuarios
- Segmentación: Control granular del tráfico por departamento
- Rendimiento: Reducción de dominios de colisión y broadcast

Beneficios de Seguridad

- Perímetro Protegido: Firewall ASA como barrera de seguridad
- Acceso Controlado: VLANs limitan comunicación no autorizada
- Monitoreo Centralizado: Logs y estadísticas en puntos clave
- Redundancia: Doble path para servicios críticos

Beneficios de Conectividad

- Internet Compartido: NAT eficiente para todos los usuarios
- Servicios Unificados: Correo, web, FTP centralizados
- Comunicación Interna: Chat y mensajería entre departamentos
- Acceso Remoto: Preparado para VPN y acceso externo

20. NORMATIVAS DE SEGURIDAD E INFRAESTRUCTURA

Gestión de Contraseñas y Accesos

NORMA 001 - Política de Contraseñas

- Cambio obligatorio de contraseñas cada 90 días.
- Contraseñas mínimas de 8 caracteres con mayúsculas, minúsculas y números.
- Prohibido usar contraseñas por defecto (ej. cisco, red).
- Implementar autenticación de doble factor para acceso administrativo.

NORMA 002 - Control de Acceso Físico

- Acceso restringido al cuarto de servidores y equipos de red.
- Registro de entrada/salida de personal técnico.
- Videovigilancia 24/7 en áreas críticas de infraestructura.
- Llaves/tarjetas de acceso solo para personal autorizado.

Monitoreo y Mantenimiento

NORMA 003 - Monitoreo Continuo

- Revisión diaria de logs del Firewall ASA.
- Monitoreo de estado HSRP cada 4 horas.
- Verificación semanal de conectividad entre VLANs.
- Alertas automáticas por caída de servicios críticos.

NORMA 004 - Mantenimiento Preventivo

- Actualización de firmware de equipos cada 6 meses.
- Limpieza física de equipos mensualmente.
- Verificación de ventilación y temperatura semanalmente.
- Pruebas de failover HSRP trimestralmente.

Respaldo y Recuperación

NORMA 005 - Backup de Configuraciones

- Respaldo automático de configuraciones cada 24 horas.
- Almacenamiento de backups en servidor externo seguro.
- Versionado de configuraciones con fecha y responsable.
- Pruebas de restauración mensuales.

NORMA 006 - Plan de Contingencia

- Procedimiento documentado para falla de switch principal.
- Tiempo máximo de recuperación: 15 minutos.
- Personal de guardia disponible 24/7 para emergencias.
- Equipos de repuesto disponibles en sitio.

Seguridad de Red

NORMA 007 - Firewall y ACLs

- Revisión mensual de reglas del firewall.
- Eliminación trimestral de reglas no utilizadas.
- Documentación obligatoria de cambios en ACLs.
- Principio de menor privilegio en todas las reglas.

NORMA 008 - Segmentación de VLANs

- Prohibido crear VLANs sin autorización del administrador.
- Documentación de usuarios por VLAN actualizada mensualmente.
- Pruebas de aislamiento entre VLANs cada 6 meses.
- Monitoreo de tráfico inter-VLAN sospechoso.

Gestión de Cambios

NORMA 009 - Control de Cambios

- Toda modificación requiere solicitud formal aprobada.
- Ventana de mantenimiento: Domingos 2:00-6:00 AM.
- Rollback plan obligatorio para cambios críticos.
- Documentación post-cambio en 24 horas.

NORMA 010 - Gestión de Incidentes

- Clasificación de incidentes: Crítico, Alto, Medio, Bajo.
- Respuesta a incidentes críticos: máximo 30 minutos.
- Documentación completa de resolución de problemas.
- Análisis post-incidente para prevenir recurrencias.

Cumplimiento y Auditoría

NORMA 011 - Auditorías de Seguridad

- Auditoría interna trimestral de configuraciones.
- Auditoría externa anual de seguridad de red.
- Pruebas de penetración semestrales.
- Corrección de vulnerabilidades en 48 horas.

NORMA 012 - Documentación Técnica

- Actualización de diagramas de red tras cada cambio.
- Manual de procedimientos actualizado mensualmente.
- Inventario de equipos y licencias al día.
- Registro de configuraciones con control de versiones.

