 <b>SAT</b> SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	<b>TÉRMINOS DE REFERENCIA</b>	
	15.04.2023	
	<b>SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT</b>	

#### I. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Transmisión de Datos, Internet y Seguridad Gestionada de la Red del SAT

#### II. FINALIDAD PÚBLICA

Poder atender a los ciudadanos en los diferentes locales, con todos los servicios que brinda el SAT

#### III. OBJETIVOS DE LA CONTRATACIÓN

Implementar una red de comunicación privada que permita al Servicio de Administración Tributaria, tener acceso dedicado a internet con un esquema de seguridad perimetral y establecer un canal de comunicación de datos entre su Sede Principal y las oficinas de la entidad ubicadas en la ciudad de Lima, para la transmisión de datos, voz y video sobre IP.

#### IV. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

##### A. Antecedentes:

El SAT, requiere para la realización de sus actividades de una plataforma tecnológica que le permita brindar sus servicios en forma efectiva.

Para esto cuenta actualmente con una red WAN que interconecte sus oficinas en Lima a fin de dinamizar sus procesos internos y compartir la información que se generan entre todos sus grupos de trabajo así también cuenta con una plataforma para la seguridad perimetral para el acceso a Internet.

Como parte de sus planes de desarrollo y mejora, la institución desea modernizar los servicios de telecomunicaciones con los que cuenta actualmente, así como prepararse para la implementación de nuevas aplicaciones que sirvan para el logro de sus objetivos.

##### B. Objetivos

Implementar una red de comunicación privada que permita al Servicio de Administración Tributaria, tener acceso dedicado a internet con un esquema de seguridad perimetral y establecer un canal de comunicación de datos entre su Sede Principal y las oficinas de la entidad ubicadas en la ciudad de Lima para la transmisión de datos, voz y video sobre IP.

##### C. De la persona jurídica que preste el servicio

- El proveedor deberá contar con un centro de operación de red (NOC) local propio o tercerizado. Que será acreditada mediante declaración jurada u otra documentación que demuestre dicha característica, deberá ser entrega para la suscripción del contrato.
- El proveedor deberá contar con un centro de operación de seguridad (SOC) local propio o tercerizado. Que será acreditada mediante declaración jurada u otra documentación que demuestre dicha característica, deberá ser entrega para la suscripción del contrato.
- Contar con un Call Center Técnico y con números de emergencia para reportar los servicios y averías (24x7x365). Que será acreditada mediante declaración jurada u otra documentación que demuestre dicha característica, deberá ser entrega para la suscripción del contrato.



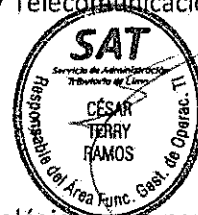
##### D. Requerimientos Generales

- Para el cumplimiento de los objetivos mencionados se requiere la contratación de una empresa de



telecomunicaciones que sea capaz de brindar los servicios solicitados, según los términos de referencia descritas en este documento.

- La relación de sedes que están comprendidas en el presente documento que se detalla en el cuadro N.º 01.
- La empresa contratada brindará el servicio de transmisión de datos entre todas las sedes de la entidad. En el cuadro N.º 01 se describen los anchos de banda de acceso solicitados.
- La empresa contratada brindará el servicio de Internet de la sede Principal del SAT.
- Toda la plataforma que el postor brinde al SAT deberá estar preparada para una migración futura a IPv6.
- El proveedor deberá considerar los servicios de la migración de IPv4 a IPv6 en el momento que lo considere necesario el SAT. Los servicios de dicha migración no deberán generar un costo adicional para la institución.
- El cumplimiento de la obligación de calidad requerida en el servicio, se restringe al cumplimiento de las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Telecomunicaciones y el OSIPTEL.



