



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería de Telecomunicaciones

**Optimización del sistema de interconexión, seguridad
perimetral y de comunicación entre sedes de empresa
minera con migración de tecnología MPLS a IP sobre
enlaces dedicados de internet**

TRABAJO DE SUFICIENCIA PROFESIONAL

**Para optar el Título Profesional de Ingeniero en
Telecomunicaciones**

AUTOR

Luis Antonio RODRIGUEZ VIGIL

ASESOR

Mg. Rejis Renato PAREDES PEÑAFIEL

Lima, Perú

2023



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

Rodriguez, L. (2023). *Optimización del sistema de interconexión, seguridad perimetral y de comunicación entre sedes de empresa minera con migración de tecnología MPLS a IP sobre enlaces dedicados de internet*. [Trabajo de Suficiencia Profesional, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Luis Antonio Rodriguez Vigil
Tipo de documento de identidad	DNI
Número de documento de identidad	70477954
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	REJIS RENATO PAREDES PEÑAFIEL
Tipo de documento de identidad	DNI
Número de documento de identidad	06758404
URL de ORCID	https://orcid.org/0000-0003-4829-8953
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	OSCAR ARMANDO CASIMIRO PARIASCA
Tipo de documento	DNI
Número de documento de identidad	06592392
Miembro del jurado 1	
Nombres y apellidos	JUAN FRANCISCO TISZA CONTRERAS
Tipo de documento	DNI
Número de documento de identidad	08596442
Datos de investigación	
Línea de investigación	C.0.3.3. Desarrollo de modelos y aplicación de las tecnologías de información y comunicaciones
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: América Móvil Perú SAC País: Perú Departamento: Lima Provincia: Lima Distrito: La Victoria

	Latitud: -12.086303345664362 Longitud: -77.01452721745714
Año o rango de años en que se realizó la investigación	Enero 2019 - Mayo 2021
URL de disciplinas OCDE	Telecomunicaciones http://purl.org/pe-repo/ocde/ford#2.02.05 Ingeniería de sistemas y comunicaciones http://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERIA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 062/FIEE-EPIE/2023

Los suscritos Miembros, nombrados por la Dirección de la Escuela profesional de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia del **ING. OSCAR ARMANDO CASIMIRO PARIASCA**, integrado por el **MG. JUAN FRANCISCO TISZA CONTRERAS**, **MG. RICARDO YAURI RODRIGUEZ** y Miembro Asesor el **MG. REJIS RENATO PAREDES PEÑAFIEL**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. LUIS ANTONIO RODRIGUEZ VIGIL** con código N° **11190192** que para optar el Título Profesional de Ingeniero en Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **OPTIMIZACIÓN DEL SISTEMA DE INTERCONEXIÓN, SEGURIDAD PERIMETRAL Y DE COMUNICACIÓN ENTRE SEDES DE EMPRESA MINERA CON MIGRACION DE TECNOLOGIA MPLS A IP SOBRE ENLACES DEDICADOS DE INTERNET**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió aprobar otorgándole el calificativo de **diecisiete (17)**.

Ciudad Universitaria, 20 de mayo del 2023

ING. OSCAR ARMANDO CASIMIRO PARIASCA

Presidente de Jurado

MG. JUAN FRANCISCO TISZA CONTRERAS

Miembro Jurado

MG. RICARDO YAURI RODRIGUEZ

Miembro de Jurado

MG. REJIS RENATO PAREDES PEÑAFIEL

Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
ESCUELA PROFESIONAL DE INGENIERIA DE TELECOMUNICACIONES

INFORME DE ORIGINALIDAD

1. Facultad de Ingeniería Electrónica y Eléctrica.
2. Escuela Profesional de Ingeniería de Telecomunicaciones.
3. Emisor del Informe el Director de la Escuela Profesional de Telecomunicaciones.
4. Operador del programa informático de similitudes: **Roberto Florentino Unsihuay Tovar.**
5. Documento evaluado: Trabajo de Suficiencia Profesional para título de (pregrado)
OPTIMIZACIÓN DEL SISTEMA DE INTERCONEXIÓN, SEGURIDAD PERIMETRAL Y DE COMUNICACIÓN ENTRE SEDES DE EMPRESA MINERA CON MIGRACION DE TECNOLOGIA MPLS A IP SOBRE ENLACES DEDICADOS DE INTERNET.
6. Autor de la tesis: **LUIS ANTONIO RODRIGUEZ VIGIL.** Fecha de aplicación de recepción del documento: 17 -03 - 2023
7. Fecha de aplicación del programa informático de similitudes: 17 -03 - 2023
8. Software utilizado: Turnitin.
9. Configuración del programa detector de similitudes:
 - Excluye citas.
 - Excluye bibliografía.
 - Excluye cadenas menores de 40 palabras
10. Porcentaje de similitudes según programa detector: Seis por ciento – 6%
11. Fuentes originales de las similitudes encontradas.

1. www.claro.com.pe	2% Fuente de Internet
2. cybertesis.uni.edu.pe	2% Fuente de Internet
3. Hdl.handle.net	1% Fuente de Internet
4. Lopezvictor01.jimdofree.com	<1% Fuente de Internet
12. Observaciones: Ninguna.
13. Calificación de originalidad.
 - Documento cumple criterios de originalidad, sin observaciones.
14. Fecha del informe: 29 de mayo del 2023. Atentamente,

Mg. Roberto Florentino Unsihuay Tovar
Director de la Escuela Profesional de Telecomunicaciones



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
ESCUELA PROFESIONAL DE INGENIERIA DE TELECOMUNICACIONES

Anexo 1

OPTIMIZACION DEL SISTEMA DE INTERCONEXIÓN, SEGURIDAD PERIMETRAL Y DE COMUNICACIÓN ENTRE SEDES DE EMPRESA MINERA CON MIGRACION DE TECNOLOGIA MPLS A IP SOBRE ENLACES DEDICADOS DE INTERNET

Fecha de entrega: 17-mar-2023 01:44 pm - AUT: 05000

Identificador de la entrega: 2039536737
por Luis Antonio Rodríguez Vigil

Nombre del archivo: TSP_Luis_Rodriguez_F2023_4.pdf (2.62M)

Total de palabras: 12953

Total de caracteres: 73739



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
ESCUELA PROFESIONAL DE INGENIERIA DE TELECOMUNICACIONES

OPTIMIZACION DEL SISTEMA DE INTERCONEXIÓN, SEGURIDAD PERIMETRAL Y DE COMUNICACIÓN ENTRE SEDES DE EMPRESA MINERA CON MIGRACION DE TECNOLOGIA MPLS A IP SOBRE ENLACES DEDICADOS DE INTERNET

INFORME DE ORIGINALIDAD

6%

INDICE DE SIMILITUD

6%

FUENTES DE INTERNET

0%

PUBLICACIONES

4%

TRABAJOS DEL
ESTUDIANTE

FUENTES PRIMARIAS

1

www.claro.com.pe

Fuente de Internet

2%

2

cybertesis.uni.edu.pe

Fuente de Internet

2%

3

hdl.handle.net

Fuente de Internet

1%

4

lopezvictor01.jimdofree.com

Fuente de Internet

<1%

DEDICATORIA

A mi madre, Rosa, por brindarme educación y permitirme llegar a donde estoy y estaré, todo es por ella.

A mi hijo, Nicolás, y a mi novia, Gaby, por ser mi principal motivo para crecer y desarrollarme mucho más siempre, por ellos y para ellos.

AGRADECIMIENTOS

A la Facultad por darnos la oportunidad de poder acceder al título profesional de Ingeniería de Telecomunicaciones mediante el programa de Titulación por Trabajo de Suficiencia Profesional y habernos preparado para el reto de ser profesionales de primer nivel en el mundo competitivo de las telecomunicaciones.

Gracias a mi madre, mi familia y amigos, que de muchas formas directa o indirectamente interactuaron para no rendirme en el camino de lograr mi profesión. Gracias a la empresa Claro Perú, por permitir desarrollarme como profesional, abrirme las puertas para crecer y aplicar en gran medida mis conocimientos.

RESUMEN

El presente trabajo de suficiencia profesional presenta el diseño e implementación de un proyecto de optimización del sistema de comunicaciones en 3 sedes de una empresa minera, dicha empresa inicialmente contaba con un sistema limitado y desfasado en tecnología, tanto en anchos de banda como equipamientos, se ofreció un planteamiento de mejora de sedes remotas migrando la tecnología de su proveedor actual de MPLS con anchos de banda de baja capacidad hacia enlaces de internet dedicado en cada punto con mejoras considerables de anchos de banda que mejoraron hasta en 300% la transferencia de datos.

Se realizaron análisis adecuados donde se buscó resguardar la operatividad de la interconexión, accesos a servidores, mejorar las plataformas de seguridad perimetral y poder brindar una solución de telefonía IP independientes con gestión centralizada.

La solución está considerada como optimización y es capaz de proyectar desarrollos sin generar gastos adicionales. Por ejemplo, las migraciones a la nube (correos, servidores), uso de VoWifi en las unidades mineras sin señal móvil.

Palabras claves: minería, MPLS, internet, ancho de banda, optimizaciones.

TABLA DE CONTENIDO

DEDICATORIA	II
AGRADECIMIENTOS	III
RESUMEN.....	IV
TABLA DE CONTENIDO.....	V
INDICE DE ILUSTRACIONES.....	VII
INDICE DE TABLAS.....	VIII
CAPITULO I: INTRODUCCIÓN.....	1
<i>1.1 Levantamiento de información.....</i>	<i>1</i>
<i>1.2 Diseño de la solución.....</i>	<i>1</i>
<i>1.3 Presentación a cliente.....</i>	<i>1</i>
<i>1.4 Aceptación e implementación del proyecto.....</i>	<i>1</i>
CAPITULO II: CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA 3	
<i>2.1 Empresa</i>	<i>3</i>
<i>2.2 Nuestra Visión.</i>	<i>4</i>
<i>2.3 Nuestra Misión.</i>	<i>4</i>
<i>2.4 Organización de la empresa.....</i>	<i>5</i>
<i>2.5 Área, cargo y funciones desempeñadas</i>	<i>5</i>
<i>2.6 Experiencia Profesional realizada en la organización</i>	<i>5</i>
CAPITULO III: ACTIVIDADES DESARROLLADAS	7
<i>3.1 Situación del Problema</i>	<i>7</i>
<i>3.2 Determinación del Problema</i>	<i>7</i>

3.2.1	Formulación del Problema.....	7
3.3	<i>Solución</i>	8
3.3.1	Objetivos.....	8
3.3.2	Alcance	8
3.3.3	Etapas y Metodología	9
3.3.4	Levantamiento e Implementación.....	9
3.4	<i>Evaluación Económica</i>	44
CAPITULO IV: REFLEXIÓN CRÍTICA DE LA EXPERIENCIA.....		47
CAPITULO V: CONCLUSIONES Y RECOMENDACIONES		49
5.1	<i>Conclusiones</i>	49
5.2	<i>Recomendaciones</i>	49
5.3	<i>Fuentes de información</i>	50
5.4	<i>Glosario</i>	51
CAPITULO VI: ANEXOS		56
6.1	<i>ESTUDIO DE FACTIBILIDAD EN GABINETE PARA SEDE LIMA</i>	56
6.2	<i>ESTUDIO DE FACTIBILIDAD EN GABINETE PARA U.M EL SANTO</i>	58
6.3	<i>APROVISIONAMIENTO EN SEDE FISCAL LIMA</i>	59
6.4	<i>APROVISIONAMIENTO EN U.M EL SANTO</i>	60
6.5	<i>CONFIGURACION Y TOPOLOGIAS</i>	62
6.6	<i>PRUEBAS DE CONFIGURACION EN U.M EL SANTO</i>	79
6.7	<i>PRUEBAS DE CONFIGURACION EN U.M SUYCKUTAMBO</i>	80

INDICE DE ILUSTRACIONES

<i>Ilustración 1</i> Organigrama de la Empresa.....	5
<i>Ilustración 2</i> Análisis y verificación de POP cercano.....	¡Error! Marcador no definido.
<i>Ilustración 3</i> Diseño de tendido de fibra desde MUFA hacia cliente}	¡Error! Marcador no definido.
<i>Ilustración 4</i> Validación de puertos disponibles en POP	¡Error! Marcador no definido.
<i>Ilustración 5</i> Validación de tipo de equipamiento en POP	¡Error! Marcador no definido.
<i>Ilustración 6</i> Reserva de recursos de POP	¡Error! Marcador no definido.
<i>Ilustración 7</i> Asignación de recurso y marcación de puntos....	¡Error! Marcador no definido.
<i>Ilustración 8:</i> Vista Geográfica y Perfil de elevación, primer enfoque....	¡Error! Marcador no definido.
<i>Ilustración 9:</i> Vista Geográfica y Perfil de elevación, segundo enfoque .	¡Error! Marcador no definido.
<i>Ilustración 10:</i> Vista Geográfica y Perfil de elevación, tercer enfoque ...	¡Error! Marcador no definido.
<i>Ilustración 11</i> Validación de energía en Site Caylloma	¡Error! Marcador no definido.
<i>Ilustración 12</i> Validación de energía en cliente	17
<i>Ilustración 13</i> Análisis de ubicación de antena e U.M El Santo	17
<i>Ilustración 14</i> TSS de ubicación de equipamiento en Repetidora de cliente.....	18
<i>Ilustración 15</i> Revisión de aplazamiento.....	20
<i>Ilustración 16</i> Primer análisis para ubicación de antena	20
<i>Ilustración 17</i> Segundo análisis de ubicación de Antena	21
<i>Ilustración 18</i> Topología de proyect.....	28
<i>Ilustración 19</i> Topología incluyendo soluciones de seguridad y voz	29
<i>Ilustración 20</i> Cronograma presentado a cliente	35

<i>Ilustración 21 Ruta reservada para proyecto de fibra</i>	<i>36</i>
<i>Ilustración 22 Topología de red final</i>	<i>37</i>

INDICE DE TABLAS

<i>Tabla 1 Distribución de usuarios por sede</i>	10
<i>Tabla 2 Escenario actual de cliente</i>	11
<i>Tabla 3 Análisis de Ventajas y Desventajas de Soluciones</i>	12
<i>Tabla 4 Proyectos derivados a análisis de factibilidad</i>	13
<i>Tabla 5 Tipo de estudio por sede de cliente</i>	13
<i>Tabla 6 Equipamiento radio - Site Caylloma</i>	16
<i>Tabla 7 Equipamiento radio - Site Repetidora cliente</i>	16
<i>Tabla 8 Equipamiento radio - Site cliente U.M El Santo</i>	16
<i>Tabla 9 Descripción de equipamiento necesario para instalación</i>	19
<i>Tabla 10 Detalles técnicos para instalación</i>	19
<i>Tabla 11 Revisión de ubicación de antena</i>	21
<i>Tabla 12 Tabla de equipamiento y montaje</i>	21
<i>Tabla 13 Revisión de energía y puesta a tierra</i>	22
<i>Tabla 14 Definición de equipamiento</i>	22
<i>Tabla 15 Comparativo de 3 marcas para la solución</i>	24
<i>Tabla 16 Elección de equipamiento para seguridad</i>	24
<i>Tabla 17 Presentación económica de solución hacia cliente</i>	30
<i>Tabla 18 Presentación económica de solución</i>	31
<i>Tabla 19 Descripción de pasos para implementación</i>	32
<i>Tabla 20 Características y equipos a instalar</i>	41
<i>Tabla 21 Validación de potencia de transmisión</i>	41
<i>Tabla 22 Comparativo económico entre antigua solución vs nueva planteada</i>	45
<i>Tabla 23 Detallado descriptivo de solución para cliente</i>	46

CAPITULO I: INTRODUCCIÓN

El presente informe de Suficiencia Profesional detalla el proceso de optimización del sistema de comunicaciones de una empresa minera, cliente de Claro Perú, que indica la necesidad de realizar mejoras en todo el sistema de comunicaciones, desde la interconexión entre sedes remotas y los accesos a servidores hasta las plataformas de telefonía y acceso a la nube.

El proceso de mejoramiento tuvo el siguiente flujo para llegar a una solución adecuada para el cliente:

1.1 Levantamiento de información.

Es en este proceso donde se generan todos los lineamientos del proyecto según la necesidad del cliente, en esta etapa encontramos que los servicios de conectividad, seguridad y telefonía en las 3 sedes del cliente eran muy limitados para desarrollar las actividades de manera óptima o plantear mejoras a nivel de Tecnologías de la Información.

1.2 Diseño de la solución.

Posterior a tener los detalles de la necesidad del cliente, junto al área de consultoría y factibilidad, desarrollamos diseños de solución para las 3 sedes remotas de cliente, teniendo siempre en cuenta la optimización de anchos de banda, seguridad y telefonía. Se plantean cambios de MPLS a Internet, instalación de nuevos Firewalls y utilizar Telefonía IP.

1.3 Presentación a cliente.

Se realizar una presentación con el diseño de la solución planteada, para realizar cambios, ajustes o mejoras, se presenta el costo del proyecto para el cliente, tiempos de implementación y recomendaciones.

1.4 Aceptación e implementación del proyecto.

Una vez ajustada la solución exactamente a lo que necesita el cliente, se procede a la

aceptación de condiciones de servicio, esto da pie a iniciar la instalación de la solución.

La implementación del proyecto plantea realizar visitas de prediseño en sitio para realizar análisis de Planta Externa y Planta Interna en las 3 sedes de cliente.

Se solicitan los permisos adecuados para realizar los trabajos de implementación.

Se presentaron diversos retos durante la implementación del proyecto, la pandemia generó retrasos considerables, la posición de la empresa, los nuevos permisos, nuevas direcciones generales de la empresa, significaron cambios a la hora de la ejecución del proyecto.

Todas estas superadas para finalizar correctamente el proyecto.

CAPITULO II: CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA

2.1 Empresa

América Móvil actualmente está considerada como la operadora latinoamericana líder en el sector de Telecomunicaciones Opera bajo la marca Claro en 16 países del continente: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana y Uruguay. En sucursales distintas a Latinoamérica se identifica con otra denominación, como Tracfone

La compañía ha crecido orgánicamente y ha efectuado importantes adquisiciones en toda América Latina, Estados Unidos, el Caribe y Europa ofreciendo una amplia gama de servicios y productos que varían de un mercado a otros, incluyendo servicios de voz móvil, servicios de datos móviles, servicios de valor agregado, servicios de voz fija, servicio de datos fijos, servicios de acceso a Internet en banda ancha, servicios de IT, servicios de televisión de paga, servicios de venta en contenido y otros servicios relacionados.

El propósito de la compañía consiste en ofrecer el mejor servicio de atención a clientes. Para ello, América Móvil cuenta con 120,000 empleados, aproximadamente, que se dedican a estas funciones y se empeñan en mejorar constantemente la experiencia de sus clientes tanto a través de sus servicios y productos como de sus redes de ventas y distribución.

Al 31 de marzo de 2022, la compañía contaba con 422 millones de líneas de acceso, que incluyen 307.4 millones de suscriptores móviles y 124.4 millones de unidades generadoras de ingreso fijas (telefonía fija, banda ancha y televisión de paga).

Claro Perú es subsidiaria de América Móvil, S.A.B. de C.V. y opera en el país desde el 10 de agosto de 2005.

Somos una empresa de comunicación, información y entretenimiento.

La experiencia latinoamericana ha permitido posicionarse actualmente como una de las compañías líderes en el sector telecomunicaciones en Perú.

Desde el inicio de nuestras operaciones en el país, nuestro principal compromiso es ofrecer una red de alta calidad y amplia cobertura en los 24 departamentos del Perú, para generar oportunidades de crecimiento a través de los servicios de telecomunicaciones que ofrecemos.

Contamos con un sólido programa de inversiones orientado al despliegue sostenible de infraestructura de telecomunicaciones, mejorar nuestros sistemas de atención, desarrollar medios digitales de auto atención y compra, y la permanente actualización tecnológica para potenciar nuestra red 4.5G. Asimismo, nos enfocamos en ampliar el alcance de las conexiones de fibra disponibles en nuestros sitios móviles que nos permitirán continuar aportando al desarrollo del país, promoviendo la inclusión digital de cada vez más peruanos.

2.2 Nuestra Visión.

Ser la empresa líder en telecomunicaciones en el Perú.

2.3 Nuestra Misión.

Brindar servicios de telecomunicaciones de alta calidad, crecer y ampliar la cobertura de los servicios, siendo constantes en innovación para anticiparnos a las necesidades de comunicación de nuestros clientes; generar el mayor bienestar y desarrollo personal y profesional de nuestros trabajadores, proporcionar bienestar y desarrollo a la comunidad y exceder los objetivos financieros y de crecimiento de nuestros accionistas.

2.4 Organización de la empresa

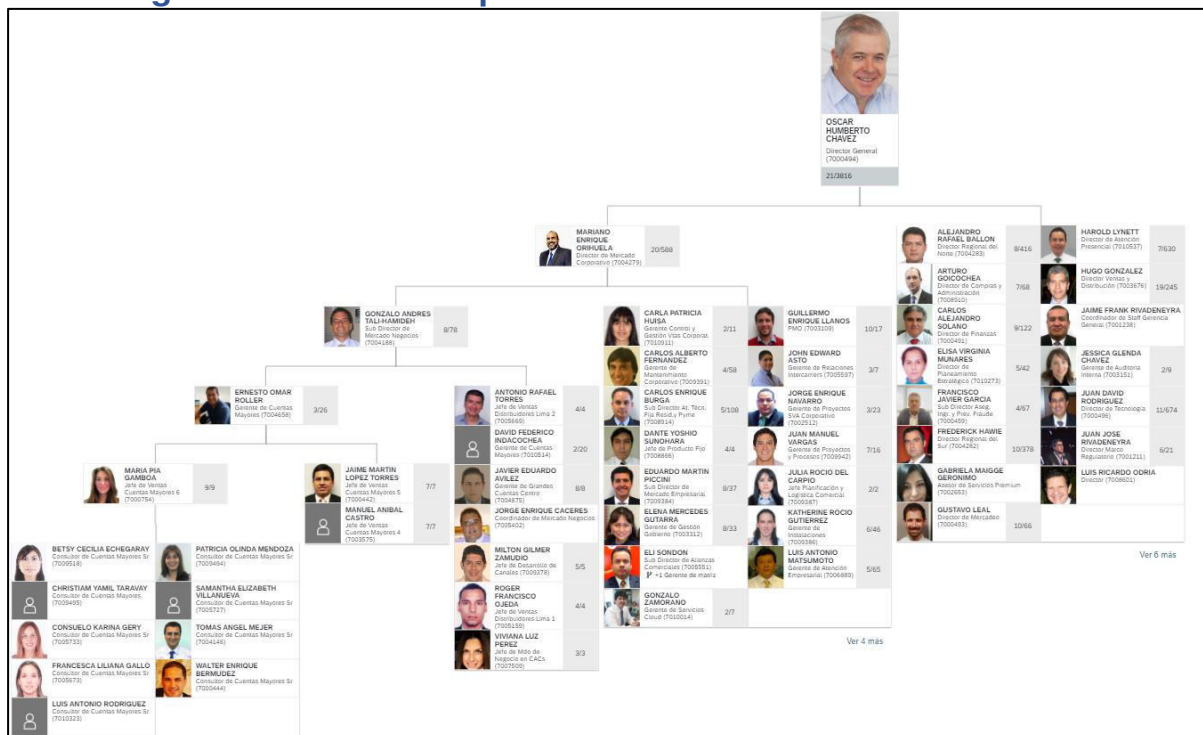


Ilustración 1 Organigrama de la Empresa

Fuente: Success Factor Claro Perú

2.5 Área, cargo y funciones desempeñadas

Mi experiencia profesional tiene mayor énfasis en el desarrollo e implementación de proyectos, en Claro Perú pude explotar los 3 años de experiencia adquirida en años anteriores y me posicionó en los proyectos principales en el sector de Grandes Empresa, mi trabajo durante los primeros años en Claro Perú, como Ingeniero de Preventa, impactaba directamente en el diseño de soluciones y participaba en la venta técnica final.

