



PERÚ

Presidencia del
Consejo de
Ministros

Proyecto Especial
Legado

Dirección de Desarrollo
Tecnológico y
Transmisiones

Subdirección de
Desarrollo
Tecnológico

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Unidad, la Paz y el Desarrollo"

TÉRMINOS DE REFERENCIA

SERVICIO DE INTERNET DEDICADO CON SEGURIDAD Y ANCHO DE BANDA GERENCIADA PARA OPTIMIZAR OPERACIONES ESTRATÉGICAS Y CONECTIVIDAD DE RECINTOS DEL PROYECTO ESPECIAL LEGADO

1 DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de internet dedicado con seguridad y ancho de banda gerenciada para optimizar operaciones estratégicas y conectividad de recintos del proyecto especial legado.

2 ÁREA USUARIA

Dirección de Desarrollo Tecnológico y Transmisiones (DDTT).

3 FINALIDAD PÚBLICA

Brindar el Servicio de Internet Dedicado con Seguridad y Ancho de Banda Gerenciada para el desarrollo eficiente de las actividades estratégicas y operativas del Proyecto Legado y contar con el servicio de Enlace de Datos para interconexión de los recintos legado y la Oficina Principal en pro del desarrollo eficiente de las actividades estratégicas y operativas del Proyecto Especial, orientadas a beneficiar a los usuarios del Proyecto Especial.

4 JUSTIFICACIÓN

Contar con el servicio de Enlace de Datos para interconexión de los recintos legado y la Oficina Principal para disponer de comunicación interna entre las sedes, un servicio de internet con seguridad y ancho de banda gerenciada permitirá tener una correcta comunicación interna, externa, acceso a recursos cloud, extranet de manera oportuna y segura.

5 OBJETIVOS DE LA CONTRATACIÓN

Contratar a un proveedor que brinde el servicio de Internet Dedicado con Seguridad y Ancho de Banda Gerenciada el Proyecto Especial Legado y interconexión de datos de los recintos legado

Objetivo Especifico:

- Contar con el servicio de Internet Dedicado en Alta Disponibilidad.
- Contar con el servicio de Seguridad Gerenciada en Alta Disponibilidad.
- Contar con el servicio de un Equipo Administrador de Ancho de Banda.
- Contar con un rango de IP's públicas.
- Permitir asegurar y garantizar la comunicación interna de manera óptima, rápida y segura.

6 Sistema de contratación

El sistema de contratación es SUMA ALZADA.



BICENTENARIO
DEL PERÚ
2021 - 2024

Av. San Luis S/N cdra. 11
Lima – Perú - Puerta 6 VIDENA
www.gob.pe/proyectolegado



7 ALCANCES Y DESCRIPCION DEL SERVICIO

7.1 Características Generales de los Servicios

- El proveedor deberá suministrar todos los equipos y sistemas de telecomunicaciones necesarios que permitan el correcto funcionamiento de los servicios solicitados. La Entidad brindará las facilidades de acceso que se necesite para la realización de los trabajos al interior del recinto.
- Todos los servicios deben contemplar la gestión y monitoreo activo de los equipos de seguridad y administrador de ancho de banda. Ante la caída del servicio, el centro de gestión del proveedor deberá comunicarse con el responsable del área de Telecomunicaciones e Infraestructura de Red del Proyecto Especial de manera proactiva e informar del posible incidente, este monitoreo activo será controlado por la Dirección de Desarrollo Tecnológico y Transmisiones. Así mismo, el personal de Tecnología del Proyecto Especial debe tener acceso a estas herramientas: 02 usuarios de lectura.
- El proveedor deberá cumplir con todas las disposiciones regulatorias que conducen a salvaguardar el secreto de las telecomunicaciones exigidas por el ente regulador OSIPTEL, además de contar con las autorizaciones de los ministerios competentes. Se precisa que lo señalado en el término de referencia, obedece a los parámetros de calidad establecidos y/o aceptados por el ente regulador OSIPTEL y el MTC según corresponda.

7.2 Características Generales del Servicio de Internet Dedicado

- Incluir la provisión y configuración de todos los equipos y accesorios necesarios para la implementación del servicio.
- Ancho de banda de 500Mbps, [overbooking 1:1 a nivel nacional hasta el router de borde del contratista hacia el proveedor internacional](#) ¹ y simétrico
- El medio de transporte debe de ser fibra óptica.
- Debe incluir un mínimo de /28 en IP Públicas; tomando en cuenta que se aceptará la suma de diferentes segmentos para cumplir con esta cantidad; [por tanto, se precisa que los 3 IPs para la configuración, compuestos por el IP de red, IP de broadcast e IP de puerta de enlace, se encuentran incluidos dentro del requerimiento](#) ².
- Se requiere una herramienta de control para monitorear la capacidad, uso y disponibilidad del enlace, basado en plataforma web. Debe guardar estadísticas históricas de tráfico. La herramienta debe también permitir ver el tráfico en detalle.
- La salida internacional hacia internet del proveedor deberá contar con contingencia de rutas y equipos.

¹ En respuesta a la consulta N°2 formulada por el participante NEXTNET S.A.C

² En respuesta a la consulta N°3 formulada por el participante NEXTNET S.A.C.

- Para el servicio en alta disponibilidad, tanto la ruta principal como de respaldo deben de ir a nodos diferentes del proveedor, asimismo cada enlace tiene su propio CPE en el lado cliente, la cual debe de estar documentado y ser parte del informe final. El CPE podrá ser un router o un switch L2/L3 acorde al mejor diseño propuesto por el proveedor³.
- El proveedor debe tener una red que participe en internet como TIER1 y/o TIER2 y/o TIER3 ⁴.
- El SLA requerido para el servicio no debe ser menor a 99.7% y se aplica de manera mensual. Si el servicio se ve afectado por hechos fortuitos ajenos al proveedor, no será responsabilidad del proveedor, ni será materia de penalidad.

7.3 Características Generales de la Seguridad Gerenciada

- La seguridad gerenciada se realizará desde el Data Center del Proveedor a través de firewalls virtuales o firewalls físicos. En caso de ser equipos físicos, queda a potestad de que el equipo sea de **primer y/o segundo uso; dichos equipos deberán garantizar el soporte y licenciamiento para el servicio durante todo el periodo de contrato independientemente del equipo que esté instalado en su red⁵**.
- Estos firewalls virtuales o físicos deberán tener como mínimo las siguientes funcionalidades:
 - Protección contra ataques de intrusión (IPS).
 - Protección contra virus (Antivirus).
 - Control de Aplicaciones.
 - Soporte contra malware de Zero Day mediante técnicas de Sandboxing (Puede ser en el Datacenter del fabricante o en el Datacenter del ISP).
 - Protección contra malware (AntiMalware).
 - Protección contra spyware (AntiSpyware).
 - Capacidad de filtrado de páginas web (URL Filtering).
 - SSL VPN Client to Site. (Debe estar licenciado la creación de VPN con dispositivos IOS, Android). No es de doble autenticación y se estima un promedio para 500 usuarios concurrentes VPN IPSEC Site to Site.

³ En respuesta a la consulta N°4 formulada por el participante NEXTNET S.A.C., se confirma que la Entidad brindará puertos en el switch de acceso. A fin de realizar la configuración del servicio.

⁴ En respuesta a la consulta N°5 formulada por el participante NEXTNET S.A.C., Se aclara que para la acreditación del requerimiento será suficiente con la presentación del ANEXO 3 "Declaración Jurada de cumplimiento de los términos de referencia", presentado en la oferta. Asimismo, a fin de dar respuesta al participante se indica que, de forma adicional, podrá presentar un diagrama donde se indique que el contratista tiene conexión con al menos un proveedor TIER-1 indicando el nombre del mismo. En respuesta de la observación N°50 formulada por el participante GTD PERÚ S.A.

