LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

TÉRMINOS DE REFERENCIA

SERVICIO DE INTERNET Y RED DE DATOS PARA LIMA Y PROVINCIAS, E IMPLEMENTACIÓN DE LA SOLUCIÓN DE ENLACE DE FIBRA ÓPTICA OSCURA ENTRE LOS LOCALES SEDE CENTRAL Y LA ESCUELA NACIONAL DE CONTROL DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ

I. ÁREA USUARIA

Subgerencia de Operaciones y Plataforma Tecnológica.

II. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de internet y red de datos para Lima y provincias, e implementación de la solución de enlace de fibra óptica oscura entre los locales Sede Central y la Escuela Nacional de Control de la Contraloría General de la República del Perú.

III. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

La presente contratación busca contar con el servicio de Internet y red de datos para las sedes de la CGR, así como la interconexión en la Sede Central y Escuela Nacional de Control, estos servicios permitirán asegurar la continuidad de las comunicaciones, enlaces y transmisión de datos entre las sedes y el acceso al servicio de Internet, con la finalidad de garantizar y mejorar la calidad de los servicios a los clientes internos y externos, así como para mejorar la “Gestión de Riesgos” y “Gestión de la Continuidad del Negocio” de la Contraloría General de la República (CGR), lo que contribuirá con la Institución en la continuidad de sus operaciones y en su labor de fiscalización y lucha contra la corrupción.

IV. OBJETIVO GENERAL DE LA CONTRATACIÓN

1. La Gerencia de Tecnologías de la Información como encargado de dirigir y ejecutar las actividades relacionadas con las tecnologías de la información (TI), la operatividad de los equipos de procesamiento de información y el buen funcionamiento de la red de transmisión de comunicaciones que soporte los procesos de la Contraloría General de la República, ha contemplado la contratación de una empresa especializada en telecomunicaciones que brinde el servicio de Internet y red de datos cuyo medio de comunicación este basado en cableado de fibra óptica; con la finalidad de garantizar y mejorar la calidad de los servicios de TI, así como para mejorar la “Gestión de Riesgos” y “Gestión de la Continuidad del Negocio” de la Institución, lo que contribuirá en su labor de fiscalización y lucha contra la corrupción. Este servicio debe ser brindado de manera ininterrumpidamente las veinticuatro (24) horas del día, durante el plazo de ejecución contractual y estará dirigido para las siguientes sedes:
   a) Los Órganos Instructores de Arequipa, Lambayeque y Junín.
   b) Las Gerencias Regionales de Control: Ica, Ancash-Local-1, San Martín, Junín-local-1, Apurímac, Cusco, Huánuco, Arequipa, Tacna, La Libertad, Cajamarca, Piura, Lambayeque, Puno, Loreto, Ayacucho, Moquegua, Huancavelica, Junín-local-2, Ucayali, Tumbes, Amazonas, Madre de Dios, Ancash-Local-2, Pasco y Lima Provincias.
   c) Las sedes en Lima: Cusipata, Javier Prado, Sede Central y Sede Escuela Nacional de Control (ENC), Arequipa-1593, Sede-Ancón, Sede-01, Sede-02 y Sede-03.

2. Contratar una empresa que se encargará de brindar el servicio de implementación de solución de enlace de fibra óptica oscura entre los locales sede Central y la Escuela Nacional de Control (ENC).

V. ALCANCE Y ACTIVIDADES A DESARROLLAR

a) Brindar servicio de Internet a la CGR, mediante dos enlaces independientes (los cuales deberán provenir de nodos diferentes) y a través de fibra óptica.
b) Brindar el medio de comunicación en todas las sedes de la CGR, mediante dos enlaces independientes (los cuales deberán provenir de nodos diferentes) y a través de fibra óptica sobre la red MPLS.
c) Brindar una comunicación entre la Sede Central y la Escuela Nacional de Control mediante enlaces por fibra óptica oscura monomodo.

VI. CARACTERÍSTICAS DEL SERVICIO

1. ÍTEM 01: SERVICIO DE INTERNET Y RED DE DATOS PARA LIMA Y PROVINCIAS PARA LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ

1.1. PRESTACION PRINCIPAL

1.1.1. SERVICIO DE INTERNET

1.1.1.1. REQUISITOS GENERALES:

Brindar el medio de comunicación para el servicio de Internet en la Sede Central y Sede Escuela Nacional de Control, basado en cableado de fibra óptica.
El servicio de Internet brindado a la CGR por parte del contratista, debe incluir la dotación, instalación, configuración del hardware y software para la implementación y puesta en producción del presente servicio.

Por la importancia de este servicio para la gestión de la CGR, se requiere que el contratista garantice una disponibilidad del 99.90% mensual del servicio, siendo necesario que el contratista incluya la implementación de los enlaces solicitados, con la finalidad de garantizar la continuidad del servicio ante una falla.

1.1.1.2. CARACTERÍSTICAS TÉCNICAS:

El servicio de Internet debe ser del tipo digital, haciendo uso de cableado de fibra óptica (FO), la implementación y configuración del equipamiento asociado debe ser ejecutada por el contratista, además este servicio debe brindar un ancho de banda mínimo de mil veinticuatro (1024) Mbps para cada uno de los dos enlaces (Sede Central y Sede Escuela Nacional de Control), de acuerdo a lo siguiente:

a) Se debe implementar dos enlaces (Principal y Secundario) que operarán en modo activo-activo.
b) El enlace Principal estará implementado en la Sede Central y el enlace Secundario estará implementado en la sede Escuela Nacional de Control (ENC).
c) El enlace en la Sede Central operará de modo activo, será instalado en la Sede Central de la CGR con dirección Jr. Camilo Carrillo 114, Jesús María – Lima.
d) El enlace de la Sede Escuela Nacional de Control operará de modo activo, será instalado en la Sede de la Escuela Nacional de Control (ENC) con dirección Jr. Bartolomé Herrera 255, Lince, Lima.
e) Los enlaces instalados en la Sede Central y en la Sede de la Escuela Nacional deben estar configurado (en redundancia) y en balanceo de carga; es decir, ante la caída de uno de los enlaces, todo el tráfico pueda pasar por el segundo enlace de manera automática.
f) Los enlaces operarán en circuitos independientes, se precisa que, ante la caída de uno de los enlaces, conmute automática e inmediatamente hacia el segundo enlace. Una vez que el enlace caído, se encuentre, nuevamente activo, todo regresa al esquema original, de tal manera que, ante la caída de uno de los enlaces, el otro enlace mantenga operativa las conexiones. Cabe resaltar que para que se cumpla esto el tendido de FO (fibra óptica) los circuitos deben tener diferente ruta y diferente nodo de acceso en todo su recorrido.
g) Los dos enlaces deben estar configurados en modo balanceo de carga, asimismo, ante la caída de uno de los enlaces, el otro enlace debe aumentar (al doble) de su capacidad de ancho de banda (2048Mbps), mientras dure la caída de uno de los enlaces.

Características de los enlaces a Internet:

h) Overbooking Garantizando de 1:1 (Local)
i) Ancho de Banda 100% garantizado, (Upstream y Downstream simétrico)
j) Disponibilidad del servicio de Internet debe ser como mínimo del 99.90% mensual.
k) Proporcionar el DNS y asignación de 160 direcciones IPv4 públicas estáticas permanentes (divididas en 2 bloques: primer bloque de 128 direcciones IPv4 consecutivas y segundo bloque de 32 direcciones IPv4 consecutivas) y de 160 direcciones IPv6 públicas estáticas permanentes consecutivas (incluye la dirección IP Lan router principal, IP Lan router Back up, IP Virtual, IP de Red, IP de Broadcast).
l) Uso de Internet sin restricciones y tráfico limpio, con lo cual se asegurará el funcionamiento de cualquier tipo de aplicación que se ejecute sobre el protocolo TCP/IP.
m) Acceso abierto y sin restricciones, donde CGR pueda enviar información y servicios al alcance de cualquier usuario conectado a Internet.
n) Todos los equipos que sean utilizados en la infraestructura de comunicaciones deberán ser de tecnología vigente (deben de tener como máximo dos (2) años de fabricación, contabilizados desde la convocatoria del servicio) y que no entren en obsolescencia durante el periodo del servicio, contando con el respaldo de la marca, en la cual el contratista debe presentar una carta del fabricante donde indique que el equipamiento no está en EOS (Fin de Venta o End Of Sale) y EOL (Fin de Vida o End Of Live) y que cuenta con soporte vigente del fabricante (durante el plazo de ejecución contractual), dicha carta será presentada conjuntamente con el Plan de trabajo (numeral 1,6, literal a). Además, estos equipos deberán estar debidamente etiquetados, rotulados y acondicionados con la finalidad de evitar la manipulación por personal no autorizado.
o) El recorrido de los enlaces de Internet deberá ser canalizado: subterráneo o aéreo, desde el nodo más cercano del contratista hasta el ambiente proporcionado por la CGR.
p) El backbone de la red local del contratista deberá ser de anillos de fibra óptica redundante. Se aclara que se necesita que el contratista tenga por lo menos dos (2) operadores internacionales cuyos enlaces deben estar implementados con fibra óptica.
q) El contratista deberá contar con acceso de salida internacional al Backbone de Internet, a través de rutas distintas y redundantes; además, debe contar por lo menos con dos (2) proveedores internacionales como mínimo y con capacidades de 20 Gbps (las capacidades es la suma de los dos (2) proveedores internacionales) como mínimo, para evitar problemas de indisponibilidad del servicio de acceso a Internet contratado.
r) Se requiere que el medio de transmisión sea de alta flexibilidad y conectividad para el uso de video e imagen.
s) El servicio podrá tener capacidad de servidores caches distribuidos en la red sobre la cual se ofrece el servicio, a nivel nacional. Este servicio permitirá almacenar temporalmente sitios de mayor consulta.
t) El servicio debe contar con una latencia promedio máximo de red de 20 ms en el acceso, el cual será medido desde el equipo con Internet desplegado por el contratista en la CGR y el nodo más cercano del contratista.
u) El servicio debe contar con múltiple redundancia dentro de la red, el contratista deberá adjuntar el esquema topológico (diagramas) de cada punto solicitado, el cual será presentado para el perfeccionamiento del contrato.
    i. Redundancia en los equipos de ruteo
    ii. Redundancia en el Backbone
    iii. Redundancia en los servidores DNS.
    iv. Redundancia en los enlaces de Salida Internacional
v) Los equipos no podrán tener la contraseña por defecto, ni contraseñas fáciles de deducir. Además, no podrán ser accedidos mediante protocolos inseguros para su administración y sólo podrá ser gestionado desde las direcciones IP del contratista (debe tener lista de control de acceso implementadas).
w) Contar con un sistema de monitoreo vía web del servicio contratado en forma permanente, las mismas que deben estar disponibles para el personal responsable

de Informática de la CGR. Deberá proporcionar informes del consumo del ancho de banda de ingreso y egreso del enlace (en Kbps o Mbps) en forma diaria, mensual e histórica de los últimos 12 meses. El sistema de monitoreo deberá medir el rendimiento y comportamiento de los enlaces, para ello como mínimo deberá medir los siguientes parámetros: disponibilidad, latencia, pérdida de paquetes.

x) El contratista debe estar en la capacidad de entregar los registros (a solicitud de la CGR) del tráfico del consumo de ancho de banda de todas las sedes a nivel nacional durante el plazo de ejecución del servicio.

y) Todos los permisos, licencias y obras civiles requeridas para el servicio, si fuera el caso, estas se realizarán en su totalidad por cuenta del contratista.

z) El contratista brindará el servicio del registro de nuevos dominios y nuevos registros DNS asociados a un dominio creado directo e inverso entre otros para todas las direcciones IP que se le indique, la atención será las 24 horas los 7 días durante el plazo de ejecución del servicio, asimismo se solicita la posibilidad que sea administrado por el personal de la CGR.

aa) El contratista brindará el servicio de la migración de los dominios y registros DNS actuales.

bb) El contratista brindará una plataforma en la nube (accedida a través de una dirección IP Pública), con las siguientes características:

i. Espacio de almacenamiento mínimo de 1 TB para alojar información o archivos (tipo PDF, Word, Excel, Imágenes, etc.), a modo de Web Hosting, el cual será administrado por personal de la CGR.

ii. Deberá poseer una IP púbica, y debe brindar el soporte necesario para cargas y descargas ilimitadas de archivos.

iii. Deberá soportar un tráfico de ancho de banda de subida y bajada (mínimo 300 Mbps) para la transferencia de los documentos que se necesiten publicar y los documentos que se necesiten descargar.

iv. La IP pública deberá estar asociado al servidor doc.contraloria.gob.pe.

v. El contratista debe proporcionar e instalar un certificado digital del tipo EV para el servidor doc.contraloria.gob.pe por un periodo según el plazo de ejecución del servicio, en el servidor de la plataforma.

vi. La plataforma deberá tener habilitado los puertos HTTP, HTTPS, FTP, RDP y adicionalmente se deberá habilitar otros puertos a demanda de la CGR en coordinación con el Ingeniero residente dedicado del contratista.

vii. 32GRAM; Windows Server 2022; 4 procesadores con 8 cores cada uno con velocidad mínima de 3.9GHZ cada procesador, velocidad de la tarjeta de red de 1Gbps.

viii. La administración del servidor será de acceso restringido por IP o a través de un enlace VPN.

cc) El contratista estará a cargo de la configuración del servicio de acuerdo a las necesidades de la CGR.

dd) Se dará conformidad a la validación de los enlaces luego de cumplir como mínimo las siguientes acciones:

i. Instalación y configuración de los equipos de telecomunicaciones.

ii. Pruebas de Validación, tendrán como objetivo validar la correcta instalación, configuración y funcionamiento de cada enlace; al término de las pruebas de validación se firmará un “Acta de validación” por cada enlace instalado.

iii. Sincronizar los equipos de telecomunicaciones que forman parte de la Red con el Servidor NTP (Network Time Protocol) que CGR tiene instalado.

ee) El contratista deberá presentar un cuadro con los costos desagregados del servicio brindado a cada una de las sedes.

SERVICIO DE INSTALACIÓN

El contratista se obliga a ejecutar la instalación de los equipos, materiales, accesorios y todo lo necesario para brindar el servicio en todas las sedes a nivel nacional según corresponda, a fin de dejar completamente habilitado la prestación del servicio a entera satisfacción de la Contraloría General de la República del Perú.

Cada uno de los enlaces solicitados deben tener equipos de comunicación independientes del segundo enlace; es decir, cada enlace con sus propios equipos, de tal manera que la disponibilidad y la calidad de los servicios estén garantizados.

1.1.2. SERVICIO DE RED MPLS

1.1.2.1. REQUISITOS GENERALES:

Brindar el medio de comunicación a través fibra óptica (aéreo o subterráneo), mediante dos enlaces Principal y Secundario para el servicio de transmisión de datos, voz, video, video-conferencia, video-vigilancia y aplicaciones sobre la red MPLS del contratista en todas las sedes de la CGR a nivel nacional (ver Tabla N° 01), el cual permita el acceso a los servidores principales ubicados en los Centros de Datos de Lima, para lo cual incluye los siguientes enlaces:

a) Cada Sede Remota, se debe implementar dos enlaces (Principal y Secundario)
b) Los dos enlaces (Principal y Secundario) deben operar en modo activo-activo
c) Para el caso de Nodo Origen: Sede Central y Sede ENC:
    i) Enlace Principal: Deberá hacer la instalación de un enlace el que funcionará en modo activo de tal manera que reciba las peticiones o comunicaciones de las sedes remotas, este enlace será instalado en la Sede Central ubicado en la dirección de Jr. Camilo Carrillo114, Jesús María – Lima, y
    ii) Enlace Secundario: Deberá hacer la instalación de un enlace el que funcionará en modo activo de tal manera que reciba las peticiones o comunicaciones de las sedes remotas, este enlace será instalado en la Sede de la Escuela Nacional de Control ubicado en la Dirección Jr. Bartolomé Herrera 255, Lince, Lima.
d) Los enlaces (Principal y Secundario) instalados deben estar configurado (en redundancia) y en balanceo de carga; es decir, ante la caída de uno de los enlaces, todo el tráfico pueda pasar por el segundo enlace el cual debe aumentar (al doble) de su capacidad de ancho de banda, mientras dure la caída del primer enlace.
e) Los enlaces operarán en circuitos independientes, se precisa que, ante la caída de uno de los enlaces (Principal o Secundario), todo el tráfico será realizado a través del segundo enlace de manera automática e inmediata. Una vez que el enlace caído, se encuentre, nuevamente activo, todo regresa al esquema original, de tal manera que, ante la caída de uno de los enlaces, el otro enlace mantenga operativa las conexiones. Cabe resaltar que para que se cumpla esto el tendido de FO (fibra óptica) los circuitos deben tener diferente ruta y diferente nodo de acceso en todo su recorrido.
f) Los dos enlaces deben ser por medio de fibra óptica en todo su recorrido de la red MPLS.

El servicio brindado a la CGR por parte del contratista, debe incluir la dotación, instalación, configuración, y el licenciamiento total del hardware y software involucrado para la implementación y puesta en producción del servicio. Cabe precisar que:

g) En el Nodo Origen (Sede Central y Sede Escuela Nacional de Control) y la Sedes a nivel nacional (Sedes Remotas), cuentan con switch LAN, gabinetes o racks, tendido de cableado eléctrico y pozo a tierra en las salas de comunicaciones.
h) En el Nodo Origen (Sede Central y Sede Escuela Nacional de Control) cuenta con energía estabilizada y UPS.

Por lo que, el contratista deberá proveer para las Sedes Remotas todo lo necesario relacionado a la operación del servicio como:

- UPS (monitoreable), para lo cual el contratista deberá brindar como mínimo una interfaz web para el monitoreo del estado del equipo, el UPS debe soportar como mínimo protocolos ICMP, SNMP, HTTP y HTTPS, y debe permitir su integración a una herramienta de monitoreo web también brindada por el contratista.
- Patch cord,
- entre otros de tal manera que permita asegurar la operatividad del servicio.