Los proyectos en los que participaba generaban ingresos a la empresa con facturaciones de hasta S/40,000.00 mensuales, estas participaciones significaron la oportunidad de desempeñarme directamente con una cartera de clientes, me brindaron un cargo de Consultor de Cuentas Mayores Senior para poder realizar el levantamiento de información, dimensionamiento, presentación de propuestas y cierres de proyectos.

2.6 Experiencia Profesional realizada en la organización

Mi experiencia en Claro Perú fue de las mejores, me permitió crecer profesionalmente y

aprender y aplicar mis conocimientos de todos los flancos de las tecnologías de la información y comunicaciones, desde networking, seguridad perimetral, hasta comunicaciones unificadas, data center y cloud solutions.

Mi primera posición inició como Ingeniero de Preventa, como indiqué en el punto anterior, esta disposición de trabajo me permitió ascender rápidamente a la posición de Consultor de Cuentas Mayores Senior, actualmente me vengo desempeñando más de 2 años en el cargo y me ha permitido participar de proyectos directamente involucrados en los desarrollos tecnológicos de muchas empresas, más aún en los tiempos de pandemia, que significó un reto de los tipos de planteamientos y soluciones integradas que podríamos brindar.

A la fecha me mantengo en la posición generando mensualmente ingresos importantes a la empresa y los proyectos de integración como el que presentamos en este Trabajo de Suficiencia Profesional son parte del desarrollo e implementaciones mensuales en los cuales puedo participar.

Particularmente para motivos del informe presente el trabajo se desarrolla en el Área de Ventas Cuentas Mayores (VCM) para una empresa Minera con presencia Nacional, donde participo en todo el procedimiento desde contacto, levantamiento de información, diseño de solución, planteamiento de propuesta e implementación, bajo el liderazgo de mi Jefatura – María Pia Gamboa Cavenecia, con correo: mgamboa@claro.com.pe. El proyecto tuvo una duración aproximada de 13 meses entre procesos de estudios de factibilidad el 11 de Noviembre de 2019 hasta la instalación y configuración integral de la solución final el 8 Junio de 2021, considerando también que parte del proceso de instalación y contactos se dieron con el inicio de la pandemia, con el alcance de mis funciones se deja detallado que los trabajos fueron llevados desde las oficinas principales de América Móvil Perú SAC: Av. Nicolás Arriola 480 – La Victoria – Lima – Lima. Cod. Postal: 15034.

CAPITULO III: ACTIVIDADES DESARROLLADAS

En este capítulo se presenta la Determinación del Problema, los objetivos generales y específicos, el alcance y los fundamentos teóricos necesarios para el trabajo de investigación. Seguidamente se muestra el desarrollo de cada fase de la aplicación de la metodología.

3.1 Situación del Problema

Se realizó una auditoría interna en la empresa minera donde identificaron problemas para comunicarse entre sedes remotas debido a los anchos de banda brindados por su proveedor de telecomunicaciones que no permiten desempeñar funciones corporativas de seguridad, comunicación entre los campamentos mineros y la sede central de manera óptima ni desarrollar proyectos de migración a la nube.

3.2 Determinación del Problema

3.2.1 Formulación del Problema

3.2.1.1 Problema General

- a) ¿Cómo podemos Optimizar el sistema de interconexión, seguridad perimetral y de comunicación entre sedes de la empresa minera?

3.2.1.2 Problemas Específicos

- b) ¿Cómo obtener la información de la situación actual de la empresa en torno a las comunicaciones con las sedes remotas?
- c) ¿Se pueden mejorar los anchos de banda de los enlaces satelitales?
- d) ¿Cómo mejorar el sistema de comunicación actual y accesos a servidores locales en las sedes unidades mineras?
- e) ¿Cómo medir el impacto al realizar la optimización de los sistemas de comunicaciones?

3.3 Solución

3.3.1 Objetivos

3.3.1.1 Objetivo General

Optimizar el sistema de interconexión, seguridad perimetral y de comunicación entre sedes de empresa minera con migración de tecnología MPLS a IP sobre enlaces dedicados de internet.

3.3.1.2 Objetivos Específicos

Analizar la situación actual del cliente según a los anchos de banda que poseen en las sedes remotas.

Plantear soluciones y mejoras para los enlaces satelitales actuales.

Diseñar e implementar una solución integral de comunicación para las sedes productivas y administrativas de cliente minero con migración de soluciones de tecnología MPLS a IP sobre enlaces dedicados de internet.

Evaluar el impacto de la optimización en la comunicación de las áreas productivas en los campamentos mineros.

3.3.2 Alcance

El presente trabajo brinda información sobre el proceso de optimización del sistema de comunicaciones integral de una empresa minera, considerando en todo momento el resguardo de la información, mejora en las comunicaciones empresariales, accesos a servidores y tiempos de respuesta de información de las unidades mineras ubicadas en las provincias de Cusco y Arequipa para con la sede principal en Lima.

El proyecto no solo busca el desarrollo y mejora de la situación actual, sino también tener un sistema que permita realizar optimización de costos con futuras migraciones a la nube y optimizaciones de comunicación a través de VoWifi o nuevas tecnologías.

3.3.3 Etapas y Metodología

El proyecto tiene un flujo de trabajo trazado por Claro Perú, que marca lineamientos para la atención de un cliente corporativo, estos se dividen en 4 etapas que enmarcaran el desarrollo total del proyecto:

3.3.3.1 Levantamiento de información.

Es la etapa en la cual se detecta la necesidad del cliente sobre los sistemas de comunicaciones actuales. Es prioritario realizar un correcto levantamiento de información para poder orientar específicamente las soluciones necesarias de cliente.

3.3.3.2 Diseño de la solución.

Preparación de una propuesta de diseño con alternativas tecnológicas que buscan cubrir todas las necesidades de comunicaciones de cliente.

3.3.3.3 Presentación a cliente.

Posterior a realizar la propuesta y diseño de solución, se realiza una presentación de puntos a favor de la alternativa planteada, comparándola con los alcances antiguos que se cubrían.

3.3.3.4 Aceptación e implementación del proyecto.

Luego de la presentación de cliente, y en caso no existan modificaciones o detalles para tener en cuenta, el cliente acepta los alcances y nos brinda la buena pro de ejecución del proyecto, generamos ordenes de trabajo y se empiezan los trabajos para realizar la implementación.

3.3.4 Levantamiento e Implementación

Estas etapas son con las que se desarrollará la presentación del proyecto en el Trabajo de Suficiencia Profesional:

3.3.4.1 Fase de Análisis

i. Levantamiento de información:

En esta etapa posterior a la auditoría realizada por el cliente, Claro Perú realiza una visita

para el levantamiento de información de los requerimientos del cliente.

En esta etapa encontramos los requerimientos generales que necesita la empresa minera para mejorar operaciones y la situación actual, de esto determinamos lo siguiente:

- a) Mejora de enlaces satelitales presentes en las unidades mineras (U.M) de Suyckutambo (Cusco) y El Santo (Arequipa) que cuenta capacidades asimétricas de 4Mbps/2Mbps en ambas sedes.
- b) Esquema de MPLS centralizado a una sede principal Lima, con salida independiente.
- c) Mejora de enlaces de fibra óptica dedicada en la sede principal de Lima que cuenta con una capacidad de 20 Mbps 1:1.
- d) Optimización de la comunicación y acceso a servidores, considerando la seguridad de la información de la empresa, actualmente con presencia de lentitud de acceso desde las unidades mineras a los servidores en Lima, generando mayor gasto de horas hombre y tiempo de respuesta de solicitudes.
- e) Mantener el esquema de seguridad perimetral y políticas que mantiene un escenario de Firewall centralizado y extensión de políticas a través de MPLS privada de la empresa.
- f) Optimización del sistema de telefonía, actualmente establecido con líneas analógicas remotas, que no permite comunicación entre anexos de diferentes sedes.
- g) Cantidad de usuarios por sede es la siguiente:

Tabla 1 Distribución de usuarios por sede

CANTIDAD DE USUARIOS	
PRINCIPAL	80 Usuarios administrativos
SUYCKUTAMBO	30 Usuarios administrativos y entre 120 a 200 operarios
EL SANTO	20 Usuarios administrativos y 80 a 120 operarios

- h) Mejora de costos actuales para la empresa, en las soluciones de T.I, que gestiona un presupuesto aproximado de S/350,000 anuales.
- i) Tenemos como resultado el acceso a la información del escenario actual de los puntos clave:

Tabla 2 Escenario actual de cliente

ESCENARIO ACTUAL	
Conectividad	Red Privada Virtual Centralizada con BW limitados
Seguridad	Equipo de seguridad antiguo. Sin licenciamiento vigente ni soporte
Telefonía	Equipos telefónicos analógicos.

Dentro del análisis de esta etapa es necesario realizar acotaciones importantes para considerar que el levantamiento de información ha sido correcto, más allá de los puntos clave, que son los requerimientos del cliente, hay consideraciones importantes que nos permitirán realizar el correcto diseño del proyecto. Estas son siempre considerables, más aún en proyectos de alta relevancia:

- a) Puntos de energía habilitados y brindados por cliente para equipos.
- b) Espacio en gabinetes para equipos.
- c) Puntos y puertos de red disponibles en switches de cliente.
- d) De este modo podemos tener un alcance más real a los que se puede establecer en la etapa de diseño como una solución correctamente dimensionada.

ii. Diseño de solución

Para establecer un diseño de solución según las necesidades del cliente, se tienen en cuenta los factores principales de mejora que necesitan. Estos, según el levantamiento de información nos permiten realizar los siguientes estudios para validar factibilidad en zonas:

ii.i. Análisis de situación actual

Con los requerimientos validados en torno a los recursos que solicita el cliente se plantean las siguientes soluciones:

- a) Mantener el escenario centralizado de Red Privada Virtual, donde se tiene la topología que mantiene una salida principal de internet y acceso a servidores.
- b) Migrar los enlaces de datos hacia enlaces de internet independiente sin centralización.

Se analizan los puntos a favor y en contra de cada sede que necesita conectividad:

Tabla 3 Análisis de Ventajas y Desventajas de Soluciones

	Solución Integral con Enlaces de Datos por RPV	Solución Integral con Enlaces de Internet
Ventajas	Acceso a servidores de Lima a través MPLS. Tiempo de respuesta más rápido.	Accesos a Internet independiente en cada sede (Principal y Unidades Mineras)
	Mantiene la solución de telefonía analógica, no existe recableado	Costos más económicos
	Comunicación de Voz centralizada. Central Telefónica en la sede principal	Mejor garantía de accesos a plataformas en la nube
	Políticas de Seguridad centralizadas asignadas desde la sede principal.	Comunicación de voz puede ser independiente. Cada sede con una centralita
		Cada sede debería contar con un Firewall independiente con gestión desde plataforma de UTM
Desventajas	Solución actualizada podría contar con calidad de servicio (QoS)	Solución no garantiza QoS
	Navegación a internet limitada por capacidad de BW satelital	
	Salida de internet Centralizada en Lima	
	Costos elevados	
	Demora y lentitud en accesos a plataformas en la nube	

Teniendo en cuenta la tabla anterior, en base a experiencia de usuario y posibilidad de accesos a la nube y salida directa de internet a usuarios en las unidades mineras, se opta trabajar la solución con Internet en cada punto.

Se realizan estudios de Factibilidad para validar recursos y posibilidad de atención con Fibra Óptica o Microondas, en Lima y Unidades Mineras.

Se crean proyectos en las ubicaciones de sedes correspondientes con los siguientes alcances:

Tabla 4 Proyectos derivados a análisis de factibilidad

SEDE	DIRECCION	BW
Sede Principal	Av. Alfredo Benavides Nro. 1555 Int. 403 Lima - Lima - Miraflores	50 MB
Sede El Santo	Nro. S/N Fnd. Tayayaque Trinidad Quespemachay Arequipa - Caylloma - Caylloma	12 MB
Sede Suyckutambo	Nro. Sector Puca Poca (C.C. Ichoccollo) Cusco - Espinar - Suyckutambo	12 MB

Lo que se busca con estos proyectos es tener alcance si en los puntos mencionados Claro cuenta con facilidades técnicas en torno a planta externa y capacidad solicitada.

El estudio de factibilidad nos muestra resultados para poder escoger el medio de transmisión que pueda aprovisionar en los puntos indicados, estos según resultados pueden ser: Fibra Óptica, Microondas o Enlace Satelital.

El estudio de factibilidad en primera instancia puede realizarse en Gabinete, precisando que no todo estudio en gabinete puede ser implementado pues existen diversas casuísticas en sitio que pueden llevar a realizar cambios en las implementaciones.

Estos estudios permiten tener el alcance de costo (CAPEX) de inversión que se trasladaría al proyecto.

Para estos casos particularmente, se realizaron los siguientes análisis.

Tabla 5 Tipo de estudio por sede de cliente

SEDE	DIRECCION	BW	TIPO DE ESTUDIO
Sede Principal	Av. Alfredo Benavides Nro. 1555 Int. 403 Lima - Lima - Miraflores	50 MB	Estudio en Gabinete
Sede El Santo	Nro. S/N Fnd. Tayayaque Trinidad Quespemachay Arequipa - Caylloma - Caylloma	12 MB	Estudio de Campo TSS
Sede Suyckutambo	Nro. Sector Puca Poca (C.C. Ichoccollo) Cusco - Espinar - Suyckutambo	12 MB	Estudio de Campo

Los estudios de campo nos dieron como resultados los siguientes alcances para dimensionamiento e implementación.

ii.ii. Estudio en Gabinete de Sede Principal

Siguiendo el orden de validación de aprovisionamientos, la primera opción de infraestructura es validar un despliegue de fibra óptica.

Para el caso de la sede Principal, la ubicación geográfica es en Lima, para mayor especificación en el distrito de Miraflores, adicionalmente a la especificación de las tareas, se muestran las imágenes de las asignaciones y recursos asignados a nivel de software interno en el ANEXO 6.1. ESTUDIO DE FACTIBILIDAD EN GABINETE PARA SEDE LIMA.

- a) En estos casos los análisis en gabinete son 95% confiables para despliegues, en la mayoría de los casos en Lima se obtiene el 100% según la zona; en este caso la ubicación es un edificio y zona empresarial, por lo cual podemos estar seguros de trabajar con este tipo de análisis.

Los alcances del estudio en gabinete destacan los análisis siguientes:

- b) Ruta desde MUFA y canalizado existente hasta ingreso.
- c) Se realizar validación de POP que aprovisiona MUFA, se verifica estado de puertos disponibles:
- d) Se generan reservas provisionales y preconfiguración, actualizando estado de puertos asignados vigentes.
- e) Se realiza reserva de recursos físicos em MUFA de análisis.

ii.iii. Estudio de Campo TSS en Sede El Santo.

El orden de realización es validar en primer lugar si se puede realizar un despliegue de fibra óptica.

Debido a las condiciones geográficas y de ubicación, en el estudio de gabinete se determinó que el medio de aprovisionamiento puede ser Microondas o Satelital, el detalle sobre el estudio en gabinete y cálculos sobre software se encuentran en el ANEXO 6.2. ESTUDIO DE FACTIBILIDAD EN GABINETE PARA U.M EL SANTO, donde se verá la vista geográfica y perfil de elevación en unos diversos enfoques según la siguiente descripción:

- a) Primer enfoque: Se analizó en gabinete la posibilidad de realizar la instalación por medio de Microondas. Se realizaron estudios de perfil de elevación para validar línea de vista.
- b) Segundo enfoque: En este primer estudio de perfil se comprobó que existe impedimento geográfico para llegar al campamento, se analizó la posibilidad de instalar una torre de 30 metros considerado una inviabilidad por costos de implementación. Durante el estudio se determinó existencia de una antena a 720 metros del campamento que es propiedad de cliente.
- c) Tercer enfoque: Se realizó un segundo análisis utilizando las coordenadas de la ubicación de la antena existente y se realizó el estudio de perfil de elevación, como resultado se encuentra viable la posibilidad de realizar la instalación de equipos y realizar un salto adicional para llegar al Campamento.

Como procedimiento adicional se valida perfil de elevación adecuado desde repetidora de empresa minera hacia el campamento Minero.

Con este procedimiento en gabinete aprobado, se realiza gestión de visita de campo para realizar las validaciones complementarias a la adecuación de servicio. En esta visita se determina lo siguiente:

- a) Se utilizará torre repetidora de cliente para realizar la instalación de antena

microondas de las siguientes características.

Tabla 6 Equipamiento radio - Site Caylloma

SITE:AR3991_CAYLLOMA			
EQUIPO/MATERIAL A INSTALAR	DIMENSIONES	PESO	CONSUMO DE ENERGIA DC (Watts)
RADIO: IP-20S, ETSI, No MIMO support, 23GHz-TX high	(H)230mm x (W)233mm x (D)98mm	6 kg	35Watts
Antena: 23GHz, Crgn &Std UBR220 Int -RFS	Diámetro: 0.3 m	7 kg	-
Soporte de Antena Tipo pata de gallo	Dimensión: 80 cm	10 kg	-
Uso de 1 Breaker DC			
		PESO EN TORRE: 23 KG MAX	CONSUMO TOTAL: 35 Watts

Tabla 7 Equipamiento radio - Site Repetidora cliente

SITE: REPETIDORA U.M			
EQUIPO/MATERIAL A INSTALAR	DIMENSIONES	PESO	CONSUMO DE ENERGIA DC (Watts)
2 RADIO: IP-20S, ETSI, No MIMO support, 23GHz-TX high	(H)230mm x (W)233mm x (D)98mm	12 kg	70Watts
Antena: 23GHz, Crgn &Std UBR220 Int -RFS	Diámetro: 0.3 m	14 kg	-
Soporte de Antena Tipo pata de gallo	Dimensión: 80 cm	20 kg	-
Uso de 1 Breaker DC			
		PESO EN TORRE: 46 KG MAX	CONSUMO TOTAL: 35 Watts

...

Tabla 8 Equipamiento radio - Site cliente U.M El Santo

SITE: LADO CLIENTE U.M EL SANTO			
EQUIPO/MATERIAL A INSTALAR	DIMENSIONES	PESO	CONSUMO DE ENERGIA DC (Watts)
RADIO: IP-20S, ETSI, No MIMO support, 23GHz-TX high	(H)230mm x (W)233mm x (D)98mm	6 kg	35Watts
Antena: 23GHz, Crgn &Std UBR220 Int -RFS	Diámetro: 0.3 m	7 kg	-
Soporte de Antena Tipo pata de gallo	Dimensión: 80 cm	10 kg	-
Uso de 1 Breaker DC			
		PESO EN TORRE: 23KG MAX	CONSUMO TOTAL: 35 Watts

...

b) Se realiza validación de energía en puertos eléctricos en site,



Ilustración 2 Validación de energía en Site Caylloma

Fuente: Informe TSS

- c) En lado de cliente se valida energía disponible y pozo a tierra por lo cual es viable la instalación de antena de recepción en U.M y Router.

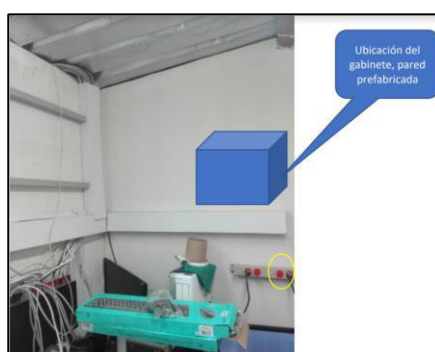


Ilustración 3 Validación de energía en cliente

Fuente: Informe TSS

- d) Se valida así mismo espacio para mástil, ubicación e ingresos para equipamiento de microondas.

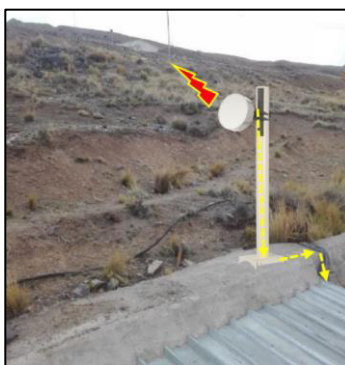


Ilustración 4 Análisis de ubicación de antena e U.M El Santo

Fuente: Informe TSS

- e) En la torre repetidora el cliente se encargará de realizar un tendido eléctrico desde el campamento, proyecto que ejecutará en 1 a 2 años, por lo cual se realiza un análisis económico de implementación de energía solar.
- f) Se analiza consumo de energía solar según consumo total de tabla – 70 Watts.

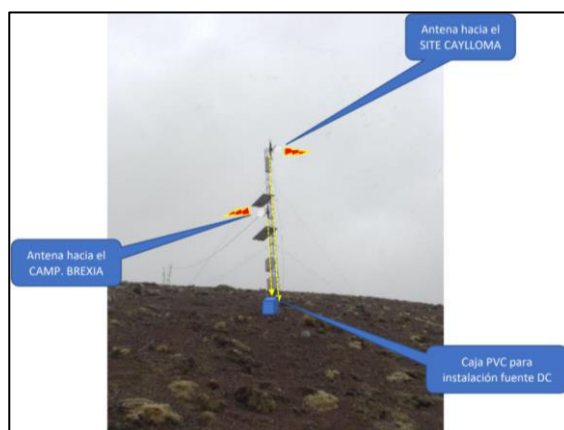


Ilustración 5 TSS de ubicación de equipamiento en Repetidora de cliente

Fuente: Informe TSS

La infraestructura de red dispondrá de lo siguiente según lo indicado en el cuadro 1, 2 y 3:

- a) En Site de aprovisionamiento: 1 Equipo de Radio (IDU – ODU) + Antena + Kit de montaje.
- b) En Repetidora de Mina: 2 Equipo de Radio (IDU – ODU) + 2 Antena + 2 Kit de montaje + abastecimiento de energía solar
- c) En Unidad Minera: 1 Equipo de Radio (IDU – ODU) + Antena + Kit de montaje.
- d) En la Unidad Minera: 1 Router para conectividad hacia internet y cableado de fibra desde Radio a CPE.

ii.iv. Estudio de Campo de Sede Suykutambo.

Para el análisis de servicio Satelital, trabajamos con un socio estratégico llamado SpeedCast, con quien se realizan proyectos mineros y de toda índole interna a nivel de toda Latinoamérica.

Para nuestro territorio y nuestros proyectos, se opera bajo las redes satelitales NSS10 en banda C, Anik Fly Satmex 7 en banda KU con una buena cobertura, permitiendo que las estaciones remotas VSAT reciban eficientemente la señal emitida con antenas desde 1,2 metros, 1,8 metros y 2.4 metros.