⁵ En respuesta a la consulta N°6 formulada por el participante NEXTNET S.A.C

- Inspección del tráfico tanto de entrada y salida.
- Soporte de feature Prevención de fuga de información (DLP). Esta característica es opcional.
- Generación de reportes.
- El proveedor será administrador de la plataforma de seguridad, donde al proyecto especial se le otorgará 02 usuarios de lectura distintos para dicha plataforma.
- Para los reportes:
 - El contratista deberá otorgar, un sistema de reportes y administración de logs para el sistema de seguridad perimetral, el cual se deberá ingresar con un usuario y contraseña. Dicho sistema podrá ser brindado por una solución en la nube del operador, embebido en el firewall o como equipo appliance de propósito específico.
 - El sistema de reportes debe contar con una mínima de 4 TB de almacenamiento.
 - La solución deberá permitir generar reportes en tiempo real.
 - La solución deberá permitir generar reportes históricos.
 - La solución deberá permitir generar reportes de actividad de los usuarios, aplicaciones, servicios, equipos.
 - La solución deberá permitir generar reportes de actividad del malware, virus, spyware detectado.
 - La solución deberá tener la capacidad de enviar reportes programados por correo electrónico.
 - La solución deberá permitir exportar los reportes generados en los siguientes formatos al menos: PDF, HTML, XML y CSV.

7.4 Características Generales del servicio de interconexión de sedes.

- Brindar el servicio de enlace de datos entre los recintos indicados.
- En el caso de los equipos CPE a proveer para los enlaces, será potestad del proveedor que éstos sean de primer uso, toda vez que el criterio de cumplimiento es el SLA solicitado. En caso de ser de segundo uso, el año de fabricación no deberá ser mayor a 3 años. Asimismo, los equipos deben estar vigentes en venta y soporte por parte del fabricante. **El postor deberá presentar conjuntamente con los documentos para el perfeccionamiento del contrato⁶, una carta del fabricante y/o ficha técnica (datasheets) y/o especificaciones del equipo ofertado y/o información publicada en la web y/o publicación oficial del**

⁶ En respuesta a la consulta N°23 formulada por el participante NEXTNET S.A.C.

fabricante y/o manuales e instructivos del fabricante del equipo ofertado, con la finalidad de acreditar el cumplimiento de no tener notificación de estar fuera del Ciclo de Vida y Ciclo de Venta y que el año de fabricación no sea mayor a 3 años. Contabilizado desde la presentación de ofertas.

- Para todo el alcance del presente servicio se debe incluir la instalación, configuración, puesta en operación del servicio y soporte técnico al equipamiento que corresponda.
- Los equipos que se instalen en las sedes mencionadas deben soportar un crecimiento del 20% respecto del ancho de banda solicitado en caso se requiera ampliación en la etapa contractual. El equipo correspondiente al TER Edificio Administrativo de Videna debe soportar un crecimiento del 50%.
- La plataforma de red WAN vía MPLS ofrecida por el proveedor, debe de soportar crecimiento ante la solicitud de servicios por parte de la entidad.
- Todos los CPE's (routers) a implementarse en cada uno de los recintos de legado, debe soportar el feature VRF, para que ante alguna solicitud por parte de la entidad (programación de eventos), se pueda dividir el tráfico sin la necesidad de incurrir en costos adicionales.
- El Proyecto Especial se reserva el derecho de realizar y/o solicitar a lo largo del servicio otras pruebas de monitoreo que validen el cumplimiento del SLA, así como el ancho de banda solicitado. En caso los resultados de estas no cumplan con los valores establecidos en los presentes términos de referencia, dichos resultados obligarán al proveedor a la revisión, ejecución y solución que corresponda a fin de lograr el cumplimiento de lo solicitado.
- Los cambios de configuraciones de los equipos que el Proyecto Especial solicite durante el plazo de ejecución del servicio deben ser realizados por el proveedor y éstos deben iniciar como máximo a las 4 horas de haber recibido la notificación, vía correo electrónico o llamada telefónica. Estos cambios en las configuraciones no generarán costos adicionales para el Proyecto Especial.

7.5 Características mínimas específicas de los servicios de datos

7.5.1 Características del servicio de internet

Item	Características mínimas
Ancho de banda	500mbps
Simetría	Simétrico
Overbooking	overbooking 1:1 a nivel nacional hasta el router de borde del contratista hacia el proveedor internacional simétrico
Direcciones IP públicas	/28
Herramienta de control y monitoreo	Sí
Salida internacional contingencia de rutas y equipos en el proveedor	Sí
Nivel del TIER a nivel de proveedor	Podrá ser TIER1 y/o TIER2 y/o TIER3

Item	Características mínimas
Medio de transporte	Fibra óptica
Alta disponibilidad del servicio	Se debe tener un enlace principal y un enlace de backup con llegada a nodos distintos. Cada enlace deberá tener su propio CPE instalada en el lado cliente, este CPE podrá ser un router, un switch L2/L3, o acorde al mejor diseño del proveedor asegurando la seguridad perimetral.
Proveedor miembro del NAP Perú	El proveedor deberá ser miembro del NAP Perú ó deberá tener un punto de intercambio a través de un miembro activo del NAP Perú ⁷ .
Red backbone de la ruta brindada	Fibra Óptica
Red de acceso – última milla	Fibra Óptica
Proveedor cuenta con NOC propio	Sí
Proveedor cuenta con SOC propio y/o por tercero	Sí

7.5.2 Características del servicio de interconexión de sedes

El alcance del servicio incluye la implementación de los enlaces de datos para interconexión de los recintos legado, incluyendo la Oficinal Principal del Proyecto Especial, con la sede de la VIDENA.

Enlace de Datos	Ancho de Banda	Duración
TER Edificio Administrativo (Videna Puerta 2)	400 Mbps	12 meses
Complejo Villa María del Triunfo – VIDENA (TER)	150 Mbps	12 meses
Polideportivo de Villa El Salvador – VIDENA (TER)	150 Mbps	12 meses
Punta Rocas - VIDENA (TER)	150 Mbps	12 meses

NOTA: El servicio tendrá una duración de trescientos sesenta y seis 366 días calendario (dado que el año 2024 es año bisiesto) o equivalente a doce 12 meses⁸

⁷ En respuesta a la consulta №9 formulada por el participante NEXTNET S.A.C.

⁸ En respuesta a la consulta №52 formulada por el participante GTD PERU S.A.

El enlace de datos en cada uno de los casos deberá ser **overbooking 1:1 a nivel nacional hasta el router de borde del contratista hacia el proveedor internacional** simétrico basado en fibra óptica.

Dirección de los recintos:

- Los Data Centers se encuentra en la mayoría de los casos en un primer piso, solo Videna, se encuentra en un segundo piso.

