**TÉRMINOS DE REFERENCIA SERVICIO INTERNET BELLAVISTA**

## 1 OBJETO DEL CONTRATO:

Se requiere contratar el servicio de Internet de Banda Ancha con seguridad gestionada para la Sede Administrativa de Puno ubicado a 3825 msnm en el departamento de Puno. El transporte de datos a través del internet utilizará medio no-satelital, con seguridad gestionada por parte del operador.

## 2 FINALIDAD PÚBLICA:

Proveer el Servicio de acceso a Internet con seguridad administrada para el servicio de todos los colaboradores y provisión de información en cumplimiento con las disposiciones y cumplimientos normativos vigentes.

## 3 ANTECEDENTES DE LA CONTRATACIÓN:

San Gabán S.A. para asegurar sus operaciones administrativas y operativas requiere contar con un servicio de internet robusto y tolerante a fallas con un 99.5% de disponibilidad anual.

## 4 OBJETIVO GENERAL Y ESPECÍFICOS:

### 4.1 Objetivo General

Mantener los servicios de comunicaciones a través de internet con servicio de seguridad gestionada que provea el mismo operador.

### 4.2 Objetivos Específicos

- Contratar servicios de internet con una disponibilidad anual como mínimo, para la publicación de servicios por este medio, al 99.5%.
- Contratar servicios de internet con seguridad gestionada de 24x7, que permitan implementar políticas de seguridad de acceso y control perimetral, de acuerdo a las necesidades de San Gabán S.A.
- Optimizar los servicios de seguridad gestionada en un entorno de trabajo remoto y teletrabajo con el fin de contar con los servicios de nube que lo permitan.
- Contar con un servicio de seguridad antispam.

## 5 SISTEMA DE CONTRATACIÓN:

El presente procedimiento se rige por el sistema de Suma Alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

## 6 ADELANTOS (FACULTATIVO):

No Aplica.

## 7 SUBCONTRATACIÓN

Será posible la subcontratación para actividades de implementación, servicio técnico, mantenimiento, atención de averías, y aquellos que permitan la sostenibilidad del servicio de internet, el cual no podrá exceder del 40% del monto total del contrato original.

El Postor ganador de la Buena Pro es el único responsable de la ejecución total de las prestaciones frente a la Entidad, y que las obligaciones y responsabilidades derivadas de la subcontratación son ajenas a San Gabán S.A.

## 8 NORMAS OBLIGATORIAS Y/O VOLUNTARIAS:

No Aplica.

## 9 DESCRIPCIÓN TÉCNICA DEL SERVICIO:

Servicio de Internet con Seguridad Administrada Sub Estación San Gabán II

## 9.1 Especificaciones del servicio

El servicio por cada Ítem debe contar con las siguientes especificaciones generales mínimas.

| Requerimiento | Valor Mínimo Requerido | Valor Ofertado |
|---|---|---|
| **Ancho de Banda** | 70 Mbps | |
| **Disponibilidad del servicio de internet y sus componentes.** | Se requiere una disponibilidad del 99.5% en los siguientes:<br>- Servicio de Internet y equipo router.<br>- Conexiones Remotas | |
| **Seguridad Administrativa** | Servicio de seguridad administrada con un SLA 24x7 con acceso por el cliente.<br>Con una disponibilidad del servicio y equipamiento al 96%. **Según alcance del punto 9.2.** | |
| **Seguridad Avanzada** | Monitoreo de amenazas y nivel de compromiso de la infraestructura de la Sede Administrativa. **Según alcance del punto 9.3.** | |
| **Conexión Remota** | Sesenta (60) Conexiones Remotas, con punto de Acceso en Perú y con conexión al NAP Perú, optimizado para el trabajo remoto. **Según alcance del punto 9.4.** | |
| **Servicio de Antispam Administrado** | Servicio de Antispam (para Exchange Server 2019 hibrido) para 140 Buzones administrado por el operador, y con acceso por el cliente. **Según alcance del punto 9.5** | |
| **Características del Overbooking** | El Overbooking solicitado de 1:1 100% garantizado enlace simétrico garantizado al 100% el ancho de banda las 24 horas. | |
| **Protocolos de Red** | La empresa postora ganadora de la buena pro del servicio debe contar con protocolos de red que permitan administrar calidad de servicio, tales como MPLS, SDH, otros, dentro de su backbone. | |
| **SLA Servicio** | • La degradación total o parcial de los servicios de internet y seguridad debe ser repuesto en un plazo no mayor a 24 horas. | |
| **Medio Físico de transporte** | • Deberá ser mediante fibra óptica desde el punto de presencia del postor ganador de la buena pro. Este backbone también deberá ser íntegramente de fibra óptica.<br>• No se aceptarán enlaces o conexiones inalámbricas y/o radiales.<br>• Los equipos de conexión a Internet deberán ser administrados por el postor ganador de la buena pro del servicio. | |
| **Equipo de Seguridad Firewall** | El equipo de seguridad debe tener la capacidad de gestionar un segundo enlace internet de contingencia que San Gabán S.A. contratará con otro operador que se encontrará en modo Activo. **Según el punto 9.2.** | |
| **Router a instalarse** | • El router deberá ser de última tecnología y tendrá como mínimo una interfaz LAN y no realizará la función de NAT mientras se cuente con un equipo firewall. Éste y los demás equipos o accesorios necesarios para la provisión del servicio deberán ser provistos en calidad de alquiler, los cuales serán configurados por el postor ganador de la buena pro:<br>• Ancho de banda soportado, de al menos 200 Mbps.<br>• Deberá incluir como mínimo (4) interfaces 10/100/1000BaseT, un (01) puertos SFP. Todos los | |

