



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Optimización de la infraestructura de red LAN y
WAN, para las empresas del grupo Inversiones Educa
S.A. basado en la metodología PPDIOO Cisco**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Miguel Angel TORIBIO SARMIENTO

ASESOR

Raúl Marcelo ARMAS CALDERÓN

Lima, Perú

2021



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Toribio, M. (2021). *Optimización de la infraestructura de red LAN y WAN, para las empresas del grupo Inversiones Educa S.A. basado en la metodología PPDIOO Cisco*. [Trabajo de Suficiencia Profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Miguel Angel Toribio Sarmiento
DNI	46580775
URL de ORCID	https://orcid.org/0000-0002-1496-3348
Datos de asesor	
Nombres y apellidos	Raúl Marcelo Armas Calderón
DNI	07156168
URL de ORCID	https://orcid.org/0000-0003-4624-3705
Datos de investigación	
Línea de investigación	- Redes de Datos - Tecnologías IP - Gestión de los Sistemas informáticos y de la información
Grupo de investigación	GI12 INFRAESTRUCTURA TECNOLÓGICA, REDES DE COMUNICACIONES, SEGURIDAD INFORMÁTICA, SEGURIDAD DE LA INFORMACIÓN
Agencia de financiamiento	Financiamiento Propio
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Carabayllo Latitud: -11.897608 Longitud: -77.034982

Año o rango de años en que se realizó la investigación	Abril 2019 – Agosto 2019
URL de disciplinas OCDE	Ingemiería de Sistemas y Comunicaciones https://purl.org/perepo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05 Hardware, Arquitectura de computadoras https://purl.org/pe-repo/ocde/ford#2.02.06



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 19:00 horas del día 21 de julio del año 2021, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Ing. Rodríguez Rodríguez Ciro (Presidente), Ing. Cordero Sánchez Hugo Rafael (Miembro) y el Ing. Armas Calderón Raúl Marcelo (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/kgf-nfym-mzu>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE RED LAN Y WAN, PARA LAS EMPRESAS DEL GRUPO INVERSIONES EDUCA S.A. BASADO EN LA METODOLOGÍA PPDIOO CISCO”**, por el Bachiller **Toribio Sarmiento Miguel Angel**; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de **16 DIECISÉIS**.

A continuación el Presidente de Jurados el Ing. Rodríguez Rodríguez Ciro, declara al Bachiller **Ingeniero de Sistemas**.

Siendo las 19:55horas, se levantó la sesión.

Presidente

Ing. Rodríguez Rodríguez Ciro

Miembro

Ing. Cordero Sánchez Hugo Rafael

Miembro Asesor

Ing. Armas Calderón Raúl Marcelo

Dedicatoria

A mis Padres por todo el apoyo, dedicación
Valores inculcados y todo su amor que me
brindaron,

Y a mis hijos por ser la motivación más grande
que uno puede tener.

AGRADECIMIENTO:

Agradecer a mis padres por darme todo y acompañarme en cada etapa importante de mi vida, A mi hermano por sus consejos en cada decisión y proyecto emprendido.

A mi esposa y a mis hijos por todo su apoyo y motivación brindado.

TABLA DE CONTENIDO

Índice de Figuras	5
Índice de Tablas	7
RESUMEN	9
INTRODUCCION	11
CAPITULO I - TRAYECTORIA PROFESIONAL	12
CAPITULO II - CONTEXTO EN EL QUE SE DESAROLLO LA EXPERIENCIA	20
2.1 EMPRESA - ACTIVIDAD QUE REALIZA	20
2.2 VISION	21
2.3 MISION	21
2.4 ORGANIZACION DE LA EMPRESA	21
2.5 AREA, CARGO Y FUNCIONES DESEMPEÑADAS	22
2.6 EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN	22
CAPITULO III - ACTIVIDADES DESARROLLADAS	23
3.1 SITUACION PROBLEMÁTICA	23
3.1.1 DEFINICION DEL PROBLEMA	23
3.2 SOLUCION	24
3.2.1 OBJETIVOS	24
3.2.2 ALCANCE	25
3.2.3 ETAPAS Y METODOLOGIA	27
3.2.4 FUNDAMENTOS UTILIZADOS	34
3.2.5 PLANIFICACION,DISEÑO E IMPLEMENTACION DE UNA RED CORPORATIVA LAN Y WAN HACIENDO USO DE BUENAS PRACTICAS	50
3.3 EVALUACION	143
3.3.1 EVALUACION ECONOMICA	143
CAPITULO IV. REFLEXION CRITICA DE LA EXPERIENCIA	148
4.1 APORTE/LECCIONES APRENDIDAS/EN QUE SE PUEDE MEJORAR	148
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	149
5.1 CONCLUSIONES	149
5.2 RECOMENDACIONES	149
FUENTES DE INFORMACIÓN	150
GLOSARIO	151
ANEXOS – Documentación Adicional	152

INDICE DE FIGURAS

Figura 1. "Organigrama Inversiones Educa S.A"	21
Figura 2. "Organigrama Área TI - Inversiones Educa S.A."	25
Figura 3. Lima Metropolitana	26
Figura 4. Dirección Fiscal Inversiones Educa. S.A	26
Figura 5. Cisco PPDIOO Ciclo de Vida de una RED	27
Figura 6. Metodología Agile SCRUM	31
Figura 7. Modelo Jerárquico Cisco inc	34
Figura 8. Modelo Enterprise Campus Cisco inc	35
Figura 9. Clases de Direcccionamiento IP Privado	38
Figura 10. Protocolo HSRP Funcionamiento	39
Figura 11. Calidad de servicio Telefonía Voip	41
Figura 12. Funcionamiento sdwan	42
Figura 13. Tipos de Tecnologías WAN	43
Figura 14. Tecnología MPLS	45
Figura 15. Zona Desmilitarizada	46
Figura 16. Modelo Top and down – Diseño	47
Figura 17. Topología Full Mesh	47
Figura 18. Componentes Stack	48
Figura 19. Formato Control de Cambios	56
Figura 20. Topología de RED FISICA – WAN IEDUCA	88
Figura 21. Topología de RED SDWAN –IEDUCA	91
Figura 22. Topología de Telefonía IP	93
Figura 23. Calidad de Servicio WAN	99
Figura 23. Grupos de Active Directory	106
Figura 25. Servidores AD Certus	106
Figura 26. Colector FSSO	107
Figura 27. Servidores LDAP – Fortigate	107
Figura 28. Servidores LDAP – ieduca 192.168.7.253	108
Figura 29. VPN SSL – Restricciones por País	108
Figura 30. Sensor IPS	109
Figura 31. Topología DMZ	110
Figura 32. Listado de IPS nateadas	111
Figura 33. Configuración DNS Primario y Secundario	112
Figura 34. Configuración Traffic Shaper – Fortigate	113
Figura 35. Configuración Policy Horarios	113
Figura 36. Configuración Policy Horarios	123
Figura 37. Trafico Interface Eth1/1	124
Figura 38. Cantidad de Errores Físicos – Interface LAN	124
Figura 39. Estatus Etherchannel	125
Figura 40. Cantidad de Paquetes trafico Multicas, Unicast	125
Figura 41. Historial de consumo CPU Sw core	125
Figura 42. Espacio disponible memoria – sw core	126
Figura 43. Listado de Interfaces - sw distribución	126
Figura 44. Trafico Interface troncal hacia sw core	126
Figura 45. Estatus Interfaces PorthChannel – sw distribución	127

Figura 46. Cantidad de Errores Acumulados	127
Figura 47. Cantidad de paquetes trafico multicas y broadcast	128
Figura 48. Historial de consumo Cpu – sw distribución	128
Figura 49. Cantidad de memoria disponible	128
Figura 50. Listado de Interfaces - sw Access	129
Figura 51. Trafico interface troncal sw Access	129
Figura 52. Cantidad de errores físicos – sw Access	130
Figura 53. Cantidad de paquetes de trafico multicast, broadcast	130
Figura 54. Configuración Switches Access modo Stack – Javier Prado	131
Figura 55. Historial consumo cpu – sw Access	131
Figura 56. Cantidad de memoria disponible – sw Access	132
Figura 57. Cantidad VLANS creadas – sw core	132
Figura 58. Configuración STP – sw core	132
Figura 59. Tabla de enrutamiento – sw core	133
Figura 60. Listado de rutas estáticas – sw core	133
Figura 61. Configuración HSRP – Alta disponibilidad SW CORE	133
Figura 62. Cantidad de Vlans – sw distribución	134
Figura 63. Protocolo STP – sw distribución	134
Figura 64. Cantidad de vlans credas – sw Access	134
Figura 65. Protocolo STP – sw Access	135
Figura 66. Usuarios de conexión sw core	135
Figura 67. Usuarios de conexión sw distribución	135
Figura 68. Listas de Accesos – sw distribución	135
Figura 69. Conexión virtual telnet ssh	136
Figura 70. Configuración Interface sw access	136
Figura 71. Configuración Lista de Acceso	136
Figura 72. Conexión virtual telnet ssh – sw Access	137
Figura 73. Usuarios de conexión sw Access	137
Figura 74. Trafico consumo Internet – TLS router principal	140
Figura 75. Consumo de CPU router principal tls	140
Figura 76. Consumo de memoria router principal tls	140
Figura 77. Trafico consumo Internet – CERTUS router principal	141
Figura 78. Consumo de CPU router principal certus	141
Figura 79. Consumo de memoria router principal certus	141
Figura 80. Herramienta de Monitoreo Switches Core Certus - Cacti	142
Figura 81. Trafico consumo de red Router Sede surco – certus	142

INDICE DE TABLAS

Tabla 1. Áreas de Conocimiento y Grupos de procesos PMI	30
Tabla 2. Componentes Básicos de Scrum	31
Tabla 3. Metodología de Diseño PPDIOO	33
Tabla 4. Lista de Entregable	52
Tabla 5. Lista de Entregables	52
Tabla 6. Ítems de Presupuestas	53
Tabla 7. Ítems de Recursos	55
Tabla 8. Descripción de Riesgos	55
Tabla 9. Descripción de Roles	58
Tabla 10. Cronograma de Actividades – 64	66
Tabla 11. Inventario de Servidores - 65	67
Tabla 12. Inventario de Servidores Privados	68
Tabla 13. Inventario de Servidores Públicos	68
Tabla 14. Inventario de Servidores Públicos	69
Tabla 15. Inventario de Segmentos de RED y VLAN	69
Tabla 16. Inventario de Reglas de Firewall	72
Tabla 17. Inventario de Sistemas de Call Center IEDUCA	73
Tabla 18. Inventario de Centrales telefónicas IEDUCA	73
Tabla 19. Inventario de Cámaras IP	75
Tabla 20. Inventario de Dispositivos NVR/DVR	75
Tabla 21. Direcciones de Sedes y Unidades de Negocio	78
Tabla 22. Anchos de banda requeridos Internet y MPLS	79
Tabla 23. Características de Seguridad Firewall	80
Tabla 24. Características de Seguridad Firewall DMZ	80
Tabla 25. Listado Equipos Soporte SMARNET	81
Tabla 26. Listado de comandos CLI	83
Tabla 27. Inventario Equipos Certus sede Principal	86
Tabla 28. Plan de Direccionamiento IP Sedes (molina, chacarilla, surco)	95
Tabla 29. Resumen Sumarizado Direccionamiento IP Sedes IEDUCA	96
Tabla 30. Listado Equipamiento Router	97
Tabla 31. Listado Equipamiento Lan	97
Tabla 32. Listado Equipamiento Firewall y DMZ	98
Tabla 33. Listado Equipamiento Faz y Componentes	98
Tabla 34. Configuración Interface Lan	101
Tabla 35. Perfiles de Navegación WEB	105
Tabla 36. Configuración Interface LAN – Port Security	110
Tabla 37. Cableado Estructurado – Sede TLS Javier Prado	122
Tabla 38. Plantillas de configuración SW CORE	137
Tabla 39. Análisis WAN ICMP	138
Tabla 40. Análisis WAN Internet	139
Tabla 41. Gastos mensuales servicio de internet 2018	143
Tabla 42. Lista de costos por licencia CCVOX	144
Tabla 43. Lista de costos por licencia Genesys	144
Tabla 44. Gastos mensuales servicio de internet 2019	145

FICHA CATALOGRAFICA

OPTIMIZACION DE LA INFRAESTRUCTURA DE RED LAN Y WAN, PARA LAS EMPRESAS DEL GRUPO INVERSIONES EDUCA S.A. BASADO EN LA METODOLOGIA PPDIOO CISCO INC.

AUTOR: TORIBIO SARMIENTO, MIGUEL

ASESOR: ARMAS CALDERON, RAUL

LIMA- PERU, 2021.

TITULO PROFESIONAL: Ingeniero de Sistemas

AREA/PROGRAMA/LINEA DE INVESTIGACION:

Ingenierías / Plataforma TIC / Redes TIC

PREGRADO: Universidad Nacional Mayor de San Marcos – Facultad de Ingeniería de Sistemas e informática – Escuela Profesional de Ingeniería de Sistemas.

Formato 28 x 20 cm

Páginas:165

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Optimización de la infraestructura de red LAN y WAN, para las empresas del grupo
Inversiones Educa s.a. basado en la metodología PPDIOO cisco inc.**

Autor: Toribio Sarmiento, Miguel

Asesor: Armas Calderón, Raúl

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniera
de Sistemas

Fecha: Junio de 2021

RESUMEN

El presente trabajo de suficiencia profesional detalla los pasos que se ejecutaron durante el proyecto de Optimización de la infraestructura de Red Lan y WAN para las empresas del grupo Inversiones Educa S.A., para lo cual se aplicó la Metodología de Diseño PPDIOO de Cisco inc.

El principal objetivo de este proyecto es Optimizar la Red actual que poseen las 3 unidades de negocio Certus, Toulouse, y Ucal en una sola red empresarial que brinde funcionalidades de Alta disponibilidad, tolerancia a fallos, escalabilidad, calidad de servicio y seguridad perimetral.

Adicionalmente esta nueva arquitectura de red brinda la facilidad de compartir recursos entre las 3 empresas sin necesidad de incurrir en gastos operativos o tener que hacer inversiones a largo plazo.

La coyuntura actual de pandemia hizo que muchas empresas den saltos agigantados en inversión para mejorar su infraestructura a nivel de disponibilidad de internet y principalmente reforzar aspectos de seguridad, la nueva red implementada para Inversiones Educa S.A. posee alta resiliencia a este cambio debido a que se implementó la funcionad de SDWAN tecnología que brinda la ventaja de optimizar el uso de internet al tener 2 canales disponibles y en el aspecto de seguridad se reforzó esta capa con 2 firewall perimetrales.

Palabras claves: Optimización, Alta Disponibilidad, PPDIOO, Seguridad Perimetral, SDWAN

**NATIONAL MAJOR UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS ENGINEERING AND INFORMATICS
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING**

**Optimization of the LAN and WAN network infrastructure, for the companies of the
Inversiones Educa S.A group. based on the PPDIOO Methodology cisco inc.**

Author: Toribio Sarmiento, Miguel

Advisor Armas Calderón, Raúl

Title: Work of Professional Sufficiency to opt for the Professional Title of Systems
Engineering

Date: Junio de 2021

ABSTRACT

This work of professional sufficiency details the steps that were executed during the project of Optimization of the Red Lan and WAN infrastructure for the companies of the Inversiones Educa S.A. group, for which the PPDIOO Design Methodology of Cisco Inc.

The main objective of this project is to Optimize the current Network that the 3 Certus, Toulouse, and Ucal business units have in a single business network that provides High availability, fault tolerance, scalability, quality of service and perimeter security functionalities. Additionally, this new network architecture provides the facility to share resources between the 3 companies without incurring operating expenses or having to make long-term investments.

The current pandemic situation made many companies take giant leaps in investment to improve their infrastructure at the level of internet availability and mainly to reinforce security aspects, the new network implemented for Inversiones Educa S.A. It has high resilience to this change due to the fact that the SDWAN technology function was implemented that provides the advantage of optimizing the use of the Internet by having 2 channels available and in the security aspect, this layer was reinforced with 2 perimeter firewalls.

Keywords: Optimization, High Availability, PPDIOO, Perimeter Security, SDWAN

INTRODUCCION

El presente trabajo de experiencia profesional describe el Proyecto de Análisis, Diseño e implementación de una Red LAN y WAN Centralizada, tomando como referencia

La metodología de Diseño PPDIOO de Cisco inc., La funcionalidad de SDWAN de Fortinet inc., y Finalmente para la ejecución del proyecto la metodología de PMI.

Inversiones Educa S.A. brinda soporte Financiero, Logístico y Tecnológico a las 3 Unidades de Negocio del Rubro Educación en el Perú, Integrada por los Institutos Certus, Institutos Toulouse Lautrec y la Universidad UCAL. En este informe nos centraremos en el Análisis, Diseño e Implementación de la Arquitectura de RED Privada, con el fin de buscar optimizar el uso de los recursos entre todas las sedes correspondientes a cada Une y establecer comunicación directa entre todas, gracias a las buenas practicas del modelo Jerárquico establecido por Cisco y durante toda la ejecución del proyecto aplicando las buenas prácticas de la metodología PMI.

El trabajo de suficiencia profesional fue abordado a través del siguiente contenido:

En el CAPITULO I se detalla en orden crónico cargos y tareas desempeñadas, en los diferentes centros de labor público o privado, se precisa también la experiencia laboral generada.

En el CAPITULO II se hace mención a la información correspondiente al Holding educativo del grupo Enfoca, Inversiones Educa S.A. aquí se detalla su organigrama, visión, misión y una breve descripción de los servicios que ofrece.

El CAPITULO III brinda el detalle de las actividades dedicadas a Optimizar la infraestructura de RED LAN y WAN la cual brinde Alta Disponibilidad, escalabilidad, calidad de servicio y seguridad entre todas las Unes de INVERSIONES EDUCA S.A., específicamente el desarrollo del proyecto se basó en el uso de la metodología PPDIOO.

El CAPITULO IV se refiere al aporte del autor, el desarrollo profesional que le demandó, las necesidades que se atendieron, la experiencia y la capacitación requeridas.

El CAPITULO V muestra las conclusiones y recomendaciones finales.

CAPITULO I - TRAYECTORIA PROFESIONAL

1.1 PRESENTACION PROFESIONAL

El autor del presente trabajo cuenta con el grado de Bachiller en la carrera de Ingeniería de Sistemas de la Universidad Nacional Mayor de San Marcos. Cuento con Certificaciones de distintas marcas como Cisco Certified Network Associate (CCNA), Network Security Professional (NSE4), ITIL Foundation, y Scrum Foundation Professional Certificate. Poseo Habilidades en Networking, Servidores, Ejecución de Proyectos con Metodologías Agiles, Ciberseguridad, Telefonía IP, Soluciones de Redes Inalámbricas, Implementación de Data Center, con una trayectoria de más de 5 años de experiencia laboral en el área de Infraestructura & Networking.

1.2 EXPERIENCIA PROFESIONAL

Enero 2019 - Actualidad	INVERSIONES EDUCA S.A. Cargo: Administrador de Red ✓ Administración Networking UNES (CERTUS - UNIVERSIDAD UCAL - TOULOUSE) ✓ Administración Soluciones Inalámbricas Wifi (Aruba, Aironet, Meraki) ✓ Administración Soluciones Colaboración (AVAYA, CISCO) ✓ Administración de Telefonía IP Centrales Telefónicas (AVAYA, CISCO) ✓ Administración de Telefonía VOIP (Genesys, CCVOX) ✓ Administrador de Servidores DHCP, DNS, FTP, ActiveDirectory ✓ Administración de Sistema de Video Vigilancia (DVR, NVR, ALHUA, Cámaras IP DOMO) ✓ Administración de SIP TRUNK, PRIMARIOS E1 ✓ Administración de Equipos WAN (CPE, MEDIA CONVERTER) ✓ Monitoreo de RED herramientas (CACTI, PRTG, ZABBIX)
------------------------------------	---

	✓ Diseño e Implementación de Nuevas Sedes y Data Center, Cuartos de Comunicaciones, Cableado Estructurado. ✓ Análisis de Cobertura de Red Wifi (EKAHAU) ✓ Administración de Servicios Clearpass CPPM, MobilityMaster, Airwave ✓ Atención de Requerimientos e Incidencias. ✓ Gestor de Proyectos de Telecomunicaciones. ✓ Configuración de Equipos LAN - WAN - WIRELESS – TELEFONIA - FIREWALL ✓ Estructuración de Roles y Políticas en equipos de seguridad perimetral (Firewall) ✓ Documentación de procedimientos y diagramas de nuevas implementaciones. ✓ Ejecución de Proyectos Agiles (SCRUM), PMP ✓ Integración de Active Directory – Firewall Fortinet. ✓ Seguridad Perimetral Fortinet (Políticas de Firewall, Nat/Autenticación, Web Filtering/Antivirus, Proxies, Control de Apps, VPN IPSec, VPN SSL, Alta disponibilidad HA).
Octubre 2018 – Marzo - 2019	GRUPO EDUCA_d Cargo: Coordinador de RED ✓ Administrador de RED (SISE - UNIVERSIDAD CIENTÍFICA - USISE) - Atención de Requerimientos e Incidencias. ✓ Gestor de Proyectos de Telecomunicaciones. ✓ Configuración de Equipos LAN - WAN - WIRELESS – TELEFONIA – FIREWALL ✓ Estructuración de Roles y Políticas en equipos de seguridad perimetral (Firewall) ✓ Diseño y Segmentación de Red. ✓ Diseño, Implementación, y Despliegue de Eventos Universitarios. ✓ Troubleshooting y Publicación de servicios.

	✓ Implementación del servicio WiFi Meraki en todas las sedes. ✓ Implementación de servidor tacacs+ basado en Linux (autenticación de ingreso hacia los equipos de comunicaciones). ✓ Documentación de procedimientos y diagramas de nuevas implementaciones. ✓ Migración de Operador Claro a Optical Networks. ✓ Elaboración del Assessment de redes y comunicaciones. ✓ Capacitaciones al personal de redes. ✓ Implementación de nuevas redes (nuevas sucursales tecnología Meraki). ✓ Integración de Active Directory – Firewall Fortinet. ✓ Seguridad Perimetral Fortinet (Políticas de Firewall, ✓ Nat/Autenticación, Web Filtering/Antivirus, Proxies, Control de Apps, VPN IPSec, VPN SSL, Alta disponibilidad HA).
--	--

Septiembre 2017 – Septiembre 2018	CLOUDSOC PERU S.A.C Cargo: INGENIERO DE SOPORTE CORPORATIVO Proyecto: América Móvil S.A. ✓ GRUPO INTERCORP RETAIL (Plaza Vea, Homecenter, Financiera Oh!, oeschle) ✓ Instalaciones, bajas, Upgrade, migraciones de Servicios RPV (VPN), Servicios de Telefonía, Servicios Monitoreo de Red Avanzado en Equipos de diferentes marcas (CISCO Series 2911, 2811, ISR, ASR, GSR, 890 – HUAWEI – ALCATEL Series 7750,7705 – JUNIPER) aplicando Calidad de Servicio QOS, Voip, HSRP, protocolos EIGRP, RIP, BGP, OSPF. ✓ Instalación de Enlaces Microondas en Equipos (CERAGON – NEC – UBIQUITI -CAMBIUM).
--	--

	✓ Instalación y configuración de Routers y Switches en L3 (Ruteo Estático, Dinámico, Alta disponibilidad) en L2 (Vlan, Trunk, Etherchannel, Qos, Balanceo de Carga, Análisis de Redes. ✓ Administración Red WAN / LAN / Centrales Telefónicas. ✓ Coordinación con el personal de mantenimiento, la atención de las averías en las sedes del cliente. ✓ Generación de Tickets de averías, requerimientos y escalamiento ✓ Elaboración de Plan de contingencia y Alta disponibilidad a nivel LAN. ✓ Monitoreo proactivo de enlaces redundantes ✓ Preparar informes y reportes de SLA y Averías Masivas. ✓ Pruebas de redundancia y backups para lograr la alta disponibilidad. Coordinación y Ejecución de Mantenimientos Preventivos en los equipos de red a nivel nacional. ✓ Seguridad Perimetral Fortinet (Políticas de Firewall, Nat/Autenticación, Web Filtering/Antivirus, Proxies, Control de Apps, VPN IPSec, VPN SSL, Alta disponibilidad HA).
Marzo 2017 – Agosto 2017	CORPORACION SAPIA S.A. Cargo: INGENIERO RESIDENTE Proyecto: América Móvil S.A. ✓ GRUPO RIPLEY – GRUPO SAGA FALABELLA (Ripley, Tottus, PROMART, Saga Falabella, Banco Falabella, Banco Ripley). ✓ Instalaciones, bajas, Upgrade, migraciones de Servicios RPV (VPN), Servicios de Telefonía, Servicios Monitoreo de Red Avanzado en Equipos de diferentes marcas (CISCO Series 2911, 2811, ISR, ASR, GSR, 890 – HUAWEI – ALCATEL Series 7750,7705 – JUNIPER) aplicando Calidad de Servicio QOS, Voip, HSRP, protocolos EIGRP, RIP, BGP, OSPF.

	✓ Instalación de Enlaces Microondas en Equipos (CERAGON – NEC – UBIQUITI -CAMBIUM). ✓ Instalación y configuración de Routers y Switches en L3 (Ruteo Estático, Dinámico, Alta disponibilidad) en L2 (Vlan, Trunk, Etherchannel, Qos, Balanceo de Carga, Análisis de Redes. ✓ Administración Red WAN / LAN / Centrales Telefónicas. ✓ Seguimiento a los tickets de atención generados. ✓ Planificación, diseño e implementación de alta disponibilidad y redundancia en la red del cliente. ✓ Elaborar reportes de SLA y Averías Masivas. ✓ Informar diariamente al cliente sobre el estado de su red, coordinando reuniones. presenciales de ser necesario. ✓ Pruebas de redundancia y backups para lograr la alta disponibilidad. Coordinación y Ejecución de Mantenimientos Preventivos en los equipos de red a nivel nacional. ✓ Seguridad Perimetral Fortinet (Políticas de Firewall, Nat/Autenticación, Web Filtering/Antivirus, Proxies, Control de Apps, VPN IPSec, VPN SSL, Alta disponibilidad HA).
--	--

Enero 2015 – Febrero 2017	OESIA PERU SAC Cargo: PROFESIONAL REDES LAN/WAN Proyecto: Telefónica del Perú S.A. INGENIERO RESIDENTE MINERA BROCAL Y MAPFRE
--------------------------------------	---

	✓ Administración del CUCM - Wireless LAN Controller - Access Point ✓ Administración de redes WAN Y LAN ✓ Instalación, Configuración y equipos de comunicaciones (Router, Switches, AP's) ✓ Gestión de Averías y Requerimientos ✓ Manejo de Herramientas de monitoreo (Spectrum – Solarwinds – iDirect – iMonitor- Bifrost – iBuilder – PRTG – Sigmars – HP OPEN View) ✓ Configuración de equipos Cisco para servicios: Internet, IP-VPN, DIGIRED (Telefónica del Perú) para diferentes empresas, aplicando Calidad de Servicio QOS, Voip, HSRP, protocolos EIGRP, RIP, BGP, OSPF. ✓ Gestión de averías desplazamiento de personal de empresas colaboradoras (COBRA.LARI MANTTO, DOMINION). ✓ Telefonía IP Hosteada. ✓ Telefonía IP Gestionada. - LAN Gestionada. ✓ Cumplimiento de SLA. ✓ Elaboración de Backups - Informes Mensuales. ✓ Gestión de garantías RMA CISCO. ✓ Monitorio de Circuitos Digitales (Routers - Switches).
--	--

1.3 FORMACION ACADEMICA

2009 - 2015	Grado Académico Bachiller en Ingeniería de Sistemas – Escuela Académico Profesional en Ingeniería de Sistemas - Facultad de Ingeniería de Sistemas e Informática - Universidad Nacional Mayor de San Marcos.
--------------------	--

1.4 CERTIFICADOS

Septiembre 2020	CCNA: Enterprise Networking, Security, and Automation.
Julio 2020	Introducción to Cybersecurity.
Agosto 2020	Scrum Foundation Professional Certificate.
Enero 2017	CCNA: Switching, Routing, and Wireless Essentials.
Junio 2020	CCNA: Introducción to Networks.
Febrero 2021	NSE 4 Network Security Professional.
Agosto 2017	Itil Foundation Certificate.

1.5 IDIOMAS

2015 - 2016	Británico – Ingles nivel intermedio
--------------------	--

1.6 OTROS CONOCIMIENTOS

PROGRAMACION	Python, JEE, Android, Ruby, Django.
S.O.	Windows 10,9,7, RHEL, Ubuntu, Fedora,CentOS,Debian.
SISTEMAS DE BD	SQL, MYSQL.
VIRTUALIZACION	VMWARE, VEEM, CITRIX.
COLABORACION	AVAYA , CISCO CUCM.

WIFI	ARUBA CPPM, ARUBA Mobility Master, Airwave, Meraki, Aironet.
CENTRALES VOIP	GENESYS, CCVOX,Asterisck.
LICENCIA DE CONducir	Categoría A1.

CAPITULO II - CONTEXTO EN EL QUE SE DESAROLLO LA EXPERIENCIA

2.1. EMPRESA - ACTIVIDAD QUE REALIZA

INVERSIONES EDUCA S.A. es un Holding de sector Educación del Grupo ENFOCA quien brinda soporte TI, FINANZAS, LOGISTICA a sus 3 Unidades de Negocio que son

- ✓ Institutos Certus
- ✓ Institutos Toulouse Lautrec
- ✓ Universidad de Ciencias y Artes de América Latina - UCAL

Datos de Empresa: Razón Social: Inversiones Educa S.A.

Domicilio Legal: Av. Primavera Nro. 970 Santiago de Surco - Lima

Teléfono: 630-7272

RUC: 20544705688

Socios Estratégicos – Vendor

- CISCO
- AVAYA
- FORTINET
- ARUBA / HP
- CISCO MERAKI
- HUAWEI
- ERP SAP FIORI
- VMWARE
- LENOBO

2.2. VISION

Ser líderes en inclusión educativa, innovación académica y crecimiento de negocio
400x600x250.

2.3. MISION

Impulsar a más personas a liberar su potencial para lograr sus objetivos de vida y construir una mejor sociedad.

2.4. ORGANIGRAMA

Organigrama:

A continuación, se muestra en la Figura 1 la Estructura de organización de INVERSIONES EDUCA S.A.

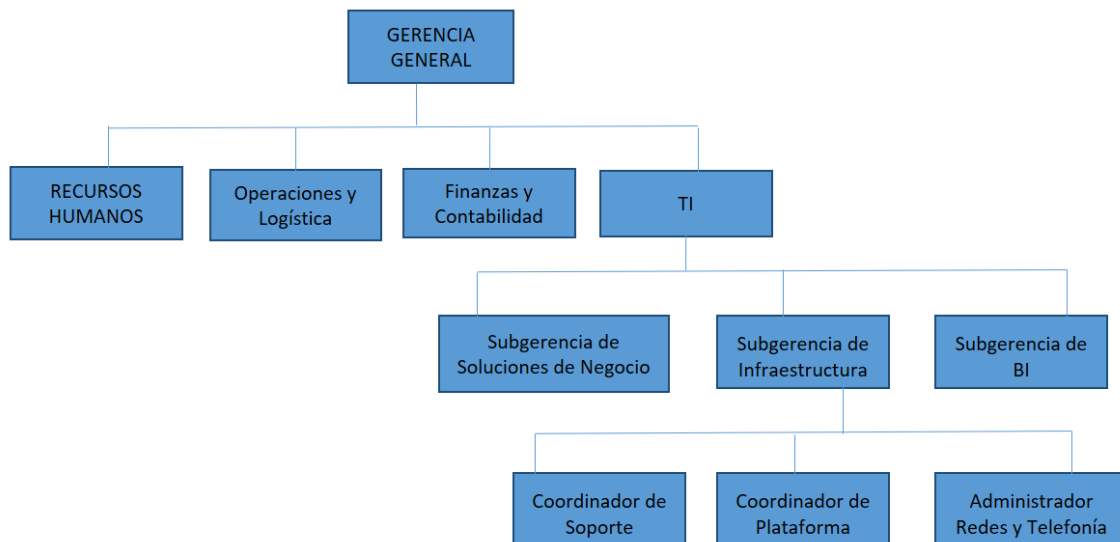


Figura 1. "Organigrama Inversiones Educa S.A."

Fuente: (Intranet Interna – Ieducu 2019)

2.5. AREA, CARGO Y FUNCIONES DESEMPEÑADAS

Durante la ejecución del proyecto el autor del informe se desempeñó como Líder Técnico y a la fecha ocupa el puesto de Administrador de Red, en el área de Infraestructura de INVERIONES EDUCA S.A.

2.6. EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN

Responsabilidades:

- ✓ Realizar el levantamiento de Información de Cada UNEs, Sedes Remotas y Data Center.
- ✓ Análisis y Diseño de nuevo esquema de Direccionamiento IPv4
- ✓ Configuración de Nuevo Esquema de Direccionamiento IPv4 Equipos L2/L3
- ✓ Ordenamiento LAN a nivel del esquema de nuevo Direccionamiento IPv4
- ✓ Orientar al personal de Soporte a configurar las nuevas direcciones IPv4 (FIJA, DINAMICO)
- ✓ Elaborar Checklist Final
- ✓ Elaborar Plan de Trabajo y Plan de Rollback
- ✓ Elaborar Plan de Pruebas
- ✓ Validación de Informes Técnicos Recorrido de Ingreso de Fibra Óptica a cada Sede.
- ✓ Configuración Equipos CORE L3 Direccionamiento IPv4
- ✓ Elaboración de Gantt Final del Proyecto
- ✓ Apoyar al proveedor a realizar la Cross conexión entre equipos Router y Core L3
- ✓ Elaboración de Plan de Pruebas de Conexión
- ✓ Elaboración de Plan de Pruebas de Calidad de Servicio
- ✓ Elaboración de Plan de Pruebas de Alta Disponibilidad
- ✓ Elaboración de Plan de Pruebas de Saturación de BW
- ✓ Elaboración de Plan de Pruebas de Features de Firewall
- ✓ Elaboración de CheckList de comunicación a servicios y Servidores
- ✓ Apoyar al proveedor en Ordenamiento de Políticas IPv4 Firewall
- ✓ Apoyar al proveedor en el levantamiento y depuración de Políticas IPv4 Firewall
- ✓ Apoyar al proveedor en la Ejecución de Enrutamiento hacia sedes Remotas.