Para este escenario se realiza una validación de las coordenadas de ubicación del campamento minero y validación de ubicación contra satélite.

a) U.M Suyckutambo:

b) 15°4'8.35" Latitud Sur - 71°44'55" Longitud Oeste

c) Datos de Instalación:

Tabla 9 Descripción de equipamiento necesario para instalación

ITEM	DESCRIPCION	SI/NO	CANTIDAD
1	Antena 2.4	SI	1
2	Pozo a tierra	SI	1
3	Pararrayos	SI	1
4	Losa de concreto	NO	0

d) Datos Técnicos:

Tabla 10 Detalles técnicos para instalación

Satélite	IS14
Localización	45.W°
Azímüt	62.5°
Elevación	54.5°
Operadores Celulares en la zona	FUERA DE COBERTURA

Se ejecuta un planeamiento de aplazamiento para validar en sitio un TSS a nivel satelital de ubicación y un prediseño de ubicación:

a) Plano de Aplazamiento



Ilustración 6 Revisión de aplazamiento

Fuente: Informe TSS

Visión y elevación de aplazamiento, se realiza un montaje de ubicación satelital con direccionamiento al satélite. Se plantean dos opciones:

- b) La loza de concreto debe ser construida 1 metro por encima del nivel donde se encuentra actualmente (línea azul) para ganar mayor altura. Esta loza debe ir a 10m de distancia hacia atrás de la loza existente.

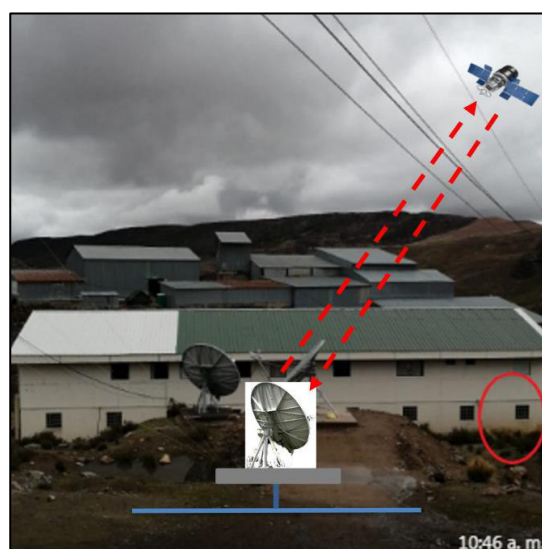


Ilustración 7 Primer análisis para ubicación de antena

Fuente: Informe TSS

- c) Cliente debe rellenar el espacio hueco para nivelar, hasta llegar a 1 m por encima del actual de referencia que es la línea azul

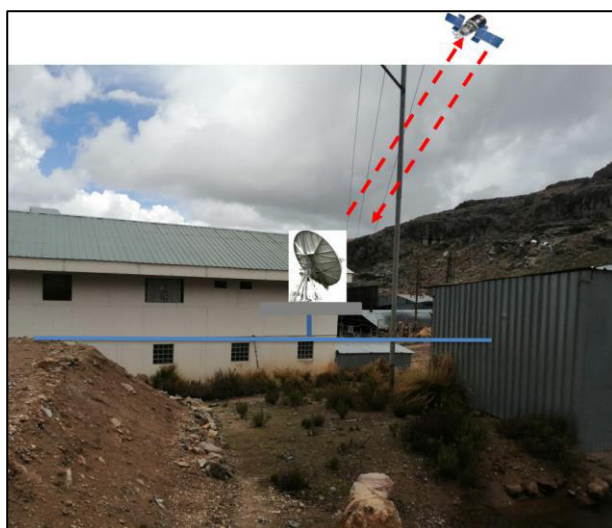


Ilustración 8 Segundo análisis de ubicación de Antena

Fuente: Informe TSS

Como resultado se valida que hay vista libre para INTELSAT 14 y para el satélite GALAXY 28 (G28), donde se consideran las siguientes validaciones adicionales

- a) Por lugar de ubicación

Tabla 11 Revisión de ubicación de antena

Elevación sobre el nivel del mar	4384.1 msnm
¿Existe alguna edificación que obstaculice la visión de la antena? (¿Cuál es la solución?)	No
¿Se podría mover algún objeto para mejorar la visión?	No

- b) Por Tipo de montaje:

Tabla 12 Tabla de equipamiento y montaje

Tipo de Montaje (Tejado superficial, Suelo superficial, Suelo con mástil o trípode, Pared, otros): Suelo con trípode
Consideraciones especiales para el montaje: Al finalizar el montaje de la antena, se deberá sellar con silicona para evitar que el agua filtre el techo. Composición de la superficie (concreto, asfalto, tierra). Loza de Cemento
¿Se requiere enrejado? No, el área donde se situará la antena no tiene tránsito peatonal
¿Se requiere Obra civil (Losa)? SI
Tamaño de antena: 2.4 mt
¿Se requiere algún tipo de permiso para instalar la antena? La coordinación con el ingeniero responsable de la sede.

¿Se requiere, escaleras, grúas u otros medios para acceso y montaje? **Escalera, para fijar el tubo por donde baja el cable Coaxial**

c) Validación de energía con el siguiente reporte:

Tabla 13 Revisión de energía y puesta a tierra

CA Monofásica/trifásica	MONOFASICO CA
Potencia mínima requerida por el equipamiento	Monofásica 24Watts
¿Existen tomas de CA próximas al equipo?	SI
¿Se dispone de energía estabilizada?	SI
¿Se dispone de energía comercial 220V?	SI
Distancia de Punto de Energía hasta Gabinete de Datos	Existe energía dentro del Gabinete
¿Existe pozo de puesta a tierra dedicado al pararrayos? (Medidas)	SI
¿Existe protección contra rayos?	SI
¿Se encuentra la instalación bajo su cobertura?	NO

ii.v. Análisis de equipamientos que son necesarios utilizar para cumplir los alcances de BW

Los equipos se dimensionan, según los BW y/o soluciones añadidas que utilizan el medio de Fibra como transporte, ejemplo: Habilitar una troncal SIP adicional al servicio de Internet.

Según los BW dimensionados corresponde colocar equipos homologados por Claro que nos permitan brindar estos servicios y en las ubicaciones de cliente.

Para este caso los análisis nos llevan a revisar que puedan soportar la presión y la temperatura en los campamentos mineros. Para este alcance se revisan los datasheets y tenemos el siguiente listado de equipos Enrutadores para habilitación de servicios:

a) La sede Lima por solicitud de cliente debe tener una Troncal SIP habilitada, por lo que la solución nos lleva a definir en este punto los siguientes equipos.

Tabla 14 Definición de equipamiento

SEDE	DIRECCION	BW	Router
Sede Principal	Av. Alfredo Benavides Nro. 1555 Int. 403 Lima - Lima - Miraflores	50 MB	CISCO ISRC 1111-4P
Sede El Santo	Nro. S/N Fnd. Tayayaque Trinidad Qquespemachay Arequipa - Caylloma - Caylloma	14 MB	HUAWEI AR651C

Sede Suyckutambo	Nro. Sector Puca Puca (C.C. Ichoccollo) Cusco - Espinar - Suyckutambo	12 MB	MODEM
-----------------------------	--	-------	-------

Respecto a las soluciones solicitadas de Internet, se realiza un planteamiento para gestionar las políticas de seguridad perimetral y reglas de gestión actual.

- a) Se realiza un análisis del sistema de seguridad actual, como resultado de las validaciones se tiene un Firewall FortiGate FG-90D con licenciamiento vencido.
- b) Las políticas establecidas en el sistema no replicaron de manera correcta, se realizó un análisis del equipo y se verificó que, debido a la falta de licenciamiento, las características del equipo no respondían de manera correcta. Se indicó y dio detalle de las características en ese momento.

Respecto a las características de seguridad necesarias para despliegue, responsable de TI nos indicó lo siguiente:

- a) Gestión del equipo, posibilidad de administrar o habilitar políticas.
- b) Mejorar condicionamiento de SPAM en correos, considerando migración futura a plataforma cloud de office 365, es decir se cambiaría el servidor local que tienen por la nube.
- c) Habilitar restricciones de acceso para usuarios por bloques, gestionar los BW.
- d) Utilizar VPN para trabajo remoto.
- e) Proteger de phishing, Spoofing y ramsonware, amenazas avanzadas, APT (Amenazas persistentes avanzadas), ataque de día cero, denegación de servicios que ya se presentaron en los últimos meses.

Con las características descritas anteriormente se plantean tres soluciones comparables en

capa 7 de protección en el mercado y con las que se tiene homologación:

Tabla 15 Comparativo de 3 marcas para la solución

Funcionalidades	Sonicwall	Fortinet	Palo Alto
Firewall (FW)	ok	ok	ok
Antivirus (AV)	ok	ok	ok
AntiSpam (AS), SMTP, IMAP, POP3. (No es reemplazo de un antispam dedicado)	ok	ok	No incluye Antispam.
IPS (Sistema de Prevención de Intrusos)	ok	ok	ok
Filtro Web (WEB)	ok	ok	ok
Traffic Shaping (Función Limitar el tráfico). Su uso implica generar lentitud sobre el tráfico limitado. No se recomienda su uso.	ok	ok	ok
Control de Aplicaciones	ok	ok	ok
Inspección de Tráfico SSL	ok	ok	ok
Data Leakage Prevention (DLP)	ok	ok	ok
Sandboxing (SB) Permite la detección de malware avanzado (APT – Advanced persistent threats) y amenazas de día cero.	ok	Requiere de FortiSanbox. (no está incluido en EL SERVICIO, se debe considerar como adicional)	Requiere de suscripción WildFire. (no está incluido en EL SERVICIO, se debe considerar como adicional)
Balanceo de Carga (Balanceo de tráfico basado en un criterio L4/L3, con funciones básicas del tipo PBR)	ok	ok	ok
SSL o IPSEC VPN	Requiere de una suscripción para VPN Client to Site SSL o IPSEC	ok	Requiere de suscripción Global Protect si para usar en Smartphone (tiene un costo adicional, no incluido en EL SERVICIO). Para usar en laptop/pc o terminal de trabajo no requiere suscripción (no tiene costo adicional)

Teniendo el valor y experiencia de usuario se plantea utilizar FortiGate, utilizamos también una relación de producto homologado con la marca Fortinet para determinar equipo ideal a utilizar según condiciones, BW y usuarios, determinando la siguiente distribución.

Tabla 16 Elección de equipamiento para seguridad

SEDE	DIRECCION	BW	Cantidad de Usuarios	Equipo
Sede Principal	Av. Alfredo Benavides Nro. 1555 Int. 403 Lima - Lima – Miraflores	50 MB	100	FortiGate60E

Sede El Santo	Nro. S/N Fnd. Tayayaque Trinidad Quespemachay Arequipa - Caylloma - Caylloma	14 MB	200	FortiGate80E
Sede Suyckutambo	Nro. Sector Puca Puca (C.C. Ichoccollo) Cusco - Espinar - Suyckutambo	12 MB	300	FortiGate80E

Dentro de los servicios adicionales se solicitó la mejora de la solución actual de telefonía, la cual se constató que contaban con una centralita analógica en cada unidad minera y en la sede principal.

La solución actual mantiene una línea analógica habilitada en Lima y replicada a través de una MPLS donde se configuran los anexos extendidos contra las centralitas.

Planteamos migrar el escenario actual a una solución IP por completo, por la necesidad de crecimiento y la forma de comunicación solicitada (Internet en cada sede) se necesita una configuración a nivel IP.

De esta forma dimensionamos una solución de telefonía IP con centrales independientes en cada punto, con una distribución de anexos solicitada.

3.3.4.2 Fase de Definición

Dentro de los dimensionamientos proyectados de los levantamientos y visitas se realizaron validaciones para poder asociar todas a una presentación que definía por completo nuestra solución ofertada. Esta presentación tiene los siguientes alcances:

3.3.4.2.1 Conectividad:

a) Enlace Sede Principal

- Enlace dedicado de Fibra Óptica con el B W al 100% Overbooking 1:1, simétrico.
- Se entregan pool de 8 IPs (5 utilizables para el cliente para usos que configure)

b) Enlace Arequipa – El Santo

- Enlace vía microondas desde el POP BASE Caylloma, hacia sede cliente. El enlace habilitará 12 MB. Desde la ubicación de la antena y se realizará la implementación un enlace de repetidora con equipamiento de las mismas características en ambos extremos.
- El aprovisionamiento de la energía debe brindarse por el cliente. La energía que necesita el equipo de radio comunicación es el siguiente. CONSUMO TOTAL: 35 Watts. Por bloque de equipos (IDU, ODU, CPE)
- Enlace dedicado de Microondas con el B W al 100%. Overbooking 1:1, simétrico.
- Se entregan pool de 8 IPs (5 utilizables para el cliente para usos que configure)

c) **Enlace Cuzco – Suyckutambo**

- Enlace Satelital, brindado en banda C, 70% Garantizado de B W. Enlace de Down link de 12 MB / 4 MB de uplink, se optimiza sobre calidad de servicio.
- La disponibilidad de Backbone es de 99.6% mensual sobre core de Claro.
- Telepuerto ubicado en la Ciudad de Lima, Operación 7 d x 24 h x.365 días.
- Para el servicio Satelital Internet LITE, se considera el siguiente equipamiento satelital: Antena 2.4 m, BUC y LNB, Modem iDirect, como equipos optimizados.
- Solución no contempla la instalación de Equipo Anti-ICE, este alcance se define porque no existen temperaturas que afecten los equipos ya homologados para las temperaturas de la zona, se colocan los correctos y necesarios para la solución.

3.3.4.2.2 Seguridad y Telefonía

- a) Para la solución de Seguridad Perimetral y telefonía, se buscó la alternativa que unifique ambas soluciones, la comunicación entre sedes, accesos a servidores y

anexos extendidos.

- b) Como propuesta de solución. Colocamos la opción de 2 equipos de Seguridad Administrada FortiGate-80E (Recomendado por las características) para las sedes El Santo y Suyckutambo y un equipo de Seguridad Administrada FortiGate-80E.
- c) La solución de seguridad es necesaria para mantener el escenario actual de telefonía. Esto debido a que se planteó la interconexión a través de VPNs que se realizaría entre sedes y centrales telefónicas de voz, como se mostrará en la topología en capítulos siguientes.
- d) La propuesta de servicio englobará conectividad de sedes, solución de telefonía sobre una solución gestionada por varios Gateway conversores y Firewalls como equipos de seguridad perimetral, esto va orientado a mantener el escenario de voz que tiene el cliente y mejorando las plataformas de Internet que tendría el cliente una vez finalizado el proyecto
- e) Se plantea la mejora de la plataforma de seguridad, cada sede tendrá su propio firewall y a la vez funcionarán como uno solo por la característica de Security Fabric, esto será visible a través de un solo Dashboard donde se podrán ver los 3 equipos de seguridad y mejorar las plataformas de servicio para aplicación de políticas y administración de redes.
- f) Esta es una solución mejorada respecto a colocar solo firewalls de voz, como se manejaba previo al proyecto, ya que la conexión a través de interconexión con gateway de voz analógicos está limitada al alcance de cantidades y despliegue de funcionalidades.

b) Diseño de solución considerando las plataformas de voz y seguridad

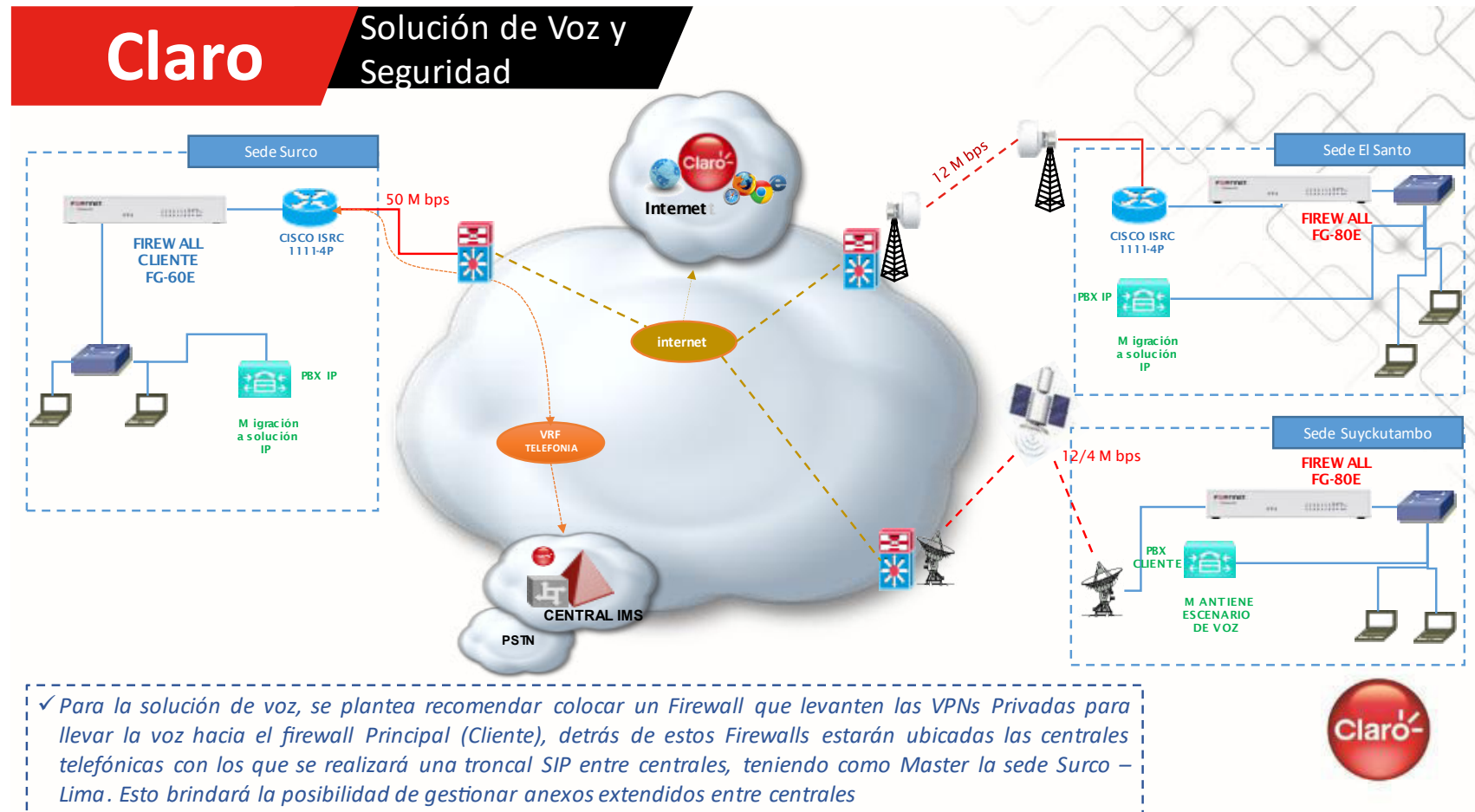


Ilustración 10 Topología incluyendo soluciones de seguridad y voz

Fuente: Elaboración Propia

Estos diseños se presentaron con sustento técnico y con referencia del levantamiento de información.

Se detallan las soluciones de la siguiente manera:

- Soluciones de conectividad con salida directa hacia internet considerando colocar un Firewall Principal, manteniendo políticas centralizadas y control desde Oficina Principal en Lima, este planteamiento busca interconectar las 3 sedes de servicio y que se puedan acceder a los servicios locales (data y voz) y en la nube a través de una conexión privada de red a través de internet por VPN (Virtual Private Network)

3.3.4.2.4 *Presentación Comercial*

Los costos de conectividad considerando los CAPEX y retorno de inversión fueron los siguientes. Se detalla en Anexo “Retorno de Inversión” los márgenes de inversión y rentabilidad:

Tabla 17 Presentación económica de solución hacia cliente

Servicio	Precio de Instalación	% Descuento Instalación	Precio SIN IGV	Tiempo de Contrato
Internet Corporativo 40 MB Incluye Router: CISCO ISRC1111-4P	\$ 0.00	100%	\$ 1,000.00	36 meses
Internet Corporativo 12 MB Incluye Router: CISCO ISRC1111-4P	\$ 0.00	100%		36 meses
Internet Satelital 8/4 MB Incluye Router: - Antena, BUC, LNB	\$ 0.00	100%	S/.10,900.00	36 meses
Herramientas de Monitoreo (MRA) Para los enlaces	\$ 0.00	100%	S/.0.00	Por todo el tiempo de contrato

Considerando los alcances de seguridad y telefonía dimensionados, considerando los costos

de inversión y el retorno:

- a) La propuesta orientada hacia telefonía IP mantiene el escenario de conectividad. El único cambio que se realizaría sería migrar la telefonía que ingresa a la sede Lima, de líneas analógicas hacia IP.
- b) Los túneles VPNs tendrían que mantenerse con los firewalls, y la calidad de servicio mejoraría. Utilizaríamos IP en todo segmento de red y no existirían conversores de tecnología IP | Digital (Gateway).
- c) En cada sede se colocarían centralitas, que soporten la solución IP, con la cantidad de anexos descrita también en la siguiente tabla

Tabla 18 Presentación económica de solución

Servicio	Precio de Instalación	% Descuento Instalación	Precio SIN IGV	Tiempo de Contrato
Equipos de Seguridad Gestionada FortiGate 60E para 2 sedes	\$ 0.00	100%	S/. 1,747.00	36 meses
Central Telefónica IP Gestionada 18 anexos – Lima – 1 Operadora				
Central Telefónica IP Gestionada 16 anexos - Arequipa				
Central Telefónica IP Gestionada 16 anexos - Cusco				

3.3.4.3 Fase de Implementación:

La estrategia descrita en las siguientes líneas detalla brevemente el proceso de implementación.

El jefe de Proyecto de Claro provee el recurso y experiencia necesarios para asegurar que la implementación del diseño y el plan cumplan con los objetivos de costo, cronograma y rendimiento ofrecidos. Este personal es entrenado extensamente y posee gran experiencia siguiendo los estándares de Claro y el uso de procesos de mejora continua para asegurar una implementación de proyecto exitosa.

Estos procesos de Claro son certificados ISO9001:2000 y forman parte de la metodología de control de calidad que se utiliza para la implementación de proyectos.

Se definen cinco (05) fases para la implementación de una o un grupo de sedes. El administrador de proyecto mantendrá esta metodología en cada caso. A continuación, se muestra las fases:

Tabla 19 Descripción de pasos para implementación

Fase	Descripción
1	Planificación
2	Ejecución
3	Pruebas y puesta de servicio
4	Cierre
5	Operación y servicio

3.3.4.3.1 Fase 1: Planificación

Esta fase incluye todas las tareas relacionadas a la planificación de la implementación de todos los servicios ofertados, así como las tareas previas que deben realizarse.

Las principales tareas de esta fase son:

- a) *Reunión de Inicio de Proyecto:* Es la reunión de presentación del grupo de trabajo de Claro con el cliente a fin de iniciar oficialmente las labores del proyecto.
- b) *Revisión del Plan:* Involucra la revisión de las principales partes del plan de proyecto, como son las actividades por desarrollarse y el cronograma presentado en la Propuesta, con el fin de aclarar cualquier duda del cliente.
- c) *Planificación de Planta Externa:* incluye la revisión de todos los planos realizados durante los estudios de factibilidad asociados al proyecto. Esta parte se enfoca especialmente en los diseños finales de planta externa de los locales donde Claro todavía no brinda servicios a la fecha de presentación de la propuesta (como es el

caso en este proyecto), o sedes que aún no cuentan con enlaces de contingencias. En esta etapa se incluye el tiempo requerido para la solicitud y aprobación formal de las autorizaciones a las Municipalidades donde se encuentran ubicados los locales del Cliente.