Es responsabilidad del contratista realizar el cableado que sea necesario desde sus nodos de acceso hasta el switch del Nodo Origen (Sede Central y Sede Escuela Nacional de Control) y de las Sedes remotas.

Para el caso de los equipos UPS, el contratista deberá proporcionar dos equipos con una capacidad de 2 Kw (cada uno, como mínimo) para todas las sedes (indicadas en la Tabla N° 01) a excepción en el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), de modo que pueda brindar soporte a los equipos que se encuentran en cada uno de los gabinetes de cómputo de las sedes.

Por la importancia de este servicio se necesita que el contratista garantice:

i) Una disponibilidad del servicio mínimo del 99.90% mensual para el servicio en el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), Sedes Remotas (dentro de Lima Metropolitana), cabeceras de la red MPLS y
j) Una disponibilidad del servicio mínimo del 99.70% mensual para el servicio en cada uno de las Sedes Remotas en Provincia (fuera de Lima Metropolitana) indicada en la Tabla N° 01.

Es necesario que el contratista realice la implementación de los enlaces Principal y Secundario en el Nodo Origen (Sede Central y Sede Escuela Nacional de Control) de la red MPLS, con la finalidad de garantizar la continuidad del servicio ante una falla de uno de los enlaces.

Para cumplir la disponibilidad solicitada (continuidad del servicio), el enlace Secundario deberá ser por diferentes rutas y diferentes nodos de acceso del enlace Principal en todo su recorrido.
La solución debe proveer el equipamiento necesario que permita la administración y gestión de los logs generados en los equipos de telecomunicaciones de los enlaces de las Sedes Remotas y Nodo Origen (Sede Central y Sede Escuela Nacional de Control).

La comunicación a través de la red MPLS deberá estar cifrada para lo cual el contratista deberá proveer equipos de seguridad en cada uno del Nodo Origen (Sede Central y Sede Escuela Nacional de Control) y las Sedes Remotas (Tabla N° 01), tal como se indica en el punto 1.1.4.

1.1.2.2. CARACTERÍSTICAS TÉCNICAS:

Los enlaces deben ser del tipo digital con tecnología MPLS, haciendo uso de cableado por fibra óptica, la configuración del equipamiento asociado debe ser ejecutada por el contratista, de acuerdo al siguiente detalle:

Tabla N° 01
Características de los enlaces MPLS por sedes a nivel nacional

Nº	Nodo Origen *1	Nodo Destino a Nivel Nacional		Velocidad Mbps (de cada enlace)
		Sedes a nivel nacional (SEDES REMOTAS)	Dirección	
1	Sede Central: Enlace Principal – Velocidad (Sumatoria del ancho de banda de todos los enlaces **PRINCIPALES** de las **SEDES**	Gerencia Regional de Control Ica	Av. Los Maestros D-12 - Urb. San José - Ica, Ica, Ica	40
2		Gerencia Regional de Control Ancash – Local 1	Jr. José de Sucre N° 877, 879-A, 879-B, (Zona Comercial Mz C-6, Lote 4), distrito Huaraz, Provincia Huaraz y Departamento de Ancash.	40
3		Gerencia Regional de Control San Martín	Jr. Callao cdra. 5 S/N (al costado del local INEI y frente al hotel Bethel) Barrio de Calvario, Mz. 3140 lote 21, Sector Pueblo Tradicional Cercado de	40

Nº	Nodo Origen *1	Nodo Destino a Nivel Nacional		Velocidad Mbps (de cada enlace)
		Sedes a nivel nacional (SEDES REMOTAS)	Dirección	
	REMOTAS que se encuentran **ACTIVAS u OPERATIVAS**) Mbps y Sede ENC: Enlace Secundario - Velocidad (Sumatoria del ancho de banda de todos los enlaces **SECUNDARIOS** de las **SEDES REMOTAS** que se encuentran **ACTIVAS u OPERATIVAS**) Mbps.		Moyobamba, distrito y provincia de Moyobamba, departamento de San Martín	
4		Gerencia Regional de Control Junín - Local 1	Jr. Lima N° 338-346 - Huancayo, Junín, Junín.	40
5		Gerencia Regional de Control Apurímac	Jr. Junín N° 215 - Abancay, Abancay, Abancay	40
6		Gerencia Regional de Control Cusco	Avenida Pachacutec N° 609, distrito de Wanchaq, provincia de Cusco	40
7		Gerencia Regional de Control Huánuco	Jr. Dos de Mayo N° 1759 - 1763 - Huánuco, Huánuco, Huánuco	40
8		Gerencia Regional de Control Arequipa	Cl. Peral N° 102-104 Cercado - Arequipa, Arequipa, Arequipa	40
9		Gerencia Regional de Control Tacna	Calle Los Alamos N° 1978 - 1979, Urbanización Quinta Aurora, Tacna, Tacna, Tacna	40
10		Gerencia Regional de Control La Libertad	Jr. Juan Pablo II N° 583 – Trujillo, Trujillo, La Libertad.	40
11		Gerencia Regional de Control Cajamarca	Mz. C Lote 4 Jr. Cápac Yupanqui S/N Sector Bellavista, Complejo Qhapac Ñan – Cajamarca, Cajamarca, Cajamarca.	40
12		Gerencia Regional de Control Piura	Esq. Jr., Lima c/ Huánuco s/n - Piura, Piura, Piura	40
13		Gerencia Regional de Control Lambayeque	Av. Elías Aguirre N° 896 - Chiclayo, Chiclayo, Lambayeque	40
14		Gerencia Regional de Control Puno	Jr. Deustua 822 - Puno, Puno, Puno	40
15		Gerencia Regional de Control Loreto	Jr. Tacna 432, distrito de Iquitos, provincia de Maynas, departamento de Loreto.	25
16		Gerencia Regional de Control Ayacucho	Av. Carmen Alto S/N Sublote 1A-4 distrito Carmen Alto provincia Huamanga, Ayacucho	40
17		Gerencia Regional de Control Moquegua	Cl. Cusco N° 421 - Moquegua, Mariscal Nieto, Moquegua	40
18		Gerencia Regional de Control Huancavelica	Jirón Antonio Raymondi N°247 Huancavelica	40
19		Gerencia Regional de Control Junín - Local 2	Av. Daniel Alcides Carrión N° 1481 - Huancayo, Junín, Junín	40
20		Gerencia Regional de Control Ucayali	Jr. Atahualpa 945, Mz.24, Lote 06 - Callería, Coronel Portillo, Ucayali	40
21		Gerencia Regional de Control Tumbes	Av. Fernando Belaunde T. Mz 1 Lote 17 - Urb. Andrés Araujo Morán, Tumbes, Tumbes	40
22		Órgano Instructor Lambayeque	Cl. Juan Cuglievan N° 470 - Chiclayo, Chiclayo, Lambayeque	40
23		Órgano Instructor Junín	Av. Arequipa N° 215, 215-A, 217 - El Tambo, Huancayo, Junín	40
24		Órgano Instructor Arequipa	Av. Cayma N° 304 - Cayma, Arequipa, Arequipa	40
25		Gerencia Regional de Control Amazonas	Jr. Hermosura N° 720 - Chachapoyas, Chachapoyas, Amazonas	40
26		Gerencia Regional de Control Madre de Dios	Jr. Manuel Gonzáles Prada N° 241 - Puerto Maldonado, Tambopata, Madre de Dios.	40

Nº	Nodo Origen *1	Nodo Destino a Nivel Nacional		Velocidad Mbps (de cada enlace)
		Sedes a nivel nacional (SEDES REMOTAS)	Dirección	
27		Oficina de enlace de la Gerencia Regional de Control Ancash -Local 2	Mz. F2 Lote. 10 Sector 5D, Urbanización. Buenos Aires – Nuevo Chimbote, Santa, Ancash	40
28		Gerencia Regional de Control de Pasco	Jirón San Martín 116, Urbanización San Juan de Pampa, Yanacancha, Pasco, Pasco, Intercepción con Jirón Ramón Castilla	40
29		Gerencia Regional de Control Lima Provincias	Av. Túpac Amaru N° 209-211, ciudad de Huacho, provincia de Huaura, departamento de Lima.	40
30		Cusipata	Prolongación Los Álamos 983 Urb. Cusipata Km. 24 Carretera Central, Lima Metropolitana	40
31		Javier Prado	Calle Los Sauces Nº 450 Urb. Jacarandá - San Borja – Lima Metropolitana	40
32		Sede-Ancón	LL, A-2, Kartodromo de Santa Rosa, distrito de Santa Rosa, provincia de Lima, departamento de Lima, Lima Metropolitana	200
33		Arequipa-N°1593	Av. Arequipa N° 1593-1599, esquina con el Jr. Emilio Althaus, Cercado de Lima, Lima	1000
34		Sede-01	La Perla, Callao.	1000
35		Sede-02	Lima Metropolitana - Miraflores	1000
36		Sede-03	Lima Metropolitana - Magdalena	1000

***1:** Sólo se brindará conformidad por el ancho de banda ACTIVO (Sumatorias de los anchos de bandas de las Sedes Remotas operativos) para los Enlaces Principal y Secundario del Nodo Origen.

a) La Entidad comunicará al contratista el inicio de la implementación del servicio en las sedes: Sede-Ancón, Sede-01, Sede-02 y Sede-03, por tanto, no se realizará pago por estas cuatro sedes mientras no se tenga habilitado el servicio. El plazo de implementación será contabilizado desde la notificación de la CGR para iniciar las actividades de implementación, y será en un plazo máximo de 90 días calendarios. Para el inicio del servicio y facturación deberá ser a partir del día siguiente a la fecha de la firma del “Acta de Activación del Servicio”, previa coordinación con la Entidad.

b) El inicio del servicio y facturación correspondiente a la sede Arequipa-N°1593, deberá ser a partir del día siguiente a la fecha de firma del “Acta de Activación del Servicio”, previa coordinación con la Entidad.

c) Cada uno de los enlaces solicitados deben tener equipos de comunicación independientes del segundo enlace; es decir, cada enlace con sus propios equipos, de tal manera que la disponibilidad y la calidad de los servicios estén garantizados

d) El contratista debe proveer una aplicación Web (software) que permita monitorear todos los circuitos del enlace de forma centralizada. La red de datos deberá estar basada en la implementación de enlaces permanentes y anchos de banda solicitados.

e) Para la comunicación de la red MPLS se deberá utilizar una topología estrella con el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), los cuales deberán tener comunicación directa con cada uno de los locales de las Sedes Remotas. Los segmentos de red de datos y voz de estos locales (Sedes Remotas) no podrán comunicarse entre sí y solo lo harán con el Nodo Origen.

La red del contratista deberá contar con un backbone redundante, es decir que llegue a dos (2) nodos diferentes, hecho íntegramente en fibra óptica. La CGR podrá

solicitar al contratista la evidencia que sustente lo solicitado, puede incluir una visita a los nodos de conexión.

f) El contratista deberá proveer los equipos de tecnología vigente (los equipos solicitados deben de tener como máximo dos (2) años de fabricación, contabilizados desde la convocatoria del servicio) y de última generación. La CGR podrá solicitar la redistribución de los anchos de banda de la red MPLS por cada Sede Remota (la redistribución máxima será hasta 100 Mbps en cada Sede Remota) y el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), siempre y cuando no se sobrepase el ancho de banda contratado, dicha actividad será sin costo alguno para la entidad y será solicitada con un plazo de antelación de 72 horas al contratista para su ejecución (la redistribución será ejecutada previo que el contratista valide las facilidades técnicas).

g) Todos los equipos que sean utilizados en la infraestructura de comunicaciones deberán ser de tecnología vigente (deben de tener como máximo dos (2) años de fabricación, contabilizados desde la convocatoria del servicio) y que no entren en obsolescencia mientras se encuentre en ejecución del servicio, contando con el respaldo de la marca, en la cual el contratista debe presentar una carta del fabricante donde indique el equipamiento no está en EOS (Fin de Venta o End Of Sale) y EOL (Fin de Vida o End Of Live) y que cuenta con soporte vigente del fabricante (durante el plazo de ejecución contractual), dicha carta será presentada conjuntamente con el Plan de trabajo (numeral 1.6, literal a). Además, estos deberán estar debidamente señalizados y acondicionados con la finalidad de evitar la manipulación por personal no autorizado.

h) La trasmisión de los datos y la voz debe realizarse sobre un canal seguro de extremo a extremo (desde cada Sede Remota hacia el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), considerando que se debe utilizar el esquema de encriptación AES (Advanced Encryption Standard) con tamaño de clave de 256 bits o superior, todos los componentes de encriptación deben ser redundantes. El contratista es responsable de contar con las licencias y equipos requeridos para asegurar el cifrado del canal, para lo cual, el contratista debe proveer equipos de seguridad en cada uno del Nodo Origen (Sede Central y Sede Escuela Nacional de Control) y en las Sedes Remotas (Tabla N° 01), tal como se indica en el punto 1.1.2.2.

i) El tráfico de red generado dentro de los canales seguros debe ser registrados dentro de una base de datos de recolección de log, donde se pueda generar reportes de auditoría de manera programada y ejecutado a demanda por la CGR, este registro debe ser almacenado por equipamiento provisto por el contratista dentro de la Sede Central, se debe incluir como mínimo los siguientes reportes:
   i) Registro IP origen, destino, puerto de destino (protocolo de capa 4 y 7 de acuerdo al modelo OSI).
   ii) Registro de acceso de los equipos provistos por el contratista y las acciones realizadas durante el inicio de sesión.
   iii) Registro de caída de los enlaces contratados y la degradación de servicio o conmutación al enlace

j) Cada Sede Remota debe contar con dos enlaces y deben operar en modo activo-activo, de tal manera que se use ambos enlaces de manera simultánea y/o ante la ocupación del uso de toda la capacidad del enlace principal se continúe la ocupación del segundo enlace.

k) Para todas las Sedes Remotas, las cuales deben contar con doble enlace, cada enlace debe provenir de un nodo distinto del otro enlace instalado en la sede, para esto se requiere que la infraestructura del contratista tenga una topología anillo mediante rutas independientes (en todo su recorrido), de modo que pueda proveer el respaldo permanente ante una posible avería en la ruta de la interconexión; para lo cual, el contratista deberá adjuntar el esquema topológico (diagramas) de la redundancia de los enlaces, el cual debe será presentado para el perfeccionamiento del contrato.

l) El contratista debe realizar la configuración del equipamiento y de los enlaces instalado en el Nodo Origen (Sede Central y Sede Escuela Nacional de Control), de tal manera que, ante una falla de uno de los enlaces, conmute de manera automática e inmediata hacia el otro enlace. La conmutación por la falla y su

restablecimiento posterior a esta, debe ejecutarse sin reducir ninguna característica solicitada (seguridad y conectividad a las Sedes Remotas).

m) El contratista debe garantizar la continuidad del servicio ante la falla de uno de los enlaces contratados (Principal y Secundario) para cada una de las Sedes Remotas, la conmutación entre enlace Principal y enlace de Secundario debe ser automática ante la pérdida de conectividad y cuando se genere una degradación del servicio de alguno de los enlaces instalados, la conmutación por la falla y su restablecimiento posterior a esta, debe ejecutarse sin reducir ninguna característica solicitada (seguridad o conectividad al Nodo Origen).

n) La solución brindada por el contratista debe soportar la característica de Corrección de Errores hacia Adelante (FEC – Forward Error Correction) que implemente duplicación de paquetes para corrección de errores, para así lograr alta confiabilidad en la transmisión y recepción de datos.

o) De encontrarse alguna vulnerabilidad de seguridad en la configuración de los equipos para el presente servicio, esta debe ser corregida por el contratista.

p) Los equipos de la solución deben contener la versión del sistema operativo y/o firmware estable más recientes disponible por el fabricante al inicio del presente servicio de acuerdo a los modelos de los equipos que proporcionará el contratista. En caso se detecte o se publique alguna vulnerabilidad de seguridad en los sistemas operativos y/o firmwares usados, el contratista, a solicitud de la CGR, deberá eliminar dichas vulnerabilidades, lo cual puede implicar la actualización del mismo sistema operativo y/o firmware

q) El contratista será responsable de la restauración de las configuraciones y de los sistemas operativos de los equipos propuesto en caso estos sufran averías, para lo cual deberá mantener las respectivas copias de respaldo.

r) Los equipos de enrutamiento provistos por el contratista deben incluir las siguientes características como mínimo:
   i) Soporte de NetFlow o Sflow o similares.
   ii) Soporte de NBAR o funcionalidad similar para el descubrimiento, clasificación e identificación de protocolos.
   iii) Los router a dotar deben incluir las interfaces necesarias para la integración con la red de la CGR.
   iv) Será de responsabilidad del contratista dimensionar la cantidad de puertos WAN y LAN que requieran para la prestación de sus servicios.
   v) Así mismo el contratista asumirá la total responsabilidad de la instalación, soporte, configuración, garantía y mantenimiento de los routers a instalarse en las sedes de la institución.
   vi) Soporte de Syslog y SNMPv2 en adelante.
   vii) Para el caso del Nodo Origen (Sede Central y Sede Escuela Nacional de Control), deben incluir (en cada sede) mínimo dos interfaces operativos para la integración con la red CGR.

s) Los equipos de telecomunicaciones (equipamiento de enrutamiento, equipamiento de encriptación, entre otros) provistos por el contratista como parte del servicio, para el Nodo Origen (Sede Central y Sede Escuela Nacional de Control) y Sedes Remotas deben tener las interfaces necesarias para interconexión con la red de voz y datos de la CGR.