CAPITULO III - ACTIVIDADES DESARROLLADAS

3.1. SITUACION PROBLEMÁTICA

3.1.1 DEFINICIÓN DEL PROBLEMA

Inversiones Educa S.A. brinda soporte Financiero, Logístico y Tecnológico a las 3 Unidades de Negocio del Rubro Educación en el Perú, Integrada por los Institutos Certus, Institutos Toulouse Lautrec y la Universidad UCAL.

A partir del año 2019 Inversiones Educa S.A. decide Integrar todas las unidades de negocio en una sola RED PRIVADA debido a que al tener 3 proveedores de Telecomunicaciones los cuales son:

1. Telefónica del Perú brinda servicios de Telecomunicaciones a ITLS. SAC.
2. CenturyLink brinda servicios de Telecomunicaciones a Certus.
3. América Móvil brinda servicios de Telecomunicaciones a UCAL.

Es por esta razón que uno de los grandes problemas que se tiene es la administración de los recursos en cada Unidad de Negocio, así como la gestión de las sedes remotas y los Data Center.

La Arquitectura de red actual no permite compartir recursos como son:

- Centrales Telefónicas
- Soluciones de Wifi Centralizado
- File Server, Bases de Datos
- Aplicaciones
- Sistemas de Video Vigilancia
- Sistemas de Colaboración Video Llamadas

3.2 SOLUCIÓN

Optimizar e Implementar una RED CORPORATIVA LAN y WAN usando la metodología PPDIOO Cisco inc., y para la Gestión del proyecto usar de referencia la metodología de PMI.

3.2.1 OBJETIVOS

OBJETIVO GENERAL

Optimizar la Infraestructura de Red LAN y WAN utilizando la metodología PPDIOO de Cisco inc., para las Unidades de Negocio de la Empresa INVERSIONES EDUCA S.A. del Grupo ENFOCA.

OBJETIVOS ESPECIFICOS

- A. Optimizar el acceso hacia Internet, incrementando su disponibilidad.
- B. Mejora de la Gestión y administración de Sedes Remotas de cada Une.
- C. Brindar la facilidad de compartir recursos entre Unes tales como (Voip, Wifi, FilServer, DB, Colaboración, Video Vigilancia).
- D. Mejora en la capacidad de la RED en relación a tiempos de respuesta, anchos de banda y Escalabilidad.
- E. Mejorar el Nivel de SLA para incidentes y Requerimientos.
- F. Mejora en la Seguridad Perimetral.

3.2.2 ALCANCE

ALCANCE FUNCIONAL

Se define que el alcance funcional para el proyecto corresponde a Operaciones TI e Infraestructura de TI.

ALCANCE ORGANIZACIONAL

La Gerencia de TI, que está conformada por 3 Subgerencias (SOLUCIONES,INFRA,BI), de las cuales la subgerencia de Infraestructura es responsable, la Jefatura de Mesa de Ayuda, la Jefatura de Plataforma de Servidores y la Jefatura de Centro de Datos y Redes.

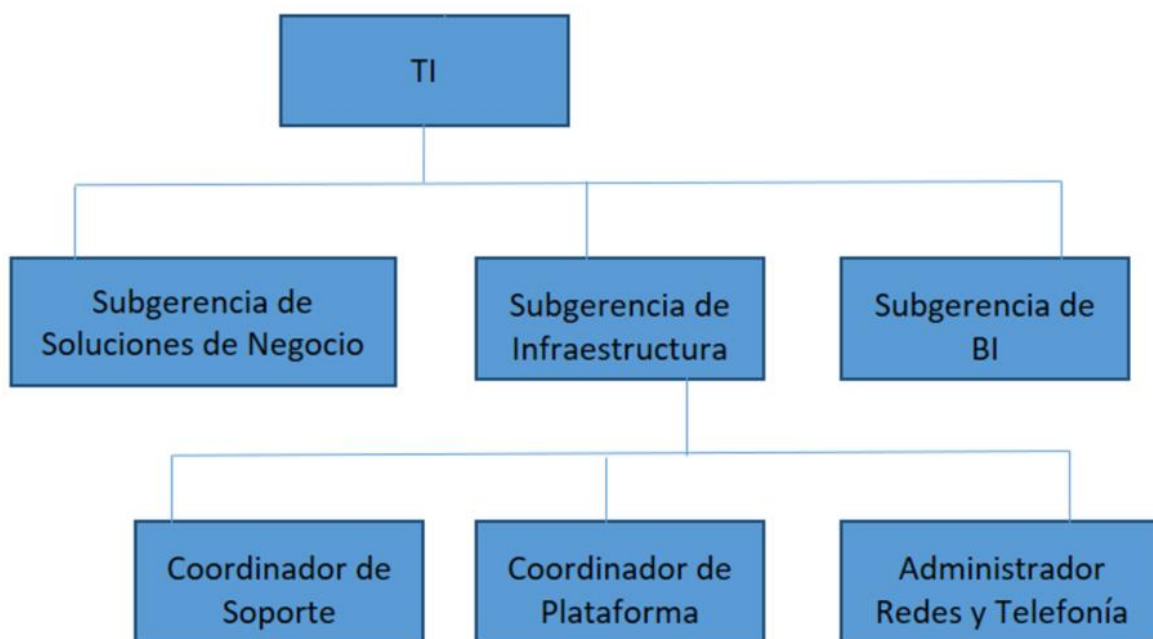


Figura 2. "Organigrama Área TI - Inversiones Educa S.A."

Fuente: (Intranet Interna – Ieducu 2019)

INVERSIONES EDUCA S.A. en Lima, distrito de Santiago de Surco, en la Av. Primavera
Nro. 970



3.2.3 ETAPAS Y METODOLOGÍA

3.2.3.1 Metodología PPDIOO

El Cisco (PPDIOO) define un ciclo continuo de fases en la vida de una red. Cada fase incluye pasos clave para la preparación, planificación, diseño, implementación, operación, y finalmente la optimización. El enfoque de diseño de arriba hacia abajo para el diseño de redes se adapta a la infraestructura de red, a las necesidades de las aplicaciones de red.

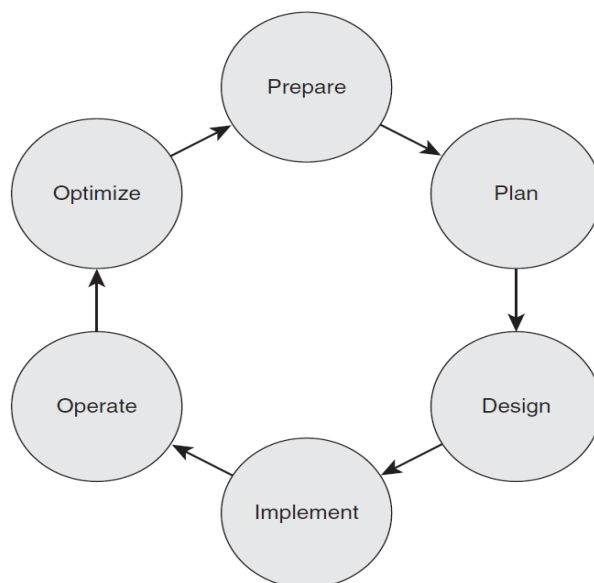


Figura 5. Cisco PPDIOO Ciclo de Vida de una RED
Fuente: (Cisco PPDIO CCDA)

A. Preparación

En esta fase de preparación se identificarán los requisitos y necesidad para el desarrollo de un Nuevo diseño de red.

B. Planificación

Se crea y se pone en marcha el plan a ejecutar durante el Proyecto indica las tareas a realizar en los tiempos establecidos.

C. Diseño

Esta fase del ciclo de vida define la elaboración del diseño a nivel de 3 capas de cisco tomando en cuenta requerimientos técnicos, limitaciones técnicas, objetivos del negocio y limitaciones del negocio.

D. Implementación

Se pone en marcha la implementación y configuración que deben tener los equipos a nivel LAN, WAN y seguridad.

E. Operación

En esta fase se recomienda tener un personal especializado en la verificación de la red ya que es necesario hacer un seguimiento día a día del avance de la red y mostrar posibles fallas del proceso y poder corregirlas.

F. Optimización

En esta fase se identifican y resuelven los daños que afecten a la red. Posiblemente se cree una modificación al diseño si aparecen inconvenientes.

El Cisco PPDIIOO ciclo de vida brinda 4 beneficios esenciales:

- Reducir el costo total del equipamiento.
- Mejorar el nivel de disponibilidad de la arquitectura de red
- Mejorar la agilidad empresarial mediante el establecimiento de tecnología y requisitos empresariales.
- Optimizar el uso de aplicaciones a nivel red.

El PPDIOO tiene tres pasos que se aplican a las 3 primeras etapas del ciclo de vida de la red.

Fase 1: Mapear requisitos de red del cliente

Fase 2: Exponer la red actual

Fase 3: Diseñar la topología de red y soluciones.

3.2.3.2 Metodología PMI (PMBOK®)

Para la planificación y organización del proyecto se hace uso de la metodología PMI basado en la guía de PMBOK en la cual se brindan las siguientes Áreas de conocimiento y grupos de procesos.

Áreas de Conocimiento

1. Gestión de la integración
2. Gestión del alcance
3. Gestión del tiempo
4. Gestión de los costos
5. Gestión de la calidad
6. Gestión de los recursos humanos
7. Gestión de las comunicaciones
8. Gestión de los riesgos
9. Gestión de las adquisiciones

Grupos de Procesos

- a. Inicio
- b. Planeación
- c. Ejecución
- d. Monitoreo y Control
- e. Cierre

Grupos de Procesos	Áreas de Conocimiento
a. Inicio	1. Gestión de la integración
b. Planeación	2. Gestión del alcance
c. Ejecución	3. Gestión del tiempo
d. Monitoreo y Control	4. Gestión de los costos
e. Cierre	5. Gestión de la calidad
 Project Management Institute	6. Gestión de los recursos humanos
	7. Gestión de las comunicaciones
	8. Gestión de los riesgos
	9. Gestión de las adquisiciones
	10. Gestión de los interesados

Tabla 1. Areas de Conocimiento y Grupos de procesos PMI

Fuente: (Elaboracion propia)

3.2.3.3 Metodología Agile Scrum

Durante la ejecución del proyecto se hizo uso de la metodología Ágil Scrum para abordar las sesiones también conocidas como dayli en la cual se tenía reuniones de 15 a 30 min con el negocio, equipo técnico y el proveedor.

En estas sesiones se brindan los avances, pendientes, tareas bloqueadas, tareas completadas a través del uso de la herramienta TRELLO en la cual se listaron las tarjetas de mayor prioridad y menor prioridad.

El encargado de llevar a cabo las reuniones(Dayli) y organizar las tarjetas era el mismo PM responsable de llevar a cabo la planificación del proyecto haciendo uso de PMI.



Figura 6. Metodología Agile SCRUM
Fuente: (<https://comunidad.iebschool.com/metodologiasagiles>)

Componentes Básicos de Scrum

Artefactos	Prácticas	Roles
Product Backlog	Planificación del Sprint	Scrum Master
Sprint Backlog	Scrum Diario (Dayli)	Product Owner
		Equipo de Desarrollo

Tabla 2. Componentes Basicos de Scrum

Fuente: (Elaboracion propia)

CICLO DE VIDA	METODOLOGIA DE DISEÑO		
	ACTIVIDADES	DOCUMENTACION	HERRAMIENTAS
PREPARAR	Paso 1: Mapear apps, servidores, servicios. Paso 2: Definir metas del negocio. Paso 3: Detallar todas las limitantes del negocio. Paso 4: Detallar metas a alcanzar a nivel técnico. Paso 5: Detallar bloqueos técnicos y limitantes.	Documento de Requerimientos del cliente.	-Herramienta Trello para realizar el seguimiento y la asignación de tareas relacionadas al levantamiento de información.
PLANIFICAR	Paso 1: Identificar información, documentación de la organización. Paso 2: Realizar una auditoría de red que agregue detalles a la descripción de la red. Paso 3: hacer uso de herramientas de análisis y captura de paquetes, sniffer.	Documento de Arquitectura de RED ACTUAL.	-Trello -Ejecución de comandos -Show tech-support -Show processes cpu -Show version -Show log -Netflow -SNMP -Checklist -Wireshark -Ekahau site Survey -Network Security scanner
DISEÑO	Top-Down Paso 1: Análisis de los requisitos de la aplicación y organización		

	Paso 2: Diseño desde la parte superior del modelo de referencia OSI Paso 3: Definir requisitos de capas superiores (aplicación, presentación, sesión) Paso 4: Especificar la infraestructura para las capas OSI inferiores (transporte, red, enlace de datos, físico) Paso 5: Reunir datos adicionales en la red.	Documento de Diseño Plan de Migración	
IMPLEMENTACION		Plan de Implementación Plan de Pruebas Plan de Rollback	
OPERAR		incidencias requerimientos gestion de cambios capacidad de red sistemas de backups criterios de seguridad	
OPTIMIZAR			

Tabla 3. Metodologia de Diseño PPDIOO
Fuente: (Preparacion propia)

3.2.4 FUNDAMENTOS UTILIZADOS

Arquitectura de Red Jerárquica

Los modelos jerárquicos nos brindan la facilidad de diseñar una arquitectura de red en 3 capas
La cual nos brindar beneficios a nivel de alta disponibilidad, escalabilidad, seguridad.

Estas 3 capas están conformadas por:

- Core
- Distribución
- Access

Cada capa puede centrarse en funciones específicas, lo que le permite elegir los sistemas y características adecuados para cada capa. Los modelos jerárquicos se aplican al diseño de LAN y WAN.

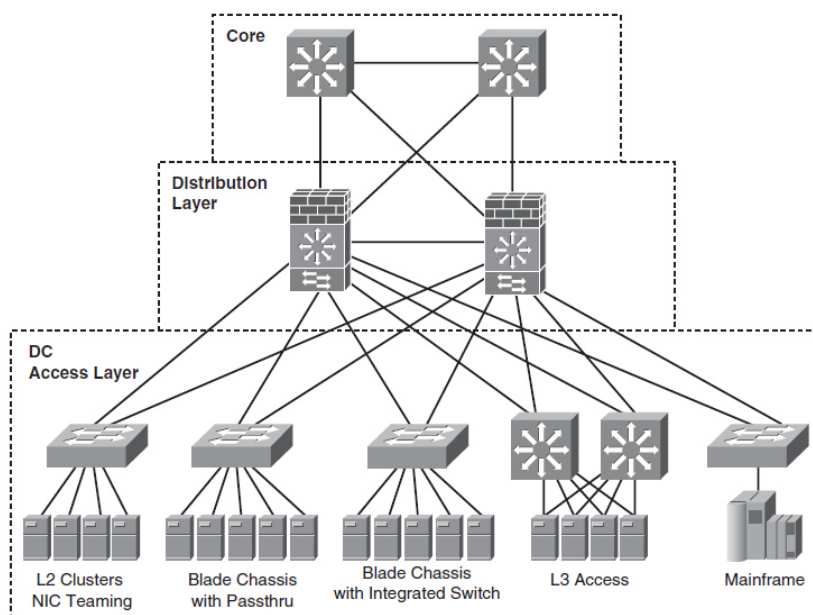


Figura 7. Modelo Jerarquico Cisco inc.
Fuente: (CCDA Cisco)

Beneficios del modelo jerárquico

- ✓ Ahorros económicos.
- ✓ Enlaces redundantes hacia capas superiores e inferiores
- ✓ Escalabilidad
- ✓ Tolerancia de fallas

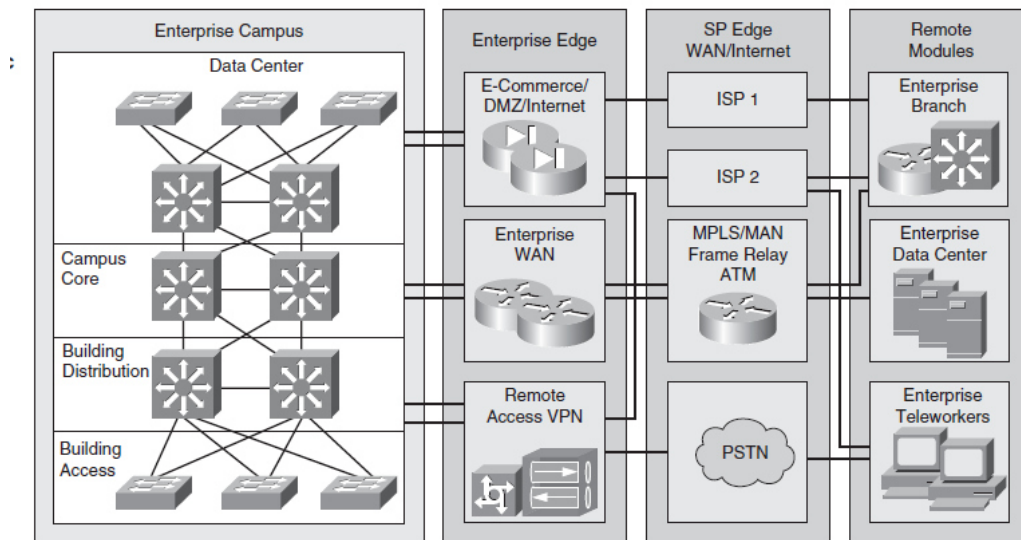


Figura 8. Modelo Enterprise Campus Cisco inc.
Fuente: (CCDA Cisco)

Capa de Núcleo

El Core es la columna vertebral de la RED a nivel de enrutamiento y conmutación de paquetes en alta velocidad.

Características:

- Transporte rápido
- Segura
- Alta disponibilidad
- Resiliente
- Niveles bajos de latencia y delay.
- Clasificación de calidad de servicio (QoS)

Capa de Distribución

Esta capa es la intermedia entre el Core y Access. La capa de distribución incluye las siguientes funciones.

- Conectividad basada en Policy (La red se reenvía por una interfaz mientras que el resto del tráfico se reenvía por otra interfaz)
- Redundancia y equilibrio de carga
- Agregación de armarios de cableado LAN
- Agregación de conexiones WAN
- QoS
- filtrado de seguridad
- Agregación o resumen de direcciones o áreas
- Acceso departamental o de grupo de trabajo
- Definición de dominio de difusión o multidifusión
- Intervlan routing.
- Filtrado por dirección de origen o destino
- Filtrado en puertos de entrada o salida
- Enrutamiento estático
- Mecanismos de QoS, como las colas basadas en prioridades

Capa de Acceso

Finalmente, esta capa proporciona conexión directa con los dispositivos finales como Access point, PC/laptop, etc.

Las funciones de la capa de acceso incluyen las siguientes:

- Conmutación de capa 2
- Alta disponibilidad
- Seguridad portuaria
- Supresión de transmisiones
- Clasificación y marcado de QoS y límites de confianza
- Tasa de limitación / vigilancia
- Inspección del Protocolo de resolución de direcciones (ARP)
- Listas de control de acceso virtual (VACL)
- Árbol de expansión
- Clasificación de confianza
- Power over Ethernet (PoE) y VLAN auxiliares para VoIP
- VLAN auxiliares

IPv4 Direccionamiento

Algunos números de red dentro del espacio de direcciones IPv4 están reservados para uso privado. Estos los números no se enrutan en Internet. Hoy en día, muchas organizaciones utilizan direcciones privadas en sus redes internas con NAT para acceder a Internet. Las direcciones privadas fueron uno de los primeros pasos para abordar la preocupación de que el espacio de direcciones IPv4 único a nivel mundial se agote. La disponibilidad de direcciones privadas combinadas con NAT reduce la necesidad de que las organizaciones Defina cuidadosamente las subredes para minimizar el desperdicio de direcciones IP globales públicas asignadas.

El espacio de direcciones de red IP reservado para las redes privadas es

10/8, 172.16 / 12 y 192.168 / 16. Incluye una red de clase A, 16 redes de clase B y 256 redes de clase C.

Class Type	Start Address	End Address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

Figura 9. Clases de Direccionamiento IP Privado.
Fuente: (CCDA Cisco)

Alta Disponibilidad

Al diseñar una topología de red para un cliente que tiene sistemas, servicios o rutas de red, debe determinar la probabilidad de que estos componentes fallen y diseñar redundancia cuando sea necesario. Considere incorporar uno de los siguientes tipos de redundancia en su diseño:

- Redundancia de estación de trabajo a enrutador en la capa de acceso al edificio
- Redundancia de servidores en el módulo de la granja de servidores
- Redundancia de rutas dentro y entre componentes de red
- Redundancia de medios de enlace en la capa de acceso

Redundancia del servidor

Algunos entornos necesitan servidores de aplicaciones y archivos completamente redundantes (reflejados). Los servidores redundantes pueden replicar los datos. Cisco Unified Communications Servidores del administrador (CUCM) en grupos para la redundancia. Los servidores deben estar en diferentes redes y utilice fuentes de alimentación redundantes. Para brindar alta disponibilidad en el servidor módulo de granja, tiene las siguientes opciones:

- (HSRP, GLBP, VRRP) para encontrar dinámicamente enrutadores alternativos.
- tarjetas de interfaz (NIC).

- Paquetes de puertos Fast EtherChannel (FEC) y Gigabit EtherChannel (GEC)

Protocolo HSRP

El protocolo Cisco HSRP proporciona una forma para estaciones de trabajo IP que admiten solo un enrutador predeterminado para seguir comunicándose en la red incluso si su enrutador predeterminado no está disponible.

HSRP funciona creando un enrutador virtual que tiene sus propias direcciones IP y MAC. Las estaciones de trabajo utilizan esta dirección IP virtual como su enrutador predeterminado. Los enrutadores HSRP en una LAN se comunican entre sí para designar dos enrutadores como activos y en espera. El enrutador activo envía mensajes de saludo periódicos. Los otros enrutadores HSRP escuchan los mensajes de saludo. Si el enrutador activo falla y los otros enrutadores HSRP dejan de recibir mensajes de saludo, el enrutador en espera toma el control y se convierte en el enrutador activo.

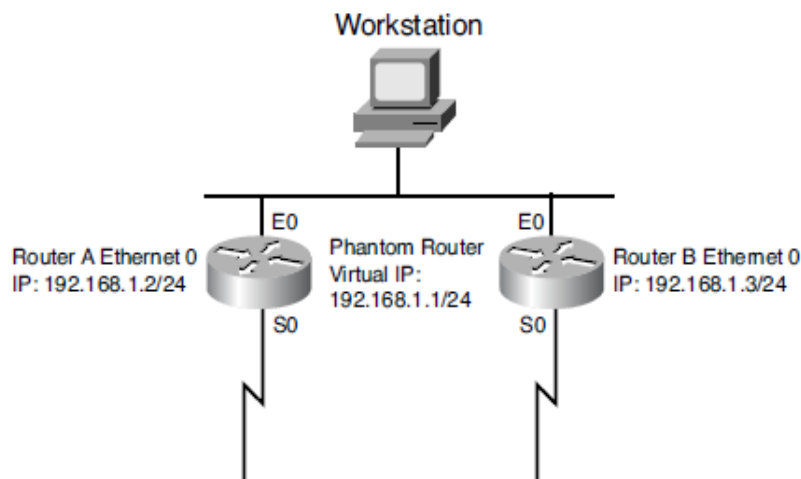


Figura 10. Protocolo HSRP Funcionamiento
Fuente: (CCDA Cisco)

Protocolo VRRP

VRRP especifica un protocolo electoral que asigna dinámicamente la responsabilidad de un enrutador a uno de los enrutadores VRRP en una LAN. El enrutador VRRP que controla las direcciones IP asociado con un enrutador virtual se llama maestro y reenvía los paquetes enviados a estas direcciones IP. El proceso de elección proporciona una falla dinámica en la responsabilidad de reenvío, en caso de que el maestro no esté disponible. Esto permite que cualquier IP del enrutador virtual direcciones en la LAN que los hosts finales utilizarán como enrutador de primer salto predeterminado.

Calidad de Servicio (QoS)

El concepto de calidad de servicio es aplicado en cada capa de la red jerárquica, básicamente consiste en realizar un proceso de clasificación, marcación y asignación de ancho de banda específico para cada tráfico.

El tráfico que se puede marcar es todo aquel que pase el filtro de clasificación, estos pueden ser segmentos de red dedicados a brindar servicios de voz y video, conexión hacia internet, tráfico crítico y no crítico como conexiones a bases de datos, consultas sql, etc.

El marcado establece ciertos bits en un paquete o trama que ha sido clasificado. Marcar también es llamado colorear o etiquetar.

El estándar IEEE 802.1D-1998 describe la aceleración de la clase de tráfico IEEE 802.1p.

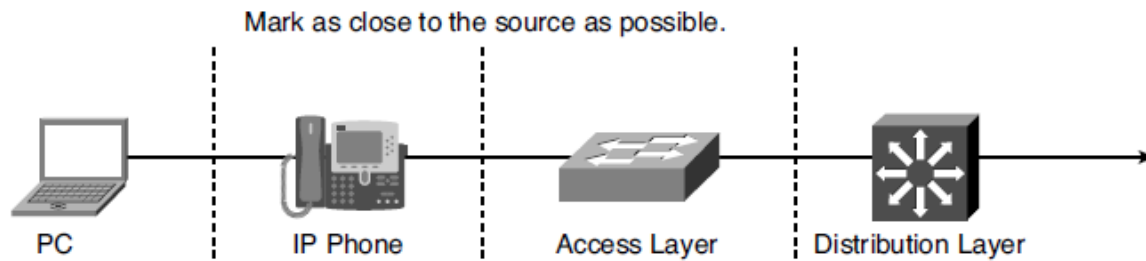


Figura 11. Calidad de servicio Telefonía Voip
Fuente: (CCDA Cisco)

Funcionalidad SDWAN

Esta tecnología WAN definida por software se presenta como la evolución a redes tradicionales como son MPLS.

La red SDWAN principalmente brinda la facilidad de escalar a nivel de conexiones hacia Internet o nubes privadas, haciendo uso de 2 enlaces en modo activo-activo brinda beneficios de conexión y anchos de banda.

El funcionamiento está definido por establecer conexiones virtuales a través de Internet, Redes MPLS, 4G/5G. el protocolo utilizado es IPSEC la cual genera conexiones que van censando el medio de transmisión en base a tiempos de respuesta, latencia, delay, intermitencia.

Y en base a esta información que toma la decisión de enrutar los paquetes por un camino o el otro.

Esta tecnología se aprovecha al máximo cuando se tienen escenarios con 2 proveedores ISP distintos.

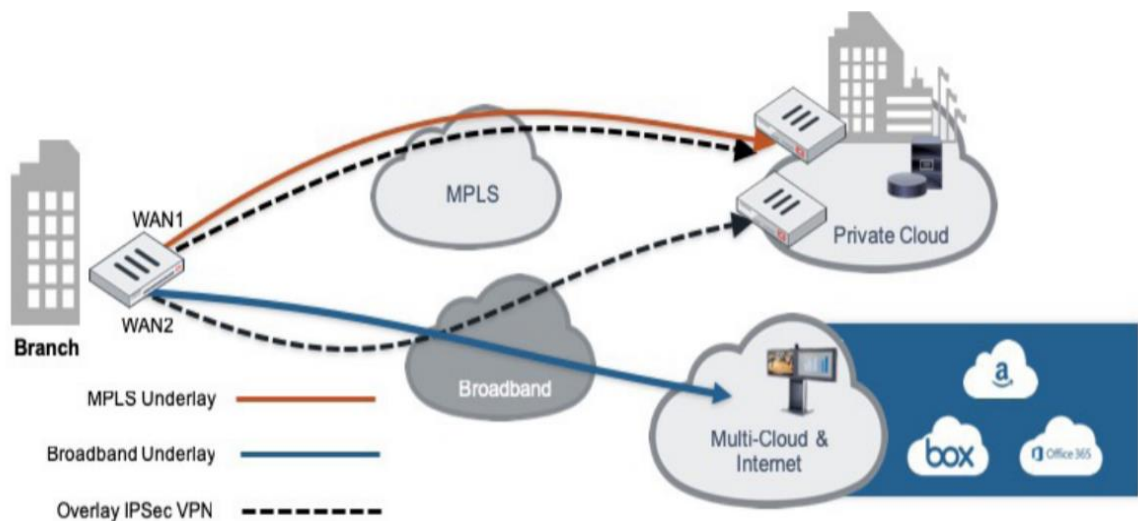


Figura 12. Funcionamiento sdwan
Fuente: (Fortinet cookbook)

Seguridad de Red

Establecer políticas de seguridad de Red es un punto muy importante que todo negocio medio o grande debe considerar, esta parte fundamental básicamente se centra en establecer mecanismos que eviten la vulneración de seguridad de una infraestructura hacia lo servidores, equipos Core y prevenir ataques de manera interna y externa.

La parte más importante y el primer frente de contención de ataques es la seguridad perimetral mediante firewalls se evita ataques externos provenientes de distintas partes del mundo.

Componentes que ayudan a contener ciberataques:

- Sanboxing
- Antiddos
- Reforzar endpoint (EDR)

Consideraciones de seguridad a tener en cuenta:

- Bloquear el acceso de atacantes externos a la red
- Permitir el acceso solo a usuarios autorizados
- Evitar que los ataques provengan de fuentes internas
- Compatible con diferentes niveles de acceso de usuarios
- Protección de los datos contra alteraciones o uso indebido

Tecnologías WAN

Se deben considerar varios factores al seleccionar una tecnología de transporte WAN. Las opciones de WAN están basadas en Internet pública y algunas están basadas en WAN privadas. La Geografía también juega un papel clave en las tecnologías WAN disponibles en un área determinada. Ciudades importantes tienen la mayor cantidad de opciones de transporte WAN, y las áreas rurales son más limitadas en cuanto a disponibilidad de las opciones de servicio WAN.

WAN Technology	Bandwidth	Reliability	Latency	Cost
ISDN	Low	Medium	Medium	Low
DSL	Low/medium	Low	Medium	Low
Cable	Low/Medium	Low	Medium	Low
Wireless	Low/Medium	Low	Medium	Medium
Frame Relay	Low/Medium	Medium	Low	Medium
TDM	Medium	High	Low	Medium
Metro Ethernet	Medium/high	High	Low	Medium
SONET/SDH	High	High	Low	High
MPLS	High	High	Low	High
Dark fiber	High	High	Low	High
DWDM	High	High	Low	High

Figura 13. Tipos de Tecnologías WAN
Fuente: (CCDA Cisco)

Esta información también refleja las diferentes características de cada tecnología WAN. Sin embargo, tenga en cuenta que las ofertas de su proveedor de servicios Limite las opciones de tecnología WAN disponibles para usted durante su selección.

MPLS (Multiprotocol Label Switching)

MPLS es tecnología para la entrega de servicios IP utilizando etiquetas (números) para reenviar paquetes. En entornos enrutados normales, los paquetes se reenvían salto a salto desde el origen al destino. Cada enrutador en la ruta realiza una dirección de destino de Capa 3 búsqueda, reescribe la dirección de Capa 2 y reenvía el paquete al destino. Sin embargo, MPLS funciona marcando encabezados de paquetes que incluyen información de etiquetas. Tan pronto como Los paquetes están marcados con una etiqueta, se pueden diseñar rutas específicas a través de la red para corresponden a esa etiqueta distinta. Las etiquetas MPLS se pueden configurar en parámetros como direcciones de origen, ID de circuito de capa 2 o valor de QoS. Normalmente, las etiquetas corresponden a la dirección de destino de la Capa 3, lo que hace que MPLS sea lo mismo que el enrutamiento basado en destino.

Los paquetes MPLS pueden ejecutarse en la mayoría de las tecnologías de Capa 2, como ATM, Frame Relay, POS y Ethernet. El objetivo de MPLS es maximizar la conmutación mediante etiquetas y minimizar Enrutamiento de capa 3. En las implementaciones de MPLS, existen enrutadores de borde de cliente (CE) y de borde de proveedor (PE). El enrutador CE reside en las instalaciones del cliente y, por lo general, es allí donde los internos y externos se intercambia información de enrutamiento. El enrutador CE luego se conecta al enrutador PE, que es el ingreso a la red del proveedor de servicios MPLS.

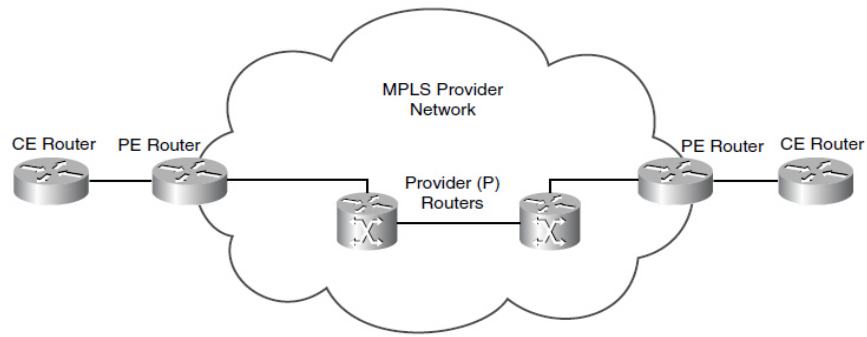


Figura 14. Tecnología MPLS
Fuente: (CCDA Cisco)

VPN

Red privada virtual es una tecnología muy usada que consiste en emular la conexión hacia servicios internos como si estuvieras dentro de la red LAN de la empresa.