- d) *Planificación de los Servicios Gestionados:* Reserva de equipamiento y preparación de plantillas de configuración. Esta parte ahondará las soluciones de Seguridad y Telefonía.
- e) *Servicio de Telecomunicaciones:* incluye las tareas siguientes asociadas a los servicios ofertados.
 - *Diseño de Planta Interna:* Esto incluye la elaboración del documento de diseño de la implementación del servicio, en donde se especifican detalles precisos de equipamiento de última milla, materiales menores, distancias de cableado UTP a usar, recorrido de fibra, canaletas, energía, estudio de factibilidad para enlaces inalámbricos, etc, a utilizar de acuerdo con el cuarto de telecomunicaciones del cliente. Este documento será utilizado en el proceso de ejecución.
 - Para los casos de los proyectos en las Unidades Mineras de Arequipa y Cusco, los TSS realizados tienen definido la canalización de Planta Interna y la ruta de servicio de Planta Externa es decir el tipo de enlace y la distancia para aprovisionamiento de los mismos.
 - Para el caso del proyecto en la sede de Lima, la validación se realiza en paralelo a la fase de ejecución de Planta Externa para realizar una reconfirmación del correcto tendido externo e interno de la fibra óptica.
 - Revisión de equipos involucrados: CPE (Router) y equipos que involucran a los

Servicios Gestionados, se eligen según los BW, cantidad de usuarios, performance de equipo y tipo de procesamiento que implicará para transmisión de datos independientes y entre sedes.

- Planificación de las configuraciones de hardware y software asociados a los servicios de telecomunicaciones ofertados de acuerdo con lo solicitado, considerando tipos de configuración y requerimientos de cliente respecto a reglas o performance de equipos de cliente.
- Definición de los protocolos de pruebas asociados a los servicios de telecomunicaciones ofertados, según indicaciones, validaciones de jefe de proyecto y jefe de I.T de empresa cliente.

Parte final de la etapa de planificación es la presentación y envío de diagrama de Gantt para ejecutar el proceso de instalación, este debe ser aceptado para poder iniciar el proyecto de cliente teniendo en cuenta múltiples acciones que debemos tomar por casuísticas especiales en cada etapa.

a) Diagrama de *Gantt* presentado a cliente

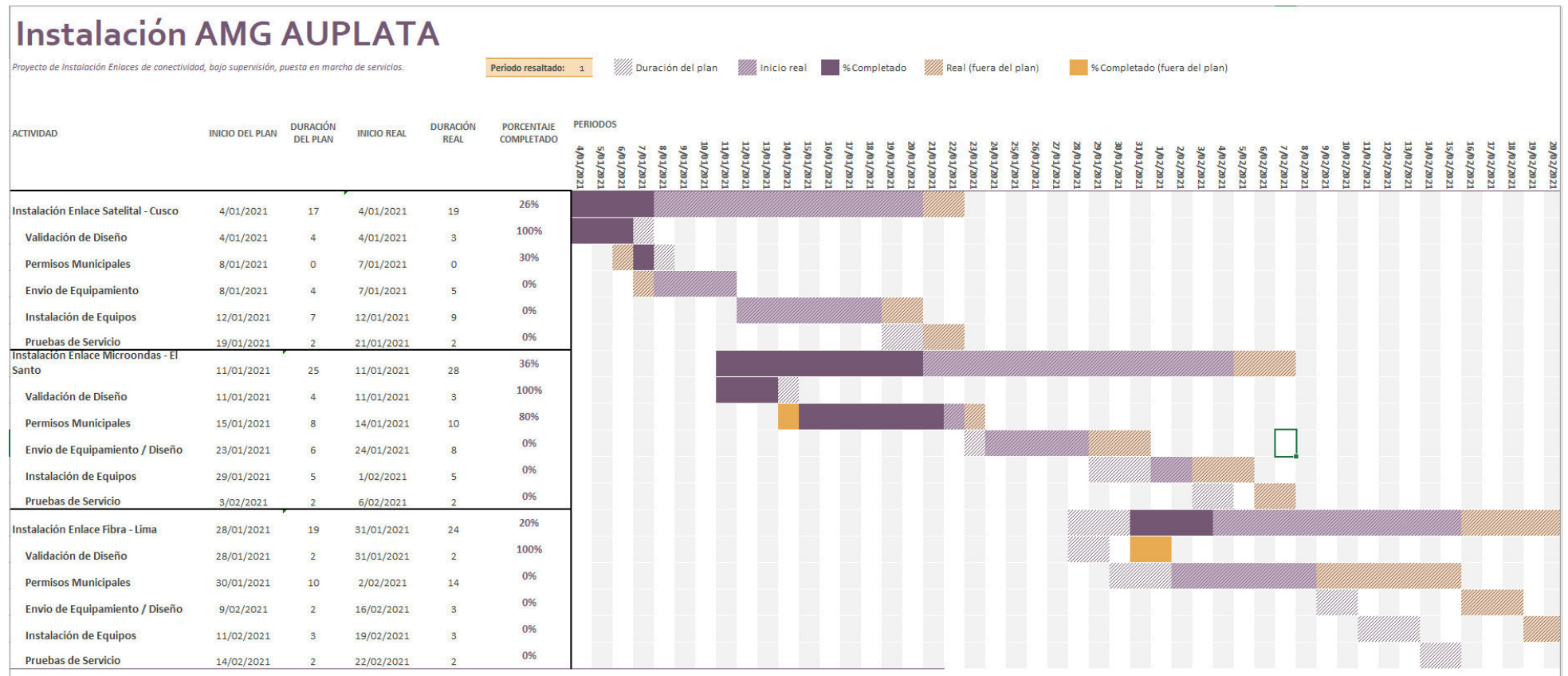


Ilustración 11 Cronograma presentado a cliente

Fuente: Elaboración propia

3.3.4.3.2 Fase 2: Ejecución

Instalación de Planta Externa: Estas labores serán iniciadas una vez obtenida, para el nodo, la autorización municipal correspondiente.

Para el caso del proyecto tenemos el despliegue de Planta Externa con fibra óptica en la sede de Lima, el despliegue y validación de LOS de Microondas para la sede Arequipa y el despliegue y validación de enlace Satelital para la sede Cusco.

Para el proceso de instalación detallaremos los casos según los procesos divididos detallados por sede:

a) Sede Lima:

- Implementación del enlace a través de fibra óptica utilizando los recursos factibilizados y reservados para el proyecto.

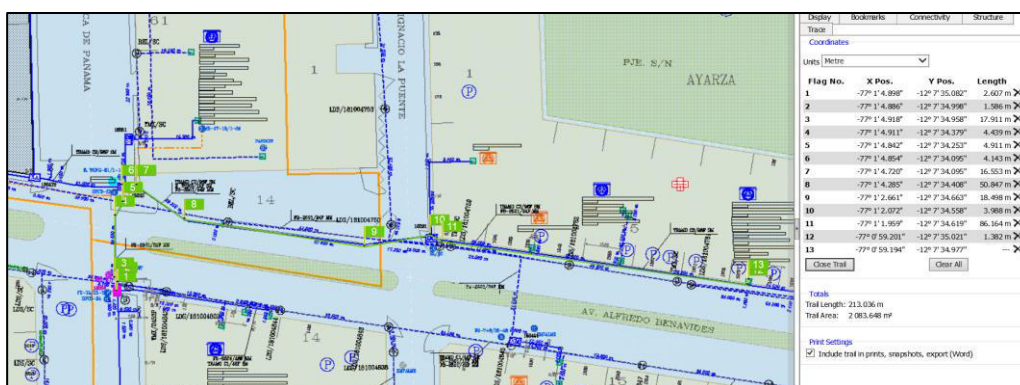


Ilustración 12 Ruta reservada para proyecto de fibra

Fuente: SGA, Sistema de Gestión de Activos

- Se muestra el trabajo de tendido y/o fusión de fibra óptica para la sede del cliente hasta el respectivo cuarto de telecomunicaciones en el ANEXO 6.3 APROVISIONAMIENTO EN SEDE FISCAL LIMA, la cual tendrá el siguiente detalle:

- Se mostrará la ubicación del POP (Point of Presence) Roosevelt, donde se

encuentra los equipos TMETRO para aprovisionamiento de servicios fijos dedicados

- Se mostrará imagen de gabinete completo con los equipos instalados.
 - Se mostrará también la bandeja de fusión de fibras para detallar, buscar la asignada y etiquetar la que se asignará a cliente.
 - Se detalla el diseño de gabinete de cliente para validar ubicación y muestrear también el hilo de llegada asignado.
 - Se instala CPE en cliente y se etiqueta según hilo de llegada a gabinete para identificación de los recursos correctos.
- Se realizan los trabajos de implementación basados en los diseños de planta externa e interna planteados, encontramos habilitación de Rack en POP, asignando de esta manera un puerto del TMETRO para habilitación de cliente
 - Habilitación, instalación e identificación de los circuitos de llegada para el servicio ofertado.

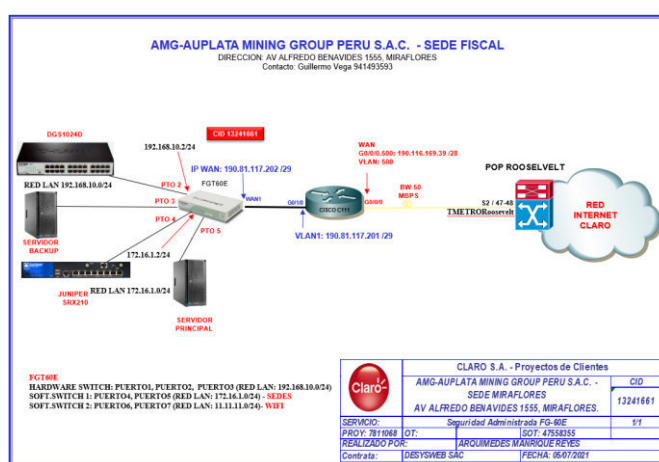


Ilustración 13 Topología de red final

Fuente: Orden de Trabajo

- Instalación de Firewall replicando políticas de firewall actual de cliente,

priorizando tráfico de VPNs entre sedes.

- Configuración de tráfico VPN Site to Site
- Configuración de acceso a servidores remotos. Lima es cabecera de acceso de servidores
- Instalación de Central Telefónica en Sede Principal.
 - Migración de E1 PRI de cliente a troncal SIP. Se mantiene numeración con proceso de portabilidad de líneas fijas.
 - Habilitación de puerto de Router para conexión a Central PBX y configuración de segmento de Red de Voz para Telefonía.
 - Validación de señalización local de telefonía (Ping a PBX principal de Claro) y configuración de PBX con numeración de cliente, IVR y anexos locales.
 - Configuración de troncal SIP entre centrales Telefónica remotas a través de VPN.

b) Sede Arequipa – El Santo

- Implementación de enlaces tipo microondas utilizando los recursos reservados del estudio de factibilidad.
- Se presentan imágenes del proceso de Instalación de enlaces inalámbricos microondas, hasta el punto de conectividad en gabinete de cliente en el ANEXO 6.4 APROVISIONAMIENTO EN U.M EL SANTO, en este se mostrará lo siguiente.

- Aprovevisionamiento desde el Site Principal hacia antena repetidora en montaña, torreo instalada por cliente.
- Desde este punto se verá también el aprovisionamiento de las antenas de recepción y la segunda antena de transmisión que va hacia el punto final el cual será la U.M el Santo.
- Se verá cableado que se realizó hasta el en las torres (Site, primera repetidora y transmisión hasta antena de recepción a gabinete)
- Se tendrán las siguientes descripciones:
 - Antena de servicio instalada en Site de Claro para aprovisionamiento de Internet Corporativo
 - Cableado, conectorización de equipos y etiquetado desde antena hacia Sala de Comunicaciones de Nodo de Transmisión
 - Antena de Servicio Instalada en Torre cliente para recepción de señal desde Nodo de Tx y cableado desde antena hacia gabinete de energía solar.
 - Antena de servicio de internet dedicado por microondas instalada y cableado desde antena hacia sala de comunicaciones de cliente en Unidad Minera.
- Habilitación, instalación e identificación de los circuitos de llegada para el servicio ofertado.
 - Validación de servicio aprovisionado, pruebas y test de velocidad, se encuentran en ANEXO 6.6 PRUEBAS DE CONFIGURACION EN U.M

EL SANTO

- Instalación de Firewall nuevo en cliente, se replican políticas generales de Lima para aplicarlas en el entorno local de la U.M el Santo.
 - Como puntos principales se configuran VPNs site to site con validación a sede Lima, adicionalmente se configura traffic shaping para aplicaciones de servicio (ERP Sede principal)
 - Proceso de configuración, reglas aplicadas y firewall se encuentran en ANEXO 6.5 CONFIGURACIÓN Y TOPOLOGIA.
- Instalación de Central Telefónica en U.M El Santo
 - Configuración de Central Telefónica en conjunto a anexos telefónicos, esta validación también involucra la configuración de troncal SIP a través de puerto de Firewall configurado con VPN site to site.
 - Validación de conectividad entre PBX (Lima – UM El Santo), pruebas de llamada y timbrado, validación de anexos y continuidad numérica, se apertura singularidad de centrales en sede

c) Sede Cusco – U.M Suyckutambo

- Implementación de enlaces tipo Satelital utilizando los recursos reservados del estudio de factibilidad. Se presentan imágenes del proceso de Instalación de enlaces inalámbricos Satelitales, hasta el punto de conectividad en gabinete de cliente.
- Habilidad, instalación e identificación de los circuitos de llegada para el servicio ofertado.

- Se realiza el aprovisionamiento de la estación X7-68520 con el siguiente equipamiento

Tabla 20 Características y equipos a instalar

Componente	Cantidad	Descripción	Serial
Antena	1	Banda C, 2.40m	Prodelin
Modem Satelital	1	Idirect X7	039658
Buc	1	10W, Banda C	A00579A27
LNB	1	PLL Banda C	A14506A53
Feed	1	Banda C	-
Mástil	1	Soporte tipo Trípode	-
Cable RG - 11	30m	Cable coaxial	RG11

- Durante el aprovisionamiento realizado al servicio en mención, se logró obtener los siguientes niveles de potencia y telemetría del servicio:

Tabla 21 Validación de potencia de transmisión

Parámetros	
Plataforma	Idirect
Potencia	-18.0 dBm
Down C/N	11.70 dB
UP C/No	73.0 dB Hz.
Aislamiento	31 dB
Nivel apuntamiento	15.40 V

- Instalación de Antena Satelital, recorrido de cableado e instalación de modem.

		
Antena de servicio satelital instalada y cableado desde antena hacia Sala de Comunicaciones e Instalación de modem satelital en gabinete de cliente.		

- Instalación de Firewall nuevo en cliente, se replican políticas generales de Lima para aplicarlas en el entorno local de la U.M Suyckutambo.
 - Como puntos principales se configuran VPNs site to site con validación a

sede Lima, adicionalmente se configura traffic shaping para aplicaciones de servicio (ERP Sede principal)

- Proceso de configuración, reglas aplicadas y firewall se encuentran en ANEXO 6.5 CONFIGURACIÓN Y TOPOLOGIA.
- Instalación de Central Telefónica en U.M Suyckutambo
 - Configuración de Central Telefónica en conjunto a anexos telefónicos, esta validación también involucra la configuración de troncal SIP a través de puerto de Firewall configurado con VPN site to site.
 - Validación de conectividad entre PBX (Lima – UM El Santo), pruebas de llamada y timbrado, validación de anexos y continuidad numérica, se apertura singularidad de centrales en sedes.
- Habilitación, instalación e identificación de los circuitos de llegada para el servicio ofertado.
 - Validación de servicio provisionado, pruebas y test de velocidad, se encuentran en ANEXO 6.7 PRUEBAS DE CONFIGURACION EN U.M SUYCKUTAMBO

3.3.4.3.3 Fase 3: Pruebas y puesta de servicio

Esta fase incluye la aplicación de los protocolos de pruebas definidas durante la fase 1 de planificación para cada uno de los servicios instalados durante la fase 2 anterior. Esto incluye:

- a) Pruebas del servicio:
 - Esta parte se concentra en la verificación de las configuraciones de los equipos: CPE (ruteadores) consideradas en el servicio ofertado.

- Las pruebas incluyen la medición del consumo de ancho de banda por cada acceso y el rendimiento observado en cada equipo.

Se anexan al presente informen, las capturas de pruebas de medición de los servicios instalados en cliente.

3.3.4.3.4 Fase 4: Cierre

La fase de cierre corresponde a la parte final del proyecto de implementación que se concentra en la solución de los posibles pendientes de Claro surgidos durante las fases 2 y 3. En esta etapa serán revisados todos los compromisos establecidos en esta propuesta.

En la reunión de cierre de proyecto, el jefe de Proyecto Claro presenta un informe al Cliente, mostrando la lista de entregables cumplidos y el resultado de las pruebas realizadas durante la fase 3.

El Cliente revisa la documentación presentada y verifica la estabilidad de los servicios implementados, luego de lo cual se emitirá el Acta de Inicio de Operaciones.

Se anexan al presente informen, las actas de cierre validadas por cliente.

3.3.4.3.5 Fase 5: Operación y Servicio

La fase 5 constituye la etapa de utilización propiamente dicha de los servicios por parte del Cliente, después de concluida satisfactoriamente la parte de implementación a cargo de Claro.

La fase de operación del servicio está definida por los eventos alertados por el Cliente o detectados directamente por CLARO que pueden afectar la calidad del servicio comprometido en esta propuesta

Básicamente comprende todas las actividades de mantenimiento preventivo y mantenimiento correctivo. Para mayor referencia de estos servicios de soporte, les pedimos

referirse a los capítulos “Descripción de los Servicios ofertados”.

Verificación de las condiciones en cada uno de los cuartos de comunicaciones, de acuerdo con lo indicado como requisitos a cargo del Cliente en la presente Propuesta Técnica.

3.4 Evaluación Económica

Proceso de inversión y cálculo de recurrentes mensuales para contratación de servicio al cliente.

Parte del proceso de evaluación de la solución fueron los resultados presentados a AMG para toma de decisión en directiva.

Esta información fue compartida posterior a la implementación del servicio con el fin de poder mostrar los resultados y mejoras del proceso

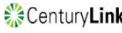
a) A continuación, se presenta el desglose comparativo de servicios

Tabla 22 Comparativo económico entre antigua solución vs nueva planteada

 Auplata Mining Group												
Conectividad - Internet y VPN												
ANTES			DESPUES									
LIMA	Proveedor	Century Link Perú SA.	LIMA	Proveedor	CLARO	Proveedor	CLARO	Telefonía	51 anexos IP distribuidos en las 3 sedes. 1 centralita en Cada Sede			
	Tecnología	VPN		Tecnología	INTERNET DEDICADO - F. O	Tecnología	Telefonía IP					
	Ancho de Banda	6 Mb		Ancho de Banda	50MB	Utilidad	Comunicación local - nacional	Seguridad	2 Fortinet FG-80E. 1 en cada sede remota			
	subida	0 Mb		subida	50MB	Conectividad	Anexos Extendidos por VPN					
	descarga	0 Mb		descarga	50MB	Plus	Interconectadas e independientes					
LIMA	Proveedor	Century Link Perú SA.	EL SANTO	Proveedor	CLARO	Proveedor	CLARO	Proveedor	CLARO			
	Tecnología	Internet dedicado		Tecnología	INTERNET DEDICADO - Radio enlace	Tecnología	Seguridad Perimetral	Tecnología	Telefonía IP			
	Ancho de Banda	20 Mb		Ancho de Banda	14 Mb	Utilidad	VPN - Interconexión	Utilidad	Comunicación local - nacional			
	subida	0 Mb		subida	14 Mb	subida	Definido por consumo	Conectividad	Anexos Extendidos por VPN			
	descarga	0 Mb		descarga	14 Mb	descarga	Definido por consumo	Plus	Interconectadas e independientes			
EL DIABLO	Proveedor	Century Link Perú SA.	SUYCKUTAMBO	Proveedor	CLARO	Proveedor	CLARO	Proveedor	CLARO			
	Tecnología	Radio enlace		Tecnología	SATELITAL	Tecnología	Seguridad Perimetral	Tecnología	Telefonía IP			
	Ancho de Banda	3 Mb		Ancho de Banda	12 Mb	Utilidad	VPN - Interconexión	Utilidad	Comunicación local - nacional			
	subida	1 Mb		subida	12 Mb	subida	Definido por consumo	Conectividad	Anexos Extendidos por VPN			
	descarga	2 Mb		descarga	12 Mb	descarga	Definido por consumo	Plus	Interconectadas e independientes			
SOPORTE	Por Teléfono	NO	SOPORTE	Por Teléfono	SI							
	Por correo	SI		Por correo	SI							
	Remoto	NO		Remoto	SI							
	Tiempo	no se sabe		Tiempo	INMEDIATO, MAXIMO 4HORAS							
	Sistema-Ticket	SI		Sistema-Ticket	SI							
	TOTAL	\$7,080.00		TOTAL	\$5,143.73							

b) Resumen detallado presentado por cliente

Tabla 23 Detallado descriptivo de solución para cliente

 Auplata Mining Group																			
Conectividad - Internet y VPN																			
	INTERNET			VPN			SEGURIDAD / FIREWALL			SOPORTE				COSTO MENSUAL	TELEFONIA FIJA			COSTO MENSUAL	
	LIMA	EL SANTO	SUYKU-TAMBO	LIMA	EL SANTO	SUYCKU-TAMBO	LIMA	EL SANTO	SUYCKU-TAMBO	TELEFONO	CORREO	TIEMPO RPTA.	TICKET		LIMA	EL SANTO	SUYCKU-TAMBO		
	20MB	3MB	3MB	6MB	3MB	3MB	SI	NO	NO	NO	SI	INMEDIAT O	SI	\$7,080.00	ANALOGA	VOIP	VOIP	incluido	
	FIBRA OPTICA	SATELITAL	SATELITAL	ROUTER	ROUTER	ROUTER	FORTINET	-	-			MAXIMO 4 HORAS			CENTRAL PANASONIC	CENTRAL PANASONIC	CENTRAL PANASONIC	PROPIO	
							ANTIGUO	-	-										
															Anexos análogos Panasonic antiguos				
	50MB	14MB	12MB	Por uso	Por uso	Por uso	SI	SI	SI	SI	SI	INMEDIAT O	SI	\$5,143.73	51 ANEXOS A REPARTIR EN LAS 3 SEDES			S/ 2,288.00	
	FIBRA OPTICA	RADIO ENLACE	SATELITAL	FORTINET	FORTINET	FORTINET	FORTINET	FORTINET	FORTINET			MAXIMO 4 HORAS			DIGITAL - IP CENTRAL	DIGITAL - IP CENTRAL	DIGITAL - IP CENTRAL		
				El tráfico VPN se realiza según demanda de paquetes de consulta hacia los servidores. Durante diseño se validó tráfico a servidores de aprox. 2-3 MB. Se comporta según lo que necesiten, en caso requieran darle control, se puede asignar el BW en Firewall.			FG-60E. 1	FG-80E. 1	FG-80E. 1										
							Sistema de seguridad optimizado, interconectado e independiente. Permitirá mejoras en tráfico, uso de aplicaciones y trabajo remoto.												
															Anexos Extendidos por VPN				
															Interconectadas e independientes. Pueden operar interconectadas y también como centrales independientes en cada punto.				

CAPITULO IV: REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

Este proyecto se planteó como solicitud de mejora de la empresa a varios ISP en Perú, con el objetivo de realizar un proyecto homogéneo y perdurable para sus operaciones.

Anteriormente la empresa Minera tuvo servicios de Telecomunicaciones de pobre calidad lo que limitaba las operaciones y la calidad de comunicaciones del personal, el pobre porcentaje de BW fue el principal criterio de búsqueda de nuevas alternativas. El levantamiento de información adicional compartida por el cliente y referenciada por los ingenieros del proyecto y mi persona fueron vitales para poder realizar un planteamiento que no solo se aboque a mejorar la plataforma de comunicaciones sino también orientarse a futuros requerimientos, migraciones y orientado a la protección de datos (ciberseguridad). Los dimensionamientos fueron adecuados y óptimos en equipos, lo cual nos permitió poder plantear una Propuesta Técnica y Económica dentro de los márgenes de presupuesto esperado por la Minera.

