TERMINOS DE REFERENCIA

SERVICIO DE INTERNET DEDICADO, INTERCONEXION y CONECTIVIDAD DE DATOS, SEGURIDAD GESTIONADA Y CENTRAL TELEFONICA FIJA

1. AREA USUARIA

Subgerencia de Tecnologías de la Información

2. FINALIDAD PÚBLICA

Las tecnologías de telecomunicaciones tales como internet dedicado, interconexión de datos, seguridad gestionada y central telefónica, son herramientas imprescindibles necesarios que coadyuvan al cumplimiento de los objetivos de las unidades orgánicas.

El procedimiento de selección busca contar con acceso dedicado a internet y transmisión de datos para atender los procesos internos de navegación a sitios externos.

3. OBJETIVOS DE LA CONTRATACIÓN

Proveer a la municipalidad distrital de San Luis el servicio de internet con línea dedicada y un ancho de 1000 Mbps, servicio de interconexión de datos simétrico 1:1 por medio de fibra óptica, servicio de seguridad gestionada para 500 usuarios y servicio de telefonía fija con central telefónica.

4. DESCRIPCION DEL SERVICIO

4.1. SERVICIO DE INTERNET DEDICADO

Local	Dirección	Ancho de Banda
Sede Principal	Av. del aire N.º 1540 - San Luis	Principal 1000 Mbps

a) El proveedor deberá proporcionar un enlace principal por medio de fibra óptica con un ancho de banda de 1,000 Mbps 1:1 cada uno configurados en alta disponibilidad activo/pasivo.
b) El proveedor deberá proporcionar, para la Sede Principal, un enlace de contingencia de 1,000 Mbps 1:1 mediante fibra óptica, el enlace de contingencia deberá ser de un recorrido y nodo distinto al del enlace principal.
c) El proveedor deberá contar con un backbone anillado 100% en fibra óptica, con tecnología MPLS, no se aceptarán propuestas donde el proveedor tenga tramos inalámbricos, deberá presentar un diagrama de su red.
d) Los nodos del backbone del proveedor deben estar implementados por fibra óptica.
e) La última milla debe ser 100% fibra óptica desde el punto de conexión del proveedor hasta la municipalidad distrital de San Luis.
f) La infraestructura de salida internacional hacia internet deberá ser de fibra óptica redundante, deberá contar con mínimo tres (03) operadores, así mismo deberá acreditarlo en la propuesta, mediante copia de carta y/o constancia y/o contratos suscritos con el proveedor de la salida internacional.
g) El proveedor del servicio deberá garantizar que el ancho de banda contratado para el enlace deberá ser de uso exclusivo para la entidad desde la puerta WAN del router en el local de la municipalidad distrital de San Luis hasta el router de borde del proveedor del servicio internet nacional.
h) El protocolo utilizado para el transporte de datos debe ser TCP/IP.
i) La capacidad de crecimiento del ancho de banda a futuro para el enlace como mínimo será de 75%.
j) El nivel de disponibilidad del servicio deberá ser de 99.9 %, medido mes a mes, durante el tiempo de duración del contrato.
k) Se deberá proveer16 direcciones IP públicas, 13 de las cuáles serán disponibles como minimo.
l) El proveedor del servicio debe tener autorización del ministerio de transportes y comunicaciones para servicio de valor añadido, con cobertura a nivel nacional.
m) El servicio proporcionado debe contar con una herramienta de gestión para monitoreo del ancho de banda vía web con acceso mediante un usuario y contraseña.

n) El proveedor deberá entregar un informe final con los detalles técnicos y de infraestructura de telecomunicaciones implementados en la Municipalidad distrital de San Luis.
o) El servicio de internet deberá ser brindado las veinticuatro (24) horas del día, los siete (07) días de la semana, durante el plazo contractual.
p) El proveedor del servicio debe acreditar ser miembro del NAP (Network Access Point) para garantizar el rápido intercambio de datos entre los proveedores locales de Internet para ello, el proveedor deberá acreditarlo en la propuesta mediante copia de la constancia de miembro activo de la asociación NAP.
q) Permitir el transporte de voz, datos y video sobre el Protocolo IP.
r) El servicio deberá estar disponible y operativo las 24 horas del día durante el tiempo de duración del contrato.
s) El proveedor deberá instalar todos los equipos, dispositivos y/o componentes necesarios para la puesta en funcionamiento del servicio sin que esto implique costo adicional para Municipalidad Distrital de San Luis.
t) El servicio deberá considerar la gestión y mantenimiento de los equipos de acceso a internet instalados por el contratista.
u) Soporte técnico 24x7x365 con un tiempo de respuesta de acuerdo a la gravedad de la avería estableciéndose como un máximo de 2 horas siempre y cuando la avería es grave, después de haberse generado la interrupción

4.2. SERVICIO DE INTERCONEXIÓN DE DATOS:

El proveedor implementara el servicio de interconexión de datos para interconectar el Palacio Municipal San Luis, dirección: Av. Del Aire N.º 1540 con:

- Biblioteca municipal con dirección calle capea Nº 180 urbanización villa jardín a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Archivo central con dirección avenida Mariscal Nieto N.º 200 urbanización el Pino a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Base seguridad Ciudadana con dirección Av. Nicolas Arriola S/N Altura del puente Echandía a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Piscina Municipal con dirección en cruce Av. Circunvalación S/N con Beingolea a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Cancha Deportiva con dirección en …….. a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Mercurio Bombero con dirección en …….. a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.
- Teatro Bernaola con dirección en …….. a través de una conexión de L2L de fibra óptica considerando el ancho de banda de 200 Mbps.

Las velocidades serán simétricas, con una contención en la calidad del servicio de 1:1 del ancho de banda en el tramo local, sin utilizar esquemas de acceso compartido o acceso del tipo asimétrico.
La última milla debe ser 100% fibra óptica desde el punto de conexión del palacio municipal hasta las sedes de Biblioteca municipal, Archivo Central, Base Serenazgo, Piscina Municipal, Cancha Deportiva, Mercurio Bombero y Teatro Bernaola.