| Requerimiento | Valor Mínimo Requerido | Valor Ofertado |
|---|---|---|
| | puertos solicitados de forma independiente podrán operar en capa 3 y capa 2 del modelo OSI. | |
| **Protocolo de ruteo** | El postor ganador de la buena pro deberá tener disponibilidad protocolos IP V4 e IP V6, TCP/IP. | |
| **Del postor ganador de la buena pro del servicio** | • El backbone de la red local deberá ser redundante en la ciudad de Puno.<br>• Deberá contar con doble salida internacional a Internet.<br>• Debe tener autorización del Ministerio de Transportes y Comunicaciones para servicio de valor añadido, con cobertura a nivel nacional.<br>• Debe poseer un centro de gestión propio o tercerizado para la atención y solución de averías (ventanilla única de atención) el que debe estar activo en horario de 24x7. | |
| **NAP Perú (Network Access Point)** | El prestador del servicio debe pertenecer al NAP Perú. Se considerarán miembros del NAP aquellos proveedores que cuenten con un enlace propio al NAP Perú activo y 100% operativo. | |
| **Reparaciones** | El postor ganador de la buena pro deberá reparar o remplazar, sin costo, los equipos o componentes que sean necesarios para asegurar la prestación del servicio. | |
| **Herramientas de Gestión y Reporte de Tráfico para el servicio ofertado por el postor ganador de la buena pro del servicio** | • El equipo de enrutamiento en el local del cliente debe ser de última tecnología, para una prestación de tipo industrial de 24x7.<br>• Debe tener una conexión hasta el backbone de Internet entregado mediante enlaces redundantes dentro de su bac365kbone.<br>• Deberá proporcionar un usuario y password de acceso para el cliente al sistema de monitoreo vía web<br>• El protocolo de comunicación será TCP/IP.<br>• El postor ganador de la buena pro del servicio debe contar con los siguientes puntos en su red:<br>▪ Redundancia en equipos de ruteo en sus instalaciones.<br>▪ Redundancia en backbone de routers de su red.<br>▪ Redundancia en los servidores DNS.<br>▪ Redundancia en los enlaces de Salida Internacional.<br>• En caso la red de San Gabán S.A. esté siendo vulnerada por ataques externos, el postor ganador de la buena pro deberá tomar acciones correctivas de seguridad, lo que debe ser reportado a San Gabán. | |
| **Tiempo máximo para la activación del servicio** | Cuarenta (40) días calendarios luego de la firma del contrato, pudiendo atender fuera de horario de oficina en coordinación con el administrador del contrato. | |
| **Acceso a los servicios de Internet** | Acceso total a los servicios de Internet sin restricción de protocolo, puerto o aplicación. | |
| **Direcciones IP Públicas del postor ganador de la buena pro** | En concordancia con recomendaciones de ARIN y LACNIC, deberá proveer como mínimo (ocho) 8 direcciones IP públicas para la Sub Estación San Gabán: WAN, Gateway, red, broadcast y 4 direcciones, con registro DNS, es decir | |

| Requerimiento | Valor Mínimo Requerido | Valor Ofertado |
|---|---|---|
| | inscripción de nuestros dominios.<br>Estos dominios deberán ser registrables en la rcp.net.pe.<br>Se proveerá un correo y acceso telefónico y/o mediante acceso por URL con usuario/contraseña, con el DNS MASTER del Postor ganador, para gestiones de registro. | |
| **Trabajos de instalación y configuración** | El postor ganador de la buena pro deberá realizar los trabajos necesarios dentro o fuera del local, incluyendo otros necesarios sin que esto implique costo adicional para SAN GABÁN S.A**.**<br>San Gabán S.A. brindará todas las facilidades técnicas que sean necesarias; así como todos los accesos que correspondan, teniendo a su cargo la responsabilidad de gestionar las autorizaciones de ingreso necesarias, de desocupar los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación, así como la provisión de los servicios correspondientes para la instalación de cualquier equipo.<br>Finalmente de requerirse una excepción para el cumplimiento de una meta, se puede coordinar con el administrador del contrato y evaluar la posibilidad de trabajos fuera del horario de oficina los que deben ser previamente autorizado por el Administrador de Contrato y los Responsables de las Sede. | |
| **Soporte Adicional VPN** | Actualmente se cuenta con VPNs configurados en el Firewall los mismos que deben ser reconfigurados en los nuevos equipos de seguridad provistos por el postor ganador de la buena pro:<br>- Red de datos en contingencia Site-to-Site entre las dos oficinas (Oficina Administrativa de Puno y Central Hidroeléctrica):<br>- Red administrativa Site-to-Client para trabajadores remotos con equipos Windows o MAC. | |

## 9.2 Solución de Seguridad Administrada

La solución de seguridad administrada debe ser propuesta según los siguientes alcances:

### 9.2.1 Descripción

- Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance y que deban ser del mismo fabricante.
- En relación al RMA, el fabricante debe contar con depósito de partes, o equipos completos con presencia local en el país y poder ofrecer mínimamente reemplazo de partes en el próximo día hábil, conocido por las siglas en ingles NBD (next business day), para poder garantizar el funcionamiento de la solución.
- El fabricante debe estar en el cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 5 reportes.
- El fabricante debe estar como líder en el último informe de Forrester Wave Automated Malware Analysis.
- El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.

- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7 del modelo OSI.
- 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 (Fin de Vida o Fin de Ventas o Fin de Soporte).

### 9.2.2 Capacidad

- Throughput de 260 Mbps como mínimo medido con tráfico real (transacciones http 64KB o transacciones usando una mixtura de aplicaciones), con las siguientes funcionalidades habilitadas simultáneamente: Firewall con clasificación y control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Anti-malware de red, Anti-spyware (o AntiBot), control de amenazas avanzadas de día cero (Sandboxing) y logging activo. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
- No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
- La plataforma de hardware debe soportar hasta 64 mil conexiones simultaneas sin desencriptar.
- Capacidad de descifrado de SSL/TLS de al menos 6,400 sesiones simultaneas.
- Fuente de energía redundante en AC
- Disco interno para almacenamiento de 32 GB de capacidad como mínimo
- Mínimo 8 (ocho) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red de la Entidad.
- Mínimo 1 (una) interfaz de red 10/100/1000 dedicada para administración que no debe estar en el bus de datos (out-of-the-band);
- Mínimo 1 (una) interfaz de tipo consola o similar;
- Soporte de, como mínimo, 3 (tres) ruteadores virtuales;
- Soporte de, como mínimo, 15 (quince) zonas de seguridad;
- Estar licenciada para soportar 250 clientes de VPN SSL simultáneos del estilo cliente-servidor para las PCs de la Entidad;
- Estar licenciada para 1,000 (mil) túneles de VPN IPSec simultáneos del estilo sitio-a-sitio.

### 9.2.3 Características General del Equipo

- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Seguridad contra anti-spoofing;
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
- Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;
- Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo;
- Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos o dominios virtuales:
    - Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red;
    - Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;

- Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default gateway de las redes protegidas;
- Modo Transparente, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico a nivel de aplicación sobre 2 puertos en modo bridge/transparente.