## E. Servicio de Transmisión de Datos

### Características

- El servicio de transmisión de datos debe estar basado en componentes tecnológicos que permitan el adecuado manejo de Clases de Servicio de extremo a extremo, y soporten el ancho de banda establecido para todas las sedes indicadas en el cuadro N.º 01.
- El medio de última milla debe ser en fibra óptica, así mismo la topología implementada debe permitir la comunicación full mesh.
- El proveedor no podrá emplear el Internet como medio de transporte para la interconexión de las oficinas (ni en los enlaces principales ni en los de contingencia), no se aceptará una solución basada en túneles a través de Internet.
- La infraestructura de red del Postor debe soportar internamente las tecnologías utilizadas para el manejo de Clases de servicio y la diferenciación del tráfico de extremo a extremo por aplicación, diferenciando por lo menos el tráfico de datos, voz y video, dichas clases deben ser administradas por el proveedor del servicio y justificadas con la presentación de una topología de red de cómo se administran dichas clases de servicio de su red.
- Para la conexión de cada sede a la Red Wan debe garantizarse la priorización del tráfico de voz sobre el tráfico de datos.
- Los medios de acceso de última milla para los enlaces principales deberán ser en fibra óptica.
- El nivel de indisponibilidad del servicio de enlaces de datos principales deberá ser como máximo de 4 horas, medido mes a mes, durante el tiempo de duración del contrato. Se debe estipular también 4 horas como máximo de indisponibilidad mensual en todos los enlaces de respaldo, caso contrario se aplicará la penalidad del 5% del costo total mensual del enlace afectado.
- Los enlaces de la sede central y los enlaces de las oficinas descritas en el cuadro N.º 01, debe ser simétrico y 100% garantizado.
- El protocolo utilizado para el transporte de datos deber ser TCP/IP.
- La Red WAN debe soportar el transporte del tráfico de telefonía IP y de otras aplicaciones de misión crítica que serán implementados en el futuro por la Entidad.
- En cada una de las sedes se deben instalar equipos de comunicación (routers), que soporten las velocidades mínimas solicitadas y las funcionalidades técnicas indicadas en el Cuadro 01. Estos equipos deberán ser configurados inicialmente por el Postor y entregados en calidad de alquiler por el tiempo de duración del contrato sin incurrir en costos adicionales a lo estrictamente presentado en su propuesta económica. El proveedor del servicio deberá proporcionar una cuenta de



**SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT**

monitoreo para acceder a todos los equipos routers del servicio brindado y poder ejecutar comandos "show", además deberá proporcionar una cuenta con permisos de escritura en los equipos de seguridad perimetral.

- Los equipos de comunicación para los enlaces (routers, modem, Gateway, conversores, etc.) propuesto en cada Sede deberá, deberá tener un equipo de contingencia, los cuales funcionaran de manera automática es caso de caída del equipo principal.
- El router deberá presentar como mínimo un puerto Ethernet (conector UTP) para la conexión a la red LAN en cada sede.

Los equipos activos como enrutadores, balanceadores de enlace, firewalls y demás componentes que sean instalados en línea o que no disponga de interfaces de by-pass, deberán ser redundantes y no representar un único punto de falla. El postor deberá incorporar los componentes/accesorios necesarios para garantizar la disponibilidad solicitada.

- Se debe considerar, que el postor debe instalar enlaces de respaldo para cada sede y asumir el costo en que incurriese el SAT por el uso del servicio alterno, con el fin de asegurar la continuidad del servicio, los cuales garanticen el ancho de banda al 100% dedicados, simétricos 1:1. estos deberán atenderse desde POP diferentes.
- El servicio debe incluir el router, modem, Gateway, conversores y otros equipos propuestos por el proveedor, en modalidad de alquiler sin incurrir en un costo alguno adicional a lo estrictamente presentado en la propuesta económica del postor.
- Para la sede Principal (Jr. Camana N° 370) el enlace de contingencia debe ser en fibra óptica, siendo el POP de atención y recorrido de la fibra óptica diferente para el enlace de contingencia en comparación con el enlace principal.
- El ancho de banda de los enlaces de contingencia se detalla en el Cuadro N.º 01.
- El backbone de la red del Postor deberá ser redundante en equipos y en nodos.
- Todos los elementos, equipos y accesorios que sean utilizados en la infraestructura de comunicaciones deberán estar debidamente señalizados y acondicionados con la finalidad de evitar la manipulación por personal no autorizado.
- Si fuera necesario realizar obras civiles dentro o fuera de la Entidad, para la instalación de los servicios propuestos, estos deberán ser realizados por el Postor quien asumirá los costos de las obras a realizar.
- Es responsabilidad del proveedor contemplar todas las actividades, dispositivos, componentes y accesorios de datos, relacionados al servicio de datos e internet, hasta el nivel del Router terminal, para el correcto funcionamiento del servicio solicitado sin que esto implique costo adicional para SAT.