4.3. SERVICIO DE CONECTIVIDAD DE CAMARAS DE VIDEOVIGILANCIA:

a) Se requiere servicio de transporte de datos para 55 camaras de videovigilancia de acuerdo al ***ANEXO 01 – Ubicación de puntos de video vigilancia.***
b) El ancho de banda por cada punto de video vigilancia sera de 15 Mbps.
c) La visualizacion de las camaras del enlace en su totalidad debe ser en la Central de Monitoreo de la Municipalidad Distrital de San Luis.
d) El servicio debe estar disponible y operativo las 24*7*365.
e) La red por instalar será independiente a la de la Municipalidad Distrital de San Luis.
f) La red de fibra óptica debe tener la capacidad para soportar datos, video y manejar QoS (control de tráfico y calidad de servicio).

g) La red de fibra óptica deberá permitir el transporte de voz sobre IP sin restricciones de filtrado.
h) La red de fibra óptica no deberá tener ningún tipo de compresión de datos para el correcto funcionamiento del servicio del sistema de CCTV.
i) El sistema estará constituido por hardware y software, que permita la transferencia de datos y/o aplicaciones aprovechando los recursos de la red actual de la municipalidad provincial del Callao.
j) La interconexión se realizará en su totalidad, debiéndose validar la conectividad de todo el sistema.
k) La red de fibra óptica debe tener continuidad, por lo que se entregará una conexión en forma de anillo al centro de monitoreo, desde su nodo más cercano, para evitar el corte de servicio por problemas en aún punto existente y perjudique a la entidad.
l) La instalación de estos enlaces debe estar basada en el uso de un medio seguro, con tiempos de respuesta óptimos.
m) En caso de pérdida de conexión por falla de equipos de media converter, el contratista tendrá que remplazar dicho equipo, en un plazo máximo de 01 día calendario, contados a partir de recibida la comunicación de parte de la subgerencia de serenazgo.
n) La red del contratista debe contar con un backbone íntegramente en fibra óptica; además la infraestructura de su red deberá estar interconectada en fibra óptica (nodos, pop´s).
o) La red de fibra óptica podrá ser aérea, canalizada o micro canalizada.
p) La supervisión del servicio de instalación estará a cargo del personal de la empresa, técnico y administrador de video vigilancia.

4.4. SERVICIO PARA POSTE INTELIGENTE EN UBICACIONES ESTRATEGICAS

a) Se requiere el servicio de cuatro (04) unidades de postes inteligentes que se ubicaran en puntos estratégicos en el distrito de San Luis y de acuerdo con el ***ANEXO 02 – Ubicación de Postes Inteligentes.***
b) El poste se implementará con una cámara de video vigilancia y un Access Point para acceso a WIFI con un ancho de banda de 20Mbps, se instalara sobre poste existente designado por la Entidad dentro del distrito.
c) La cámara de videovigilancia deberá contar con las siguientes características como mínimo:

- Sensor de Imagen: 1/2.8" CMOS
- Pixel : 2560(H)x1440(V)
- WDR : 120 Db
- BLC , HLC
- Velocidad de obturación : Auto/Manual, 1/1~1/30,000s
- Sistema de escaneo : Progresivo
- Distancia focal : 5mm – 125mm
- Máxima apertura: F 1.6 – F3.6
- Campo de visión: H: 51.9˚-3.0˚; V: 39.7-2.2˚; D: 63.1˚-3.7˚
- Rango de giro/inclinación/rotación: Panorámica: 0˚~360˚; Inclinación: -15˚~ +90˚; Rotación: 180˚
- Detección de rostro: Admite detección de rostros, cuadro delimitador de rostros, captura de instantáneas, carga de instantáneas de rostros, mejora de imágenes de rostros, extracción de atributos como género, edad, gafas, máscara, bigote y expresiones.
- Detección de movimiento
- Compresión de video: H.265; H.264M; H.264H; H.264B; MJPEG
- Compresión de audio: G.711a; G.711Mu; PCM; G.726; MPEG2; G723
- Rotación de imagen: 180˚
- Distancia de enforque cercano: 0.1m – 0.5m
- Alarma de eventos: Detección de movimiento/manipulación; detección de audio; detección de desconexión de red; detección de conflictos de IP; detección del estado de la tarjeta de memoria; detección de espacio de memoria.
- Suministro de energía: 12 VDC/3A ± 10% ; PoE+ (802.3at)
- Consumo de energía: Básico: 7 W; Max: 13 W
- IP66
- Audio entrada/salida 1/1 canal
- Alarma entrada/salida 2/1 canal
- Temperatura de operación: -40° C ~ +65° C

d) Con respecto a la gestión de grabación de las cámaras se requerirá que, sea de tipo remoto en servidores en la nube (cloud), de propiedad del proveedor. Este requerimiento tendrá un alcance para cuatro (04) cámaras durante 45 días de grabación.
e) El VMS del proveedor deberá contar con certificado de ciberseguridad que actúe como un sistema de detección de intrusos.
f) Deberá contar con las siguientes características como mínimo:

Para el soporte ONVIF PTZ

- El VMS deberá admitir el acceso PTZ por proxy para cámaras ONVIF.
- El VMS deberá habilitar automáticamente el proxy PTZ para cámaras que admitan el servicio ONVIF PTZ; no se requiere configuración de usuario en el VMS para esta función.
- Soporte de eventos ONVIF
- El VMS deberá admitir eventos de proxy generados por cámaras ONVIF.
- El VMS permitirá habilitar automáticamente el proxy de eventos para las cámaras que admitan el servicio de eventos ONVIF; no se requiere configuración de usuario en el VMS para esta función.
- El VMS deberá admitir el acceso de entrada digital por proxy para cámaras ONVIF.
- El cambio de la configuración de entrada digital debe realizarse a través de la interfaz web de la cámara.
- Compatibilidad con el administrador de ancho de banda de las plataformas existentes
- El VMS admitirá el uso de un administrador de ancho de banda para limitar el ancho de banda utilizado por las transmisiones entre las cámaras y el VMS.

Para la configuración de la grabación:

- Debe permitir iniciar una grabación instantánea de video tiempo real vista en un panel de video
- Debe tener la capacidad de iniciar solo grabación de video o de audio y video.
- Debe permitir poder configurar el programa de grabación de las cámaras mediante la creación de trabajos de grabación en NVR.
- La grabación debe ser las 24 horas, todos los días.
- En caso de alarma o evento: especificar el protocolo de transporte que se utilizará para la grabación (TCP, UDP, Multicast)
- Debe permitir especificar si el audio se grabará con el video.
- Debe permitir especificar si la grabación debe ser protegida cuando se produce una alarma o evento (de un tiempo determinado antes de la alarma/evento)
- Debe permitir activar o desactivar los trabajos de grabación temporalmente
- Debe permitir eliminar los trabajos de grabación
- Debe permitir copiar los trabajos de grabación de una cámara a otra cámara en el mismo NVR.
- Grabación y reproducción de manera simultánea y a máxima tasa de cuadros, transmisiones de video a máxima resolución desde cualquier codificador o cámara IP conectado.

4.4. SERVICIO DE SEGURIDAD GESTIONADA CON EQUIPO FISICO:

El postor deberá incluir como parte del servicio de Internet funcionalidades de seguridad a través de un equipo dedicado del tipo Next Generation Firewall de 1Ru y Fuentes Redundantes como parte del servicio, el SOC del postor deberá atender requerimientos para configurar políticas de seguridad en una cobertura 7x24 durante el periodo del contrato del servicio.

El fabricante debe estar en el último reporte del cuadrante de líderes de Gartner para Network Firewall.

La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.

Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

Administración compartida del Firewalls vía web que permita dar permisos de red.

El proveedor brindará una protección perimetral de acceso dedicado con funcionalidades como Firewall, Prevención de intrusos IPS, Antivirus de Gateway, Antispam, Filtros de contenido Web y conexiones teletrabajo VPN SSL, VPN IPSEC el cual será dos equipos appliance de seguridad de red configurados en alta disponibilidad con funcionalidades de Next Generation Firewall (NGFW) instalados en las instalaciones de la MDSL.