- Modo mixto de trabajo Sniffer, Transparente, L2 y L3 simultáneamente en diferentes interfaces físicas del mismo equipo.

### 9.2.4 Funcionalidades del Firewall

- Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Control, inspección y descifrado de SSL/TLS por política para tráfico de entrada (Inbound) y salida (Outbound).
- Debe procesar e inspeccionar tráfico HTTP/2.
- Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
- Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
  - Mostrar la primera y última vez que se utilizó una regla de seguridad.
  - Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

### 9.2.5 Control de Aplicaciones

- Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIp, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389;
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VoIP que utilizan cifrado propietario;
- Para tráfico cifrado (SSL/TLS y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
- Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, por ejemplo, compartir archivos dentro de una sesión Webex.
- Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa;
- Debe alertar al usuario cuando una aplicación fuera bloqueada;
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
  - Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol).
  - Nivel de riesgo de las aplicaciones.
  - Categoría y sub-categoría de aplicaciones.

    - Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.
- Debe contar con un módulo en la consola web que permita identificar las reglas de firewall que no cuenten con un control basado en aplicaciones, con la finalidad de facilitar la adopción del control basado en aplicaciones.

### 9.2.6 Prevención de Amenazas Conocidas

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Anti-malware de red), Anti-Spyware (o Antibot) y DNS SinkHole integrados en el propio appliance.
- Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
- Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/Pasivo;
- Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
- Debe contar con firmas específicas para la mitigación de ataques DoS, buffer overflow, C2 (comando and control)
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP e POP3;
- Identificar y bloquear comunicaciones con botnets;
- Debe soportar referencia cruzada como CVE.

### 9.2.7 Análisis de Malware Moderno

- Poseer la capacidad de análisis de amenazas no conocidas;
- El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en nube, donde el archivo será ejecutado y simulado en un ambiente controlado. La nube deberá ser propia del mismo fabricante y no tercerizada con otras empresas.
- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X y Android;
- Debe soportar el monitoreo de archivos transferidos por internet (HTTP, HTTP/2, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB.
- El sistema de análisis en nube debe proveer informaciones sobre las acciones del malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo malware y proveer información sobre el usuario infectado (su dirección IP y su login de red);
- Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia interfaz de administración.
- Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP y RAR) archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
- Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.

- La solución de sandboxing debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor, inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

### 9.2.8 Filtro de Contenido

- Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local.
- Debe permitir visualizar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio
- Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- Debe poseer al menos 60 categorías de URLs y permitir la creación de categorías personalizadas.
- Debe permitir la customización de la página de bloqueo
- Debe permitir bloquear o informar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
- Debe evitar la fuga de credenciales corporativas desde o hacia sitios web, es decir debe identificar el envío de credenciales a sitios web no autorizados, previniendo ataques de phishing.
- Debe poder prevenir acceso a páginas de malware y phishing.

### 9.2.9 Identificación de Usuarios

- Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de directorio, autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
- Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente instalado en un equipo del dominio.
- Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios
- Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios.

### 9.2.10 QoS

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto audio como vídeo streaming y todo el inventario de aplicaciones soportadas por la solución de seguridad.
- Soportar la creación de políticas de QoS por:

    - Dirección de origen
    - Dirección de destino
    - Por usuario y grupo de LDAP/AD.
    - Por aplicaciones
    - Por puerto;
- El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
- Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
- Disponer de estadísticas Real Time para clases de QoS, monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

### 9.2.11 Filtro de Datos

- Los archivos deben ser identificados por extensión y firmas;
- Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular;
- Debe poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP.

### 9.2.12 VPN

- Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL;
- La VPN IPSec debe soportar:
    - DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
    - Autenticación MD5, SHA-1, SHA-2;
    - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
    - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Permitir la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles VPN;
- Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- Debe tener la opción de ocultar el agente de VPN instalado en el cliente remoto, tornándose invisible para el usuario;
- Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site;
- Soportar autenticación vía AD/LDAP, Secure id, doble factor de autenticación, certificado del lado del cliente y base de usuarios local.

### 9.2.13 Consola de Administración y Monitoreo

- La administración de las políticas de seguridad debe realizarse sobre hardware dedicado para dicho propósito ya sea dentro de los mismos appliances de seguridad o mediante un servidor o appliance dedicado.
- La solución debe contar con interface gráfica de usuario (GUI), vía Web por HTTP y/o HTTPS compatible al menos con, Windows, Linux y Mac OS, en la cual se podrá elegir entre los idiomas inglés o español.
- La solución debe contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

- La solución debe poseer una interface basada en línea de comando (CLI) usando SSH, Telnet o puerto serial dedicado.
- La solución debe contar con la capacidad de asignar un perfil de administración basado en roles (RBAC) que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
- Ante escenarios donde existan dos o más administradores del next generation firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- Debe permitir monitorear los eventos de la plataforma vía SNMP
- Debe posibilitar la integración con otras soluciones de SIEM del mercado
- Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
- Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- Generar alertas automáticas vía:
    - Email;
    - SNMP;
    - Syslog;
- La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

### 9.2.14 Servicio Gestionado

1. El postor ganador de la buena pro del servicio deberá contar con un sistema de gestión a través de una ventanilla única, es decir un punto único de contacto para el Proyecto, para reporte de fallas, atención a nuevas solicitudes o tratamiento de reclamos.
2. Operación de Plataforma Administrada o Centro de Gestión especializado en Seguridad (*Security Operations Center* - SOC: configuraciones y creación de reglas), previo requerimiento de SAN GABÁN S.A. Esto puede ser propio o tercerizado.
3. Atención de tickets de manera ilimitada y sin costo adicional.
4. Mantenimientos Preventivos a nivel de sistema operativo de la plataforma se hará de manera remota, coordinada con SAN GABÁN S.A.
5. Cambios a la configuración del equipo de seguridad sin límite.
6. Soporte Correctivo (atención solicitada por SAN GABÁN S.A. o generada por un evento casual que requiera corregir un mal funcionamiento o un riesgo tecnológico de la plataforma).
7. Generación de Reportes Mensuales (reporte técnico que podrá ser generado por una herramienta automática de reportes, y entregados dentro de los 10 primeros días hábiles de cada mes).
8. El soporte técnico brindado deberá estar disponible las 24 horas x 7 días durante el periodo del contrato.
9. Igualmente, el postor deberá contar con facilidades de monitoreo de los enlaces en forma permanente, las mismas que deberán estar disponibles para el personal del proyecto (del postor ganador de la buena pro así como de SAN GABÁN S.A.), a través de una interfaz del tipo Web.
10. Contar con Backup de la Configuración del o de los equipos firewall por medio de un proceso de respaldo diario y automáticos de las reglas de los equipos del proyecto. Para la configuración

del router, se contará con un backup al final de la configuración inicial y se actualizará en el caso de alguna modificación y actualización posterior.