   Será de responsabilidad del contratista dimensionar la cantidad de puertos WAN y LAN en los equipos de enrutamiento del Nodo Origen (Sede Central y Sede Escuela Nacional de Control) que requieran para la prestación de sus servicios.

t) Se dará conformidad a la validación de los enlaces luego de cumplir como mínimo las siguientes acciones:
   i) Instalación y configuración de los equipos de telecomunicaciones.
   ii) Pruebas de Validación, tendrán como objetivo validar la correcta instalación, configuración y funcionamiento de cada enlace según el Protocolo de Pruebas presentado en el “Plan de Trabajo” y evaluado por la CGR; al término de las

pruebas de validación se firmará un “Acta de validación” por cada enlace instalado.

iii) Sincronizar los equipos de telecomunicaciones que forman parte de la Red con el Servidor NTP (Network Time Protocol) que CGR tiene instalado.

u) El contratista deberá presentar un cuadro con los costos desagregados del servicio brindado a cada una de las sedes de la red MPLS.

NODO ORIGEN (SEDE CENTRAL Y SEDE ESCUELA NACIONAL DE CONTROL)

Ancho de Banda Sede Central: El enlace de la Sede Central configurado en activo, con ancho de Banda igual a la Sumatoria del ancho de banda de todos los enlaces PRINCIPALES de las SEDES REMOTAS que se encuentran ACTIVAS u OPERATIVAS Mbps.

Ancho de Banda Sede ENC: El enlace de la Sede ENC configurado en activo, con ancho de Banda igual a la Sumatoria del ancho de banda de todos los enlaces SECUNDARIOS de las SEDES REMOTAS que se encuentran ACTIVAS u OPERATIVAS Mbps

Medio de Trasmisión: Fibra Óptica

Los enlaces de la Sede Central configurados en activo, Sede ENC en modo activo, los cuales deben ser atendidos de diferentes nodos de acceso.

Tipo de enlace: Simétrico y overbooking 1:1

Tipo de Red: IP (Soporte tráfico de voz, datos, video, video-conferencia, video-vigilancia, aplicaciones, etc.)

SEDES REMOTAS

Ancho de Banda: Ver detalle de la Tabla N° 01.

Medio de Trasmisión: Fibra Óptica para todas las sedes a nivel nacional.

Los enlaces de la Tabla N° 1 deben ser configurados en activo-activo, deben ser atendidos de diferentes nodos de acceso.

Tipo de enlace: Simétrico y overbooking 1:1

Tipo de Red: IP (Soporte tráfico de voz, datos, video, video-conferencia, video-vigilancia aplicaciones, etc.)

Nota a considerar:

Los equipos de comunicaciones suministrados por el contratista deben ser compatibles con las interfaces Ethernet de la red LAN proporcionados por la CGR, el cual debe soportar tráfico en modo acceso (sin etiquetar) y etiquetados (VLAN).

1.1.3. EQUIPOS DE ENRUTAMIENTO DE INTERNET Y RED MPLS Y UPS

a) Los equipos proporcionados por el contratista deberán ser de tecnología vigente en todas las sedes a fin de poder brindar la mayor disponibilidad posible (los equipos solicitados deben de tener como máximo dos (2) años de fabricación, contabilizados desde la convocatoria del servicio), tanto para el caso del servicio de Internet de la sede central y para la red MPLS.

b) El contratista deberá proveer el equipamiento necesario para la administración y gestión centralizada de los equipos propuestos. El contratista deberá realizar la administración de los equipos de enrutamiento, demarcadores (solo si los hubiera), UPS las 24 horas por los 7 días durante el plazo de ejecución del servicio, además el contratista deberá proveer el equipamiento necesario para la administración y gestión centralizada de los equipos propuestos. Se brindará al personal encargado por la CGR el perfil de acceso de solo lectura para ejecución de comandos de monitoreo. Asimismo, deberá habilitar en la CGR consolas de monitoreo de todos los equipos de enrutamiento, UPS y enlaces solicitados.

c) En caso de daño de uno de los equipos en cada sede (incluido los equipos UPS de las Sede Remotas), el contratista deberá reemplazar el (los) equipo(s) en un plazo máximo de veinte cuatro (24) horas para los equipos de la Sede Central, Sede ENC y cuarenta y ocho (48) horas para las Sedes Remotas. Los equipos de enrutamiento deben garantizar la calidad y disponibilidad del servicio de Internet y el servicio de red privada sobre una red MPLS, solicitada por la CGR.

d) El contratista deberá presentar un cuadro con los costos desagregados del equipamiento UPS brindado a cada una de las sedes de la red MPLS.

1.1.4. EQUIPAMIENTO DE SEGURIDAD PERIMETRAL

El Contratista deberá proporcionar el siguiente equipamiento a fin de mantener la seguridad perimetral de la red CGR:

a) Los bienes que conformen el Equipamiento de Solución Tecnológica, deben estar en perfectas condiciones para su uso y deben ser nuevos (los equipos solicitados deben de tener como máximo dos (2) años de fabricación, contabilizados desde la convocatoria del servicio) y que no entren en obsolescencia mientras se encuentre en ejecución del servicio, en donde los rótulos permitan identificar las características, la marca respectiva y si fuera el caso, deberá estar impreso en el mismo bien.
b) No se aceptarán equipos reciclados, reensamblados o reacondicionados, tampoco se aceptarán aquellos que tengan la denominación “refurbished”, “remarketing” o su equivalente comercial.
c) Los bienes, deben estar vigentes en el mercado y posicionarse dentro de la familia de equipos de última generación en tecnología publicadas por el fabricante, adjuntar carta del fabricante o representante local autorizado, que respalde lo solicitado. Asimismo, no deberán estar descontinuados (end-of-life).
d) El Contratista debe considerar todo lo necesario para el correcto funcionamiento de la solución propuesta (accesorios y licencias).
e) Las características que corresponden a las especificaciones técnicas de los equipos de seguridad perimetral se describen de la siguiente manera:
    i. Para las cabeceras principales (Sede Central y Sede ENC) se encuentran en el Anexo N°01.
    ii. Para Sedes Remotas (Tabla-01, del numeral 1 al 31) se encuentran en el Anexo N°02.
    iii. Para Sede Remota (Tabla-01, del numeral 32), Sede-Ancón, se encuentran en el Anexo N°03.
    iv. Para Sedes Remotas (Tabla-01, del numeral 33 al 36), Arequipa-N°1593, Sede-01, Sede-02 y Sede-03, se encuentran en el Anexo N°04.
f) Como parte de la implementación del equipamiento solicitado (Anexo N° 01) se debe establecer tres (03) particiones lógicas del equipamiento con la finalidad de establecer zonas de seguridad independientes, asimismo se debe integrar a una topología interna donde se definirá contextos o VRFs o tenants, donde se involucrará enrutamiento dinámico haciendo uso de OSPF y BGP.
g) El soporte y licenciamiento del equipamiento será por parte del contratista por el plazo que dure el servicio contratado.
h) El contratista deberá presentar un cuadro con los costos desagregados del equipamiento de seguridad perimetral brindado a cada una de las sedes (La red MPLS e Internet).

1.1.5. SOLUCIÓN PARA LA PROTECCIÓN DE APLICACIONES Y SERVICIOS

1.1.5.1. SOLUCIÓN DE ESCANEO DE VULNERABILIDADES PARA INFRAESTRUCTURA TECNOLÓGICA

La solución deberá cumplir las siguientes funcionalidades mínimos:

a) Debe estar licenciado para un mínimo de 5 usuarios para realizar sin límite de escaneos.
b) Debe permitir identificar y gestionar efectivamente las vulnerabilidades de los activos tecnológicos.
c) Debe contar con funcionalidades activas para el escaneo de 500 activos de TI, entre ellos estaciones de trabajo, servidores, dispositivos de red, plataformas de virtualización y otros sistemas conectados.

d) Debe contar con un sistema de gestión centralizada on-premise y múltiples escáneres distribuidos sin límites en cantidad de instancias. La consola de gestión propuesta podrá tener algunas funcionalidades en Cloud, siempre y cuando cumplan con los requerimientos técnicos solicitados, además los componentes de tipo cloud deberán ser propios del mismo fabricante de la solución y deberán contar con certificación de seguridad y privacidad de datos.
e) Debe admitir montar múltiples organizaciones lógicas de forma de gestionar la plataforma en modalidad multi-tenancy y que los datos de cada tenant no se vean comprometidos por usuarios que no corresponda.
f) Debe contar con un catálogo de vulnerabilidades que incluyan más de 140 mil evaluaciones diferentes y al menos 57 mil vulnerabilidades conocidas por un período no menor a 15 años.
g) Debe proveer un mecanismo de priorización de vulnerabilidades automático basado en la probabilidad de explotación y que ofrezca información alternativa al CVSS (Common Vulnerability Scoring System) basada en Inteligencia de amenazas reales recabada de diversas fuentes como Deep Web, Dark Web, redes sociales, sitios de divulgación y otros centros de investigación.
h) Debe ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA STIG, PCI y otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Bases de Datos, Aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Esta funcionalidad es también conocida como Policy Compliance. Se requiere esta capacidad sin límites de licenciamiento.
i) Debe contar con la posibilidad de definir objetivos para ser cumplidos por los diferentes usuarios de la solución a fin de asegurar y medir la efectividad de las prácticas de gestión mediante un tablero de cumplimiento. Dichos objetivos pueden estar alineados con normativas como CIS, ISO o personalizada y utilizar métricas de evaluación. Ejemplo, el 90% de los sistemas deben haber sido escaneados en los últimos 30 días, el 100% de los sistemas deben estar libres de vulnerabilidades de Alta criticidad con antigüedad mayor a 120 días, etc.
j) Debe entregar indicadores de madurez de la práctica de gestión de vulnerabilidades, evaluando la frecuencia, profundidad y cobertura de los escaneos.
k) Debe crear automáticamente planes de remediación con actividades recomendadas concretas y estimaciones sobre cuál será el impacto en la reducción de riesgo previo a su ejecución. Esta capacidad deberá ser global y permitirá aplicar filtros por grupo de activos específico.
l) Debe calcular indicadores numéricos que nos permitan entender el nivel de ciberexposición actual basado en el riesgo, producto de las vulnerabilidades encontradas y la criticidad de los activos.
m) Todos los elementos que conforman la solución deberán ser actualizables automáticamente con intervención opcional de un administrador, incluyendo nuevas versiones de software/firmware, updates de contenido (nuevas vulnerabilidades) y feeds de inteligencia.
n) La solución debe tener una gestión de usuarios como mínimo con las siguientes características:
    i) Debe estar basada en roles y permisos que limiten el acceso a conjuntos de datos puntuales, grupos de activos y a acciones concretas tales como reporting, análisis, escaneo, aceptar riesgos o reclasificarlos, etc.
    ii) Debe integrarse con sistemas LDAP.
    iii) Debe permitir autenticación SAML para integración con soluciones de Single Sign-On tales como Okta, OneLogin o Microsoft ADFS.
o) Tanto la consola como los escáneres deben ser desplegables en modalidad software y appliance virtual en VMware y Hyper-V.
p) Debe permitir la configuración y almacenamiento seguro de credenciales de usuario para escanear mediante cuentas locales y de dominio Windows, cuentas ssh para sistemas Unix/Linux y dispositivos de red. Deberá permitir elevar privilegios mediante “su” y “sudo” y no deberá tener limitaciones en cantidad de

credenciales. Además, el sistema deberá integrarse con soluciones de bóvedas digitales como Cyberark, Centrify, Beyondtrust y otras.

q) La solución debe ser capaz de generar un inventario de activos, poblándolo mediante escaneos de descubrimiento sin límites de licenciamiento. Deberá también permitir agregar activos importándolas de fuentes externas. Deberá auto-clasificar los activos por diversos criterios tales como localización, red en la que se encuentra, tipo de dispositivo, propietario o responsable del dispositivo, criticidad para el negocio, se ha sido escaneado o no, si se cuentan con credenciales funcionales o no, si está comprometido por malware y otros criterios de agrupamiento, se podrá cubrir esta funcionalidad con una herramienta tecnológica complementaria.
r) La solución debe agrupar activos que posean una base de datos, que posean aplicaciones web, que no resuelvan nombre, que contengan vulnerabilidades explotables y otras agrupaciones dinámicas.
s) Debe ser capaz de obtener vulnerabilidades de estaciones de trabajo en Internet (teletrabajo) y otros ambientes no conectados a la red de la entidad, mediante agente Windows, Linux y MacOS. Los agentes deberán reportar dichas vulnerabilidades a un servicio en Internet que luego pueda ser consultado por la consola on-premise.
t) Debe contar con escaneos que solo auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas).
u) Debe mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición.
v) Debe ser capaz de identificar sistemas comprometidos por malware y otros códigos maliciosos. También deberá ser capaz de identificar la ejecución y nivel de firmas del sistema de Antimalware presente en el dispositivo.
w) Debe reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de que forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.
x) Debe contar con capacidades de reporting y dashboards completamente personalizables mediante gráficos, texto, filtros, querys y lógicas complejas. Además, deberá contar con más de 300 templates listos para ser usados y editables. No deberá estar limitado por licenciamiento y si lo estuviese, considerar el módulo de reporting más completo incluyendo plantillas de cumplimiento CIS, ISO27001, y PCI.
y) Debe ser capaz de integrarse a un Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas independientes y nativas en el producto como así también integrarse a una solución de SIEM y de Orquestación (SOAR). Se espera que la solución alerte cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables.
z) Debe contar con un sistema de ticketing nativo para seguimiento de vulnerabilidades y también integrarse con sistemas de ticketing externos tales como Atlassian o Servicenow.
aa) Debe realizar un escaneo de vulnerabilidades
bb) Debe realizar un escaneo de puertos, servicios y aplicaciones.
cc) Debe realizar tareas programadas de escaneo de vulnerabilidades en redes y aplicaciones.
dd) Debe realizar auditoria de configuración para el cumplimiento de políticas y estándares.
ee) Debe realizar escaneo de múltiples redes IPv4, IPv6 y redes híbridas.
ff) Debe realizar identificación de datos sensibles en objetivos a escanear.
gg) Debe realizar descubrimiento de activos en la red incluyendo cortafuegos de nueva generación, sistemas operativos, bases de datos, aplicaciones web, ambientes virtuales y servicios en la nube.
hh) Debe realizar escaneo con credenciales y sin credenciales.

ii) Debe realizar el escaneo selectivo.
jj) Debe realizar análisis automático de escaneo.
kk) Debe realizar la priorización de acciones de remediación y recomendaciones para su corrección.
ll) Debe categorizar la vulnerabilidad encontrada por nivel de criticidad.
mm) Debe realizar un escaneo basado en agentes.
nn) Debe permitir gestionar y compartir recursos de escaneo desde una consola central.
oo) Debe contar con actualizaciones de contenido como vulnerabilidades, amenazas avanzadas, día cero, y nuevos tipos de configuraciones de cumplimiento regulatorio.
pp) Debe realizar la gestión de usuarios y grupos.
qq) Debe integrarse a otras soluciones de gestión de parches.
rr) Debe realizar informes flexibles y personalizados para la clasificar por vulnerabilidad o servidor, creación de resumen ejecutivo o comparación de resultados.
ss) Debe generar informes en formato XML, PDF, CSV y HTML.
tt) Debe contar con tableros de control.

1.1.5.2. SOLUCIÓN PARA EL ANÁLISIS DE SEGURIDAD DE LAS APLICACIONES WEB.

La solución deberá cumplir las siguientes funcionalidades mínimos:

a) Debe estar licenciado para un mínimo de 5 usuarios para realizar sin límite de análisis dinámicos.
b) Debe contar con un modelo de licencias perpetuas perpetuas o licencias por suscripción por el tiempo del servicio en sitio de soluciones de Análisis Dinámico (DAST - Dynamic Application Security Testing) y estático (SAST - Static Application Security Testing)
c) Debe incluir sin costo adicional en sus licencias perpetuas o licencias por suscripción por el tiempo del servicio de Análisis Dinámico el soporte al Análisis Híbrido o Interactivo (IAST - Interactive Application Security Testing) en aplicaciones basadas en los lenguajes de programación Java y .NET
d) Debe contar con un modelo de servicios paquetizados por evento o por suscripción de ejecución de pruebas de Análisis Dinámico (DAST - Dynamic Application Security Testing).
e) Debe incluir en los servicios de ejecución de pruebas de Análisis Dinámico la posibilidad de realizar Análisis Híbrido o Interactivo (IAST - Interactive Application Security Testing) en aplicaciones basadas en los lenguajes de programación Java y .NET
f) Debe brindar un modelo de servicios paquetizados por evento o por suscripción de ejecución de pruebas de seguridad en aplicaciones móviles en las plataformas iOS, Android.
g) Debe tener la capacidad de integrar en un sistema central de gestión de vulnerabilidades los resultados y hallazgos asociados a las pruebas estáticas (SAST), dinámicas (DAST), interactivas (IAST) o equivalente.
h) La solución propuesta opcionalmente soporta y detalla cómo es la integración de sus soluciones de pruebas dinámicas (DAST) con soluciones WAF e IPS, ya sea con licencias en sitio o como servicios. Los resultados generados por este componente deben ofrecer la posibilidad de integrarse con las soluciones de seguridad como mínimo F5 con el fin de importar los hallazgos y convertirlos en forma de vacunas digitales, parches virtuales o reglas de protección
i) La solución basa su portafolio de soluciones en los modelos y enfoques de seguridad aplicativa OpenSAMM, BSIMM o equivalente.
j) Debe contar con la capacidad de analizar incrementalmente aplicaciones web, web services, sitios web para dispositivos móviles y servicios web del backend de aplicaciones móviles.
k) Debe contar con la capacidad de descubrimiento crawling basada en los siguientes métodos: Automatic Crawl-and-Audit, Automatic Crawl-Only, Automatic Audit Only,

Workflow-Driven Scan (macro), List-Driven Scan (TXT or XML input), Restrict-ToFolder o equivalente.

l) Debe tener la posibilidad de analizar aplicaciones de forma calendarizada y en batch, así como de hacer descubrimiento de aplicaciones web y servicios web en diferentes segmentos de la red interna del cliente.