Capacidad:

- Throughput de Next Generation firewall mínimo de 3.0Gbps / IPS 5.0 Gbps / Threat Protection 2.8 Gbps/ Concurrent SSL-VPN 450 usuarios.
- La plataforma de hardware debe soportar un mínimo de sesiones simultaneas de 2500000 conexiones concurrentes. y 130 mil nuevas sesiones por segundo.
- Mínimo 10 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red de la entidad.
- Mínimo 02 interfaces de red 1G / 10G en formato SFP / SFP+ para el tráfico de datos de la red de la entidad.
- La plataforma deberá contar con al menos 02 interfaces adicionales 10/100/1000 dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad.

Características generales:

- Debe contener proxies de aplicación específicos que permitan controlar granularmente al menos los siguientes protocolos: FTP, H323, HTTP, HTTPS, POP3, DNS, SMTP, SIP -ALG.
- Los proxies específicos deben permitir proteger a los servidores contra ataques de día zero y adicionalmente ofrecer protecciones robustas como ocultamiento de cookies, limitar los comandos a ejecutar, etc.
- Debe contar con características de protección contra ataque DoS.
- El producto debe tener una herramienta que permita ver en tiempo real lo que está ocurriendo con el tráfico para de esta manera poder tomar una acción ante un problema..
- Las reglas del firewall deben analizar las conexiones que atraviesan el equipo, entre interfaces y VLANs.
- Soportar granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico origen y destino, Ips origen y destino, horarios, usuarios, grupos de LDAP, AD u Open LDAP, servicios o grupos de servicios.
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
- Capacidad para hacer NAT estático, Nat dinámico, PAT
- El modo de configuración del equipo debe ser tanto por una consola de administración propietaria como por Web Seguro (SSL).
- La consola de administración debe permitir generar un histórico de políticas para poder hacer rollback ante cualquier incidencia
- Funcionalidad DHCP: Como Servidor, Cliente y Relay.
- Soporte para ruteo estático y dinámico (BGP, OSPF, RIP V1, V2)
- El equipo debe ser capaz de detección de caídas en su enlace principal y automáticamente mover el tráfico a un segundo enlace, estos enlaces pueden estar en ACTIVO, ACTIVO+ PASIVO y puede soportar hasta 4 enlaces WAN. Debe además poder revisar el jitter, perdida de paquetes para en base a eso determinar cuál es el mejor enlace disponible en un momento determinado.
- El balanceo de enlaces (SDWAN) debe ser posible al menos de las siguientes formas: Failover / Round-Robin.
- El equipo debe permitir hacer backup de las políticas de seguridad y backup de las configuraciones completas del equipo,
- El equipo debe ser capaz de auto-ordenar las reglas creadas por el administrador, de tal manera que las más críticas o especificas tengan mayor prioridad que las más genéricas
- El equipo debe soportar integrarse con DNS dinámico.
- El Proxy SMTP debe ser capaz de iniciar sesiones TLS para correo seguro.
- El equipo debe permitir tener logs en tiempo real que indiquen al administrador que es lo que está ocurriendo en la red.
- Certificaciones Comon Criteria EAL4+.

VPN IPSEC.

- Soporta de certificados digitales para construcción de VPNs cliente a sitio (client-to-site)
- Soporte de VPNs con algoritmos de cifrado: AES 256-128 bits, DES, 3 DES.
- Uso de SHA-2 y IKE v1/v2.

- Posibilidad de crear VPNs entre gateways y clientes con IPSec. Esto es, VPNs IPSec site-to-site y VPNs Ipsec client-to-site.
- Debe ser posible configurar la VPN, para que solamente el usuario o la red que se conecte con una VPN especifica pueda ingresar a determinadas puertos, aplicaciones, y maquinas específicas de la Red LAN, protegida por el firewall.
- El mecanismo de autenticación para Clientes VPN debe ser por LDAP o por usuarios locales, pudiendo el administrador del firewall limitar el acceso a los usuarios a una sesión a la vez de ser necesario.

AUTENTICACION:
- Capacidad de integrarse con servidores de autenticación Radius, SAML.
- Capacidad de conectarse con directorios LDAP.
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto Single-Sign-ON.
- Es deseable también permitir la autenticación a solicitud (Prompt – http) y el redireccionamiento automático a una página web configurada por el administrador.
- El equipo debe ser capaz de detectar y limitar el número de logins de un usuario y denegar de acuerdo al umbral limite que requiera el administrador del firewall.

LIMITACION DE ANCHO DE BANDA
- Capacidad de asignar parámetros de administración de ancho de banda por interface del firewall.
- Capacidad de limitar el ancho de banda por aplicación.
- Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia.
- Las reglas de QoS deben aplicarse también por regla del firewall.

CARACTERISTICAS ANTIVIRUS PERIMETRAL.
- Debe ser capaz de analizar en tiempo real tráfico HTTP, FTP, SMTP, POP3 de conexiones por segundo por tipo de paquete (syn, icmp, udp).
- El antivirus en tiempo real debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- La configuración de Antivirus en tiempo real deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.
- El antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware pudiendo complementarse con otros motores para dichas tareas.
- Entre las acciones a tomar para el antivirus a nivel de smtp debe considerarse: Permitir / Denegar / Bloquear el Adjunto / Opcionalmente mandar a cuarentena (en este caso el software de cuarentena debe venir licenciado).
- Las actualizaciones se realizarán de manera automática tanto de motores como de definiciones de virus.
- El producto debe ser capaz de realizar un pre-filtro de la página web, antes de hacer la consulta con la base de datos, para detectar paginas perniciosas o que contengan contenido no apropiado y bloquearlas antes de hacer análisis antivirus.

CARACTERISTICAS ANTISPAM PERIMETRAL
- El filtro antispam debe permitir asignar un score de reputación a la IP del servidor de correo que envía, basado en el comportamiento del tráfico que este genera y un componente heurístico, de esta manera bloquear el correo no deseado.
- El filtro antispam debe permitir crear listas blancas y listas negras a partir de correos electrónicos o subredes de IP.
- El antispam debe detectar también SPAM, vía POP3
- Características de Filtrado de contenido Web.

- Configurable directamente desde la interfaz de administración del dispositivo appliance, con capacidad para permitir esta protección por política de control de acceso.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes por categorías) dependiendo de la IP, usuario o grupo de usuarios de donde inicie la conexión.
- Las reglas deben poder crearse por usuarios locales (dentro del firewall) o externos (AD, LDAP,etc).
- Capacidad de filtrado de Active X/ Java Applets, Java Scripts, SOAP, asi como de la ejecución de ciertos comandos a nivel de http (ejemplo, MOVE, TRACE, MERGE) asi como el bloqueo de ciertos parámetros de la cabecera Web (Cache-Control, Authorization, Mime, Referer, etc.)
- Debe actualizarse al menos diariamente.
- El equipo deberá ser capaz de desencriptar las sesiones SSL, para poder revisar el tipo de tráfico y reconocer si están tratando de hacer tunneling para ingresar a páginas no autorizadas (ejemplo: https://meebo.com, https://facebook.com ,etc.)