11. El tiempo de respuesta máximo para la atención de un problema (avería) será de 30 minutos, contadas desde que el Proyecto reporta la incidencia a la ventanilla del postor ganador de la buena pro y hasta que se le asigna un ticket de atención. El postor ganador de la buena pro deberá indicar la información sobre los medios de atención o contactos para la gestión adecuada del servicio: ficha de servicio post-venta que será alcanzada durante la implementación del servicio.
12. Las averías de mayor gravedad, motivadas por problemas originados por fallas en planta externa y/o en la sede de SAN GABÁN S.A., serán atendidas y/o solucionadas de acuerdo a la gravedad de la ocurrencia en el menor plazo y previo informe justificatorio que será evaluado por el personal técnico de SAN GABÁN S.A. Soporte Remoto una vez escalado al postor ganador de la buena pro de servicio (por cada soporte o requerimiento se debe genera un ticket con el detalle). Dichos tiempos será detallado en la propuesta técnica presentada por el Postor.
13. Reporte de Tickets de problemas y reclamos al servicio de asistencia para el cual deberá de brindar los números telefónicos para su atención 24x7.

Nota: Para validar las características solicitadas del equipo de seguridad se podrá realizar a través de carta de fabricante o declaración jurada o data sheet del equipamiento..

### 9.3 Centro de soporte de seguridad avanzada

Se solicita un servicio de soporte de seguridad propio o de un socio estratégico del postor ganador de la buena pro, con certificación ISO27001 o ISO22301, que, mediante el análisis de logs de la solución de seguridad perimetral (Firewall) permita realizar:

1. Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
2. Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) basadas en la información contextual granular y el uso de herramientas de minería de datos. Deberá poder recolectar información de fuentes como, por ejemplo:
    - CERT Nacionales
    - IBM Talos
    - Darkweb
    - CIRCL OSINT Feed
    - Diamondfox_panels
    - Feodo IP Blocklist
    - US-CERT
    - blocklist.de/lists/all.txt
    - abuse.ch SSL IPBL
    - blocklist.greensnow.co
    - URL Haus Malware URLs
3. Caza de amenazas identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
4. Respuesta y mitigación de incidentes en tiempo real ante ciber-amenazas.
5. Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones COI y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
6. Investigación forense de procesos en cursos de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados. Mínimo de 10 horas mensuales de ser requerido.
7. La solución deberá procesar logs de más de 700 integraciones entre cloud y on-premise.
8. El centro de soporte de seguridad tiene como alcance la información recibida del firewall perimetral.
9. Mínimo de 60 días de retención de logs.
10. Los logs deberán ser enviados de forma segura mediante VRF del postor ganador de la buena pro sin necesidad de instalar colectores de tráfico locales en la red de la institución.
11. El servicio de seguridad avanzada debe ser compatible al 100% con los equipos de seguridad ofrecidos.
12. Informe mensual de los eventos y nivel de compromiso del equipo de seguridad.
13. Respuesta proactiva de bloqueo o remediación ante ataques de seguridad.

## 9.4 Conexión segura para usuarios remotos

Se requiere conexiones para que usuarios remotos de la entidad envíen el tráfico en su totalidad (no split-tunnel) a través del túnel VPN que hará uso del Datagram Transport Layer Security (DTLS) como protocolo de comunicación seguro e incluirá MFA como autenticación de segundo nivel para todos los usuarios.

Para poder garantizar una conexión segura para los usuarios remotos, el operador debe contar con los siguientes requerimientos técnicos:

1. Contar con un centro de operaciones de seguridad propio o de un socio estratégico .
2. La navegación de internet seguro debe realizarse desde el centro de operaciones sin que afecte el equipo de seguridad (Firewall).
3. San Gabán S.A. garantiza un enlace superior a 10 MB entre el firewall y el centro de operaciones, para la comunicación entre los usuarios remotos y los recursos internos de la entidad.
4. El centro de operaciones deberá brindar todo el procesamiento de seguridad en su punto de presencia para las conexiones VPN y seguridad de navegación para las conexiones de los clientes.
5. El centro de operaciones de seguridad se enlazará por intermedio de una VPN IPSec al firewall de la entidad, esta VPN IPSec servirá como canal de comunicación entre los usuarios VPN y los recursos internos de la empresa.
6. La conexión VPN IPSec entre el centro de operaciones y el firewall de la entidad, debe garantizar como mínimo 10Mbps de ancho de banda, para la comunicación entre los usuarios remotos y los recursos internos de la entidad
7. El centro de operaciones de seguridad deberá contar con un punto de presencia en Perú, con múltiples puntos de redundancia en América del sur, América del norte, Europa y Asia para efectos de continuidad de servicio.
8. El centro de operaciones de seguridad a través de su punto de presencia deberá poder brindar una capa de seguridad adicional de navegación a nivel de filtrado web por categorías, visibilidad de aplicaciones, gestión de ancho de banda por aplicaciones y detección de malware mediante escaneo de firmas comparadas con una base de datos de archivos maliciosos. Deberá también como segundo nivel de detección permitir un análisis más exhaustivo mediante el uso de modelos predictivos y machine learning para la protección de archivos maliciosos y de día cero.
9. El centro de operaciones de seguridad a través de su punto de presencia deberá brindar políticas de seguridad basado en aplicaciones, políticas de seguridad basado en horarios, filtros de seguridad web, protección de IPS y un SIEM con capacidad de almacenamiento de LOGs de al menos seis (06) meses.
10. Se deberá también bloquear accesos indebidos a la red corporativa basado en firmas de comportamiento, análisis de reputación, vulnerabilidades conocidas, anti-bot (C&C), análisis de comportamiento de red, validación de protocolo y restricción por geolocalización.
11. Se deberá habilitar la inspección vía TLS para la protección de amenazas avanzadas.
12. Este sistema de seguridad deberá incluir técnicas de optimización de tráfico como aceleración de TCP y retransmisión de UDP para reducir el impacto de paquetes perdidos durante la comunicación.
13. Reporte de tráfico mensual de los usuarios conectados por VPN, en donde se considere el periodo de conexión, número de conexiones por día y el horario de conexión por usuario el que podrá ser modificado según la necesidad de San Gabán.