Se puede usar 2 tipos de conexiones VPN:

- VPN SSL para conexión remota de usuarios a través de un cliente
- VPN IPSEC para establecer una conexión lógica a través de internet para acceder y crear un canal virtual de conexión hacia servicios internos.

DMZ (zona Desmilitarizada)

Dentro de la red lan de una organización se puede segmentar de manera interna la lan para poder establecer una red DMZ que principalmente consiste en aislar el segmento dmz de los ataques provenientes del exterior o interior.

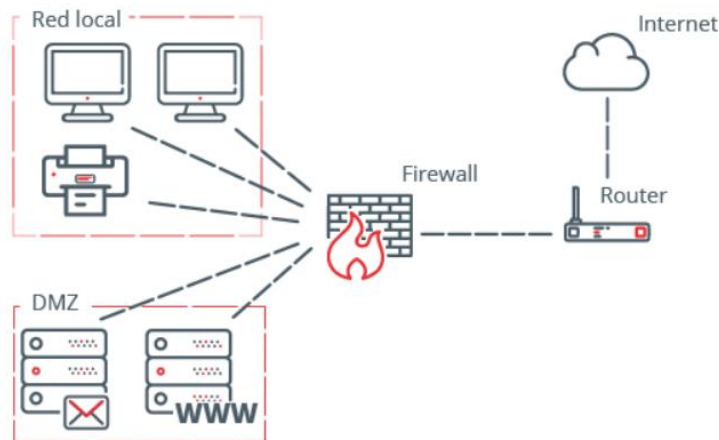


Figura 15. Zona Desmilitarizada
Fuente: (fortigate cookbook)

Para ejecutar esto es necesario contar con un equipo de capa 4 y seguridad firewall dedicado para soportar conexiones y sesiones entrantes y salientes aplicando políticas de seguridad que permitan o denieguen cierto tráfico.

Método de diseño Top and Down

La metodología PPDIOO establece un método que facilita la elaboración del diseño de una red. Esta es conocida como Top and down. También establece otro método llamado down and top que consiste en iniciar el diseño desde la parte inferior del modelo OSI hacia capas superiores.

El método consiste en comenzar el diseño partiendo de las capas superiores del modelo de referencia OSI:

- Aplicación
- Presentación
- Sesión
- Transporte
- Red

- Enlace de datos
- físico

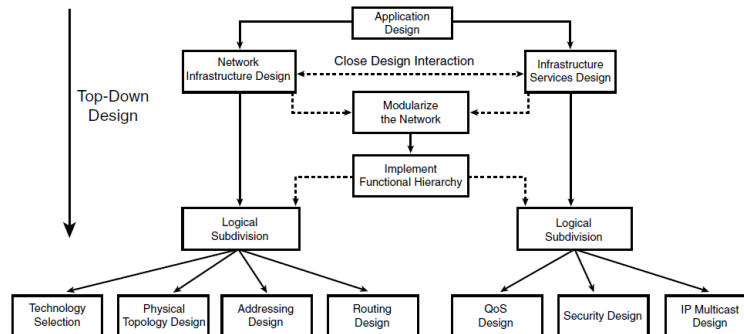


Figura 16. Modelo Top and down - Diseño
Fuente: (CCDA Cisco)

Topología Full Mesh

Este tipo de topología especifica la facilidad de conexión entre nodos remotos de forma todos entre todos. Es un tipo de red que posee un alto grado de disponibilidad puesto que se generan enlaces redundantes hacia cada nodo.

Finalmente se establece una malla que brinda comunicación y el beneficio de compartir recursos de todos los nodos entre todos.

Por lo general este tipo de topología es una evolución a las topologías hub and spoke.

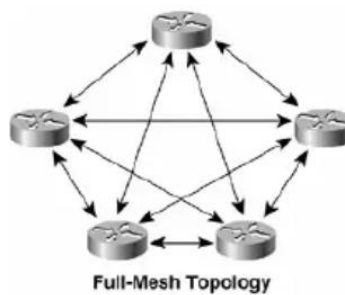


Figura 17. Topologia Full Mesh
Fuente: (CCDA Cisco)

Tecnología Stacking

A nivel de la infraestructura de Networking, el término "pila" (o apilable) se refiere a un grupo de conmutadores físicos que se han cableado y agrupado en un único conmutador lógico. A lo largo de los años, las funciones de apilamiento han pasado de ser una función Premium (y costosa) a una capacidad central de casi todos los conmutadores de nivel empresarial (y también en varios modelos de pymes).



Figura 18. Componentes Stack
Fuente: (Cisco Meraki)

Estándar TIA

Este estándar establece lineamientos para ejecutar el cableado estructurado de manera correcta y haciendo uso de buenas prácticas, se definen los requerimientos mínimos para establecer cuartos de comunicaciones, data center, cableados horizontales y verticales.

El estándar nos muestra las categorías de cableado que podemos usar que son:

Categoría 5e

Categoría 3

Categoría 6

Por lo general para el cableado de tipo backbone se suele utiliza fibra óptica, debido al gran ancho de banda que puede manejar.

Para el cableado horizontal se suele usar cable de cobre categoría 5e y 6.

3.2.5 DISEÑO E IMPLEMENTACION DE UNA RED CORPORATIVA LAN Y WAN HACIENDO USO DE BUENAS PRACTICAS

3.2.5.1 Planificación y Gestión del Proyecto

I. Gestión de la Integración

Alcance del Producto

Todas las bondades de la Implementación y Unificación de las Unes de Inversiones Educa S.A. se enfocan en lo siguiente:

- Poder Compartir recursos Voip, Wifi, FilServer, DB, Colaboración, Video Vigilancia).
- Poder asistir de manera oportuna requerimientos e incidentes en la RED PRIVADA.
- Poder incrementar el ancho de banda de manera rápida y a demanda según sea necesario.
- Poder contar con 2 rutas de navegación a internet, y ante cualquier caída de servicio de conexión Internacional, tener el respaldo de una segunda ruta.
- Poder manejar permisos de navegación a Internet y bloqueos oportunos
- Brindar la seguridad Perimetral ante ataques de DDoS, Ataques de Día Zero, Ransomware, Ataques de Fuerza Bruta, etc.
- Brindar acceso hacia todos los recursos de las 3 Unes a través de una sola configuración de VPN SSL.
- Conocer el estado de los Enlaces de RED, así como el status de los mismos (Consumo de Ancho de Banda, Uso de CPU, RAM, etc.)
- Permitir la extracción de Reportes de Ataques, Consumo de Ancho de Banda, top 10 usuarios de mayor consumo, Top 10 Aplicaciones más usadas. Etc.
- Permitir la Publicación de Servicios y Aplicaciones bajo el mismo Direcccionamiento IP Publico.

II. Asunciones

1. La Gerencia de TI de Inversiones Educa. S.A. brindará todas las facilidades a nivel de recursos y tiempos durante todo el periodo de ejecución del proyecto.
2. El Área de REDES estarán brindando las facilidades a los proveedores durante todo el proyecto, así como las visitas técnicas a cada sede y finalmente para la revisión y validación de los Informes Técnicos de ingreso de Fibra a las sedes.
3. Personal del Equipo y Subgerencia de Soluciones y BI deberán asignar un recurso para el proyecto durante el levantamiento de Información y posterior validación del cambio.
4. Personal de cada Área Funcional (Académica, Finanzas, Logística) deberán asignar un recurso para validar a nivel funcional el correcto funcionamiento de las aplicaciones y servicios.
5. Los representantes Legales de cada UNE deberán autorizar los pases a producción durante el fin de semana que este programando realizar la migración.
6. La gerencia de RR. HH deberá prepara un comunicado en caso algún servicio no se encuentre disponible durante y post Migración.

III. Condiciones

1. Para la gestión y planificación del proyecto se usará la metodología PMI de la cual se abarcará solo algunas áreas del conocimiento.
2. El diseño de la nueva Arquitectura estará basada en la especificación de la metodología PPDIOO y el diseño en 3 capas de Cisco inc.
3. La funcionalidad de SDWAN será basada en las buenas Practicas ofrecidas por Fortinet inc.
4. La implementación final a realizar en Inversiones Educa S.A. está sujeta al presupuesto asignado para el proyecto. Para la adquisición y adjudicación del proveedor y conseguir objetivos técnicos y del negocio detallados en el alcance.

IV. Requerimientos del Proyecto

La Optimización de una RED LAN y WAN Centralizada en Inversiones Educa S.A. significa realizar los siguientes entregables listados a continuación.

Código	Descripción
TILEV01	Listado de Servicios Críticos No Críticos
TILEV02	Propuesta de Arquitectura de RED
TILEV03	Diseño de RED
TILEV04	Planeación y Ejecución

Tabla 4. Lista de Entregables
Fuente: (Elaboracion propia)

V. Hitos y Entregables de la gestión de proyectos

Para la gestión del proyecto, se han definido los siguientes entregables:

Actividad	Fecha Estimada	Responsable
Acta de Constitución del Proyecto	10/07/2019	MTORIBIO
EDT	10/08/2019	MTORIBIO
Cronograma de gestión del proyecto	25/08/2019	MTORIBIO
Cronograma de ejecución del proyecto	25/09/2019	MTORIBIO

Tabla 5. Lista de Entregables
Fuente: (Elaboracion propia)

VI. Presupuesto

El presupuesto asignado por parte de la gerencia y subgerencia de TI de debe considerar los siguientes ítems.

Ítem	Origen del Presupuesto
Recursos humanos para el proyecto.	La contratación de personal temporal o la reasignación de personal para liderar, gestionar y ejecutar el proyecto El área de proyectos deberá proponer un PM y la subgerencia de TI designar el líder técnico.
Alquiler tecnológico	Esto será cubierto por el presupuesto anual separado y asignado a la gerencia de TI para el uso de alquiler de equipos por 3 años con el proveedor y compra de equipos de ser necesario.
Servicios Mensuales Internet	El presupuesto anual y asignado al proyecto será destinado un porcentaje a cubrir este gasto opex.

Tabla 6. Items de Presupuesto
Fuente: (Elaboracion propia)

VII. Recursos

Para la Implementación del proyecto se ha determinado que será necesario definir y asignar los siguientes ítems.

Recursos	Detalle
Equipo técnico y proyectos.	El equipo estará conformado por 2 especialistas ingenieros de sistemas. Y 1 Analista de Redes para ejecución de Pruebas y cambios.
Equipamiento Tecnológico	Routers Cabecera, Firewall Perimetral, Router CPE, Fortianalyzer, MediaConverter, Fibra Optica, Racks, Gabinetes RU, UPS, transceiver.

Tabla 7. Items de Recursos
Fuente: (Elaboracion propia)

VIII. Riesgos

Se listan todos los peligros involucrados que ponen en riesgo el éxito del proyecto.

Descripción de Riesgo	Probabilidad
Deserción temporal de miembros del equipo técnico	60%
Deserción definitivo de miembros del equipo del proyecto	60%
Permisos y Licencias Municipales para ejecución de Obra Civil	70%
Demora en la importación de equipamiento Router, Firewall.	60%
Modificación del alcance	35%

Baja retroalimentación entre el equipo de Redes y proveedor.	10%
Anuncio de algún curso o matrícula que impidan realizar el pase a producción	40%
Equipamiento Tecnológico inadecuado	35%
Falta de Experiencia al momento de ejecutar la migración	25%
Informes Técnicos no aprobados por el negocio y corrección del mismo para la ruta de ingreso de la Fibra.	45%
Deficiencia en la entrega de Información de servicio Críticos y no Críticos	55%

Tabla 8. Descripción de Riesgos
Fuente: (Elaboración propia)

IX. Control de Cambios

A continuación, se especifica el formato del documento que oficializará los requerimientos de cambios dentro del proyecto.

	<i>Gestión de Cambios</i>	Redes y Telecomunicaciones
Pág. 1 de 1	Formato RFC - genérico	CONFIDENCIAL

+

Solicitante del Cambio	ID de Req. de Cambio:	RFC-0005		
	Responsable del Cambio:			
	Solicitante del Cambio:		Fecha de Solicitud:	
	Descripción del cambio:	Estimados Requerimos un listado de las reglas de firewall solicitadas de los ambientes productivo y no productivo		
	Agenda del Cambio:	¿Cuándo debería implementarse el cambio?		
	Metas y Objetivos:	¿Por qué el cambio es necesario?		
		¿Cuál es el resultado deseado del cambio?		
¿Cuáles son las consecuencias si el cambio es rechazado o pospuesto?				
INDICACIONES ADICIONALES				

□

Figura 19. Formato Control de Cambios
Fuente: (Formatos proyectos ieduca)

Gestión del Alcance

I. Enunciado del alcance de proyecto

El alcance del Proyecto “OPTIMIZACION DE LA INFRAESTRUCTURA DE RED LAN Y WAN, PARA LAS EMPRESAS DEL GRUPO INVERSIONES EDUCA S.A. BASADO EN LA METODOLOGIA PPDIOO CISCO Inc.” a nivel de detalle se listan los siguientes objetivos.

- Realizar el levantamiento de Información de Servicio Críticos y No Críticos, procesos de operaciones Actuales de las Áreas: Académicas, Ventas, Logística de cada UNE de Inversiones Educa S.A.
- Realizar un análisis y Diseño de una nueva arquitectura Centralizada y nuevo Direccionamiento IP.
- Establecer la nueva Arquitectura y Direccionamiento IP mediante el uso de Tecnología Cisco Diseño de Capas y SDWAN de Fortinet.
- Planificar la implementación de la nueva red con la participación del nuevo proveedor de Servicios ISP que permitan a las UNES de Inversiones Educa poder estar centralizados en una sola Red LAN Privada y compartir Recursos.
- Integración del servicio de Telefonía
- Brindar una conexión hacia internet redundante.
- Mejora de la Gestión y administración de Sedes Remotas de cada Une al estar integradas sobre una sola red Privada.
- Brindar la facilidad de compartir recursos entre Unes tales como (Voip, Wifi, FilServer, DB, Colaboración, Video Vigilancia).
- Mejora en la capacidad de la RED en relación a tiempos de respuesta, anchos de banda y Escalabilidad.
- Mejora en los tiempos de Atención de Incidentes y Requerimientos.
- Mejora en la Seguridad Perimetral ante ataques externos e Internos.

Para lo cual se consideran las siguientes actividades:

- i. Definición, Organización y Roles del Proyecto.

- ii. Coordinar al equipo de proyecto, Explicar y documentar claramente cuáles son los roles que cada integrante del equipo cumplirá

Roles	Descripción
Project Manager	Liderar, gestionar la ejecución del proyecto
Administrador de Red	Líder Técnico
Analista de Redes	Personal de Apoyo para ejecución de cambios, pruebas.
Analista de Infraestructura	Personal de Apoyo para ejecución de cambios, pruebas.

Tabla 9. Descripción de Roles
Fuente: (Elaboración propia)

- iii. Coordinar con Inversiones Educa S.A. la permuta del presupuesto.

- a. Identificación de Interesados.
- Inversiones Educa. S.A
 - ITLS SAC
 - Universidad de Ciencias y Artes - UCAL
 - Institutos CERTUS
 - CEO IEDUCA S.A.
 - Personas que validan los resultados del proyecto
 - Personas que proponen mejoras del proyecto
- b. Actividades del Proyecto
- Definir Áreas Afectadas del Proyecto

Revisión de documentación existente, relacionada con los servicios publicados por cada UNE actuales

II. Entregables del proyecto

Como entregables del proyecto se definen los siguientes documentos.

- ✓ Evaluación de la situación actual y mejoras en la Arquitectura de RED.
- ✓ Plan de ejecución del proyecto - Gantt

Además de esto durante la implementación se hará uso de los tableros KANBAN para el seguimiento y por eso se entregará:

- ✓ tablero en la herramienta TRELLO

También en base al diseño en 3 Capas sugerida por CISCO, se entregará

- ✓ Diagrama de Diseño de Red en 3 Capas (Distribución, Core, Acceso)

II.1 Diagnóstico de la Situación Actual

Este documento contiene el levantamiento de información realizado a los servicios internos y a los componentes de red con que cuenta actualmente INVERSIONES EDUCA S.A. actualmente.

II.2 Planificación para la Gestión e Implementación del Proyecto

Se detallará las actividades mapeadas para la ejecución del proyecto abarcando las fases de la metodología PPDIIO.

II.3 Análisis Tecnológico

En este entregable se detalla todo el equipamiento necesario, así como el datasheet correspondiente a cada componente.

- Equipos Físicos de Telecomunicaciones - Routers.
- Equipos de conexión Fibra óptica, cobre de conexión hacia internet y sedes remotas.
- Hardware y tecnologías de Seguridad Perimetral.
- Reportes Fortianalyzer.
- Componentes de Telecomunicaciones
- Software Herramienta de Monitoreo de Enlaces de RED.
- Software Herramienta de Reportes, Consumos de Ancho de banda, etc.

III. Fuera de Alcance

Los siguientes aspectos no están considerados dentro del alcance del proyecto y, por lo tanto, no serán abordados en el mismo:

- ❖ Brindar Soporte al Software, Aplicaciones, Servicios Web.
- ❖ Instalar Equipamiento no definido en el Alcance como (Balanceadores, Optimizadores, etc.)
- ❖ Realizar Upgrade de Anchos de Banda que no fueron definidos en el alcance.
- ❖ Instalar Componentes como Transceiver que no fueron considerados en el alcance.

IV. Objetivos del Proyecto

Objetivo general

Brindar lineamientos generales para la preparación, planificación diseño e implementación de una nueva arquitectura de RED para las unidades de negocio de la empresa INVERSIONES EDUCA S.A., a fin de mejorar la gestión, optimizar los recursos, mejorar la calidad del servicio y, a su vez, aumentar su resiliencia.

Objetivos específicos

- ✓ Ejecutar el levantamiento de información de servicios y servidores críticos actuales de cada Unidad de Negocio de la empresa Inversiones Educa S.A.
- ✓ Efectuar un análisis y diseño de un nuevo esquema de direccionamiento IP para que cada sede de cada Unidad de negocio sea independiente y la gestión no provoque duplicidad de redes.
- ✓ Establecer una Arquitectura de Red Centralizada que permita la mejora de la gestión oportuna de las sedes y recursos de las mismas, mediante el uso del diseño en 3 capas y la funcionalidad de SDWAN.
- ✓ Planificar la implementación de la nueva Arquitectura de RED que permitan a Inversiones Educa S.A. ofrecer un mejor servicio a sus Unidades de Negocio, mediante una RED CENTRALIZADA y con el uso de SDWAN.

Cronograma de Actividades

A continuación, se detallan las actividades identificadas que comprenden desde la planificación hasta la puesta en marcha y posterior cierre.

Cronograma del Proyecto

Actividades	Duración	Comienzo	Fin	Responsable	% completado
Proyecto de Migración RED Datos e Internet CERTUS/TLS/UCAL	120 días	01/09/18	25/12/18	GERENCIA TI	0%
Reuniones del Proyecto	x días	01/09/18	25/12/18	GERENCIA TI	17%
Reunión 01 – Presentación del Proyecto – Necesidad	x días	01/09/18	25/12/18	JNAVARRO	100%
Reunión 02 – Kickof	x días	01/09/18	25/12/18	JNAVARRO	0%
1. PLANIFICACION DEL PROYECTO	30 días	01/09/18	25/12/18	JNAVARRO	0%
1.1 Asignación de Recursos	x días	01/09/18	25/12/18	JNAVARRO	100%
1.2 Elaboración de RFP	x días	01/09/18	25/12/18	MTORIBIO	100%
1.3 Autorización de Owners para el cambio	x días	01/09/18	25/12/18	JNAVARRO	100%
1.4 Elaboración de Gantt del proyecto	x días	01/09/18	25/12/18	IEDUCA	100%
2. PREPARACION	10 días	01/09/18	25/12/18	MTORIBIO	2%
2.1 Realizar Inventario de Aplicaciones y Servicios de cada UNE	x días	01/09/18	25/12/18	MTORIBIO	8%
2.1.1 Realizar Inventario de Servidores Públicos y Privados	x días	01/09/18	25/12/18	MTORIBIO	0%
2.1.2 Realizar Inventario de segmentos de red LAN	x días	01/09/18	25/12/18	MTORIBIO	0%
2.1.3 Realizar Inventario de VLANS	x días	01/09/18	25/12/18	MTORIBIO	0%
2.1.4 Realizar Inventario de Reglas de Firewall	x días	01/09/18	25/12/18	MTORIBIO	0%
2.1.5 Realizar Inventario de Servidores VOIP	x días	01/09/18	25/12/18	MTORIBIO	0%
2.1.6 Realizar Inventario de NVR/DVR Video Vigilancia	x días	01/09/18	25/12/18	MTORIBIO	0%
2.2 Identificación de Objetivos y Limitaciones de la organización	x días	01/09/18	25/12/18	MTORIBIO	100%
2.3 Identificación de Objetivos Técnicos y Limitaciones Técnicas de la organización	x días	01/09/18	25/12/18	MTORIBIO	100%
3. PLANEACION	10 días	01/09/18	25/12/18		0%
3.1 Diagnóstico	x días	01/09/18	25/12/18	MTORIBIO	0%
3.1.2 Ejecución diagnóstico de red lan	x días	01/09/18	25/12/18	MTORIBIO	0%
3.1.3 Ejecución diagnóstico de red wan	x días	01/09/18	25/12/18	MTORIBIO	0%
3.1.4 Ejecución diagnóstico de red dmz	x días	01/09/18	25/12/18	MTORIBIO	0%

3.1.5 Elaboración de informe de diagnóstico de red	x días	01/09/18	25/12/18	MTORIBIO	0%
3.2 Auditoria de RED	x días	01/09/18	25/12/18	MTORIBIO	0%
3.2.1 Ejecución de Auditoria	x días	01/09/18	25/12/18	MTORIBIO	0%
3.2.2 Elaboración de informe de Auditoria	x días	01/09/18	25/12/18	MTORIBIO	0%
4. DISEÑO	10 días	01/09/18	25/12/18		0%
4.1 Elaboración de Diseños	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.1 Elaboración de Diseño de red LAN	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.2 Elaboración de Diseño de red wan y sdwan	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.3 Elaboración de Diseño de telefonía IP	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.4 Elaboración de Diseño de Direcccionamiento IPV4	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5 Elaboración de Diseño de Seguridad	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.6 Elaboración de perfiles de seguridad fsso	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.7 Elaboración de políticas de seguridad	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.8 Elaboración de perfiles web y app control	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.9 Elaboración de perfiles seguridad LAN Y dmz	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.10 Elaboración de diseño de parte superior OSI	x días	01/09/18	25/12/18	MTORIBIO	0%
4.1.5.11 Elaboración de diseño de QoS	x días	01/09/18	25/12/18	MTORIBIO	0%
4.2 Selección de Equipamiento LAN/WAN/Seguridad	x días	01/09/18	25/12/18	MTORIBIO	0%
5. IMPLEMENTACION	60 días	01/09/18	25/12/18		0%
5.1 Dimensionamiento	x días	01/09/18	25/12/18	MTORIBIO	0%
5.2 Reunión de Kick off	x días	01/09/18	25/12/18	MTORIBIO	0%
5.3 Coordinación de visitas Técnicas	x días	01/09/18	25/12/18	MTORIBIO	0%
5.4 Reunión técnica	x días	01/09/18	25/12/18	MTORIBIO	0%
5.5 Elaboración cronograma de pase a producción	x días	01/09/18	25/12/18	MTORIBIO	0%
5.6 Elaboración plan de rollback	x días	01/09/18	25/12/18	MTORIBIO	0%
5.7 Elaboración de Plan de Evaluación y Validación	x días	01/09/18	25/12/18	MTORIBIO	0%
Ordenamiento LAN Direcccionamiento Ipv4 y vlan	x días	01/09/18	25/12/18	MTORIBIO	
5.8 Implementación RED DATOS, Internet	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1 Sede Krumdieck	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%

5.5.1.4 Configuración de VDOM	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.5 Configuración de features de seguridad	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.6 Configuración de tuneles ipsec	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.6 Configuración de portales vpn ssl	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.6 Configuración de sandboxing cloud	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.6 Configuración de antiddos cloud	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.6 Configuración de fortianalyzer	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.5.2 Sede Chacarilla	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación equipos DMZ	x días	01/09/18	25/12/18	MTORIBIO/ON	
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Javier Prado	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede La Molina	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Surco Certus	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%

5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Norte	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Ate	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Villa	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Callao	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Arequipa	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede Chiclayo	x días	01/09/18	25/12/18	MTORIBIO/ON	0%

5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1 Sede San Miguel	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.1 Visita Técnica	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.2 Instalación Fibra	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.3 Instalación Equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.1.1.4 Ejecución de pruebas de Alta Disponibilidad y Saturación	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.9 Migración de Políticas de Seguridad	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.10 Ordenamiento y depuración de políticas	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
5.12 Conexión y configuración de equipos	x días	01/09/18	25/12/18	MTORIBIO/ON	0%
Cierre			25/12/18		

Tabla 10. Cronograma de Actividades
Fuente: (Elaboracion propia)

3.2.5.2 Fase de Preparación

Identificar Aplicaciones de red y servicios.

En este punto se validaron todas las aplicaciones y servicios que actualmente se brindan y están soportados en la arquitectura de red actual, posteriormente se realizó un inventario de aplicaciones y servicios que poseen direccionamiento publico estático configurado en algún archivo etc/host, realmlist de su configuración.

UNE	Servicio	Owner
CERTUS	Servidor RDP para alumnos SINTAD	AFOX
CERTUS	Controlador de dominio CERTUS - AD DNS	AFOX
CERTUS	Consola de Antivirus Kaspersky	UNAVARRO
CERTUS	Moodle Pruebas Juan Eladio	UNAVARRO
CERTUS	Servidore RDP - CERTUS	GSANCHEZ
TLS DMZ	Portal de Transparencia UCAL	GSANCHEZ
TLS DMZ	Servidor GENESYS - Base de datos de interacciones Chat y Correo	AFOX
CERTUS	wsbannerdev - DOCKER	AFOX
CERTUS LVL3	Zabbix Proxy new	UNAVARRO
TLS DMZ	Intranet Toulouse	UNAVARRO
TLS CHA	Satelites web de TLS y UCAL PRD	GSANCHEZ
CERTUS LVL3	wsbanner - DOCKER	GSANCHEZ
TLS CHA	Prometeo DB	AFOX
CERTUS LVL3	Web Certus Institucional PRD	AFOX
CERTUS LVL3	Web Certus Institucional DEV	UNAVARRO
CERTUS LVL3	ETHOS	UNAVARRO
CERTUS LVL3	Banner	GSANCHEZ
TLS CHA	Servidor GENESYS - Framework Genesys, Base de datos y Reportes	GSANCHEZ
TLS CHA	RDBMS	AFOX
TLS CHA	ADMIN PAGES	AFOX
TLS JP	ADMIN PAGES	UNAVARRO
TLS JP	Banner	UNAVARRO
TLS JP	AUTOSERVICIOS BANNERS 9.1	GSANCHEZ
UCAL	Servidor IIS Desarrollo	GSANCHEZ
UCAL	WS IEDUCA PRD	UNAVARRO
UCAL	Portal CERTUS DEV	UNAVARRO

Tabla 11. Inventario de Servidores

Fuente: (Elaboracion propia)

IP Privada	Hostname	Ambiente	S.O.
10.100.54.62	SRV-SQL01	PROD	Microsoft Windows Server 2003(64-bits)
10.100.54.4	SRVCENTER	PROD	Microsoft Windows Server 2019(64-bits)
10.100.54.30	SRVPRCADS02	PROD	Microsoft Windows Server 2019(64-bits)
10.100.54.34	SRVPRCADS1	PROD	Microsoft Windows Server 2019(64-bits)
10.100.54.125	SRVPRCAVTESTC	DEV	Red Hat Enterprise Linux 7(64-bits)
172.16.1.12	tlssursrv3.grupotls.edu	PROD	Microsoft Windows Server 2019(64-bits)
172.16.1.20	Tlssursrv2.grupotls.edu	PROD	Centos 7
10.100.54.85	SRVSURMUDEV	DEV	Microsoft Windows Server 2019(64-bits)
10.200.1.152	SRVETHPRD	PROD	Microsoft Windows Server 2019(64-bits)
172.16.1.6	Tlssursrv9.grupotls.edu	DEV	Microsoft Windows Server 2019(64-bits)
192.168.6.171	TLSSUP.grupotls.edu	DEV	Microsoft Windows Server 2019(64-bits)
10.200.1.51	SRVAUTPRD1_2	PROD	Debian 10
192.168.6.174	Tlssursrv1.grupotls.edu	PROD	Red Hat Enterprise Linux 7(64-bits)
10.200.1.70	SRVAUTPRD01	PROD	Red Hat Enterprise Linux 7(64-bits)
10.200.1.75	SRVAUTPRD12	DEV	Microsoft Windows Server 2019(64-bits)
10.200.1.76	SRVAUTPRD11	PROD	VMware Photon OS (64-bits)
10.200.1.79	SRVAUTPRD10	PROD	Microsoft Windows Server 2019(64-bits)
192.168.6.193	tlssursrv3.grupotls.edu	PROD	Microsoft Windows Server 2019(64-bits)
192.168.6.228	tlssursrv3.grupotls.edu	PROD	Microsoft Windows Server 2012(64-bits)
192.168.6.229	tlssursrv3.grupotls.edu	PROD	Debian GNU/Linux 10
10.40.54.120	MS_WS-TLS-PRD	PROD	Microsoft Windows Server 2019(64-bits)
10.40.54.121	MS01_W-TLS-PRD	PROD	Microsoft Windows Server 2019(64-bits)
10.40.54.122	MS_CRM-TLS-PRD	PROD	Microsoft Windows Server 2008(64-bits)
10.150.14.82	ucalesx01.ucal.edu.pe	DEV	Microsoft Windows Server 2019(64-bits)
10.150.14.84	ucalesx02.ucal.edu.pe	PROD	Microsoft Windows Server 2019(64-bits)
10.150.14.90	ucalesx03.ucal.edu.pe	DEV	Microsoft Windows Server 2019(64-bits)

Tabla 12. Inventario de Servidores Privados

Fuente: (Elaboracion propia)

UNE	Servicios	Owner
CERTUS	schedule-becasavanzape	GSANCHEZ
TLS	schedule-prd--srv-deb9-certus-docker	GSANCHEZ
UCAL	schedule-prd-srv-win19-mssql-up	AFOX
TLS	schedule-prd-wscampus-deb9	AFOX
TLS	schedule-tls-landing	UNAVARRO
UCAL	schedule-prd-srv-ub16-web-ucal-penu	UNAVARRO
CERTUS	schedule-prd--srv-deb9-comercial-docker	JNAVARRO
TLS	schedule--srv-centos7-zabbix-web	JNAVARRO

Tabla 13. Inventario de Servidores Publicos

Fuente: (Elaboracion propia)

IP Publica	Hostname	Ambiente	S.O.
35.237.198.70	GCP_usa01	DEV	Debian GNU/Linux 10 (64-bit)
35.243.186.9	GCP_usa02	PROD	Debian GNU/Linux 10 (64-bit)
35.185.92.25	GCP_usa03	PROD	Debian GNU/Linux 10 (64-bit)
34.75.220.239	GCP_usa04	PROD	Debian GNU/Linux 10 (64-bit)
34.74.72.82	GCP_usa05	PROD	Debian GNU/Linux 10 (64-bit)
34.75.207.122	GCP_usa06	PROD	Ubuntu GNU/Linux 18 (64-bit)
35.231.65.45	GCP_usa07	DEV	Ubuntu GNU/Linux 18 (64-bit)
35.229.66.195	GCP_usa08	DEV	Debian GNU/Linux 9 (64-bit)

Tabla 14. Inventario de Servidores Publicos

Fuente: (Elaboracion propia)

VLAN ID	VLAN Descripción	Subred
201	Gerentes	131.119.201.0/26
202	Invitados (Ger / Corp)	131.119.202.0/26
299	Corporativo	131.119.199.0/26
501	Administrativos Sede	131.119.200.0/26
504	Servidores / Alarmas	172.100.9.0/24
601	Impresoras	131.119.111.0/27
1	Switch's / AP	131.119.117.0/24
10	Switch's / AP 2	10.100.10.0/24
999	Red de Routers	-
603	VoIP / Telefonos IP	131.119.113.0/26
604	Video streaming	131.119.114.0/27
605	DHCP (WiFi Adm) [priv]	131.119.115.0/27
606	DHCP (WiFi Edu) [pub]	131.119.116.0/24
610	Soporte Everest	131.119.124.0/26
702	Módulos / TV	131.119.2.0/27
703	Sala de Docentes	131.119.3.0/27
704	Cabinas	131.119.4.0/26
705	Aulas	131.119.5.0/26
706	Proyectores	131.119.6.0/26
712	Laboratorio 02	131.119.20.0/26
713	Laboratorio 03	131.119.30.0/26
714	Laboratorio 04	131.119.40.0/26
715	Laboratorio 05	131.119.50.0/26

Tabla 15. Inventario de Segmentos de RED y VLAN

Fuente: (Elaboracion propia)

Inventario de Reglas de Firewall

ID	IP PUBLICA	ORIGEN	DESTINO	IP DESTINO	PUERTOS
866	200.41.102.78	All	NAT_200.41.102.78_10.100.54.39_3389	10.100.54.39	all
828	200.41.102.78	104.208.166.28/32	NAT_200.41.102.78_10.200.4.50_1433 PRUEBAS_APPWEB	10.200.4.50 10.200.4.50	all
403	200.41.102.78	All	Mundo_certus-200.41.102.78	10.200.1.30	all
796	200.41.102.78	35.224.144.76/32 35.245.24.73/32	PRUEBAS_APPWEB	10.200.4.50	all
425	200.41.102.80	All	NAT_200.41.102.80_10.100.54.47	10.100.54.47	all
340	201.234.127.23	10.200.4.0/23	all	all	all
800	201.234.127.23	10.200.1.78/32	all	all	all
253	201.234.127.23	ESET	Actualizaciones_ESET		all
244	201.234.127.23	10.100.54.25/32 10.100.54.26/32 10.100.54.29/32 10.100.54.32/32 10.100.54.33/32	update.microsoft.com windowsupdate.microsoft.com windowsupdate.com download.windowsupdate.com download.microsoft.com test.stats.update.microsoft.com ntservicepack.microsoft.com	all	all
218	201.234.127.23	10.100.54.33/32	all	all	all
716	200.41.102.72	All	mip-campus-200.41.102.72:21 mip-campus-200.41.102.72:23	10.200.1.46 10.200.1.46	FTP TELNET
644	200.41.102.72	All	mip-campus-200.41.102.72:80 mip-campus-200.41.102.72:443 mip-campus-200.41.102.72:8080	10.100.54.40 10.100.54.40 10.100.54.40	all
608	201.234.127.25	137.116.34.22/32 201.234.127.25/32	201.234.127.25-10.100.54.4:389	10.100.54.4	LDAP LDAP_UDP

		54.210.97.57_32 83.48.109.149/32 52.170.169.172/32 34.73.75.107/32 52.186.41.212/32 52.190.39.225/32			
835	201.234.127.25	10.200.1.51/32	200.121.226.127/32 34.73.37.239/32 34.73.75.107/32	200.121.226.127/32 34.73.37.239/32 34.73.75.107/32	all
862	201.234.127.25	10.200.1.52	200.121.226.127/32 34.73.37.239/32 34.73.75.107/32	200.121.226.127/32 34.73.37.239/32 34.73.75.107/32	all
904	201.234.127.25	All	PAT_201.234.127.25-10.200.4.153:7007 PAT_201.234.127.25-10.200.4.153:8007	10.200.4.153 10.200.4.153	all
481	201.234.127.24	10.200.4.62/32	mip-201.234.127.24	10.100.54.34	all
482	201.234.127.24	All	mip-201.234.127.24	10.100.54.34	all
10	201.234.127.22	All	201.234.127.22	10.100.54.100	all
185	190,216,168,151	10.100.54.100/32	all	all	all
86	190,216,168,151	All	mip-190.216.168.151	10.100.54.100	all
184	200.41.102.68	All	mip-campus-200.41.102.68 mip-srvsatelite-200.41.102.75	10.200.1.60 10.200.1.50	all
396	200.41.102.76	All	mip-Intercon-200.41.102.76 mip-Intercon-200.41.102.76	10.200.1.68 10.200.1.68	all
821	200.41.102.81	All	NAT_200.41.102.81_10.200.1.70	10.200.1.70	MYSQL
428	200.41.102.81	all	NAT_200.41.102.81_10.200.1.70	10.200.1.70	HTTP HTTPS SSH SMTP TCP_587 TCP_6379 TCP_11211

					TCP_5432
					TCP_11300
					TCP_39732
					TCP_54370
					TCP_54364
					TCP_54372
					TCP_54366
					TCP_40532
					TCP_47526
					TCP_47522
					TCP_34645
					TCP_3306

Tabla 16. Inventario de Reglas de Firewall
Fuente: (Elaboracion propia)

Durante el levantamiento de Información correspondiente a Políticas de Firewall Ipv4 se encontraron las siguientes brechas de seguridad y malas prácticas.