Mi trabajo como Consultor Corporativo se orientó a la participación en todas las fases del proyecto, debido a los márgenes altos de ganancia, estuve involucrado en el contacto, levantamiento de información, diseño, presentación y cierre técnico comercial del proyecto, sin embargo, estuve activamente involucrado en todo el proceso de implementación del proyecto hasta el cierre de este. Mi función principal se orientó a presentarle al cliente que nuestra solución era la óptima técnicamente, se realizaron diversas reuniones para descartar dudas y responder todas las consultas técnicas de implementación desde los planteamientos y permisos municipales para la fibra óptica en Lima, los permisos y gestión energética en Arequipa y las características y condiciones ambientales para el enlace satelital en Cusco.

Los principales retos que encontramos se presentaron durante las visitas de preinstalación en los campamentos mineros, los cuales se pueden señalar como puntos críticos pero que fueron

absueltos con aplicación de ingeniería:

- a) Falta de energía estabilizada en la U.M El Santo, este punto fue indicado posterior a rezagos presupuestarios dejados por pandemia, inicialmente la Minera iba a colocar la energía en la antena desde el campamento, pero el tendido eléctrico se descartó por falta de presupuesto. Ante este acontecimiento y revalidación del proyecto, planteamos la solución de energía solar para aprovisionamiento de esta a los equipos de comunicaciones.
- b) Reflejos por techos de calamina e interferencia de señal satelital en U.M Suykutambo, lo que provocaba que el BW adquirido no llegue a la totalidad, este punto se verificó durante la visita de prediseño, donde se realizaron dos planteamientos, movilizar la posición de la antena satelital o realizar un reacondicionamiento de la red satelital para optimizar la señal en la ubicación. La primera alternativa fue descartada porque generaba costos adicionales de cableado, personal y doble desplazamiento de equipo, por lo que a nivel de red se tomó la decisión de instalar el servicio sin costo y realizar la adecuación de red satelital para optimización de BW.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El levantamiento de información ante la implementación de un futuro proyecto es clave para la obtención de los resultados esperados, estas indicaciones validadas por el cliente es básicamente la necesidad y volcada en cuanto a experiencia significa una clave para el éxito técnico y comercial en la venta de un proyecto.

Se analizaron varios escenarios desde la solución anterior hasta la proyección a futuro de la empresa en cuanto a sus sistemas de comunicaciones.

Las mejoras fueron recibidas y visibles desde el primer momento de la implementación, porcentualmente se tuvo una mejora de 300% en los sistemas de comunicación.

Se optimizaron los sistemas de seguridad perimetral, lo que nos dio una mejora adicional en el uso correcto del BW para las labores empresariales en los campamentos mineros.

Se mejoraron los tiempos de respuesta y acceso a servidores, cuando cambiamos el medio satelital a microondas de 800ms a 80ms.

El proceso de migración de comunicación analógica a IP fue totalmente aceptado para las comunicaciones entre sedes, esto mejoró los procesos logísticos para la empresa.

5.2 Recomendaciones

La recomendación principal para este proyecto es mantener la línea de optimización de comunicaciones, los procesos de servicios fijos han mejorado la producción.

Los sistemas de comunicaciones generarán mayor necesidad de estos mismos, pues se irán necesitando más ancho de banda por los aplicativos que se irán integrando, esto generará

plantear un proyecto de ampliación de capacidad.

Los presupuestos deben orientarse a realizar estas mejoras, sin embargo, los sistemas de comunicaciones son siempre propuestos para reducción de inversión, para este caso se debe reorientar presupuesto pues se generará un mayor índice de requerimientos, esto por experiencia en gran minería

Los nuevos procesos irán generando necesidades operativas, donde la red local de comunicaciones en los campamentos mineros será un factor importante para la automatización, control y monitoreo de múltiples sistemas mineros.

Se deben plantear un proyecto para llevar fibra óptica a los campamentos mineros, planteando dos opciones:

- c) Primera opción: Minera sacar fibra a través de postes propios hacia el lugar de acceso más próximo a nodos de operador
- d) Segunda opción: Realizar tendido de fibra a través de los postes de energía eléctrica que llegan al campamento.

5.3 Fuentes de información

[1] Solar Energy: The Physics and Engineering of Photovoltaic Conversion Technologies and Systems , UIT, Arno Smets, Klaus Jager, Olindo Isabella, René Van Swaaj, Miro Zeeman. Publicado el año 2018.

[2] CCNP Routing and Switching Publicado el año 2015. ROUTE 300101 Official Cert Guide, Kevin Wallace.

[3] Free Cybersecurity Training, and On-Demand Labs (2022).
<https://www.fortinet.com/training/cybersecurity-professionals>

5.4 Glosario

SMTP: El SMTP (Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo) es un protocolo que permite el envío de correos electrónicos en internet.

IMAP: Internet Message Access Protocol o protocolo de acceso a mensajes de Internet, es un protocolo que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

POP3: Protocolo de Oficina de Correo o "Protocolo de Oficina Postal se usa en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP.

IPS: Es un sistema de prevención de intrusiones. Se encarga de identificar, clasifican y detienen el tráfico malicioso, como, por ejemplo, gusanos, spyware y adware, virus de redes, y abuso de aplicaciones, antes de que afecten su computadora o red.

Traffic Shaping: También conocida como "packet shaping" es un mecanismo que se utiliza para realizar un control inteligente del tráfico de datos en una red de computadoras, este control produce una mejora en el rendimiento de la red de datos que se aprecia en el aumento de su velocidad disponible.

APT: Advanced Persistent Threat o amenaza persistente avanzada. Es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica.

L4/L3: Capa 4 y capa 3 del Modelo OSI.

PBR: Policy Based Routing o enrutamiento basado en políticas. Es un mecanismo para implementar decisiones de enrutamiento de paquetes de datos basados en políticas definidas por el administrador de red.

IPSEC: Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos

VPN: Virtual Private Network o Red Privada Virtual. Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

SSH: Secure SHell. Es un protocolo cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

HTTPS: Hypertext Transfer Protocol Secure o Protocolo seguro de transferencia de hipertexto. Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

VRF: El Enrutamiento Virtual y Reenvío (VRF) es una tecnología incluida en Router de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente.

NPM: Network performance management o Gestión del rendimiento de la red. Es la técnica colectiva que permite, gestiona y garantiza niveles óptimos de rendimiento de una red informática.

Logs: En informática, se usa el término log, historial de log o registro, se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular.

NAT: Network Address Translation o Traducción de Direcciones de Red. Es un mecanismo que permite por ejemplo que múltiples dispositivos compartan una sola dirección IP pública de Internet.

Capa 3: Capa 3 del modelo OSI.

Rutas Estáticas: La ruta estática se configura para conseguir conectividad con un enlace de datos que no está directamente conectado al router.

NGFW: Los Next Generation Firewalls (NGFW) son Firewall que han evolucionado incorporando muchas otras funcionalidades de seguridad como Anti-malware (anti-virus, anti-spyware, anti-spam), IPS (Sistema de Prevención anti Intrusiones), VPN (Red Privada Virtual), entre otras.

HTTP: Hypertext Transfer Protocol o Protocolo de transferencia de hipertexto. Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

Phishing: Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas de tarjetas de crédito y otros, haciéndose pasar por una comunicación confiable y legítima.

Streaming Media: Es un método utilizado para entregar elementos multimedia, generalmente video o audio, desde un proveedor de servicios de transmisión de datos hasta un usuario final. Utiliza protocolos básicos HTTP, TCP / IP y HTML.

SPAM: Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados

en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Spoofing (MIME header check): La suplantación de identidad, en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Modelo OSI: Open System Interconnection. Modelo de interconexión de sistemas abiertos. Es un modelo de referencia para los protocolos de red que divide las comunicaciones en 7 capas.

Zona DMZ - Zona LAN - Zona Internet: Demilitarized zone o zona desmilitarizada. Es una red local que se ubica entre la red interna (Zona LAN) de una organización y una red externa, generalmente en Internet (Zona Internet).

Bugs: Es un error de un programa o software que desencadena un resultado indeseado.

Endpoint: Es un dispositivo informático que se comunica con una red a la que está conectado.

RMA: Return Merchandise Authorization o Autorización de Retorno de Mercancía. Es un proceso de devolución de un producto para recibir un reemplazo o reparación durante el período de garantía del producto.

LED: Es una fuente de luz constituida por un material semiconductor dotado de dos terminales.

CPU: La unidad de procesamiento central o central processing unit es el hardware dentro de un ordenador u otros dispositivos programables, que interpreta las instrucciones de un programa informático.

URL Filtering: Filtrado de URL es una tecnología que compara todo el tráfico web con una base de datos de filtrado de URL, permitiendo o negando el acceso en función de la información que contiene.

Forticare: Soporte técnico de Fortinet.

Fortiguard: Servicio de Fortinet

UTM: United Threat Management o Gestión unificada de amenazas. Hace referencia a un dispositivo de red con múltiples funciones, como antivirus, Firewall, Antispyware y otros.

Data Leakage Prevention (DLP): Se refiere a una solución que evita la fuga de datos. Se centra en la detección y prevención de la filtración de datos confidenciales y / o datos perdidos.

DNS Lookup: Herramienta de red basada en navegador que muestra registros DNS que muestran públicamente el nombre de dominio que se consulta.

CA: Certification Authority o autoridad de certificación, señalan a una entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública.

Inspección SSL (o SSL inspection): Es una función de seguridad que protege la red de amenazas, permite desbloquear sesiones encriptadas, ver paquetes encriptados, encontrar amenazas y bloquearlas. SSL inspection no solo protege de ataques que usan HTTPS, sino también de otros protocolos codificados comúnmente utilizados, como SMTPS, POP3S, IMAPS, FTPS.

CAPITULO VI: ANEXOS

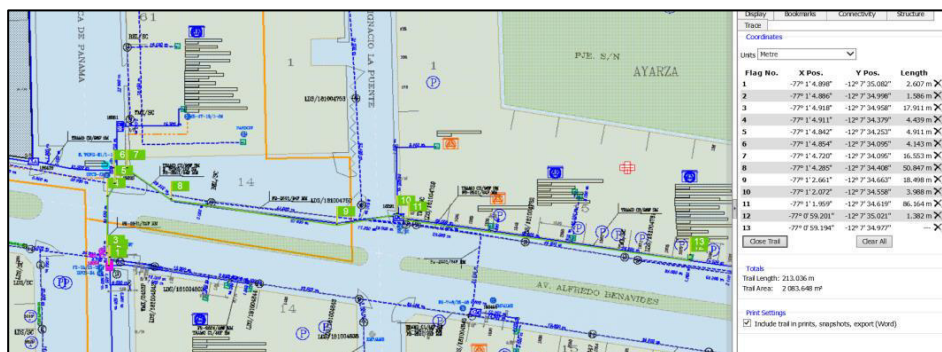
6.1 ESTUDIO DE FACTIBILIDAD EN GABINETE PARA SEDE LIMA

- d) En estos casos los análisis en gabinete son 95% confiables para despliegues, en la mayoría de los casos en Lima se obtiene el 100% según la zona; en este caso la ubicación es un edificio y zona empresarial, por lo cual podemos estar seguros de trabajar con este tipo de análisis.

Project Name	Type	Status	Location	Other Details
PROYECTO 1	...	...	...	...
PROYECTO 2	...	...	...	...
PROYECTO 3	...	...	...	...
PROYECTO 4	...	...	...	...
PROYECTO 5	...	...	...	...
PROYECTO 6	...	...	...	...
PROYECTO 7	...	...	...	...
PROYECTO 8	...	...	...	...
PROYECTO 9	...	...	...	...
PROYECTO 10	...	...	...	...
PROYECTO 11	...	...	...	...
PROYECTO 12	...	...	...	...
PROYECTO 13	...	...	...	...
PROYECTO 14	...	...	...	...
PROYECTO 15	...	...	...	...
PROYECTO 16	...	...	...	...
PROYECTO 17	...	...	...	...
PROYECTO 18	...	...	...	...
PROYECTO 19	...	...	...	...
PROYECTO 20	...	...	...	...
PROYECTO 21	...	...	...	...
PROYECTO 22	...	...	...	...
PROYECTO 23	...	...	...	...
PROYECTO 24	...	...	...	...
PROYECTO 25	...	...	...	...
PROYECTO 26	...	...	...	...
PROYECTO 27	...	...	...	...
PROYECTO 28	...	...	...	...
PROYECTO 29	...	...	...	...
PROYECTO 30	...	...	...	...
PROYECTO 31	...	...	...	...
PROYECTO 32	...	...	...	...
PROYECTO 33	...	...	...	...
PROYECTO 34	...	...	...	...
PROYECTO 35	...	...	...	...
PROYECTO 36	...	...	...	...
PROYECTO 37	...	...	...	...
PROYECTO 38	...	...	...	...
PROYECTO 39	...	...	...	...
PROYECTO 40	...	...	...	...
PROYECTO 41	...	...	...	...
PROYECTO 42	...	...	...	...
PROYECTO 43	...	...	...	...
PROYECTO 44	...	...	...	...
PROYECTO 45	...	...	...	...
PROYECTO 46	...	...	...	...
PROYECTO 47	...	...	...	...
PROYECTO 48	...	...	...	...
PROYECTO 49	...	...	...	...
PROYECTO 50	...	...	...	...
PROYECTO 51	...	...	...	...
PROYECTO 52	...	...	...	...
PROYECTO 53	...	...	...	...
PROYECTO 54	...	...	...	...
PROYECTO 55	...	...	...	...
PROYECTO 56	...	...	...	...
PROYECTO 57	...	...	...	...
PROYECTO 58	...	...	...	...
PROYECTO 59	...	...	...	...
PROYECTO 60	...	...	...	...
PROYECTO 61	...	...	...	...
PROYECTO 62	...	...	...	...
PROYECTO 63	...	...	...	...
PROYECTO 64	...	...	...	...
PROYECTO 65	...	...	...	...
PROYECTO 66	...	...	...	...
PROYECTO 67	...	...	...	...
PROYECTO 68	...	...	...	...
PROYECTO 69	...	...	...	...
PROYECTO 70	...	...	...	...
PROYECTO 71	...	...	...	...
PROYECTO 72	...	...	...	...
PROYECTO 73	...	...	...	...
PROYECTO 74	...	...	...	...
PROYECTO 75	...	...	...	...
PROYECTO 76	...	...	...	...
PROYECTO 77	...	...	...	...
PROYECTO 78	...	...	...	...
PROYECTO 79	...	...	...	...
PROYECTO 80	...	...	...	...
PROYECTO 81	...	...	...	...
PROYECTO 82	...	...	...	...
PROYECTO 83	...	...	...	...
PROYECTO 84	...	...	...	...
PROYECTO 85	...	...	...	...
PROYECTO 86	...	...	...	...
PROYECTO 87	...	...	...	...
PROYECTO 88	...	...	...	...
PROYECTO 89	...	...	...	...
PROYECTO 90	...	...	...	...
PROYECTO 91	...	...	...	...
PROYECTO 92	...	...	...	...
PROYECTO 93	...	...	...	...
PROYECTO 94	...	...	...	...
PROYECTO 95	...	...	...	...
PROYECTO 96	...	...	...	...
PROYECTO 97	...	...	...	...
PROYECTO 98	...	...	...	...
PROYECTO 99	...	...	...	...
PROYECTO 100	...	...	...	...

Los alcances del estudio en gabinete destacan los análisis siguientes:

- e) Ruta desde MUFA y canalizado existente hasta ingreso.



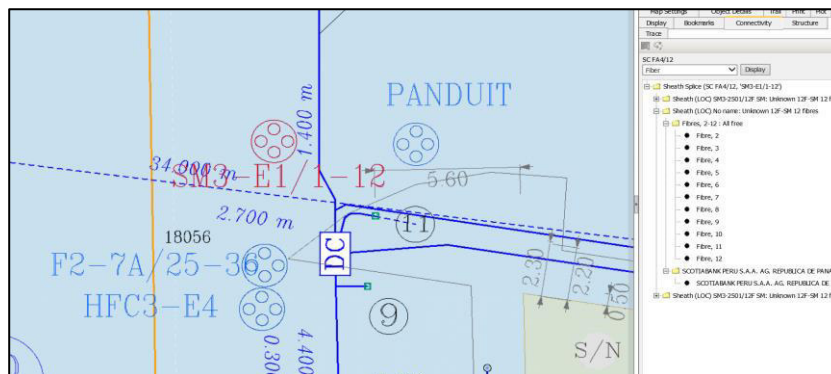
- f) Se realizar validación de POP que aprovisiona MUFA, se verifica estado de puertos disponibles:

Asignación de Puerto														
N°	Sala	Ambiente	Equipo	Tipo Tarjeta	Tarjeta	Interfaz	Stat	S.Stat	Puerto	Estado	ICSE	Descripción	Medio de Tx. (F)	Coordenadas
25	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	39-48	Shutdown		Fibra		
26	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	41-42	Active		676281 DE 676281 CD 10663322	CD 10777737	Fibra
27	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	43-44	Shutdown				
28	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	45-46	Shutdown				
29	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	47-48	Shutdown				
30	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	49-50	Shutdown				
31	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	51-52	Shutdown				
32	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	5-6	Active		674588 DE 674588 CD 10084762	MINISTERIO DE Fina	
33	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	7-8	Shutdown				
34	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	62	0	9-10	Shutdown				
35	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	64	0	11-12	Shutdown				
36	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	64	0	1-2	Shutdown				
37	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	64	0	13-14	Shutdown				
38	POP Roosevelt	Sala Pop	TIETRO/Roosevelt	EWOPR2	EWOPR2 Ie	EWOPR2 Ie	64	0	15-16	Shutdown				

g) Se generan reservas provisionales y preconfiguración, actualizando estado de puertos asignados vigentes.

POP Roosevelt														
Cable	Term.	Tipo Term.	Unidad Cable Terminal	Fibra	Estado	Observación	F. Instalac.	F. Baja	Cliente	Dirección	Proyecto	Mis. Servicio	Estado Serv.	
3011	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	35	Reservado	24/07/2018		SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES	AV JOSE RAMIREZ DIAZTON 175 PRO 1	000528447	CD 0549695	Active	2
3012	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	37	Reservado	03/09/2018		UNIVERSIDAD DE SAN MARTIN DE PORRES	CA NUNTA DOLADO 101 SAN ANTONIO	000671390		Active	2
3013	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	39	Reservado	10/09/2018		EURCAPITAL SERVICIOS FINANCIEROS S.A.C.	AV FREDDY BRAHVES 197 PRO 1 VORHO	000530786	CD 0457606	Active	2
3014	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	41	Reservado	06/06/2018		TAI LOY S.A.	AV FREDDY BRAHVES 197 PRO 1 VORHO	000530626	CD 4751638	Active	4
3015	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	43	Reservado	22/05/2018		SCOTT BANK PERU S.A.A.	AV REPUBLICA DE PANAMA-6201	000530626	CD 3913003	Active	2
3016	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	45	Reservado	28/10/2018		PLAYA PERROS S.A.C.	AV REPUBLICA DE PANAMA-6201	000530626	CD 8896406	Active	2
3017	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	47	Reservado	16/05/2018		ASOCIACION DE BANCOS DEL PERU	URBANIZACION 005318154	000530626	CD 1465759	Active	4
3018	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	49	Reservado	12/01/2017		MINISTERIO DE AGRICULTURA	AV FREDDY BRAHVES 197 PRO 1 VORHO	000530626	CD 0548616	Cancelled	1
3019	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	51	Reservado	11/10/2018		SCOTT BANK PERU S.A.A.	CALLEADUO AMOLLO 130 CALLEADUO	000530626	CD 1009166	Active	1
3020	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	53	Reservado	17/09/2018		BANCO DE CREDITO DEL PERU	URBANIZACION 144 762	000530626	CD 1041160	Active	1
3021	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	55	Reservado	14/02/2018		ALTRA S.A.	AV FREDDY BRAHVES 197 PRO 1 VORHO	000530626	CD 7836838	Active	2
3022	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	57	Reservado	06/10/2018		ASOCIACION DE BANCOS DEL PERU	AV REPUBLICA DE PANAMA-6201	000530626	CD 0602916	Active	2
3023	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	59	Reservado	29/10/2018		PLAYA PERROS S.A.C.	AV REPUBLICAS 108 ENTE LA VANDER	000530626	CD 8896411	Active	2
3024	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	61	Reservado	07/05/2019		MINISTERIO DE LA RIEUA Y POBLACIONES VULNERABLES	AV FREDDY BRAHVES 197 PRO 1 VORHO	000530626	CD 10084762	Active	1
3025	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	63	Reservado	16/07/2018		PLAYA PERROS S.A.C.	AV REPUBLICAS 108 ENTE LA VANDER	000530626	CD 0548616	Cancelled	1
3026	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	65	Reservado	22/05/2018		MULTIPLEX S.A.C.	AV REPUBLICAS 108 ENTE LA VANDER	000530626	CD 000413984	Active	1
3027	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	67	Reservado	13/09/2018		RP SUPORT SOCIEDAD ANONIMA CERRADA	AV JOSE GABRIEL SANCHEZ 429	000530626	CD 000413984	Active	1
3028	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	69	Reservado	09/10/2018		PERUAM PERU S.A.C.	ALTRA 000530626	000530626	CD 000413984	Active	1
POP Tiro Lento Hilo														
3029	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	71	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3030	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	73	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3031	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	75	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3032	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	77	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3033	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	79	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3034	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	81	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3035	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	83	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3036	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	85	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3037	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	87	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3038	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	89	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3039	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	91	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3040	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	93	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3041	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	95	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3042	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	97	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3043	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	99	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3044	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	101	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3045	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	103	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3046	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	105	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3047	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	107	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3048	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	109	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3049	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	111	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3050	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	113	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3051	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	115	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3052	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	117	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3053	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	119	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3054	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	121	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3055	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	123	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3056	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	125	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3057	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	127	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3058	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	129	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3059	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	131	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3060	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	133	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3061	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	135	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3062	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	137	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3063	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	139	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3064	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	141	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3065	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	143	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3066	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	145	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3067	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	147	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3068	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	149	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3069	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	151	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3070	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	153	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3071	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	155	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3072	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	157	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3073	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	159	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3074	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	161	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3075	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	163	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3076	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	165	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3077	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	167	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3078	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	169	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3079	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	171	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3080	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	173	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3081	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	175	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3082	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	177	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3083	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	179	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3084	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	181	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3085	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	183	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3086	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	185	Reservado	11/02/2019		AV REPUBLICA DE PANAMA-6403	AV REPUBLICA DE PANAMA-6403	000530626	CD 000413984	Active	1
3087	6	6	Reservado	AV REPUBLICA DE PANAMA-6403	187	Reservado	11/02/2019		AV REP					

h) Se realiza reserva de recursos físicos en MUFA de análisis



6.2 ESTUDIO DE FACTIBILIDAD EN GABINETE PARA U.M EL SANTO

a) Primer enfoque



Vista Geográfica y Perfil de elevación, primer enfoque

b) Segundo enfoque:



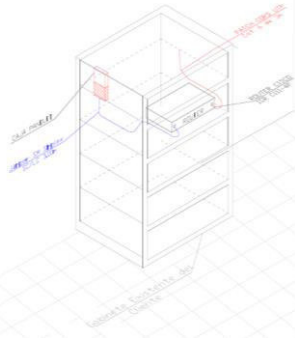
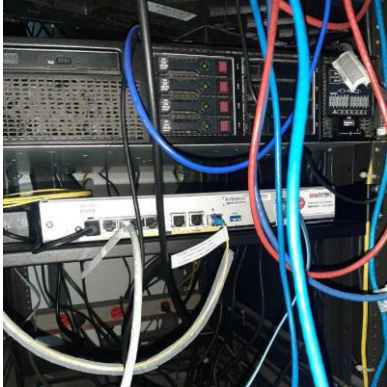
Vista Geográfica y Perfil de elevación, segundo enfoque

a) Tercer enfoque:



Vista Geográfica y Perfil de elevación, tercer enfoque

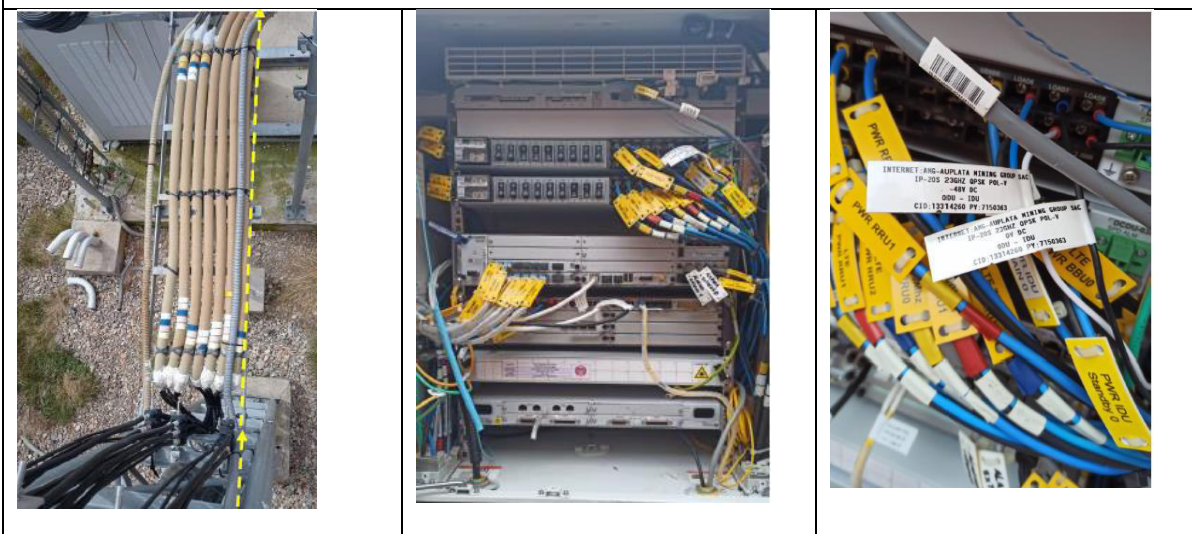
6.3 APROVISIONAMIENTO EN SEDE FISCAL LIMA

		
Ubicación de POP Roosevelt	Ubicación TMETRO	Bandeja para fusión de Fibra
		
Diseño gabinete Cliente	Instalación de Router CPE	Etiquetado de cables

6.4 APROVISIONAMIENTO EN U.M EL SANTO



Antena de servicio instalada en Site de Claro para aprovisionamiento de Internet Corporativo



Cableado, conectorización de equipos y etiquetado desde antena hacia Sala de Comunicaciones de Nodo de Transmisión



Antena de Servicio Instalada en Torre cliente para recepción de señal desde Nodo de Tx y cableado desde antena hacia gabinete de energía solar.