Recinto	Dirección	Latitud	Longitud
Villa Deportiva Nacional - VIDENA (TER)	Av. Del Aire Cdra. 8 s/n, San Luis. Puerta 2.	12°04'48.4"S	77°00'05.5"W
Complejo Deportivo Villa María del Triunfo	Av. Primavera 1491, Puerta N°5 Villa María del Triunfo	12°08'53.1"S	76°57'11.2"W
Polideportivo Villa El Salvador	Av. Mariano Pastor Sevilla s/n, Villa El Salvador	12°11'58.8"S	76°57'30.3"W
Complejo Deportivo Punta Rocas	Antigua Panamericana Sur Km. 47.5 Punta Negra	12°21'06.7"S	76°48'56.6"W

SERVICIO DE ENLACE DE DATOS	
DESCRIPCIÓN	CARACTERÍSTICAS MINIMAS
Aspectos Generales	<ul style="list-style-type: none">Se requiere conexión de enlace de datos basada en la tecnología MPLS para interconectar las sedes, de acuerdo con el alcance indicado.Se deberá considerar la integración, configuración y puesta en funcionamiento de la solución propuesta de acuerdo con el alcance y descripción.Ancho de banda garantizado al 100% por cada sede de manera simétrica.La red de datos del Proveedor y los routers CPE's deberán manejar calidad de servicio, diferenciación y priorización de tráfico de datos, video y voz. Estas funcionalidades deberán estar configuradas en ambos extremos de los enlaces de datos y/o voz solicitados.El Proveedor al final de la instalación y configuración de los enlaces solicitados deberá realizar pruebas de conectividad y de saturación de ancho de banda. Estas pruebas serán supervisadas por responsable de Tecnología de la Dirección de Desarrollo Tecnológico y Transmisiones, y el resultado de éstas deberá estar consignado en el documento del informe final entregado por el Proveedor.El Proveedor deberá sustentar técnicamente las configuraciones realizadas en los equipos de comunicaciones y sus componentes de cada una de las sedes. Esto será incluido en el informe final.

SERVICIO DE ENLACE DE DATOS	
DESCRIPCIÓN	CARACTERÍSTICAS MINIMAS
Enlaces	<p>En todas las sedes, el medio de acceso de última milla deberá ser fibra óptica, en canalización subterránea o aérea fuera de las sedes. Al interior de la sede, hay que señalar que los recintos de legado cuentan con buzones de comunicaciones para la entrada de los servicios del Proveedor. El proveedor debe de realizar la obra civil para Interconectar su ducto con el buzón de telecomunicaciones de la Entidad.</p> <p>Para satisfacer las comunicaciones se requiere lo siguiente:</p> <ul style="list-style-type: none"> a) Ancho de banda de ambas sedes será de acuerdo con el alcance indicado. b) Modalidad de conexión a la red del Proveedor deberá ser a través de la tecnología MPLS. c) Ancho de banda garantizado al 100%. d) Enlace simétrico/Overbooking 1:1 a nivel nacional hasta el router de borde del contratista hacia el proveedor internacional e) El Proveedor deberá garantizar el control del tráfico por medio del equipo considerado CPE (router) permitiendo que el tráfico necesario sea el que únicamente pueda ingresar a ser parte del servicio para la red WAN. f) El servicio deberá conservar la actual distribución de direcciones IP privadas existentes en las redes LAN de cada sede. El CPE debe de ser capa 3. g) Los enlaces deberán asegurar la priorización de tráfico de voz, video sobre la de datos o viceversa
Calidad de Servicio	<p>La calidad de servicio se medirá en los siguientes términos:</p> <ul style="list-style-type: none"> a) Disponibilidad del servicio: la red de comunicaciones a ser ofertada deberá tener una disponibilidad de servicio mínima de 99.5% en un periodo mensual para las sedes del enlace tal como se indica en la siguiente fórmula: $\text{Disponibilidad} = \frac{[1 - \text{Tiempo total de caída mensual en min.}] \times 100}{\text{Total de minutos mensual}}$ <p>Nota: Se entiende por "caída" a la interrupción del servicio, es decir, que alguna de las sedes no pueda recibir o transmitir datos, la cual se calcula desde que el Proyecto Especial reporta la falla al Proveedor por teléfono y/o correo, y recibe un ticket de atención, hasta que el Proveedor restablezca el servicio. Si el servicio se ve afectado por hechos fortuitos ajenos al proveedor, no será responsabilidad del proveedor, ni será materia de penalidad.</p>

7.6 Características mínimas específicas del servicio de seguridad gerenciada

DESCRIPCIÓN	CARACTERÍSTICAS MÍNIMAS
Arquitectura	Se requiere una solución robusta que permita soportar las operaciones del Proyecto Especial acordes al ancho de banda solicitada sin verse comprometidos los recursos de hardware.
Performance	<ul style="list-style-type: none"> El throughput de IPS, de VPN IPSEC y SSL deberán ser 10 suficiente robusto para un óptimo rendimiento de las operaciones. 500,000 de conexiones o sesiones concurrentes como mínimo. La solución deberá soportar al menos 500 usuarios concurrentes. En caso requerir licencias estas deberán estar incluidas para la solución propuesta.
Capacidades	<ul style="list-style-type: none"> Debe tener una alta disponibilidad (HA), trabajando en un esquema de alta de tipo activo-pasivo o activo-activo con balanceo de carga. con todas las licencias de habilitadas para no permitir la pérdida de conexiones, deberán estar siempre sincronizados. Queda a potestad del proveedor ofrecer un buen diseño de red los firewall virtuales/físicos en su Data Center. La solución deberá enviar alertas para eventos críticos relacionados con hardware o software.
Filtro URL	<ul style="list-style-type: none"> El filtrado de URL debe ser basado en categorías o similares y permitir crear grupos personalizados Debe cubrir más de 30 millones de sitios web en al menos 20 categorías. Debe incluir un mecanismo que permita al administrador negar o permitir URLs específicos, que no necesariamente están definidos en una categoría, para poder ser utilizados en la definición de nuevas reglas. Debe permitir la creación de excepciones basadas en la definición de objetos de red. Debe proveer la opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página. El dispositivo debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0 El dispositivo debe tener la capacidad de identificar y bloquear herramientas de "proxy bypass" sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales) Debe bloquear Malware sobre sitios web y web 2.0 Debe Inspeccionar el trafico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. La solución debe hacer dicha inspección sin la necesidad de utilizar herramientas de terceros, servidores o licencias adicionales

	<ul style="list-style-type: none"> • Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando cual URLs a través de la integración con • servicios de directorio activo, autenticación vía LDAP, Active Directory y base de datos local. • Debe ser posible crear políticas por usuario, de usuario, ips, redes y zonas de seguridad. • Debe permitir publicar los logs de URL con la información de los usuarios con servicios de directorio.
VPN	<ul style="list-style-type: none"> • Debe incluir soporte a las topologías VPNs site-to-site • Soporte a VPNs client-to-site basadas en IPSEC. • VPNs IPSec debe soportar: DES, 3DES; • Autenticación MD5 y SHA-1; • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; • Algoritmo Internet Key Exchange (IKE); • AES 128, 192 y 256 (Advanced Encryption Standard) • Autenticación vía certificado IKE PKI. • Las VPN SSL deben soportar: <ul style="list-style-type: none"> ○ Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB ○ Las funcionalidades de VPN SSL deben ser atendidas con el uso de agente, opcionalmente sin el uso de agente ○ La asignación de dirección IP en los clientes remotos de VPN ○ La asignación de DNS en los clientes remotos de VPN • Debe tener la posibilidad de realizar VPNs clientes • SSL para acceso remoto, sin necesidad de instalar un cliente. • Soporte a VPNs tipo L2TP, incluyendo el soporte al cliente L2TP del Iphone • La VPN SSL deberá soportar asignación de aplicaciones permitidas por grupo de usuarios. El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN. • Soporte de conexiones VPN del Client to Site con dispositivos Celulares/móviles. • Deberá de permitir la comunicación de la VPN a través de SSL y IPSec. • Deberá soportar el acceso VPN SSL mínimo de 50 usuarios concurrentes. • Debe poder establecer VPNs IPSec con gateways que tengan direcciones IP dinámicas públicas.