- Existen políticas que tienen expuestos todos los puertos TCP/UDP
- No se tiene un orden de agrupación de servicio o puertos.
- No se tienen identificados los orígenes, se evidencian políticas all to all
- Se evidencio que los puertos de Mysql se encontraron expuestos y no se tenía identificados los orígenes
- Se encontró políticas que no tienen aplicados Filtros de web y control de aplicaciones.
- Se encontró políticas que no tenían aplicado la inspección ssl
- Se encontró políticas que tenían activado la recolección de logs.

Telefonía Voip

A nivel del servicio VOIP en el Holding IEDUCA se tenía los siguientes sistemas:

UNE	Sistema VOIP	SERVER SIP	Ubicación	Cantidad de Licencias
CERTUS	CCVOX	10.200.2.230	Data Center LVL3	63
TLS	GENESYS	192.168.6.120	Data Center Chacarilla	23
UCAL	GENESYS	10.150.3.20	Data Center UCAL	15

Tabla 17. Inventario de Sistemas de Call Center IEDUCA

Fuente: (Elaboracion propia)

Ambos sistemas VOIP al encontrarse en redes WAN diferentes no es posible compartir el recurso con las demás Unes, en certus se tienen licencias disponibles por usar, pero no puede ser compartido a menos que todo se encuentre integrado dentro de una sola RED WAN.

Telefonía IP SIPTRUNK

UNE	CENTRAL TELEFONICA	SERVER SIP	Ubicación
CERTUS	AVAYA IPO	10.100.54.250	Data Center LVL3
TLS	CISCO CUCM	10.20.90.10	Data Center Chacarilla
UCAL	CISCO CUCM	10.150.90.10	Data Center UCAL

Tabla 18. Inventario de Centrales telefonicas IEDUCA

Fuente: (Elaboracion propia)

Lo mismo pasa con el uso de las centrales telefónicas de cada UNE que poseen licencias disponibles pero su uso está limitado a la arquitectura de RED actual.

Sistema de Video Vigilancia

El sistema de video Vigilancia es muy importante para la organización, puesto que a través de este sistema personal de seguridad puedo monitorear y vigilar en tiempo real zonas vulnerables dentro del predio de cada sede de cada Une.

Durante el levantamiento de información se encontró que existen gran cantidad de cámaras y dispositivos NVR que graban y guardan dichas grabaciones para posteriormente ser consultados por el administrador del sistema, este sistema solo puede ser consultado estando en la misma sede donde se encuentra el NVR, no es posible visualizar la grabación de las cámaras desde una sede remota puesto que la arquitectura WAN no lo permite al contar con 3 redes privadas totalmente separadas.

1. Inventario de Cámaras

UNE	SEDE	Q CAMARAS	TIPO	
TLS	CHACARILLA	40/25	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	JAVIER PRADO	20/20	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	NORTE	10/10	IP BULLET 2MP WDR	IP DOMO 2MP WDR
CERTUS	SURCO	44/27	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	NORTE	40/20	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	SJL	40/15	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	ATE	40/17	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	VES	43/9	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	CALLAO	41/23	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	AQP	25/10	IP BULLET 2MP WDR	IP DOMO 2MP WDR

	CIX	24/7	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	SAN MIGUEL	12/8	IP BULLET 2MP WDR	IP DOMO 2MP WDR
	OLIVOS	40/7	IP BULLET 2MP WDR	IP DOMO 2MP WDR
UCAL	MOLINA	31/22	IP BULLET 2MP WDR	IP DOMO 2MP WDR

Tabla 19. Inventario de Camaras IP
Fuente: (Elaboracion propia)

2. Inventario de NVR/DVR

EQUIPO	VLAN	IP	MODELO	SEDES
NVR_1_CERTUS	200	10.100.6.250	DHI-NVR5864-4KS2	CERTUS/SURCO
NVR_2_UCAL	100	10.150.20.251	DHI-NVR5864-4KS2	UCAL/MOLINA
NVR_970	506	10.40.70.253	DSS7016DR	TLS/CHACARILLA
		10.40.70.253		
		DSS CLIENT		
PC_MONITOREO	230	10.40.6.249	DSS7016DR	TLS/CHACARILLA

Tabla 20. Inventario de Dispositivos NVR/DVR
Fuente: (Elaboracion propia)

Se verifica que se tiene hasta 4 dispositivos de grabación en cada sede de cada Une. Dichos equipos guardan hasta 3 meses de grabación.

Definir objetivos de la organización.

A continuación, se presentan los objetivos considerados por la organización

- ✓ Reducción de costos de operación

- ✓ Adicionar productos de Vanguardia tecnológica
- ✓ Mantener una posición competitiva en el mercado
- ✓ Brindar servicios con disponibilidad al 100%
- ✓ Mejorar la experiencia de Navegación de los alumnos
- ✓ Asegurar la continuidad del negocio
- ✓ Incrementar la productividad

Definir posibles limitaciones de la organización.

- Presupuesto
- Tiempo
- Políticas de Seguridad de la Información
- No afectar procesos de matrícula o campañas de call center clave durante la migración

Definir Objetivos Técnicos.

Los objetivos técnicos identificados a continuación están alineados a los objetivos de la organización.

- ✓ Renovación Tecnológica.
- ✓ Simplificar la administración de Enlaces WAN.
- ✓ Reducir tiempos de atención de Incidentes y Requerimientos SLA.
- ✓ Proveer escalabilidad a la red.
- ✓ Proveer seguridad Perimetral a la red lan.
- ✓ Permitir compartir recursos y servicios.
- ✓ Proveer enlaces redundantes hacia internet
- ✓ Proveer una RED con calidad de Servicio (QoS).

Elaboración de RFP y Proceso de Licitación:

- ✓ Elaboración de RFP o Alcance Técnico
- ✓ Comunicación de Licitación para el Proyecto a Proveedores
- ✓ Elaboración de Cronograma de Visitas Técnicas para evaluar Factibilidad por parte del proveedor.
- ✓ Elaboración de Cronograma de Consultas Técnicas vía google Meet.
- ✓ Recepción de Propuestas Técnicas para evaluación.
- ✓ Evaluación de Propuestas Técnicas.
- ✓ Comunicación de proveedor Adjudicador y proveedores que no ganaron

RFP:

Descripción de los Servicios:

- Internet
- Datos (mpls)
- Seguridad Cloud
- Seguridad DMZ
- Soporte SMARTNET

Sedes: Se detallan las sedes Remotas por cada Unidad de Negocio y los Data Center en donde se tienen alojados los servicios Core de negocio.

UNE	SEDES REMOTAS	TAMAÑO	Dirección
ITLS	CAMPUS CHACARILLA	GRANDE	Av. Primavera 970
	CAMPUS JAVIER PRADO	GRANDE	Av. Javier Prado Oeste 980
	SEDE SAN MIGUEL	MEDIANO	Av. Universitaria 1027
	SEDE LIMA NORTE	MEDIANO	Centro Comercial Plaza Norte
UCAL	CAMPUS UCAL	GRANDE	Av. La molina 3755
	SEDE SURCO	GRANDE	Av. Santiago de Surco N° 4717

CERTUS	SEDE NORTE	GRANDE	Av. Industrial N° 3733
	SEDE SJL	GRANDE	Av. Pirámide del Sol N° 810
	SEDE ATE	GRANDE	Av. Nicolás Ayllón N° 816-818
	SEDE AREQUIPA	GRANDE	Av. Los Incas Lote 1, Arequipa
	SEDE VILLA EL SALVADOR	GRANDE	Av. Pachacutec N° 403
	SEDE CALLAO	GRANDE	Av. Argentina N° 2430
	SEDE CHICLAYO	GRANDE	Calle Manuel Urteaga N° 540
	DATA CENTER LUMEN	GRANDE	Data Center Lima PERU
	SEDE SAN MIGUEL	MEDIANO	Av. La Marina N° 3315
	SEDE LOS OLIVOS	MEDIANO	Jr. Cajahuamán N° 863

Tabla 21. Direcciones de Sedes y Unidades de Negocio
Fuente: (Elaboracion propia)

Anchos de Banda: Aquí se definen los anchos de banda solicitados para cada sede y la data center donde se tiene alojados los servicios Core, en la tabla se detallan el esquema de alta disponibilidad aplicado.

Esquema de Alta Disponibilidad CERTUS: Activo – Pasivo

Esquema de Alta Disponibilidad ITLS: Activo – Activo

Esquema de Alta Disponibilidad UCAL: Activo - Activo

UNE	SEDE	TIPO	BW MPLS	BW INTERNET PRINCIPAL	BW INTERNET BACKUP
CERTUS	SEDE SURCO	PRINCIPAL	200 Mbps	1 Gbps	1 Gbps
	SEDE SURCO	BACKUP	200 Mbps		
	SEDE SJL	PRINCIPAL	100 Mbps		
	SEDE SJL	BACKUP	100 Mbps		
	SEDE AQP	PRINCIPAL	100 Mbps		
	SEDE AQP	BACKUP	100 Mbps		
	SEDE CALLAO	PRINCIPAL	100 Mbps		
	SEDE CALLAO	BACKUP	100 Mbps		
	SEDE SM	PRINCIPAL	50 Mbps		
	SEDE SM	BACKUP	50 Mbps		
	SEDE NORTE	PRINCIPAL	50 Mbps		
	SEDE NORTE	BACKUP	50 Mbps		
	SEDE ATE	PRINCIPAL	50 Mbps		
	SEDE ATE	BACKUP	50 Mbps		
	SEDE VES	PRINCIPAL	100 Mbps		
	SEDE VES	BACKUP	100 Mbps		
	SEDE CIX	PRINCIPAL	50 Mbps		
	SEDE CIX	BACKUP	50 Mbps		
	SEDE LOO	PRINCIPAL	50 Mbps		
	SEDE LOO	BACKUP	50 Mbps		
	SEDE LVL3	PRINCIPAL	200 Mbps		
	SEDE LVL3	BACKUP	200 Mbps		
ITLS	SEDE CHA	PRINCIPAL	200 Mbps	600 Mbps	-
	SEDE JP	PRINCIPAL	150 Mbps	540 Mbps	-
	SEDE NORTE	PRINCIPAL	40 Mbps	50 Mbps	-
	SEDE SM	PRINCIPAL	40 Mbps	50 Mbps	-
UCAL	SEDE MOLINA	PRINCIPAL	100 Mbps	300 Mbps	-
DC - ISP	KRUMDIECK	PRINCIPAL	-	600 Mbps	600 Mbps
DC - ISP	KRUMDIECK	BACKUP	-	600 Mbps	600 Mbps

Tabla 22. Anchos de banda requeridos Internet y MPLS
Fuente: (Elaboracion propia)

Seguridad Cloud: En este punto se solicitó aspectos y Características de seguridad perimetral que fueron alineados a las necesidades del negocio y la creciente amenaza de ataques cibernéticos hacia servicios Core del negocio.

UNE	Equipo de Seguridad	Características
Certus	Firewall Perimetral	Antivirus, IPS, FILTRO WEB, CONTRO APPS
	Cloud	VPN SSL, VPN IPSEC, Esquema HA.
	AntiDDos Cloud	Protección de Ataques Volumétricos y Fuerza bruta
ITLS/UCAL	Firewall Perimetral	Antivirus, IPS, FILTRO WEB, CONTRO APPS, VPN SSL, VPN IPSEC, Esquema HA.
	Sandboxing Cloud	Protección Ransomware, Antispyware, zero day
	AntiDDos Cloud	Protección de Ataques Volumétricos y Fuerza bruta.
	WAF Cloud	Protección Servicios Publicados.

Tabla 23. Características de Seguridad Firewall

Fuente: (Elaboracion propia)

Seguridad DMZ: En la sede TLS Chacarilla se consideraron 2 Equipos FW para mantener la DMZ existente, así como las conexiones hacia el SW CORE L3.

UNE	Equipo de Seguridad DMZ	Características
TLS SEDE CHACARILLA	FIREWALL DMZ	Antivirus, IPS, FILTRO WEB, CONTRO APPS
		DNS FILTERING, WAF

Tabla 24. Características de Seguridad Firewall DMZ

Fuente: (Elaboracion propia)

Soporte SMARTNET: Se solicitó al proveedor brindar un contrato de Soporte SMARTNET con el fabricante CISCO debido a que algunos equipos CORE se encontraron fuera de soporte.

SEDES	MARCA	MODELO	HA	SMARTNET
CHACARILLA	CISCO	Nexus9000 C9372PX chassis	PRINCIPAL	1 Años
CHACARILLA	CISCO	Nexus9000 C9372PX chassis	BACKUP	1 Años
JAVIER PRADO	CISCO	Nexus9000 93180YC-EX chassis	PRINCIPAL	1 Años
JAVIER PRADO	CISCO	Nexus9000 93180YC-EX chassis	BACKUP	1 Años

Tabla 25. Listado Equipos Soporte SMARNET

Fuente: (Elaboracion propia)

Condiciones de Soporte y SLA:

- El nivel de servicio debe ser al menos al 99.95%
- Tiempos de Atención ante incidentes menores a 4 hrs de resolución
- Tiempos de Atención ante requerimientos menores a 8 hrs de resolución

Condiciones de Entrega y Forma de Pago:

Aquí se definen los anchos de banda solicitados para cada sede y el data center donde se tiene alojados los servicios Core, en la tabla se detallan el esquema de alta disponibilidad aplicado.

- Se deberá efectuar en 45 días calendario como máximo
- Los pagos se realizan en nuevos soles, dentro de los 90 días de presentada la factura
- El contrato tendrá una duración de 24 meses como mínimo.

Definir posibles limitaciones técnicas.

- Cantidad de IPS publicas
- Capacidad de interfaces de red (transceiver, patch Core de fibra)
- Integración con otras marcas utilización de protocolos estándar
- Direccionamiento IP Publico usado en entornos privados

- Cantidad de segmentos de red sin sumarizar

3.2.5.3 Fase de Planeación

En esta etapa se realiza la planificación técnica para la ejecución del cambio de proveedor ISP, migración de servicio de internet e implementación de buenas prácticas y aplicación de mejoras al campo de la seguridad perimetral.

Siguiendo el modelo de Referencia PPDIOO de cisco se tiene los siguientes 3 pasos.

Paso 1: Identificar Información, documentación de la Organización

En este punto se realiza una revisión general de la red actual, se ejecuta el levantamiento de información buscando deficiencias

Para identificar información se hace uso de herramientas que permitan levantar información de red de equipos de borde como routers cpe, switches core, firewall, conexiones a nivel de interfaces físicas.

Existen herramientas que permiten recoger datos de la red como uso de memoria, CPU de equipos cisco u otros fabricantes. Se puede hacer uso de un Cisco Prime en equipos de marca cisco o un airwave en el caso de la marca Aruba y HP.

Es importante recoger la siguiente información:

- a. Uso de CPU/RAM no más de 75% por intervalos de 5 minutos.
- b. Tiempos de respuesta hacia internet, estos deben ser menores a 50 ms.
- c. Tiempos de respuesta entre sedes remotas debe ser menores a 3 ms.
- d. Las conexiones a nivel WAN deberán tener un uso menor al 70%
- e. Validar si existe segmentación Lógica a nivel de direccionamiento IPv4/IPv6

- f. Validar si todos los segmentos de red trabajan con direccionamiento privado
- g. Validar si existen aplicaciones que están asociados a alguna IP Publica en sus archivos de configuración.
- h. Validar la cantidad de IPS Publicas
- i. Identificar la cantidad y tipos de puertos que se tienen abiertos por aplicación o servicio.
- j. Validar el tipo de calidad de servicio y caudales asignados a los tipos de trafico
- k. Validar políticas de seguridad, permisos, accesos.
- l. Identificar cantidad de conexiones IPSEC.
- m. Identificar cantidad de portales VPN SSL.

Paso 2: Realizar una Auditoria de red que agregue detalles a la descripción de la red.

El proceso de levantamiento de información conlleva la ejecución de comandos a través de la línea de comandos CLI usando comandos SHOW, DEBUG, LOG, TRAZAS, ICMP, todo esto aplicado a las 3 Capas (Acceso, Distribución y Core)

>SHOW VERSION
>SHOW RUN
>SHOW IP INT BRIEF
>SHOW PROCESS CPU HISTORY
>DEBUG IP ROUTE
>SHOW LOG
>TRACERT [IP]
>PING [IP]

Tabla 26. Listado de comandos CLI
Fuente: (Elaboracion propia)

Estos comandos también fueron aplicados al equipo de seguridad Firewall Fortinet

Paso 3: Herramientas para inventario de RED

A continuación, se muestra el inventario de equipos recogidos con la herramienta Airwave de Aruba en la cual se muestran los datos del equipo a nivel de Networking y Wireless, la unidad de negocio de Certus el 80% de su equipamiento a nivel LAN y Wireless están bajo un esquema de alquiler.

Para la recolección de Información correspondiente a las UNES de TLS y UCAL se utilizó una herramienta de cisco prime en la cual se identificación equipamiento fuera de soporte.

Equipamiento UNE TLS y UCAL fuera de Soporte:

SURCO

- Nexus9000 C9372PX chassis - SN: SAL2006Y5TE
- Nexus9000 C9372PX chassis - SN: SAL2006Y9M0

JAVIER PRADO

- Nexus9000 93180YC-EX chassis - SN: FDO204203SV
- Nexus9000 93180YC-EX chassis - SN: FDO204203TX

MOLINA

- Nexus3500 C3548P-10GX Chassis - SN: FOC2246R0WS
- Nexus3500 C3548P-10GX Chassis - SN: FOC2246R0ZS

Ubicación	Piso	Nombre de Switch / AP	Rol	Marca	Modelo	SW Version	SW Imagen
Datacenter		CERLIMSURSWCORE_01	CORE	HP	A5820X-24XG-SFP+	5.20.105	5.20.105, Release 1808P27
		CERLIMSURSWCORE_01	CORE	HP	A5820X-24XG-SFP+	5.20.105	5.20.105, Release 1808P27
Pabellón	1	CERLIMASURSWACS_Piso1	ACCESO	HP	J9729A 2920-48G-PoE+	WB.15.16	WB.15.16.0005
		CERLIMASURSWACS_CIDOC	ACCESO	HP	HP J9147A 2910al-48G	N.11.15	N.11.15
Pabellón	2	CERLIMASURSWACS_01P2	ACCESO	HP	HP J9147A 2910al-48G	W.15.14	W.15.14.0009
		CERLIMASURSWACS_02P2	ACCESO	HP	J9147A 2910al-48G	W.15.14	W.15.14.0009
Pabellón	3	CERLIMSURSWACS_P03_01	ACCESO	HP	5500-48G-PoE+-4SFP	5.20.99	5.20.99 Release 5501P03
		CERLIMSURSWACS_P03_01	ACCESO	HP	5500-48G-PoE+-4SFP	5.20.99	5.20.99 Release 5501P03
		CERLIMSURSWACS_P03_04	ACCESO	HP	ProCurve J9022A Switch 2810-48G	N.11.15	N.11.15
		CERLIMSURSWACS_P03_02	ACCESO	HP	J9147A 2910al-48G	W.14.06	W.15.14.0009
		CERLIMSURSWACS_P03_03	ACCESO	HP	HP J9729A 2920-48G-PoE+	WB.16.01	WB.16.01
		WLC_PRC_P3	CONTROLADOR	ARUBA	Aruba7030	8.5.0.4	8.5.0.4
Pabellón	4	CERLIMSURSWACS_P04_01	ACCESO	HP	J9727A 2920-24G-PoE+	WB.15.16	WB.15.16.0005
		CERLIMSURSWACS_P04_02	ACCESO	HP	ProCurve J9147A 2910al-48G	W.14.06	W.14.38
Pabellón	5	CERLIMSURSWACS_P05_02	ACCESO	HP	J9145A 2910al-24G	W.14.38	W.14.38
		CERLIMSURSWACS_P05_03	ACCESO	CISCO	WS-C2960S-48FPS-L	12.2(55)SE3	C2960S-
Pabellón	6	CERLIMSURSWACS_P06_02	ACCESO	HP	J9729A 2920-48G-PoE+	WB.16.03	WB.16.03.0003
		CERLIMSURSWACS_P06_03	ACCESO	HP	J9729A 2920-48G-PoE+	WB.16.02	WB.15.15.0012

Pabellón	7	CERLIMSURSWACS_P07_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.03	WB.16.03.0003
		CERLIMSURSWACS_P07_02	ACCESO	HP	J9145A 2910a1-24G	W.15.14	W.15.14.0009
Pabellón	8	CERLIMSURSWACS_P08_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
		CERLIMSURSWACS_P08_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
Pabellón	9	CERLIMSURSWACS_P09_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
		CERLIMSURSWACS_P09_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
Pabellón	10	CERLIMSURSWACS_P10_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
		CERLIMSURSWACS_P10_01	ACCESO	HP	J9729A 2920-48G-POE+	WB.16.01	WB.16.01.0007
Access Poin		AP_PRC_P9_PZO2	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P9_PZO1	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P8_PAS	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_P7_PZO2	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P7_PZO1	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P6_PZO2	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_P6_PZO1	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_P4_LAB4	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P2_PZO2	ACCESS POINT	ARUBA	215	8.5.0.4	8.5.0.4_72900
		AP_PRC_P1_PAT	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_P1_COMEDOR	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_P1_CID	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP_PRC_Backup2	ACCESS POINT	ARUBA	315	8.5.0.4	8.5.0.4_72900
		AP143	ACCESS POINT	ARUBA	115	8.5.0.4	8.5.0.4_72900
		AP142	ACCESS POINT	ARUBA	115	8.5.0.4	8.5.0.4_72900
		AP141	ACCESS POINT	ARUBA	115	8.5.0.4	8.5.0.4_72900

Tabla 27. Inventario Equipos Certus sede Principal
Fuente: (Elaboracion propia)

3.2.5.4 Fase de Diseño

Finalmente, después de realizar el recojo de información y la auditoria a la red para saber su estado de salud actual, con todo esto se procede a desarrollar y proponer el Diseño de la RED que tienen 4 Ejes fundamentales los cuales se encuentran alineados a las necesidades y objetivos de la organización.

- ✓ Esquema de direccionamiento IPv4
- ✓ Diagrama de Diseño de RED WAN LAN
- ✓ Diagrama de Diseño de Seguridad
- ✓ Diseño de Calidad de Servicio para Telefonía IP

Así mismo continuando con el proceso de diseño definido en la metodología PPDIIOO los pasos a seguir son los siguientes:

Paso 1: Análisis de los requisitos de la aplicación y organización

En este paso se realiza una evaluación de todos los requisitos que se obtuvieron del levantamiento de información adicionalmente se usa la información de la salud de red incluyendo el rendimiento de las conexiones, equipamiento y componentes de red.

Se analiza también los tiempos de respuesta hacia internet y nubes privadas, conexión entre sedes remotas, se miden los tiempos de respuesta delay, intermitencia, jitter.

El diseño se consideró en base a los lineamientos, objetivos y necesidades del negocio.

Diseño de RED WAN

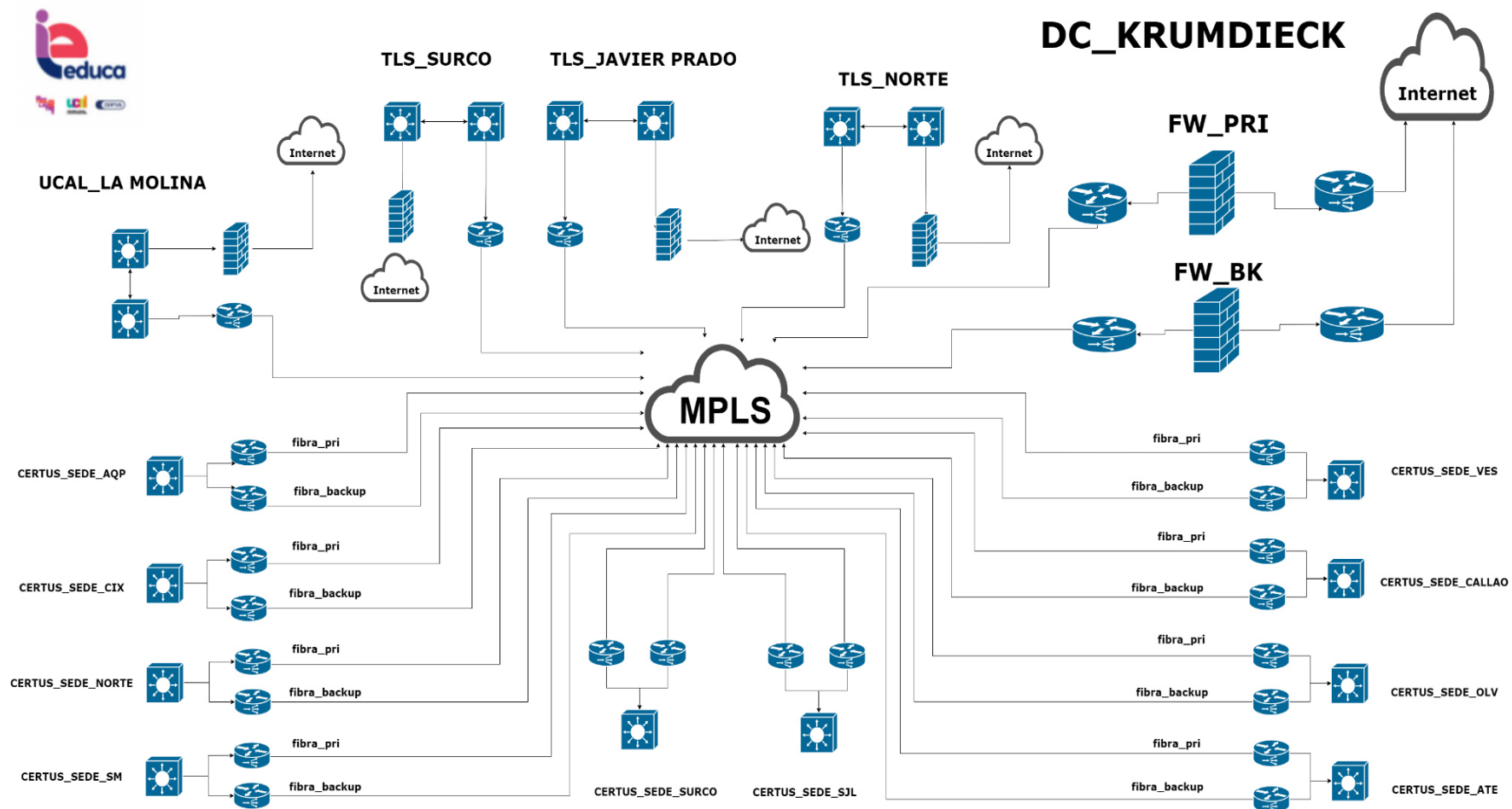


Figura 20. Diseñ de RED FISICA – WAN IEDUCA
Fuente: (Formatos proyectos ieduca)

Consideraciones del Diseño:

1. En el diagrama de red físico se plantea un esquema de arquitectura FULL MESH, en la cual cada sede correspondiente a cada UNE puede comunicarse con otra sin necesidad de ir a una cabecera central.
2. La arquitectura Full Mesh tiene como ventajas reducir los tiempos de respuesta entre sedes remotas y asegurar la comunicación directa sin aumentar los saltos entre ambas.
3. Para la UNE CERTUS se plantea un esquema de Activo – Pasivo, en la cual tanto el enlace principal como contingencia tienen rutas distintas y aseguran la alta disponibilidad de la sede.
4. El internet centralizado para CERTUS se encuentra ubicado en el Data Center del proveedor el cual es un Data Center tier3 que brinda contingencia a nivel de salidas internacionales hacia internet.
5. Tanto para TLS/UCAL se plantea un Esquema Activo – Activo en la cual ambos enlaces tanto MPLS como Internet se encuentran activos y es la funcionalidad de SDWAN de los equipos Fortinet quien decide el mejor camino para enrutar los paquetes hacia los destinos.
6. Cada sede remota de TLS/UCAL cuenta con un internet en cada sede la cual brinda conexión hacia internet y seguridad perimetral en cada sede.
7. Las publicaciones o nateos se realizan en cada SEDE DE TLS/UCAL reduciendo con esto los tiempos de respuesta hacia dichos servicios.
8. Ante la caída del servicio de Internet en las sedes de TLS/UCAL los Equipos Fortigate 200E instalados en cada sede toman la decisión de conmutar los paquetes hacia la salida de Internet Centralizada ubicada en el DC de Krumdieck del proveedor.
9. En cada sede se consideraron equipos router que puedan soportar los anchos de banda definidos en el RFP, así como al incremento a futuro en caso de realizar un upgrade.
10. Bajo este diseño se logra mejorar la gestión de las sedes remotas bajo una sola plataforma de administración y control.

11. La arquitectura Full Mesh nos permite compartir recursos y servicios bajo la tecnología MPLS aplicando Calidad de servicio según el tráfico sea encapsulado.
12. Al tener un mayor control de las sedes y monitoreo se logra ejecutar un proceso de troubleshooting mas rápido y reporte en caso de una avería por parte del proveedor.
13. Para la conectividad se consideró enrutamiento estático, creando rutas hacia cada sede remota.