Los equipos de enrutamiento deben ser equipos con las siguientes características mínimas:

- Los equipos deberán ser de marcas que se encuentren ligadas a fabricantes de equipos de telecomunicaciones, tener vigencia tecnológica y soporte activo para su mantenimiento respectivo, sin costo alguno para la entidad
- Dicho equipo no deberá ser de propósito genérico (PC o Servidor) sobre el cual pueda instalarse algún sistema operativo base como GNU/Linux, BSD, Sun Solaris, Microsoft Windows, Apple OS-X, etc.
- Deberá contener una interfaz para la conexión al puerto de administración.
- El postor deberá considerar mantener un puerto adicional libre el cual será usada como puerto de diagnóstico para alguna eventualidad en caso de troubleshooting.
- Deberá proveer la cantidad de Interfaces necesarias el cual permita la correcta configuración del equipo los mismos que deberán poseer puertos de 10/100/1000BaseT + 2SFP o puertos de 10/100/1000BaseT + 1 puerto GE Combo.

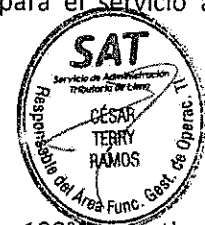


- Routing: BGP, OSPF, RIP v1/v2.
- Disponibilidad: Activo/Activo, Activo/Pasivo, VRRP o HSRP.
- Gestión de tráfico (QoS): Garantizar ancho de banda, máximo ancho de banda, políticas de ingreso de tráfico, priorización de utilización de ancho de banda, marcado DiffServ.
- Opcional: Switching L2: LACP, autenticación de puerto basada en 802.1x.
- Capacidad mínima de memoria RAM de 4GB y FLASH de 1GB.
- Los equipos deberán soportar la versión del protocolo de IPv6 para una migración futura de nuestra red e incluso podrá trabajar en Dual Stack
- El SAT solo brindará dentro de sus instalaciones los espacios adecuados con la infraestructura necesaria (pozo a tierra, ups, aire acondicionado y energía estabilizada) para el servicio a ser instalación por el postor.