Prevención de amenazas	<ul style="list-style-type: none"> • Para seguridad del ambiente contra ataques, los dispositivos de deben poseer módulo de IPS, Antivirus y Anti-Spyware o Antimalware. • Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware o Antimalware). • sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo y Activo/pasivo. • permitir la inspección en archivos comprimidos que utilizan el algoritmo deflate (zip, gzip, etc.). • Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP. • Debe contar con funcionalidad de Análisis de archivos sospechosos o detección de malware desconocido en la nube (emulación de sandboxing). • Debe incluir protecciones para los protocolos POP3 e IMAP. • Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP. • Capacidad de actualización automática o manual de firmas. • El IPS debe proveer al menos dos políticas o perfiles predefinidos, para ser usados inmediatamente. • El administrador debe poder activar automáticamente nuevas firmas, basados en parámetros de configuración definidos previamente • (impacto en el desempeño, severidad de la amenaza, tipo de protección: server o client).
Administración	<ul style="list-style-type: none"> • La solución debe administrarse desde una única consola gráfica, se prefiere que sea basada en Web en equipos Windows o Linux con navegadores Microsoft Internet Explorer (Windows), Chrome, Mozilla Firefox (Windows/Linux). • La solución deberá soportar acceso vía SSH, cliente WEB (HTTPS) o interfaz GUI. • En caso de que sea necesario la instalación de cliente para administración de la solución el mismo debe ser compatible con sistemas operativos windows. • La solución deberá poder realizar respaldos y restauraciones de las configuraciones.
Autenticación de usuarios	<ul style="list-style-type: none"> • La solución deberá poder integrarse con Active Directory de Microsoft, se prefiere que no sea necesario instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se

	<p>efectúe por medio de cuentas de usuarios y grupos de administración basadas en el Active Directory.</p> <ul style="list-style-type: none"> Administración Basada en Roles: Es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad del de Sistemas y de otras unidades definidas en el Active Directory. La solución deberá permitir la segregación de funciones de forma granular, permitiendo así definir al alcance o posibilidades de gestión para cada administrador. La solución tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.
Reportes	<ul style="list-style-type: none"> El contratista deberá otorgar, un sistema de y administración de logs para el sistema de Seguridad perimetral, el cual se deberá ingresar con un usuario y contraseña. Dicho sistema podrá ser brindado por una solución en la nube del operador, embebido en el firewall o como equipo appliance de propósito específico. Se evaluará costo beneficio. El sistema de reportes debe contar con una capacidad de 4TB como mínimo de almacenamiento. La solución deberá permitir generar reportes en tiempo real. La solución deberá permitir generar reportes históricos. La solución deberá permitir generar reportes de actividad de los usuarios, aplicaciones, servicios, equipos. La solución deberá permitir generar reportes de actividad del malware, virus, spyware detectado. La solución deberá tener la capacidad de enviar reportes programados por correo electrónico. La solución deberá permitir exportar los reportes generados en los siguientes formatos al menos: PDF, HTML, XML y CSV.

7.7 Características mínimas específicas del equipo administrador de ancho de banda

DESCRIPCIÓN	CARACTERÍSTICAS MÍNIMAS
Arquitectura	Hardware del tipo appliance, queda a potestad del proveedor, que el hardware del tipo appliance sea de primer o segundo uso; dicho equipo deberá garantizar el soporte y licenciamiento para el servicio durante todo el periodo de

	<p>contrato ⁹ Solo un equipo, no HA. Un equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras. Deberá contar al menos con 2 bridges, es decir, 4 puertos como mínimo en 1GE RJ45 o de fibra óptica¹⁰. Todos los bridges deberán contar con bypass interno que impida la interrupción ante eventos de falla por energía del equipo. Deberá poseer al menos 1 puerto 10/100/1000 RJ45 para su administración. El equipo podrá tener múltiples funcionalidades como caching, aceleración, pero solo se necesita licenciamiento para la administración del ancho de banda solicitado. En lo posible, se deberá tener licencia de prueba para las funcionalidades de caching y aceleración en caso la Entidad lo requiera.</p>
Performance y capacidades	<p>La solución deberá brindar Calidad de Servicio (QoS) para proteger el ancho de banda de aplicaciones críticas de la Entidad y contener el tráfico no deseado tanto en IPv4 e IPv6. Deberá contar con al menos 3,000 aplicaciones identificadas, independientemente del puerto que estén utilizando. Así como permitir la creación de aplicaciones personalizadas por la propia Entidad. Deberá agrupar las aplicaciones en categorías como: Redes Sociales, P2P, Actualizaciones de Software, Video y Música, entre otros. Así como permitir la creación de grupos de aplicaciones personalizados. Deberá estar licenciado para poder gestionar 500 Mbps de throughput simétrico inicialmente, con capacidad de poder incrementar (con licenciamiento adicional) a 600 Mbps de requerirse. Deberá soportar como mínimo 750,000 flujos concurrentes¹¹. Deberá permitir la creación de múltiples políticas o reglas de control de ancho de banda que realicen la priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo de ancho de banda permitido. La solución deberá integrarse con los Directorios Activos (AD) de la Entidad con la finalidad de</p>

⁹ En respuesta a la consulta №10 y 18 formulada por el participante NEXTNET S.A.C.

¹⁰ En repuesta a la consulta №11 formulada por el participante NEXTNET S.A.C.

¹¹ En respuesta a la consulta №13 formulada por el participante NEXTNET S.A.C.

	<p>manejar políticas basadas en usuarios. El equipo deberá poder actualizarse automáticamente a la última versión de software publicado.</p> <p>El equipo debe garantizar el almacenamiento de datos en su disco duro interno de por lo menos los últimos 12 meses, para la posterior generación de reportes y estadísticas. Monitoreo en tiempo real con actualizaciones cada segundo a través de tablas con filtros y gráficos, que permitan realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.</p>
Administración	<p>Deberá considerar una consola de administración web en el mismo equipo que permita, de forma gráfica, administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. La Entidad deberá contar con acceso de lectura al equipo para la obtención de reportes en cualquier momento, para 02 usuarios de lectura.</p> <p>Deberá poseer al menos 1 puerto 10/100/1000 rj45 para su administración.</p>
Reportes	<p>Deberá permitir la creación de los siguientes reportes históricos basados en gráficos para el periodo contratado:</p> <ul style="list-style-type: none"> • Tráfico de descarga y subida. • Los hosts con mayor consumo. • Los usuarios con mayor consumo. • Las aplicaciones con mayor consumo. <p>Mostrar históricamente distintas métricas de desempeño como:</p> <ul style="list-style-type: none"> • Throughput In/Out. • Bytes transmitidos. • Número de sesiones activas. • Paquetes descartados. • Desempeño de la calidad de las aplicaciones.

7.8 Procedimiento

7.8.1 Interconexión de sedes

- El Proveedor deberá suministrar todos los equipos y sistemas de telecomunicaciones necesarios que permitan el correcto funcionamiento de todos los servicios solicitados.
- Todos los servicios deben contemplar la gestión y monitoreo activo de los mismos. Ante la caída del servicio, el centro de gestión (NOC/SOC) del Proveedor deberá comunicarse con el contacto del área de Telecomunicaciones e Infraestructura de Red del Proyecto Especial e informar del posible incidente. Así mismo, el personal

de Tecnología del Proyecto Especial debe tener acceso a estas herramientas de monitoreo: 02 usuarios distintos de lectura.

- El Proveedor deberá cumplir con todas las disposiciones regulatorias que conducen a salvaguardar el secreto de las telecomunicaciones exigidas por el ente regulador OSIPTEL, además de contar con las autorizaciones de los ministerios competentes. Se precisa que lo señalado en el término de referencia, obedece a los parámetros de calidad establecidos y/o aceptados por el ente regulador OSIPTEL y el MTC según corresponda.

