TÉRMINOS DE REFERENCIA SERVICIO INTERNET BANDA ANCHA CHSGII

1 OBJETO DEL CONTRATO:

Se requiere contratar el servicio de Internet de Banda Ancha con seguridad gestionada para la Central Hidroeléctrica San Gabán II ubicado en la provincia de Carabaya a 1500 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 de 24 x 7 x 365.

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 96.0% 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 96.0% (en la subestación San Gabán II)
- 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.

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	80 Mbps	
Conexión Remota	Veinte (20) Conexiones Remotas, con punto de Acceso en Perú y con conexión al NAP Perú, optimizado para el trabajo remoto. **Según el punto 9.3.**	
Seguridad Administrativa	Servicio de seguridad administrada con un SLA 24x7 con acceso por el cliente.	
Seguridad Avanzada	Monitoreo de amenazas y nivel de compromiso de la infraestructura. **Según el punto 9.4.**	
Disponibilidad de la solución	Se requiere una disponibilidad de los servicios de internet, y Seguridad del 96.0%	
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. • No se aceptarán enlaces o conexiones inalámbricas y/o radiales. • 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: • Ancho de banda soportado, de al menos 200 Mbps. • Deberá incluir como mínimo (4) interfaces 10/100/1000BaseT, un (01) puertos SFP. Todos los 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	• El backbone de la red local deberá ser redundante en la ciudad de Puno.	

Requerimiento	Valor Mínimo Requerido	Valor Ofertado
buena pro del servicio	• Deberá contar con doble salida internacional a Internet. • Debe tener autorización del Ministerio de Transportes y Comunicaciones para servicio de valor añadido, con cobertura a nivel nacional. • Debe poseer un centro de gestión propio o tercerizado para la atención y solución de averías.	
NAP Perú (Network Access Point)	El postor ganador de la buena pro debe pertenecer al NAP Perú; no se permitirá aquellos postores que formulen tener acceso al NAP a través de un miembro integrante del NAP. Se considerarán miembros del NAP los Postores que cuenten con un enlace propio al NAP Perú activo y 100% operativo, los mismos que deberán ser acreditados con la constancia respectiva presentándola en de su oferta técnica.	
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. • Debe tener una conexión hasta el backbone de Internet entregado mediante enlaces redundantes dentro de su backbone. • Deberá proporcionar un usuario y password de acceso para el cliente al sistema de monitoreo vía web • El protocolo de comunicación será TCP/IP. • El postor ganador de la buena pro del servicio debe contar con los siguientes puntos en su red: ▪ Redundancia en equipos de ruteo en sus instalaciones. ▪ Redundancia en backbone de routers de su red. ▪ Redundancia en los servidores DNS. ▪ Redundancia en los enlaces de Salida Internacional. • 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	Treinta (30) 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 inscripción de nuestros dominios. Estos dominios deberán ser registrables en la rcp.net.pe. 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.	

Requerimiento	Valor Mínimo Requerido	Valor Ofertado
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**.**	
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: - Red de datos en contingencia Site-to-Site entre las dos oficinas (Oficina Administrativa de Puno y Central Hidroeléctrica): - Red administrativa Site-to-Client para trabajadores remotos.	

9.2 Solución de Seguridad Administrada

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

9.2.1 Capacidades

1. Throughput de por lo menos 20 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6.
2. Soporte a por lo menos: 2M conexiones simultáneas; y 135K nuevas conexiones por segundo.
3. Throughput de al menos 7.5 Gbps de VPN IPSec.
4. Estar licenciado para, o soportar sin necesidad de licencia: Túneles de VPN IPSec site-to-site simultáneos; y túneles de clientes VPN IPSec simultáneos.
5. Throughput de al menos 900 Mbps de VPN SSL.
6. Soportar al menos: 100 clientes de VPN SSL simultáneos; 2.2 Gbps de throughput de IPS; 820 Mbps de throughput de Inspección SSL; 3.5 Gbps de throughput de Application Control; 1.8 Mbps de throughput de NGFW; y 1.2 Mbps de throughput de Threat Protection.
7. Permitir gestionar al menos 128 Access Points.
8. Tener al menos dieciséis (16) interfaces 1Gbps RJ45; y cuatro (04) interfaces SFP.
9. Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance con su soporte respectivo.