Antena de Servicio Instalada en Torre cliente para transmisión de señal hacia U.M El Santo y Cableado desde antena hacia gabinete de energía solar.



Antena de servicio de internet dedicado por microondas instalada y cableado desde antena hacia sala de comunicaciones de cliente en Unidad Minera

6.5 CONFIGURACION Y TOPOLOGIAS



SERVICIO ADMINISTRATIVA - FIREWALL

NOMBRE DEL PROVEEDOR DESYSWEB SOT en donde se carga la document 47558355

* Toda la pestaña la llena por proveedor

1.1 - ALCANCE DEL SERVICIO Y SOPORTE POST VENTA DEL PROVEEDOR.

* En caso, el servicio está bajo el alcance del gestionado, dejar en blanco columna B.

OC / POS	Alcance del servicio	Equipo sobre el cual se da el servicio	Fecha inicio del servicio	Fecha fin del servicio	SOT Instalación	CID
N/A	Seguridad Administrada, Estandar	FG-60E	5/07/2021	5/07/2024	47558355	13241661

1.2 - LICENCIAS Y GARANTÍAS POST VENTA DEL PROVEEDOR.

Nombre Licencia o Garantía	nro de serie del equipo	OC (Si es no es recurrente)	POS	SOT	CID	Fecha Inicio	Fecha Fin	Observaciones
Licencia	FGT60ETK19088124	N/A	N/A	47558355	13241661	5/07/2021	5/07/2024	
Garantía	FGT60ETK19088124	N/A	N/A	47558355	13241661	5/07/2021	5/07/2024	

1.2 - CONDICIONES DE DESPLAZAMIENTO DEL PROVEEDOR.

Calda severidad 1

1.3 - SLA BRINDA EL PROVEEDOR

	NIVEL DE CRITICIDAD
	NIVEL 1 (Suspension total del servicio) NIVEL 2 (Inoperatividad parcial del servicio) NIVEL 3 (No hay perdida del servicio)
Tiempo de respuesta	30 Minutos 2 Horas 4 Horas
Tiempo para reponer equipos / desplazamiento	4 Horas 4 Horas 4 Horas
Tiempo de solución	2 horas 4 Horas 24 Horas
Tiempo entrega de informe técnicos	24 Horas 24 Horas 24 Horas

1.4 - EQUIPOS SPARE

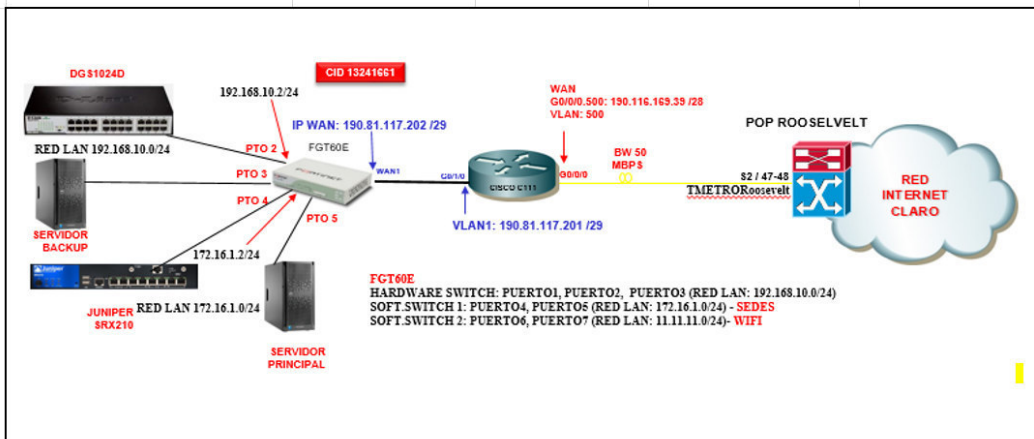
Descripción (Modelo / Cantidades)	Necesita licencia para funcionamiento	Número de Serie	Ubicación (Proveedor, Claro)	Observación (Velocidad, versión, RMA, soporte de fábrica, etc.)
Claro	N/A	N/A	Claro	N/A

1.6- PRUEBAS Y REPORTES DE ENTREGA DEL SERVICIO

1. Protocolo de Pruebas.
2. Prueba de servicios externos.
3. Prueba de acceso.
4. Prueba de acceso remoto (VPN SSL)

1.7- TOPOLOGÍA (Identificar servicios existentes por CID, detallar modelo de equipos, IP, anchos de banda por enlace, medios de transmisión (Fibra y cu), tipo del puerto (Gi, Eth), en que puerto se esta conectando cada equipo, la propiedad del cableado o equipos si pertenece a Claro o al cliente, en caso de que Claro lo ha colocado que proveedor ejecuta el soporte)

Topología del servicio



1.8- SERVICIOS NO INCLUIDOS

A llenar por proveedor

Enumerar que servicios no se encuentran incluidos en la atención del proyecto, por ejemplo:

1. Reparación de equipos X
2. Monitoreo de equipos en sitio X
3. Desinstalación o reinstalación del equipo (Prevía coordinación con el cliente en caso amerite)
4. Limpieza exterior X
5. La operación misma de los sistemas X
6. Respaldos de la información X
7. Grupos
8. Remoción de blacklist.

GESTIÓN INTERNA

Cantidad de Enlaces	1 - Claro
Ancho de Banda	25
Marca/Modelo del Equipo	FORTIGATE 60E
Sistema Operativo de Equipo FW	v6.2.4
Nueva Implementación/Migración Firewall	Nueva Implementación
Cliente tiene Gestión de FW	SI: NO: (X)
Se valida Gestión Interna y Remota	SI: NO: (X)
Puerta de Enlace (Router):	190.81.117.201
IP privada asignada al FW:	190.81.117.202
Puerto que conecta al SW - CPE	HS(1-3) SS(4-5) SS(6-7) - WAN1
Velocidad / Duplex de la Interfaz:	LAN:1000/Full
Servidor DNS:	8.8.8.8 200.24.191.11

INFORMACIÓN DE RED

RED [Dirección IPv4 del segmento de red. Por ejemplo: 192.168.10.0], NOMBRE DE RED [Nombre en particular de la red del cliente. Por ejemplo: RED LAN, RED DMZ, RED SERVIDORES, etc.], MÁSCARA [Define la máscara de red.

Nº		NOMBRE RED		RED	MÁSCARA	PUERTA DE SALIDA		DESCRIPCIÓN
Name ▾	Type ▾	Members ▾	IP/Netmask ▾	Administrative Access ▾	DHCP Clients ▾	DHCP Ranges ▾	Ref. ▾	
⚙ Disabled ⓘ								
⬆ Up ⓘ								
INTERNET	Zone	INTERNET L3 (wan1) INTERNET CLARO (wan2)	0.0.0.0/0.0.0				29	
INTERNET L3 (wan1)	Physical Interface		190.81.117.202/255.255.255.248	PING HTTPS SSH SNMP FMG-Access			11	
LAN	Hardware Switch	internal1 internal2 internal3	192.168.10.2/255.255.255.0	PING HTTPS SSH	21	192.168.10.150-192.168.10.249	28	
SEDES	Software Switch	internal4 internal5	172.16.1.2/255.255.255.0	PING HTTPS ccu			29	

INFORMACIÓN DE NAT

ninguna

Información relacionada a las reglas de NAT

N°	NOMBRE NAT	IP PÚBLICA	IP PRIVADA	PUERTO DESTINO	DESCRIPCIÓN
Name	Details	Interfaces	Services	Ref.	
IPv4 Virtual IP					
WebCam	190.81.117.203 → 172.16.3.251	INTERNET L3 (wan1)	2		
Terminal Server	190.81.117.204 → 172.16.1.6	INTERNET L3 (wan1)	2		
RDP_server	190.81.117.205 → 172.16.1.3	INTERNET L3 (wan1)	0		

INFORMACIÓN DE GRUPO DE USUARIOS

Información relacionada a los grupos de usuarios (que serán usadas en las políticas de seguridad)

N°	NOMBRE DE GRUPO	IP INICIO	IP FIN	EXCEPCIONES	DESCRIPCIÓN
ninguno					

INFORMACIÓN DE SERVICIOS PÚBLICOS

Información relacionadas a los servicios publicados por el cliente.

N°	NOMBRE SERVIDOR	IP INICIO	IP FIN	PUERTO TCP/UDP	DESCRIPCIÓN

POLITICAS DE SEGURIDAD

Inspección del estado de las conexiones de red y sus propiedades como source address, source port, destination address, destination port, protocolo de transmisión entre otras.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
10	PUBLICACIONES 2	all	Terminal Server WebCam	always	ALL	ACCEPT	Disabled	high_security certificate-inspection	All	0 B
11	PUBLICACIONES	all	Terminal Server WebCam	always	ALL	ACCEPT	Disabled	high_security certificate-inspection	All	11.25 GB
25	Bloqueo mywork.chc.net	all	mywork.chc.net	always	ALL	DENY			All	0 B
20	prueba	192.168.10.140	all	always	ALL	ACCEPT	Enabled	AV_BREXIA WF_GERENCIA AP_GERENCIA protect_client certificate-inspection	All	0 B
36	LIBRE NAVEGACION 2	all	all	always	ALL	ACCEPT	Enabled	AV_BREXIA certificate-inspection	All	85.05 GB
32	LIBRE NAVEGACIÓN	IP_192.168.10.157	all	always	ALL	ACCEPT	Enabled	AV_BREXIA certificate-inspection	All	0 B
24	FTP innovexplo	192.168.10.140	all	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
17	ANTIVIRUS	all	AVAST_23.194.17.11 ESET1_91.228.167.128 ESET2_91.228.166.47 KASPERSKY1_69.164.25.144 KASPERSKY2_69.164.26.173 SYMANTEC1_155.64.16.51 SYMANTEC2_155.64.49.54 ESET3_91.228.166.14	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
16		all	files.mycloud.com mycloud.com	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
14	nas	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
7	DISPOSITIVOS GERENTES	all	all	always	ALL	ACCEPT	Enabled	AV_BREXIA WF_GERENCIA AP_GERENCIA protect_client certificate-inspection	All	0 B
27		IP_192.168.10.138	all	always	ALL	ACCEPT	Enabled	AV_BREXIA LIBRE LIBRE protect_client certificate-inspection	All	0 B
9	LIBRE	all	all	always	ALL	ACCEPT	Enabled	AV_BREXIA LIBRE LIBRE protect_client certificate-inspection	All	0 B
12	USUARIOS HORARIOS	all	all	horario	ALL	ACCEPT	Enabled	AV_BREXIA WF_HORARIOS AP_HORARIO protect_client certificate-inspection	All	0 B
4	USUARIOS	all	all	always	ALL	ACCEPT	Enabled	AV_BREXIA WF_DEFAULT AP_DEFAULT protect_client certificate-inspection	All	0 B

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
LAN → SEDES 1										
2		all	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	8.59 GB
LAN → VPN Prueba 1										
22	vpn_VPN Prueba_local	VPN Prueba_local	VPN Prueba_remote	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	UTM	0 B
LAN → VPN AREQUIPA 1										
39	LIMA - AREQUIPA	LAN_VPN_LIMA	LAN_VPN AREQUIPA	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	0 B
SEDES → INTERNET 10										
38	rpp.pe	all	rpp.pe	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	0 B
28	LIBRE NAVEGACION	GR_SIN_RESTRICCIONES IP_172.16.3.160	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	0 B
26	bloqueo mywork.chc.net	all	mywork.chc.net	always	ALL	✗ DENY			✓ All	0 B
15	Deny Geo	all	CHINA TAIWAN EGIPTO ICELAND ARABIASAUDITA NORUEGA THAILANDIA	always	ALL	✗ DENY			✓ All	37.55 kB
37	Whatsapp web	IP_172.16.2.132	all	always	ALL	✓ ACCEPT	Enabled	AV_AV_BREXIA APP WhatsappWeb SSL certificate-inspection	✓ All	0 B
35	YOUTUBE	all	IP_172.217.192.91 youtube 172.217.192.0/24	always	ALL	✓ ACCEPT	Enabled	AV_AV_BREXIA SSL certificate-inspection	✓ All	16.15 kB
33	office 365	all	Microsoft-Office365	always	Internet Service	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	67.53 MB

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
33	office 365	all	Microsoft-Office365	always	Internet Service	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	67.53 MB
21	ANTIVIRUS SEDES	all	AVAST_23.194.17.11 ESET1_91.228.167.1... ESET2_91.228.166.47 KASPERSKY1_69.16... KASPERSKY2_69.16... SYMANTEC1_155.6... SYMANTEC2_155.6... ESET3_91.228.166.14	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	0 B
19		all	files.mycloud.com mycloud.com	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	0 B
18	AudiCodec	AudioCodec1 AudioCodec2	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	✓ All	0 B
13	USER MINAS HORARIO	all	all	horario	ALL	✓ ACCEPT	Enabled	AV_AV_BREXIA WEB WF_HORARIOS APP AP_HORARIO IPS protect_client SSL certificate-inspection	✓ All	29.61 MB
29	MINA_ACCESO_RS	IP_172.16.2.151	all	always	ALL	✓ ACCEPT	Enabled	AV_AV_BREXIA WEB WF_CELULARES_M... APP AC_CELULARES_M... IPS protect_client SSL certificate-inspection	✓ All	0 B
5	USER MINAS	all	all	always	ALL	✓ ACCEPT	Enabled	AV_AV_BREXIA WEB WF_CELULARES_M... APP AC_CELULARES_M... IPS protect_client SSL certificate-inspection	✓ All	4.69 GB

SEDES → LAN 1										
3		all	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	15.95 MB
SEDES → VPN AREQUIPA 1										
41	LIMA → AREQUIPA	LAN_VPN_LIMA	LAN_VPN AREQUIPA	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	249.45 MB
SEDES → VPN CUSCO 1										
42		LAN_VPN_LIMA	LAN_VPN_CUSCO	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	255.53 MB
SSL-VPN tunnel interface (ssl.root) → LAN 1										
30	VPNSSL to LAN	all USERS_VPNSSL	LAN	always	ALL	✓ ACCEPT	Disabled	AV_AV_BREXIA SSL certificate-inspection	✓ All	187.18 MB
SSL-VPN tunnel interface (ssl.root) → SEDES 1										
31	VPN SSL to SEDES	all USERS_VPNSSL	SEDES1 SEDES2 SEDES3	always	ALL	✓ ACCEPT	Disabled	AV_AV_BREXIA SSL certificate-inspection	✓ All	367.38 MB
VPN Prueba → LAN 1										
23	vpn_VPN Prueba_remote	VPN Prueba_remote	VPN Prueba_local	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VPN AREQUIPA → SEDES 1										
40	AREQUIPA-LIMA	LAN_VPN AREQUIPA	LAN_VPN_LIMA	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	101.10 MB
VPN CUSCO → SEDES 1										
43		LAN_VPN_CUSCO	LAN_VPN_LIMA	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	✓ All	95.34 MB
Implicit 1										

FILTRADO DE URL (VER ANEXO B)								
Permite controlar el uso del Internet previniendo el acceso a contenido WEB inapropiado. Se puede bloquear o permitir el acceso a paginas WEB por URL o por categoría predefinida.								
N°		APLICACIONES PREDEFINIDAS		VIP	MEDIO	BASICO		
Name ⇅		Comments ⇅		Ref. ⇅				
 LIBRE				2				
 WF_CELULARES_MINA				1				
 WF_CELULARES_MINA_RS				1				
 WF_DEFAULT		default web filtering		1				
 WF_GERENCIA				2				
 WF_HORARIOS				2				
 default		default web filtering		0				
 flow-monitor-all		monitor and log all visited URLs, flow based		0				
 monitor-all		monitor and log all visited URLs, proxy based		0				
 web-filter-flow		flow-based web filter profile		0				
 wifi-default		Default configuration for offloading WiFi traffic.		1				
FILTRADO DE APLICACIONES (VER PESTAÑA - ANEXO A)								
Para controlar aplicaciones evasivas que no son detectadas por un Firewall estándar que funciona en capa 3 o en capa4, que permite un control a través de la capa 7 (OSI) en la que se inspecciona el contenido real de la carga útil.								
Name ⇅		Comments ⇅		Ref. ⇅	MEDIO	BASICO		
 AC_CELUIARES_MINA				1				
 AC_CELULARES_MINA_RS				1				
 AP_DEFAULT		monitor all applications		1				
 AP_GERENCIA				2				
 AP_HORARIO		monitor all applications		2				
 LIBRE				2				
 WhatsappWeb				1				
 block-high-risk				0				
 block-p2p				0				
 default		monitor all applications		0				
 monitor-p2p-and-media				0				
 wifi-default		Default configuration for offloading WiFi traffic.		1				
FILTRADO DE ANTIVIRUS								
Primera contención de malware proveniente de Internet, solución que consulta a la nube de SOPHOS, inspecciona protocolos HTTP, HTP, SMTP, IMAP y POP3 y podrá ser habilitado/deshabilitado en cada política según la necesidad								
Name ⇅		Comments ⇅		Ref. ⇅	SERVICIOS	ACCIÓN		
 AV_flow		flow based scan and delete virus		0				
 AV_BREXIA		scan and delete virus		15				
 default		scan and delete virus		0				
 wifi-default		Default configuration for offloading WiFi traffic.		1				
FILTRADO DE ANTISPAM								
Examina los mensajes de correo electronico para identificar cuales son SPAMs y bloquearlos. Funciona como un complemento al servidor ANTISPAM dedicado del cliente. Nota: El perfil de inspección solo considerará el servicio								
N°		NOMBRE REGLA	IP SERV CORREO	IP SERV ANTISPAM	SERVICIO	DESCRIPCIÓN		
1								
FILTRADO DE CONTENIDOS								
Permite o bloquea cierto tipo de tráfico basado en: Tipo de MIME, extensión de archivo, Listas de comandos permitidos y denegados.								
N°		NOMBRE REGLA	RANGO IP	EXTENSION ARCHIVO	SERVICIO	ACCIÓN		
1								
FILTRADO DE GEO-IP								
IP-based Geolocation (GeoIP) es el mapeo de una dirección IP con la ubicación geográfica de un dispositivo conectado a Internet. Permite filtrar tráfico hacia y desde regiones específicas del mundo.								
N°		NOMBRE REGLA	PAISES A BLOQUEAR		DESCRIPCIÓN			
1								
FILTRADO DE SANDBOXING								
Los archivos sospechosos son ejecutados y analizados en un ambiente seguro, generalmente en maquinas virtuales con herramientas de análisis. Los archivos son cargados a estos sistemas y ejecutados por varios minutos, una vez								
N°		NOMBRE REGLA	RANGO IP	SERVICIO	DESCRIPCIÓN			
1								
ANTIDOS LITE								
Previene los ataques de negación de servicio basado en umbrales								
HABILITAR IPS								
N°		NOMBRE REGLA	IP ORIGEN	IP DESTINO	SERVICIOS	ACCIÓN		
Name ⇅		Comments ⇅		Ref. ⇅				
 all_default		all predefined signatures with default setting		0				
 all_default_pass		all predefined signatures with PASS action		0				
 default		prevent critical attacks		0				
 high_security		Blocks all Critical/High/Medium and some Low severity vulnerabilities		2				
 protect_client		protect against client-side vulnerabilities		9				
 protect_email_server		protect against EMail server-side vulnerabilities		0				
 protect_http_server		protect against HTTP server-side vulnerabilities		0				
 wifi-default		Default configuration for offloading WiFi traffic.		1				
HABILITAR C&C - ANTIMALWARE								
Command-and-control (C&C) server. Como sugiere el propio nombre, los servidores de comando y control se utilizan para enviar remotamente comandos malintencionados a una red de bots, o una red comprometida de								
N°		NOMBRE REGLA	IP ORIGEN	IP DESTINO	SERVICIOS	ACCIÓN		