CARACTERISTICAS DE GEOLOCALIZACION:

- El producto debe ser capaz de agregar permisos o bloqueos dependiendo del país del que se conecten los usuarios para acceder a los servicios.
- Debe ser capaz de crear exclusiones por IP.
- La base de datos de Geolocalización debe ser actualizable automáticamente.

CARACTERISTICAS IPS:

- Las firmas de IPS serán usadas por sensores que podrán estar configuradas por tipo de atributos a proteger (por ejemplo, protocolo, aplicación, objetivo, etc
- El perfil de IPS se deberá poder aplicar sobre la política de firewall donde el origen y destino este sujeto a dicha política.
- El IPS deberá estar orientado para la protección de redes y estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.
- La interfaz de administración de IPS deberá ser perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio.
- El Detector de intrusos deberá de mitigar los efectos de los ataques de negación de servicios.
- El IPS deberá conversar con el firewall, y ante la detección de ataques de red consecutivos, el IPS deberá conversar con el firewall y crear listas negras de manera automática para impedir que estas IPs puedan establecer cualquier tipo de sesión con el firewall mediante un tiempo especificado por el administrador.
- Mecanismos de detección de ataques:
    - *Reconocimiento de firmas, análisis de protocolos*
    - *Detección de anomalías*
    - *Detección de ataques de RPC*
    - *Protección contra ataques de Windows o Netbios*
    - *Protección contra ataques SMTP, IMAP, POP*
    - *Protección contra ataques DNS*
    - *Protección contra Gusanos y Virus (en conjunto con el antivirus perimetral), Exploits, Backdoor, DoS, Bots*
- Métodos de notificación: Alarmas mostradas en la consola de administración del appliance y alertas vía correo electrónico.

CARACTERÍSTICAS DEL CONTROL DE APLICACIÓN:

- El dispositivo deberá detectar programas P2P y de mensajería instantánea soportando al menos: Yahoo Messenger, MSN Messenger, ICQ, AOL, Skype, AIM y BitTorrent, TorrentZ, eDonkey, Gnutella, Kazaa para P2P.
- El appliance de seguridad perimetral debe tener la capacidad de reconocer las aplicaciones por protocolo y por puertos para facilitar la inspección para prevenir acciones evasivas que utilizan puertos no estándar, port-hopping o tunneling.

- El equipo appliance de seguridad deberá permitir políticas de control más granulares, como por ejemplo permitir el Yahoo Messenger como mensajería instantánea pero que no pueda transferir archivos).
- Descubrimiento (independientemente de puertos y protocolos), control y bloqueo, visualización y reporting de aplicaciones:
- La solución debe permitir descubrir, controlar y bloquear aplicaciones como:
    - *Business*
    - *Database*
    - *Games*
    - *Mail and collaboration*
    - *Network Protocols*
    - *File Transfer*
    - *Instant Messaging*
    - *Mobile*
    - *Bypass proxies and Tunnels*
    - *Web IM*

MANEJO DE LOGS, SERVICIO DE REPORTES:

- El postor deberá brindar un servicio de manejo de logs, centralizados para las funciones de: análisis de bitácoras de seguridad, reportes gráficos, almacenamiento de contenido, análisis de red.
- El postor debe contar con un Security Operation center instalado con personal calificado para las labores de gestión y soporte técnico de la solución planteada.
- El sistema de almacenamiento de LOGS del postor debe permitir guardar toda la data generada por el plazo de duración del contrato, pudiendo el cliente pedir reportes de hechos o eventos con antigüedad de hasta 12 meses.
- El sistema de almacenamiento de logs debe ser en forma automática y estar disponible 7 x 24
- Los reportes deben ser completamente personalizables a solicitud de la institución.
- El contenido de los reportes debe incluir los datos en forma tabular (tablas) y/o graficas (pie-chart, graph-chart).
- Debe poder generar reportes de: Utilización de la red (ancho de banda, aplicaciones, conexiones), usuarios, grupos de usuarios, direcciones IP y/o servicios de mayor consumo de recursos, reglas del firewall que más se han usado o reglas del firewall que permitieron el acceso a Internet a determinado tipo de aplicación o servicio, y hacía que países se conectaron o que países se conectaron a los servicios protegidos por el firewall.
- Debe poder generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red por fuente y/o destino.
- Debe poder generar reporte s de las páginas y o categorías de URLs visitadas con mayor frecuencia, por fuente y/o destino. Debe mostrar no solamente las direcciones IP remotas, sino también las URLs a las cuales los usuarios se conectaron.
- El sistema de reportes debe mostrar los servicios más usados, los usuarios que más tiempo emplean navegando, las páginas web empleadas por los usuarios, las páginas web y los usuarios más filtrados, las categorías más filtradas, el tiempo de navegación por usuario.
- El uso del FTP y de correo, el uso de las VPNS
- Los virus y los spyware más encontrados. Además, los eventos de IPS más encontrados.
- Debe poder generar un reporte de las actividades administrativas realizadas.
- Debe permitir personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.
- Los reportes deben indicar también que:
    - Debe permitir el envío automático (programado) de reportes.
    - Debe permitir generar reportes en formato HTML y PDF.
    - Debe poder enviar el reporte vía correo electrónico.

CAPACITACION:

- Capacitación teórica sobre el equipo de Seguridad instalado y configurado a fin de que el personal de la Subgerencia de Desarrollo de Tecnologías de la Información y Estadística será el primer punto de respuestas de soporte.

4.4. SERVICIO DE CENTRAL TELEFÓNICA ON PREMISE:

a) Provisión y configuración de una central telefónica Fisica en Palacio Municipal.
b) La central telefónica deberá soportar hasta 300 anexos.
c) La central telefónica será configurada con 30 canales IP para llamadas entrantes y salientes.
d) El proveedor deberá configurar los equipos de comunicación para que los teléfonos estén correctamente operativos.
e) Las conexiones a la red de datos, equipos, adaptadores y cualquier otro material o accesorio requeridos para la instalación inicial serán por cuenta del proveedor, quien antes de la instalación del servicio deberá verificar todo lo que considere necesario para incluir en su propuesta. Cualquier omisión implicará que dicho costo sea asumido por el proveedor. Los permisos y demás requerimientos administrativos y técnicos ante las autoridades competentes quedaran a cargo del proveedor.
f) La operatividad y continuidad (disponibilidad del servicio) no podrá ser menor de 99.9% en un período de 30 días calendario durante las 24 horas del día.
g) El proveedor deberá incluir dentro de su propuesta una central telefonica.
h) El proveedor deberá brindar un usuario a la consola de administración de la central, con los permisos para administrar las políticas, creación de usuarios, restricción de números, etc., así como generar reportes desde la misma central.
i) El proveedor se encargará de portar los números de la entidad.
j) Proporcionar una bolsa de minutos mensuales de acuerdo con el siguiente detalle:

Destino	Minutos mensuales
Fijo Local	12,000
Movil	15,000

k) Las características mínimas de la central telefónica IP son:
   - ✓ 1 Tera de capacidad de almacenamiento para grabación en llamadas.
   - ✓ Múltiples medios de conexión:
     - ❖ Teléfono IP de escritorio.
   - ✓ Presencia en múltiples dispositivos con la misma extensión:
     - ❖ Softphone en pc de escritorio..
   - ✓ Reportes históricos y en tiempo real de llamadas.
   - ✓ Lista negra para números de teléfonos.
   - ✓ Lista negra para direcciones IP sospechosas.
   - ✓ Ring GROUP (ring all, priority hunt).
   - ✓ Los DIDS pueden ser enrutados directamente a una extensión, IVR y grupos de timbrado.
   - ✓ Llamada en espera
   - ✓ Call parking.
   - ✓ Call pickup.
   - ✓ Followme.
   - ✓ Música de espera.
   - ✓ Mínimo 3000 minutos de grabaciones de voicemail.
   - ✓ Voicemail to email.
   - ✓ Paging (uso exclusivo en dispositivos IP físicos).
   - ✓ Conferencia de voz.

l) Módulo de Call Center:
   El módulo de call center debe estar diseñado soportar mínimo las siguientes características y/o funcionalidades:

- ✓ Colas de llamadas.
- ✓ Estrategias de enrutamiento:
  - ❖ Timbrar a todos.
  - ❖ Búsqueda priorizada.
  - ❖ Iniciar búsqueda aleatoria.
  - ❖ Round robin.
  - ❖ Espera más larga.
  - ❖ Menor tiempo de conversación.
  - ❖ Menor cantidad de respuestas.
  - ❖ Timbrar aleatorio de a tres.
  - ❖ Timbrar de a tres en orden.
- ✓ Devolución de llamadas.
- ✓ Anuncio al llamante de su posición en la cola
- ✓ Transferencia de llamadas
- ✓ Transferencia supervisada
- ✓ Tiempo de finalización
- ✓ Reportes predefinidos
  - ❖ Gráfico de tiempo promedio de espera en la cola.
  - ❖ Gráfico de llamadas contestadas en la cola.
  - ❖ Gráfico de llamadas no contestadas en la cola.
  - ❖ Estadísticas detalladas en la cola.
  - ❖ Llamadas abandonadas en la cola.
  - ❖ Estadísticas de los agentes en cola.
  - ❖ Historial de inicio de sesión del agente.
- ✓ Envió de reportes predefinidos a correo electrónico
- ✓ Grabación de llamadas, 15gb como mínimo.
- ✓ Perfiles de usuarios call center
  - ❖ **Perfil supervisor**:
    - Modo intervención de llamada, modo interacción con agente y modo escucha.
    - Recepción de notificaciones de las colas por correo electrónico (opcional):
      - Notifique al supervisor de las colas por correo electrónico cuando se incumpla el tiempo de SLA.
      - Notifique al supervisor de las colas cuando se realice una devolución de llamada.
      - Notifique al supervisor de las colas cuando falle una devolución de llamada.
      - Notifique al supervisor de las colas cuando se pierda una llamada en cola.
    - Panel de monitoreo general:
      - Llamadas en espera.
      - Llamadas atendidas.
      - Llamadas abandonadas.
      - Llamadas totales.
      - Llamadas devueltas.
      - Tiempo de espera.
      - Agentes ocupados.
  - ❖ **Perfil agente:**
    - Logueo y deslogueo de colas independientes.
    - Transferir llamadas.
    - Acceso a sus propias grabaciones.

l) Soporte técnico: La central telefónica debe contar con soporte técnico sobre cualquier incidencia por un periodo contractual, dicho soporte puede ser remoto o presencial según la gravedad del problema.

m) El contratista deberá proporcionar 30 teléfonos IP sin que esto implique costo adicional para Municipalidad Distrital de San Luis, con las siguientes características mínimas:
  - ❖ 02 cuentas SIP (02 líneas)

- ❖ Pantalla LCD 128x48 píxeles + Retroiluminación
- ❖ 02 Puertos Ethernet 10/100Mbps
- ❖ 01 Puerto Auricular RJ9
- ❖ Fondo de pantalla retroiluminado
- ❖ Soporte de cliente VPN
- ❖ Conferencia de tres partes
- ❖ Soporta PoE e incluye fuente externa +5VDC

4.5. SERVICIO DE COPIA DE SEGURIDAD EN LA NUBE

El contratista deberá incluir un servicio de copia de seguridad en nube con una capacidad mínima de tres (03) Terabytes hasta para 10 servidores. El servicio brindado deberá tener las siguientes características:

a) Deberá permitir copia de seguridad desde servidores basados en sistema operativos Windows o Linux.
b) Deberá garantizar la seguridad del respaldo de los datos frente a malware.
c) Deberá brindar una protección antiransomware con certificación mediante blockchain.
d) Deberá permitir copia de seguridad de archivos y de imagen de disco.
e) Deberá proporcionar almacenamiento altamente disponible, seguro, duradero, escalable y redundante
f) Deben cifrar los datos en tránsito y en reposo
g) Deberá permitir copia de seguridad desde sistemas VMware y desde máquinas virtuales.
h) Deberá ser miembro del Cloud Security Alliance (CSA), miembro de la Antimalware Testing Standard Organization, miembro del APWG (Anti-Phishing Working Group) y miembro de la Biblioteca Criptográfica certificada por FIPS 140-2.
i) Deberá tener la Certificación ISO 27001:2013.
j) Debe tener la herramienta de gestión de Backup para hacer la programación de Backup, encriptación de datos, compresión de datos, programa de retención de datos, almacenamiento seguro en línea, control de versiones de datos, copia de seguridad diferencial, capacidad de restaurar en una fecha en particular, la verificación de copia de seguridad y recursos compartidos de red de copia de seguridad, entre otros.
k) Deberá permitir ingresos incrementales rápidamente ya sea en entornos físicos o virtuales, in situ o en la nube.
l) Deberá brindar el análisis de malware integrado permitiendo una copia de seguridad limpia sin malware durante la restauración.
m) Deberá almacenar los datos en un formato de copia de seguridad unificado que permita recuperar en cualquier plataforma, independientemente del sistema de origen.
n) Deberá permitir restaurar los sistemas Windows o Linux en hardware diferente, incluidos equipos físicos sin sistema operativo, y entornos virtuales o en la nube.
o) Deberá poder restaurar hacia VMWare
p) Restauración a nivel de archivo desde un Backup basado en una imagen
q) Deberá permitir la captura exclusiva de los bloques que contienen datos que han cambiado desde la copia de seguridad anterior.
r) Debe incluir la restauración de la capacidad total del respaldo en nube por lo menos en 4 oportunidades como mínimo durante el período del contrato sin incurrir en costo adicional
s) Debe incluir una herramienta para estadísticas de uso del servicio, reportes e indicadores
t) Soporte presencial, vía teléfono, correo electrónico, Teams o cualquier otra herramienta de soporte remoto, en modalidad 24x7
u) El tiempo de respuesta para la atención de averías debe ser como máximo de dos (02) horas, luego de registrada la avería.
v) El tiempo de resolución de averías debe ser como máximo de doce (12) horas, luego de registrada la avería. Para los casos especiales en los que el tiempo de resolución se estime mayor a 12 horas, sea o no responsabilidad del proveedor; la institución establecerá también un procedimiento especial para atender estos casos.