7.8.2 Servicio de Internet y Seguridad gestionada

- Realización de mesas de trabajo técnica de manera conjunta con la Dirección de Desarrollo Tecnológico y Transmisiones antes de la implementación.
- Envío de la lista de actividades, protocolo de pruebas y personal involucrado en la implementación y gestión. Personal de campo deberá contar con todos los seguros e implementos de seguridad y bio seguridad para la realización del trabajo. La lista más el seguro debe de ser enviada con 24 horas a lo mucho al contacto/responsable del área de Telecomunicaciones e Infraestructura de Red.
- El Proyecto Especial gestionará el acceso del personal del proveedor y confirmará vía correo electrónico.
- Para los trabajos, se contará con personal de la Subdirección de Tecnología quien supervisará los trabajos.
- El proveedor ejecutará los protocolos de pruebas para el servicio.
- El proveedor deberá resanar cualquier alteración en la infraestructura de la sede donde se realizan los trabajos y deberá mantener la estética del lugar utilizando pintura, drywall, etc. necesarios.
- Monitoreo presencial o remoto en los días posteriores a la implementación, al menos los primeros 7 días calendarios.
- Firma del acta de servicio por la Sub-Dirección de Desarrollo Tecnológico y Transmisiones una vez estén estable los servicios.

7.9 Plan de trabajo

El proveedor deberá presentar el plazo de dentro de los 05 días posteriores al perfeccionamiento del contrato; el Plan de Trabajo debe contener como mínimo la siguiente información:

- Recursos necesarios (Personal, Equipos, Otros).
- Protocolo de pruebas del objeto de la contratación.
- BoM del equipamiento.
- Layout del equipamiento en visio o similar.
- Topología propuesta.
- Plan de bajo nivel.
- Responsable por actividad.
- Cronograma de actividades.
- Riesgos advertidos.

Dicho, Plan de trabajo será presentado a la entidad a través de mesa de partes virtual en el siguiente link <https://legado.gob.pe/formulario-mesa-de-partes> o físicamente en Mesa de Partes: Av. San Luis cuadra 11 S/N, Sede de la Villa Deportiva Nacional

(VIDENA) Puerta N°6-Cruce Av. Del Aire, distrito San Luis, provincia y departamento de Lima de 8:30 a.m. a 4:30 p.m

Al respecto, el área usuaria a través de su responsable técnico tendrá un (01) día calendario para revisar y aprobar el plan de trabajo contados a partir del día siguiente de la recepción de dicho Plan;

De existir observaciones, se enviará el pliego de observaciones a ser absuelto por el Contratista, el cual deberá absolverlo en un plazo que no exceda un (01) día calendario contabilizado al día siguiente de recibida la comunicación.

La Entidad revisará en un plazo máximo de un (01) **día calendario** contabilizado a partir del día siguiente de recibida el plan de trabajo y/o la absolución de observaciones y comunicará por correo electrónico, la aprobación del Plan de Trabajo.

7.10 Seguros

El personal del proveedor que realice la implementación y gestión de la solución deberá contar con el Seguro Complementario de Trabajo de Riesgo (SCTR) de salud, así como también con sus equipos de protección personal.

7.11 Recursos y facilidades a ser provistos por la Entidad

La entidad proveerá de espacio en rack y elementos básicos en la sala técnica de la DDTT. (energía estabilizada, UPS, aire acondicionado).

7.12 Soporte Técnico, Garantía y Capacitación.

7.12.1 Soporte técnico del Internet Dedicado por el periodo contratado

El proveedor deberá contar con un Centro de Operación de Red: NOC - Network Operation Center, que como mínimo cumpla con lo siguiente:

- Soporte para averías, modalidad presencial y en línea (por diferentes medios), del tipo 24x7 por el periodo contratado. La atención en línea debe ser inmediata.
- La cantidad de atenciones de las averías deberán ser ilimitadas sujeta al tiempo de la garantía de los equipos.
- El tiempo de resolución de averías del CPE (router, switch) se encuentra tipificado de la siguiente manera como mínimo:
 - Tiempo de respuesta: (30 minutos) desde que el cliente llama, se realiza los primeros descartes y hasta que se genera el ticket de atención, **tiempo de resolución: será computada a partir de la generación del ticket¹².**
 - Tiempo de resolución: indicado de acuerdo con el nivel de afectación.

¹² En respuesta a la consulta N°36 formulada por el participante NEXTNET S.A.C

- Nivel 1 (Grave): La funcionalidad anexa no se encuentra operando en su totalidad.
- Nivel 2 (Severa): El equipo opera con inconvenientes afectando a más de un 20% de los puestos de trabajo o al servicio de operadora.
- Nivel 3 (Leve): El equipo opera parcialmente afectando a menos de un 20% de los puestos de trabajo.
- Nivel 4 (Normal - Cambio de configuración): El equipo opera con normalidad. El evento: afecta el puesto de trabajo de un usuario, no se encuentra contemplado en los niveles 1-2-3 o es considerado cambio de configuración.

Nivel	Tipificación	Tiempo de Resolución
1	Grave	4 horas
2	Severa	5 horas
3	Leve	6 horas
4	Normal	7 horas

- En caso de falla de hardware, se debe disponer de un equipo de reemplazo en un tiempo máximo de 4 horas. El proveedor deberá realizar el diagnóstico correspondiente para determinar la falla de hardware, siendo válidas soluciones de spare (reemplazo) con equipos similares de forma temporal, hasta tener el equipo definitivo gestionado a través del contrato con el fabricante. Se realizarán las evaluaciones pertinentes para la determinación de las responsabilidades. En caso se determine que la responsabilidad sea imputada a la Entidad, será la Entidad quien asuma los costos adicionales.
- Se aceptarán como hechos fortuitos ajenos al proveedor y que podrían afectar la continuidad del servicio, mas no el nivel de servicio requerido del mismo, aquellos ocasionados por atentados o desastres naturales. Previa evaluación, se determinará la no responsabilidad del proveedor, ni será materia de penalidad. Cabe precisar que dicha situación, debe de encontrarse debidamente sustentada y/o motivada, en el marco de la normativa de contrataciones.
- Se contará con una atención preferencial por parte de los ejecutivos asignados dentro del horario de oficina, el cual será comunicado al Proyecto Especial.

7.12.2 Soporte técnico de la Seguridad y Ancho de Banda Gerenciada por el periodo contratado

El proveedor deberá contar con un Centro de Operación de Seguridad: SOC - Security Operation Center, que como mínimo cumpla con lo siguiente:

- Soporte para averías, configuraciones en modalidad presencial y en línea (por diferentes medios), del tipo 24x7 por el periodo contratado. La atención en línea debe ser inmediata.
- La cantidad de atenciones de las averías deberán ser ilimitadas sujeta al tiempo de la garantía de los equipos.
- El tiempo de resolución de averías y de ejecución de configuraciones se encuentra tipificado de siguiente manera como mínimo:

Ejecución de Configuraciones:

- Tiempo de respuesta: (30 minutos) desde que el cliente llama, se realiza los primeros descartes y hasta que se genera el ticket de atención.
- Tiempo de resolución: de acuerdo con la complejidad de la solicitud
 - Nivel 1 (Grave): La configuración de 4 o menos reglas o filtros, habilitación de URLY aplicaciones, habilitación de NAT estático, sincronización con el AD. Políticas de ancho de banda por grupos o aplicaciones detectadas, etc.
 - Nivel 2 (Severa): La configuración de VPNs site to site y servicios complementarios en el firewall y administrador de ancho de banda.
 - Nivel 3 (Leve): La configuración de reglas con más de 4 filtros y con más de 5 reglas concurrentes.
 - Nivel 4 (Normal - Cambio de configuración): Configuraciones complejas que requieren cambio de topología.