Capacitación y Personal

NORMA 013 - Competencias del Personal

- Certificación mínima CCNA para administradores.
- Capacitación anual en nuevas tecnologías.
- Entrenamiento en procedimientos de emergencia.
- Evaluación técnica semestral del equipo.

NORMA 014 - Responsabilidades Definidas

- Administrador principal y respaldo asignados.
- Matriz RACI para tareas críticas de red.
- Procedimiento de escalamiento bien definido.
- Contactos de emergencia actualizados.

Cumplimiento Regulatorio

NORMA 015 - Protección de Datos

- Cifrado de datos sensibles en tránsito.
- Logs de acceso conservados por 12 meses.
- Política de retención de información definida.
- Cumplimiento con normativas locales de privacidad.

21. AGRADECIMIENTOS

El reconocimiento a los creadores de redes de computadoras es fundamental, ya que su visión y avances han permitido el desarrollo de tecnologías críticas como OSPF, esenciales para la gestión y el enrutamiento eficiente de grandes redes. Su trabajo ha revolucionado la forma en que se interconectan los sistemas, habilitando el monitoreo, la seguridad, y la escalabilidad de redes empresariales en un mundo cada vez más digital. Gracias a ellos, hoy podemos disfrutar de una comunicación fluida y confiable a nivel global.

Extendemos nuestro reconocimiento a los ingenieros de redes de la Universidad Católica de Santa María por su excelente labor docente en el curso Computación Red III. Su claridad, compromiso y apoyo constante fueron claves en nuestra formación.

22. CONCLUCIONES

La infraestructura de red de AUTODEMA está organizada en una topología modular con siete módulos interconectados mediante fibra óptica, lo cual permite una distribución lógica del tráfico. Sin embargo, se identificó la falta de implementación de VLANs y el uso de protocolos inseguros como Telnet y HTTP, lo que expone la red a riesgos operativos y cibernéticos. Se propuso la implementación de interfaces VLAN virtuales (SVI) en los switches principales para mejorar la segmentación, control del tráfico y seguridad.

El análisis del direccionamiento IP reveló un bajo aprovechamiento del espacio de red disponible, utilizando menos del 4% del total. Esto indica que existe capacidad suficiente para escalar sin modificar el esquema actual, siempre que se realice una planificación más estructurada y estandarizada del uso de las direcciones IP, incluyendo asignaciones dinámicas con DHCP y reservas para dispositivos críticos.

En cuanto a la seguridad física y lógica, se encontraron deficiencias importantes: cableado desorganizado, etiquetado inadecuado, falta de sistemas de puesta a tierra en varios módulos y acceso débilmente controlado al centro de datos. Para corregir esto, se recomienda adoptar normativas técnicas claras basadas en estándares internacionales como ISO/IEC 27001, implementar políticas estrictas de contraseñas, autenticación de doble factor, monitoreo continuo de logs y capacitación técnica continua del personal encargado de la gestión de la red.

23. REFERENCIAS

Ciberseguridad. (s. f.). https://www.oas.org/ext/es/seguridad/prog-ciber

AUTODEMA – Proyecto Especial Majes Siguas – Proyecto Especial Majes Siguas – Recursos Hidricos – PEMSII –. (s. f.). https://www.autodema.gob.pe/

24. ANEXOS

Enlace de documentos relacionados al desarrollo del trabajo.
https://github.com/SantiagoCusirramosChiri/Redes2/tree/main/F3/P6%20-%20Diario_Ingeniera