4.6. SERVICIO DE SERVIDOR HOSTING WEB Y BASE DE DATOS EN NUBE

La solución debe de ser implementada en la nube (Cloud Hosting). Se requiere dos (02) máquinas virtuales con las siguientes características:

a) Deberá incluir un servicio de Storage Service: 480 MB por cada uno de los dos servidores
b) Deberá incluir licenciamiento Linux.
c) Deberá incluir base de datos que soporte MYSQL.
d) Deberá incluir un procesador Intel XEON E-2386G 12 CORE
e) Deberá incluir CPU virtual: 2
f) Deberá incluir memoria RAM de 8 GB
g) Deberá incluir subida y descarga de datos ilimitada.
h) Deberá incluir 20 Mbps de trafico de internet al mes.
i) El proveedor deberá proveer un portal web para la gestión del servidor privado virtual contratado y para la gestión de tickets de soporte.
j) La entidad será la responsable de la migración del servidor.

4.7. SERVICIO DE TRASLADO DE DATA CENTER

El contratista deberá incluir en su propuesta, el servicio de traslado del Data Center principal a otro ambiente dentro del mismo local. El trasladó será en el palacio municipal de la Municipalidad Distrital de San Luis, el movimiento será del piso 02 al piso 01, para estos trabajos se debe considerar como mínimo lo siguiente:

- Traslado de equipos (equipos de comunicación y Gabinetes)
- Peinado y ordenamiento del cableado.
- Si es necesario realizar cableado para conectar los equipos en el nuevo ambiente debe realizarse.
- El cableado de red deberá ser categoría 6A y se deberá colocar swicht nuevos administrables que soporten la conexión de fibra óptica.
- El cableado entre swicht deberá ser con fibra óptica

4.8. SERVICIO DE ATENCION DE AVERIAS

Las averías se clasificarán en grupos esenciales las cuales deben ser resueltas en un tiempo máximo de atención según lo señalado indicado en los presentes Términos de Referencia; Para una adecuada identificación, se detalla que los tipos averías son:

a. Averías ocasionadas por terceros: La evaluación de la avería será evaluada conjuntamente entre la municipalidad y el proveedor de servicio la municipalidad se comunicará al contratista vía correo electrónico y/o teléfono de la empresa, dándose un plazo prudencial para su subsanación, en función a la complejidad del servicio.

El plazo de respuesta del correo comunicando la avería al contratista no será mayor a dos (02) días calendarios a partir del siguiente día de la recepción del correo.

En el caso de rotura de fibra óptica el plazo para resolver la avería no será mayor de dos (02) días calendarios contados desde el día siguiente a la notificación; con la salvedad
de que se requiera un mantenimiento mayor para lo cual el contratista deberá solicitar la ampliación correspondiente, debidamente sustentada.

b. Averías ocasionadas por situaciones propias del servicio. En caso de presentarse desperfectos en la comunicación de fibra óptica parciales o totales, durante la prestación del servicio, se procederá:

- Comunicar al contratista vía correo electrónico y/o teléfono de la empresa, dándose un plazo prudencial para su subsanación, en función a la complejidad del servicio.
- El plazo de respuesta del correo comunicando la avería al contratista no será mayor a 01 día calendario a partir del siguiente día de la recepción del correo.
- El plazo para resolver la avería no será mayor de dos (02) días calendarios contados
desde el día siguiente a la notificación; con la salvedad de que se requiera un mantenimiento mayor para lo cual el contratista deberá solicitar la ampliación correspondiente, debidamente sustentada.

En caso de presentarse desperfectos en los equipos, durante la prestación del servicio, se procederá:
- Comunicar al contratista vía correo electrónico y/o teléfono de la empresa, dándose un plazo prudencial para su subsanación, en función a la complejidad del servicio.
- El plazo de respuesta del correo comunicando la avería al proveedor de servicio no será mayor a 01 calendarios a partir del día de la recepción del correo.
- El plazo máximo de solución no deberá mayor a los 2 días calendarios a partir del siguiente día de la recepción del correo; con la salvedad de que se requiera un mantenimiento mayor para lo cual el contratista deberá solicitar la ampliación correspondiente, debidamente sustentada.

5. LUGAR, PLAZO E IMPLEMENTACION DE ENTREGA DEL SERVICIO

- ✓ **LUGAR:** La prestación del Servicio se llevará a cabo en las ubicaciones descritas en el numeral 4. DESCRIPCION DEL SERVICIO y ANEXO 01 descritos en los presentes Términos de Referencia.

- ✓ **PLAZO:** La ejecución del servicio se realizará en el plazo de ejecución de 36 meses (1080) días calendarios, computados a partir del día siguiente de suscrita el acta de Instalación del servicio.

- ✓ **IMPLEMENTACION:** El tiempo de implementación será de 30 días calendario.

6. CONFORMIDAD

La conformidad del servicio será otorgada por la Oficina de Tecnologías de la Información, la cual será de forma mensual por los (36) treinta y seis meses de contrato.
La ejecución del servicio será a partir del día siguiente de la instalación del servicio para la cual se suscribirá el acta de instalación e inicio del servicio.

7. FORMA Y CONDICIONES DE PAGO

La forma de pago será de manera mensual, previa presentación del comprobante de pago y de la emisión de la conformidad por la prestación del servicio.

8. CONFIDENCIALIDAD

El proveedor se compromete a mantener reserva y no revelar a terceros la información que le sea suministrada para el cumplimiento el presente servicio. El proveedor es responsable de la custodia de la información que se le entreguen para el cumplimiento de su prestación. Los documentos elaborados como consecuencia de la prestación del presente servicio serán de propiedad exclusiva de la entidad, quien es la única autorizada para permitir su difusión, reproducción o reserva

9. PENALIDADES

Las establecidas por el reglamento de la Ley de Contrataciones del Estado.