VPN site to site - Client to Site									
Indicar la cantidad de VPN Site to Site y Client to Site que efectua en el Firewall.									
N°	NOMBRE REGLA		IP ORIGEN		IP DESTINO		SERVICIOS	ACCIÓN	
41	LIMA->AREQUIPA	LAN_VPN_LIMA	LAN_VPN_AREQUIPA	always	ALL	ACCEPT Disabled no-inspection	All	249.81 MB	
42	SEDES->VPN_CUSCO	LAN_VPN_LIMA	LAN_VPN_CUSCO	always	ALL	ACCEPT Disabled no-inspection	All	255.67 MB	
30	VPNSSL to LAN	all USERS_VPNSSL	LAN	always	ALL	ACCEPT Disabled AV_BREXIA certificate-inspection	All	187.18 MB	
31	VPN SSL to SEDES	all USERS_VPNSSL	SEDES1 SEDES2 SEDES3	always	ALL	ACCEPT Disabled AV_BREXIA certificate-inspection	All	367.38 MB	
23	vpn_VPN Prueba_remote	VPN Prueba_remote	VPN Prueba_local	always	ALL	ACCEPT Disabled no-inspection	U	0 B	
40	AREQUIPA-LIMA	LAN_VPN_AREQUIPA	LAN_VPN_LIMA	always	ALL	ACCEPT Disabled no-inspection	All	101.14 MB	
43	VPN CUSCO->SEDES	LAN_VPN_CUSCO	LAN_VPN_LIMA	always	ALL	ACCEPT Disabled no-inspection	All	95.62 MB	
Indicar otras características que deberá considerar el servicio									
Name	Read Only	Comments		Ref.					
BrexiaCor_SSL				0					
Brexia_SSL				0					
certificate-inspection		SSL handshake inspection.		17					
custom deep-inspection		Customizable deep inspection profile.		0					
deep-inspection		Read-only deep inspection profile.		0					
no-inspection		Read-only profile that does no inspection.		19					

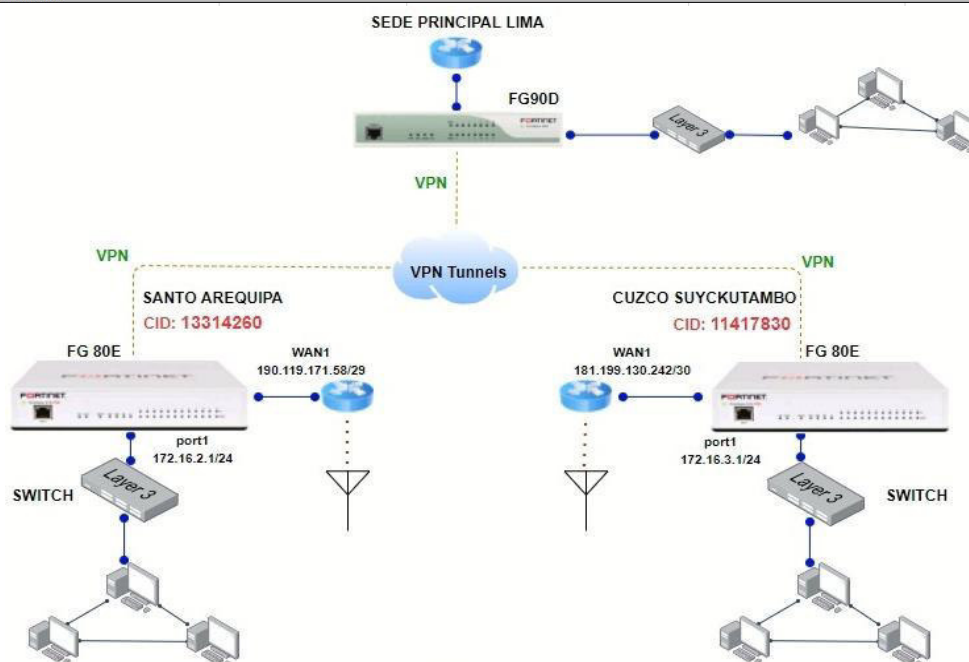
Claró

Solución a la Medida

NOMBRE DEL PROVEEDOR		Desyareb	SOT en donde se carga la documentación		42196689									
* Toda la prueba la realiza el proveedor														
1.1 - ALCANCE DEL SERVICIO Y SOPORTE POST VENTA DEL PROVEEDOR.														
* En caso, el servicio esta bajo el alcance del gestionado, dejar en blanco columna 8.														
OC / POS	Alcance del servicio		Equipo sobre el cual se da el servicio		Fecha inicio del servicio		Fecha fin del servicio		SOT Instalación	CID				
6500423825 / 020	INSTALACIÓN DE FIREWALL		Fortigate 80E		6/05/2021		6/05/2024		42196689	13314260				
6500414961 / 050	SOPORTE PROVEEDOR X 12 MESES		Fortigate 80E		6/05/2021		6/05/2024		42196689	13314260				
6500414961 / 060	SOPORTE PROVEEDOR X 12 MESES (FORTIANALYZER CLOUD - COLECCIÓN DE LOGS Y REPORTES)		FORTIANALYZER CLOUD		6/05/2021		6/05/2024		42196689	13314260				
1.2 - LICENCIAS Y GARANTIAS POST VENTA DEL PROVEEDOR.														
Nombre Licencia o Garantía		Origen de serie del equipo	OC (Si es no es recurrente)		POS		SOT		CID	Fecha Inicio	Fecha Fin	Observaciones		
Licencia		FG T80E TK-2000P4020	-		-		42196689		13314260					
Garantía		FG T80E TK-2000P4020	-		-		42196689		13314260					
1.3 - CONDICIONES DE DESPLAZAMIENTO DEL PROVEEDOR.														
Caída total de servicio (Severidad 1)														
1.3 - SIA BRINDA EL PROVEEDOR														
NIVEL DE CRITICIDAD														
NIVEL 1 (Suspension total de NIVEL 2) (Inoperatividad parcial del servicio), NIVEL 3 (No hay perdida del servicio)														
Tiempo de respuesta		4 horas	4 horas		4 horas		4 horas		4 horas	4 horas	4 horas	4 horas		
Tiempo para responder equipos / desplazamiento		48 horas	48 horas		48 horas		48 horas		48 horas	48 horas	48 horas	48 horas		
Tiempo de solución		4 horas	4 horas		4 horas		4 horas		4 horas	4 horas	4 horas	4 horas		
Tiempo entrega de informe técnicos		24 horas	24 horas		24 horas		24 horas		24 horas	24 horas	24 horas	24 horas		
1.4 - EQUIPOS SPARE														
Descripción (Modelo / Cantidades)		Necesita licencia para funcionamiento		Número de Serie		Ubicación (Proveedor, Cliente)		Observación (Velocidad, versión, FMA, soporte de fabrica, etc.)						
SI - Claro						Claro								

1.5 - PREVENTIVO				
Incluye Preventivo	Periodo de los preventivos (Mensual, cada 6 meses, anual)	ALCANCE DEL PREVENTIVO (equipo, gabinete, pozos a tierra, energía, etc)	Equipos que se ejecutará preventivo	Observaciones
Si	Anual	Equipo	Equipo Firewall	No se abrirá el equipo del cliente, pero se validará el estado de LEDs, actualización a la versión del sistema operativo recomendada por el fabricante y verificación de memoria, CPU almacenamiento de equipo.
1.6 - PRUEBAS Y REPORTES DE ENTREGA DEL SERVICIO				
1. Protocolo de Pruebas. 2. Prueba de servicios externos. 3. Prueba de acceso. 4. Prueba de VPN y conectividad entre sedes.				
1.7- TOPOLOGÍA (Identificar servicios existentes por CID, detallar modelo de equipos, IP, anchos de banda por enlace, medios de transmisión (Fibra y cu), tipo del puerto (G, Eth), en que puerto se esta conectando cada equipo , la propiedad del cableado o equipos si pertenece a Claro o al cliente, en caso de que Claro lo ha colocado que proveedor ejecuta el soporte)				

Topología del servicio



1.8 - SERVICIOS NO INCLUIDOS

- Enumerar que servicios no se encuentran incluidos en la atención del proyecto, por ejemplo :
1. Reparación de equipos X
 2. Monitoreo de equipos en sitio X
 3. Desinstalación o reinstalación del equipo (Previa coordinación con el cliente en caso amerite)
 4. Limpieza exterior X
 5. La operación misma de los sistemas X
 6. Respaldo de la información X 77, Gruas
 7. Gruas
 8. Remoción de blacklist.

A llenar por proveedor

GESTIÓN INTERNA -

Cantidad de Enlaces	Claro		
Ancho de Banda	15 - 8 MB		
Marca/Modelo del Equipo	FortiGate 80E		
Sistema Operativo de Equipo FW	v6.2.4		
Nueva Implementación/Migración Firewall	Implementacion	No Aplica	
Cliente tiene Gestión de FW	(X) SI : NO:X	Lectura :	Escritura:
Se valido Gestión Interna y Remota	(X) SI : X NO:		
Puerta de Enlace (Router) :	190.119.171.57		
IP privada asignada al FW :	190.119.171.58		
Puerta de Enlace (Router) :	181.199.130.241		
IP privada asignada al FW :	181.199.130.242		
Puerto que conecta al SW - CPE	WAN G0/0 - LAN G0/1		
Velocidad / Duplex de la Interfaz:	WAN:1000/Full Duplex- LAN:1000/Full		
Servidor DNS :	8.8.4.4/4.4.4.4		

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

admin

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Antivirus

Web Filter

DNS Filter

Application Control

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

WAN1

LAN

Interfaces

Create New

Edit

Delete

Search

Group By Type

Name	Type	Members	IP/netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
Hardware Switch							
lan	Hardware Switch	port1 port2 port3 port4	172.16.2.1/255.255.255.0		PING HTTPS SSH	76	172.16.2.2-172.16.2.254
Physical Interface							
CLARO_AREQUIPA(wan1)	Physical Interface		190.119.174.50/255.255.255.248		PING HTTPS SSH SNMP HTTP		
dmz	Physical Interface		10.10.10.1/255.255.255.0		PING HTTPS HTTP RMS-Access Security Fabric Connection		
ha	Physical Interface		0.0.0.0/0.0.0.0				
port11	Physical Interface		0.0.0.0/0.0.0.0				
RED-WIFI(port12)	Physical Interface		192.168.0.1/255.255.255.0		PING HTTPS		192.168.0.2-192.168.0.254

INFORMACIÓN DE GRUPO DE USUARIOS

Create New

Edit

Clone

Delete

Search

Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (SSO)		1

POLÍTICAS DE SEGURIDAD

Create New

Edit

Delete

Policy Lookup

Search

Interface Pair View

By Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
lan	CLARO_AREQUIPA(wan1)									
lan	VPN_CUZCO									
lan	VPN_LIMA									
RED-WIFI(port12)	CLARO_AREQUIPA(wan1)									
VPN_CUZCO	lan									
VPN_LIMA	lan									
Implicit										

FILTRADO DE URL

Create New

Edit

Clone

Delete

Search

Name	Comments	
WF_ESTANDARD		0
WF_ESTANDARD_WIFI		0
default	Default web filtering.	0
monitor-all	Monitor and log all visited URLs, flow-based.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

FILTRADO DE APLICACIONES

Create New

View

Clone

Delete

Search

Name	Comments	
AC_ESTANDARD		0
AC_ESTANDARD_WIFI		0
block-high-risk		0
default	Monitor all applications.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

AntiVirus

Create New

Edit

Clone

Delete

Search

FILTRADO DE ANTIVIRUS

Name	Comments	
default	Scan files and block viruses.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

Create New

Edit

Clone

Delete

Search

VPN site to site - Client to Site

Tunnel	Interface Binding	Status	
Custom			
VPN_CUZCO	CLARO_AREQUIPA (wan1)	Up	4
VPN_LIMA	CLARO_AREQUIPA (wan1)	Up	4

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

VPN Location Map

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit VPN Tunnel

Name

VPN_CUZCO

Comments

Comments

0/255

Network

Edit

Remote Gateway : Static IP Address (181.199.130.242) , Local Gateway: 190.119.171.58, Interface : wan1

Authentication

Edit

Authentication Method : Pre-shared Key

IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal

Edit

Algorithms : AES256-SHA384

Diffie-Hellman Groups : 14, 5

XAUTH

Edit

Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address	
VPN_CUZCO	LAN_VPN_AREQUIPA	LAN_VPN_CUZCO	

Add

FortiGate 80E

CLARO_AREQUIPA_EL_SANTO

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Device
WiFi & Switch Controller
Log & Report
Monitor

Edit VPN Tunnel

Name

VPN_LIMA

Comments

Comments

0/255

Network

Remote Gateway : Static IP Address (190.81.117.202) , Local Gateway: 190.119.171.58, Interface : wan1

Edit

Authentication

Authentication Method : Pre-shared Key

IKE Version : 1 , Mode : Main (ID protection)

Edit

Phase 1 Proposal

Algorithms : AES256-SHA384

Diffie-Hellman Groups : 14, 5

Edit

XAUTH

Type : Disabled

Edit

Phase 2 Selectors

Name	Local Address	Remote Address
VPN_LIMA	LAN_VPN_AREQUIPA	LAN_VPN_LIMA

Add

FORTIANALIZER CLOUD									
☐	Device Name	IP Address	Platform	Logs					
☐	FG80E_AMG_AUPLATA_AREQUIPA	190.119.171.58	FortiGate-80E	Real Time					
☐	FG80E_AMG_AUPLATA_CUZCO	181.199.130.242	FortiGate-80E	Real Time					

LOG ALMACENADOS									
FG80E_AMG_AUPLATA_AREQUIPA									
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Ap...	Sent/Received
1	13:08:20	FGT80ETH20005020	✓	172.16.2.55		179.6.60.33	HTTPS		19.9 KB/814.9 ...
2	13:08:20	FGT80ETH20005020	✓	AGH02-008PC		192.163.142.9	DNS		100.0 B/188.0 B
3	13:08:20	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		71.0 B/144.0 B
4	13:08:19	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		0 B/0 B
5	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		34.107.165.5	HTTPS		1.9 KB/1.4 KB
6	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		142.250.64.202	HTTPS		2.2 KB/2.5 KB
7	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		34.107.165.5	HTTPS		3.0 KB/1.6 KB
8	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		142.250.64.202	HTTPS		3.3 KB/2.6 KB
9	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		157.240.197.17	HTTP		1.1 KB/402.0 B
10	13:08:19	FGT80ETH20005020	✓	PLN02-008PC		34.107.165.5	HTTPS		2.8 KB/1.5 KB
11	13:08:19	FGT80ETH20005020	✓	AGH02-006PC.bgp...		52.177.166.224	HTTPS		7.3 KB/12.4 KB
12	13:08:19	FGT80ETH20005020	✓	172.16.2.2		90.119.6.149	IKE		16.3 KB/7.7 KB
13	13:08:19	FGT80ETH20005020	✓	PLN03-004PC.bgp...		36.90.215	HTTPS		3.9 KB/6.0 KB
14	13:08:18	FGT80ETH20005020	✓	PLN02-008PC		34.107.165.5	HTTPS		3.0 KB/1.6 KB
15	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		108.177.11.188	tcp/5228		1.2 KB/4.8 KB
16	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		13.107.18.11	HTTPS		64.0 KB/423.2 ...
17	13:08:18	FGT80ETH20005020	✓	AGH02-008PC		192.163.142.9	DNS		66.0 B/164.0 B
18	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		62.0 B/107.0 B
19	13:08:18	FGT80ETH20005020	✓	GLG03-004PC		8.4.4	DNS		251.0 B/148.0 B
20	13:08:18	FGT80ETH20005020	✓	GLG03-004PC		8.4.4	DNS		0 B/0 B
21	13:08:18	FGT80ETH20005020	✓	AGH02-008PC		192.163.142.9	DNS		100.0 B/268.0 B
22	13:08:18	FGT80ETH20005020	✓	PLN02-008PC		34.107.165.5	HTTPS		2.8 KB/1.4 KB
23	13:08:18	FGT80ETH20005020	✓	GLG03-004PC		8.8.8	DNS		75.0 B/148.0 B
24	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		70.0 B/143.0 B
25	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		0 B/0 B
26	13:08:18	FGT80ETH20005020	✓	GLG03-004PC		8.8.8	DNS		0 B/0 B
27	13:08:18	FGT80ETH20005020	✓	SSO03-004PC		8.8.8	DNS		74.0 B/147.0 B

Solución a la Medida

NOMBRE DEL PROVEEDOR		SOT en donde se carga la documentación	
Desysweb		42196618	

Toda la gestión la realiza el proveedor

1.1 - ALCANCE DEL SERVICIO Y SOPORTE POST VENTA DEL PROVEEDOR.

En caso, el servicio está bajo el alcance del gestionado, dejar en blanco columna B.

OC / POS	Alcance del servicio	Equipo sobre el cual se da el servicio	Fecha inicio del servicio	Fecha fin del servicio	SOT Instalación	CD
4500422825 / 020	INSTALACIÓN DE FIREWALL	Fortigate 80E	8/05/2021	8/05/2024	42196618	13417830
4500414961 / 020	SOPORTE PROVEEDOR X 12 MESES	Fortigate 80E	8/05/2021	8/05/2024	42196618	13417830
4500414961 / 030	SOPORTE PROVEEDOR X 12 MESES (FORTIANALYZER CLOUD - COLECCIÓN DE LOGS Y DE PUENTES)	FortiAnalyzer Cloud	8/05/2021	8/05/2024	42196618	13417830

1.2 - LICENCIA Y GARANTÍA POST VENTA DEL PROVEEDOR.

Nombre Licencia o Garantía	no de serie del equipo	OC (SI es no es recurrente)	POS	SOT	CD	Fecha Inicio	Fecha Fin	Observaciones
Licencia	FGT80E-TK19007309	-	-	42196618	13417830			
Garantía	FGT80E-TK19007309	-	-	42196618	13417830			

1.3 - CONDICIONES DE DESPLAZAMIENTO DEL PROVEEDOR.

Caída total del servicio (Severidad 1)

1.3 - SLA BRINDA EL PROVEEDOR

NIVEL DE CRÍTICIDAD			
	NIVEL 1 (Suspensión total de APEX)	NIVEL 2 (Operatividad parcial del servicio)	NIVEL 3 (No hay pérdida del servicio)
Tiempo de respuesta	4 Horas	4 Horas	4 Horas
Tiempo para reponer equipos / desplazamiento	48 Horas	48 Horas	N/A
Tiempo de solución	4 Horas	8 Horas	8 Horas
Tiempo entrega de informe técnico	24 Horas	24 Horas	N/A

1.4 - EQUIPOS SPARE

Descripción (Modelo / Cantidad)	Necesita licencia para funcionamiento	Número de Serie	Ubicación (Proveedor)	Observación (Velocidad, versión, FMA, soporte de fábrica, etc.)
SI - Claro	-	-	Claro	-

1.5 - PREVENTIVO

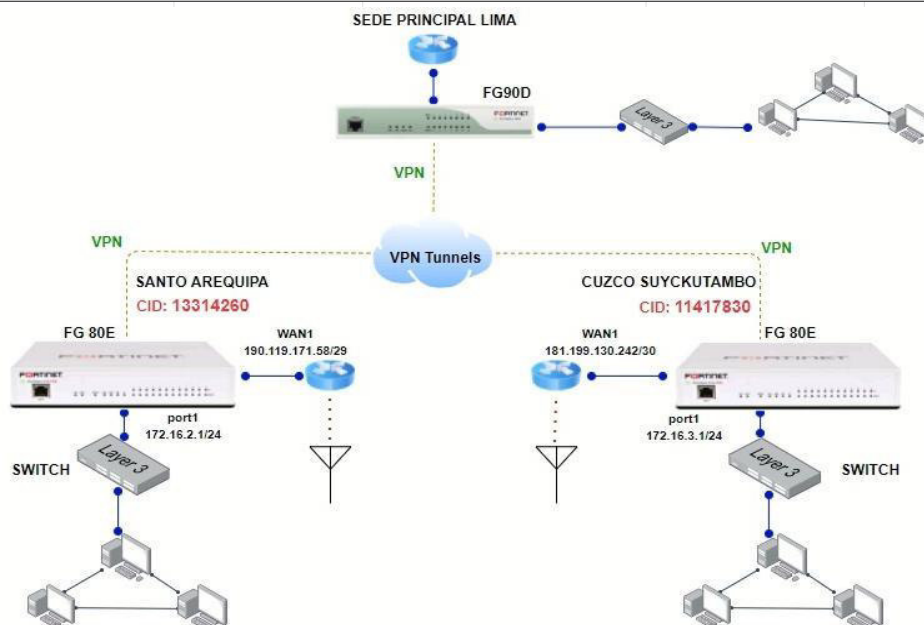
Incluye Preventivo	Periodo de los preventivos (Mensual, cada 6 meses, anual)	ALCANCE DEL PREVENTIVO (equipo, gabinete, pozos a tierra, energía, etc)	Equipos que se ejecutará preventivo	Observaciones
SI	Anual	Equipo	Equipo Firewall	No se abrirá el equipo del cliente, pero se validará el estado de LEDs, actualización a la versión del sistema operativo recomendada por el fabricante y verificación de memoria, CPU almacenamiento de equipo.

1.6 - PRUEBAS Y REPORTES DE ENTREGA DEL SERVICIO

- Protocolo de Pruebas.
- Prueba de servicios externos.
- Prueba de acceso.
- Prueba de VPN y conectividad entre sedes.

1.7- TOPOLOGÍA (Identificar servicios existentes por CID, detallar modelo de equipos, IP, anchos de banda por enlace, medios de transmisión (Fibra y cu), tipo del puerto (Gi, Eth), en que puerto se esta conectando cada equipo , la propiedad del cableado o equipos si pertenece a Claro o al cliente, en caso de que Claro lo ha colocado que proveedor ejecuta el soporte)

Topología del servicio



Enumerar que servicios no se encuentran incluidos en la atención del proyecto, por ejemplo :

1. Reparación de equipos X
2. Monitoreo de equipos en sitio X
3. Desinstalación o reinstalación del equipo (Previa coordinación con el cliente en caso amerite)
4. Limpieza exterior X
5. La operación misma de los sistemas X
6. Respaldos de la información X 77, Gruas
7. Gruas
8. Remoción de blacklist.