SLA Servicios de Configuración Firewall y Administrador de Ancho de Banda

Nivel	Tipificación	Tiempo de Resolución
1	Grave	1 horas
2	Severa	2 horas
3	Leve	4 horas
4	Normal	7 horas

- Se contará con una atención preferencial por parte de los ejecutivos asignados dentro del horario de oficina, el cual será comunicado al Proyecto Especial.
- El contratista deberá contemplar una bolsa de soporte de configuración de 15 horas por el periodo de contrato, para cambios de ingeniería que sean necesarios en la solución post implementado. Aplica el mismo SLA especificado para la atención de incidentes. Las bolsas de horas de configuración serán contadas una vez el especialista esté conectado a los equipos. Esta configuración podrá darse de manera remota y/o presencial dependiendo de la complejidad de los cambios. Esta bolsa de horas aplica para requerimientos que el Proyecto Especial tenga tanto

para el CPE como para el firewall y administrador de ancho de banda.

- El proveedor deberá considerar proactivamente la actualización del firmware del equipo sin incurrir en gastos adicionales ni consumo de horas de la bolsa al Proyecto Especial. Esta actividad debe ser parte del servicio. [La actualización quedará a criterio del contratista siendo este responsable del correcto funcionamiento con la versión de firmware más estable.](#)¹³

7.12.3 Soporte técnico de Interconexión de sedes

- Soporte para averías, modalidad presencial y en línea (por diferentes medios), del tipo 24x7 por el periodo contratado. La atención en línea debe ser inmediata.
- El tiempo de resolución de averías se encuentra tipificado de la siguiente manera como mínimo:
 - Tiempo de respuesta: (30 minutos) Desde que el cliente llama, se realiza los primeros descartes y hasta que se genera el ticket de atención.
 - Tiempo de resolución: determinado por el nivel de afectación.
 - Nivel 1 (Grave): El servicio o una funcionalidad anexa no se encuentra operando en su totalidad.
 - Nivel 2 (Severa): El servicio opera con inconvenientes afectando a más de un 20% de los puestos de trabajo o al servicio de operadora.
 - Nivel 3 (Leve): El Servicio opera parcialmente afectando a menos de un 20% de los puestos de trabajo.
 - Nivel 4 (Normal - Cambio de configuración): El servicio opera con normalidad. El evento: afecta el puesto de trabajo de un usuario, no se encuentra contemplado en los niveles 1-2-3 o es considerado cambio de configuración.

Nivel	Tipificación	Tiempo de Resolución
1	Grave	4 horas
2	Severa	5 horas
3	Leve	6 horas
4	Normal	10 horas

- En caso de falla de hardware, se debe disponer de un equipo de reemplazo en un tiempo máximo de 4 horas. El Proveedor deberá realizar el diagnóstico correspondiente para determinar la falla de hardware. Serán válidas soluciones de spare con equipos similares de forma temporal, hasta tener el equipo definitivo gestionado a través del contrato con el fabricante. Se realizarán las evaluaciones pertinentes para la determinación de las

¹³ En respuesta a la consulta №14 formulada por el participante NEXTNET S.A.C.

responsabilidades. En caso se determine que la responsabilidad sea imputada a la Entidad, será la Entidad quien asuma los costos adicionales.

- Si el servicio se ve afectado por hechos fortuitos y ajenos al proveedor, estos no formarán parte del SLA y ni será responsabilidad del proveedor, dicha situación, debe de encontrarse debidamente sustentada y/o motivada, en el marco de la normativa de contrataciones.
- Se contará con una atención preferencial por parte de los ejecutivos asignados dentro del horario de oficina¹⁴. Dicha información deberá ser presentada en la etapa de perfeccionamiento del contrato.

7.12.4 Capacitación y/o entrenamiento

El proveedor deberá brindar una transferencia de conocimiento de lo implementado de 9 horas para 02 personas como mínimo de la Dirección de Desarrollo Tecnológico y Transmisiones sobre la administración, configuración y troubleshooting del sistema de seguridad y ancho de banda gerenciada.

N° DIAS	Tema	Horas
Día 1	Administración y configuración del Sistema de Seguridad. Plataforma de Monitoreo.	3
Día 2	Troubleshooting del Sistema de Seguridad. Generación de Reportes.	3
Día 3	Administración, configuración y troubleshooting.	3

La transferencia de conocimiento se realizará dentro de los 15 días calendario contados a partir del día siguiente de suscrita el acta de conformidad técnica para el inicio de la ejecución del servicio¹⁵. La transferencia de conocimiento deberá realizarse de manera presencial y/o virtual, se coordinará oportunamente con el área de Telecomunicaciones de la Dirección de Desarrollo Tecnológico y Transmisiones.

El expositor deberá tener certificación del fabricante en la solución a implementar, la cual deberá acreditar mediante constancia previa a la capacitación brindada.

7.12.5 Requerimientos del proveedor y de su personal

Requisitos del Postor

El Proveedor deberá cumplir con los siguientes requisitos:

- No estar impedido para contratar con el Estado.

¹⁴ En respuesta a la consulta N°23 formulada por el participante NEXTNET S.A.C.

¹⁵ En respuesta a la consulta N°38 formulada por el participante NEXTNET S.A.C.

- Contar con el RNP vigente al rubro objeto de la contratación.
- El postor debe acreditar un monto facturado acumulado equivalente a S/.400,000 (cuatrocientos mil con 00/100 soles), servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.
- En el caso de postores que declaren en el Anexo correspondiente tener la condición de micro y pequeña empresa, se acredita una experiencia S/.50,000 (cincuenta mil con 00/100), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Implementación y puesta en marcha de Internet con Seguridad Gerenciada via MPLS nacional y/o internacional.
- Servicio de Internet.
- Servicio de Internet Dedicado por medio de Fibra óptica.
- Servicio de Internet de Banda Ancha por medio de Fibra óptica,
- Servicio de Internet y/o Servicios de Transmisión de Datos y/o
- Transportes de Datos.
- Servicio de Acceso Corporativo a Internet y Seguridad Gestionada.
- Servicio de Internet Dedicado con Alta Disponibilidad y Seguridad Gestionada.
- Servicio de Acceso a Internet.
- Servicio de Internet Dedicado.
- Servicio de Internet Dedicado con Administrador de Ancho de Banda.
- Servicio de Internet Dedicado con Seguridad Gerenciada o Centralizada en Nube.
- Servicio de Internet e interconexión de datos
- Servicios de Internet con Fibra óptica
- Servicios de Internet basado en MPLS,
- Servicios de interconexión de datos vía protocolo MPLS nacional e internacional,
- Servicio de enlace de datos,
- Servicio de acceso e interconexión de enlace MPLS,
- Servicio de enlace dedicado MPLS,
- Servicio de interconexión de datos y servicios de interconexión a nivel nacional,
- Servicio de transmisión de datos.

Perfil del Proveedor

- El proveedor deberá ser i) partner certificado del fabricante de la solución ofertada o ii) el distribuidor del proveedor deberá ser partner certificado del fabricante de la solución ofertada, en dicho caso, deberá presentar documentación que demuestre la relación comercial del distribuidor con el proveedor o iii) el proveedor deberá estar habilitado en la venta de productos del fabricante de la solución a ofrecer; cualquiera que sea la condición del proveedor, deberá ser acreditada mediante certificado, constancia o carta, la cual se presentará para el perfeccionamiento del contrato.
- El proveedor debe ser miembro activo del NAP Perú, o podrá tener un punto de intercambio a través de un miembro activo del NAP Perú, se acreditará con la copia del certificado o declaración jurada o carta emitida por dicha entidad, el cual se presentará para el perfeccionamiento del contrato.
- El proveedor deberá contar con una red principal o Backbone propia y redundante, que tenga como medio de transporte fibra óptica.
- El proveedor deberá contar con una red de acceso propia y redundante, que tenga como medio de transporte fibra óptica.
- Debe contar con un NOC (Network Operations Center) propio, se acreditará con una Declaración Jurada, el cual se presentará para el perfeccionamiento del contrato.
- Debe contar con un SOC (Security Operations Center) propio o por un tercero, se acreditará con una Declaración Jurada, el cual se presentará para el perfeccionamiento del contrato.
- Podrá ser TIER1 y/o TIER2 y/o TIER3, se acreditará con una Declaración Jurada, el cual se presentará para el perfeccionamiento del contrato.