10. REQUISITOS DE CALIFICACION

A.	**CAPACIDAD LEGAL**
A.1.	**HABILITACIÓN DEL POSTOR**
	Requisitos: o *El postor deberá contar con registro de servicio de valor añadido, para la prestación del servicio de conmutación de datos por paquetes, emitido por el Ministerio de Transportes y Comunicaciones, con cobertura a nivel nacional.* o *El postor deberá contar con concesión para servicios públicos de telecomunicaciones.* o *El postor debera contar como minimo con (03) tres salidas internacionales a traves de distintos proveedores.* o *El postor deberá ser miembro activo del NAP Perú.*

	○ *El postor deberá cumplir con los requisitos minimos de la ISO 27001 para su sistema de gestion de la seguridad de la informacion, para al menos los servicios de: Internet y/o ciberseguridad y/o seguridad electrónica y/o conectividad por fibra optica.* *<u>Acreditación:</u>* ○ *Certificado de registro para servicio de valor añadido, para la prestación del servicio de conmutación de datos por paquetes, emitido por el ministerio de transportes y comunicaciones con cobertura a nivel nacional.* ○ *Resolución ministerial otorgando concesión para brindar servicios públicos de telecomunicaciones a nivel nacional, emitido por el Ministerio de Transportes y Comunicaciones con cobertura a nivel nacional.* ○ *Contratos y/o constancias y/o certificados emitidos y/o suscritos con los proveedores de las salidas internacionales.* ○ *Constancia y/o certificado de membresía de la Asociación NAP Perú, emitido por el NAP Peru.*

B	**CAPACIDAD TECNICA Y PROFESIONAL**
	B.1. FORMACION ACADEMICA
	Requisitos: **(*01) Gerente de proyectos de telecomunicaciones*** ○ Título profesional en Ingeniería de telecomunicaciones y/o electrónico. ***(01) Especialista de seguridad para servicios ciberneticos*** ○ Título profesional en Ingeniería de *sistemas* y/o *informática*. . **(*01) Ingeniero de implementacion de planta externa*** ○ Título profesional en Ingeniería de telecomunicaciones y/o civil. ○ Profesional debe ser colegiado y habilitado ***(01) Ingeniero de soporte y mantenimiento de servicio*** ○ *Título profesional en Ingeniería de sistemas y/o informática* *Acreditación:* *El TÍTULO PROFESIONAL 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 TÍTULO PROFESIONAL REQUERIDO 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
	<u>Requisitos:</u> ***(01) Gerente de proyectos de telecomunicaciones*** *Tres (03) años de experiencia en gestión y/o direccion de proyectos de redes de telecomunicaciones para servicios de conectividad y/o internet dedicado y/o seguridad gestionada.* ***(01) Especialista de seguridad para servicios ciberneticos*** *Tres (03) años de experiencia en implementacion y/o consultoria y/o diseño de servicios de seguridad gestionada y/o ciberseguridad.* ***(01) Ingeniero de implementacion de planta externa*** *Tres (03) años de experiencia en implementación de infraestructura y/o planta externa para servicios de telecomunicaciones.*

	(01) Ingeniero de soporte y mantenimiento de servicio *Tres (03) años de experiencia en soporte y/o mantenimiento y/o supervision de seguridad gestionada y redes de fibra optica.*
	B.3. CAPACITACIÓN DEL PERSONAL CLAVE
	Requisitos: ***(01) Gerente de proyectos de telecomunicaciones*** o Certificado y/o constancia de curso de project management for professionals (PMP), de mínimo 20 horas o Certificado y/o constancia de capacitación del VMS de la solución propuesta, emitido por el fabricante, de mínimo 10 horas o Certificación ISO/IEC 27001:2017 certified lead implementer o Certificación ITIL Foundation in IT Service management o Certificación Scrum Foundation Professional ***(01) Especialista de seguridad para servicios ciberneticos*** o Certificado y/o constancia de curso de project management for professionals (PMP), de mínimo 20 horas o Certificado y/o diploma de diplomado en gestión estratégica de la información, de mínimo 70 horas ***(01) Ingeniero de implementacion de planta externa*** o Certificado y/o constancia de capacitacion y/o curso de operación y/o mantenimiento del equipo de medición de fibra optica emitido por un distribuidor oficial del equipamiento, de minimo 15 horas. o Certificado y/o constancia de curso project management for professionals (PMP), de mínimo 20 horas o Certificado y/o constancia de capacitación de cámaras IP PTZ u otros temas relacionados a videovigilancia, emitido por un fabricante de videovigilancia, de mínimo 10 horas ***(01) Ingeniero de soporte y mantenimiento de servicio*** o Certificado y/o constancia de capacitacion y/o curso de operación y/o mantenimiento del equipo de medición de fibra optica emitido por un distribuidor oficial del equipamiento, de minimo 15 horas. o Certificado y/o constancia de curso y/o capacitacion de redes y fusiones de fibra optica, de minimo 34 horas, de mínimo 20 horas o Certificado y/o constancia de capacitación del VMS de la solución propuesta, emitido por el fabricante, de mínimo 20 horas

C.	EXPERIENCIA DEL POSTOR
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a **TRES VECES EL VALOR ESTIMADO** 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: **Servicio de internet dedicado y/o acceso a internet dedicado *para entidades del estado.***

	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[1], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad **Importante**

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"
(…)
"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

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

ANEXO 01 – Ubicación de puntos de video vigilancia

No. Conexión	Cámara de Video Vigilancia	Ubicacion	Ancho de Banda
Cámara N.º 01	PARQUE PERIODISTA	JR. RAUL VILLARAN / PSJ. LA VIÑA	15 Mbps
Cámara Nº 02	PARQUE PATIÑO	JR. HORACIO PATIÑO / CALLE GALVEZ SILVERA	15 Mbps
Cámara Nº 03	PARQUE SAN CARLOS DEL PINAR	JR. VIRGEN DE FATIMA / JR. SAN CARLOS DEL PINAR	15 Mbps
Cámara Nº 04	PARQUE ÁLAMO	JR. LOS ROSALES / JR. LA MADRILEÑA	15 Mbps
Cámara Nº 05	PARQUE MIGUEL GRAU	PSJE. ANTONIO UGARTE / PSJE. CAYRA	15 Mbps
Cámara Nº 06	ALMUDENA	JR. ALMUDENA / JR. LA TRINIDAD	15 Mbps
Cámara Nº 07	MANUEL BEINGOLEA	JR. MANUEL BEINGOLEA / JR. AUGUSTO DURAND	15 Mbps
Cámara Nº 08	BOULEVARD DE YERBATEROS	AV. 28 DE DICIEMBRE / JR. OLLANTA	15 Mbps
Cámara Nº 09	26 DE JULIO	AV. 26 DE JULIO / JR. JORGE CHAVEZ	15 Mbps
Cámara Nº 10	LORENZO ASTRANA	AV. CIRCUNVALACION / JR. LORENZO AZTRANA	15 Mbps
Cámara Nº 11	OVALO DE ARRIOLA	AV. SAN JUAN / AV. AVIACION	15 Mbps
Cámara Nº 12	POMACANCHI	JR. POMACANCHI / AV. SAN JUAN	15 Mbps
Cámara Nº 13	CACHITA EMADI	JR. POMACANCHI / JR. CAYRA	15 Mbps
Cámara Nº 14	PLAZOLETA SAN JUAN MACÍAS	JR. SURIMANA / JR. MARCELA CASTRO	15 Mbps
Cámara Nº 15	TOMAS CATARÍ	AV. SAN JUAN / JR. TOMAS CATARÍ	15 Mbps
Cámara Nº 16	RIO CHINCHA	AV. SAN JUAN / JR. RIO CHINCHA	15 Mbps
Cámara Nº 17	RIO PIURA	AV. SAN JUAN / JR. RIO PIURA	15 Mbps
Cámara Nº 18	RIO AMAZONAS	R. RIO PIURA / JR. RIO AMAZONAS	15 Mbps
Cámara Nº 19	AVENIDA SAN LUIS	AV. SAN JUAN / AV. SAN LUIS	15 Mbps
Cámara Nº 20	NICOLÁS ARRIOLA	AV. NICOLÁS ARRIOLA / AV. DE LA ROSA TORO	15 Mbps