Topología SDWAN

DISEÑO SD WAN - IEDUCA

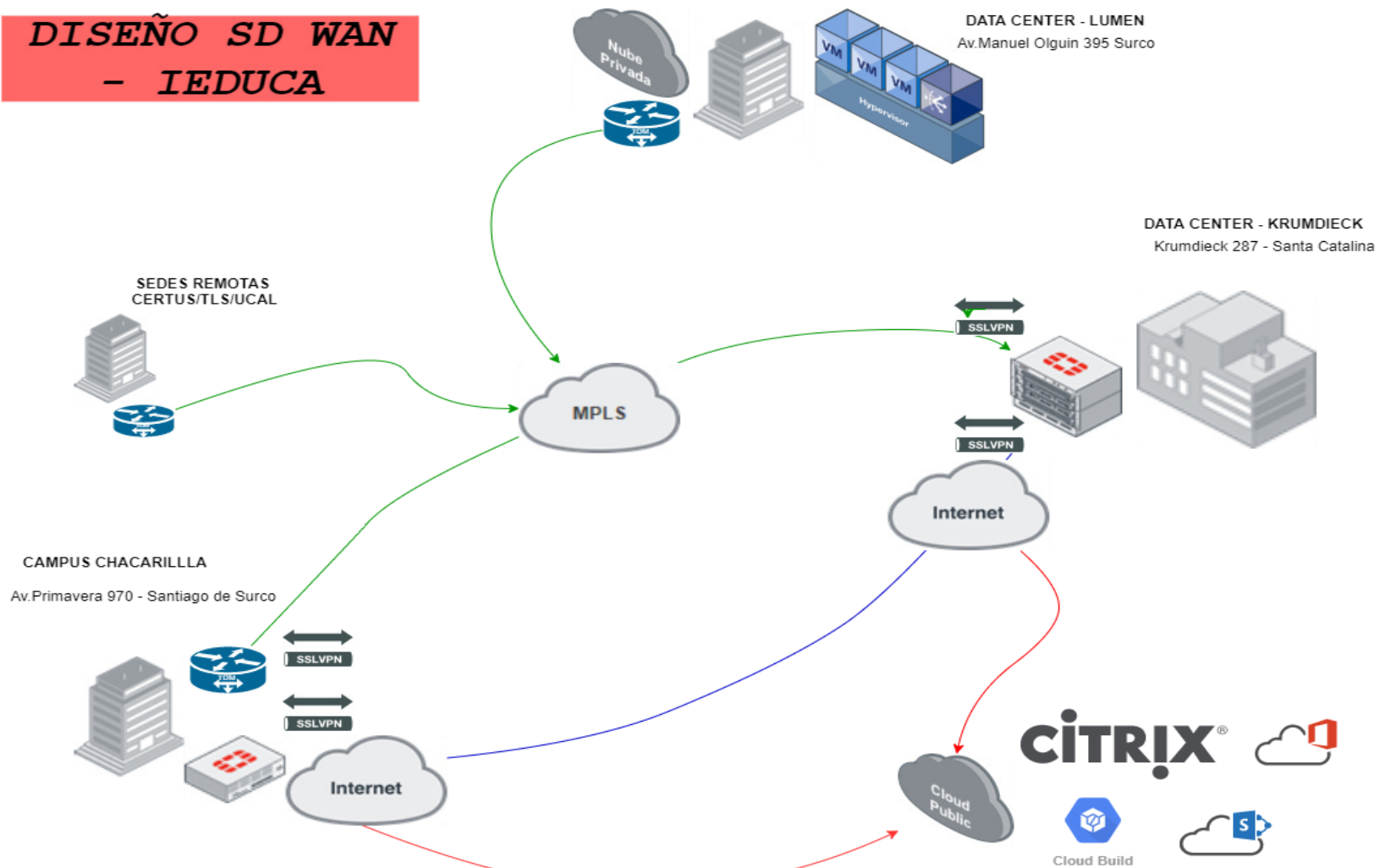


Figura 21. Topología de RED SDWAN –IEDUCA
Fuente: (Formatos proyectos ieduca)

Consideraciones del Diseño:

1. Se aprovecha la funcionalidad de SDWAN embebida en los equipos Fortinet sin necesidad de contar con un licenciamiento especial que encarezca la solución.
2. Dicha funcionalidad principalmente establece que al tener 2 salidas hacia internet ya sea a través de diferentes tecnologías como (INTERNET, MPLS, 4G/5G ETC), se puede utilizar ambas para enviar el tráfico por el mejor camino en términos de Latencia, Delay, Perdida de paquetes, Jitter.
3. La topología diseñada permite aprovechar el uso de SDWAN al tener 2 salidas de Internet uno en las sedes de TLS/UCAL y la otra usando el internet centralizado de CERTUS, sin perder comunicación hacia los servicios hosteados en las nubes privadas que actualmente se tienen.
4. Los servicios que se encuentran publicados están configurados de tal manera que al utilizar una IP Publica en determinado momento puedan usar otra sin necesidad de cambio o configuración a nivel del DNS, esto debido a que cada publicación o nateo se asigna a un POOL de direcciones IPS registradas en la sede remota y la sede centralizada.

Topología de RED Telefonía VOIP

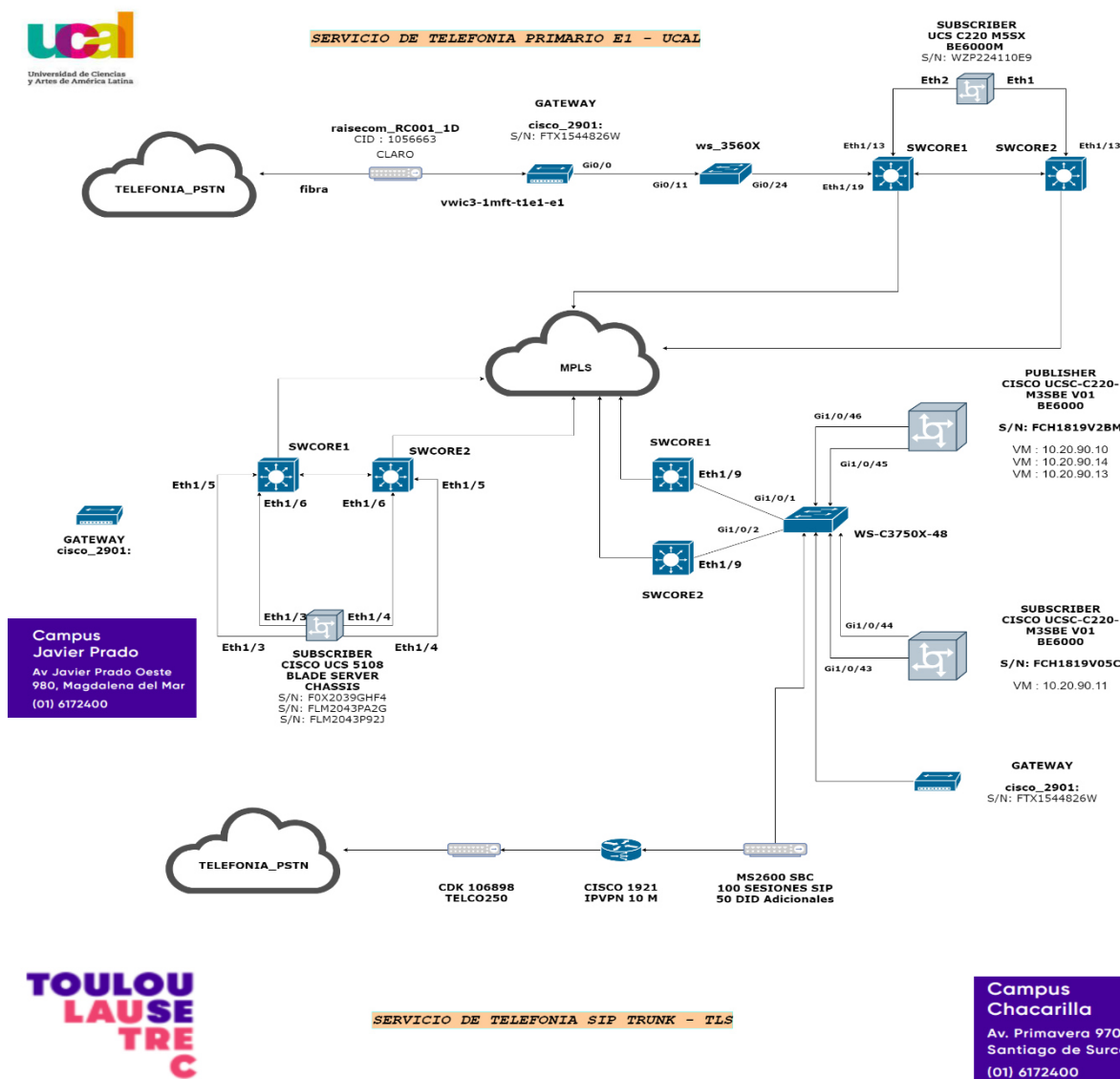


Figura 22. Topología de Telefonía IP
Fuente: (Formatos proyectos ieduca)

Consideraciones del Diseño:

1. Para mejorar el uso de recursos a nivel de Telefonía IP se aprovecha el diseño de red WAN utilizando MPLS para priorizar el tráfico de VOZ entre las sedes.

2. Bajo este esquema se pueden utilizar ambos sistemas de Telefonía IP (AVAYA, CISCO), y de esta forma poder aprovechar mejor los recursos del negocio sin incurrir en más gastos.
3. En el diseño se observa que TLS y UCAL ahora pueden compartir la central telefónica y ante una avería en cualquiera de las sedes el servicio permanezca activo gracias al esquema de replicación de servidores IP que se plantea.
4. Así mismo los anexos telefónicos de cada sede se registrarán en cada equipo SUBSCRIBER y PUBLISHER para de esta forma tener redundancia ante la caída de cualquier de estos equipos.
5. El ingreso de las llamadas permanece en cada sede y se mantienen los números de cada central telefónica correspondientemente.

Plan de Direcccionamiento IPv4

El esquema de direccionamiento IPv4 Propuesto obedece principalmente a solucionar los siguientes problemas:

- Duplicidad de IPs
- Traslape de Subredes
- reducir los dominios de Broadcast
- Optimizar el tráfico Broadcast LAN.
- Optimizar el uso de segmentos de red LAN virtual (VLAN)
- Sumarizar segmentos de RED.

UNE	Sedes	RED	Descripción	VLAN ID	Segmento de SUBRED
CERTUS	Sede Surco	ADMIN	red_cableada	100	10.100.54.0/24
			red_wifi	101	10.100.54.0/24
			red_servidores	102	10.100.54.0/24
			red_telefonia	103	10.100.54.0/24
			red_videovigilancia	104	10.100.54.0/24
			red_gestion	105	10.100.54.0/24
			red_dispositivos	106	10.100.54.0/24
		ACAD	red_aulas_labos	200	10.201.2.0/23

			red_wifi	201	10.201.4.0/22
ITLS	Campus Chacarilla	ADMIN	red_cableada	100	10.30.0.0/24
			red_wifi	101	10.30.1.0/24
			red_Servidores	102	192.168.0.0/23
			red_telefonia	103	10.30.2.0/24
			red_videovigilancia	104	10.30.3.0/24
			red_gestion	105	10.30.4.0/24
			red_dispositivos	106	10.30.5.0/24
			red_DMZ	107	172.16.0.0/23
		ACAD	red_cableada	200	10.31.54.0/24
			red_wifi	201	10.31.54.4/22
			red_servidores	202	10.31.54.8/24
UCAL	Campus La Molina	ADMIN	red_cableada	100	10.150.0.0/24
			red_wifi	101	10.150.1.0/24
			red_Servidores	102	10.150.2.0/24
			red_telefonia	103	10.150.3.0/24
			red_videovigilancia	104	10.150.4.0/24
			red_gestion	105	10.150.5.0/24
			red_dispositivos	106	10.150.6.0/24
			red_DMZ	107	10.150.7.0/24
		ACAD	red_cableada	200	10.151.0.0/24
			red_wifi	201	10.151.4.0/22
			red_servidores	202	10.151.0.0/24

Tabla 28. Plan de Direccionamiento IP Sedes (molina, chacarilla, surco)

Fuente: (Elaboracion propia)

La tabla 28 nos muestra el detalle de las sedes más críticas de cada UNE y el direccionamiento IP utilizado.

En la mayoría de casos se hizo uso de un direccionamiento privado IPv4 clase A, debido a la cantidad de subredes que el negocio requiere.

Los segmentos de RED Wifi son los que mayor cantidad de IPS utilizables tienen debido a que en cada campus o sede de las UNES se brinda el servicio de Wifi a los estudiantes.

UNE	Sedes	RED ADMIN	RED ACAD
	Sede Surco	10.100.0.0/16	10.101.0.0/16
	Sede SJL	10.120.0.0/16	10.121.0.0/16
	Sede Norte	10.125.0.0/16	10.126.0.0/16
	Sede Ate	10.136.0.0/16	10.137.0.0/16

CERTUS	Sede Olivos	10.130.0.0/16	10.230.0.0/16
	Sede VES	10.102.0.0/16	10.202.0.0/16
	Sede Callao	10.131.0.0/16	10.231.0.0/16
	Sede Arequipa	10.132.0.0/16	10.232.0.0/16
	Sede Chiclayo	10.160.0.0/16	10.161.0.0/16
	Sede San Miguel	10.115.0.0/16	10.116.0.0/16
ITLS	Campus Chacarilla	10.30.0.0/16	10.31.0.0/16
	Campus Javier Prado	10.40.0.0/16	10.41.0.0/16
	Sede Lima Norte	10.10.0.0/16	10.11.0.0/16
	Sede San Miguel	10.20.0.0/16	10.21.0.0/16
UCAL	Campus La Molina	10.150.0.0/16	10.151.0.0/16

Tabla 29. Resumen Sumarizado Plan de Direccionamiento IP Sedes IEDUCA
Fuente: (Elaboracion propia)

La tabla 29 muestra un resumen de las REDES por cada unidad de negocio y sus respectivas sedes.

En esta podemos observar que todas las Redes son distintas y se corrige el problema de duplicidad que dificulta la comunicación bajo un esquema de red full mesh.

Listado de Equipamiento:

A continuación, se lista el total de equipos considerados para implementar la Arquitectura de Red.

Equipamiento WAN

Equipos	Tipo	Cantidad	Imagen	Detalles
CISCO ASR 920	Router	4		Ver ANEXO 1: DATASHEET Cisco ASR 920

FG-200E	Router	8		Ver ANEXO 2: DATASHEET FG-200E.
CISCO ISR 1100	Router	4		Ver ANEXO 3: DATASHEET CISCO ISR 1100 4 p
FG-501E	Router	2		Ver ANEXO 4: DATASHEET FG-501E.
FG-60F	Router	16		Ver ANEXO 5: DATASHEET FG-60F

Tabla 30. Listado Equipamiento Router
Fuente: (Elaboracion propia)

Equipamiento LAN

Equipos	Tipo	Cantidad	Imagen	Detalles
Nexus 9k	Switch Core	2		Ver ANEXO 6: DATASHEET Cisco Nexus 9k

Tabla 31. Listado Equipamiento Lan
Fuente: (Elaboracion propia)

Equipamiento DMZ y Seguridad Perimetral

Equipos	Tipo	Cantidad	Imagen	Detalles
Fortinet	Firewall Cabecera	2		Ver ANEXO 7: DATASHEET FG5001E

Fortinet	Firewall DMZ	2		Ver ANEXO 8: DATASHEET Cisco FG501E
Fortinet	Firewall SDWAN	4		Ver ANEXO 9: DATASHEET FG200E

Tabla 32. Listado Equipamiento Firewall y DMZ
Fuente: (Elaboracion propia)

Equipamiento Reporteador y Componentes

Equipos	Tipo	Cantidad	Imagen	Detalles
Fortinet	FAZ	1		Ver ANEXO 10: DATASHEET T 800F
Componentes	Transceiver	15		Ver ANEXO 11: DATASHEET T

Tabla 33. Listado Equipamiento Faz y Componentes
Fuente: (Elaboracion propia)

Diseño de Calidad de Servicio a Nivel LAN/WAN y Telefonía IP

Calidad de Servicio

El tratamiento de tráfico bajo políticas de Calidad de Servicio (QoS) que permitan la administración de las Clases de Servicio para brindar priorización del tráfico de datos, Voz y Video garantizando de esta manera el funcionamiento de sus aplicaciones, brindando además la ampliación de planes hasta 5 Calidades de Servicio (03 Calidades de Servicio de manera estándar).

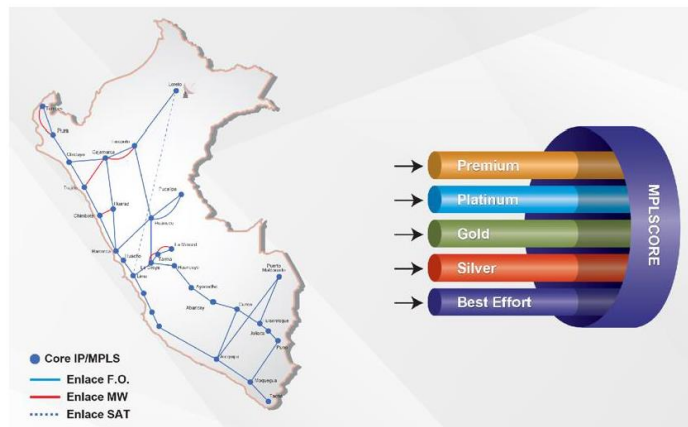


Figura 23. Calidad de Servicio WAN
Fuente: (Proveedor America Movil)

La calidad de servicio se mantendrá dinámico con la siguiente característica:

- ✓ El COS1 podrá utilizar todo el ancho de banda disponible en caso no sea utilizado por el COS2 y COS3.
- ✓ El COS2 podrá utilizar el ancho de banda del COS1 y COS3 siempre y cuando se tenga ancho de banda disponible y será remarcado con COS1.
- ✓ El COS3 sólo utilizará el ancho de banda propuesto en cada sede, el excedente será descartado.

Basado en la necesidad del negocio de priorizar ciertos tipos de tráfico se identificaron los siguientes tipos de tráfico

1. Tráfico de Datos Críticos
2. Tráfico de Datos No Críticos (Internet)
3. Tráfico de Voz y Video

Para el manejo del tráfico de voz, datos y video se aplicará la marcación de paquetes a **dscp** bajo este esquema se definen la siguiente secuencia para realizar la aplicación de la calidad de servicio.

```
ip access-list extended AUTOQOS_VOIP_DATA_CLASS
permit 10.30.3.0 0.255.255.255
permit 10.40.3.0 0.255.255.255
permit 10.150.3.0 0.255.255.255
deny ip any any
```

Primero se realiza un filtrado de segmentos de red a los cuales se desea aplicar el marcado de paquetes.

```
class-map match-all AUTOQOS_VOIP_DATA_CLASS
match access-group name
AUTOQOS_VOIP_DATA_CLASS
match ip dscp ef
```

Segundo se realiza un proceso de cotejo de paquetes para identificar el tipo de tráfico proveniente de la Lista de Acceso anteriormente definido y se aplica el valor de dscp a los paquetes permitidos.

Tercero, ya teniendo identificado el tráfico a priorizar se aplica un ancho de banda definido para dicho tráfico.

interface GigabitEthernet1/0/6	<i>Numero de Interface</i>
switchport access vlan 20	<i>Vlan de datos</i>
switchport mode access	<i>Tipo de Puerto</i>
switchport voice vlan 100	<i>Vlan de voz</i>
switchport port-security maximum 2	<i>Cantidad de host permitidos 2</i>
switchport port-security violation restrict	<i>Politica de bloqueo</i>
srr-queue bandwidth share 1 30 35 5 AUTOQOS-QOS-VOIP-POLICY	<i>Aplicación de Politica QoS</i>

Tabla 34. Configuración Interface Lan
Fuente: (Elaboración propia)

Finalmente, esta última política se aplica en la interface que va conectada a los endpoint.

Diseño de Seguridad

Este punto muy importante que es la seguridad de la información se aborda en este punto desde el punto de vista perimetral puesto que el equipo de seguridad propuesta brinda las funcionalidades necesarias para evitar ataques y prevenir cualquier robo o secuestro de información.

El diseño de seguridad se abordará desde 3 frentes.

- SEGURIDAD PERIMETRAL
- SEGURIDAD DMZ
- SEGURIDAD LAN NETWORKING

Seguridad Perimetral

Perfiles de Navegación WEB

En este punto se identificaron tipos de usuarios finales por cada UNE y cada sede respectivamente además de esto los servicios Web que usan recurrentemente fueron mapeados para posteriormente Permitir o Denegar su acceso.

Debido a que todo el personal administrativo se encuentra dispersado en cada SEDE de las UNES, es aquí donde se aplicaran perfiles de navegación distintos en base a las necesidades del negocio y de los mismos trabajadores.

Tipos de Usuarios Administrativos:

- **Gerentes**
- **Jefe de Sede**
- **Personal de Ventas**
- **Personal de Cobranza**
- **Personal de Seguridad**
- **Invitados y Proveedores**

En base a esta identificación se definen los siguientes grupos con sus respectivos filtros web y control de aplicaciones.

1. **Grupo Gerentes:** Acceso Total y llamadas por Internet.
2. **Nivel3:** Nivel2 + Acceso a Streaming Video (Netflix, Spotify)
3. **Nivel2:** Nivel1 + Acceso a Descargas y Share Bandwidth
4. **Nivel1:** Nivel0 + Acceso a Redes Sociales
5. **Nivel0:** Grupo con accesos a paginas intranet, Gobierno, Correo.

Perfiles de Seguridad FSSO

		Gerentes	Nivel 0	Nivel 1	Nivel 2	Nivel 3
	MARCAR CON X PARA BLOQUEAR					
Filtro de Aplicaciones	Skype			X	X	X
	P2P			X		
	Juegos	X	X	X	X	X
	Actualizaciones					
	Redes Sociales (Social Media)			X		
	Video/Audio			X	X	
	MARCAR CON X PARA BLOQUEAR					
Filtro Web						
	Abuso infantil	X				
	Discriminación	X				
	Abuso de drogas	X	X	X	X	X
	Violencia explícita	X	X	X	X	X
	Grupos extremistas	X	X	X	X	X
	Hacking	X	X	X	X	X
	ilegal o poco ética	X	X	X	X	X
	Plagio	X	X	X	X	X
	Anulación de Proxy	X	X	X	X	X
	Contenido para adultos	X	X	X	X	X
	Pornografía	X	X	X	X	X
	Educación sexual	X	X	X	X	X

Caza deportiva y juegos de guerra	X	X	X	X	X
Tabacco	X	X	X	X	X
Armas (ventas)	X	X	X	X	X
Consumo de ancho de banda	X	X	X	X	X
Intercambio de archivos y almacenamiento	X	X	X	X	X
Freeware y descargas de software					
Radio y TV por internet	X		X	X	
Telefonía por internet	X		X	X	X
Intercambio de archivos punto a punto	X		X	X	X
Streaming de medios y descarga	X		X	X	X
Riesgo de seguridad	X		X	X	X
Páginas web maliciosas	X		X	X	X
Suplantación de identidad					
URL de spam	X	x	X	x	x
Juegos	X		X	X	
Religión global	X		X	X	
Salud y Bienestar	X		X	X	
Mensajería instantánea	X				

Redes sociales	X		X	X	
Excepciones	Gmail	Gmail	Gmail	Gmail	Gmail
	bancos	bancos	bancos	bancos	bancos
	Ministerios	Ministerios	Ministerios	Ministerios	Ministerios
	infocorp	infocorp	infocorp	infocorp	infocorp
	indecopi	indecopi	indecopi	indecopi	indecopi
	sunat	sunat	sunat	sunat	sunat
	admincrm.cer tus.edu.pe	admincrm.c ertus.edu.pe	admincrm.c ertus.edu.pe	admincrm.c ertus.edu.pe	admincrm.cer tus.edu.pe
	adminpagovir tual.certus.ed u.pe	adminpagov irtual.certus. edu.pe	adminpagov irtual.certus. edu.pe	adminpagov irtual.certus. edu.pe	adminpagovir tual.certus.ed u.pe
	adminpagovir tualdev.certus .edu.pe	adminpagov irtualdev.ce rtus.edu.pe	adminpagov irtualdev.ce rtus.edu.pe	adminpagov irtualdev.ce rtus.edu.pe	adminpagovir tualdev.certus .edu.pe

Tabla 35. Perfiles de Navegacion WEB

Fuente: (Elaboracion propia)

Filtros WEB y Control de Aplicaciones

El servicio de Contenido Web Filtro busca optimizar recursos de red del negocio, así como enfocar los recursos humanos a tareas principalmente del negocio.

El equipo de seguridad aplicara el filtro web que corresponda según el grupo de AD que detecte durante la sesión de los usuarios y la conexión a la RED en cualquier sede remota de cada UNE.

Sincronización FSSO:

Una vez completado el formato de navegación web, se realiza la integración de Agente FSSO de Fortinet con el Active Directory para recolectar los intentos de conexión y aplicar la política según el grupo que se encuentre el usuario autenticado.

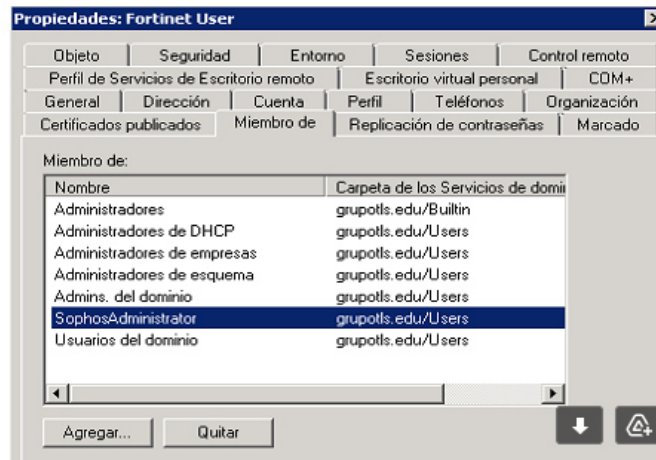


Figura 24. Grupos de Active Directory
Fuente: (Elaboracion Propia)

Después de crear los grupos de AD y agregar los usuarios a cada grupo según corresponda, se procede a seleccionar los controladores de dominio de los cuales se recogerá los intentos de conexión.

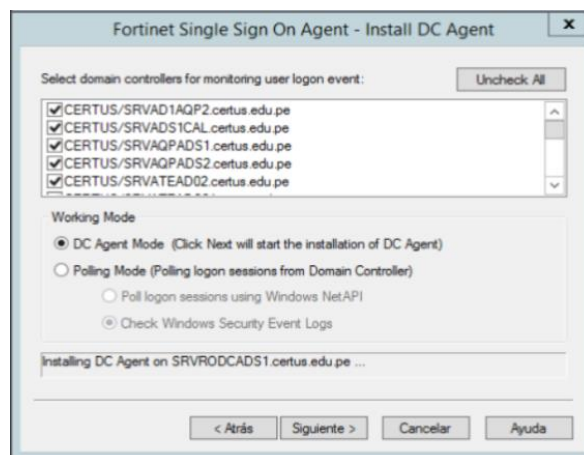


Figura 25. Servidores AD Certus
Fuente: (Elaboracion Propia)

En este punto se muestran los controladores de Dominio disponible con los cuales se establecerá conexión y se recogerán las autenticaciones.

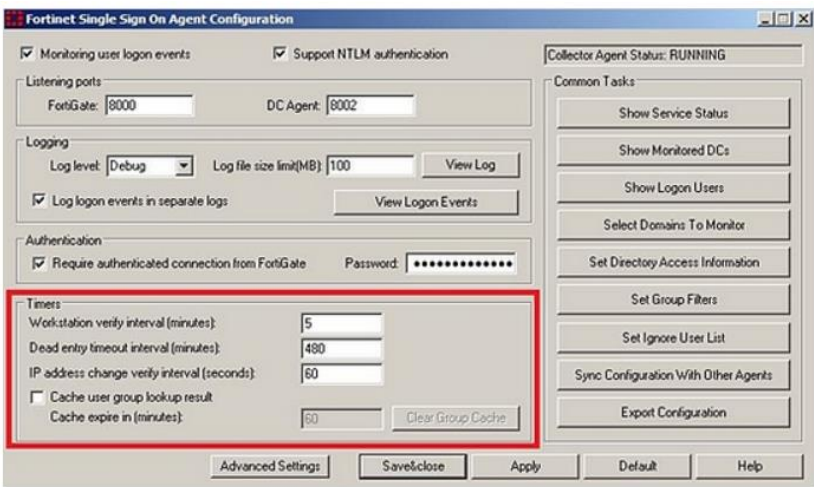


Figura 26. Colector FSSO
Fuente: (Elaboracion Propia)

Finalmente se instala el agente colector FSSO Fortinet para recolectar las sesiones y también es usado para realizar troubleshooting.

Conexión Remota VPN SLL

Para temas de conexión remota se consideró realizar la conexión hacia el AD mediante LDAP para que de esta forma los usuarios que deseen conectarse de manera remota a los servicios internos de la empresa, lo puedan hacer de manera simple usando su cuenta de dominio o correo.

Sincronización LDAP para conexión VPN SSL

Name	Server IP/Name	Port	Common Name Identifier	Distinguished Name
LDAP_192.168.7.3	192.168.7.3	389	samAccountName	DC=grupotls,DC=edu
LDAP_TOULOUSE_SURCO	192.168.6.3	389	samAccountName	DC=grupotls,DC=edu
SERVER_LDAP_IEDUCA	192.168.7.253	389	samAccountName	DC=ieduca,DC=edu,DC=pe

Figura 27. Servidores LDAP - Fortigate
Fuente: (Elaboracion Propia)

Name	SERVER_LDAP_IEDUCA
Server IP/Name	192.168.7.253
Server Port	389
Common Name Identifier	samAccountName
Distinguished Name	DC=ieduca,DC=edu,DC=f Fetch DN
Bind Type	Simple Anonymous Regular
User DN	CN=LDAP Forticlient,CN=
Password	••••••••
Secure Connection	☒
Test	

Figura 28. Servidores LDAP – ieduca 192.168.7.253
Fuente: (Elaboracion Propia)

Adicionalmente de la Sincronización se realizó la restricción a las conexiones VPN SSL limitando el acceso a IPS Publicas solo desde Perú y Venezuela.

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s)

INTERNET_CD71993_50M (Inter ✕)

Listen on Port

10443

Web mode access will be listening at <https://200.4.231.194:10443>

Restrict Access

Allow access from any host Limit access to specific hosts

IP_200.8.179.130 ✕

IP_200.8.190.244 ✕

Peru ✕

Venezuela ✕

Figura 29. VPN SSL – Restricciones por Pais.
Fuente: (Elaboracion Propia)

Para prevenir Ataques de Fuerza Bruta se consideró aplicar políticas de sensores IPS y proteger ambientes de producción y desarrollo que cuentan con servidores WINDOWS.

Edit IPS Sensor

RDP.connection.Brute.Force

Name

RDP.connection.Brute.Force

[\[View IPS Signatures\]](#)

Comments

0/255

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
MS.RDP.Connection.Brute.Force	0	High	Server	TCP	Windows	Block	

Figura 30. Sensor IPS
Fuente: (Elaboracion Propia)

Sanboxing Cloud

Se aprovechará este servicio brindado por el proveedor ISP en la cual se brinda análisis de tráfico y envió hacia un sistema Sanboxing cloud en la cual se evitará tener archivos infectados que afecten la red, prevenir ataques de día Zero.

Seguridad a Nivel LAN

A nivel LAN las consideraciones de seguridad que se aplicaron fueron restringir los puertos de acceso a máximo 2 dispositivos (Teléfono y PC/LAPTOP), si por alguna razón se excede el número de dispositivos conectados este puerto se bloquea.

Con esto evitamos que se usen los puertos disponibles como un punto troncal donde se pueda conectar un repetidor y conectar más de 1 dispositivo.

PortSecurity

interface GigabitEthernet1/0/6	<i>Numero de Interface</i>
switchport access vlan 20	<i>Vlan de datos</i>
switchport mode access	<i>Tipo de Puerto</i>
switchport voice vlan 100	<i>Vlan de voz</i>
switchport port-security maximum 2	<i>Cantidad de host permitidos 2</i>

switchport port-security violation restrict srr-queue bandwidth share 1 30 35 5 AUTOQOS-QOS-VOIP-POLICY	<i>Política de bloqueo</i> <i>Al exceder la cantidad de dispositivos permitidos.</i>
--	---

Tabla 36. Configuración Interface LAN – Port Security

Fuente: (Elaboración propia)

La funcionalidad de PortSecurity es usada para lograr cerrar un hueco de seguridad interna.

Seguridad DMZ

Debido al incremento de Ciberataques se consideró reforzar la zona DMZ considerando 2 Equipos en Alta disponibilidad y adicionando una licencia de Seguridad WAF.

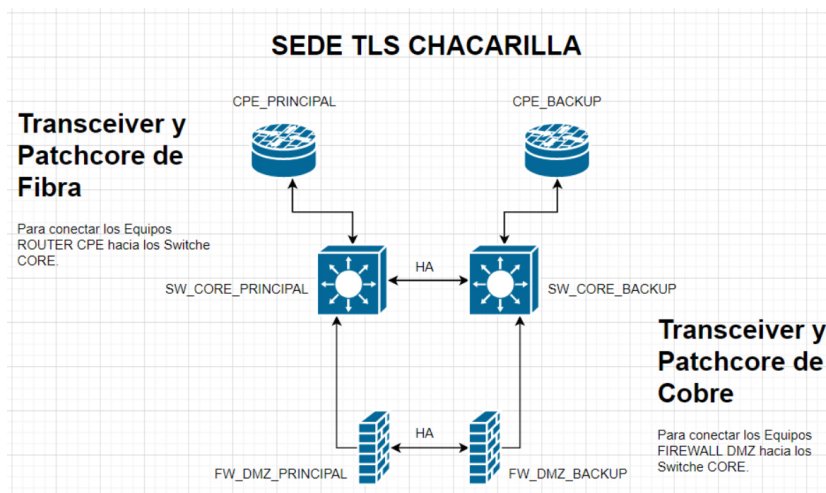


Figura 31. Topología DMZ
Fuente: (Elaboración Propia)

Debido a los servicios críticos que se tiene hosteados en la sede de Chacarilla se realizó la instalación de 2 equipos FG-501E en un esquema de alta disponibilidad Activo – Pasivo.

Al tener 2 equipos lo suficientemente robustos como para soportar la carga de conexiones y trafico saliente y entrante se realizó el movimiento de servidores que se encontraron en la red LAN hacia la red DMZ y así brindarle una capa de seguridad adicional.

Con la funcionalidad y licencia de WAF se incorpora un filtro de seguridad adicional para servicios publicados.