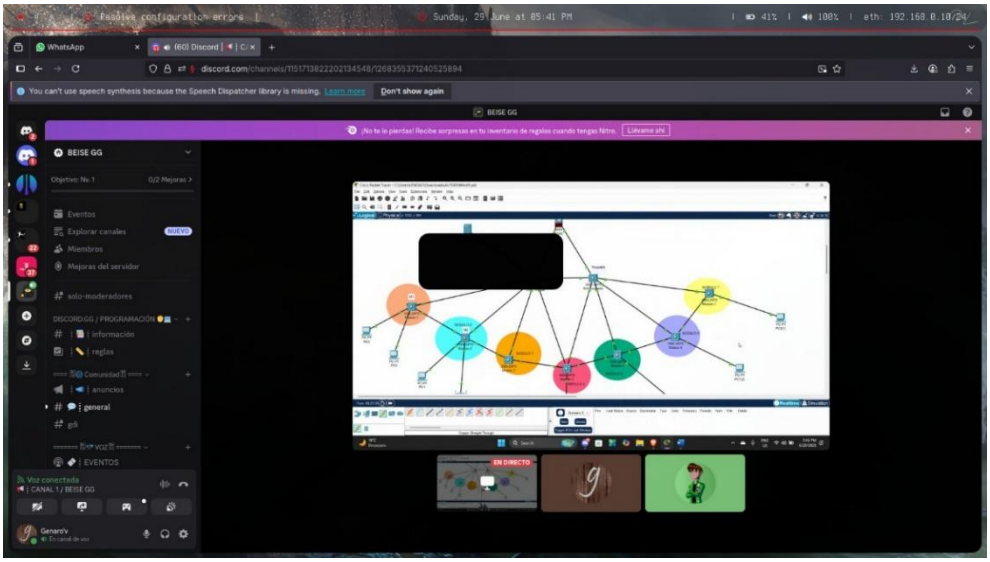


Ilustración 24: Reunión en plataforma Discord

Referencia: Foto tomada por los autores del documento

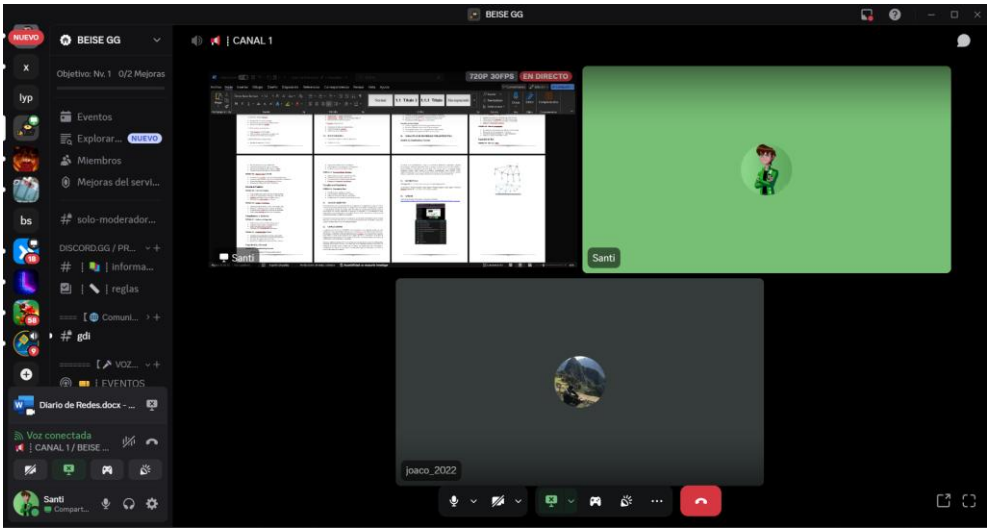


Ilustración 25: Reunión en plataforma Discord

Referencia: Foto tomada por los autores del documento

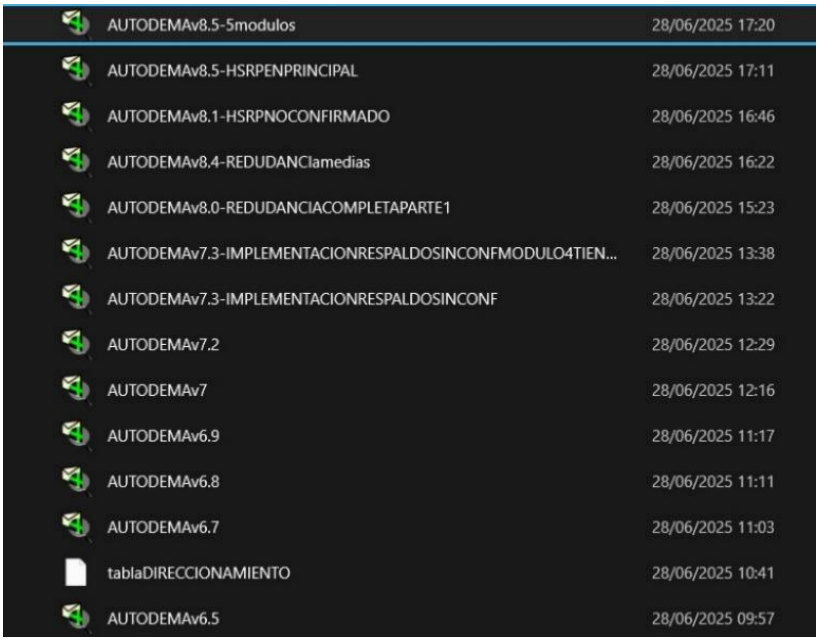