## F. Servicio de Internet

### Características

- Enlace de comunicación dedicado como mínimo será de 90 Mbps, simétrico y 100% garantizado el enlace principal y 40 Mbps para el enlace secundario, simétrico y 100% garantizado.
- Los medios de acceso de última milla para el enlace principal y secundario a ofertar deberán ser: Fibra Óptica, garantizando la confiabilidad y disponibilidad del servicio. El nivel de indisponibilidad en cualquiera de los dos enlaces (Principal y Secundario) del servicio deberá ser como máximo de 4 horas, medido mes a mes, durante el tiempo de duración del contrato, caso contrario se aplicará la penalidad del 5% del costo total mensual del enlace afectado.
- El backbone del postor deberán ser necesariamente de 100% fibra óptica.
- El enlace dedicado a Internet deberá ser instalado en la sede central del SAT, Jr. Camana 370 Lima.
- Nivel de compresión 1/1 (Overboking 1:1) desde el router instalado en las oficinas del SAT, hasta el POP internacional (Incluye la última milla, el Backbone Local y el servicio de acceso a Internet hasta el Backbone).
- Se debe instalar un enlace y equipo de contingencia (diferente al principal) a través de fibra óptica, con el mismo ancho de banda, cuyo POP de atención sea diferente al enlace principal y el recorrido de la fibra óptica en la vía pública sea diferente.
- Registro del DNS y asignación de las direcciones IP públicas necesarias (mínimo 32 en IPv4 y IPv6), así como, el respectivo acceso a Internet y la inscripción de dominios en los servidores del ISP.
- Así mismo se requiere de la reserva de un direccionamiento de 32 IPs en IPv4 y 32 IPs en IPv6 dentro de las cuales el SAT podrá solicitar la configuración de algunas de las IPs en Dual Stack según se considere necesario.
- El proveedor deberá contar con un sistema de DNS's redundantes.
- La infraestructura de red local del proveedor deberá ser propia y hasta la salida internacional deberá ser de fibra óptica redundante por rutas físicas diferentes.
- El postor deberá contar con salidas internacionales redundantes geográficamente para garantizar disponibilidad en cuanto al servicio.
- El postor deberá de poseer un ancho de banda hacia el Internet Internacional de 10 Gbps como mínimo.
- El postor deberá contar con dos operadores TIER1 internacionales distintos con rutas físicas diferentes con los que deberá tener conexión directa a través de enlaces de Fibra Óptica. Se aceptará un solo operador TIER1, solo en caso el postor sea TIER1.
- El postor deberá proveer equipos de enrutamiento (routers), los que deberán soportar los anchos de banda indicados. Las características mínimas de los equipos enrutadores, son las siguientes:



**SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT**

- Los equipos deberán ser de marcas que se encuentren ligadas a fabricantes de equipos de telecomunicaciones, tener vigencia tecnológica y soporte activo para su mantenimiento respectivo, sin costo alguno para la entidad.
- Dicho equipo no deberá ser de propósito genérico (PC o Servidor) sobre el cual pueda instalarse algún sistema operativo base como GNU/Linux, BSD, Sun Solaris, Microsoft Windows, Apple OS-X, etc.
- Deberá contener una interfaz para la conexión al puerto de administración.
- El postor deberá considerar mantener un puerto adicional libre el cual será usada como puerto de diagnóstico para alguna eventualidad en caso de troubleshooting.
- Deberá proveer la cantidad de Interfaces necesarias el cual permita la correcta configuración del equipo los mismos que deberán poseer puertos de 10/100/1000BaseT + 2SFP o puertos de 10/100/1000BaseT + 1 puerto GE Combo.
- Routing: BGP, OSPF, RIP v1/v2.
- Disponibilidad: Activo/Activo, Activo/Pasivo, VRRP o HSRP.
- Gestión de tráfico (QoS): Garantizar ancho de banda, máximo ancho de banda, políticas de ingreso de tráfico, priorización de utilización de ancho de banda, marcado DiffServ.
- Opcional: Switching L2: LACP, autenticación de puerto basada en 802.1x.
- Capacidad mínima de memoria RAM de 4GB y FLASH de 1GB.
- Los equipos deberán soportar la versión del protocolo de IPv6 para una migración futura de nuestra red e incluso podrá trabajar en Dual Stack.

**G. Herramienta de Monitoreo de Circuitos**

El proveedor deberá brindar una herramienta de monitoreo avanzado de todos los Circuitos (enlaces principales y contingencia) brindados, los mismos que deberán mostrar la siguiente información:

- Tráfico por aplicación / servicio. Este servicio es sólo para el tráfico en IPv4.
- Tráfico por IP de Origen y Destino
- Consumo del ancho de banda en línea e históricas (mínimo 6 semanas)

Dicha información deberá ser accedida por personal de informática del SAT, desde una interfaz WEB del proveedor.