IPv4 Virtual IP (79)	
SRV-UCAL-WS	200.4.231.198 --> 192.168.5.246
SRV-UCAL-APP	200.4.231.200 --> 192.168.6.189
SRV-TLS-WS	200.4.231.197 --> 192.168.6.171
PC-ADMIN_80	200.4.231.195 --> 172.16.1.13 (T
SRL-TLS-VIP	200.4.231.202 --> 172.16.1.10
UCALSURAPL2	200.4.231.203 --> 172.16.1.12
SRV_STUN	200.4.231.205 --> 172.16.1.22
VIP_200.4.231.204	200.4.231.204 --> 172.16.1.6
SRV_genesyswebface	200.4.231.201 --> 172.16.1.21
SRV_genesyseservices	200.4.231.196 --> 172.16.1.20 (T
PC-ADMIN_443	200.4.231.195 --> 172.16.1.13 (T
TLSSURHD1.grupotls.edu_81	200.4.231.195 --> 172.16.1.17 (T
TLSSURHD1.grupotls.edu_8080	200.4.231.195 --> 172.16.1.17 (T
VIP_200.4.231.195_21	200.4.231.195 --> 172.16.1.13 (T
VIP_200.4.231.195_22	200.4.231.195 --> 172.16.1.13 (T
VIP_FAZ_HTTPS	200.4.231.195 --> 192.168.99.99
VIP_FAZ_SYSLOG_TCP	200.4.231.195 --> 192.168.99.99
VIP_FAZ_SYSLOG_UDP	200.4.231.195 --> 192.168.99.99
SRV_genesyseservices_2	200.4.231.196 --> 172.16.1.20 (T
SRV_genesyseservices_3	200.4.231.196 --> 172.16.1.20 (T

Figura 32. Listado de IPS nateadas
Fuente: (Preparacion Propia)

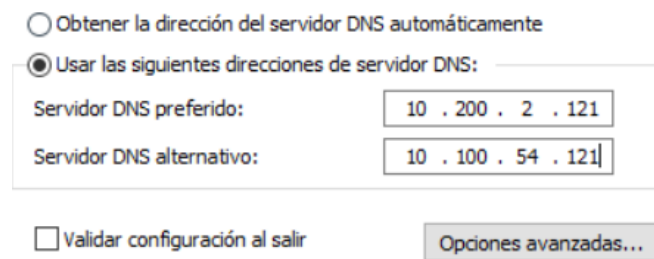
La imagen 32 se lista la cantidad de servicios publicados que brinda TLS. Se evidencia también que algunos servidores se encuentran configurados en la red LAN el cual siempre se encuentra expuesto a cualquier ataque interno o externo, este problema fue solucionado con el movimiento de servicios hacia la interface DMZ la cual tiene mayores filtros de seguridad y no se encuentra expuesta a ataques de manera interna.

Paso 2: Diseño desde la parte superior del modelo de referencia OSI

Alta Disponibilidad a Nivel del Resolución DNS

Para no perder la conexión hacia servicios internos e internet se planteó instalar un servidor DNS Local y un DNS Remoto ubicado en el Data Center del Proveedor.

Se configuro un servidor principal y secundario en cada tarjeta de red de los dispositivos finales.



The image shows a screenshot of the Windows Network Settings application. At the top, there are two radio buttons: 'Obtener la dirección del servidor DNS automáticamente' (which is unselected) and 'Usar las siguientes direcciones de servidor DNS:' (which is selected). Below the selected option, there are two text input fields. The first is labeled 'Servidor DNS preferido:' and contains the IP address '10 . 200 . 2 . 121'. The second is labeled 'Servidor DNS alternativo:' and contains the IP address '10 . 100 . 54 . 121'. At the bottom left, there is a checkbox labeled 'Validar configuración al salir' which is unchecked. At the bottom right, there is a button labeled 'Opciones avanzadas...'. The entire configuration area is enclosed in a light gray border.

Figura 33. Configuración DNS Primario y Secundario
Fuente: (Elaboración Propia)

Alta Disponibilidad a Nivel del servicio DHCP

El servicio DHCP se consideró implementarlo bajo un esquema de alta disponibilidad para no perder la asignación de direcciones IPs públicas ante la caída del servidor WINDOWS quien es el servidor principal, el servidor secundario se encuentra ubicado en los equipos router.

Paso 3: Reunir datos adicionales en la red.

Adicionalmente para hacer un uso correcto del ancho de banda se definieron configurar los siguientes **Traffic Shaper** para poder asignar estos a cada servicio o subredes LAN.

Esta funcionalidad permite establecer porcentajes de ancho de banda reservados.

Name	Type	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization
Call-Center_250MB	Shared	204800 Kbps	256000 Kbps	0 B/s
TS-1MB	Shared	1000 Kbps	1024 Kbps	0 B/s
TS-2MB	Shared	2000 Kbps	2048 Kbps	10.31 kB/s
TS-3MB	Shared	3072 Kbps	3072 Kbps	0 B/s
TS-5MB	Shared	5000 Kbps	5120 Kbps	0 B/s
TS-6MB	Shared	6000 Kbps	6144 Kbps	0 B/s
TS-8MB	Shared	8000 Kbps	8192 Kbps	0 B/s
TS-10MB	Shared	10000 Kbps	10240 Kbps	0 B/s
TS-15MB	Shared	14500 Kbps	15000 Kbps	0 B/s
TS-20MB	Shared	20000 Kbps	20480 Kbps	0 B/s
TS-25MB	Shared	25000 Kbps	25600 Kbps	0 B/s
TS-30MB	Shared	30000 Kbps	30720 Kbps	0 B/s
TS-60MB	Shared	60000 Kbps	61440 Kbps	0 B/s
TS-80MB	Shared	80000 Kbps	81920 Kbps	0 B/s
TS_30M	Shared	30720 Kbps	30720 Kbps	0 B/s
TS_40M	Shared	40924 Kbps	40924 Kbps	0 B/s
TS_100_MB	Shared	102400 Kbps	102400 Kbps	0 B/s
TS_100MB	Shared	102400 Kbps	102400 Kbps	2.54 MB/s

Figura 34. Configuración Traffic Shaper - Fortigate
Fuente: (Elaboración Propia)

También se consideró aplicar horarios a las políticas del firewall para que se puedan descargar actualizaciones de Windows o de antivirus durante un horario no productivo que afecte el ancho de banda.

Recurring (19)	
Horaiosemanal2	Monday Tuesday Wednesday Thursday Friday Saturday
Horario_Semanal	Monday Tuesday Wednesday Thursday Friday
Horario_sabados	Saturday
Hors_Policy_ID253	Wednesday Friday
Lunes_a_Viernes	Monday Tuesday Wednesday Thursday Friday
Martes15Noviembre	Tuesday
Nivel_B_Lunes	Monday
Nivel_B_Viernes	Friday
PROVI_192.168.7.[11-20]	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
PROV_192.168.10.[2-9]	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
RANGOS_DOT10_LV	Monday Tuesday Wednesday Thursday Friday
RANGOS_DOT10_S	Saturday
alumnos_nivelA	Tuesday
always	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
horario_17:00_22:30	Sunday Monday Tuesday Wednesday Thursday Friday
lunes-vi	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
lunes-viernes	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
temporal	Tuesday Wednesday Thursday Friday Saturday
web NIVELB	Wednesday

Figura 35. Configuración Policy Horarios
Fuente: (Elaboración Propia)

3.2.5.5 Fase de Implementación

En esta etapa se sigue con la instalación de equipos físicos, así como su configuración en esta etapa se debe proponer a detalle el plan de contingencia y un plan de rollback en caso de falla total. El objetivo principal que debe ser cumplido es implementar los nuevos equipos sin comprometer la disponibilidad de la red y no interrumpir el servicio en horario laboral, de ser necesario se definen ventanas de trabajo previa autorización de lo PO del negocio.

De preferencia se recomienda migrar un segmento de red no crítico y validar su funcionamiento después del pase a producción, e ir migrando todos los servicios paulatinamente.

A continuación, se detallan las actividades a nivel técnico que se ejecutaran durante el proceso de cambio de operador, también se detalla el plan de rollback en el caso se presente algún inconveniente y se pueda dar solución dentro de un ambiente controlado.

Finalmente, se estable el Checklist para validar que todas las actividades fueron concretadas de manera exitosa.

Plan de Trabajo pase a Producción

Plan de Trabajo	Implementación de servicios Datos e Internet
Proyecto	Migración operador Internet y Datos
Breve Descripción	Implementación de servicios Datos e Internet
Responsable del Plan de Trabajo	Miguel Toribio
Alcance	Asociados al Negocio

Tareas Previas							
Actividades	Disponibilida d de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
	No	12/21/2018	12/22/2018	15 minutos	11:00 p. m.	11:15 p. m.	ON
	No	12/21/2018	12/22/2018	15 minutos	11:15 p. m.	11:30 p. m.	ON
	si	12/21/2018	12/22/2018	10 minutos	11:20 p. m.	11:30 p. m.	CLIENTE
Migración Sede Chacarilla							
Actividad	Disponibilida d de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
Apagar interface vlan 931,936,835,731	No	12/21/2018	12/22/2018	30 minutos	11:00 p. m.	11:30 p. m.	ON
Activar Interfaces Vlan 331,332 fortinet ON	Si	12/21/2018	12/22/2018	30 minutos	11:30 p. m.	12:00 a. m.	ON
Cambio de DNS públicos (PUNTO.PE y GCP)	Si	12/21/2018	12/22/2018	10 minutos	12:00 a. m.	12:10 a. m.	ON
Eliminar enrutamiento de las vlan	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Limpiar la tabla ARP para refrescar las MAC	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE

Pruebas de navegación de la vlan	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Pruebas de comunicación de entre las vlan	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Validar configuración de NAT en Fortinet ON	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Punto de Rollback							
Pruebas de VPN SSL							
Actividad	Disponibilidad de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
Validar acceso a la red mediante la VPN SSL	No	12/21/2018	12/22/2018	30 minutos	11:00 p. m.	11:30 p. m.	ON
Validar conexiones a los servidores mediante la VPN SSL	Si	12/21/2018	12/22/2018	30 minutos	11:30 p. m.	12:00 a. m.	ON
Validar navegación mediante el agente FSSO desde la red local	Si	12/21/2018	12/22/2018	10 minutos	12:00 a. m.	12:10 a. m.	ON
Validación de Internet de las sedes que NO estén por ON	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Pruebas de navegación desde las remotas (no migradas) hacia internet por century	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Validar con ISEG Conexión hacia ATE,SAN MIGUEL, SJL, NORTE	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
PRUEBAS INFRAESTRUCTURA							
Actividad	Disponibilidad de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
Batería de pruebas de conectividad DC SURCO 10.100.54.x vs CENTURY 10.200.1/2/	No	12/21/2018	12/22/2018	30 minutos	11:00 p. m.	11:30 p. m.	ON
Revision de conectividad entre servidores(BANNER)	Si	12/21/2018	12/22/2018	30 minutos	11:30 p. m.	12:00 a. m.	ON

Validacion de servicios publicados(BRIM-MOBILE)	Si	12/21/2018	12/22/2018	10 minutos	12:00 a. m.	12:10 a. m.	ON
Batería de pruebas de conectividad CENTURY vs DC SURCO	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Batería de pruebas de conectividad a publicaciones	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Pruebas de salida hacia internet con IP publica desde dc century PRD	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Pruebas de conexión a internet desde redes century	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE
Solicitud de conexiones balanceadas a LUMEN (F5)	Si	12/21/2018	12/22/2018	30 minutos	12:00 a. m.	12:40 a. m.	ON CLIENTE

Pruebas de servicio de Redundancia - Internet Krumdieck

Actividad	Disponibilidad de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
Configuración de HSRP INTERNET BACKUP	No	12/21/2018	12/22/2018	30 minuto	11:00 p. m.	11:30 p. m.	ON
Desactivar rutas estaticas y activar BGP hacia blade	No	12/21/2018	12/22/2018	30 minuto	11:30 p. m.	12:00 a. m.	ON
Conmutación de enlace principal a backup y validación de correcta conmutación.	Si	12/21/2018	12/22/2018	10 minuto	12:00 a. m.	12:10 a. m.	ON
Hacer la conmutación del enlace backup de Santiago de surco L2L	Si	12/21/2018	12/22/2018	10 minuto	12:10 a. m.	12:20 a. m.	ON
Hacer la conmutación del enlace backup de Krumdieck L2L	Si	12/21/2018	12/22/2018	10 minuto	12:20 a. m.	12:30 a. m.	ON
Pruebas de conectividad hacia a internet	Si	12/21/2018	12/22/2018	10 minuto	12:30 a. m.	1:00 a. m.	Miguel Toribio ON
Pruebas de servicios totales con personal del cliente	si	12/21/2018	12/22/2018	Por definir	1:00 a. m.	Por definir	Miguel Toribio

PRUEBAS FUNCIONALES							
Actividad	Disponibilidad de Servicio	fecha inicio	fecha fin	Duración	Hora Inicio	Hora Fin	Responsable
Validación de flujo academico (PORTAL CERTUS)	Si	12/21/2018	12/22/2018	Por definir	11:00 p. m.	11:30 p. m.	Miguel Toribio
Validación de flujo academico (BANNER)	Si	12/21/2018	12/22/2018	10 minuto	11:30 p. m.	12:00 a. m.	KVASQUEZ
Validación de flujo academico (SATELITES)	Si	12/21/2018	12/22/2018	Por definir	12:00 a. m.	12:10 a. m.	IEDUCA - KVASQUEZ
Acceso exactus PRD	Si	12/21/2018	12/22/2018	10 minuto	12:10 a. m.	12:20 a. m.	IEDUCA - KVASQUEZ
Validación de flujo comercial	Si	12/21/2018	12/22/2018	Por definir	12:20 a. m.	12:30 a. m.	IEDUCA - LGUIMAREY
Validación de flujo tesoreria	Si	12/21/2018	12/22/2018	10 minuto	12:30 a. m.	1:00 a. m.	IEDUCA - PLIZARRAG A
Validación de flujo tesoreria	Si	12/21/2018	12/22/2018	Por definir	11:00 p. m.	11:30 p. m.	LLEIVA
Validación de flujo academico (BANNER)	Si	12/21/2018	12/22/2018	10 minuto	11:30 p. m.	12:00 a. m.	CBONIFACIO
Validación de flujo academico (BANNER)	Si	12/21/2018	12/22/2018	Por definir	12:00 a. m.	12:10 a. m.	PDIAZ
Validación de flujo contabilidad	Si	12/21/2018	12/22/2018	10 minuto	12:10 a. m.	12:20 a. m.	IEDUCA- KOLORTEGU I
Validación de moodle PRD (campus digital)	Si	12/21/2018	12/22/2018	Por definir	12:20 a. m.	12:30 a. m.	IEDUCA- JKACHUMANTA
Validación de RDP colaboradores PRD	Si	12/21/2018	12/22/2018	10 minuto	12:30 a. m.	1:00 a. m.	JSANCHEZR- ERODRIGUE ZC
validación de acceso a SAP desde RDP	Si	12/21/2018	12/22/2018	Por definir	11:00 p. m.	11:30 p. m.	IEDUCA - LLEIVA
validación de acceso a Pegaso desde VPN	Si	12/21/2018	12/22/2018	10 minuto	11:30 p. m.	12:00 a. m.	IEDUCA - LLEIVA

Validación de MULESOFT (PRD)	Si	12/21/2018	12/22/2018	Por definir	12:00 a. m.	12:10 a. m.	IEDUCA - LLEIVA
Validación de conexión BI (PRD)	Si	12/21/2018	12/22/2018	10 minuto	12:10 a. m.	12:20 a. m.	IEDUCA - EMEJIA
validación interconexión bancaria BCP	Si	12/21/2018	12/22/2018	Por definir	12:20 a. m.	12:30 a. m.	IEDUCA - LGALLARDO
Validación de flujo academico (BANNER)	Si	12/21/2018	12/22/2018	10 minuto	12:30 a. m.	1:00 a. m.	LLEIVA - MCAJUSOL
Validación de flujo contabilidad	Si	12/21/2018	12/22/2018	Por definir	11:00 p. m.	11:30 p. m.	LLEIVA - MCAJUSOL
validación interconexión bancaria BBVA	Si	12/21/2018	12/22/2018	10 minuto	11:30 p. m.	12:00 a. m.	LLEIVA - MCAJUSOL
validación interconexión bancaria SCOTIABANK	Si	12/21/2018	12/22/2018	10 minuto	12:00 a. m.	12:10 a. m.	DDEZA - DGUARDIA
validación de web CERTUS	Si	12/21/2018	12/22/2018	10 minuto	12:10 a. m.	12:20 a. m.	IEDUCA - MMOSCOSO
validacion CCVOX	Si	12/21/2018	12/22/2018	10 minuto	12:20 a. m.	12:30 a. m.	CGARCES
Validación de acceso SINTAD	Si	12/21/2018	12/22/2018	10 minuto	12:30 a. m.	1:00 a. m.	IEDUCA - KVASQUEZ

Plan de Rollback

Plan de trabajo	Plan de Rollback
Proyecto	
Breve Descripción	Plan de Rollback
Responsable del Plan de Trabajo	Miguel Toribio
Alcance	
Fecha y hora de Inicio	23:00 hrs – 06:00 am

Plan de Actividades								
Item	Actividad	Cliente	Disponibilidad de Servicio	Fecha		Duración	Estado	Responsable
MIGRACION IS - SEDE CENTURY								
01	Apagar las interfaces vlan 931,936,835,731,936	DESARROLLO EDUCATIVO SAC	No	12/21/2018	0:40	2min.	0%	ON - MTORIBIO
02	Prender las interface vlan 931,936,835,731,936	DESARROLLO EDUCATIVO SAC	No	12/21/2018	0:42	3min.	0%	ON - MTORIBIO
	Agregar enrutamiento del POOL de IP de VPN SSL	DESARROLLO EDUCATIVO SAC		12/21/2018	0:45	5min.		ON - MTORIBIO
03	Cambio de DNS públicos (PUNTO.PE)	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	0:40	5 min.	0%	IEDUCA - MIGUEL TORIBIO
04	Validaciones de publicaciones por su proveedor actual	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	1:00	30 min.	0%	IEDUCA - MIGUEL TORIBIO

CAMBIO DE VPN SSL (IP PUBLICA ACTUAL)								
09	Validar VPN SSL por Century	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	0:40	5 min.	100%	IEDUCA - MIGUEL TORIBIO
10	Conectarse por VPN, validar comunicación con todas su VLANs por MPLS de Lv3	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	0:45	min.	100%	IEDUCA - MIGUEL TORIBIO
CAMBIO DE VPN SITE TO SITE (POR DEFINIR)								
11	Cambio de IP PUBLICA	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	0:50	5min.	0%	ON - VICENTE PISCO SOC - MARCO REYES
12	Cambio de contraseña	DESARROLLO EDUCATIVO SAC		12/21/2018	0:55	5min.		ON - VICENTE PISCO SOC - MARCO REYES
13	Pruebas de comunicación por VPN Site to Site	DESARROLLO EDUCATIVO SAC	SI	12/21/2018	1:00	20 min.	0%	ON - VICENTE PISCO SOC - MARCO REYES

PLAN DE EVALUACION

Diagnóstico de red a nivel LAN: Evaluamos cada capa del modelo Jerárquico bajo los siguientes puntos:

1. Evaluación Física
2. Evaluación Lógica
3. Evaluación de Seguridad

CAPA CORE

- Evaluación Física

Primero identificamos la categoría del cableado y validamos si cumple con los siguientes ítems del estándar establecidos por TIA:

- ✓ Distancia límite de conexión punto a punto
- ✓ Resistencia
- ✓ Atenuación
- ✓ Capacitancia

	Detalle de Cableado Vertical				
	Coaxial	Fibra	STP	UTP cat3	UTP cat5 o cat6
Vertical 1		X			
Vertical 2		X			
	Detalle de Cableado Horizontal				
	Coaxial	Fibra	STP	UTP cat3	UTP cat5 o cat6
Bloque 1					X
Bloque 2					X
Bloque 3					X
Bloque 4					X
Bloque 5					X
Bloque 6					X
Bloque 7					X
Bloque 8					X
Bloque 9					X
Bloque 10				X	

Tabla 37. Cableado Estructurado – Sede TLS Javier Prado
Fuente: (Elaboracion propia)

Segundo validamos funcionamiento, configuración y errores presentes en las Interfaces físicas.

```
N9K-CORE1-PRIMAVERA# sh int brief
```

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.0.201	1000	1500

Ethernet Interface	VLAN	Type	Mode	Status	Reason	speed	Port Ch #
Eth1/1	--	eth	routed	up	none	1000(D)	--
Eth1/2	131	eth	access	up	none	1000(D)	--
Eth1/3	131	eth	access	up	none	1000(D)	--
Eth1/4	141	eth	access	up	none	1000(D)	--
Eth1/5	141	eth	access	down	Link not connected	auto(D)	--
Eth1/6	131	eth	access	up	none	1000(D)	--
Eth1/7	1	eth	trunk	up	none	10G(D)	1
Eth1/8	1	eth	trunk	up	none	10G(D)	2
Eth1/9	1	eth	trunk	up	none	1000(D)	3
Eth1/10	1	eth	trunk	up	none	10G(D)	4
Eth1/11	1	eth	trunk	up	none	10G(D)	5
Eth1/12	1	eth	trunk	down	Link not connected	auto(D)	6
Eth1/13	1	eth	trunk	up	none	10G(D)	--
Eth1/14	1	eth	access	down	XCVR not inserted	auto(D)	--
Eth1/15	40	eth	access	down	XCVR not inserted	auto(D)	--
Eth1/16	1	eth	access	down	XCVR not inserted	auto(D)	--
Eth1/17	110	eth	access	down	XCVR not inserted	auto(D)	--
Eth1/18	1	eth	access	down	XCVR not inserted	auto(D)	--
Eth1/19	190	eth	trunk	up	none	1000(D)	7
Eth1/20	190	eth	trunk	up	none	1000(D)	7
Eth1/21	190	eth	trunk	up	none	1000(D)	7
Eth1/22	190	eth	trunk	up	none	1000(D)	7
Eth1/23	1	eth	trunk	up	none	10G(D)	--
Eth1/24	1	eth	trunk	down	LinkFlapErrDisabled	auto(D)	--

Figura 36. Configuración Policy Horarios
Fuente: (Elaboración Propia)

- Se puede evidenciar que todas las interfaces se encuentran configuradas a velocidades de más de 1 Gbps.
- Se verifican errores en la Interface Eth1/24 “**LinkFlapErrDisabled**”
- Se verifica que se tienen puertos físicos que no se encuentran apagados lógicamente.
- Se verifica puertos configurados en Modo Acceso en la CAPA CORE donde no se puede tener este tipo de puertos.

Tercero Verificamos la cantidad de tráfico que está pasando por la interface conectada hacia la WAN.

```

N9K-CORE1-PRIMAVERA# sh int Eth1/2 | i rate
30 seconds input rate 10696 bits/sec, 9 packets/sec
30 seconds output rate 206296 bits/sec, 141 packets/sec
input rate 16.46 kbps, 26 pps; output rate 409.30 kbps, 133 pps
N9K-CORE1-PRIMAVERA#

```

Figura 37. Trafico Interface Eth1/1
Fuente: (Elaboracion Propia)

- Se verifica que se tiene un tráfico de 16.46 Kbps de descarga y 409.30 kbps de subida.

```

RX
1894400430 unicast packets 17239119 multicast packets 84 broadcast packets
1911639633 input packets 177479903975 bytes
0 jumbo packets 0 storm suppression packets
0 runs 0 giants 0 CRC 0 no buffer
0 input error 0 short frame 0 overrun 0 underrun 0 ignored
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
0 input with dribble 0 input discard
0 Rx pause
TX
14675037454 unicast packets 58991574 multicast packets 171 broadcast packets
14734029199 output packets 4903117552844 bytes
0 jumbo packets
0 output error 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 124 output discard
0 Tx pause

```

Figura 38. Cantidad de Errores Fisicos – Inteface LAN
Fuente: (Elaboracion Propia)

- No se evidencia errores físicos en las conexiones y conectores (ERRORES CRC), ni mucho menos dropeo y descarte de paquetes.

Group	Port-channel	Type	Protocol	Member Ports
1	Po1(SU)	Eth	LACP	Eth1/7(P)
2	Po2(SU)	Eth	LACP	Eth1/8(P)
3	Po3(SU)	Eth	LACP	Eth1/9(P)
4	Po4(SU)	Eth	LACP	Eth1/10(P)
5	Po5(SU)	Eth	LACP	Eth1/11(P)
6	Po6(SD)	Eth	LACP	Eth1/12(D)
7	Po7(SU)	Eth	NONE	Eth1/19(P) Eth1/20(P) Eth1/21(P)
				Eth1/22(P)
8	Po8(SD)	Eth	LACP	Eth1/39(D) Eth1/40(D)
20	Po20(SU)	Eth	LACP	Eth1/49(P) Eth1/50(P)
30	Po30(RU)	Eth	NONE	Eth1/47(P) Eth1/48(P)

Figura 39. Estatus Etherchannel
Fuente: (Elaboracion Propia)

- Se valida el funcionamiento correcto a nivel de EtherChannel, cada conexión se encuentra disponible.

Port	OutMcastPkts	OutBcastPkts
mgmt0	738275	25
Eth1/1	738230	90309
Eth1/2	58992412	171
Eth1/3	57365572	170
Eth1/4	23624885	2134013
Eth1/5	0	0
Eth1/6	57362484	169
Eth1/7	1618841538	835585602
Eth1/8	1693728965	873646177
Eth1/9	1551929403	976880456
Eth1/10	1603788469	783444177
Eth1/11	1018397593	790680293
Eth1/12	0	0
Eth1/13	2347709932	1625441270
Eth1/14	0	0
Eth1/15	0	0
Eth1/16	0	0
Eth1/17	0	0

Figura 40. Cantidad de Paquetes trafico Multicas, Unicast
Fuente: (Elaboracion Propia)

- Se verifica que las Interfaces de mayor tráfico broadcast y multicast son: Eth1/7, Eth1/8, Eth1/9, Estas interfaces hacen conexión hacia la capa de Distribución.

Cuarto: Se verifica el estado del procesamiento CPU y Memoria

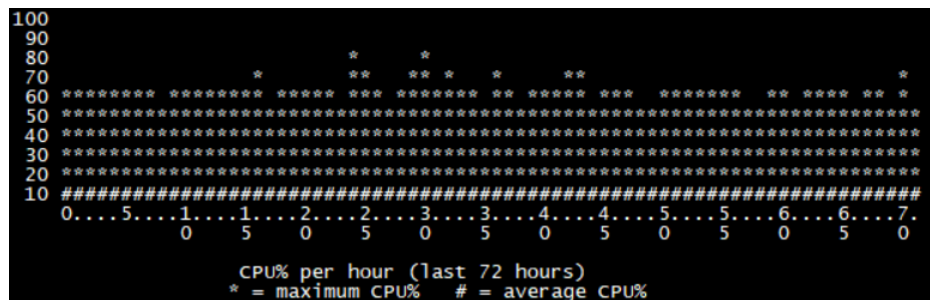


Figura 41. Historial de consumo CPU Sw core
Fuente: (Elaboracion Propia)

```
N9K-CORE1-PRIMAVERA# show system resources
Load average: 1 minute: 0.50 5 minutes: 0.43 15 minutes: 0.40
Processes : 534 total, 1 running
CPU states : 16.16% user, 2.27% kernel, 81.56% idle
CPU0 states : 13.13% user, 4.04% kernel, 82.82% idle
CPU1 states : 15.30% user, 3.06% kernel, 81.63% idle
CPU2 states : 33.33% user, 1.96% kernel, 64.70% idle
CPU3 states : 2.04% user, 1.02% kernel, 96.93% idle
Memory usage: 16401952k total, 5992064k used, 10409888k free
Current memory status: OK
N9K-CORE1-PRIMAVERA#
```

Figura 42. Espacio disponible memoria – sw core
Fuente: (Elaboracion Propia)

CAPA DISTRIBUCION

Evaluación Física

Primero: Al igual que en la capa superior CORE, se realiza la validación del cableado según el estándar TIA.

Segundo: Verificamos el estado de las Interfaces Físicas.

```
SW-DST-RACK4#sh int status
```

Port	Name	Status	vlan	Duplex	Speed	Type
Gi1/0/1		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/2		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/3		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/4		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/5		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/6		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/7		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/8		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/9		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/10		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/11		connected	60	a-full	a-100	10/100/1000BaseTX
Gi1/0/12		connected	60	a-full	a-100	10/100/1000BaseTX
Gi1/0/13		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/14		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/15		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/16		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/17		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/18		notconnect	60	auto	auto	10/100/1000BaseTX
Gi1/0/19		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/20		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/21		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/22		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/23	ENLACE_TRONCAL_ANT	connected	trunk	a-full	a-1000	10/100/1000BaseTX
Gi1/0/24	TRONCAL_ACC1_RACK4	connected	trunk	a-full	a-1000	10/100/1000BaseTX
Gi1/0/25		connected	40	a-full	a-100	10/100/1000BaseTX
Gi1/0/26		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/27		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/28		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/29		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/30		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/31		notconnect	40	auto	auto	10/100/1000BaseTX
Gi1/0/32		connected	40	a-full	a-1000	10/100/1000BaseTX
Gi1/0/33	TRONCAL_ACC3_RACK4	connected	trunk	a-full	a-1000	10/100/1000BaseTX

Figura 43. Listado de Interfaces - sw distribucion

Fuente: (Elaboracion Propia)

- Se verifica que todas las interfaces se encuentran configuradas en modo Automático.
- Se verifica puertos que no están apagados a nivel lógico.
- Se verifica conexiones a nivel de puertos de Acceso hacia equipos finales.

Tercero Verificamos la cantidad de tráfico que está pasando por la interface conectada hacia el CORE.

```
SW-DST-RACK4#sh interfaces port-channel 1 | i rate
Queueing strategy: fifo
5 minute input rate 61121000 bits/sec, 6224 packets/sec
5 minute output rate 10035000 bits/sec, 5340 packets/sec
SW-DST-RACK4#
```

Figura 44. Trafico Interface troncal hacia sw core

Fuente: (Elaboracion Propia)

- Se verifica que se tiene un tráfico de 60 Mbps de input y 10 Mbps de carga.

```
SW-DST-RACK4#sh etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP        Te1/0/1(P) Te1/0/2(P)
```

Figura 45. Estatus Interfaces PorthChannel – sw distribucion
Fuente: (Elaboracion Propia)

- Se valida el funcionamiento correcto a nivel de EtherChannel, la conexión hacia el CORE se encuentra disponible.

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1086151113 multicast, 0 pause input
0 input packets with dribble condition detected
134942323349 packets output, 31581040946244 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Figura 46. Cantidad de Errores Acumulados
Fuente: (Elaboracion Propia)

- No se evidencia errores físicos en las conexiones y conectores (ERRORES CRC), ni mucho menos dropeo y descarte de paquetes.

```
SW-DST-RACK4#sh interfaces counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi1/0/1	29958256444	83576655	18669403	3624767
Gi1/0/2	6091827968	29480545	652740	730275
Gi1/0/3	3941920383	22447068	438975	334048
Gi1/0/4	5792780227	29245595	645098	728023
Gi1/0/5	0	0	0	0
Gi1/0/6	0	0	0	0
Gi1/0/7	5950868538	28074543	524705	577016
Gi1/0/8	5604089423	26947507	655794	472691
Gi1/0/9	7059964537	30976715	648157	762317
Gi1/0/10	8785095052	32360384	520678	558927
Gi1/0/11	7230894700	32385712	665627	664610
Gi1/0/12	7035971804	32786715	657397	684756
Gi1/0/13	7402959589	30850108	667266	746611
Gi1/0/14	0	0	0	0
Gi1/0/15	7009334434	29452953	632870	720880
Gi1/0/16	6215661476	29422038	653077	714875
Gi1/0/17	7617095366	30328001	619639	749502

Figura 47. Cantidad de paquetes trafico multicas y broadcast
Fuente: (preparacion propia)

- Se verifica que las Interfaces de mayor tráfico broadcast y multicast son: Gi1/0/1, Esta interface realiza la conexión hacia el Core.

Cuarto: Se verifica el estado del procesamiento CPU y Memoria

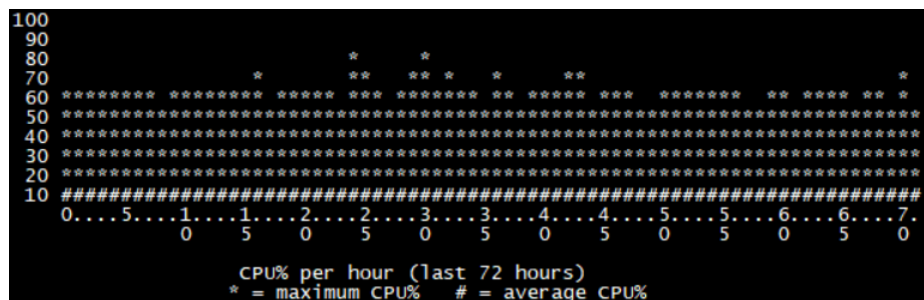


Figura 48. Historial de consumo Cpu – sw distribucion
Fuente: (preparacion propia)

```
N9K-CORE1-PRIMAVERA# show system resources
Load average: 1 minute: 0.50 5 minutes: 0.43 15 minutes: 0.40
Processes : 534 total, 1 running
CPU states : 16.16% user, 2.27% kernel, 81.56% idle
CPU0 states : 13.13% user, 4.04% kernel, 82.82% idle
CPU1 states : 15.30% user, 3.06% kernel, 81.63% idle
CPU2 states : 33.33% user, 1.96% kernel, 64.70% idle
CPU3 states : 2.04% user, 1.02% kernel, 96.93% idle
Memory usage: 16401952K total, 5992064k used, 10409888k free
Current memory status: OK
N9K-CORE1-PRIMAVERA#
```

Figura 49. Cantidad de memoria disponible
Fuente: (preparacion propia)

CAPA ACCESO

Evaluación Física

Primero: Al igual que en la capa superior DISTRIBUCION, se realiza la validación del cableado según el estándar TIA.

Segundo: Verificamos el estado de las Interfaces Físicas.