Ilustración 26: Versiones de la Propuesta

Referencia: Realizada por los autores del documento

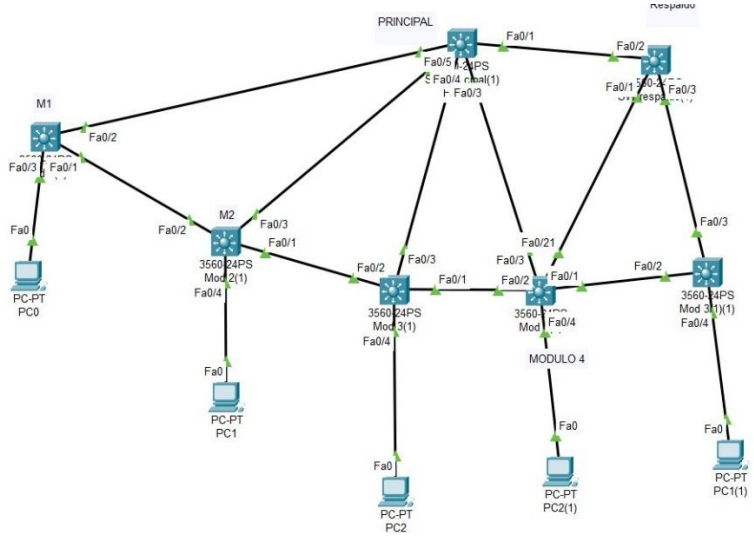


Ilustración 27: Boceto de la Propuesta

Referencia: Realizada por los autores del documento

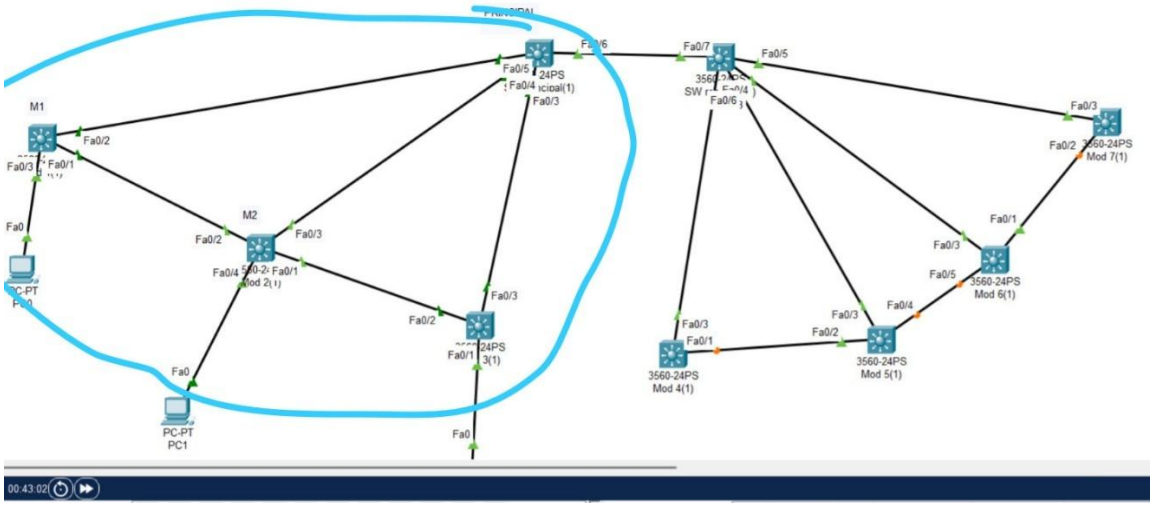


Ilustración 28: Boceto de la Propuesta

Referencia: Realizada por los autores del documento