Cámara Nº 21	AVENIDA CIRCUNVALACIÓN	AV. DEL AIRE / AV. CIRCUNVALACIÓN	15 Mbps
Cámara Nº 22	AVENIDA DE LA ROSA TORO	AV. DEL AIRE / AV. DE LA ROSA TORO	15 Mbps
Cámara Nº 23	AV. DEL AIRE / AV. SAN LUIS	AV. DEL AIRE / AV. SAN LUIS	15 Mbps
Cámara Nº 24	AV. DEL AIRE / JR. RIO PIURA	AV. DEL AIRE / JR. RIO PIURA	15 Mbps
Cámara Nº 25	DIEGO CRISTÓBAL	AV. DEL AIRE / JR. DIEGO CRISTÓBAL	15 Mbps
Cámara Nº 26	AV. DEL AIRE	AV. DEL AIRE / AV. AVIACIÓN	15 Mbps
Cámara Nº 27	LIMATAMBO	AV. AVIACIÓN / JR. LIMATAMBO NORTE	15 Mbps
Cámara Nº 28	GERONA	AV. SAN LUIS / JR. GERONA	15 Mbps
Cámara Nº 29	CELENDÍN	JR. SAN MIGUEL / JR. CELENDÍN	15 Mbps
Cámara Nº 30	AVENIDA CIRCUNVALACIÓN	AV. CIRCUNVALACIÓN / AV. CANADÁ	15 Mbps
Cámara Nº 31	JR. LOS JAZMINES / FRENTE AL PARQUE LOS NOVIOS	PARQUE LOS NOVIOS	15 Mbps
Cámara Nº 32	BASE SERENAZGO	AV. NICOLAS ARRIOLA CUADRA 27	15 Mbps
Cámara Nº 33	CALLE PUERTO BERMUDEZ / FRENTE PQ. JOSE CARLOS MAREATEGUI	PARQUE LINCOLN	15 Mbps
Cámara Nº 34	MARCONA	AV. NICOLÁS AYLLÓN – JR. MARCONA	15 Mbps
Cámara Nº 35	AV. DE LA ROSA TORO	AV. SAN JUAN – AV. DE LA ROSA TORO	15 Mbps
Cámara Nº 36	GRUTA EDIFICIOS EMADI	PJE. KIKIJANA CDRA./ PJE. CAYRA	15 Mbps
Cámara Nº 37	ELOY URETA	AV. ELOY URETA – AV. AGUSTÍN GAMARRA	15 Mbps
Cámara Nº 38	AVENIDA CANADÁ	AV. CANADÁ – AV. DE LA ROSA TORO	15 Mbps
Cámara Nº 39	LÉRIDA	JR. LÉRIDA – JR. ALICANTE	15 Mbps
Cámara Nº 40	TORRE	AV. DEL AIRE 1540 (PALACION MUNICIPAL)	15 Mbps
Cámara Nº 41	JR. FRANCISCO VIDAL DE LAOS / PSJE, ALARCON	PARQUE DE LA DIGNIDAD	15 Mbps
Cámara Nº 42	JR. RIO ICA / FRENTE AL PARQUE SAN LUIS	PARQUE SAN LUIS	15 Mbps
Cámara Nº 43	LEÓNIDAS LA SERRÉ	AV. MANUEL ECHANDÍA – JR. LEÓNIDAS LA SERRÉ	15 Mbps
Cámara Nº 44	SANCHEZ CERRO	AV. SANCHEZ CERRO / AV. 06 DE DICIEMBRE	15 Mbps
Cámara Nº 45	JR. LA MADRILEÑA / JR. ALMUDENA	PARQUE QUIÑONES	15 Mbps
Cámara Nº 46	JR. ALGECIRAS / JR. MURCI	PARQUE MEDALLA MILAGROSA	15 Mbps
Cámara Nº 47	ESTACIONAMIENTO LA LIBERTAD	AV. AVIACIÓN CDRA. N° 17	15 Mbps
Cámara Nº 48	ESTACIONAMIENTO LA FORTALEZA	AV. AVIACIÓN CDRA. N° 16	15 Mbps
Cámara Nº 49	PJE. LA CULTURA	PSJE. LA CULTURA / AVIACION Nº16	15 Mbps
Cámara Nº 50	PARQUE CÁCERES	CALLE JOSE GABRIEL AGUILAR / CALLE ANTONIO BASTIDAS	15 Mbps
Cámara Nº 51	AV. NICOLÁS. ARRIOLA CDRA. N°14 / INGRESO A ASOCIACION DE PLATANOS	AV. NICOLÁS. ARRIOLA CDRA. N°14	15 Mbps
Cámara Nº 52	AV. NICOLÁS. ARRIOLA CDRA. Nº21 / FRENTE AL GRIFO REPSOL	AV. NICOLÁS. ARRIOLA / AV. SAN LUIS	15 Mbps

Cámara Nº 53	PARQUE LAS MORAS	JR. RIO TUMBES / FRANTE AL PARQUE LAS MORAS	15 Mbps
Cámara Nº 54	MARISCAL OSCAR BENAVIDES	AV. NICOLÁS. ARRIOLA – JR. MARISCAL OSCAR BENAVIDES	15 Mbps
Cámara Nº 55	*PARQUE LO REYES*	*CALLE PUERTO ETEN / CALLE PUERTO COLOMA*	15 Mbps

ANEXO 02 – Ubicación de postes inteligentes

Nº Conexión	***Nombre***	***Ubicación***	***Tipo de Conexión***	***Ancho de Banda - Wifi***
01	Parque Horacio Patiño	Horacio Patiño Cruzati 770 – San Luis	Punto Wifi	20 Mbps
02	Parque San Juan Macias	Jr. Almudena San Luis	Punto Wifi	20 Mbps
03	Colegio San Juan Macias	Jr. Rio Piura 201	Punto de Red	20 Mbps
04	Colegio San Luis	Calle Francisco Vidal de Laos 601	Punto de Red	20 Mbps
05	Colegio villa Jardín	Jr la Capea 150	Punto de Red	20 Mbps
06	Colegio Miguel Grau Seminario	Jr. Rio Ica 249	Punto de Red	20 Mbps
07	Colegio Madre Admirable	Calle Ollanta S/N	Punto de Red	20 Mbps