**H. Herramienta de Monitoreo de equipos de Red**

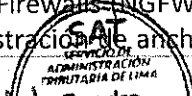
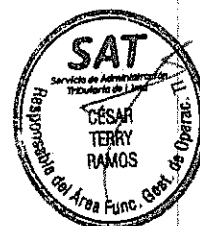
El proveedor deberá brindar un software de monitoreo instalado en el SAT, el mismo que podrá ser instalado en un ambiente virtual que el SAT podrá proveer. Dicha herramienta de monitoreo deberá:

- Contar con las licencias para un total de 200 interfaces o dispositivos de red de distintas marcas como mínimo.
- Poder monitorear la salud de las interfaces, estado de otros recursos del equipo.
- Poder emitir alertas sonoras y posibilidad de envío de mails.
- Contar con un dashboard personalizable y contar con plantillas predeterminadas.

**I. Solución integral de seguridad perimetral de internet**

La Solución integral de seguridad debe incluir lo siguiente:

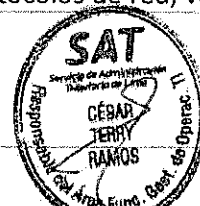
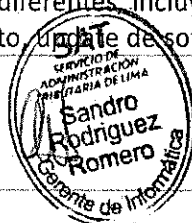
- Protección de la red perimetral con Next Generation Firewalls (NGFW), los cuales tienen funcionalidades de filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL,



IPS, prevención contra amenazas de virus, spyware y malware conocido, así como desconocido o "Zero Day"

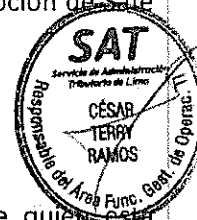
### 11. Firewalls perimetrales

- La solución debe consistir en dos appliances de seguridad de tecnología vigente con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo.
- Los firewalls ofertados deben implementar Disponibilidad en modo Activo-Activo y/o modo Activo-Pasivo.
- La solución de seguridad debe permitir la configuración de clusters en modo de operación en alta disponibilidad (HA), tanto para IPv4 como para IPv6.
- Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa7.
- La solución de seguridad debe estar presente en los últimos 3 reportes de Gartner, en el cuadrante de Líderes para Network Enterprise Firewalls.
- Los firewalls ofertados deben realizar inspección profunda en todos los niveles de la capa OSI (Open System Interconnection) incluido tráfico cifrado.
- El equipo debe permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como direcciones y redes, identificador de usuarios y aplicaciones.
- La solución debe ser capaz de crear políticas basadas en aplicaciones.
- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
- Los firewalls deben detectar y filtrar ataques DoS
- El dispositivo debe ser un equipo de propósito específico. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
- El equipo NGFW debe ser provisto con al menos 8 interfaces de cobre 10/100/1000 Base-T RJ45 de uso dedicado y exclusivo para las zonas que el SAT requiera, las mismas que no podrán ser utilizadas para la configuración del HA del Cluster.
- El equipo NGFW debe ser provisto con al menos 4 interfaces 1Gb SFP (cobre/fibra óptica).
- El equipo NGFW debe contar con 1 (una) interfaz de red 10/100/1000 dedicada para la administración como mínimo.
- El equipo NGFW debe contar con 1 (una) interfaz de tipo consola o similar como mínimo.
- Soporte de 100GB como mínimo para almacenamiento de logs.
- Throughput mínimo de 900 Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando, con logging debidamente activo para cada una de ellas: control de aplicaciones, IPS, Antivirus y protección contra amenazas de día 0 adicionalmente deberá cumplir con Antispyware o Antibot. En caso de que la plataforma de seguridad maneje distintas bases de datos de firmas o distintos métodos de inspección, la medición deberá realizarse con la base de datos y método más estricto de inspección.
- La medición de throughput deberá hacerse con tráfico http como mínimo o de lo contrario en condiciones de tráfico productivo, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.
- Soporte a como mínimo 240,000 sesiones simultaneas por equipo y 48,000 nuevas sesiones por segundo.
- Soportar la creación de políticas por Geolocalización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, mas no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, uso de software, protocolos de red, vozip, audio, vídeo,