```
SW-ACC3-RACK4#sh int status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/0/1		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/2		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/3		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/4		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/5		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/6		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/7		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/8		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/9		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/10		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/11		connected	60	a-full	a-100	10/100/1000BaseTX
Gi1/0/12		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/13		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/14		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/15		connected	60	a-full	a-100	10/100/1000BaseTX
Gi1/0/16		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/17		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/18		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/19		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/20		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/21		connected	60	a-full	a-10	10/100/1000BaseTX
Gi1/0/22		connected	60	a-full	a-1000	10/100/1000BaseTX
Gi1/0/23		connected	60	a-full	a-100	10/100/1000BaseTX
Gi1/0/24	ENLACE TRONCAL	connected	trunk	a-full	a-1000	10/100/1000BaseTX

Figura 50. Listado de Interfaces - sw access

Fuente: (Elaboracion Propia)

- Se verifica que todas las interfaces se encuentran configuradas en modo Automático.
- Se verifica que no existen puertos disponibles.

Tercero Verificamos la cantidad de tráfico que está pasando por la interface conectada hacia la sala de DISTRIBUCION.

```
SW-ACC3-RACK4#sh int Gi1/0/24 | i rate
Queueing strategy: fifo
5 minute input rate 77000 bits/sec, 115 packets/sec
5 minute output rate 18000 bits/sec, 24 packets/sec
SW-ACC3-RACK4#
```

Figura 51. Trafico interface troncal sw access

Fuente: (Elaboracion Propia)

- Se verifica que se tiene un tráfico de 77 Kbps de input y 18 Kbps de carga.

```

Received 1701214002 broadcasts (907743941 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 907743941 multicast, 0 pause input
0 input packets with dribble condition detected
305202401 packets output, 90550840420 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

```

Figura 52. Cantidad de errores físicos – sw access
Fuente: (Elaboracion Propia)

- No se evidencia errores físicos en las conexiones y conectores (ERRORES CRC), ni mucho menos dropeo y descarte de paquetes.

```

SW-ACC3-RACK4#sh int counters

```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi1/0/1	4652947824	12263055	372797	288104
Gi1/0/2	4601481919	12459289	375355	274019
Gi1/0/3	3730134186	11837299	394571	275979
Gi1/0/4	4290849009	12314258	390231	311989
Gi1/0/5	5325740188	12564667	379996	295300
Gi1/0/6	3831839794	13282616	391683	312393
Gi1/0/7	4394007535	11126453	398794	305168
Gi1/0/8	4683868121	11697018	394499	302468
Gi1/0/9	5097944330	14104991	394662	294376
Gi1/0/10	4142421152	12515172	438549	341571
Gi1/0/11	5851375636	20716585	1142484	532890
Gi1/0/12	4907490654	13816778	437820	639907
Gi1/0/13	5575344502	14275152	438092	505402
Gi1/0/14	5643743978	13736332	438941	508396
Gi1/0/15	4291524256	16278512	494571	769719
Gi1/0/16	4869293276	12778719	437531	553636
Gi1/0/17	5521314551	14671052	496014	555282
Gi1/0/18	3360230374	12524565	447165	699527
Gi1/0/19	3732181010	12068081	449639	741137
Gi1/0/20	4425523916	15437238	460328	634549
Gi1/0/21	4784559765	17289806	483133	350928
Gi1/0/22	5082364676	14556893	496697	676844
Gi1/0/23	561253609	2206118	670830	86
Gi1/0/24	51966225299	635627973	907745831	793471856

Figura 53. Cantidad de paquetes de tráfico multicast, broadcast
Fuente: (Elaboracion Propia)

- Se verifica que las Interfaces de mayor tráfico broadcast y multicast son: Gi1/0/24, Esta interface realiza la conexión hacia la capa de DISTRIBUCION.

CAPA CORE

- Evaluación Lógica

Primero: Verificamos el estado y la cantidad de Segmentos de RED

Segundo: Verificamos la cantidad de VLANS creadas

```
N9K-CORE1-PRIMAVERA# sh vlan summary
Number of existing VLANs           : 46
Number of existing user VLANs      : 46
Number of existing extended VLANs  : 0
Number of existing assigned controller VLANs: 0
```

Figura 57. Cantidad VLANS creadas – sw core
Fuente: (Elaboracion Propia)

Tercero: Verificamos el estado del protocolo Spanning Tree

```
VLAN0033
Spanning tree enabled protocol rstp
Root ID    Priority    4129
           Address    0023.04ee.be01
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    4129 (priority 4096 sys-id-ext 33)
           Address    0023.04ee.be01
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface    Role Sts Cost    Prio.Nbr Type
-----
Po1          Desg FWD 200     128.4096 (VPC) P2p
Po2          Desg FWD 200     128.4097 (VPC) P2p
Po3          Desg FWD 200     128.4098 (VPC) P2p Peer (STP)
Po4          Desg FWD 200     128.4099 (VPC) P2p
Po7          Desg FWD 200     128.4102 (VPC) P2p
Po20         Desg FWD 250     128.4115 (VPC peer-link) Network P2p
Eth1/13      Desg FWD 2000     128.13   P2p
Eth1/23      Desg FWD 2000     128.23   P2p
Eth1/32      Desg FWD 20000    128.32   P2p
```

Figura 58. Configuración STP – sw core
Fuente: (Elaboracion Propia)

Cuarto: Verificamos la tabla de Enrutamiento y las rutas creadas.

```

N9K-CORE1-PRIMAVERA# sh ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
*** denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
  *via 192.168.2.2, [1/0], 25w6d, static
10.10.5.0/28, ubest/mbest: 1/0
  *via 10.30.131.2, [1/0], 1y21w, static
10.10.10.0/24, ubest/mbest: 1/0
  *via 10.30.131.2, [1/0], 1y21w, static
10.10.10.0/30, ubest/mbest: 1/0
  *via 10.31.131.2, [1/0], 8w1d, static
10.10.30.0/24, ubest/mbest: 1/0
  *via 10.30.131.2, [1/0], 1y21w, static
10.10.50.0/24, ubest/mbest: 1/0
  *via 10.30.131.2, [1/0], 1y21w, static
10.10.70.0/24, ubest/mbest: 1/0
  *via 10.30.131.2, [1/0], 1y21w, static

```

Figura 59. Tabla de enrutamiento – sw core
Fuente: (Elaboracion Propia)

```

ip route 10.20.5.0/25 10.30.131.2 name POS_SALAVERRY
ip route 10.20.7.0/24 10.30.131.2 name SERVIDORES_SALAVERRY
ip route 10.20.9.0/24 10.30.131.2 name SISTEMAS_SALAVERRY
ip route 10.20.10.0/23 10.30.131.2 name ADMINISTRATIVOS_SALAVERRY
ip route 10.20.30.0/23 10.30.131.2 name ALUMNOS_SALAVERRY
ip route 10.20.50.0/23 10.30.131.2 name AULAS_SALAVERRY
ip route 10.20.70.0/23 10.30.131.2 name LABORATORIO_SALAVERRY
ip route 10.20.91.0/24 10.30.131.2 name ToIP_SALAVERRY
ip route 10.20.110.0/24 10.30.131.2 name GESTION_SALAVERRY
ip route 10.20.130.0/24 10.30.131.2 name WAN_SALAVERRY
ip route 10.20.150.0/24 10.30.131.2 name CCTV_SALAVERRY
ip route 10.20.170.0/24 10.30.131.2 name SERVICIOS_SALAVERRY
ip route 10.20.191.0/24 10.30.131.2 name ACCES_POINT_SALAVERRY
ip route 10.20.208.0/22 10.30.131.2 name wifi_CAMPUS_SALAVERRY
ip route 10.20.214.0/23 10.30.131.2 name wifi_ADMIN_SALAVERRY
ip route 10.20.216.0/23 10.30.131.2 name wifi_INVITADOS_SALAVERRY
ip route 10.20.218.0/23 10.30.131.2 name wifi_TI_SALAVERRY
ip route 10.30.131.16/28 10.30.131.2 name WAN_Enlace_Certus_Pri

```

Figura 60. Listado de rutas staticas – sw core
Fuente: (Elaboracion Propia)

Quinto: Validamos el estatus del protocolo HSRP para asegurar el tema de la alta disponibilidad a nivel de VLANs y hacia la WAN

```

N9K-CORE1-PRIMAVERA# sh hsrp summary
HSRP Summary:
Extended-hold (NSF) disabled
Global HSRP-BFD disabled

Total Groups: 34
  Version::      V1-IPV4: 34      V2-IPV4: 0      V2-IPV6: 0
    State::      Active: 33      Standby: 0      Listen: 0
    State::      V6-Active: 0      V6-Standby: 0      V6-Listen: 0

Total HSRP Enabled interfaces: 34

Total Packets:
  Tx - Pass: 496795257 Fail: 0
  Rx - Good: 499152541

```

Figura 61. Configuración HSRP – Alta disponibilidad SW CORE
Fuente: (Elaboracion Propia)

CAPA DISTRIBUCION

Evaluación Lógica

Primero: Verificamos la cantidad de VLANS creadas

```
SW-DST-RACK4#sh vlan summary
Number of existing VLANS           : 41
Number of existing VTP VLANS       : 41
Number of existing extended VLANs  : 0
SW-DST-RACK4#
```

Figura 62. Cantidad de Vlan – sw distribucion
Fuente: (Elaboracion Propia)

Segundo: Verificamos el estado del protocolo Spanning Tree

```
VLAN0040
Spanning tree enabled protocol ieee
Root ID    Priority    4136
           Address    0023.04ee.be01
           Cost        1
           Port        456 (Port-channel1)
           Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32808 (priority 32768 sys-id-ext 40)
           Address    f0b2.e5f7.cc00
           Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time   15 sec

Interface   Role  Sts Cost      Prio.Nbr Type
-----
Gi1/0/23    Desg FWD 4        128.23 P2p
Gi1/0/24    Desg FWD 4        128.24 P2p
Gi1/0/25    Desg FWD 19       128.25 P2p Edge
Gi1/0/32    Desg FWD 4        128.32 P2p Edge
Gi1/0/33    Desg FWD 4        128.33 P2p
Gi1/0/39    Desg FWD 4        128.39 P2p
Gi1/0/46    Desg FWD 4        128.46 P2p
Gi1/0/47    Desg FWD 4        128.47 P2p
Gi1/0/48    Desg FWD 4        128.48 P2p
Po1         Root FWD 1        128.456 P2p
```

Figura 63. Protocolo STP – sw distribucion
Fuente: (Elaboracion Propia)

CAPA ACCESO

Evaluación Lógica

Primero: Verificamos la cantidad de VLANS creadas

```
SW-ACC3-RACK4#sh vlan summary
Number of existing VLANS           : 41
Number of existing VTP VLANs       : 41
Number of existing extended VLANs  : 0
```

Figura 64. Cantidad de vlans credas – sw access
Fuente: (Elaboracion Propia)

Segundo: Verificamos el estado del protocolo Spanning Tree

```
VLAN0040
Spanning tree enabled protocol ieee
Root ID    Priority    4136
           Address    0023.04ee.be01
           Cost       5
           Port       24 (GigabitEthernet1/0/24)
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID   Priority    32808 (priority 32768 sys-id-ext 40)
           Address    f0b2.e5e8.4c80
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time  15 sec

Interface          Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/24           Root FWD 4         128.24 P2p
```

Figura 65. Protocolo STP – sw access

Fuente: (preparacion propia)

Evaluación de Seguridad

CAPA CORE

```
username admin password 5 $5$BFJIGP$msLUePYk4Sk08gEbs78CFdBCI/1.4Gx/bkW332FuSD
username eacosta password 5 $5$HIGICC$aL.NvjyeeBw1CgN6omFktqJAVn/bdIqzQi86KqEP.G/
```

Figura 66. Usuarios de conexión sw core

Fuente: (preparacion propia)

CAPA DISTRIBUCION

```
username mquinto privilege 15 secret 5 $1$ZRZx$7ctwEmD/dtYDH/Gm5TXAo0
username eacosta privilege 15 password 0 190707
```

Figura 67. Usuarios de conexión sw distribucion

Fuente: (preparacion propia)

```
ip access-list extended ACCESO
permit ip 192.168.6.0 0.0.1.255 any
permit ip 10.30.40.0 0.0.0.255 any
permit ip 10.20.10.0 0.0.0.255 any
permit ip 10.150.10.0 0.0.0.255 any
permit ip any any
```

Figura 68. Listas de Accesos – sw distribucion

Fuente: (preparacion propia)

```

login local
line vty 0 4
access-class ACCESO in
login local
length 0
transport input all
line vty 5 15
access-class ACCESO in
login local
length 0
transport input all
!
end

```

Figura 69. Conexión virtual telnet ssh
Fuente: (preparacion propia)

CAPA ACCESO

```

interface GigabitEthernet1/0/5
switchport access vlan 60
switchport mode access
switchport voice vlan 110
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qos trust cos
spanning-tree portfast

```

Figura 70. Configuración Interface sw access
Fuente: (preparacion propia)

```

ip access-list extended ACCESO
permit ip 192.168.6.0 0.0.1.255 any
permit ip 10.30.40.0 0.0.0.255 any
permit ip 10.20.10.0 0.0.0.255 any
permit ip 10.150.10.0 0.0.0.255 any
permit ip any any

```

Figura 71. Configuración Lista de Acceso
Fuente: (preparacion propia)

```

login local
line vty 0 4
access-class ACCESO in
login local
length 0
transport input all
line vty 5 15
access-class ACCESO in
login local
length 0
transport input all

```

Figura 72. Conexión virtual telnet ssh – sw access
Fuente: (preparacion propia)

```

username eacosta privilege 15 secret 5 $1$GVB3$ApBOQfy.uFpIsGov6.fUm.
username mquinto privilege 15 secret 5 $1$B3rl$QigKfVsdEjwybMHPQEWgo1

```

Figura 73. Usuarios de conexión sw access
Fuente: (preparacion propia)

Plantilla de datos de configuración

DISPOSITIVOS	Detalles
Switch Core L3	Ver ANEXO 12: Configuración SW L3

Tabla 38. Plantillas de configuracion SW CORE
Fuente: (preparacion propia)

Análisis a nivel WAN

IP FLOW TOP TALKERS PARA ANALISAR PUNTOS REMOTOS TIEMPOS DE RESPUESTA Y TRAZA

PRUEBA	IP ORIGEN	IP DESTINO	Resultado
Traza	10.30.99.254 (SEDE TLS CHACARILLA)	10.40.99.254 (SEDE TLS JP)	<pre> N9K-CORE1-PRIMAVERA# traceroute 10.40.99.254 traceroute to 10.40.99.254 (10.40.99.254), 30 hops max, 40 byte packets 1 10.30.131.3 (10.30.131.3) 0.315 ms 0.283 ms 0.424 ms 2 10.147.253.225 (10.147.253.225) 1.249 ms 1.092 ms 1.032 ms 3 10.211.253.225 (10.211.253.225) 2.319 ms 2.411 ms 2.163 ms [Label=50313 E=1 TTL=253 S=1] 4 10.211.253.226 (10.211.253.226) 1.827 ms 1.803 ms 1.82 ms 5 10.40.99.253 (10.40.99.253) 2.135 ms 2.013 ms 1.977 ms 6 10.40.99.254 (10.40.99.254) 2.055 ms 2.015 ms 1.987 ms N9K-CORE1-PRIMAVERA# </pre> - La cantidad de Saltos son 6 - El tiempo promedio que demora los paquetes en llegar a la sede Javier Prado desde Chacarilla son: T <= 2 milisegundos
ICMP	10.30.99.254 (SEDE TLS CHACARILLA)	10.40.99.254 (SEDE TLS JP)	<pre> N9K-CORE1-PRIMAVERA# ping 10.40.99.254 PING 10.40.99.254 (10.40.99.254): 56 data bytes 64 bytes from 10.40.99.254: icmp_seq=0 ttl=249 time=2.307 ms 64 bytes from 10.40.99.254: icmp_seq=1 ttl=249 time=2.022 ms 64 bytes from 10.40.99.254: icmp_seq=2 ttl=249 time=2.013 ms 64 bytes from 10.40.99.254: icmp_seq=3 ttl=249 time=2.011 ms 64 bytes from 10.40.99.254: icmp_seq=4 ttl=249 time=1.989 ms --- 10.40.99.254 ping statistics --- 5 packets transmitted, 5 packets received, 0.00% packet loss round-trip min/avg/max = 1.989/2.068/2.307 ms </pre> - Los tiempos de Respuesta tienen un valor promedio de 2 milisegundos - No se identifican perdida de paquetes en él envío y respuesta - La comunicación se efectúa sin ningún problema de Intermittencia o Delay

Tabla 39. Analisis WAN ICMP

Fuente: (preparacion propia)

PRUEBA	IP ORIGEN	IP DESTINO	Resultado
Traza	10.30.99.254 (SEDE TLS CHACARILLA)	8.8.8.8 (dns google)	<pre> N9K-CORE1-PRIMAVERA# traceroute 8.8.8.8 source-interface v1an 30 traceroute to 8.8.8.8 (8.8.8.8) from 192.168.4.2 (192.168.4.2), 30 hops max, 40 byte packets 1 192.168.2.2 (192.168.2.2) 0.317 ms 0.262 ms 0.364 ms 2 200.4.231.206 (200.4.231.206) 0.501 ms 0.421 ms 0.401 ms 3 172.22.10.125 (172.22.10.125) 1.354 ms 1.39 ms 1.291 ms 4 10.111.201.114 (10.111.201.114) 1.736 ms 1.954 ms 2.009 ms 5 10.111.201.114 (10.111.201.114) 2.603 ms 1.184 ms 1.417 ms 6 5.53.0.45 (5.53.0.45) 2.035 ms 84.16.11.205 (84.16.11.205) 1.939 ms 5.53.0.45 (5.53.0.45) 2.049 ms 7 94.142.97.70 (94.142.97.70) 34.614 ms 34.577 ms 34.818 ms 8 176.52.253.187 (176.52.253.187) 36.543 ms 36.292 ms 36.395 ms 9 * * * 10 8.8.8.8 (8.8.8.8) 36.682 ms 36.302 ms 36.337 ms N9K-CORE1-PRIMAVERA# </pre> - La cantidad de Saltos son 10 - El tiempo promedio que demora los paquetes en salir de la sede y llegar hacia los dns de google en USA. T <= 36,3 milisegundos
ICMP	10.30.99.254 (SEDE TLS CHACARILLA)	8.8.8.8 (dns google)	<pre> N9K-CORE1-PRIMAVERA# ping 8.8.8.8 source-interface v1an 30 PING 8.8.8.8 (8.8.8.8): 56 data bytes 64 bytes from 8.8.8.8: icmp_seq=0 ttl=249 time=36.516 ms 64 bytes from 8.8.8.8: icmp_seq=1 ttl=249 time=36.308 ms 64 bytes from 8.8.8.8: icmp_seq=2 ttl=249 time=36.303 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=249 time=36.326 ms 64 bytes from 8.8.8.8: icmp_seq=4 ttl=249 time=36.478 ms --- 8.8.8.8 ping statistics --- 5 packets transmitted, 5 packets received, 0.00% packet loss round-trip min/avg/max = 36.303/36.386/36.516 ms N9K-CORE1-PRIMAVERA# </pre> - Los tiempos de Respuesta tienen un valor promedio de 36,3 milisegundos - No se identifican perdida de paquetes en el envío y respuesta - La comunicación se efectúa sin ningún problema de Intermittencia o Delay

Tabla 40. Analisis WAN Internet

Fuente: (preparacion propia)

Finalmente se realizó la validación del tráfico de cada servicio de internet y conexión hacia las sedes a través de las herramientas de monitoreo proporcionados por el proveedor.

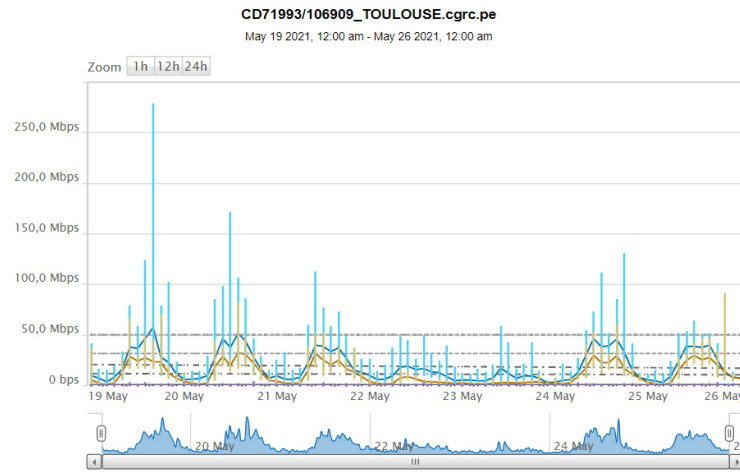


Figura 74. Trafico consumo Internet – TLS router principal
Fuente: (preparacion propia)

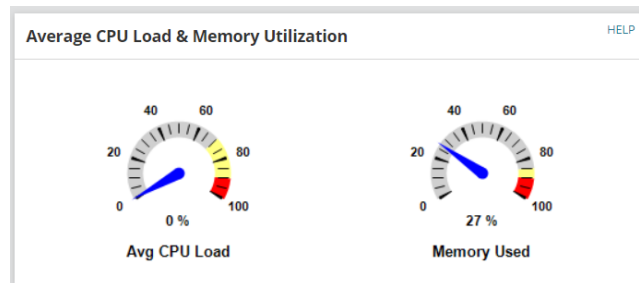


Figura 75. Consumo de CPU router principal tls
Fuente: (preparacion propia)

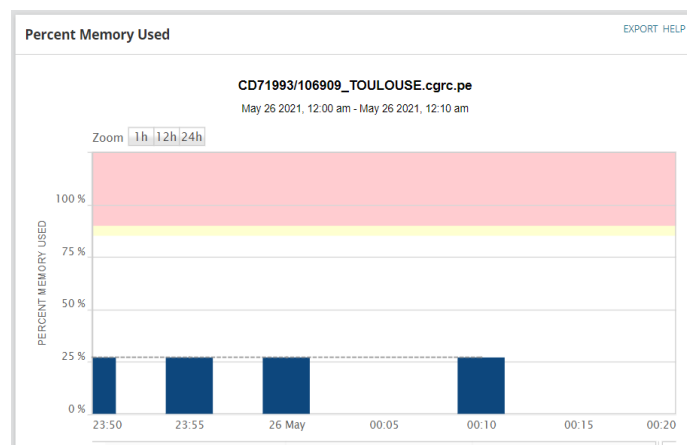


Figura 76. Consumo de memoria router principal tls
Fuente: (preparacion propia)

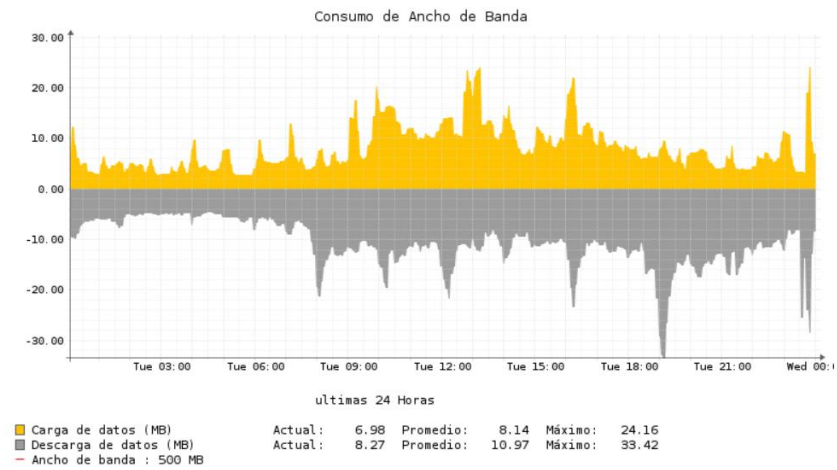


Figura 77. Trafico consumo Internet – CERTUS router principal
Fuente: (preparacion propia)

%USO CPU

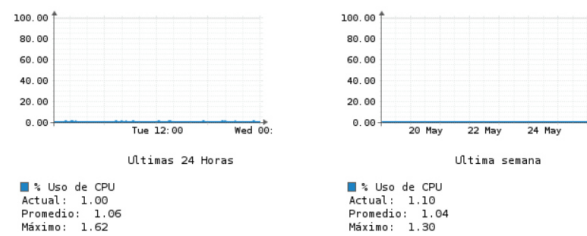


Figura 78. Consumo de CPU router principal certus
Fuente: (preparacion propia)

MEMORIA

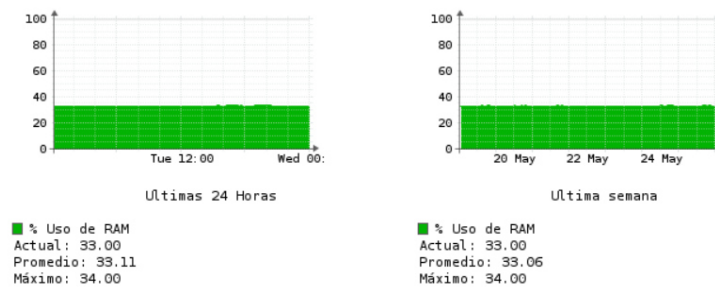


Figura 79. Consumo de memoria router principal certus
Fuente: (preparacion propia)

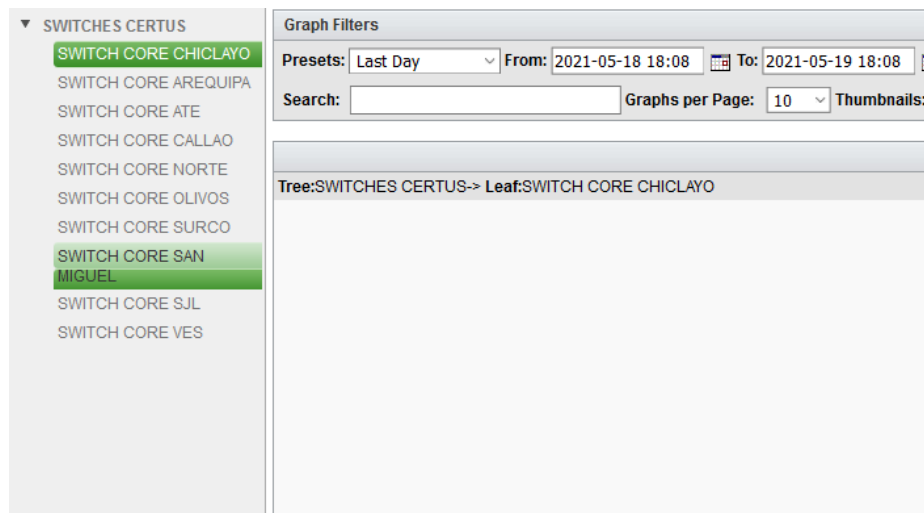


Figura 80. Herramienta de Monitoreo Switches Core Certus - Cacti
Fuente: (preparacion propia)

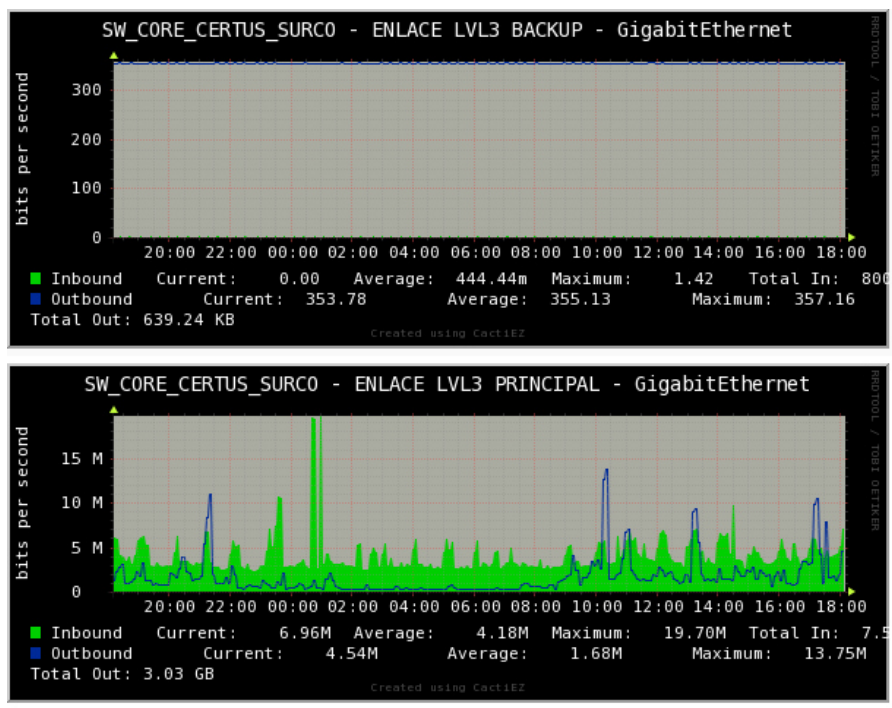


Figura 81. Trafico consumo de red Router Sede surco - certus
Fuente: (preparacion propia)

3.3 EVALUACION

3.3.1 EVALUACION ECONOMICA

En este punto se analizan 2 casos en los cuales se obtuvieron ahorros sustanciales en la parte económica.

Primero La ejecución del proyecto significo ahorros en el aspecto económico debido a que el pago mensual por los servicios de Internet y MPLS se hacían a 3 proveedores ISP diferentes, con el cambio se unifico a un solo proveedor el cual nos brindó mayores beneficios tecnológicos y ahorros económicos.

A continuación, se detallan los pagos mensuales por el servicio de Internet, Datos y seguridad que realizaron las 3 unidades de negocio antes de ejecutar el cambio durante el año 2018.

AÑO	MESES	OPEX (S/.) sin IGV		
		CERTUS	TLS	UCAL
2018	Enero	S/.67,650	S/.26,712	S/.11,269
	Febrero	S/.67,650	S/.26,712	S/.11,269
	Marzo	S/.67,650	S/.26,712	S/.11,269
	Abril	S/.67,650	S/.26,712	S/.11,269
	Mayo	S/.67,650	S/.26,712	S/.11,269
	Junio	S/.67,650	S/.26,712	S/.11,269
	Julio	S/.67,650	S/.26,712	S/.11,269
	Agosto	S/.67,650	S/.26,712	S/.11,269
	Septiembre	S/.67,650	S/.26,712	S/.11,269
	Octubre	S/.67,650	S/.26,712	S/.11,269
	Noviembre	S/.67,650	S/.26,712	S/.11,269
	Diciembre	S/.67,650	S/.26,712	S/.11,269
	TOTAL	S/.811,800	S/.320,544	S/.135,228

Tabla 41. Gastos mensuales servicio de internet 2018

Fuente: (preparacion propia)

El pago anual que se hacía durante 1 año por las 3 razones sociales hacia un monto total de **S/. 1,267.572.**

Segundo, el no poder compartir de recursos debido a que la arquitectura WAN de cada UNE no lo permite, incurría en un gasto al momento de querer dar soporte al área de call center específicamente con el uso de las licencias de sofphone para realizar sus operaciones.

A continuación, se detallan los costos por cada licencia y se muestra la comparación actual en la que estos gastos ya no son asumidos por el negocio gracias a la nueva arquitectura de Red WAN que permite hacer uso de estos sistemas.

Servicio CCVOX	Cantidad	Tipo de Costo		Costo Unitario S/.
		Mensual	Único	
<i>Licencias Basica</i>	1	S/. -	S/. 2475	S/. 2475
<i>Soporte</i>	1	S/. 200	S/. -	S/. 200
<i>Instalación</i>	1	S/. -	S/. -	S/. -
Total				S/. 2675

Tabla 42. Lista de costos por licencia CCVOX
Fuente: (preparacion propia)

Servicio GENESYS	Cantidad	Tipo de Costo		Costo Unitario S/.
		Mensual	Único	
<i>Licencias Basica</i>	1	S/. -	S/. 3225	S/. 3225
<i>Soporte</i>	1	S/. 800	S/. -	S/. 800
<i>Instalación</i>	1	S/. -	S/. -	S/. -
Total				S/. 4025

Tabla 43. Lista de costos por licencia Genesys
Fuente: (preparacion propia)

En la tabla 43 se muestra el costo que involucra comprar una licencia para call center haciendo uso del sistema CCVOX, este servicio es usado por Certus para sus campañas de ventas y cobranza.

En la tabla y se detalla el costo que involucra comprar una licencia para call center haciendo uso del sistema Genesys, este servicio es usado por TLS y UCAL para sus campañas de marketing y cobranza.

Ahora, si el equipo de ventas de cada UNE quisiera adicionar personal por temas de campañas, etc, no tendría otra opción que comprar la licencia del sistema que usa y si quiera hacer uso del otro sistema de call center, no sería posible puesto que ambos se encuentran en REDES WAN separas sin ningún medio de comunicación.

Una vez terminado de exponer los casos en los cuales se evidencia los gastos incurridos ya sea por operación propia del negocio o por la implementación de nuevos servicios y proyectos.

Ahora se muestran los beneficios generados con la implementación de la RED.

BENEFICIOS TANGIBLES

1. Ahorros de costos Servicio de Internet

A continuación, se detallan los costos actuales por el pago recurrente del servicio de Internet, Datos y seguridad perimetral que actualmente se paga por las 3 unidades de negocio.