m) Debe contar sin costo ni licencias adicionales (licencias perpetuas o licencias por suscripción por el tiempo del servicio) la posibilidad de ejecutar pruebas bajo el modelo de "Interactive Application Security Testing (IAST)", con el fin de identificar el comportamiento interno y la causa raíz del problema de las aplicaciones que se estén probando. Esta funcionalidad deberá ser propia del fabricante y no de una alianza con terceros.

n) Debe contar con API de control y uso remoto basada en servicios RESTful, con el fin de configurar nuevos análisis, recuperar información sobre el estado de los análisis y exportar los resultados de los análisis de forma automatizada.

o) Debe tener la capacidad de que las descripciones de los hallazgos y sus recomendaciones de resolución se presenten en idioma español.

p) Tener la capacidad de que los resultados deban ser categorizados utilizando la taxonomía Seven Pernicious Kingdoms (7PK), Common Weakness Enumeration (CWE) o equivalente.

q) Debe contar con la capacidad de importar análisis asociados con las herramientas Unified Functional Testing (UFT) o equivalente, con el fin de tener una amplia cobertura en las pruebas realizadas.

r) Debe soportar los siguientes tipos de autenticación: Network Authentication, Automatic, Basic, Digest, Kerberos, NTLM, Simple, Credentials entered as default Form Entries, Manually inserted cookie/session token, Forms Authentication, Login Macro, Standard reply, Paramaterized inputs, ChallengeResponse Questions (Q&A), Certificates, Client-side Certificates, PKI / Token, WSSecurity (for SOAP web services), Two-Factor, Interactive Scan (CAPTCHA, RSA ID, Virtual keyboard).

s) La solución debe mantener como mínimo los escaneos de vulnerabilidades realizados durante el periodo del servicio.

t) Debe incluir al menos 20 diferentes políticas de escaneo predefinidas, y permitir la modificación de dichas políticas, además de la generación de políticas de escaneo personalizadas.

u) Debe brindar una interfaz gráfica para la modificación manual de la criticidad o categorización de las vulnerabilidades.

v) Debe brindar la funcionalidad para la generación de reportes de diversos tipos (al menos 15 diferentes tipos), así como un editor de reportes (sin costo adicional) con los cuales sea posible modificar los existentes, extenderlos o crear reportes nuevos

w) Debe contar con al menos 40 plantillas de reportes

x) Debe soportar al menos las siguientes clasificaciones de riesgo:
   i) Crítico: Problemas de alto impacto al negocio y con alta probabilidad de ser atacados o ejecutados.
   ii) Alto: Problemas de alto impacto al negocio y con baja probabilidad de ser atacados o ejecutados.
   iii) Medio: Problemas de bajo impacto al negocio y con alta probabilidad de ser atacados o ejecutados.
   iv) Bajo: Problemas de bajo impacto al negocio y con baja probabilidad de ser atacados o ejecutados

y) Debe soportar al menos las siguientes tecnologías: JavaScript, AJAX, WSDL, SOAP, XML, JSON, Flash, HTML5, Web 2.0, SilverLight y WADL.

z) Debe contar con mecanismos automáticos de actualización tanto en su base de conocimiento, políticas y reglas, así como también en información relevante para el usuario, como nuevas versiones del producto.

aa) En los reportes que ofrece por defecto, en caso de no detectar vulnerabilidades, deberá mostrarse un listado detallado de los componentes analizados y no debe generar reportes en blanco o sin contenido.

1.1.6. TRASLADO DE SEDES

El contratista deberá realizar hasta un máximo de diez (10) traslados físicos de la red privada sobre una red MPLS o servicio de Internet (durante el plazo de ejecución contractual) a solicitud y sin generar costo adicional para la CGR. El medio y la tecnología de acceso en el lado destino serán del mismo tipo que el enlace a trasladar, debiendo incluirse el traslado del enlace y equipos de comunicación. La CGR comunicará al contratista sobre la necesidad mediante una carta formal.

El contratista deberá realizar el traslado del servicio de la sede como máximo en el plazo de sesenta (60) días calendario, contabilizado desde la recepción por parte del contratista de la "carta formal de traslado" enviada por parte de la CGR al contratista.
El contratista deberá brindar un servicio de Internet temporal en el nuevo local (local trasladado) en un plazo no mayor a quince (15) días calendario, contabilizado desde el día de la recepción de la "carta formal de traslado" enviada por la CGR al contratista, mediante un medio de transmisión de radio enlace, banda ancha o Internet 4G o superior, de mínimo de 60 Mbps con el 40% de ancho de banda garantizado (considerando una conectividad segura, hasta que se concluya el traslado físico del enlace con las características solicitadas), este servicio temporal no involucrará ningún costo adicional a la CGR.

1.1.7. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS INVOLUCRADOS EN EL SERVICIO.

a) El contratista debe encargarse de la instalación, configuración y puesta en funcionamiento de los equipos involucrados en el servicio de la solución, y debe brindar a la CGR acceso administrativo sobre los equipos de los numerales 1.1.3, 1.1.4 y 1.1.5.
b) El contratista debe encargarse de la instalación, configuración y puesta en funcionamiento de los equipos UPS (numeral 1.1.3.) considerando los accesorios necesarios para su funcionamiento.
c) Para el caso de los equipos router (numeral 1.1.3.) estos serán instalados, configurados y administrados por el contratista y la CGR podrá solicitar cambios en ancho de banda a demanda y tendrá el acceso de lectura a los mismos y será solicitado con siete (07) días calendario de anticipación.
d) El contratista deberá realizar la configuración de los equipos involucrados en el servicio de la solución, para enviar los registros de eventos a un correlacionador o SIEM que la CGR disponga, previa coordinación entre ambas partes.

1.2. PRESTACIONES ACCESORIA

1.2.1. SOPORTE TÉCNICO

a) Disponibilidad de soporte técnico las 24 horas por los 7 días durante el plazo de ejecución del servicio, relacionado con problemas de enlaces de conexión, fallos y reposición de equipos que son parte del servicio, en caso amerite, así como respuesta a consultas de carácter técnico relacionados con la disponibilidad de los enlaces, servicios de red y el equipamiento de los numerales 1.1.3, 1.1.4 y 1.1.5.
b) Disponibilidad de soporte técnico las 24 horas por los 7 días durante el plazo de ejecución del servicio, relacionado con problemas de enlaces de conexión, fallos y reposición de equipos UPS.
c) El contratista debe asignar un supervisor general del servicio para realizar las coordinaciones de los requerimientos técnicos, soporte técnico y/o averías de los servicios, siendo el primer medio de contacto con la CGR.
d) El contratista deberá brindar un ingeniero residente dedicado, para el soporte de las atenciones requeridas por la CGR en el horario (8:00 a.m. – 6:00 p.m.) y de lunes a viernes, fuera de este horario la atención será a través de la central de atención al cliente del contratista.
e) La CGR podrá enviar requerimientos de soporte gestionado para cambios en la configuración (nuevas políticas, nuevas reglas, entre otras.) en estos equipos; además, el contratista realizará el monitoreo del funcionamiento de los equipos y comunicará a la CGR mediante correo electrónico. Ante una avería por manipulación del equipamiento por parte del personal de la Entidad esta no será motivo de penalidad al contratista.
f) El contratista proporcionará el servicio de soporte técnico y monitoreo remoto de los equipos involucrados en el servicio, las 24 horas por los 7 días durante el plazo de

ejecución del servicio, por medio de un SOC y NOC propio o tercerizado para garantizar el correcto funcionamiento de los mismos.

g) La CGR puede solicitar al contratista la creación o cambios en las reglas, configuraciones, y habilitaciones en los equipos que forman parte del servicio los cuales serán atendidos sin costo adicional y en un plazo máximo de dos (2) horas (solo para el caso de los equipos de Seguridad Perimetral el plazo máximo será de cuatro (4) horas) de solicitado el requerimiento, que será vía correo electrónico o llamada telefónica.

h) El contratista es el responsable de la actualización oportuna de parches, firmware del equipo y deben hacer copias de respaldo de la configuración y políticas de los equipos instalados.

1.2.2. GESTIÓN DEL SERVICIO

1.2.2.1. ATENCIÓN DE AVERÍAS

a) Se entenderá como avería a una interrupción total del servicio, así como un decremento en la calidad del mismo.

b) Toda actividad o provisión de bienes (equipos parte del servicio) será sin costo alguno para la Entidad, debe garantizar el correcto funcionamiento de todos los equipos e infraestructura que utiliza para brindar el servicio en el periodo de tiempo de su ejecución.

c) El contratista deberá contar con un centro de atención de llamadas para reparación o asistencia técnica instalado.

d) Tiempo para la solución de las averías (interrupción total del servicio, así como un decremento en la calidad del servicio) deberá ser de 43.2 minutos como máximo (acumulados en el mes) para la red de datos (MPLS) y/o internet de la comunicación con Sede Central y Sede Escuela Nacional de Control y Sedes Remotas (dentro de Lima Metropolitana), contados desde que la CGR reporte la incidencia vía correo electrónico al ingeniero residente dedicado o al que haga de sus veces por parte del contratista. Al respecto, el contratista deberá indicar la información sobre los puntos de contacto para la gestión adecuada del servicio. La información sobre los puntos de contacto está referida al centro de atención de averías (número telefónico, correo electrónico). Esta información deberá presentarse para el perfeccionamiento del contrato.

e) Tiempo para la solución de las averías (interrupción total del servicio, así como un decremento en la calidad del servicio) deberá ser de 130 minutos como máximo (acumulados en el mes) para la red de datos (MPLS) en la comunicación con cada uno de las Sedes Remotas (fuera de Lima Metropolitana), contados desde que la CGR reporte la incidencia vía correo electrónico al ingeniero residente dedicado o al que haga de sus veces por parte del contratista. Al respecto, el contratista deberá indicar la información sobre los puntos de contacto para la gestión adecuada del servicio. La información sobre los puntos de contacto está referida al centro de atención de averías (número telefónico, correo electrónico). Esta información deberá presentarse para el perfeccionamiento del contrato.

f) El contratista deberá atender los problemas relacionados con la solución del sistema de monitoreo en el tiempo máximo de 24 horas, este tiempo será contado desde que la CGR solicita el requerimiento vía correo electrónico al ingeniero residente dedicado o al que haga de sus veces por parte del contratista.

g) El cierre del requerimiento, debe realizarse de manera coordinada entre personal del contratista y la CGR que designe para tal efecto. El requerimiento generado, sólo podrá ser cerrado cuando sea corroborada la solución y aceptada con el visto bueno por parte de la CGR.

h) Toda actividad o provisión de bienes que tenga que ejecutar el proveedor del servicio para subsanar una interrupción del servicio será sin costo alguno para la CGR.

i) La CGR podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde la 00:00 hasta las 23:59 horas.

j) Las llamadas de servicio se sujetarán a lo siguiente: Se podrá efectuar telefónicamente y por correo electrónico (considerándose todas estas formas igualmente válidas) a las direcciones acordadas entre la CGR y el contratista. La CGR notificará las anomalías que se presenten incluyendo la siguiente información: fecha y hora, descripción del problema, contacto en la CGR.

k) El contratista deberá entregar a la CGR con veinticuatro (24) horas de anticipación o a quién éste indique, una nómina del personal técnico autorizado a realizar labores de mantenimiento con sus respectivos SCTR y Certificado de Aptitud Medico Ocupacional en los locales de la CGR. Dicha nómina deberá ser actualizada cuando se produzcan cambios.

l) En caso de la inoperatividad de los equipos UPS, el contratista deberá solucionar a través de una asistencia remota o presencial en un plazo de 30 minutos (a fin de cumplir con esta necesidad el contratista debe brindar como mínimo más de un equipo UPS), en caso requiera reemplazo, este deberá ser en un plazo máximo de cuarenta y ocho (48) horas.

1.2.2.2. CAPACITACIÓN

i) El contratista deberá brindar capacitación del curso oficial del fabricante, por parte del personal certificado de la marca, en la administración y configuración de las soluciones ofertadas en los numerales 1.1.4 y 1.1.5 para seis (6) personas, en dos grupos de tres personas, designadas por la CGR con una duración mínima de cuarenta y ocho (48) horas, esta capacitación se realizará como máximo a los noventa (90) días calendario, contados a partir del día siguiente de culminado la instalación del servicio, los materiales necesarios para la capacitación deberán ser proporcionados por el contratista. Serán admitidos 2 niveles de cursos oficiales para completar el mínimo de horas requerido por la entidad. Los cursos oficiales se dictarán en idioma español, los materiales podrán estar en idioma inglés.

ii) Se precisa que las capacitaciones se realizarán en un lugar designado por el contratista o en las instalaciones de la CGR (Jr. Camilo Carrillo N° 114 – Jesús María) o a través de un ambiente virtual y con instructor en vivo (on-line), teniendo que hacer uso de alguna de las herramientas tecnológicas más usadas para este fin (lo cual no debe incurrir en ningún costo adicional para la CGR), permitiendo una adecuada interacción entre el expositor y los participantes. Esta capacitación será coordinada previamente entre el contratista y el personal de la Subgerencia de Operaciones y Plataforma Tecnológica de la CGR. Al finalizar la capacitación el contratista deberá entregar un certificado o constancia (el cual deberá ser en formato físico o digital) para cada uno de los participantes el cual deberá incluir, como mínimo, la fecha de inicio y fin de la capacitación, el nombre del instructor, así como la cantidad de horas utilizadas en la capacitación.

iii) La capacitación se brindará de lunes a viernes, el horario será en coordinación con el contratista.

1.3. PERFIL DEL PERSONAL CLAVE

El contratista deberá garantizar el siguiente personal mínimo para la implementación y soporte durante todo el servicio. El contratista debe proveer como mínimo al siguiente personal clave:

a) Un (1) Responsable o Jefe de Proyecto con experiencia profesional demostrada mínima de tres (3) años en la supervisión o conducción o dirección técnica de prestación o ejecución de servicios o gestión o implementación o trabajos de: Telecomunicaciones y/o tecnologías de la información. Debiendo ser profesional titulado, colegiado y habilitado (la colegiatura y la habilitación del profesional se requerirá para el inicio de su participación efectiva en el contrato) en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial, responsable de las coordinaciones de las actividades a realizar para la implementación del servicio y las coordinaciones con el personal designado por la CGR, para el mejor desarrollo de los mismos; para lo cual deberá contar con un equipo móvil en forma permanente y operativo para la recepción de llamadas telefónicas y mensajes.

b) Un (1) Supervisor General del Servicio con experiencia profesional demostrada mínima de tres (3) años en la supervisión o conducción o dirección técnica de prestación o ejecución de servicios o trabajos de: instalación o mantenimiento de enlaces de transmisión de datos. Debiendo ser profesional titulado, colegiado y habilitado (la colegiatura y la habilitación del profesional se requerirá para el inicio de su participación efectiva en el contrato) en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial, responsable de las actividades a realizar durante la gestión del servicio (1095 días desde el inicio del servicio) para la atención de incidentes, averías, soporte técnico y requerimientos según

coordinación con el personal designado por la CGR, efectuará las coordinaciones necesarias entre la CGR y el contratista, para el mejor desarrollo de los mismos; quien deberá contar con un equipo móvil en forma permanente y operativo con recepción de llamadas telefónicas y mensajes.

c) Un (1) Ingeniero Residente Dedicado, con experiencia profesional demostrada mínima de tres (3) años en la implementación del servicio de Internet y/o redes de datos y/o instalación y/o configuración y/o soporte técnico y/o solución de problemas de los equipos involucrados en el presente servicio. Debiendo ser profesional titulado, colegiado y habilitado (la colegiatura y la habilitación del profesional se requerirá para el inicio de su participación efectiva en el contrato) en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial, responsable de las actividades a desarrollar en el servicio de Internet, redes de datos, configuración, soporte técnico y solución de problemas(1095 días desde el inicio del servicio) con el personal designado por la CGR, efectuará las coordinaciones y configuraciones necesarias con la CGR para el mejor desarrollo de los mismos; quien deberá contar con un equipo móvil en forma permanente y operativo con recepción de llamadas telefónicas y mensajes.

d) Un (1) Especialista en Routing-Switching, con experiencia mínima de dos (2) años en la ejecución de servicios y/o trabajos y/o actividades de: instalación y/o mantenimiento de enlaces de transmisión de datos, debiendo contar como mínimo el título de técnico en Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Telecomunicaciones, o Redes y/o Comunicaciones, o con el grado bachiller en ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones. Asimismo, deberá contar con certificación vigente de la solución ofertada, siendo necesaria la presentación de dicha información para la suscripción del contrato, en su idioma original. Las actividades a realizar serán como mínimo: cambio de configuración de políticas, reglas, puertos de los equipos routers y switches de la solución.

e) Un (1) Especialista en la solución de seguridad perimetral y Un (1) Especialista en la solución para la protección de aplicaciones y servicios o se aceptarán un (01) Especialista que cumpla en la solución de seguridad perimetral y en la solución para la protección de aplicaciones y servicios, el cual debe tener como mínimo dos (2) años de experiencia en implementación en este tipo de soluciones, debiendo contar como mínimo con el título de técnico en Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Redes y Seguridad Informática, o Administración de Redes y Comunicaciones, o con el grado bachiller en ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Computación y Sistemas, o Electrónica y Telecomunicaciones. Asimismo, deberá contar con certificación vigente de la solución ofertada o de la marca propuesta, siendo necesaria la presentación de dicha información para la suscripción del contrato y en su idioma original. Las actividades a realizar serán como mínimo: cambio en las configuraciones respecto a los permisos, accesos, de los equipos de seguridad perimetral y de la solución para la protección de aplicaciones y servicios, este perfil lo puede cumplir una única persona o se aceptarán dos personas que cumplan cada uno con el perfil académico y con una certificación por solución.