Perfil del Personal

El proveedor deberá acreditar el perfil del personal solicitado a la presentación del Plan de Trabajo.

El personal del proveedor deberá contar con el siguiente perfil profesional:

Jefe de Proyecto (01 persona):

- Profesional Titulado en las carreras de Ingeniería Electrónica, Sistemas, Computación y Sistemas, Eléctrica, Redes y Comunicaciones, Industrial y/o Telecomunicaciones.
- Certificación en Project Management Professional. ¹⁶
- Experiencia en al menos tres (03) proyectos de sistemas de Internet y/o Datos como líder de equipo o experiencia en proyectos de Sistemas de Seguridad Perimetral como líder de equipo.

¹⁶ En respuesta a la consulta N°15 formulada por el participante NEXTNET S.A.C.

Especialista (01 persona):

- Bachiller o Título Profesional en las carreras de Ingeniería Electrónica, Sistemas, Computación y Sistemas, Eléctrica, Redes y Comunicaciones, Industrial y/o Telecomunicaciones.
- Experiencia laboral en al menos tres (03) proyectos implementación de sistemas de internet con seguridad gerenciada.
- Certificación vigente de nivel asociado o profesional o avanzado o técnico en la especialidad de seguridad de redes y/o en la marca del equipo firewall y/o ciberseguridad. Se acreditará con copia de certificado o constancia.

La experiencia del personal se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Las actividades mínimas que deberá desarrollar son las siguientes:

Jefe de Proyectos:

- Elaborar el cronograma de implementación del proyecto.
- Realizar el seguimiento de la implementación del proyecto.
- Supervisar la implementación del proyecto.
- Elaborar los informes de avance de la implementación del proyecto. Elaborar el plan de trabajo e informe final.

Especialista:

- Elaborar el diseño e implementación de la solución.
- Elaborar el protocolo de pruebas y la configuración de todo el equipamiento de la solución.

7.12.6 Lugar y plazo de prestación del servicio**Lugar**

Todos los equipos indicados deberán entregarse e implementarse en el Data Center del Edificio Administrativo, Av. Del Aire cdra.8 s/n, San Luis. puerta 2, Latitude: 12°04'48.4"S Longitude: 77°00'05.5"W

Plazo**Plazo de Implementación¹⁷**

El proveedor tendrá hasta **sesenta (60)** días calendarios como máximo para la implementación y puesta en marcha de la solución, contabilizados a partir del día siguiente del perfeccionamiento del contrato y concluida la implementación

¹⁷ En respuesta a la consulta N°17 formulada por el participante NEXTNET S.A.C. y las observaciones N° 45 y 46 del participante COLINANET S.A.

se suscribirá el Acta de Conformidad Técnica para el inicio de la ejecución del servicio.

Plazo de Ejecución¹⁸

El plazo de ejecución del servicio será por **trescientos sesenta y seis (366)** días calendarios, el inicio se realizará desde el día siguiente de suscrita el Acta de Conformidad Técnica.

7.13 Resultados esperados

A partir del día siguiente de suscrita el acta de conformidad técnica, el proveedor tendrá hasta siete (07) días calendarios para la presentación del informe final de la implementación del servicio en digital vía correo electrónico, se espera el siguiente contenido como mínimo:

- El BOM de los equipos implementados.
- El inicio y fin del soporte de los equipos (vigencia).
- Pantallazos de la configuración realizada.
- Saturación del enlace para la conformidad del ancho de banda contratado.
- Pantallazos de las pruebas realizadas con la integración de la red LAN.
- Anexar los protocolos de prueba.
- Topología de red a detalle de lo implementado con detalle de los nodos a donde conectan mis servicios.

Así mismo, el proveedor deberá presentar un informe mensual sobre la utilización de la solución (estadísticas de consumo, tickets generados, etc), la misma que servirá como base de la conformidad mensual de pago; esta documentación deberá presentarlo de manera digital al responsable del área de Telecomunicaciones e Infraestructura de Red a través de Mesa de Partes de la institución.

7.14 Confidencialidad

El Proveedor está obligado a cumplir con las políticas y estándares definidos por el Proyecto Especial, en materia de seguridad de la información; en tal sentido debe guardar la reserva absoluta con respecto a la información a la que tenga acceso y que se encuentre relacionada con la prestación del servicio; quedando prohibido revelar dicha información a terceros. Están inmersos en estas políticas de seguridad, la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido el servicio. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos,

¹⁸ En respuesta a la consulta N°52 formulada por el participante GTD PERU S.A.

documentos y demás documentos e información compilados o recibidos por el Proveedor.

7.15 Medidas de control durante la ejecución contractual

Áreas que coordinarán con el Proveedor

- Dirección de Desarrollo Tecnológico y Transmisiones.
- Oficina de Administración

Áreas responsables de las medidas de control

- Dirección de Desarrollo Tecnológico y Transmisiones.

Área que brindará la conformidad

- Dirección de Desarrollo Tecnológico y Transmisiones, previo informe de la Sub- Dirección de Desarrollo Tecnológico.

7.16 Conformidad:

La conformidad será otorgada por la Dirección de Desarrollo Tecnológico y Transmisiones, previo informe del especialista designado por la misma Subdirección. Asimismo, de acuerdo con el artículo 168 del Reglamento de la Ley de Contrataciones del Estado, modificado por el Decreto Supremos 168-2020-EF, la conformidad se emite en un plazo máximo de siete (7) días de producida la recepción del entregable.

"Artículo 168. Recepción y conformidad" (...)

168.3. La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, o si se trata de consultorías, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

168.4. De existir observaciones, la Entidad las comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho

(08) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar, o si se trata de consultorías, el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

7.17 Forma de pago

El Proveedor pagará de la siguiente manera:

- La forma de pago será mensual, previa presentación del comprobante de pago e Informe de la Dirección de Desarrollo Tecnológico y Transmisiones, emitiendo la conformidad de la prestación efectuada.
- El ciclo de facturación, será el más cercano a la fecha de activación del servicio. En caso de que el servicio se inicie unos días antes

del comienzo del ciclo de facturación, el primer recibo incluirá un cargo prorrateado por el servicio brindado por esos primeros días, lo mismo se presentará en el último recibo del servicio. De corresponder.

- Para el pago, el proveedor deberá presentar lo siguiente:
 - Un informe sobre la utilización de la solución (estadísticas de consumo por sede, tickets generados durante el mes a facturar, el estado de los equipos CPE's, etc); esta documentación deberá presentarlo de manera digital a través de Mesa de Partes de la institución.
 - Comprobante de Pago.
- Los entregables serán presentados a través de mesa de partes virtual en el siguiente link <https://legado.gob.pe/formulario-mesa-de-partes> o físicamente en Mesa de Partes: Av. San Luis cuadra 11 S/N, Sede de la Villa Deportiva Nacional (VIDENA) Puerta N°6- Cruce Av. Del Aire, distrito San Luis, provincia y departamento de Lima de 8:30 a.m. a 4:30 p.m, como máximo 05 días calendario después de finalizado el periodo de facturación y dirigido a la de Dirección de Desarrollo Tecnológico y Transmisiones.