## 9.5 Servicio de Anti Spam

Se debe considerar un servicio de antispam en nube; con las siguientes características.

1. Administración y configuración a través del acceso web (HTTP, HTTPS).
2. La solución debe brindar un 99,9% Disponibilidad del servicio
3. Debe tener una tasa de detección de spam de al menos > 99,7%
4. Permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.
5. Proporcionar soporte para múltiples dominios de correo electrónico.
6. Proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)
7. Almacenamiento de correo por 30 días.
8. Almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).
9. La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.
10. Generar informes por demanda o programados a intervalos de tiempo específicos
11. La solución debe generar y enviar informes en formato PDF o HTML.
12. La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing.
13. La solución debe ser capaz de realizar la inspección del correo entrante y saliente.
14. La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.
15. La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb.
16. La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing.
17. La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente.
18. La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.
19. La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.
20. La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.
21. La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web y POP3.
22. La solución debe ser capaz de programar el envío de informes de cuarentena.
23. La solución debe ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto.
24. La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega.
25. La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.

26. La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados.
27. La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.
28. La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.
29. La solución debe ser capaz de realizar análisis bayesiano para determinar si un correo es spam.
30. La solución debe ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje.
31. La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).
32. La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject) o descartar (Discard).
33. La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM.
34. La solución debe ser capaz de soportar las listas negras de terceros (Blacklist).
35. La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.
36. La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6.
37. La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP).
38. La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema.
39. La solución debe ser capaz de ejecutar el análisis antivirus / antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ y RAR.
40. La solución debe permitir la sobrescrita, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware.
41. La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).
42. La solución debe ser compatible con Sender Policy Framework (SPF).
43. La solución debe ser compatible con Domain Keys Identified Mail (DKIM).
44. La solución debe ser compatible con Domain Based Message Authentication (DMARC).
45. La solución debe poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
46. La solución debe poder definir el reenvío de correo (relay) a una IP específica con base a la IP origen del mensaje.
47. La solución debe ser compatible con Exchange y Office 365.

## 9.6 Servicio AntiDDoS en la Nube

1. El postor ganador de la buena pro deberá brindar un servicio de tráfico limpio en la nube local (territorio nacional para evitar ataques provocados dentro del territorio nacional), disponible al 99.90%, mediante el uso de una herramienta de mitigación de ataques de denegación de servicio dedicada. La solución deberá brindar protección para un volumen total de tráfico de hasta 2 veces en ancho de banda contratado. Esta herramienta deberá analizar tanto el tráfico de subida como tráfico de bajada y todos los servicios públicos que la entidad tenga o no dominio, e incluir la capacidad de detección de ataques de denegación de servicio a nivel de aplicación sin estados (stateless).

2. La solución deberá ser de tipo appliance, de tecnología específica para la mitigación de ataques de denegación de servicios, no se aceptarán soluciones en las que la protección DDOS sea una funcionalidad adicional de equipos Firewall, Next Generation Firewalls, Application Delivery Controllers, Routers u otros equipos de seguridad o redes.
3. La solución de Mitigación DDoS deberá tener un sistema de creación automática de firmas en tiempo real para la protección frente a ataques emergentes.
4. La solución de Mitigación DDoS deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos).
5. La solución deberá ser de tipo Stateless.
6. La solución deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on", también denominada en línea o siempre activa. No se aceptarán soluciones de mitigación de ataques de denegación de servicios bajo una arquitectura de derivación de tráfico.
7. El postor ganador de la buena pro deberá brindar un reporte mensual de la actividad de seguridad relacionada a los ataques de denegación de servicios detectados y mitigados. Este reporte puede ser emitido de forma automática por una herramienta del sistema o por el su centro de atención.
8. La solución deberá contar con un portal web multi-tenant y que permita a la institución acceder a un dashboard con las estadísticas y reportes de su actividad DDoS.
9. La solución debe contar adicionalmente con detección y mitigación de ataques SSL como HTTPS flood descifrando el tráfico HTTPS de la entidad con un certificado digital wildcard o del sitio en caso de sospechar de algún ataque e inspeccionar el contenido.
10. La protección de SSL debe ser stateless, actuar solo bajo sospecha de ataque para no generar latencia en tiempo de paz y debe funcionar en modo Igress-Only, sin necesidad de ver el tráfico que proviene del servidor.
    La solución debe estar en capacidad de hacer challenge and response sobre HTTPS.

## 9.7 Inspección y Pruebas

El postor ganador de la buena pro y SAN GABAN S.A. al término del plazo considerado en el Plan de Entrega, que será presentado al inicio de la implementación, realizarán en forma conjunta los procedimientos de inspección y pruebas sobre la infraestructura y equipos instalados por el postor ganador de la buena pro, de tal forma que le permita a SAN GABAN S.A. establecer que los servicios serán brindados de conformidad con lo solicitado en las presentes bases y a las prestaciones adicionales establecidas por el Postor en su oferta. Para ello SAN GABAN S.A. brindará las facilidades de espacio, energía eléctrica adecuada para los equipos del postor ganador de la buena pro.

El Plan de Entrega se alcanzará máximo a los 10 días útiles de suscrito el contrato, y contendrá lo siguiente:

- Cronograma de actividades para la implementación del servicio.
- Procedimiento(s) de atención de averías, el cual puede incluir una relación de personas de contacto y/o un servicio de personal rotativo (sin nombres específicos) y/o un servicio de *Call Center* 24 x 7, el que corresponda según la propuesta técnica a presentar por el postor ganador de la buena pro.

**Pruebas de Aceptación:**

Para las pruebas de Aceptación el Contratista ganador de la Buena Pro, deberá de hacer alcance los formatos de pruebas de aceptación por cada componentes del servicio, dichos formatos de pruebas serán utilizados para la verificación, el que se realizará en coordinación con San Gabán S.A. y el responsable del Contratista.