1.4. LUGAR DE PRESTACIÓN DEL SERVICIO

Los lugares donde se instalarán los servicios serán:

Tabla N° 02

Direcciones de los enlaces MPLS por sedes a nivel nacional

N°	Local	Dirección
1	Gerencia Regional de Control Ica	Av. Los Maestros D-12 - Urb. San José - Ica, Ica, Ica
2	Gerencia Regional de Control Ancash – Local-1	Jr. José de Sucre N° 877, 879-A, 879-B, (Zona Comercial Mz C-6, Lote 4), distrito Huaraz, Provincia Huaraz y Departamento de Ancash.
3	Gerencia Regional de Control San Martín	Jr. Callao cdra. 5 S/N (al costado del local INEI y frente al hotel Bethel) Barrio de Calvario, Mz. 3140 lote 21, Sector Pueblo Tradicional Cercado de Moyobamba, distrito y provincia de Moyobamba, departamento de San Martín

N°	Local	Dirección
4	Gerencia Regional de Control Junín - Local 1	Jr. Lima N° 338-346 - Huancayo, Junín, Junín.
5	Gerencia Regional de Control Apurímac	Jr. Junín N° 215 - Abancay, Abancay, Abancay
6	Gerencia Regional de Control Cusco	Avenida Pachacutec N° 609, distrito de Wanchaq, provincia de Cusco
7	Gerencia Regional de Control Huánuco	Jr. Dos de Mayo N° 1759 - 1763 - Huánuco, Huánuco, Huánuco
8	Gerencia Regional de Control Arequipa	Cl. Peral N° 102-104 Cercado - Arequipa, Arequipa, Arequipa
9	Gerencia Regional de Control Tacna	Calle Los Alamos N° 1978 -1979, Urbanización Quinta Aurora, Tacna, Tacna, Tacna
10	Gerencia Regional de Control La Libertad	Jr. Juan Pablo II N° 583 – Trujillo, Trujillo, La Libertad.
11	Gerencia Regional de Control Cajamarca	Mz. C Lote 4 Jr. Cápac Yupanqui S/N Sector Bellavista, Complejo Qhapac Ñan – Cajamarca, Cajamarca, Cajamarca.
12	Gerencia Regional de Control Piura	Esq. Jr., Lima c/ Huánuco s/n - Piura, Piura, Piura
13	Gerencia Regional de Control Lambayeque	Av. Elías Aguirre N° 896 - Chiclayo, Chiclayo, Lambayeque
14	Gerencia Regional de Control Puno	Jr. Deustua 822 - Puno, Puno, Puno
15	Gerencia Regional de Control Loreto	Jr. Tacna 432, distrito de Iquitos, provincia de Maynas, departamento de Loreto.
16	Gerencia Regional de Control Ayacucho	Av. Carmen Alto S/N Sublote 1A-4 distrito Carmen Alto provincia Huamanga, Ayacucho
16	Gerencia Regional de Control Moquegua	Cl. Cusco N° 421 - Moquegua, Mariscal Nieto, Moquegua
18	Gerencia Regional de Control Huancavelica	Jirón Antonio Raymondi N°247 Huancavelica
19	Gerencia Regional de Control Junín - Local 2	Av. Daniel Alcides Carrión N° 1481 - Huancayo, Junín, Junín
20	Gerencia Regional de Control Ucayali	Jr. Atahualpa 945, Mz.24, Lote 06 - Callería, Coronel Portillo, Ucayali
21	Gerencia Regional de Control Tumbes	Av. Fernando Belaunde T. Mz 1 Lote 17 - Urb. Andrés Araujo Morán, Tumbes, Tumbes
22	Órgano Instructor Lambayeque	Cl. Juan Cuglievan N° 470 - Chiclayo, Chiclayo, Lambayeque
23	Órgano Instructor Junín	Av. Arequipa N° 215, 215-A, 217 - El Tambo, Huancayo, Junín
24	Órgano Instructor Arequipa	Av. Cayma N° 304 - Cayma, Arequipa, Arequipa
25	Gerencia Regional de Control Amazonas	Jr. Hermosura N° 720 - Chachapoyas, Chachapoyas, Amazonas
26	Gerencia Regional de Control Madre de Dios	Jr. Manuel Gonzáles Prada N° 241 - Puerto Maldonado, Tambopata, Madre de Dios.
27	Oficina de enlace de la Gerencia Regional de Control Ancash -Local 2	Mz. F2 Lote. 10 Sector 5D, Urbanización. Buenos Aires – Nuevo Chimbote, Santa, Ancash
28	Gerencia Regional de Control de Pasco	Jirón San Martín 116, Urbanización San Juan de Pampa, Yanacancha, Pasco, Pasco, Intercepción con Jirón Ramón Castilla
29	Gerencia Regional de Control Lima Provincias	Av. Túpac Amaru N° 209-211, ciudad de Huacho, provincia de Huaura, departamento de Lima.
30	Cusipata	Prolongación Los Álamos 983 Urb. Cusipata Km. 24 Carretera Central, Lima Metropolitana
31	Javier Prado	Calle Los Sauces Nº 450 Urb. Jacarandá - San Borja – Lima, Lima Metropolitana
32	Sede Central (Centro de datos Principal)	Jr. Camilo Carrillo 114 – Jesús María – Lima, Lima Metropolitana
33	Sede ENC (Centro de datos Secundario)	Jirón Bartolomé Herrera 255, Lince, Lima, Lima Metropolitana
34	Sede-Ancón	LL, A-2, Kartodromo de Santa Rosa, distrito de Santa Rosa, provincia de Lima, departamento de Lima, Lima Metropolitana

N°	Local	Dirección
35	Arequipa-N°1593	Av. Arequipa N° 1593-1599, esquina con el Jr. Emilio Althaus, Cercado de Lima, Lima, Lima Metropolitana
36	Sede-01	La Perla, Callao
37	Sede-02	Lima Metropolitana - Miraflores
38	Sede-03	Lima Metropolitana - Magdalena

Las direcciones indicadas en la Tabla N° 02 podrán ser actualizadas para la firma del contrato. Asimismo, respecto a las sedes Sede-Ancón, Sede-01, Sede-02 y Sede-03, la Entidad comunicará al contratista las direcciones finales una vez que cuente con la disponibilidad.

1.5. PLAZO DE PRESTACIÓN DEL SERVICIO

El plazo del presente servicio será de 1095 días calendario, contados desde el día siguiente de la firma el "Acta de Activación del Servicio N° 01" (el cual incluye la totalidad de los servicios indicados en el presente documento a excepción de los servicios de las sedes: Arequipa-N°1593, Sede-Ancón, Sede-01, Sede-02 y Sede-03), previa coordinación con la Entidad

Para los servicios de red de Datos para las Sedes Arequipa N° 1593, Sede-Ancón, Sede-01, Sede-02 y Sede 03 se iniciarán desde el día siguiente de la firma del "Acta de Activación del Servicio":

- Acta de Activación del Servicio N° 02: Sede Arequipa N° 1593.
- Acta de Activación del Servicio N° 03: Sede Ancón.
- Acta de Activación del Servicio N° 04: Sede-01.
- Acta de Activación del Servicio N° 05: Sede-02.
- Acta de Activación del Servicio N° 06: Sede-03.

Previa coordinación con la Entidad, además, estas deberán culminar la prestación del servicio en el mismo plazo que las otras sedes mencionadas en la Tabla N° 01.

Cabe indicar, que el plazo para el término de la implementación y puesta en operación del servicio será:

a) Ciento veinte (120) días calendario contados a partir del día siguiente de la firma del contrato, los cuales corresponden a la implementación del servicio de los enlaces de la Sede Central y Sede Escuela Nacional de Control (Internet y cabecera de la red MPLS), implementación del servicio de red de datos de los enlaces de las Sedes Remotas (ver Tabla N° 1 a excepción de las sedes: Sede-Ancón, Sede-01, Sede-02 y Sede-03) y los servicios según correspondan a los especificados en los numerales 1.1.3, 1.1.4, 1.1.5 y la instalación y operatividad del UPS.

b) Quince (15) días calendario, luego de culminada la implementación del servicio a nivel nacional, el contratista deberá realizar las pruebas de los servicios implementados.
Una vez realizados los procedimientos de implementación y pruebas, la Subgerencia de Operaciones y Plataforma Tecnológica suscribirá un "Acta de Activación del Servicio N° 01" que incluya los enlaces especificados en el numeral 1.1.1 y 1.1.2 (a excepción de los servicios de las Sedes Arequipa N° 1593, Sede-Ancón, Sede-01, Sede-02 y Sede 03), además de los servicios instalados especificados en el numeral 1.1.3, 1.1.4 y 1.1.5.

c) El inicio de la operatividad de los servicios en la Sede de Arequipa N° 1593 se realizará previa coordinación con la Entidad seguidamente se firmará el "Acta de Activación del Servicio N° 02".

d) Noventa (90) días calendario de plazo para la implementación y pruebas del servicio de Red de Datos en las sedes: Sede-Ancón, Sede-01, Sede-02 y Sede-03, el cual será contabilizado desde la notificación de la CGR para iniciar las actividades de implementación.

Culminadas estás actividades se firmarán las cuatro "Acta de Activación del Servicio" por cada una de las sedes, previa coordinación con la Entidad.

1.6. ENTREGABLES

El contratista deberá entregar en medio digital e impreso, a través de mesa de partes de la entidad, los siguientes documentos:

a) El plan de trabajo como máximo a los diez (10) días calendario posteriores a la firma del contrato, en el que se deberán indicar las actividades a desarrollar, con su duración en días, dicho plan deberá contener lo siguiente:
   i. Acta de constitución del proyecto.
   ii. EDT y Diagrama de Gantt.
   iii. Registro de Riesgos y Comunicaciones.
   iv. Protocolo de pruebas: El contratista debe proponer la descripción del protocolo de pruebas según corresponda para:
      - ✓ Verificar la conectividad desde las Sedes Remotas hacia la Sede Central y Sede Escuela Nacional de Control y viceversa.
      - ✓ Transferencia de datos y voz desde las Sedes Remotas hacia la Sede Central y Sede Escuela Nacional de Control y viceversa.
      - ✓ Validar la encriptación o cifrado en la comunicación de la red MPLS de las Sedes Remotas, Sede Central y Sede Escuela Nacional de Control.

   El contratista debe presentar una carta del fabricante donde indique el equipamiento no está en EOS (Fin de Venta o End Of Sale) y EOL (Fin de Vida o End Of Live) y que cuenta con soporte vigente, dicha carta será presentada conjuntamente con el Plan de trabajo.

b) Con un plazo máximo de veinte (20) días calendario, contados a partir del día siguiente de la firma del acta de implementación del servicio:
   i. Especificaciones técnicas de los equipos propuestos.
   ii. Diagrama físico y lógico de la arquitectura tecnológica.
   iii. Literal u del numeral 1.1.1.2., deberá presentar la documentación indicada.
   iv. Literal k de la sección “Características Técnicas” del numeral 1.1.2.2., deberá presentar la documentación indicada.
   v. Pruebas de Funcionalidad.
   vi. Manuales de usuario y operación, en formato electrónico (PDF o DOC).
   vii. Procedimiento a seguir para generar los requerimientos en la ventanilla del contratista (centro de gestión).

c) Documentos que acrediten la capacitación solicitada en el numeral 1.2.2.2, deben ser presentados en el plazo de diez (10) días calendario, contados a partir del día siguiente de la culminación de la capacitación.

d) El contratista deberá entregar mensualmente para la conformidad mensual los siguientes documentos:
   i. Reporte mensual de las averías o corte de servicio detectada por sede en las fechas realizadas y en minutos, este documento debe ser firmado por el contratista.
   ii. Reporte mensual o personalizado (rango de fechas) del consumo del servicio del ancho de banda por sede o enlace, este documento debe ser firmado por el contratista.
   iii. Reporte mensual de las atenciones solicitadas por el personal de la CGR.
   iv. Reporte mensual del estado de salud de los equipos UPS.
   v. Reporte mensual del monitoreo de los equipos de seguridad perimetral.
   vi. Reporte mensual del monitoreo de la solución para la protección de aplicaciones y servicios.

1.7. OBLIGACIONES DEL PROVEEDOR

El contratista para el presente servicio se obliga a cumplir el objeto del contrato:

a) Ejecutar los trabajos de acuerdo a lo señalado el presente documento, garantizando la ejecución del servicio en su totalidad.
b) Que el servicio de transporte de datos, deberá estar basado en últimas tecnologías que permitan el adecuado manejo de servicios, así como proveer conexión entre nodos de la Sede Central, Sede Escuela Nacional de Control y la Sedes Remotas, además del servicio de Internet.
c) Asumir todos los costos que puedan involucrar en la implementación del presente servicio.
d) Cada uno de los enlaces deberá estar operativo las 24 horas por los 7 días durante plazo de ejecución.

e) El contratista se compromete a brindar el soporte técnico las 24 horas por los 7 días durante plazo de ejecución.
f) Garantizar la migración de los circuitos de datos actuales causando el mínimo impacto en las operaciones de las sedes, para lo cual se realizará la coordinación entre la entidad y el proveedor de las sedes señaladas en la Tabla N° 02.
g) Debe interpretar los traps enviados por los equipos de comunicaciones y asociarse a ellos las alarmas de:
   i) Caídas de enlace.
   ii) Consumo de ancho de banda por encima del 80%.
   iii) Capacidad de procesamiento por encima del 80%.
h) El tipo de plataforma de transporte debe ser MPLS.
i) Además, el contratista debe:
   i) Asumir la responsabilidad, obligaciones civiles y penales por los daños que puedan ocasionar sus trabajadores a la CGR, durante el desarrollo del servicio, sean estos materiales o personales.
   ii) Celebrar cuando lo solicite la CGR, reuniones de coordinación, con participación de los responsables de las partes.
   iii) Aceptar cualquier procedimiento de supervisión y/o validación (verificación del servicio solicitado: La alta disponibilidad, incremento de anchos de banda, ancho de banda contratado, etc.) que efectúe en cualquier momento y sin previo aviso personal designado por la CGR, para lo cual brindará las facilidades del caso. Esta labor de supervisión no interferirá la ejecución de los trabajos encomendados.
   iv) No contratar personal o profesionales que labore o brinde servicios expresos a la CGR.
   v) El servicio a contratar es a todo costo; es decir, el contratista tiene bajo su cargo la responsabilidad económica, tributaria, administrativa y laboral, el aporte de mano de obra, materiales, suministros, equipos y cualquier otro material de servicio que se requiera para el cumplimiento del contrato.
   vi) Responsabilizarse plenamente por el desempeño de la labor que realice el personal calificado asignado a prestar el servicio para la CGR, así como su correcto comportamiento dentro de la jornada laboral que prestan el servicio.
j) Cumplir con los Protocolos Sanitarios Sectoriales en prevención del COVID-19, con las Normas y Protocolos Sanitarios en prevención del COVID-19 establecidas por el Ministerio de Salud, con los Protocolos Sanitarios Sectoriales para la continuidad de servicios para la prevención del COVID-19, con el Plan para la Vigilancia, Prevención y Control de COVID-19 y otros que sean necesarios, para el ingreso a sus instalaciones a nivel nacional durante la implementación del requerimiento, a efectos de proteger la salud del personal que participará en la ejecución del requerimiento.
k) El postor deberá proporcionar información técnica (marca, modelo, ficha técnica) de todo el equipamiento, software o licenciamiento de los componentes que brindará para el presente servicio.
l) El servicio a contratar es del tipo llave en mano, por lo que, el contratista deberá proporcionar todo el equipamiento y accesorios necesarios para dejar operativo el servicio.

1.8. CONFIDENCIALIDAD

El contratista se obliga a mantener la confidencialidad y reserva absoluta en el manejo de información a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros.

En tal sentido, el contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Dicha obligación comprende 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 la prestación. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.

1.9. CONFORMIDAD DEL SERVICIO

Una vez realizados los procedimientos de implementación y pruebas, la Subgerencia de Operaciones y Plataforma Tecnológica suscribirá un “Acta de Activación del Servicio N° 01” del servicio que incluya la conformidad de los enlaces especificados en el numeral 1.1.1 y 1.1.2 (a excepción de las sedes de Arequipa N° 1593, Sede-Ancón, Sede-01, Sede-02 y Sede 03), además

de los servicios instalados especificados en el numeral 1.1.3, 1.1.4 y 1.1.5.

Una vez realizados los procedimientos de implementación y pruebas, la Subgerencia de Operaciones y Plataforma Tecnológica suscribirán las "Acta(s) de Activación del Servicio" (del N° 02 al N° 06) que incluya la conformidad de los enlaces de las sedes de Arequipa N° 1593, Sede-Ancón, Sede-01, Sede-02 y Sede 03.

La conformidad del servicio será otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, quien será responsable de verificar la calidad, cantidad y cumplimiento de las condiciones contractuales, debiendo emitir mensualmente la conformidad técnica por la prestación efectuada previo la recepción y verificación de la documentación indicada en el literal d, numeral 1.6. - Entregables.

1.10. FORMA DE PAGO

Se realizará el pago de la contraprestación pactada a favor del contratista de la siguiente manera:

a) Pago por la prestación principal: 100%, prorrateada en treinta y seis (36) meses, luego de la recepción de la documentación solicitada en el entregable literal d), numeral 1.6 - Entregables.
   Para efectos del pago se deberá contar con la siguiente documentación:
   - Conformidad otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, previo informe técnico del personal responsable de la verificación del servicio, quien emitirá mensualmente la conformidad técnica por la prestación efectuada.
   - Comprobante de Pago.

b) Pago por las prestaciones accesorias: 100% prorrateada en treinta y seis (36) meses, luego de la recepción de la documentación solicitada en el entregable literales c) y d) del numeral 1.6 – Entregables.
   Para efectos del pago se deberá contar con la siguiente documentación:
   - Conformidad otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, previo informe técnico del personal responsable de la verificación del servicio, quien emitirá mensualmente la conformidad técnica por la prestación efectuada.
   - Comprobante de Pago.