AÑO	MESES	OPEX (S/.) sin IGV		
		CERTUS	TLS	UCAL
2019	Enero	-	-	-
	Febrero	-	-	-
	Marzo	-	-	-
	Abril	-	-	-
	Mayo	S/.32,650	S/.21,310	S/.6,090
	Junio	S/.32,650	S/.21,310	S/.6,090
	Julio	S/.32,650	S/.21,310	S/.6,090
	Agosto	S/.32,650	S/.21,310	S/.6,090
	Septiembre	S/.32,650	S/.21,310	S/.6,090
	Octubre	S/.32,650	S/.21,310	S/.6,090
	Noviembre	S/.32,650	S/.21,310	S/.6,090
	Diciembre	S/.32,650	S/.21,310	S/.6,090
	TOTAL	S/.261,200	S/.170,400	S/.24,360

Tabla 44. Gastos mensuales servicio de internet 2019

Fuente: (Elaboracion propia)

El monto total pagado durante el primer año de contrato con el nuevo operador fue por un total de S/. 455,960 soles, parte de la negociación fue solicitar un periodo de marcha blanca por los 4 primeros meses del servicio.

Finalmente, en comparación al monto pagado en el año 2018 y el monto pagado posterior al cambio (2019) de operador e implementación del proyecto fue de S/. 811,612 soles ahorrados.

2. Ahorros de costos Operaciones

A nivel de los servicios que se brindan a las distintas áreas del negocio se encuentra una que es muy importante y critica, se trata del área de Marketing que principalmente hace uso de sistemas para hacer llamadas y captar nuevos prospectos, estos hacen uso de sistemas de call center para su operación del día a día. Bajo la nueva arquitectura el área de Marketing tiene la facilidad de usar CCVOX puesto que el sistema se encuentra disponible gracias a la implementación del proyecto, ya no es necesario comprar una licencia de GENESYS que es la más cara en comparación a CCVOX.

Con esto el negocio ahorra gastos operativos cuando el área de marketing desea agregar personal nuevo para sus campañas.

a. Gastos incurridos sin la implementación

El negocio tendría que comprar cada licencia de GENESYS a S/. 3225 soles

b. Gastos incurridos con la implementación

El negocio tendría que comprar cada licencia de CCVOX a S/. 2475 soles o en el caso las licencias de CCVOX se encuentren disponibles al tener mayor cantidad, el gasto sería S/. 0 Soles.

3. Tiempos de Servicio SLA

La implementación de la nueva RED trajo consigo mejorar los tiempos de atención tanto para requerimientos como incidentes así mismo se definió un nivel de servicio lo más cercano posible al 100% debido a que se brindan enlaces redundantes en modo Activo – Activo.

El SLA brindado por el proveedor anterior era de 99.5% en Lima y Provincias, mientras que con el proveedor actual se pudo mejorar este valor a 99.8% en Lima y Provincias.

BENEFICIOS INTANGIBLES

En esta sección se listan todos los beneficios intangibles que se generaron.

- ✓ Acceso Total a la red de las 3 unidades de negocio a través de una sola conexión VPN SSL
- ✓ Mejora de los tiempos de atención y soporte a las unidades de negocio.
- ✓ Facilidad para compartir recursos (File Server, FTP, Carpetas compartidas, Drives) entre usuarios administradores de las 3 unidades de negocio.
- ✓ Visibilidad de todas las cámaras de seguridad de todas las sedes de cada unidad de negocio desde un solo punto de control.
- ✓ Mejora en la calidad de llamada y audio de los servicios de telefonía
- ✓ Mejora en la administración de equipamiento Networking y Seguridad Firewall Centralizado
- ✓ Aumento de capacidad de anchos de banda y su distribución a demanda para cada sede en épocas de campañas de ventas, temporadas de matrícula y cierre de año contable.
- ✓ Mejora en la calidad de servicio de colaboración de Video llamadas.

CAPITULO IV – REFLEXION CRITICA DE LA EXPERIENCIA

Durante todas las etapas del proyecto parte de mi contribución fue ejercer el rol de Administrador de RED y Líder Técnico, junto con el equipo de Infraestructura y el equipo de proyectos. También se trabajó muy de cerca con los Product Owner de cada unidad de negocio y la Gerencia de TI.

La implementación de este proyecto consolida todo el conocimiento obtenido durante los primeros años de ejercicio laboral, sumado a certificaciones y conocimiento es que se pudo concretar mi aporte de manera exitosa a la ejecución del proyecto.

Los principales aportes del autor del trabajo fueron elaboración del RFP, Análisis, diseño de la arquitectura, ejecución de instalación y configuración de equipamiento networking, seguridad y finalmente la validación y aceptación del proyecto.

El éxito del proyecto también está sujeto al uso de buenas prácticas y metodologías aprendidas que fueron de gran ayuda en todo momento.

Los retos más complicados fueron hacer la migración de servicios heredados en los que se tuvo que hacer un troubleshooting con ayuda de debugs, logs, sniffer a nivel de capas superiores e inferiores del modelo OSI en los que nos llevó un tiempo dar con la solución, pero finalmente se superó el inconveniente, además de esto el tiempo estaba en contra debido que al ser un pase a producción no tenemos mucho margen de error y recurrir al rollback no era una opción.

Finalmente, la ejecución del proyecto se llevó a cabo de manera transparente para el usuario final, posterior al pase a producción se afinar temas de seguridad puntuales y temas de performance de la red.

CAPITULO V – CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La Infraestructura de RED es importante para el soporte y desarrollo del negocio puesto que sobre esta se soportan todas las soluciones que se brindan a los usuarios finales, es de vital importancia mantener de manera constante la actualización de la misma aplicando mejoras en los aspectos de Seguridad, Resiliencia, Crecimiento.

La coyuntura actual de pandemia que estamos viviendo nos hizo acelerar cambios a nivel de infraestructura para poder soportar el trabajo de manera remota, sin una arquitectura de RED resiliente a estos cambios no sería posible brindar el teletrabajo.

Esta nueva normalidad nos obliga a reforzar nuestra infraestructura en 2 aspectos importantes disponibilidad y seguridad.

5.2 RECOMENCACIONES

1. Existen sedes de Certus que cuentan con equipamiento fuera de soporte y fuera de venta por parte del proveedor, es por esto que se recomienda migrar estos equipos a un entorno cloud a través de la solución de meraki.
2. Realizar mantenimientos semestrales a los equipos de borde
3. Mantener actualizadas las firmas de seguridad del equipo perimetral ante cualquier ataque nuevo de día Zero.
4. Instalar endpoint sugerido por la marca para tener un control y visibilidad integral de toda la RED.
5. Acotar los servicios publicados por puertos lógicos y no tener expuestos todos los puertos tcp/udp
6. No publicar servicios de RDP de WINDOS puestos que se exponen a ataques cibernéticos de fuerza bruta, esto se debe aplicar usando una conexión de vpn ssl.
7. Apagar todos los puertos de RED LAN para evitar ataques internos hacia los servidores.

FUENTES DE INFORMACIÓN

- RFC 3758. Virtual Router Redundancy Protocol (VRRP)
- <https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf>
- Cisco Design Zone. www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.
- Design Zone for Borderless Networks. www.cisco.com/en/US/netsol/ns1063/networking_solutions_program_home.html.
- Cisco Data Center. www.cisco.com/en/US/netsol/ns340/ns394/ns224/architecture.html.
- ISO/IEC 7498-1: 1994. “Information Processing Systems - OSI Reference Model - The Basic Model.”
- Module 3 (Designing Basic Campus and Data Center Networks)—Designing for Cisco Internetwork Solution Course (DESGN) 2.1.

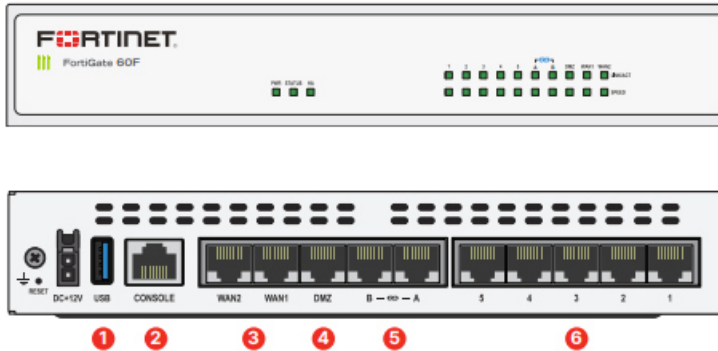
GLOSARIO

- Full Mesh
- Web filtering
- Control de aplicaciones
- FAZ
- Transceiver
- Cos1, Cos2, Cos3
- Trello
- Top And Down
- DMZ
- CCVOX
- GENESYS
- Firewall
- HSPR
- VRRP
- Enrutamiento
- Mpls
- Publisher
- Subscriber
- DVR/NVR
- troubleshooting

ANEXOS

Anexo 1: DATASHEET FORTGATE 60F.

FortiGate / FortiWiFi 60F/61F



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

Hardware Features



Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

3G/4G WAN Connectivity

The FortiGate 60F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

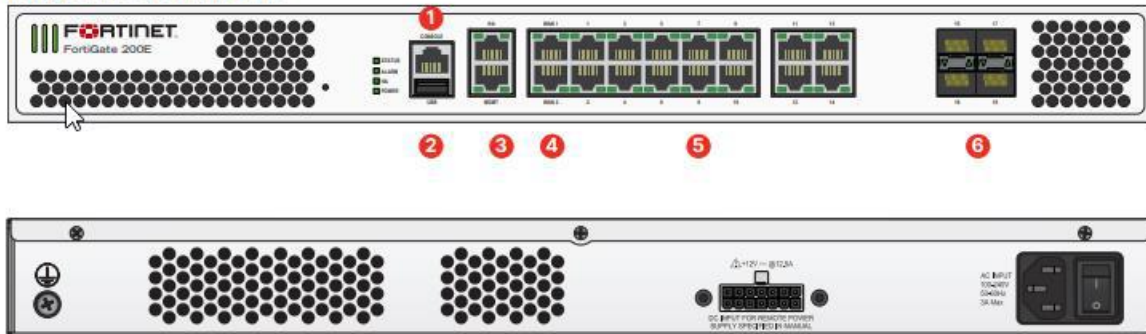
SPECIFICATIONS

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput ²		1.4 Gbps		
NGFW Throughput ^{2,4}		1 Gbps		
Threat Protection Throughput ^{2,5}		700 Mbps		
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		10/10/6 Gbps		
Firewall Latency (64 byte UDP packets)		3.3 μs		
Firewall Throughput (Packets Per Second)		9 Mpps		
Concurrent Sessions (TCP)		700,000		
New Sessions/Second (TCP)		35,000		
Firewall Policies		5,000		
IPsec VPN Throughput (512 byte) ¹		6.5 Gbps		
Gateway-to-Gateway IPsec VPN Tunnels		200		
Client-to-Gateway IPsec VPN Tunnels		500		
SSL-VPN Throughput		900 Mbps		
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		200		
SSL Inspection Throughput (IPS, avg. HTTPS) ³		630 Mbps		
SSL Inspection CPS (IPS, avg. HTTPS) ³		400		
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		55,000		
Application Control Throughput (HTTP 64K) ²		1.8 Gbps		
CAPWAP Throughput (HTTP 64K)		8 Gbps		
Virtual Domains (Default / Maximum)		10 / 10		
Maximum Number of FortiSwitches Supported		16		
Maximum Number of FortiAPs (Total / Tunnel Mode)		64 / 32		
Maximum Number of FortiTokens		500		
High Availability Configurations		Active / Active, Active / Passive, Clustering		
Dimensions				
Height x Width x Length (inches)		1.5 × 8.5 × 6.3		
Height x Width x Length (mm)		38.5 × 216 × 160 mm		
Weight		2.23 lbs (1.01 kg)		
Form Factor		Desktop		
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Anexo 2: DATASHEET FORTGATE 200E.

HARDWARE

FortiGate 200E/201E



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 MGMT/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 4x GE SFP Slots

Hardware Features



Powered by SPU

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed and secure remote access



Network Processor

The SPU NP6Lite network processor works inline with firewall and VPN functions delivering:

- Wire-speed firewall performance for any size packets
- VPN acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

SPECIFICATIONS

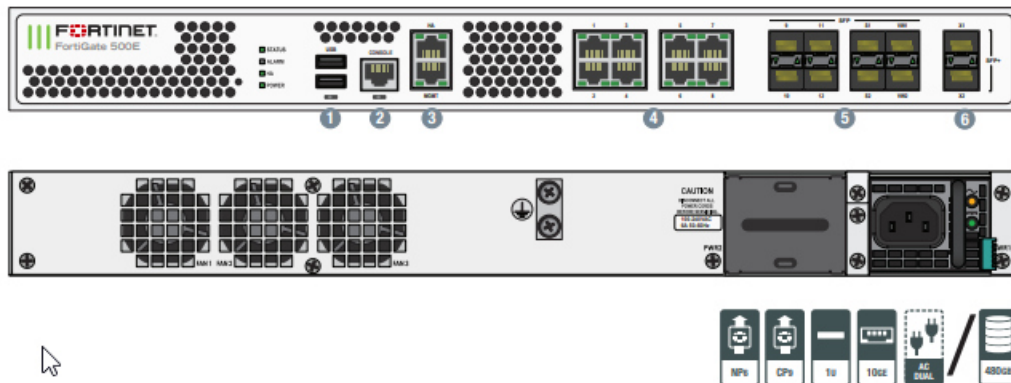
	FORTIGATE 200E	FORTIGATE 201E
Hardware Specifications		
GE RJ45 WAN Interfaces	2	
GE RJ45 Management/HA Ports	2	
GE RJ45 Ports	14	
GE SFP Slots	4	
USB port	1	
Console (RJ45)	1	
Local Storage	—	1× 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	2.2 Gbps	
NGFW Throughput ^{2,4}	1.8 Gbps	
Threat Protection Throughput ^{2,5}	1.2 Gbps	
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 9 Gbps	
Firewall Latency (64 byte UDP packets)	3 μs	
Firewall Throughput (Packets Per Second)	13.5 Mpps	
Concurrent Sessions (TCP)	2 Million	
New Sessions/Second (TCP)	135,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) ¹	7.2 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	10,000	
SSL-VPN Throughput	900 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	820 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	1,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	240,000	
Application Control Throughput (HTTP 64K) ²	3.5 Gbps	
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel Mode)	256 / 128	
Maximum Number of FortiTokens	5,000	

	FORTIGATE 200E	FORTIGATE 201E
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 11.9	
Height x Width x Length (mm)	44.45 × 432 × 301	
Weight	11.9 lbs (5.4 kg)	12.12 lbs (5.5 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Power Input	100–240V AC, 50–60 Hz	
Maximum Current	110 V / 3 A, 220 V / 0.42 A	
Power Consumption (Average / Maximum)	70.98 / 109.9 W	
Heat Dissipation	374.9 BTU/h	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	31.1 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6	

Anexo 3: DATASHEET FORTGATE 500E.

Hardware

FortiGate 500E/501E



Interfaces

- | | |
|-----------------------------|------------------------|
| 1. USB Port | 4. 8x GE RJ45 Ports |
| 2. Console Port | 5. 8x GE SFP Slots |
| 3. 2x GE RJ45 MGMT/HA Ports | 6. 2x 10 GE SFP+ Slots |

Powered by SPU

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck



Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's new, breakthrough SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection of computationally intensive security features:

- Enhanced IPS performance with unique capability of full signature matching at ASIC
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

Specifications



	FORTIGATE 500E	FORTIGATE 501E
Interfaces and Modules		
10 GE SFP+ Slots	2	
GE RJ45 Interfaces	8	
GE SFP Slots	8	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Local Storage	—	2x 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	7.9 Gbps	
NGFW Throughput ^{2,4}	5 Gbps	
Threat Protection Throughput ^{2,3}	4.7 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps	
Firewall Latency (64 byte, UDP)	2 µs	
Firewall Throughput (Packet per Second)	33 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	300,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) ¹	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	50,000	
SSL-VPN Throughput	5 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	5.7 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	3,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	800,000	
Application Control Throughput (HTTP 64K) ³	14 Gbps	
CAPWAP Throughput (1444 byte, UDP)	18 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	72	
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256	
Maximum Number of FortiTokens	5,000	
Maximum Number of Registered Endpoints	2,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 500E	FORTIGATE 501E
Dimensions and Power		
Height x Width x Length (inches)	1.75 x 17.0 x 15.0	
Height x Width x Length (mm)	44.45 x 432 x 380	
Weight	16.1 lbs (7.3 kg)	16.6 lbs (7.5 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Power Consumption (Average / Maximum)	95 W / 193 W	105 W / 200 W
Power Input	100–240V, 50–60Hz	
Current (Maximum)	6A	
Heat Dissipation	613 BTU/h	
Redundant Power Supplies (Hot Swappable)	optional	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	43 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RoHS, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

Anexo 4: DATASHEET CISCO ISR 1100 4P.

Característica arquitectónica	Beneficios / descripción
Procesadores multinúcleo	● Los procesadores multinúcleo de alto rendimiento admiten conexiones WAN de alta velocidad. El plano de datos utiliza un procesador de flujo que ofrece un rendimiento similar al de un circuito integrado específico de la aplicación (ASIC) que no se degrada a medida que se agregan los servicios.
Aceleración de hardware VPN IPsec integrada	● Aumenta la escalabilidad cuando se combina con una licencia de seguridad del software Cisco IOS XE opcional, habilita la seguridad del enlace WAN y los servicios VPN.
Puertos Gigabit Ethernet integrados	● Proporciona hasta 10 puertos Ethernet 10/100/1000 integrados para WAN o LAN (1100-8P: 2 puertos WAN y 8 puertos LAN, 1100-4P: 2 puertos WAN y 4 puertos LAN, 1101-4P: 1WAN y 4 LAN puertos, 1109-2P M2M: 1 WAN y 2 puertos LAN, y 1109-4P M2M: 1 WAN y 4 LAN). ● Todos los modelos de plataformas 1100-8P y 1100-4P tienen un puerto Ethernet 10/100/1000 que puede admitir conectividad basada en factor de forma pequeño conectable (SFP) además de conexiones RJ-45, lo que permite la conectividad de fibra o cobre. ● Dependiendo de la plataforma, PoE / PoE + se puede habilitar en interfaces Gigabit Ethernet (4 puertos PoE o 2 puertos PoE + en el 1100-8P y 2 puertos PoE o 1 PoE + en el 1100-4P), para proporcionar energía a dispositivos externos como terminales de video y puntos de acceso 802.11ac (no disponible en modelos de factor de forma más pequeño C1101 y C1109 M2M). ● Factor de forma más pequeño 1101-4P y 1109-4P con opción de tecnología Cisco WAN LTE Pluggable. Opciones de WAN adicionales como Cisco 12: 1 Serial de alta velocidad conectable.
Acceso a consola basado en USB	● Un puerto de consola micro USB tipo B admite la conectividad de administración cuando los puertos seriales tradicionales no están disponibles. El puerto de consola tradicional también está disponible en modelos seleccionados.
Actualización de PoE opcional	● Está disponible una actualización opcional para habilitar las capacidades de PoE en los módulos de conmutador Ethernet integrados. ● PoE no es compatible con 1101 y 1109.
Soporte de memoria flash	● La serie 1000 se envía con una memoria flash fija de 4 GB u 8 GB, según los modelos seleccionados. ● Los puertos USB 3.0 tipo A brindan capacidades para un almacenamiento conveniente.
DRACMA	● La serie 1000 viene con DRAM fija de 4 GB u 8 GB según los modelos seleccionados. Las series C1111, C1120 y C1160 tienen la opción de incluir una DRAM fija de 8 GB para funciones de seguridad SD-WAN avanzadas.

Anexo 5: DATASHEET CISCO ASR 920.

Major Applications

Broadband Access

The Cisco ASR 920 Router supports broadband access for delivering “any-play” services (voice, video, data, and mobility) to thousands of subscribers, with quality of service (QoS) on the Cisco ASR 920 Router capable of scaling up to a large number of queues per device. The large number of queues, combined with the three-level hierarchical QoS algorithm, results in an enhanced broadband user experience. This full-featured Layer 2 switch and Layer 3 router supports a variety of broadband applications including IPTV and video on demand (VoD), enhancing and extending the Cisco Evolved Programmable Network (EPN) architecture.

Converged Access for Mobile Applications

Deployed as a converged access platform for mobile backhaul, the Cisco ASR 920 Router can aggregate multiple base stations through multiple Ethernet and IP interfaces and can use MPLS as a transport for mobile backhaul traffic. It provides the timing services required in today’s converged access networks by offering integrated support for the Building Integrated Timing Supply (BITS), 1 Pulse Per Second (1PPS), and Time Of Day (TOD) interfaces. The Cisco ASR 920 Router also supports Synchronous Ethernet (SyncE) and IEEE-1588 and can act as the source for network clocking for time-division multiplexing (TDM), SDH and SONET, and SyncE interfaces. In addition to the timing services, the Cisco ASR 920 Router can be deployed in small and fully sealed cabinets in outside environments because of its small form factor and durability in extended temperature ranges.

Metro Ethernet Access

The Cisco ASR 920 Router is built to meet service provider requirements for Carrier Ethernet access. It is optimized for remote access and central offices for smaller aggregation sites where a full-featured, small-footprint converged platform is needed. The Router offers service flexibility and delivers Layer 2, IP, and MPLS transport for advanced L2VPN, L3VPN, and multicast services.

Major Differentiators

The Cisco ASR 920 Router helps service providers deliver differentiated, cost-effective advanced services such as residential broadband, mobile, and Metro Ethernet based on a variety of features.

Flexible Deployment Options

The Cisco ASR 920 Router is designed with a 1RU compact form factor to accommodate deployment in small spaces. Available with a range of mounting options, the router can be deployed in space-constrained locations such as ETSI 300-mm deep cabinets. A small footprint and extended temperature range allow service providers to extend the reach of their Carrier Ethernet networks to more challenging and remote locations.

Power-Supply Unit: High Availability

The Cisco ASR 920 product family offers a choice of AC and DC power supplies. They are redundant and built into the chassis. The Ethernet interfaces are available in copper and fiber, with speeds ranging from 10 Mbps to 10 Gbps.

Anexo 6: DATASHEET CISCO NEXUS 9K

Product overview

Application architectures and deployment modes are rapidly evolving. Modern applications are multinode, highly modular, and deployed over a combination of bare-metal, virtual, and cloud data center environments. In addition to that, individual departments within an organization have varying infrastructure and networking needs. These factors require that data center networks be simple, programmable, extensible, scalable, and shareable to meet the demands of applications.

The Cisco Nexus® 9000 Series Switches operate in one of two modes - Cisco Application Centric Infrastructure (Cisco ACI™) or Cisco NX-OS. In Cisco ACI mode, these switches provide a turnkey, fully automated, policy-based architecture to design and manage data center fabrics. In Cisco NX-OS mode, these switches provide the capability to use foundational layer 2/3 technologies, as well as modern technologies such as VXLAN, with a Border Gateway Protocol-Ethernet VPN (BGP-EVPN) control plane, Segment routing, Multiprotocol Label Switching (MPLS), and automation via NX-APIs.

The Cisco Nexus 9000 Series Switches include the Nexus 9500 Series modular switches and the Nexus 9200/9300 Series fixed switches.



Figure 1.
Cisco Nexus 9000 Series Switch Chassis

The Cisco Nexus 9500 Series modular switches support a comprehensive selection of line cards and fabric modules that provide 1-, 10-, 25-, 40-, 50-, 100-, 200-, and 400-Gigabit Ethernet interfaces. Using these line cards the Cisco Nexus 9500 Series switches can be configured with up to.

1. 256 400-Gigabit Ethernet ports (or)
2. 524 200-Gigabit Ethernet ports# (or)
3. 1024 100-Gigabit Ethernet ports (or)
4. 2048 50-Gigabit Ethernet ports (or)
5. 1024 40-Gigabit Ethernet ports (or)
6. 2304 25-Gigabit Ethernet ports (or)
7. 2304 1/10-Gigabit Ethernet ports

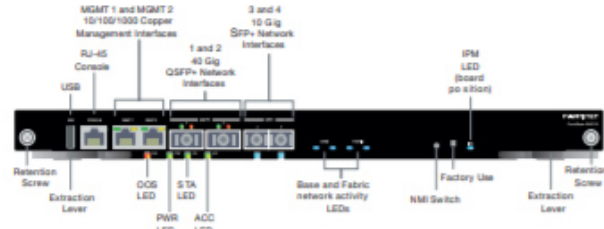
Anexo 7: DATASHEET FORTIGATE 5001E - VDOM

SECURITY BLADES

FortiGate 5001E/5001E1

Latest purpose-built FortiGate security blade with carrier-class capacity and protection.

Hardware Features

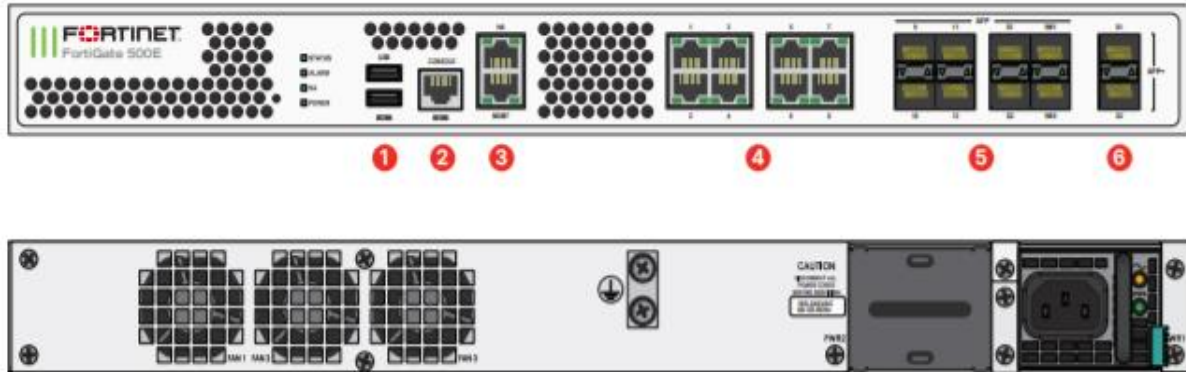


FG-5001E/5001E1	
Interfaces and Storage	
40 GE QSFP+ Ports	2
10 GE SFP+ Ports	2
GE RJ45 Ports	2
RJ45 Console Port	1
Included Transceivers	2× 10 GE SFP+ SR
Local Storage	1× 480 GB SSD (5001E1)
System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	80 / 80 / 50 Gbps
Firewall Latency (64 byte UDP packets)	3 μs
Firewall Throughput (Packets Per Second)	75 Mpps
Concurrent Sessions (TCP)	40 Million
New Sessions/Second (TCP)	640,000
Maximum Firewall Policies	200,000
IPsec VPN Throughput (512 byte packets)	45 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	64,000
SSL-VPN Throughput	9 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	25,000
IPS Throughput (HTTP / Enterprise Mix) ¹	25 / 18 Gbps
SSL Inspection Throughput ²	15 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	8,805
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	3.97 Million
Application Control Throughput ³	36 Gbps
NGFW Throughput ⁴	15 Gbps
Threat Protection Throughput ⁴	13.5 Gbps
CAPWAP Throughput	15 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiTokens	20,000
Maximum Number of Registered FortiClients	20,000
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 1,024
Power and Environment	
Power Consumption (Average / Maximum)	250 / 278 W
Heat Dissipation (Average)	948.6 BTU/h
Operating Temperature	23–131°F (-5–55°C)
Storage Temperature	-40–158°F (-40–70°C)
Humidity	10–90% non-condensing
Compliance	
Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, ICESA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
NEBS Certified	—

Anexo 8: DATASHEET FORTIGATE 500E

HARDWARE

FortiGate 500E



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 8x GE RJ45 Ports
5. 8x GE SFP Slots
6. 2x 10 GE SFP+ Slots

Hardware Features



Powered by SPU

- Fortinet's custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck



Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

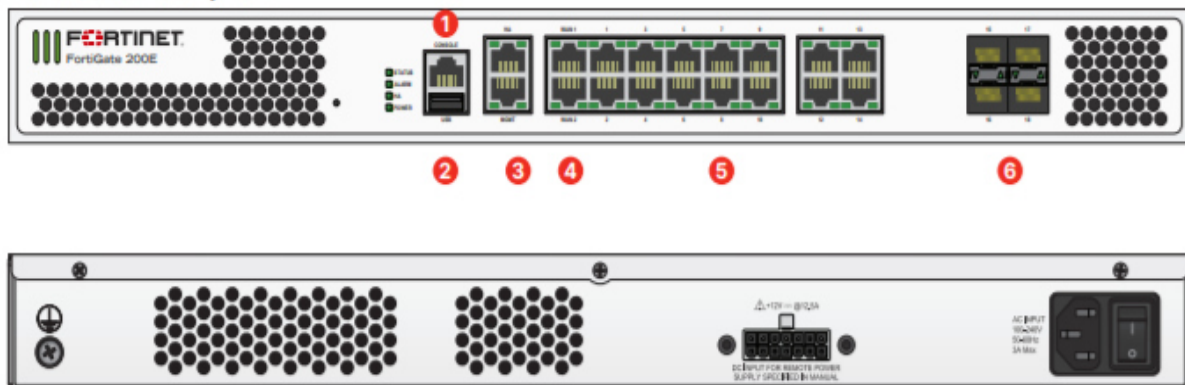
Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

Anexo 9: DATASHEET FORTIGATE 200E/201E

HARDWARE

FortiGate 200E/201E



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 MGMT/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 4x GE SFP Slots

Hardware Features



Powered by SPU

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed and secure remote access



Network Processor

The SPU NP6Lite network processor works inline with firewall and VPN functions delivering:

- Wire-speed firewall performance for any size packets
- VPN acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

Anexo 10: DATASHEET FORTIGATE 800F

SPECIFICATIONS



FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-800G
Capacity and Performance			
GB/Day of Logs	25	100	200
Analytic Sustained Rate (logs/sec)*	500	2,000	4,000
Collector Sustained Rate (logs/sec)*	750	3,000	6,000
Devices/VDOMs (Maximum)	50	180	800
Max Number of Days Analytics**	50	28	50
Options			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
SOC Subscription	✓	✓	✓
FortiGuard Outbreak Alert Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount
Total Interfaces	2 x RJ45 GE	4 x RJ45 GE	4 x RJ45 GE, 2 x SFP
Storage Capacity	4TB (2 x 2TB)	8 TB (2 x 4 TB)	16 TB (4 x 4 TB)
Usable Storage (After RAID)	2 TB	4 TB	8 TB
Removable Hard Drives	No	No	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1/5/5L/10
RAID Type	Software	Software	Hardware / Hot Swappable
Default RAID Level	1	1	10
Redundant Hot Swap Power Supplies	No	No	Optional
Dimensions			
Height x Width x Length (inches)	9.5 x 3.5 x 8	1.73 x 17.24 x 16.38	1.73 x 17.32 x 21.65
Height x Width x Length (cm)	241 x 8.9 x 20.55	4.4 x 43.8 x 41.6	4.4 x 44.0 x 55.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)
Environment			
AC Power Supply	100-240V AC, 50-60 Hz	100-240V AC, 60-50 Hz	100-240V AC, 50-60 Hz
Power Consumption (Average / Maximum)	36W / 43W	90.1W / 99 W	134W / 174.2 W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	594.4 BTU/h
Operating Temperature	32-104° F (0-40° C)	32-104° F (0-40° C)	32-104° F (0-40° C)
Storage Temperature	-4-167° F (-20-75° C)	-13-167° F (-25-75° C)	-4-167° F (-20-75° C)
Humidity	5 to 95% non-condensing	20 to 90% non-condensing	5 to 95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

Anexo 11: DATASHEET TRANSCEIVER

Cost-effective Small Form-factor Pluggable (SFP) transceivers for Gigabit Ethernet applications

Product overview

The industry-standard Cisco® Small Form-Factor Pluggable (SFP) Gigabit Interface Converter (Figure 1) links your switches and routers to the network. The hot-swappable input/output device plugs into a Gigabit Ethernet port or slot. Optical and copper models can be used on a wide variety of Cisco products and intermixed in combinations of 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-EX, 1000BASE-ZX, or 1000BASE-BX10-D/U on a port-by-port basis.



Figure 1.
Cisco Optical Gigabit Ethernet SFP



Figure 2.
Cisco 1000BASE-T Copper SFP



Figure 3.
Cisco 2-Channel 1000BASE-BX Optical SFP

Features and benefits

- Hot swappable to maximize uptime and simplify serviceability
- Flexibility of media and interface choice on a port-by-port basis, so you can "pay as you populate"
- Robust design for enhanced reliability
- Supports Digital Optical Monitoring (DOM) capability

Anexo 12: SH RUN - SW CORE

```
<CERLIMSURSWCORE_01>display current-configuration
#
version 5.20.105, Release 1808P27
#
sysname CERLIMSURSWCORE_01
#
clock timezone Bogota minus 05:00:00
#
dhcp relay server-group 0 ip 10.100.54.6
#
irf domain 1
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
irf member 1 priority 32
irf member 2 priority 16
#
domain default enable system
#
dns server 172.100.9.163
dns server 172.100.9.164
dns server 10.100.54.3
dns server 10.200.2.5
#
ip http enable
#
password-recovery enable
#
ip forward-broadcast
#
acl number 3100 name TELEFONIA
rule 10 permit ip source 10.100.63.0 0.0.0.255
rule 20 permit ip destination 10.100.63.0 0.0.0.255
#
vlan 1
#
vlan 10
#
vlan 100
name PRC_RED_CENTURY
#
vlan 101
name PRC_RED_TELEFONICA
#
vlan 102
name PRC_RED_SERVIDORES
#
vlan 103
name PRC_RED_TELEFONIA
#
vlan 683
description certus-admin683
#
vlan 702 to 706
#
vlan 711 to 719
#
vlan 720
name WIFI_LAB_MOvil
#
vlan 999
description REDROUTERS

traffic classifier voz operator and
if-match acl 3100
#
traffic behavior class_voz
remark dscp ef
remark dot1p 6
#
qos policy voz
classifier voz behavior class_voz
#
dhcp server ip-pool lab_movil_wifi
network 10.200.14.0 mask 255.255.254.0
gateway-list 10.200.14.1
dns-list 172.100.9.163 172.100.9.164
#
```