Dichas pruebas se realizarán en el lugar de la instalación. Los insumos o costos que demanden

estas pruebas, ya sea en concepto de horas máquina, personal, materiales, programas de medición de performance, etc., no implicarán en ningún caso, reconocimiento de gastos por parte de SAN GABAN S.A. y deberán ser provistos por el postor ganador de la buena pro.

La omisión en la oferta de algún componente que, al momento de la instalación, prueba y puesta en servicio y a juicio de SAN GABAN S.A. resulte necesario para la normal provisión de los servicios ofrecidos, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al postor ganador de la buena pro a proveerlo de inmediato y sin cargo adicional alguno.

Cualquier defecto notificado por SAN GABAN S.A. al postor ganador de la buena pro durante la realización de las pruebas de aceptación, será rectificado por este sin cargo alguno, teniendo como plazo máximo cinco (5) días naturales a partir de su notificación.

Una vez realizados los procedimientos de inspección y pruebas a su conformidad de SAN GABAN S.A. se levantará y entregará al postor ganador de la buena pro el Acta de Aceptación e Inicio de las Operaciones. El plazo de servicios se iniciará desde la fecha de suscripción de dicha Acta.

## 9.8 Confidencialidad

1. El Postor Ganador de la Buena Pro se compromete a mantener en reserva, y no revelar a tercero alguno sin previa conformidad escrita de SAN GABAN S.A. toda información que le sea suministrada por esta última y que restringirá la revelación de carácter estrictamente necesario dicha información para el cumplimiento del presente contrato sólo a los empleados y subcontratistas del Postor Ganador de la Buena Pro, sobre la base de "necesidad de conocer".
2. Los casos de exclusión de confidencialidad, como revelación de información pública, judicial o mandatorio en el sentido que no implique incumplimiento de las cláusulas contractuales, podrán ser explicitadas en la propuesta del Contratista.
3. La obligación de confidencialidad no resulta aplicable en los supuestos, cuando la información en cuestión:
   a) Haya sido de difusión o acceso público;
   b) Haya sido publicada antes de haber sido puesta a disposición del postor;
   c) Ya obre en poder del postor y no esté sujeta a cualquier otro impedimento o restricción que le haya sido puesto de manifiesto;
   d) Haya sido recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato;
   e) Haya sido independientemente desarrollada por el postor, siempre que no se hubiese utilizado para ello otra información confidencial; o
   f) Deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden
4. Por su parte, San Gabán S.A. conoce y está informada respecto del tratamiento de datos personales, conforme a la Ley N° 29733, Ley de Protección de Datos Personales y demás normas complementarias que administra y supervisa la Autoridad Nacional de Protección de Datos Personales, aplicables en todos los extremos en este acápite.

## 9.9 Atención de Llamadas Ante Averías o Fallas

Se entenderá por avería a una interrupción parcial o total del servicio, así como a un decremento en la calidad del servicio. Toda actividad o provisión de bienes que tenga que ejecutar el postor ganador de la buena pro para subsanar la avería serán sin costo alguno para SAN GABAN S.A.

Se entenderá por Tiempo de Subsanación, al tiempo transcurrido entre la comunicación al postor ganador de la buena pro de la existencia de una avería, por parte de SAN GABAN S.A. (llamada de servicio), y la subsanación de la misma a su satisfacción.

El postor deberá contar con un NOC por los servicio de Internet y Seguridad - centro de atención de llamadas de reparación o asistencia técnica - instalada de tal manera que le asegure a SAN GABAN S.A. que se encuentra en condiciones de cumplir con lo estipulado en las bases.

El postor ganador de la buena pro deberá entregar a SAN GABAN S.A. el procedimiento, los contactos de los responsables de la gestión del servicio; además del nivel de escalamiento. Para ello deberá presentar este procedimiento de atención de averías y la ficha de servicio post-venta, que serán presentados al inicio de la implementación.

El postor ganador de la buena pro contratado deberá reparar o reemplazar sin costo los equipos o componentes que sean necesarios para asegurar la prestación del servicio siempre y cuando la falla de estos no sea imputable a La Entidad. Pudiendo ser reemplazados por equipos de características similares mientras dure el cambio del principal por RMA.

## 9.10 Gestión del Servicio

El tiempo de solución del problema se calculará desde que SAN GABAN S.A. reporte el incidente al Centro de Servicio del postor ganador de la buena pro y se le asigna un ticket de atención:

a) El postor ganador de la buena pro deberá garantizar un eficiente sistema de gestión de sus redes de comunicación. El centro de gestión deberá estar en capacidad de realizar acciones de controles preventivos, correctivos y pruebas técnicas.
b) El postor ganador de la buena pro deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de reportes de fallas, centros de gestión, y personal de reparación de averías. Así mismo, deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten.
c) SAN GABAN S.A. se reserva la potestad de constatar la información presentada por el operador.
d) Durante el periodo de prestación del servicio, se evaluarán los tiempos de respuesta y la calidad del servicio, a fin de que SAN GABAN S.A. determine las correcciones necesarias si fuera el caso, al postor ganador de la buena pro contratado.
e) En caso no se logre establecer comunicación con los agente de soporte para le obtención del ticket de atención, esta se comunicará mediante correo electrónico al gestor de cuenta, y desde ese momento se calculará el periodo de atención. Para el cumplimiento de este punto el operador del servicio deben brindar un correo válido del gestor de cuenta (para lo cual en la ficha de servicio post-venta deberá incluir los horarios de atención), en caso esta varíe debe remitir al cliente el correo actualizado.

**Servicio de Monitoreo**

Los servicios de internet y seguridad deben ofrecer herramientas de monitoreo vía web. El postor ganador de la buena pro, asignará las cuentas de usuario correspondientes.

## 9.11 Instalación y Pruebas

Será de total y exclusiva responsabilidad del postor ganador de la buena pro contemplar todas las actividades, incluyendo la instalación de El dispositivo, componentes y accesorios, que garanticen el óptimo funcionamiento del Servicio de Internet incluyendo seguro de desplazamiento para su personal y contra accidentes.