proxy, mensajería instantánea, como partición 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 independientes del puerto y protocolo.
- Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, con o sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano.
- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer al menos 3 módulo de los 4 que se presentan a continuación: IPS, Antivirus, Antibot y Anti-Spyware integrados en el propio appliance de Firewall.
- Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware).
- Debido a los Malware hoy en día hay que ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada debe poseer funcionalidades para análisis de Malwares no conocidos incluidas en la propia herramienta.
- El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en la nube donde el archivo será ejecutado y simulado en un ambiente controlado o sandboxing.
- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows 7, Windows 10 y opcional Windows XP.
- Soportar el análisis de archivos ejecutables (EXE), ZIP cuando estos pasan por el protocolo https.
- Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), flash, y archivos java en el ambiente controlado.
- Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad.
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
- Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search este deshabilitada.
- Debe poseer al menos 60 categorías de URLs.
- Debe soportar la creación de categorías URL custom.
- Debe soportar la exclusión de URLs del bloqueo por categoría.
- Debe permitir la customización de la página de bloqueo.
- Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía Ldap, Active Directory.
- Deberá poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- Deberá poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- Deberá poseer integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
- Deberá 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).
- Soporte a autenticación Kerberos.
- Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.
- La solución debe soportar y estar licenciado para la conexión de 1000 usuarios para la conexión VPN, que permita acceder de forma segura a los servicios de red y aplicaciones, desde cualquier destino en Internet basado en el perfil del usuario.
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

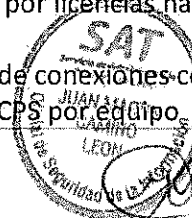
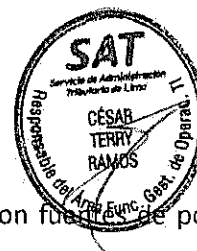


- Permitir aplicar QoS dentro de los túneles VPN.
- Soportar VPN client-to-site pudiendo operar usando el protocolo IPsec o SSL.
- Permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
- La Solución debe permitir una configuración mínima de 1000 usuarios para la conexión VPN de manera básica del equipo.
- Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar determinadas características del equipo y en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso y una combinación de ellas:
  - o Parches instalados en el cliente: según un número de parche determinado, según el nivel de criticidad del parche y proveedor del gestor de parches.
  - o Antimalware instalado en el cliente: validar si se encuentra configurado con protección en tiempo real, si las firmas se encuentran actualizadas en un número determinado de días (personalizable, por ejemplo, firmas actualizadas en los últimos 2 días), validar si se ha realizado un escaneo de malware en el cliente dentro de un número determinado de días (personalizable, por ejemplo, exigir un escaneo el último día), evaluar el proveedor de la solución de antimalware.
  - o Firewall de host: validar si el Firewall del host se encuentra habilitado, validar el proveedor del gestor de firewall.
  - o Cifrado de disco: validar si el cliente tiene instalado un software de cifrado de disco y el proveedor de la solución de cifrado.
  - o Software DLP: validar si el cliente tiene instalado un software de DLP y el proveedor de la solución de DLP.
  - o Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS)
  - o Este control deberá estar disponible al menos para equipos Windows y MacOS, en al menos 1000 dispositivos.
  - o Todos los parámetros indicados deberán poder ser realizados desde la consola gráfica de la plataforma. No se aceptarán configuraciones a través de CLI.

## 12. Capa de SSL Offloading y Balanceo de Carga

### Requerimientos generales:

- La solución debe estar compuesta por dos (02) equipos de tecnología vigente con fuentes de poder redundantes c/u.
- Cada equipo debe tener las siguientes interfaces físicas:
- 2 interfaces que soporten interfaces de fibra de 1 o 10 Gbps, para crecimiento futuro. En esta primera fase del proyecto, no es mandatorio incluir los SFP+ de 10Gbps.
- 8 Interfaces de 1 GbE RJ45
- Throughput: Inicial 6 Gbps por equipo. Debe soportar crecimiento por licencias hasta dos veces más su capacidad inicial.
- Los equipos deben tener capacidad de soportar al menos 1 Millón de conexiones concurrentes L4.
- Capacidad de soportar al menos 176.000 conexiones por segundo CPS por equipo.