Cabe indicar que el primer pago se realizará al siguiente mes de firmado el "Acta de Activación del Servicio N° 01" emitida por la Subgerencia de Operaciones y Plataforma Tecnológica, y en el caso del último pago estará condicionado al cumplimiento de la totalidad del servicio.

1.11. PENALIDADES

Si el contratista incurre en retraso injustificado en la ejecución del servicio, se le aplicará una penalidad por cada día calendario de atraso, de acuerdo al Artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Otras Penalidades

En los casos en que se produzca un retraso en la atención de averías, y el motivo del retraso sea imputable a las gestiones de acceso al local u otras causas atribuibles a la CGR, se considerará una "parada de reloj" la cual será registrada en la ficha de servicio y/o hoja de atención del contratista y se reanudará una vez superado el inconveniente a efectos de llevar el control de los tiempos de atención requeridos en los términos de referencia del servicio.

Por lo tanto, en aplicación de lo dispuesto en el artículo 163 del Reglamento de la Ley de Contrataciones del Estado. Se aplicarán otras penalidades, según lo establecido a continuación:

a. Por la no disponibilidad o disminución del ancho de banda solicitado en el servicio de Internet del numeral 1.1.1 y MPLS del 1.1.2. (Sede Central, Sede ENC y Sedes Remotas dentro de Lima Metropolitana):

No disponibilidad o disminución del ancho de banda solicitado en el servicio de los numerales 1.1.1 y 1.1.2.	Número de minutos en los que el servicio se haya interrumpido en el mes	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Hasta 43.2 minutos	Sin penalidad
	Entre 43.3 minutos hasta 73.3 minutos	10%
	Entre de 73.4 minutos hasta 103.4 minutos	20%
	Más de 103.4, por cada 60 minutos adicionales	22% más 5% por cada 60 minutos adicionales.
Para efectos del cálculo de la penalidad, se acumularán los minutos en los que el servicio se haya interrumpido en el mes, contados desde que la CGR reporte la incidencia vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

b. Por la no disponibilidad o disminución del ancho de banda solicitado en el servicio MPLS del numeral 1.1.2. (Sedes Remotas fuera de Lima Metropolitana):

No disponibilidad o disminución del ancho de banda solicitado en el servicio del numeral 1.1.2.	Número de minutos en los que el servicio se haya interrumpido en el mes	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Hasta 130 minutos	Sin penalidad
	Entre 131 minutos hasta 160 minutos	10%
	Entre de 161 minutos hasta 190 minutos	20%
	Más de 191, por cada 60 minutos adicionales	22% más 5% por cada 60 minutos adicionales.
Para efectos del cálculo de la penalidad, se acumularán los minutos en los que el servicio se haya interrumpido en el mes, contados desde que la CGR reporte la incidencia vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

c. Por la demora en la atención de requerimientos técnicos (cambio de registros DNS, problemas con el sistema de monitoreo):

Demora en la atención de requerimientos técnicos	Número de horas en exceso al requerido	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Más de veinte cuatro (24) horas	10%
	Más de cuarenta y ocho (48) horas	20%
	Más de setenta y dos (72) horas	22% más 0.5% por hora adicional.
Para efectos del cálculo de la penalidad, se acumularán las horas en exceso al requerido como “Tiempo de atención de requerimientos técnicos” en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

d. Por la demora en la atención de requerimientos técnicos relacionados al "cambio de los equipos" (numerales 1.1.3, 1.1.4 y 1.1.5) de la SEDE CENTRAL Y SEDE DE ESCUELA NACIONAL DE CONTROL:

Demora en la atención de requerimientos técnicos relacionados al "cambio de los equipos " Numerales 1.1.3, 1.1.4. y 1.1.5	Número de horas en exceso al requerido	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Más de veinticuatro (24) horas	5%
	Más de treinta y seis (36) horas	10%
	Más de cuarenta y ocho (48) horas	15% más 2.5% por hora adicional.
Para efectos del cálculo de la penalidad, se acumularán las horas en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

e. Por la demora en la atención de requerimientos técnicos relacionados al "cambio de los equipos" numerales 1.1.3, 1.1.4 y UPS de las SEDES REMOTAS:

Demora en la atención de requerimientos técnicos relacionados al "cambio de los equipos " Numerales 1.1.3 y 1.1.4	Número de horas en exceso al requerido	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Más de cuarenta y ocho (48) horas	5%
	Más de setenta y dos (72) horas	10%
	Más de ochenta y cuatro (96) horas	15% más 2.5% por hora adicional.
Para efectos del cálculo de la penalidad, se acumularán las horas en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

f. Por la demora en la atención de requerimientos de traslado del medio de comunicación de las sedes de Lima y provincia a nivel nacional, se considerará lo siguiente:

Demora por el traslado del servicio imputables al contratista	Número de días en exceso al requerido.	% Calculado respecto al monto mensual facturado correspondiente al servicio
	Más de sesenta (60) días	10%
	Más de setenta y cinco (75) días	20%
	Más de noventa (90) días	22% más 5% por día adicional.
Para efectos del cálculo de la penalidad, se acumularán los días en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

g. Por la demora en la atención de requerimientos de traslado de sede de provincia (Internet temporal), se considerará lo siguiente:

Demora en la atención de requerimientos de instalación Internet Temporal	Número de días en exceso al requerido.	Factor de penalidad
	Más de quince (15) días	5% UIT
	Más de veinte (20) días	10% UIT

	Más de veinticinco (25) días	12% UIT más 2.5% UIT por día adicional.
Para efectos del cálculo de la penalidad, se acumularán los días en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

h. Por la demora en la atención de requerimientos del servicio de gestión y soporte (numeral 1.2.1) se considerará lo siguiente:

Demora en la atención de requerimientos del servicio de gestión y soporte Numeral 1.2.1	Número de horas en exceso al requerido	Factor de penalidad
	Más de dos (02) horas	10% UIT
	Más de cuatro (04) horas	20% UIT
	Más de siete (07) horas	22% UIT más 5% por hora adicional.
Para efectos del cálculo de la penalidad, se acumularán las horas en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en el mes, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

i. Por la demora en el requerimiento del servicio de atención a la inoperatividad del UPS:

Demora en el requerimiento del servicio de atención a la inoperatividad del UPS	Número de horas en exceso al requerido	Factor de penalidad
	Hasta 30 minutos	Sin penalidad
	Entre 31 minutos hasta 60 minutos	10% UIT
	Entre de 61 minutos hasta 90 minutos	20% UIT
	Más de 91, por cada 60 minutos adicionales	22% UIT más 5% por cada 60 minutos adicionales.
Para efectos del cálculo de la penalidad, se acumularán los minutos en los que el servicio se haya interrumpido en el mes, contados desde que la CGR reporte la incidencia vía correo electrónico al supervisor general del servicio del contratista, ingeniero residente dedicado o centro de atención de averías, a quién solicitará la generación del ticket de atención, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

Nota a considerar:
La Subgerencia de Operaciones y Plataforma Tecnológica comunicará a la Subgerencia de Abastecimiento el incumplimiento realizado por el contratista, para lo cual debe detallar específicamente el incumplimiento advertido, adjuntando el sustento respectivo, a efectos de que la Subgerencia de Abastecimiento comunique al contratista dichos incumplimientos con el monto de la penalidad a aplicarse, el respectivo motivo de aplicación y los adjuntos respectivos.

1.12. DOCUMENTOS PARA EL PERFECCIONAMIENTO DEL CONTRATO

El proveedor debe ser representante de los productos ofertados, lo cual se acreditará para el perfeccionamiento del contrato.

1.13. REQUISITOS DE CALIFICACIÓN

a. Capacidad legal

Habilitación

<u>Requisitos:</u>

Contar con la autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio requerido.

Importante
De conformidad con la Opinión N° 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.

Acreditación:

Copia simple de la autorización emitida por el Ministerio de Transportes y Comunicaciones o copia del Certificado de Registros de Empresas Prestadoras de Servicio de Valor Añadido emitido por el Ministerio de Transportes y Comunicaciones.

Importante
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.

b. Capacidad Técnica y Profesional

b.1 Calificaciones Del Personal Clave

b.1.1 Formación Académica

Un (01) jefe de Proyecto

Requisitos:

Profesional titulado, colegiado y habilitado (la colegiatura y la habilitación del profesional se requerirá para el inicio de su participación efectiva en el contrato) en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial

Un (01) Supervisor General del Servicio

Requisitos:

Profesional titulado, colegiado y habilitado (la colegiatura y la habilitación del profesional se requerirá para el inicio de su participación efectiva en el contrato) en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial.

Un (01) Ingeniero Residente Dedicado

Requisitos:

Profesional titulado en Ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Mecánica o Industrial.

Un (01) Especialista en Routing-Switching

Requisitos:

Título de técnico en Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Telecomunicaciones, o Redes y/o Comunicaciones, o con el grado bachiller en ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones.

Un (01) Especialista en Seguridad Perimetral

Requisitos:

Título de técnico en Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Telecomunicaciones, o Redes y/o Comunicaciones, o Redes y Seguridad Informática, o Administración de Redes y Comunicaciones, o con el grado bachiller en ingeniería Sistemas y/o Informática, o Sistemas y/o Cómputo, o Electrónica, o Eléctrica, o Telecomunicaciones, o Redes y/o Comunicaciones.

Acreditación:

El título profesional será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe// o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda.

En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

b.2 Experiencia Del Personal Clave

Un (01) jefe de Proyecto

Jefe de Proyecto

Requisitos:
Contar con experiencia mínima de tres (3) años en la supervisión o conducción o dirección técnica de prestación o gestión o implementación o ejecución de servicios o trabajos de: Telecomunicaciones y/o tecnologías de la información.

Un (01) Supervisor General del Servicio

Requisitos:
Contar con experiencia mínima de tres (3) años en la supervisión o conducción o dirección técnica de prestación o ejecución de servicios o trabajos de: instalación o mantenimiento de enlaces de transmisión de datos.

Un (01) Ingeniero Residente Dedicado

Requisitos:

Contar con experiencia mínima de tres (3) años en la implementación del servicio de Internet y/o redes de datos y/o instalación y/o configuración y/o soporte técnico y/o solución de problemas de los equipos involucrados en el presente servicio.

Un (01) Especialista en Routing-Switching

Requisitos:

Contar con experiencia mínima de dos (2) años en la ejecución de servicios y/o trabajos y/o actividades de: instalación y/o mantenimiento de enlaces de transmisión de datos.

Un (01) Especialista en Seguridad Perimetral

Requisitos:
Contar con experiencia como mínima de dos (2) años de experiencia en implementación en este tipo de soluciones

Acreditación:
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.

Nota:
La experiencia en caso de presentar título profesional se computa desde la obtención de la colegiatura; en caso de presentar bachiller y/o título técnico, se computa a partir de la obtención del grado.

Un (01) Especialista en la solución para la protección de aplicaciones y servicios

Requisitos:
Contar con experiencia como mínima de dos (2) años de experiencia en implementación en este tipo de soluciones

Acreditación:
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.

Nota:
La experiencia en caso de presentar título profesional se computa desde la obtención de la colegiatura; en caso de presentar bachiller y/o título técnico, se computa a partir de la obtención del grado

c. Experiencia Del Postor En La Especialidad

El postor debe acreditar un monto facturado acumulado equivalente a una 8,000,000.00 (8 millones de soles), por la contratación 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.

Se consideran servicios similares a los siguientes:

i. Servicio de habilitación de enlaces de telecomunicaciones.
ii. Mantenimiento de telecomunicaciones y/o servicio de telecomunicaciones.
iii. Mantenimiento de equipos de telecomunicaciones y/o servicio de equipos de telecomunicaciones.
iv. Mantenimiento de centro de datos o data center y/o servicio de centro de datos o data center.
v. Servicio de VPN y/o MPLS y/o Red de Datos y/o transmisión de datos.
vi. Servicio de internet dedicado y/o fijo.
vii. Servicio de Internet y/o transmisión de datos

viii. Servicio de comunicación mediante fibra óptica.
ix. Servicio de acceso a Internet fijo.
x. Servicios de arrendamiento de circuitos o tránsito de Internet.
xi. Servicio de Internet y Enlace de tatos.
xii. Servicio de Transmisión-Recepción de datos a través de terminales de conexión satelital.
xiii. Servicio de Transmisión y/o conectividad de datos en general.
xiv. Servicio Administrado de Infraestructura en nube y/o Servicio de infraestructura en nube.

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.

2. ÍTEM 02: SERVICIO DE IMPLEMENTACIÓN DE SOLUCIÓN DE ENLACE DE FIBRA ÓPTICA OSCURA ENTRE LA SEDE CENTRAL Y LA SEDE ESCUELA NACIONAL DE CONTROL

2.1. PRESTACION PRINCIPAL

2.1.1. REQUISITOS GENERALES

Brindar el servicio de implementación de solución de enlace de fibra óptica oscura entre la sede Central y la Escuela Nacional de Control (ENC).

2.1.2. CARACTERÍSTICAS TÉCNICAS

a) Permitir la comunicación por medio de dos enlaces de fibra óptica oscura (Principal y Secundaria) entre los locales sede Central y la Escuela Nacional de Control, tal como se indica en la Gráfica-01.
b) Permitir la comunicación por medio de seis (06) hilos de fibra óptica oscura (cada enlace) entre la Sede Central y la Escuela Nacional de Control, tal como se indica en la Gráfica-01.
c) Los dos enlaces deben estar en modo activo/activo.
d) Las rutas de los dos enlaces de fibra óptica oscura deberán ser diferentes en todo su recorrido, desde la salida de cada sede.
e) Permitir el transporte de voz, datos y video sobre el Protocolo IP.
f) Permitir velocidades de hasta 40Gbps por cada par de hilo.
g) Medio de Transmisión: Enlaces dedicados de fibra óptica oscura monomodo.
h) Topología punto a punto.
i) Número de enlaces: dos (02)
j) Numero de hilos por enlace: seis (06)
k) Tipo de conector en los terminales: LC
l) Los hilos de fibra óptica oscura para el enlace deben terminar en una bandeja rackeada para fibra óptica y con terminales LC.
m) Para cada par de hilos de los enlaces debe de incluir dos (02) patch cord de fibra de dos metros (cada uno) con terminales LC.
n) Realizar la instalación y configuración de los equipos y accesorios que se requieran, para poner operativo el enlace, el cual estará a cargo del contratista.
o) La Entidad dará las facilidades para que los postores realicen las visitas técnicas de reconocimiento físico para que tomen conocimiento de los equipos y la ubicación de los cuartos de comunicación que cuenta cada uno de los dos locales.
p) Los postores interesados en realizar las visitas, deberán coordinar las mismas con la Subgerencia de Operaciones y Plataforma Tecnológica

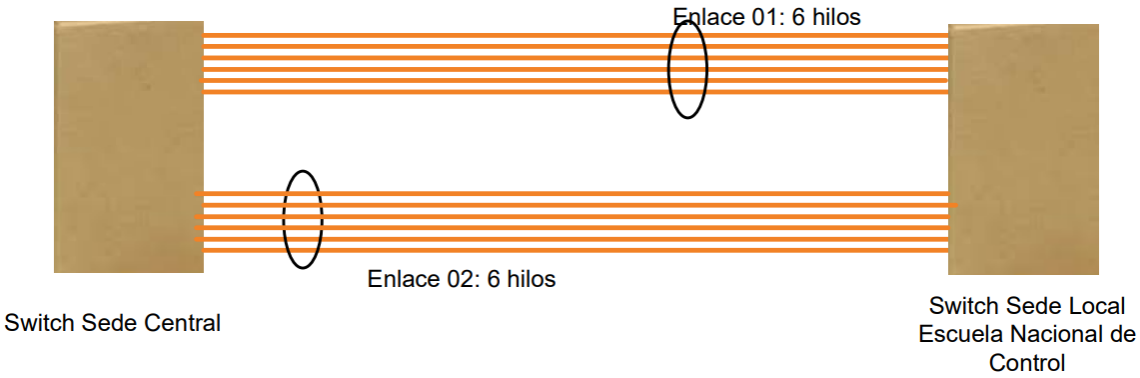
(vmoreno@contraloria.gob.pe o jinga@contraloria.gob.pe) a través de la Subgerencia de Abastecimiento, con la debida anticipación.

q) Se precisa que la entidad cuenta con switches y transceiver con puertos de velocidad de 40 GBps.

r) El servicio a contratar es del tipo llave en mano, por lo que, el contratista deberá proporcionar todo el equipamiento y accesorios necesarios para dejar operativo el servicio.

El contratista, se ceñirá aplicando las normas y estándares que existen en el mercado para este rubro (tendido de fibra óptica oscura)

ENLACE DE FIBRA ÓPTICA OSCURA ENTRE LA SEDE CENTRAL Y LA SEDE ESCUELA NACIONAL DE CONTROL



2.2. PRESTACIONES ACCESORIA

2.2.1. SOPORTE TÉCNICO

Disponibilidad de soporte técnico las 24 horas por los 7 días durante el plazo de ejecución del servicio, relacionado con problemas de enlaces de conexión, fallos y reposición de equipos que son parte del servicio, en caso amerite, así como respuesta a consultas de carácter técnico relacionados con la disponibilidad de los enlaces, servicios de red y el equipamiento de la solución de enlace de fibra óptica oscura entre la sede Central y la sede Escuela Nacional de Control.