7.18 Penalidad

En la ejecución de la prestación, en caso de retraso injustificado por el contratista, la Entidad aplicará de forma automática una penalidad por cada día de atraso. La Penalidad se calcula de la siguiente forma:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F tiene los siguientes valores:

F=0.40 para plazos menores o iguales a 60 días

F = 0.25 para plazos mayores a 60 días

Monto = Monto de la Orden de Compra o Servicio
Plazo en días = Plazo de cumplimiento de la ejecución contractual

La penalidad máxima aplicable será hasta el 10% del monto del contrato.

Asimismo, cuando se llegue a cubrir el monto máximo de la penalidad el Proyecto Especial podrá resolver la orden de compra parcial o totalmente por el incumplimiento.

7.19 Otras Penalidades

A fin de propiciar la correcta ejecución del servicio, se establecen las siguientes penalidades (basadas en el valor del UIT vigente a la firma del contrato):

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	POR LA INTERRUPCION DEL SERVICIO		

1.1	Interrupciones en el servicio no programadas e imputables al contratista (corte parcial, total o decremento en la calidad de las comunicaciones) cuya duración sea menor a una (01) hora.	Entre dos (02) y cuatro (04) interrupciones al mes	5% UIT	Informe del responsable técnico designado por el área usuaria.
		Más de cuatro (04) interrupciones al mes	10% UIT	Informe del responsable técnico designado por el área usuaria.
1.2	Interrupciones en el servicio no programadas e imputables al contratista (corte parcial, total o decremento en la calidad de las comunicaciones) cuya duración esté entre una (01) y cuatro (04) horas.	Entre dos (02) y cuatro (04) interrupciones al mes	15% UIT	Informe del responsable técnico designado por el área usuaria.
		Más de cuatro (04) interrupciones al mes	30% UIT	Informe del responsable técnico designado por el área usuaria.
2	POR RETRASO EN LA ATENCIÓN DE AVERÍAS/CONFIGURACIONES			
2.1	Tiempo de respuesta para la atención de averías/configuraciones. (Tiempo de atención y plazo para brindar una respuesta para cualquier llamada del Proyecto Especial en la que reporte una avería). Que sobrepasen el límite permitido en el numeral 7.12.1, 7.12.2 y 7.12.3	Hasta una (01) hora de retraso	1% UIT	Informe del responsable técnico designado por el área usuaria.
		Más de una (01) y dos (02) horas de retraso	2% UIT	Informe del responsable técnico designado por el área usuaria.
		Por más de dos (02) horas de retraso	3% UIT	Informe del responsable técnico designado por el área usuaria.
3	RETRASO POR REPARACIONES DE AVERÍAS			
3.1	Tiempo de resolución de averías imputables al proveedor (Tiempo en que se dará solución a avería reportada) que sobrepasen el límite permitido en el numeral 7.12.1, 7.12.2 y 7.12.3	Hasta una (01) hora de retraso	10% UIT	Informe del responsable técnico designado por el área usuaria.
		Más de una (01) y dos (02) horas de retraso	15% UIT	Informe del responsable técnico designado por el área usuaria.
		Más de dos (02) y tres (03) horas de retraso	20% UIT	Informe del responsable técnico designado por el área usuaria.
		Entre tres (03) y cuatro (04) horas de retraso	25% UIT	Informe del responsable técnico designado por el área usuaria.
		Por más de cuatro (04) horas de retraso	30% UIT	Informe del responsable técnico designado por el área usuaria.

7.20 Responsabilidad por vicios ocultos

La conformidad del servicio por parte de Área Usuaria no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto

por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por el Área Usuaria.

7.21 Resolución de Contrato

Si el proveedor incumpliera injustificadamente con las condiciones establecidas en los términos de referencia y las obligaciones contractuales, la Entidad podrá resolver el contrato en forma parcial o total, de acuerdo con lo establecido en el artículo 165 del reglamento de la Ley de Contrataciones del Estado.

7.22 Condiciones Generales

- El proveedor será el único responsable ante la Entidad de cumplir con la prestación del servicio para el cual fue adjudicado, asimismo, no podrá subcontratar en el marco de lo permitido por el artículo 35 de la Ley de Contrataciones del Estado y en el artículo 147 de su reglamento.
- Se requiere que el Proveedor suministre el Seguro Complementario de Trabajo de Riesgo (SCTR) para el personal designado a realizar la entrega del servicio, así como también con sus equipos de protección personal y de bioseguridad. El Proyecto Especial no permitirá en ninguna circunstancia que el personal del proveedor realice los trabajos sin el SCTR.
- La conformidad de recepción de los bienes no invalida el reclamo posterior por parte de la Entidad por defecto o vicios ocultos u otras situaciones anómalas no detectables o no verificables en la recepción de los bienes, reservándose la Entidad el derecho de iniciar las acciones administrativas y/o legales a que hubiese lugar.

7.23 CLÁUSULA ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

3.2 REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	Autorización del Ministerio de Transporte y Comunicaciones (MTC) para brindar los servicios de valor añadido en la modalidad de: (i) Almacenamiento y retransmisión de datos o (ii) Teleproceso y procesamiento de datos o (iii) Conmutación de datos por paquetes acompañado del Oficio del Ministerio de Transportes y Comunicaciones donde se identifique las concesiones vigentes; con cobertura en el departamento de Lima o a nivel nacional.
	<div>Importante</div> <p>De conformidad con la Opinión No 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.</p> <p>Acreditación:</p> <p>Copia del documento de la autorización emitida por el Ministerio de Transportes y Comunicaciones o copia del Registro Vigente de empresas Prestadoras de Servicios de Valor Añadido del portal del MTC, en donde se verifique la autorización para brindar servicios de valor añadido en (i) almacenamiento y retransmisión de datos o (ii) teleproceso y procesamiento de datos o (iii) Conmutación de datos por paquetes acompañado del Oficio del Ministerio de Transportes y Comunicaciones donde se identifique las concesiones vigentes; con cobertura en el departamento de Lima o a nivel nacional.</p> <div>Importante</div> <p>En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.</p>
B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p>Requisitos:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente S/ 400,000.00 (cuatrocientos mil con 00/100 soles) de la contratación, servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo correspondiente tener la condición de micro y pequeña empresa, se acredita una experiencia del S/ 50,000.00 (cincuenta mil con 00/100 soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del</p>

comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Implementación y puesta en marcha de Internet con Seguridad Gerenciada via MPLS nacional y/o internacional.
- Servicio de Internet.
- Servicio de Internet Dedicado por medio de Fibra óptica.
- Servicio de Internet de Banda Ancha por medio de Fibra óptica,
- Servicio de Internet y/o Servicios de Transmisión de Datos y/o
- Transportes de Datos.
- Servicio de Acceso Corporativo a Internet y Seguridad Gestionada.
- Servicio de Internet Dedicado con Alta Disponibilidad y Seguridad Gestionada.
- Servicio de Acceso a Internet.
- Servicio de Internet Dedicado.
- Servicio de Internet Dedicado con Administrador de Ancho de Banda.
- Servicio de Internet Dedicado con Seguridad Gerenciada o Centralizada en Nube.
- Servicio de Internet e interconexión de datos
- Servicios de Internet con Fibra óptica
- Servicios de Internet basado en MPLS,
- Servicios de interconexión de datos vía protocolo MPLS nacional e internacional,
- Servicio de enlace de datos,
- Servicio de acceso e interconexión de enlace MPLS,
- Servicio de enlace dedicado MPLS,
- Servicio de interconexión de datos y servicios de interconexión a nivel nacional,
- Servicio de transmisión de datos.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo No 7 referido a la Experiencia del Postor en la Especialidad

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentadora correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo correspondiente

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo correspondiente referido a la Experiencia del Postor en la Especialidad.

Importante

- Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.
- En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".