Es responsabilidad del postor ganador de la buena pro proporcionar al personal que brindará el servicio, quienes deberán cumplir con las normas de Seguridad Industrial y Personal, cuidado del Medio Ambiente durante las actividades de instalación. Cada trabajador deberá portar un Fotocheck, ropa de trabajo (SCTR, EPP, botines dieléctricos, guantes, muñequeras antiestáticas, cascos y otros implementos de seguridad, el cual será de uso obligatorio al momento de que ingrese a las sedes).

La instalación se efectuará sin afectar las labores normales de la institución e incluirá la verificación de las condiciones necesarias para la instalación de los equipos salvando así responsabilidades de

ambas partes.

Para la instalación de los equipos en planta el postor ganador de la buena pro contratado deberá de cumplir con los protocolos de seguridad de San Gabán S.A. para poder ingresar a las instalaciones, dicho protocolo consta en lo siguiente, y que será presentado previo al día de la ejecución de la visita programada:

- Ficha de Sintomatología COVID-19 el que será provista por San Gabán S.A.
- Evaluación de Sintomatología COVID-19 del todo el personal que se apersonará en el vehículo particular del operador adjudicado (firmada por médico colegiado).
- SCTR y plan de Vigilancia.
- Cumplimiento obligatorio del uso de mascarillas de todo el personal desde que ingresa a las instalaciones, durante toda la actividad, hasta el retiro de las instalaciones.

## 9.12 Aspectos Generales

El postor ganador de la buena pro deberá realizar el servicio de manera tal que asegure el cumplimiento de los objetivos planteados en concordancia con los presentes Términos de Referencia.

Para los efectos del servicio solicitado, se debe considerar la aplicación del DS Nº 005-2017-MTC Modifica el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo N° 020-2007-MTC, ampliatorias y modificatorias vigentes.

El postor ganador de la buena pro podrá considerar el alquiler del equipamiento y enlaces necesarios para cumplir con lo solicitado en los presentes Términos de Referencia. Igualmente, de **considerar necesario**, se encargará de hacer los estudios previos de factibilidad a fin de no representar gastos adicionales para SAN GABAN S.A.

Los equipos de comunicación y el servicio deberán de disponer de flexibilidad para ser reconfigurados (o cambiados) a mayor velocidad en los nodos.

El postor ganador de la buena pro debe contar con la infraestructura necesaria para brindar estos servicios (deben contar con equipamiento tales como: ruteadores, banco de módems, líneas hunting, etc.) enlaces redundantes a la red externa con capacidad de recuperación ante fallas. Con el fin de garantizar la confiabilidad de su servicio.

## 9.13 Calidad de Servicio (QoS)

El postor ganador de la buena pro deberá garantizar un eficiente sistema de Gestión de sus Redes de Comunicación. El Centro de Gestión deberá estar en capacidad de realizar detección de alarmas tempranas, acciones de control preventivo y correctivo, pruebas técnicas, así como deberá entregar a SAN GABAN S.A. informes mensuales (de ser posible on-line) del rendimiento de los enlaces, uso del ancho de banda, tráfico; estos informes podrán ser importados de las herramientas de monitoreo por parte de SAN GABÁN S.A.

El postor ganador de la buena pro debe garantizar la seguridad de sus redes y sistemas de información ante intrusiones que provengan de su red de core o hub, para lo cual asumirá la responsabilidad por hechos que afecten la imagen de SAN GABAN S.A. (hechos imputables al Contratista) producto de esta intrusión a sus redes. Dicha responsabilidad estará cuantificada en términos de los daños directos causados.

El postor ganador de la buena pro deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los Centros de Llamadas de Reportes de Fallas, Centros de Gestión y personal de Reparación de Averías. Así mismo deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten.

El detalle del QoS del servicio de Acceso a Internet incluye como mínimo:

- El servicio de acceso a Internet será provisto a través de un enlace vía F.O.
- El servicio de internet debe garantizar 100% del ancho de banda.
- El ancho de banda deberá ser garantizado y con un grado de concentración del servicio de 1:1 en el tramo local e internacional, debidamente garantizado desde la Sede Principal del Proyecto.
- El enlace deberá ser simétrico y dedicado 100%, sin utilizar esquemas de acceso compartido o acceso del tipo asimétrico.
- Disponibilidad de crecimiento asegurada del ancho de banda.
- El servicio deberá estar disponible y operativo las 24 horas del día durante el tiempo de duración del contrato.
- El postor ganador de la buena pro 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 del Proyecto hasta el router de borde del postor ganador de la buena pro del Servicio Internet Nacional.
- Soporte técnico 24x7x365.

En caso de ser necesario realizar reparaciones por fallas no imputables a SAN GABAN S.A. el postor ganador de la buena pro contratado asumirá los costos de reparación de equipos, pasajes y otros.

### 9.14 Devolución de Equipos

Concluido la etapa contractual del servicio, los equipos de propiedad del proveedor deberán ser retirados dentro de los próximos 30 días calendario luego de liquidado el contrato, culminado el periodo de retiro San Gabán S.A. procederá a retirar los equipos a nuestro almacén de bajas por el periodo de (un) 1 año en donde se podrá proceder a realizar el cobro por el almacenamiento eximiéndose de cualquier deterioro del equipo. Culminado el periodo de un (1) año San Gabán S.A. calificará a los equipos en abandono y procederá a trámite de baja.

## 10 REQUISITOS DE CALIFICACIÓN:

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, las cuales deben ser acreditadas documentalmente, la Entidad incorpora los requisitos de calificación que se extraen de los Términos de Referencia, no pudiendo incluirse requisitos adicionales a los previstos en las mismas, los cuales son los siguientes:

| | |
|---|---|
| **A.1** | **CAPACIDAD LEGAL** |
| | **HABILITACIÓN** |
| | Requisitos:<br>Autorización o concesión otorgada por el Ministerio de Transportes y Comunicaciones para brindar servicio de telecomunicaciones.<br>**Importante**<br>*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.*<br>Acreditación:<br>Mediante copia simple de los documentos de autorización que acrediten la habilitación.<br>**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.* |
| **A.2** | **EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD** |
| | Requisitos:<br><br>El postor debe acreditar un monto facturado acumulado equivalente S/150,000.00 Ciento Cincuenta Mil con 00/100 Nuevos 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.<br><br>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/22,500 (Veintidós mil Quinientos y 00/100 Soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.<br><br>Se consideran servicios similares a los siguientes: Transmisión de voz y datos, Instalación de enlace VPN para la Sede de contingencia, Transmisión de datos, Servicio de internet y transmisión de datos, Enlace de datos, Transporte de datos, Servicio de comunicación mediante fibra óptica, Servicio de acceso a Internet Fijo, Internet a nivel nacional, Servicio de Internet, Transmisión de Datos e Infraestructura, Enlace dedicado y acceso a Internet.<br><br>Acreditación:<br><br>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.<br><br>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.<br><br>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.<br><br>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa |

[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".*

| | |
|---|---|
| | 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.<br><br>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.<br><br>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.<br><br>Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**<br><br>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. En todo caso, el tipo de cambio venta publicado por la SBS será el que se utilizará para estos casos.<br><br>Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. |
| **B** | **MEJORAS DEL SERVICIO** *(propuesta para el Comité de Selección)* |
| | Ancho de Banda:<br><br>• Servicio de Internet de 75 Mbps<br>• Servicio de Internet de 80 Mbps<br>• Servicio de Internet de 85 Mbps<br>• Servicio de Internet de 90 Mbps |

## 11 PLAZO DE EJECUCIÓN:

El plazo de ejecución del presente contrato es de 548 días calendario, el mismo que se computa a partir de la fecha de la firma del Acta de Activación del servicio.

El plazo para la instalación, migración, y configuración de Equipamiento al nuevo servicio es de 40 días calendario, el mismo que se computa desde el día siguiente de la firma del contrato.

Para la implementación de nuestros servicios, no será necesario monitoreos arqueológicos en ninguna de nuestras sedes. Actualmente ya se cuentan con servicios de comunicaciones, que no utilizan microondas.

## 12 LUGAR DE PRESTACIÓN DEL SERVICIO:

Los servicios se realizarán en:

- Sede: Oficina Administrativa de Puno
- Dirección: Av. Floral 245, Barrio Bellavista Ciudad de Puno, Provincia de Puno, Departamento: Puno.

- Coordenadas: 15°49’57’S - 70°01’34’W

## 13 PENALIDADES:

Si el postor ganador de la buena pro contratado incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, San Gabán S.A. le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

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

Donde:
F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando postor ganador de la buena pro contratado acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de San Gabán S.A. no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

## 14 OTRAS PENALIDADES:

Penalidad por Indisponibilidad:

En caso exista una indisponibilidad del servicio por causas no asociadas a fenómenos naturales se procederá con la aplicación de las siguientes penalidades:

**Disponibilidad de Servicio de Internet, equipo Router y conexión para usuarios remotos**
Se tiene como objetivo asegurar el nivel de disponibilidad del servicio de internet contratado sin degradaciones o falla de la misma.

**DS** : Disponibilidad Solicitada = 99.5
**DMsi**: Disponibilidad Mensual servicio de Internet y conexión remota que debe ser reportado por el Operador junto con la facturación (2 reportes).
**MF** : Monto total Facturado
**FD** : Factor de Disponibilidad = 4.5
**PIsi** : Penalidad por Indisponibilidad del servicio de internet.

$$PIsi = 10\% \; x \; MFx \; (\frac{99.5 - DMsi}{4.5})$$

**Disponibilidad por Tiempo de Reposición de Seguridad Administrada**
En este punto se tiene como alcance a los componentes físicos que forman parte de la solución de internet, y tiene como objetivo asegurar que se tenga un tiempo de respuesta adecuado para el cambio de un componente hardware en falla por uno similar o igual mientras se renueva o repara el equipo en falla.

**DS** : Disponibilidad Solicitada = 96
**DMe**: Disponibilidad Mensual de los equipos el que debe ser reportado por el Operador junto con la facturación.
**MF** : Monto total Facturado

**FD** : Factor de Disponibilidad = 4.5
**PIe** : Penalidad por Indisponibilidad de equipo de Seguridad.

$$PIe = 10\% \; x \; MFx \; (\frac{96 - DMe}{2})$$

## 15 PRESTACIONES ACCESORIAS.

No aplica para la presente contratación.

## 16 REAJUSTES:

No aplica para la presente contratación.

## 17 VICIOS OCULTOS:

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por el artículo 40° de la Ley de Contrataciones del Estado y 173° de su Reglamento.

El plazo máximo de responsabilidad del postor ganador de la buena pro contratado es de un (1) año contado a partir de la conformidad otorgada por San Gabán S.A.

## 18 CONFORMIDAD:

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168° del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la División de Tecnologías de la Información.

## 19 FORMA DE PAGO:

La Entidad realizará el pago de la contraprestación pactada a favor del postor ganador de la buena pro de forma mensual.

Para efectos del pago de las contraprestaciones ejecutadas por el postor ganador de la buena pro, el contratista debe emitir los siguientes documentos:

- Comprobante de pago.
- **Reporte del nivel de disponibilidad (físico o digital) del servicio emitida por el postor ganador de la buena pro del servicio de Internet contratado.**
- **Reporte del nivel de compromiso por el Cibersoc.**

Dicha documentación se debe presentar en mesa de partes, sito en la Av. Floral 245 Bellavista, Puno, o en la ventanilla virtual: mesadepartes@sangaban.com.pe . El comprobante de pago debe alcanzarse a facturalogistica@sangaban.com.pe con copia a ccastro@sangaban.com.pe y llizares@sangaban.com.pe

Respecto al comprobante de pago se precisa que los servicios objeto de contratación podrá considerarse la emisión del Recibo de Servicios, considerando que este comprobante de pago es uno autorizado por la normativa vigente y cumple, por tanto, con todas las formalidades exigidas por SUNAT y por el OSIPTEL.

La Entidad debe pagar las contraprestaciones pactadas a favor del postor ganador de la buena pro dentro de los quince (15) días calendario siguiente a la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello.

## 20 DOMICILIO PARA NOTIFICACIÓN EN EJECUCIÓN CONTRACTUAL

El postor ganador de la buena pro, consignará un correo electrónico, a donde se le notificará todos los actos y actuaciones recaídos durante la ejecución contractual, como es el caso, entre otros, de ampliación de plazo.


Firmado digitalmente por CASTRO GUZMAN Cesar Humberto FAU 20262221335 hard
Motivo: Soy el autor de este documento
Fecha: 2021.03.19 18:42:09 -05'00'

Sello y firma del área usuaria