2.2.2. GESTIÓN DEL SERVICIO
ATENCIÓN DE AVERÍAS

a) Se entenderá como avería a una interrupción total del servicio, así como a un decremento en la calidad del mismo.

b) Toda actividad o provisión de bienes (equipos parte del servicio) será sin costo alguno para la Entidad, debe garantizar el correcto funcionamiento de todos los equipos e infraestructura que utiliza para brindar el servicio en el periodo de tiempo de su ejecución.

c) El contratista deberá contar con un centro de atención de llamadas para reparación o asistencia técnica instalado.

d) El plazo máximo para subsanar (averías o ruptura de fibra óptica en uno de los enlaces) será máximo de 08 horas y el tiempo máximo de la no disponibilidad del servicio (comunicación entre la entre la Sede Central y Sede Escuela Nacional de Control) será de 30 minutos acumulados en dos meses, ambos contados desde que la CGR reporte la incidencia vía correo electrónico al Soporte Técnico del contratista. Al respecto, el contratista deberá indicar la información sobre los puntos de contacto para la gestión adecuada del servicio. La información sobre los puntos de contacto está referida al centro de atención de averías (número telefónico, correo electrónico). Esta información deberá presentarse para el perfeccionamiento del contrato.

e) El cierre del requerimiento, debe realizarse de manera coordinada entre personal del contratista y la CGR que designe para tal efecto. El requerimiento generado,

sólo podrá ser cerrado cuando sea corroborada la solución y aceptada con el visto bueno por parte de la CGR.

f) Toda actividad o provisión de bienes que tenga que ejecutar el proveedor del servicio para subsanar una interrupción del servicio será sin costo alguno para la CGR.
g) La CGR podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde la 00:00 hasta las 23:59 horas.
h) Las llamadas de servicio se sujetarán a lo siguiente: Se podrá efectuar telefónicamente y por correo electrónico (considerándose todas estas formas igualmente válidas) a las direcciones acordadas entre la CGR y el contratista. La CGR notificará las anomalías que se presenten incluyendo la siguiente información: fecha y hora, descripción del problema, contacto en la CGR.
i) El contratista deberá entregar a la CGR una nómina del personal técnico autorizado a realizar labores de mantenimiento correctivo con sus respectivos SCTR y documentos asociados a la labor que realizará en los locales de la CGR. Dicha nómina deberá ser actualizada cuando se produzcan cambios.

2.3. LUGAR DE PRESTACIÓN DEL SERVICIO

Los locales donde deberán estar los terminales del enlace de fibra óptica oscura son:

- Sede Central, Jr. Camilo Carrillo 114, Jesús María, Lima
- Local Escuela Nacional de Control (ENC), Jirón Bartolomé Herrera 255, Lince, Lima.

2.4. ENTREGABLES

2.4.1.El Informe Final de la instalación y puesta en funcionamiento del servicio

El Informe deberá contener lo siguiente:

- Planos detallados donde se indique rutas seguidas por el cableado de fibra (en formato digital).
- Planos de acometidas (en formato digital).
- Resultado de las pruebas realizadas al enlace de fibra óptica oscura (certificación), a través de equipo certificador vigente o similar.
- Documentos de las características técnicas de la fibra óptica oscura y los accesorios que componen el enlace, o declaración jurada en la cual se precise el cumplimiento de lo solicitado.
- Documentación de los Patch Panels. Vista frontal de los paneles de distribución (patch panels), con los detalles de etiquetado de identificación de puntos de manera impresa.
- Acta del Protocolo de Prueba (validación de la instalación, implementación y puesta en funcionamiento de los enlaces).
- Carta del Contratista detallando los correos y números telefónicos para atención de Soporte Técnico por la prestación del servicio.
- Adicionalmente, el Contratista debe presentar el informe donde se detalle los equipos, dispositivos y/o componentes que está dejando en la entidad para la puesta en marcha del servicio.

2.4.2. Informe de ocurrencia

Informe de ocurrencia dentro de los dos meses del servicio facturado durante el periodo del servicio contratado, el cual se detalle las incidencias presentadas durante el periodo.

Los entregables 2.4.1 y 2.4.2 deberán ser presentados a través de la mesa de partes de la Contraloría General de la Republica.

2.5. PLAZO DE PRESTACIÓN DEL SERVICIO

- El contratista deberá efectuar la instalación e implementación y puesta en funcionamiento en un plazo máximo de setenta (70) días posteriores a la firma del contrato, tras lo cual se realizará la firma del “Acta de Culminación”.

- Culminada la instalación e implementación y puesta en funcionamiento el servicio, la Entidad contará hasta con cinco (05) días hábiles para la validación a través de un “Acta de Protocolo de Prueba” del servicio, terminada esta actividad se firmará el “Acta de Implementación“.
- El Informe Final de la instalación y puesta en funcionamiento del servicio (indicado en el punto 2.4.1) debe ser presentado cinco (05) días calendario posterior a la suscripción del “Acta de Protocolo de Prueba”.
- El plazo del presente servicio será de 1095 días calendario, contados a partir del día siguiente de haber realizado la firma del “Acta de Activación del Servicio”, el cual será posterior a la firma del “Acta de Implementación”, previa coordinación con la Entidad.
- Respecto al informe de ocurrencia, el contratista deberá presentar de acuerdo a lo indicado en el punto 2.4.2 en un plazo máximo de diez (10) días calendario de culminado los dos meses correspondientes.

2.6. OBLIGACIONES DEL PROVEEDOR

2.6.1. MATERIALES DE CABLEADO

Los materiales a usarse para el presente servicio, deberá ser proporcionado por el contratista.

2.6.2. TRASLADO

En caso fuese necesario trasladar o movilizar recursos humanos, equipos, cables, etc., objeto del contrato, serán entera responsabilidad del Contratista.

2.6.3. PERMISO DE TERCEROS

Los permisos a las diferentes entidades privadas o del estado, deberán ser coordinado por el Contratista (empresa que implemente el servicio) directamente con dichas entidades, para cumplir con el servicio.

2.6.4. RESANE Y ACABADOS

El contratista tendrá la obligación de efectuar resanes y acabados de la totalidad de las zonas donde ha efectuado trabajos, lo cual incluirá: jardines, muros, techos, pisos, puertas, ventanas, paredes, veredas, pistas, entre otros. Este resane incluirá los acabados correspondientes.

2.6.5. INSPECCIÓN Y PROTOCOLO DE PRUEBA

Una vez terminadas las actividades de instalación, el contratista antes de poner en marcha los enlaces, deberá de realizar las actividades de inspección y pruebas.

El contratista y el personal técnico de la Entidad, realizarán en forma conjunta los procedimientos de inspección y los protocolos de pruebas antes del otorgamiento de la conformidad técnica.

Si durante la realización de estas pruebas se determina que el sistema instalado no cumple con una o más de las especificaciones contratadas, el contratista deberá subsanar esta deficiencia, mediante el reemplazo, reposición o reconfiguración.

2.7. CONFORMIDAD DEL SERVICIO

La conformidad del servicio será otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, quien será responsable de verificar la calidad, cantidad y cumplimiento de las condiciones contractuales, debiendo emitir cada dos meses la conformidad técnica por la prestación efectuada previo la recepción y verificación de la documentación indicada en el numeral 2.4.2.

2.8. FORMA DE PAGO

Se realizará el pago de la contraprestación pactada a favor del contratista de la siguiente manera:

a) Pago por la prestación principal: 100%, prorrateado cada dos meses por el periodo de servicio contratado, luego de la recepción de la documentación solicitada en el entregable 2.4.2.

Para efectos del pago se deberá contar con la siguiente documentación:

- Conformidad otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, previo informe técnico del personal responsable de la verificación del servicio, quien emitirá cada dos meses la conformidad técnica por la prestación efectuada.
- Comprobante de Pago.

b) Pago por las prestaciones accesorias:

Pago por las prestaciones accesorias; 100% prorrateada cada dos meses por el periodo de servicio contratado, luego de la recepción de la documentación solicitada en el entregable 2.4.2.

Para efectos del pago se deberá contar con la siguiente documentación:

- Conformidad otorgada por la Subgerencia de Operaciones y Plataforma Tecnológica, previo informe técnico del personal responsable de la verificación del servicio, quien emitirá cada dos meses la conformidad técnica por la prestación efectuada.
- Comprobante de Pago.

Cabe indicar que el primer pago se realizará a los dos meses de firmado el acta de implementación del servicio ("Acta de implementación") emitida por la Subgerencia de Operaciones y Plataforma Tecnológica, y en el caso del último pago estará condicionado al cumplimiento de la totalidad del servicio.

2.9. PENALIDADES

La penalidad por mora se aplicará de acuerdo a lo descrito en el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Otras Penalidades:

De acuerdo al reglamento de la Ley de Contrataciones descrito en el artículo 163

a. Por la no disponibilidad del servicio (comunicación entre la Sede Central y la Escuela Nacional de Control) a través de la fibra óptica oscura:

Interrupciones del servicio	Número de minutos en los que el servicio se haya interrumpido en los dos meses	% Calculado respecto al monto cada dos meses facturado correspondiente al servicio contratado
	Hasta 30 minutos	Sin penalidad
	Entre 31 minutos hasta 60 minutos	10%
	Entre de 61 minutos hasta 120 minutos	20%
	Más de 121 minutos, por cada 60 minutos adicionales	22% más 5% por cada 60 minutos adicionales.
Para efectos del cálculo de la penalidad, se acumularán los minutos en los que el servicio se haya interrumpido en los dos meses correspondiente a la facturación, contados desde que la CGR reporte la incidencia vía correo electrónico (o teléfono) y generado el ticket, hasta una vez cerrado el ticket por parte del postor vía notificación por correo electrónico a la CGR.		

b. Por la demora en la atención de requerimientos técnicos (reposición de uno de los enlaces o los componentes que son parte del servicio):

Demora en la atención de	Número de horas en exceso al requerido	% Calculado respecto al monto cada dos meses

requerimientos técnicos		facturado correspondiente al servicio contratado
	Más de veinticuatro (24) horas	10%
	Más de cuarenta y ocho (48) horas	20%
	Más de setenta y dos (72) horas	25% más 5% por cada 24 horas adicionales.
Para efectos del cálculo de la penalidad, se acumularán las horas en exceso al requerido como "Tiempo de atención de requerimientos técnicos" en los dos meses, a partir de cuándo la CGR solicita el requerimiento vía correo electrónico (o teléfono) y generado el ticket, hasta una vez cerrado el ticket por parte del contratista vía notificación por correo electrónico a la CGR.		

2.10. REQUISITOS DE CALIFICACIÓN

A. CAPACIDAD TÉCNICA Y PROFESIONAL

A.1. CALIFICACIONES DEL PERSONAL CLAVE

FORMACIÓN ACADÉMICA

- **Un Coordinador de Proyectos**
  Requisitos:
  Ingeniero o Bachiller o técnico titulado en las especialidades de Sistema o Computación o Electrónica o Telecomunicaciones o Eléctrica, quien realizará las coordinaciones con el área usuaria para la instalación y puesta en funcionamiento del servicio.

- **Un Especialista en cableado estructurado de fibra óptica**
  Requisitos:
  Ingeniero o Bachiller o técnico en las especialidades de Sistema o Computación o Electrónica o Telecomunicaciones, quien supervisará la instalación y puesta en funcionamiento del servicio.

  Acreditación:
- El grado o título será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe// o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.

  En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

CAPACITACIÓN

- **Un Especialista en cableado estructurado de fibra óptica**
  Requisitos:
  Contar con capacitación (mínimo 24 horas) en fibra óptica.

  Acreditación:
- Se acreditará con copia simple de constancia o certificado u otros documentos, según corresponda.

A.2 EXPERIENCIA DEL PERSONAL CLAVE

- **Un Coordinador de Proyectos**
  Requisitos:
  Contar con experiencia mínima de un (01) año en coordinación de proyectos de implementación de servicio de redes y/o comunicaciones de voz y/o datos y/o servicios de telecomunicaciones tales como: Internet y/o transmisión de datos y/o comunicación de datos y/o enlace de datos y/o interconexión de datos y/o telefonía y/o seguridad.

- **Un Especialista en cableado estructurado de fibra óptica**
  Requisitos:
  Contar con experiencia mínima de un (01) año en implementación de cableado de fibra óptica e implementación de proyectos y/o servicios de telecomunicaciones tales como: internet y/o transmisión de datos y/o comunicación de datos y/o enlace de datos y/o interconexión de datos y/o telefonía y/o seguridad.

- Acreditación:
  La experiencia del personal clave 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.

B. EXPERIENCIA DEL POSTOR

Requisitos:
El postor debe acreditar un monto facturado acumulado equivalente mínimo a doscientos cincuenta mil soles (250 000.00), por la contratación 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 caso de postores que declaren tener la condición de micro y pequeña empresa, se acredita una experiencia de setenta y cinco mil soles (S/ 75 000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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 caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Servicio de Implementación o soporte de enlace de fibra óptica o
- Servicio de alquiler de enlace de fibra óptica o
- Servicio de enlaces dedicados de transmisión de datos o
- Servicio de interconexión de datos y transmisión de datos o
- Servicio de transporte de datos por fibra óptica y/o Enlaces de fibra óptica y/o enlaces de fibra oscura y/o servicio de internet por fibra óptica y/o servicios de internet dedicado por fibra óptica o
- Instalación y/o cableado y/o tendido de fibra óptica.
- Servicio de transmisión de datos en general
- Servicio de transmisión - Recepción de datos a través de terminales de conexión satelital.

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.

VII. RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte de la Contraloría General de la República 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 un (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.

VIII. SISTEMA DE CONTRATACIÓN

El Sistema de contratación es a Suma Alzada.

IX. CONFIDENCIALIDAD

El contratista se obliga a mantener la confidencialidad y reserva absoluta en el manejo de información a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros.

En tal sentido, el contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Dicha obligación comprende 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 la prestación. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.

X. SUBCONTRATACIÓN

No aplica en aquellas prestaciones que se consideren como esenciales que son parte del objeto principal del servicio, el cual corresponde al servicio de internet, servicio de red datos y servicio de fibra óptica oscura. Para el resto de servicios si aplica la subcontratación según lo establecido en el RCE

XI. CLÁUSULA ANTICORRUPCIÓN

EL CONTRATISTA se compromete a cumplir lo siguiente:

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.

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.

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.

Verificar la Política y Objetivos de Gestión Antisoborno de la CGR, en la siguiente ruta web: https://busquedas.elperuano.pe/normaslegales/aprueban-la-politica-y-objetivos-de-gestion-antisoborno-de-l-resolucion-no- 092-2021-cg-1939721-1/.

ANEXO N°01

Características Técnicas de los Dispositivos de Seguridad Perimetral

CARACTERISTICAS	DESCRIPCION
Cantidad	Dos (02) soluciones de seguridad perimetral. *Distribución: Uno (01) en la Sede Central y uno (01) en la Sede de ENC*
Descripción	a. La solución de seguridad perimetral se puede componer de uno o más equipos físicos o appliance. b. La solución de seguridad perimetral debe estar en la categoría de Next Generation Firewall (NGFW). c. La solución de seguridad perimetral debe ser de la misma marca y en su conjunto cumplan la totalidad de las especificaciones técnicas.
Alta disponibilidad	La solución debe incluir las siguientes funcionalidades como mínimo: a. activadas y licenciadas, disponibles para su uso, sin costo adicional para la CGR. b. Debe incluir la funcionalidad de alta disponibilidad para todos los componentes de la solución, en las modalidades activo-activo y/o activo-pasivo y/o activo-standby.y/o cluster
Formato	Un 01 Rack Uint (RU) como mínimo e incluir el kit de montaje del mismo fabricante de la solución, para ser instalado en el gabinete de comunicaciones.
Conectividad	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: a. Cuatro (04) puertos de 10Gbps Ethernet, incluyendo su transceiver o modulo (SFP+ o XFP) con conector del tipo LC (fibra óptica), para cada puerto b. Cuatro (04) interfaces de un (01) Gigabit Ethernet con conector RJ45. c. Un (01) puerto Gigabit Ethernet RJ45 Management o Puerto de servicio. d. Un (01) Puerto USB. e. Un (01) Puerto de Consola. f. Protocolo IPV4 e IP v6.
Gestión de la Solución	La solución debe incluir las características mencionadas a continuación como mínimo: activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: a. Comunicación serial (COM) o Interface USB (console port) b. SSH c. Syslog. d. SNMP v2c y v3. e. sFlow y/o Netflow y/o IPFIX. f. Se debe mostrar como mínimo gráficos del tráfico entrante y saliente en tiempo real, así como gráficos de tráfico por IP origen, IP destino y servicios/puertos. g. Se debe incluir la búsqueda de eventos en logs correlacionados utilizando como mínimo filtros por top IP origen, top IP destino, top aplicación/servicio, top reglas/políticas. h. Debe mostrar gráficos de eventos correlacionados como mínimo por hora, día y semana i. Como mínimo debe mostrar eventos correlacionados por aplicaciones y amenazas. j. Debe emitir reportes programados de forma diaria, semanal y mensual. k. Los reportes generados deben ser descargados y enviados por correo. l. Capacidad para gestionar dominios virtuales u otro similar con una capacidad mínima de 10 o superior.
	m. Los firewalls deben ser administrados desde una consola de administración centralizada.