- Capacidad de soportar al menos 253.000 L7 RPS por equipo
- Los equipos deben contar con aceleración de Hardware SSL
- Capacidad de conexiones SSL por segundo, con llave de 2048 bit RSA de al menos 7400 CPS por equipo.
- Capacidad de conexiones SSL con llave de 256 bit EC de al menos 4300 CPS por equipo.

**Requerimientos específicos:**

- Debe soportar monitoreo de salud TCP / UDP configurables
- Debe soportar monitoreo de salud HTTP / HTTPS
- La solución debe proveer monitoreo de salud de capa de aplicación predefinidos y configurables
- La solución debe soportar monitoreo de salud compuestos
- La solución debe soportar scripting en el monitoreo de salud
- La solución debe soportar balanceo de carga de L4 a L7 con base en la dirección IP origen o la dirección IP destino
- La solución debe soportar balanceo de carga de L4 a L7 con base en el contenido de la aplicación
- Se deben soportar como mínimo los siguientes algoritmos de balanceo: Round Robin, Fewest Number of Users, Least Amount of Connections, Minimum Misses (hash), Persistent Hash, Response Time, Hash, Server Bandwidth
- La solución debe soportar balanceo de carga con base en pesos relativos asignados a servidores reales
- La solución debe soportar balanceo de carga con base en datos SNMP
- El balanceador de carga debe soportar la funcionalidad de persistencia.
- Se debe soportar persistencia con base en la IP origen.
- Se debe soportar persistencia HTTP/ HTTPS a través de cookies.
- Se debe soportar persistencia a través URL Hash
- Se debe soportar persistencia a través de Header Hash
- Se debe soportar persistencia a través de cualquier encabezado HTTP o parámetro de cuerpo del mensaje
- Debe soportar persistencia a través del SSL ID
- Debe soportar persistencia para protocolo SIP
- Debe soportar persistencia para Windows Terminal Service
- Debe soportar persistencia para WAP/RADIUS
- Debe soportar persistencia general en protocolos TCP/UDP
- La solución debe soportar modificación de los datos del header y cuerpo de los paquetes en HTTP y HTTPS.
- La solución debe soportar modificaciones estándar de HTTP, sin necesidad de scripting.
- Debe soportar modificaciones de contenido general en protocolos TCP/UDP estándar o propietarios.
- La solución debe contar con la capacidad de scripting para tráfico HTTP y no HTTP.
- La solución debe soportar optimización de sesiones TCP y HTTP.
- El balanceador debe soportar aceleración SSL en Hardware.
- Debe soportar terminar la sesión SSL y enviar los paquetes en texto claro o con un cifrado más débil al servidor.
- Debe soportar versiones SSL/TLS seguras.
- Debe soportar ciphers de curvas elípticas y GCM.
- Debe soportar Diffie-Hellman 2048.
- Debe tener la capacidad de limitar o deshabilitar la renegociación de las sesiones de seguridad.
- Debe soportar SSL offloading con autenticación de cliente. La validación del certificado debe soportar



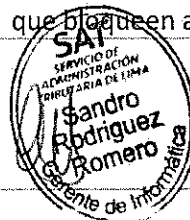
OCSP o CRL/CDP).

- Debe soportar MD5, SHA1, SHA2 (256, 384, 512).
- Debe soportar STARTTLS
- Debe soportar FTPS Offload
- La solución debe soportar compresión HTTP
- Debe soportar políticas de compresión flexibles por browser, tipo de contenido o URL.
- El balanceador de carga debe soportar cache
- La solución debe soportar web caching en compliance con RFC 2616. También tiene que tener la funcionalidad de realizar override sobre el RFC.