A llenar por proveedor

GESTIÓN INTERNA -

Cantidad de Enlaces	Claro
Ancho de Banda	15 - 8 MB
Marca/Modelo del Equipo	FortiGate 80E
Sistema Operativo de Equipo FW	v6.2.4
Nueva Implementación/Migración Firewall	Implementación
Cliente tiene Gestión de FW	(X) SI : NO:X
Se valido Gestión Interna y Remota	(X) SI : X NO:
Puerta de Enlace (Router) :	190.119.171.57
IP privada asignada al FW :	190.119.171.58
Puerta de Enlace (Router) :	181.199.130.241
IP privada asignada al FW :	181.199.130.242
Puerto que conecta al SW - CPE	WAN G0/0 - LAN G0/1
Velocidad / Duplex de la Interfaz:	WAN:1000/Full Duplex- LAN:1000/Full
Servidor DNS :	8.8.4.4/4.4.4.4

INFORMACIÓN DE RED

FortiGate 80E CLARO_CUZCO_SUYCKUTAMBO									
Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges		
lan	Hardware Switch	port1 port2 port3 port4	172.16.3.1/255.255.255.0		PING HTTPS SSH	65	172.16.3.2-172.16.3.254		
CLARO_CUZCO (wan1)	Physical Interface		181.199.130.242/255.255.255.252		PING HTTPS SSH SNMP HTTP				
dmz	Physical Interface		10.10.10.1/255.255.255.0		PING HTTPS HTTP FMG-Access Security Fabric Connection				
ha	Physical Interface		0.0.0.0/0.0.0.0						
port11	Physical Interface		0.0.0.0/0.0.0.0						
RED-WIFI (port12)	Physical Interface		192.168.0.1/255.255.255.0		PING HTTPS	17	192.168.0.2-192.168.0.254		

INFORMACIÓN DE GRUPO DE USUARIOS			
Create New Edit Clone Delete Search			
Group Name	Group Type	Members	Ref
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

POLÍTICAS DE SEGURIDAD																																																																																																													
FortiGate 80E CLARO_CUZCO_SUYCKUTAMBO Q admin																																																																																																													
Dashboard Security Fabric FortiView Network System Policy & Objects IP4 Policy Authentication Rules Addresses Internet Service Database Services Schedules	Create New Edit Clone Delete Q Policy Lookup Search Q Interface Pair View By Sequence <table> <tr> <th>ID</th><th>Name</th><th>Source</th><th>Destination</th><th>Schedule</th><th>Service</th><th>Action</th><th>NAT</th><th>Security Profiles</th><th>Log</th><th>Bytes</th></tr> <tr> <td>lan →</td><td>CLARO_CUZCO (wan1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>lan →</td><td>VPN_AREQUIPA</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>lan →</td><td>VPN_LIMA</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>RED-WIFI (port12) →</td><td>CLARO_CUZCO (wan1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>RED-WIFI (port12) →</td><td>lan</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>VPN_AREQUIPA →</td><td>lan</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>VPN_LIMA →</td><td>lan</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>Implicit</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>										ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	lan →	CLARO_CUZCO (wan1)										lan →	VPN_AREQUIPA										lan →	VPN_LIMA										RED-WIFI (port12) →	CLARO_CUZCO (wan1)										RED-WIFI (port12) →	lan										VPN_AREQUIPA →	lan										VPN_LIMA →	lan										Implicit										
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes																																																																																																			
lan →	CLARO_CUZCO (wan1)																																																																																																												
lan →	VPN_AREQUIPA																																																																																																												
lan →	VPN_LIMA																																																																																																												
RED-WIFI (port12) →	CLARO_CUZCO (wan1)																																																																																																												
RED-WIFI (port12) →	lan																																																																																																												
VPN_AREQUIPA →	lan																																																																																																												
VPN_LIMA →	lan																																																																																																												
Implicit																																																																																																													

FILTRADO DE URL

FortiGate 80E

CLARO_CUZCO_SUYCKUTAMBO

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

AntiVirus

Web Filter

DNS Filter

Create New

Edit

Clone

Delete

Search

Name	Comments	
WF_ESTANDARD		0
WF_ESTANDARD_WIFI		0
default	Default web filtering.	0
monitor-all	Monitor and log all visited URLs, flow-based.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

FILTRADO DE APLICACIONES

FortiGate 80E

CLARO_CUZCO_SUYCKUTAMBO

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

Web Application Firewall

Create New

View

Clone

Delete

Search

Name	Comments	
AC_STANDARD		0
AC_STANDARD_WIFI		0
block-high-risk		0
default	Monitor all applications.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

FILTRADO DE ANTIVIRUS

FortiGate 80E CLARO_CUZCO_SUYCKUTAMBO

Dashboard > [+ Create New](#) [Edit](#) [Clone](#) [Delete](#)

Name	Comments	
AV default	Scan files and block viruses.	0
AV wifi-default	Default configuration for offloading WiFi traffic.	1

Security Fabric >
 FortiView >
 Network >
 System > 1
 Policy & Objects >
 Security Profiles >
 AntiVirus >

VPN site to site - Client to Site

FortiGate 80E CLARO_CUZCO_SUYCKUTAMBO

Dashboard > [+ Create New](#) [Edit](#) [Delete](#)

Tunnel	Interface Binding	Status	
Custom 2			
VPN_AREQUIPA	CLARO_CUZCO (wan1)	Up	4
VPN_LIMA	CLARO_CUZCO (wan1)	Up	4

Security Fabric >
 FortiView >
 Network >
 System > 1
 Policy & Objects >
 Security Profiles >
 VPN >
 Overlay Controller VPN >
 IPsec Tunnels >
 IPsec Wizard >

FortiGate 80E CLARO_CUZCO_SUYCKUTAMBO

Dashboard > Edit VPN Tunnel

Security Fabric >
 FortiView >
 Network >
 System > 1
 Policy & Objects >
 Security Profiles >
 VPN >
 Overlay Controller VPN >
 IPsec Tunnels >
 IPsec Wizard >
 IPsec Tunnel Template >
 SSL-VPN Portals >
 SSL-VPN Settings >
 VPN Location Map >
 User & Device >
 WiFi & Switch Controller >
 Log & Report >
 Monitor >

Name: VPN_AREQUIPA

Comments: 0/255

Network [Edit](#)

Remote Gateway : Static IP Address (190.119.171.58) , Local Gateway: 181.199.130.242,
Interface : wan1

Authentication [Edit](#)

Authentication Method : Pre-shared Key
IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal [Edit](#)

Algorithms : AES256-SHA384
Diffie-Hellman Groups : 14, 5

XAUTH [Edit](#)

Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address	
VPN_AREQUIPA	LAN_VPN_CUZCO	LAN_VPN_AREQUIPA	Add Edit

FortiGate 80E
CLARO_CUZCO_SUYCKUTAMBO

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Device
WiFi & Switch Controller
Log & Report
Monitor

Edit VPN Tunnel

Name: VPN_LIMA
Comments: Comments

Network
Remote Gateway : Static IP Address (190.81.117.202) , Local Gateway: 181.199.130.242, Interface : wan1

Authentication
Authentication Method : Pre-shared Key
IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal
Algorithms : AES256-SHA384
Diffie-Hellman Groups : 14, 5

XAUTH
Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address
VPN_LIMA	LAN_VPN_CUZCO	LAN_VPN_LIMA

FORTIANALIZER CLOUD									
☐	Device Name	IP Address	Platform	Logs					
☐	FG80E_AMG_AUPLATA_AREQUIPA	190.119.171.58	FortiGate-80E	Real Time					
☐	FG80E_AMG_AUPLATA_CUZCO	181.199.130.242	FortiGate-80E	Real Time					

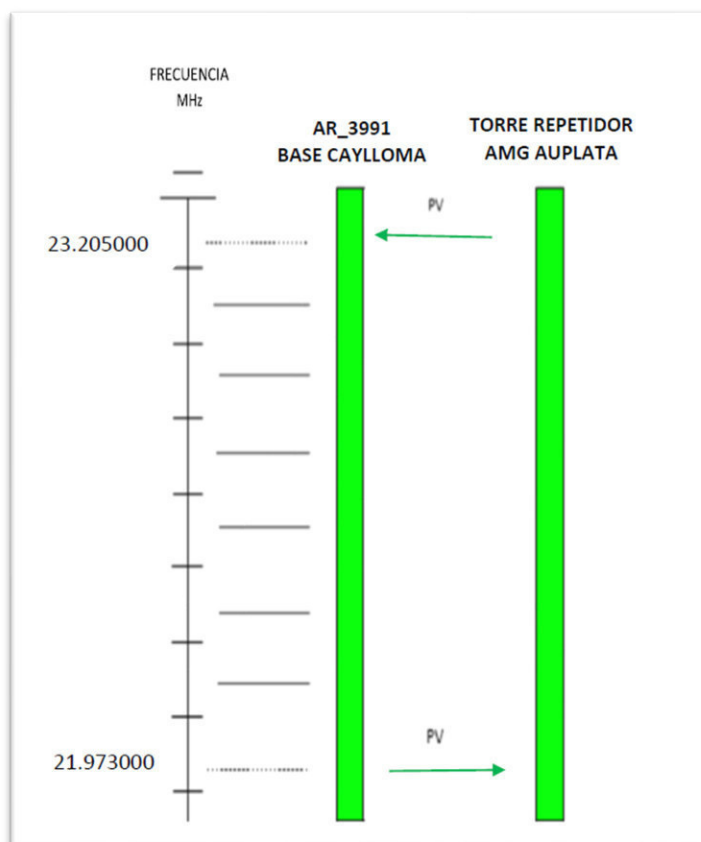
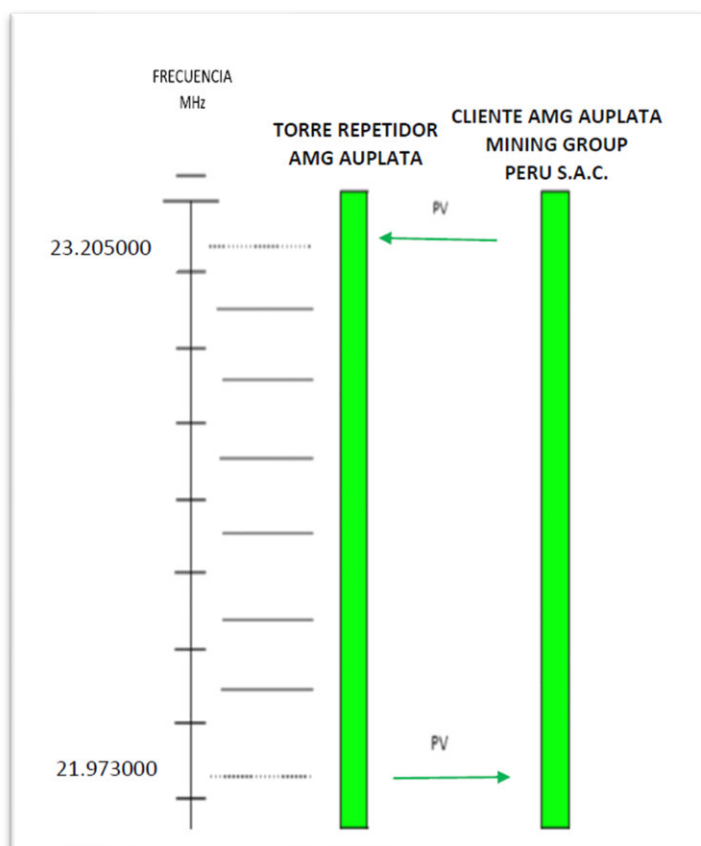
LOG ALMACENADOS									
FG80E_AMG_AUPLATA_CUZCO +									
Add Filter									
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Ap...	Sent/Received
1	13:08:37	FGT80ETK19007309	✓	SRV-MINA.bgpp.sr...		3.8.8.8	DNS		97.0 B/191.0 B
2	13:08:37	FGT80ETK19007309	✓	AMGSAN-0003...		157.240.197.15	HTTPS		100.0 B/124.0 B
3	13:08:37	FGT80ETK19007309	✓	AMGSAN-0003...		52.152.110.14	HTTPS		343.0 B/164.0 B
4	13:08:37	FGT80ETK19007309	✓	DESKTOP-TJC01L3		35.171.172.122	HTTPS		1.6 KB/944.0 B
5	13:08:37	FGT80ETK19007309	✓	DESKTOP-TJC01L3		47.9.112.100	udp/64943		262.0 B/0.0 KB
6	13:08:37	FGT80ETK19007309	✓	DESKTOP-TJC01L3		54.221.23.208	HTTPS		858.0 B/6.3 KB
7	13:08:37	FGT80ETK19007309	✓	DESKTOP-TJC01L3		47.9.112.100	udp/64943		262.0 B/0.0 KB
8	13:08:36	FGT80ETK19007309	✓	AMGSAN-0003...		172.217.162.74	HTTPS		2.3 KB/8.3 KB
9	13:08:36	FGT80ETK19007309	✓	DESKTOP-1HPM...		52.114.128.72	HTTPS		1.1 KB/6.7 KB
10	13:08:36	FGT80ETK19007309	✓	DESKTOP-TJC01L3		54.233.186.189	udp/443		16.6 KB/21.0 KB
11	13:08:36	FGT80ETK19007309	✓	AMGSAN-0003...		52.152.110.14	HTTPS		343.0 B/163.0 B
12	13:08:35	FGT80ETK19007309	✓	NAS-SUYCKUTAMB		120.239.118.159	udp/39482		446.0 B/416.0 B
13	13:08:35	FGT80ETK19007309	✓	AGH03-007PC		190.216.160.126	HTTP		408.0 B/1.4 KB
14	13:08:35	FGT80ETK19007309	✓	AGH03-007PC		190.216.160.126	HTTP		454.0 B/1.4 KB
15	13:08:34	FGT80ETK19007309	✓	DESKTOP-TJC01L3		54.221.23.208	HTTPS		698.0 B/6.1 KB
16	13:08:34	FGT80ETK19007309	✓	NAS-SUYCKUTAMB		120.239.118.159	udp/39482		446.0 B/416.0 B
17	13:08:34	FGT80ETK19007309	✓	DESKTOP-TJC01L3		157.240.14.35	HTTPS		729.0 B/2.6 KB
18	13:08:34	FGT80ETK19007309	✓	SSO02-001.bgpp.sr...		54.233.190.188	tcp/5228		15.9 KB/19.3 KB
19	13:08:34	FGT80ETK19007309	✓	NAS-SUYCKUTAMB		120.239.118.159	udp/39482		446.0 B/416.0 B
20	13:08:34	FGT80ETK19007309	✓	AMGSAN-0003...		52.152.110.14	HTTPS		343.0 B/164.0 B
21	13:08:34	FGT80ETK19007309	✓	HUAWEL Y6ll		157.240.197.34	HTTPS		3.3 KB/1.9 KB
22	13:08:34	FGT80ETK19007309	✓	LGC03-003PC.bg...		3.8.8.8	DNS		79.0 B/152.0 B
23	13:08:34	FGT80ETK19007309	✗ DNS error	LGC03-003PC.bg...		3.8.8.8	DNS		0 B/0 B
24	13:08:34	FGT80ETK19007309	✓	AGH03-007PC		3.8.8.8	DNS		73.0 B/146.0 B
25	13:08:34	FGT80ETK19007309	✗ DNS error	AGH03-007PC		3.8.8.8	DNS		0 B/0 B
26	13:08:34	FGT80ETK19007309	✓	DESKTOP-TJC01L3		35.241.56.184	HTTPS		1.0 KB/6.7 KB
27	13:08:34	FGT80ETK19007309	✓	DESKTOP-TJC01L3		54.233.190.113	HTTPS		1.0 KB/4.8 KB

❖ **CÁLCULO DE PROPAGACIÓN: HOP CONFIGURATION and PERFORMANCE**

SITE		SITE AR3991 CAYLLOMA			TORRE REPETIDOR CLIENTE AMG-AUPLATA					
		A (A)			B (B)					
1	LATITUDE	S 15°	10'	36.58"	S 15°	10'	15.30"			
2	LONGITUDE	W 71°	44'	53.53"	W 71°	49'	33.30"			
4	AZIMUTH	274°			94°					
5	ANTENNA TYPE	SB1-220CIPN			SB1-220CIPN			0.3x0.3		
6	FREQUENCY TX	23.205000 GHz			21.973000 GHz			54.00		
1	LINK TYPE	IP-205 23GHz, 32 QAM 53.870 Mbps								
7	POLARIZATION	VERTICAL								
8	ANTENNA HEIGHT	+ 30.0 m			+ 10.0 m					
9	EQUIPMENT	RF CENTRAL FREQUENCY						GHz	22.589	
10		TRANSMITTER POWER						dBm	20	
11	LINK	LINK DISTANCE						Km	8.36 Km	
12		FEEDER LENGTH AT A						m	0	
13		FEEDER LENGTH AT B						m	0	
14		FEEDER UNIT LOSS						dB/m	0	
15	GAINS	ANTENNA GAIN AT A						dB	34.06	
16		ANTENNA GAIN AT B						dB	34.06	
17		TOTAL GAIN						dB	68.1	
18	LOSSES	FREE SPACE						dB	137.92	
19		BY FLAT SURFACE						dB	0	
20		BY OBSTACLES						dB	0	
21		IN FEEDERS (A, B)						dB	0	
22		BRANCHING TX/RX						dB	1	
23		TOTAL						dB	138.92	
	LEVELS, INTERRUPTION TIME AND AVAILABILITY	LINK ATTENUATION						dB	70.80	
1		RX LEVEL WITHOUT FADING						dBm	-50.80	
2		THRESHOLD LEVEL (BER = 1E-3)						dBm	-81.00	
3		THRESHOLD LEVEL (BER = 1E-6)						dBm	-79.00	
4		FADING MARGIN (BER = 1 E-3)						dB	30.20	
5		FADING MARGIN (BER = 1 E-6)						dB	28.20	
7		OBJECTIVE INTERRUPTION TIME (BER = 1 E-3)						%	1.81.E-04	
8		OBJECTIVE INTERRUPTION TIME (BER = 1 E-6)						%	1.34.E-03	
9		FADING DEPTH (BER = 1 E-3)						dB	37.85	
10		FADING DEPTH (BER = 1 E-6)						dB	29.16	
11		RX LEVEL WITH FADING (BER = 1 E-3)						dBm	-88.65	
12		RX LEVEL WITH FADING (BER = 1 E-6)						dBm	-79.96	
13		REAL INTERRUPTION TIME (BER = 1 E-3)						%	1.05.E-03	
14		REAL INTERRUPTION TIME REAL (BER = 1 E-6)						%	1.67.E-03	
15		AVAILABILITY (BER = 1 E-6)						%	99.99833177	
16		ANNUAL REAL INTERRUPTION TIME						s	331.9400	
UIT - R OBJECTIVES HIGH GRADE									No Cumple	

SITE		TORRE REPETIDOR CLIENTE AMG-AUPLATA			CLIENTE AMG-AUPLATA MINING GROUP PERU S.A.C				
		A (A)			B (B)				
1	LATITUDE	S 15°	10'	15.30"	S 15°	10'	28.77"		
2	LONGITUDE	W 71°	49'	33.30"	W 71°	49'	45.48"		
4	AZIMUTH	221°			41°				
5	ANTENNA TYPE	SB1-220CIPN			SB1-220CIPN			0.3x0.3	
6	FREQUENCY TX	23.205000 GHz			21.973000 GHz			54.00	
1	LINK TYPE	IP-205 23Ghz, 32 QAM 53.870 Mbps							
7	POLARIZATION	VERTICAL							
8	ANTENNA HEIGHT	+ 30.0 m			+ 10.0 m				
9	EQUIPMENT	RF CENTRAL FREQUENCY						GHz	22.589
10		TRANSMITTER POWER						dBm	10
11	LINK	LINK DISTANCE						Km	0.55 Km
12		FEEDER LENGTH AT A						m	0
13		FEEDER LENGTH AT B						m	0
14		FEEDER UNIT LOSS						dB/m	0
15	GAINS	ANTENNA GAIN AT A						dB	34.06
16		ANTENNA GAIN AT B						dB	34.06
17		TOTAL GAIN						dB	68.1
18	LOSSES	FREE SPACE						dB	114.31
19		BY FLAT SURFACE						dB	0
20		BY OBSTACLES						dB	0
21		IN FEEDERS (A, B)						dB	0
22		BRANCHING TX/RX						dB	1
23		TOTAL						dB	115.31
	LEVELS, INTERRUPTION TIME AND AVAILABILITY	LINK ATTENUATION						dB	47.19
1		RX LEVEL WITHOUT FADING						dBm	-37.19
2		THRESHOLD LEVEL (BER = 1E-3)						dBm	-81.00
3		THRESHOLD LEVEL (BER = 1E-6)						dBm	-79.00
4		FADING MARGIN (BER = 1 E-3)						dB	43.81
5		FADING MARGIN (BER = 1 E-6)						dB	41.81
7		OBJECTIVE INTERRUPTION TIME (BER = 1 E-3)						%	1.19.E-05
8		OBJECTIVE INTERRUPTION TIME (BER = 1 E-6)						%	8.83.E-05
9		FADING DEPTH (BER = 1 E-3)						dB	14.25
10		FADING DEPTH (BER = 1 E-6)						dB	6
11		RX LEVEL WITH FADING (BER = 1 E-3)						dBm	-51.44
12		RX LEVEL WITH FADING (BER = 1 E-6)						dBm	-43.19
13		REAL INTERRUPTION TIME (BER = 1 E-3)						%	1.00.E-08
14		REAL INTERRUPTION TIME REAL (BER = 1 E-6)						%	2.00.E-08
15		AVAILABILITY (BER = 1 E-6)						%	99.99999998
16	ANNUAL REAL INTERRUPTION TIME						s	0.0000	
UIT - R OBJETIVES HIGH GRADE									Cumple

❖ PLAN DE FRECUENCIAS



6.6 PRUEBAS DE CONFIGURACION EN U.M EL SANTO

10.116.124.105/raiponderlog?winid=13&deviceid=0

Aplicaciones 85 GRUPO VIRTUAL MICROCOM LARECOLETA Duolingo Inicio Duolingo - Buscar c... Contactenos Navegación de IDS... Póster - Diseño sin...

CERAGON

Logout Connection Admin

CLIENTE AMG AUPLATA - TORRE REPETIDOR AMG AUPLATA: Radio Parameters

Related Pages

Filter

Unit Summary
Radio Summary
Platform
Faults
Radio
Radio Parameters
Remote Radio Parameters
Radio BER Thresholds
ATDC
Forward Encryption
Ethernet Interface
Configuration
Counters
MRMC
PM & Statistics
Diagnostics
Groups
Ethernet
Sync
Quick Configuration
Utilities

Status Parameters

Radio Location	Radio Slot 2, Port 1
Type	RPU-N-8C
XPIC support	No
Radio Interface operational status	Up
Operational TX Level (dBm)	18
RX Level (dBm)	-40
Modem MSE (dB)	-38.45
Defective Blocks	15407
TX Mute Status	Off
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	21973.000	(21760.000 ... 22400.000)
RX Frequency (MHz)	23295.000	(23000.000 ... 23600.000)
Frequency Separation (MHz)	1232.000	

☐ Set also remote unit

Configuration Parameters

Page Refresh Interval (Seconds) None

Last Loaded: 10:21:14 Refresh

10.116.124.105/raiponderlog?winid=13&deviceid=0

Aplicaciones 85 GRUPO VIRTUAL MICROCOM LARECOLETA Duolingo Inicio Duolingo - Buscar c... Contactenos Navegación de IDS... Póster - Diseño sin...

CERAGON

Logout Connection Admin

SITE AR3941 CAYLLOMA - TORRE REPETIDOR AMG AUPLATA: Radio Parameters

Related Pages

Filter

Unit Summary
Radio Summary
Platform
Faults
Radio
Radio Parameters
Remote Radio Parameters
Radio BER Thresholds
ATDC
Forward Encryption
Ethernet Interface
Configuration
Counters
MRMC
PM & Statistics
Diagnostics
Groups
Ethernet
Sync
Quick Configuration
Utilities

Status Parameters

Radio Location	Radio Slot 2, Port 1
Type	RPU-N-8C
XPIC support	No
Radio Interface operational status	Up
Operational TX Level (dBm)	20
RX Level (dBm)	-53
Modem MSE (dB)	-39.86
Defective Blocks	196297
TX Mute Status	Off
Adaptive TX power operational status	Down

Frequency control (Local)

TX Frequency (MHz)	23205.000	(23000.000 ... 23600.000)
RX Frequency (MHz)	21973.000	(21760.000 ... 22400.000)
Frequency Separation (MHz)	1232.000	

☐ Set also remote unit

Configuration Parameters

Page Refresh Interval (Seconds) None

Last Loaded: 14:31:45 Refresh



6.7 PRUEBAS DE CONFIGURACION EN U.M SUYCKUTAMBO

```

Dónde estamos | BREXIA
No seguro | brexia.pe/es/donde-estamos/

C:\Windows\system32\cmd.exe - ping www.claro.com.pe -t
Respuesta desde 95.100.87.195: bytes=32 tiempo=607ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=609ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=615ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=616ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=616ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=620ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=620ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=622ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=622ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=606ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=608ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=614ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=618ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=605ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=607ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=604ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=606ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=596ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=608ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=615ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=627ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=619ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=621ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=601ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=601ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=603ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=638ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=608ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=622ms TTL=52
Respuesta desde 95.100.87.195: bytes=32 tiempo=589ms TTL=52

```