CARACTERISTICAS	DESCRIPCION
	n. La solución de seguridad debe enviar la información de tráfico de red permitido y bloqueado, aplicaciones, accesos VPN, log de eventos de usuario y del sistema hacia un repositorio de log independiente.
	o. El repositorio de logs debe permitir la generación de reportes preestablecidos y personalizados (manual y de manera programada), asimismo la correlación de eventos, el equipamiento de correlación de la información entregada por la solución de seguridad y debe incluir una capacidad de almacenamiento de 32 TB en RAID 1.
Gestión de dispositivos y usuarios	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: a. Identificación y/o autenticación de dispositivos en base a su dirección física de red (MAC Address) o Portal cautivo que permita la autenticación de los usuarios al firewall. b. Usuarios locales. c. Integración de usuarios vía LDAP. d. Autenticación basada en el modelo AAA (Authentication, Authorization and Accounting). e. RADIUS.
Políticas de seguridad y priorización de trafico	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: a. Análisis de inspección completo de paquete (Full Packet Inspection Capa 3, Capa 4 a Capa 7 del modelo OSI). b. Modulo o característica de Firewall c. Filtrado Web, basado de en reputación de categorías de contenido. d. Control de aplicaciones basado en firmas. e. Control de acceso basado en reputación de IP. f. Protección contra intrusos. g. Protección de antivirus. h. Protección contra ataques de denegación de servicio (capa 3 a capa 7). i. Detección o escaneo de amenazas o vulnerabilidades de día cero a través de un módulo o equipamiento de sandboxing local. Debe incluir un mínimo de 20 appliances o instancias o vm's para análisis. j. Control y priorización de tráfico basado en reglas de origen, destino y aplicación Capa 7 del modelo OSI. k. Throughput de 15 Gbps para Threat prevention o Threat Protection. l. Túneles de tipo VPN SSL 10,000 m. Túneles de tipo IPSEC 12,000 n. Funcionalidad de SDWAN o Policy Based Routing (PBR). o. Sesiones de firewall o conexiones concurrentes (TCP) 13 Millones como mínimo. f. Inspección de tráfico cifrado SSL.
Sistema de alimentación de energía	a. El voltaje de entrada del equipo debe admitir voltajes de 210v y 240v AC a una frecuencia de 60Hz. b. El equipamiento debe incluir fuentes de poder redundante, listas para ser usadas, sin costo adicional para la CGR.
Consideraciones Generales	El Contratista debe tener en cuenta y encargarse de las actividades: a. La implementación de la solución debe realizar en la modalidad de llave en mano. b. Acondicionamiento eléctrico para la instalación de la solución propuesta (cableado eléctrico, tomas eléctricas, llaves y tablero). c. Acondicionamiento eléctrico para la instalación de la solución propuesta (cableado eléctrico y tomas eléctricas). d. Se deben incluir todos los accesorios, conectores, cables, entre otros requeridos para el buen funcionamiento del equipo solicitado. e. El software deberá ser ofrecido en su versión más estable y/o más avanzada. f. El soporte para los equipos debe ser del contratista y fabricante tipo 24x7 por la duración del servicio contratado con soporte presencial y remoto.

CARACTERISTICAS	DESCRIPCION
	g. En ningún caso se podrá presentar equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricados, comercializados y/o soportados durante los 3 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante. h. Los firewalls deben estar con el máximo de capacidad soportado de memoria RAM. i. Deben realizar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea(n) bloqueado(s). j. Deben mostrar los países de origen y destino en los logs de acceso.

ANEXO N°02

Características Técnicas de los Dispositivos de Seguridad Perimetral (Sede Remotas: numeral 1 al 31)

CARACTERISTICAS	DESCRIPCION
Cantidad	Dos (02) equipos de seguridad perimetral (por cada Sede Remota).
Descripción	• La solución de seguridad perimetral se debe componer de dos equipos físicos o appliance. • La solución de seguridad perimetral debe estar en la categoría de Next Generation Firewall (NGFW). • La solución de seguridad perimetral debe ser de la misma marca y en su conjunto cumplan la totalidad de las especificaciones técnicas (Deben ser de la misma marca de los equipos del ANEXO 01).
Alta disponibilidad	La solución debe incluir las siguientes funcionalidades como mínimo: • activadas y licenciadas, disponibles para su uso, sin costo adicional para la CGR. • Debe incluir la funcionalidad de alta disponibilidad para todos los componentes de la solución, en las modalidades activo-activo y/o activo-pasivo y/o activo-standby.y/o cluster
Formato	Un 01 Rack Unit (RU) como mínimo e incluir el kit de montaje del mismo fabricante de la solución, para ser instalado en el gabinete de comunicaciones.
Conectividad	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Un (01) puerto USB. • Un (01) puerto de consola. • Seis (06) puertos Gigabit Ethernet RJ45. • Protocolo IPV4 e IP v6.
Gestión de la Solución	La solución debe incluir las características mencionadas a continuación como mínimo: activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Comunicación serial (COM) o Interface USB (console port) • SSH • Syslog. • SNMP v2c y v3. • sFlow y/o Netflow y/o IPFIX. • Se debe mostrar como mínimo gráficos del tráfico entrante y saliente en tiempo real, así como gráficos de tráfico por IP origen, IP destino y servicios/puertos. • Se debe incluir la búsqueda de eventos en logs correlacionados utilizando como mínimo filtros por top IP origen, top IP destino, top aplicación/servicio, top reglas/políticas. • Debe mostrar gráficos de eventos correlacionados como mínimo por hora, día y semana • Como mínimo debe mostrar eventos correlacionados por aplicaciones y amenazas. • Debe emitir reportes automatizados o a demanda y tener la capacidad de ser enviados por correo electrónico. • La solución de seguridad debe enviar la información de tráfico de red permitido y bloqueado, aplicaciones, log de eventos de usuario y del sistema hacia un repositorio de log independiente (este repositorio está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado). • Los firewalls deben ser administrados desde una consola de administración centralizada (esta consola está definida en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado).
Gestión de dispositivos y usuarios	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR:

CARACTERISTICAS	DESCRIPCION
	• Identificación y/o autenticación de dispositivos en base a su dirección física de red (MAC Address) o Portal cautivo que permita la autenticación de los usuarios al firewall. • Usuarios locales. • Integración de usuarios vía LDAP. • Autenticación basada en el modelo AAA (Authentication, Authorization and Accounting). • RADIUS.
Políticas de seguridad y priorización de trafico	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Análisis de inspección completo de paquete (Full Packet Inspection Capa 3, Capa 4 a Capa 7 del modelo OSI). • Modulo o característica de Firewall • Filtrado Web, basado de en reputación de categorías de contenido. • Control de aplicaciones basado en firmas. • Control de acceso basado en reputación de IP. • Protección contra intrusos. • Protección de antivirus. • Protección contra ataques de denegación de servicio (capa 3 a capa 7). • Detección o escaneo de amenazas o vulnerabilidades de día cero a través de un módulo o equipamiento de sandboxing (este módulo o equipamiento está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con dicho equipamiento solicitado). • Control y priorización de tráfico basado en reglas de origen, destino y aplicación Capa 7 del modelo OSI. • Throughput de 700 Mbps para Threat prevention o Threat Protection. • Túneles de tipo VPN SSL. • Túneles de tipo IPSEC. • Funcionalidad de SDWAN o Policy Based Routing (PBR). • Sesiones de firewall o conexiones concurrentes (TCP) 600 mil como mínimo. • Inspección de tráfico cifrado SSL.
Sistema de alimentación de energía	• El voltaje de entrada del equipo debe admitir voltajes de 210v y 240v AC a una frecuencia de 60Hz.
Consideraciones Generales	El Contratista debe tener en cuenta y encargarse de las actividades: • La implementación de la solución debe realizar en la modalidad de llave en mano. • Acondicionamiento eléctrico para la instalación de la solución propuesta (cableado eléctrico y tomas eléctricas). • Se deben incluir todos los accesorios, conectores, cables, entre otros requeridos para el buen funcionamiento del equipamiento de la solución. • El software deberá ser ofrecido en su versión más estable y/o más avanzada. • El soporte para los equipos debe ser del contratista y fabricante tipo 24x7 por la duración del servicio contratado con soporte presencial y remoto. • En ningún caso se podrá presentar equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricados, comercializados y/o soportados durante los 3 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante. • Deben realizar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea(n) bloqueado(s). • Deben mostrar los países de origen y destino en los logs de acceso.

ANEXO N° 03

Características Técnicas de los Dispositivos de Seguridad Perimetral

(Sede Remotas: Sede-Ancón)

CARACTERISTICAS	DESCRIPCION
Cantidad	Dos (02) equipos de seguridad perimetral (por cada Sede Remota).
Descripción	• La solución de seguridad perimetral se debe componer de dos equipos físicos o appliance. • La solución de seguridad perimetral debe estar en la categoría de Next Generation Firewall (NGFW). • La solución de seguridad perimetral debe ser de la misma marca y en su conjunto cumplan la totalidad de las especificaciones técnicas (Deben ser de la misma marca de los equipos del ANEXO 01).
Alta disponibilidad	La solución debe incluir las siguientes funcionalidades como mínimo: • activadas y licenciadas, disponibles para su uso, sin costo adicional para la CGR. • Debe incluir la funcionalidad de alta disponibilidad para todos los componentes de la solución, en las modalidades activo-activo y/o activo-pasivo y/o activo-standby.y/o cluster
Formato	Un 01 Rack Unit (RU) como mínimo e incluir el kit de montaje del mismo fabricante de la solución, para ser instalado en el gabinete de comunicaciones.
Conectividad	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Cuatro (04) interfaces de un (01) Gigabit Ethernet con conector RJ45. • Un (01) puerto Gigabit Ethernet RJ45 Management o Puerto de servicio. • Un (01) Puerto USB. • Un (01) Puerto de Consola. • Protocolo IPV4 e IP v6.
Gestión de la Solución	La solución debe incluir las características mencionadas a continuación como mínimo: activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Comunicación serial (COM) o Interface USB (console port) • SSH • Syslog. • SNMP v2c y v3. • sFlow y/o Netflow y/o IPFIX. • Se debe mostrar como mínimo gráficos del tráfico entrante y saliente en tiempo real, así como gráficos de tráfico por IP origen, IP destino y servicios/puertos. • Se debe incluir la búsqueda de eventos en logs correlacionados utilizando como mínimo filtros por top IP origen, top IP destino, top aplicación/servicio, top reglas/políticas. • Debe mostrar gráficos de eventos correlacionados como mínimo por hora, día y semana • Como mínimo debe mostrar eventos correlacionados por aplicaciones y amenazas. • Debe emitir reportes automatizados o a demanda y tener la capacidad de ser enviados por correo electrónico. • La solución de seguridad debe enviar la información de tráfico de red permitido y bloqueado, aplicaciones, log de eventos de usuario y del sistema hacia un repositorio de log independiente (este repositorio está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado). • Los firewalls deben ser administrados desde una consola de administración centralizada (esta consola está definida en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado).

CARACTERISTICAS	DESCRIPCION
Gestión de dispositivos y usuarios	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Identificación y/o autenticación de dispositivos en base a su dirección física de red (MAC Address) o Portal cautivo que permita la autenticación de los usuarios al firewall. • Usuarios locales. • Integración de usuarios vía LDAP. • Autenticación basada en el modelo AAA (Authentication, Authorization and Accounting). • RADIUS.
Políticas de seguridad y priorización de trafico	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Análisis de inspección completo de paquete (Full Packet Inspection Capa 3, Capa 4 a Capa 7 del modelo OSI). • Modulo o característica de Firewall • Filtrado Web, basado de en reputación de categorías de contenido. • Control de aplicaciones basado en firmas. • Control de acceso basado en reputación de IP. • Protección contra intrusos. • Protección de antivirus. • Protección contra ataques de denegación de servicio (capa 3 a capa 7). • Detección o escaneo de amenazas o vulnerabilidades de día cero a través de un módulo o equipamiento de sandboxing (este módulo o equipamiento está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con dicho equipamiento solicitado). • Control y priorización de tráfico basado en reglas de origen, destino y aplicación Capa 7 del modelo OSI. • Throughput de 1 Gbps para Threat prevention o Threat Protection. • Túneles de tipo VPN SSL. • Túneles de tipo IPSEC. • Funcionalidad de SDWAN o Policy Based Routing (PBR). • Sesiones de firewall o conexiones concurrentes (TCP) 1 millón como mínimo. • Inspección de tráfico cifrado SSL.
Sistema de alimentación de energía	• El voltaje de entrada del equipo debe admitir voltajes de 210v y 240v AC a una frecuencia de 60Hz.
Consideraciones Generales	El Contratista debe tener en cuenta y encargarse de las actividades: • La implementación de la solución debe realizar en la modalidad de llave en mano. • Acondicionamiento eléctrico para la instalación de la solución propuesta (cableado eléctrico y tomas eléctricas). • Se deben incluir todos los accesorios, conectores, cables, entre otros requeridos para el buen funcionamiento del equipamiento de la solución. • El software deberá ser ofrecido en su versión más estable y/o más avanzada. • El soporte para los equipos debe ser del contratista y fabricante tipo 24x7 por la duración del servicio contratado con soporte presencial y remoto. • En ningún caso se podrá presentar equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricados, comercializados y/o soportados durante los 3 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante. • Deben realizar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea(n) bloqueado(s). • Deben mostrar los países de origen y destino en los logs de acceso.

LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

ANEXO N° 04

Características Técnicas de los Dispositivos de Seguridad Perimetral

(Sede Remotas: Arequipa-N°1593, Sede-01, Sede-02 y Sede-03)

CARACTERISTICAS	DESCRIPCION
Cantidad	Dos (02) equipos de seguridad perimetral (por cada Sede Remota).
Descripción	• La solución de seguridad perimetral se debe componer de dos equipos físicos o appliance. • La solución de seguridad perimetral debe estar en la categoría de Next Generation Firewall (NGFW). • La solución de seguridad perimetral debe ser de la misma marca y en su conjunto cumplan la totalidad de las especificaciones técnicas (Deben ser de la misma marca de los equipos del ANEXO 01).
Alta disponibilidad	La solución debe incluir las siguientes funcionalidades como mínimo: • activadas y licenciadas, disponibles para su uso, sin costo adicional para la CGR. • Debe incluir la funcionalidad de alta disponibilidad para todos los componentes de la solución, en las modalidades activo-activo y/o activo-pasivo y/o activo-standby.y/o cluster
Formato	Un 01 Rack Unit (RU) como mínimo e incluir el kit de montaje del mismo fabricante de la solución, para ser instalado en el gabinete de comunicaciones.
Conectividad	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Tres (03) puertos de 10Gbps Ethernet, incluyendo su transceiver con conector del tipo LC (fibra óptica), para cada puerto. • Cuatro (04) interfaces de un (01) Gigabit Ethernet con conector RJ45. • Un (01) puerto Gigabit Ethernet RJ45 Management o Puerto de servicio. • Un (01) Puerto USB. • Un (01) Puerto de Consola. • Protocolo IPV4 e IP v6.
Gestión de la Solución	La solución debe incluir las características mencionadas a continuación como mínimo: activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Comunicación serial (COM) o Interface USB (console port) • SSH • Syslog. • SNMP v2c y v3. • sFlow y/o Netflow y/o IPFIX. • Se debe mostrar como mínimo gráficos del tráfico entrante y saliente en tiempo real, así como gráficos de tráfico por IP origen, IP destino y servicios/puertos. • Se debe incluir la búsqueda de eventos en logs correlacionados utilizando como mínimo filtros por top IP origen, top IP destino, top aplicación/servicio, top reglas/políticas. • Debe mostrar gráficos de eventos correlacionados como mínimo por hora, día y semana • Como mínimo debe mostrar eventos correlacionados por aplicaciones y amenazas. • Debe emitir reportes automatizados o a demanda y tener la capacidad de ser enviados por correo electrónico. • La solución de seguridad debe enviar la información de tráfico de red permitido y bloqueado, aplicaciones, log de eventos de usuario y del sistema hacia un repositorio de log independiente (este repositorio está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado). • Los firewalls deben ser administrados desde una consola de administración centralizada (esta consola está definida en el ANEXO N° 01, por lo que se debe permitir su integración completa con el equipamiento solicitado).

CARACTERISTICAS	DESCRIPCION
Gestión de dispositivos y usuarios	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Identificación y/o autenticación de dispositivos en base a su dirección física de red (MAC Address) o Portal cautivo que permita la autenticación de los usuarios al firewall. • Usuarios locales. • Integración de usuarios vía LDAP. • Autenticación basada en el modelo AAA (Authentication, Authorization and Accounting). • RADIUS.
Políticas de seguridad y priorización de trafico	La solución debe incluir las características mencionadas a continuación como mínimo, activadas, licenciadas y disponibles para su uso sin costo adicional para la CGR: • Análisis de inspección completo de paquete (Full Packet Inspection Capa 3, Capa 4 a Capa 7 del modelo OSI). • Modulo o característica de Firewall • Filtrado Web, basado de en reputación de categorías de contenido. • Control de aplicaciones basado en firmas. • Control de acceso basado en reputación de IP. • Protección contra intrusos. • Protección de antivirus. • Protección contra ataques de denegación de servicio (capa 3 a capa 7). • Detección o escaneo de amenazas o vulnerabilidades de día cero a través de un módulo o equipamiento de sandboxing (este módulo o equipamiento está definido en el ANEXO N° 01, por lo que se debe permitir su integración completa con dicho equipamiento solicitado). • Control y priorización de tráfico basado en reglas de origen, destino y aplicación Capa 7 del modelo OSI. • Throughput de 3 Gbps para Threat prevention o Threat Protection. • Túneles de tipo VPN SSL. • Túneles de tipo IPSEC. • Funcionalidad de SDWAN o Policy Based Routing (PBR). • Sesiones de firewall o conexiones concurrentes (TCP) 3 millones como mínimo. • Inspección de tráfico cifrado SSL.
Sistema de alimentación de energía	• El voltaje de entrada del equipo debe admitir voltajes de 210v y 240v AC a una frecuencia de 60Hz.
Consideraciones Generales	El Contratista debe tener en cuenta y encargarse de las actividades: • La implementación de la solución debe realizar en la modalidad de llave en mano. • Acondicionamiento eléctrico para la instalación de la solución propuesta (cableado eléctrico y tomas eléctricas). • Se deben incluir todos los accesorios, conectores, cables, entre otros requeridos para el buen funcionamiento del equipamiento de la solución. • El software deberá ser ofrecido en su versión más estable y/o más avanzada. • El soporte para los equipos debe ser del contratista y fabricante tipo 24x7 por la duración del servicio contratado con soporte presencial y remoto. • En ningún caso se podrá presentar equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricados, comercializados y/o soportados durante los 3 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante. • Deben realizar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea(n) bloqueado(s). • Deben mostrar los países de origen y destino en los logs de acceso.