9.2.2 Requisitos Mínimos de Funcionalidad

a) Características Generales

1. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
2. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
3. Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
4. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
5. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación.
6. La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
7. El dispositivo de protección de red deben soportar: VLANs Tags 802.1q; agregación de enlaces 802.3ad y LACP; Policy based routing y policy based forwarding; encaminamiento de multicast (PIM-SM y PIM-DM); DHCP Relay; DHCP Server; sFlow; Jumbo Frames; y sub-interfaces Ethernet lógicas.

8. Debe ser compatible con NAT dinámica (varios-a-1) y con NAT dinámica (muchos-a-muchos).
9. Debe soportar NAT estática (1-a-1)
10. Debe admitir NAT estática (muchos-a-muchos).
11. Debe ser compatible con NAT estático bidireccional 1-a-1; con la traducción de puertos (PAT); con NAT Origen; y con NAT de destino.
12. Debe soportar NAT de origen y NAT de destino de forma simultánea y en la misma política.
13. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
14. Debe ser compatible con NAT64 y NAT46.
15. Debe implementar el protocolo ECMP.
16. Debe soportar SD-WAN de forma nativa.
17. Debe soportar el balanceo de enlace hash por IP de origen; y por hash de IP de origen y destino.
18. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces.
19. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
20. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
21. Enviar logs a sistemas de gestión externos simultáneamente.
22. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
23. Debe soporta protección contra la suplantación de identidad (anti-spoofing).
24. Implementar la optimización del tráfico entre dos dispositivos.
25. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
26. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3).
27. Soportar OSPF graceful restart.
28. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
29. Para la inspección de datos y visibilidad en línea del tráfico debe soportar modo capa - 2 (L2) y capa - 3 (L3).
30. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
31. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente; en la capa 3; y con al menos 3 dispositivos en el clúster.
32. La configuración de alta disponibilidad debe sincronizar: Sesiones; configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
33. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN; y Tablas FIB.
34. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace.
35. Debe soportar la creación de sistemas virtuales en el mismo equipo.
36. Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
37. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.
38. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
39. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos).
40. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

41. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
42. Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
43. La consola de administración debe soportar como mínimo, inglés, español y portugués.
44. La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.
45. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

b) Control por Política de Firewall

1. Debe soportar controles de zona de seguridad.
2. Debe contar con políticas de control por puerto y protocolo.
3. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
4. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
5. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad.
6. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall.
7. Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
8. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
9. Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
10. Debe soportar el protocolo estándar de la industria VXLAN.
11. La solución debe permitir la implementación sin asistencia de SD-WAN.
12. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
13. La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

c) Control de Aplicación

1. El dispositivo de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
2. Detección de miles de aplicaciones en categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
3. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
4. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.
5. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
6. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.
7. Actualización de la base de firmas de la aplicación de forma automática.
8. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.

9. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
10. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
11. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos.
12. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
13. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
14. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video.
15. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
16. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc.).
17. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
18. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
19. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

d) Prevención de Amenazas

1. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
2. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware).
3. Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
4. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad.
5. 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 y la combinación de todos estos elementos.
6. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos.
7. Debe incluir la protección contra ataques de denegación de servicio.
8. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo; análisis para detectar anomalías de protocolo; desfragmentación IP; re ensamblado de paquetes TCP; y bloqueo de paquetes con formato incorrecto (malformed packets).
9. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc.
10. Detectar y bloquear los escaneos de puertos de origen.
11. Bloquear ataques realizados por gusanos (worms) conocidos.
12. Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
13. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
14. Debe poder crear firmas personalizadas en la interfaz gráfica del producto.
15. Identificar y bloquear la comunicación con redes de bots.
16. Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
17. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.

18. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.
19. Los eventos deben identificar el país que origino la amenaza.
20. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
21. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
22. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad.
23. En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc.) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles.
24. Proporcionar protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).

e) Filtrado de URL

1. Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
2. Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
3. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
4. Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
5. Tener por lo menos 75 categorías de URL.
6. Debe tener la funcionalidad de exclusión de URLs por categoría.
7. Permitir página de bloqueo personalizada.
8. Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
9. Además del Explicit Web Proxy, soportar proxy web transparente.

f) Identificación de Usuarios

1. Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local.
2. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios.
3. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.
4. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios.
5. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.
6. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo).
7. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.

8. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
9. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
10. Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores.

g) QoS Traffic Shaping

1. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
2. Soportar la creación de políticas de QoS y Traffic Shaping: Por dirección de origen; por dirección de destino; por usuario y grupo; y para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
3. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
4. En QoS debe permitir la definición de tráfico con ancho de banda garantizado y con máximo ancho de banda.
5. En QoS debe permitir la definición de colas de prioridad.
6. Soportar marcación de paquetes DiffServ, incluso por aplicación.
7. Soportar la modificación de los valores de DSCP para Diffserv.
8. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
9. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

h) Filtro de Datos

1. Permite la creación de filtros para archivos y datos predefinidos.
2. Los archivos deben ser identificados por tamaño y tipo.
3. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
4. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
5. Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
6. Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.

i) Geo Localización

1. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países.
2. Debe permitir la visualización de los países de origen y destino en los registros de acceso.
3. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

j) VPN

1. Soporte VPN de sitio-a-sitio y cliente-a-sitio; IPSec; y SSL.
2. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512; Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14; Internet Key Exchange (IKEv1 y v2); AES de 128, 192 y 256 (Advanced Encryption Standard).
3. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
4. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
5. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que

facilita el proceso troubleshooting.

6. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
7. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
8. Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
9. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
10. Deberá mantener una conexión segura con el portal durante la sesión.
11. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Nota: Se requiere carta del fabricante validando las características solicitadas del equipo de seguridad.

9.3 Conexión segura para usuarios remotos

Se requiere que un grupo de veinte (20) 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. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Se deberá habilitar la inspección vía TLS para la protección de amenazas avanzadas.
8. 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.
9. 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.

9.4 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/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.

9.5 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. 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).
6. 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).
7. El soporte técnico brindado deberá estar disponible las 24 horas x 7 días durante el periodo del contrato.
8. 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.
9. 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.
10. 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.

11. 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.
12. Reporte de Tickets de problemas y reclamos al servicio de asistencia para el cual deberá de brindar los números telefónicos para su atención 24x7.

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, por lo que realizará 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.

La Especificación de las Pruebas de Aceptación incluirá:

a. El postor ganador de la buena pro alcanzará suficiente detalle de las pruebas a realizar para confirmar que cada uno de los elementos de la oferta adjudicada cumple con los criterios de aceptación; así como suficiente detalle de los datos de prueba que se usarán para ejecutar las Pruebas de Aceptación, y quién será el encargado de producirlos.
b. En cuanto fuera posible, un cronograma sumario de las Pruebas de Aceptación.

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 producto 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

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".

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 Postor.

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 deberá 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. 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.

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:

<table>
<tr><td>A.1</td><td>CAPACIDAD LEGAL</td></tr>
<tr><td></td><td>HABILITACIÓN</td></tr>
<tr><td></td><td>Requisitos:

Autorización o concesión otorgada por el Ministerio de Transportes y Comunicaciones para brindar servicio de telecomunicaciones.

Importante

De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.

Acreditación:

Mediante copia simple de los documentos de autorización que acrediten la habilitación.

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.</td></tr>
<tr><td>A.2</td><td>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</td></tr>
</table>

	Requisitos: 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. 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. 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. 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.

[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".*

	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. En todo caso, el tipo de cambio venta publicado por la SBS será el que se utilizará para estos casos. 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: • Servicio de Internet de 90 Mbps • Servicio de Internet de 100 Mbps • Servicio de Internet de 110 Mbps • Servicio de Internet de 120 Mbps

11 PLAZO DE EJECUCIÓN:

El plazo de ejecución del presente contrato es de 365 días calendario, el mismo que se computa a partir de la puesta en operación del servicio de Internet.

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 la Sub estación San Gabán II, en el cual se encuentra un Dataroom y un rack disponible. Está localizado en el lugar Tiuni, Km. 260 de carretera interoceánica Sur (Juliaca a San Gabán), Provincia: Carabaya, Departamento de Puno. Las coordenadas son: 13°38’48’S, 70°27’46’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:

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

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:

No se aplicarán para este servicio.

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, San Gabán S.A. debe contar con la siguiente documentación:

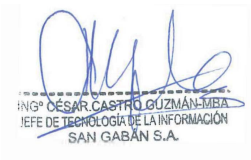
- Informe del funcionario responsable de la División de Tecnologías de la Información de San Gabán S.A., emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- **Reporte del nivel de disponibilidad (físico o digital) del servicio emitida por el postor ganador de la buena pro del servicio de Internet contratado.**

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.

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. Asimismo, señalará un domicilio legal a donde se le notificará los actos que tienen un procedimiento preestablecido de notificación, como es el caso de resolución o nulidad de contrato.



Firmado digitalmente por CASTRO GUZMAN Cesar Humberto FAU 20262221335 hard
Ubicación: Puno
Fecha: 2021.02.16 16:52:09 -05'00'

Sello y firma del área usuaria