### 13. Capa de Web Application Firewall

Requerimientos de la solución:

- La solución de Web Application Firewall (WAF) debe estar compuesta por dos (02) equipos de tecnología vigente con licencia de clúster y throughput inicial licenciado de 200 Mbps, con capacidad de crecimiento hasta 2 Gbps en el mismo hardware por equipo.
- Cada equipo debe de incluir lo siguiente:
  - Fuentes de Poder redundantes
  - 5 interfaces de 10/100/100 RJ-45
  - 2 interfaces con SFP para crecimiento futuro
  - Bypass para al menos 1 par de interfaces de cobre
- La solución debe estar configurada en arquitectura clúster de disponibilidad Activo - Activo con sincronización de reglas entre los equipos y gestión centralizada.
- La solución debe permitir la integración con un sistema DDoS para bloquear ataques basados en capa de aplicación en el perímetro.
- La solución WAF debe configurarse para proteger aplicaciones Web publicadas en internet y aplicaciones web de uso interno accedidas desde la LAN, mediante la inspección en línea del tráfico correspondiente.
- La solución WAF, debe incluir el licenciamiento necesario para la obtención de reportes históricos.
- La solución WAF debe estar certificada por ICSA LABS
- La solución WAF debe proteger contra las amenazas registradas en el OWASP Top Ten.
- La solución WAF debe soportar políticas para combatir técnicas de evasión como:
  - URL-decoding (for example, %XX)
  - Self-referencing paths (that is, use of ../ and encoded equivalents)
  - Path back-references (that is, use of ../ and encoded equivalents)
  - Mixed case
  - Excessive use of whitespace
  - Comment removal (for example, convert DELETE/\*\*/FROM to DELETE FROM)
  - Conversion of (Windows-supported) backslash characters into forward slash characters.
  - Conversion of IIS-specific Unicode encoding (%uXXXX)
  - IIS extended Unicode
  - Virtual directory route – positive folder enforcement
- La solución debe ser capaz de soportar modelos de seguridad positiva y negativa en sus filtros de seguridad.
- La solución debe proteger contra ataques de día cero.
- La solución debe soportar filtros de seguridad que bloqueen ataques de fuerza bruta.
- La solución debe soportar filtros de seguridad que bloqueen ataques a la base de datos.



**SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT**

- La solución debe soportar filtros de seguridad que bloqueen ataques de métodos y parámetros Http.
- La solución debe soportar filtros de seguridad para proteger las sesiones de usuarios remotos.
- La solución debe soportar filtros de seguridad que protejan servicios web.
- La solución debe soportar filtros de seguridad de XML.
- La solución debe soportar filtros Anti-Scraping
- La solución debe reconocer usuarios y debe ser capaz de permitir únicamente tráfico legítimo.
- La solución debe soportar aprendizaje sin manipulación del administrador.
- La solución debe registrar cambios en la configuración.
- El dispositivo debe permitir la personalización de políticas de DoS y prevenir ataques como Slowloris.
- Debe soportar los siguientes modos de operación:
  - Passive – Detección.
  - Active – Detección y prevención.
- El dispositivo debe permitir la actualización de firmas y software desde la consola Web
- La solución debe permitir hacer RFC Enforcement y prevenir ataques de tipo HTTP Request Splitting
- La solución debe permitir URL Access Restrictions
- La solución debe permitir la restricción de parámetros como logical application attack, buffer overflow, zero day attacks, mediante políticas
- La solución debe soportar protección contra ataques de tipo Webscrapping.
- La solución debe incluir una protección antibot, basada en activity tracking y fingerprinting.
- Debe contar con un mecanismo de puntuación, que haga seguimiento a orígenes que estén atacando de forma permanente y que bloquee estos orígenes maliciosos de forma automática.
- Debe permitir el bloqueo por geolocalización, Anonymous proxy, proveedores de servicio satélite y esto se debe actualizar automáticamente.
- La solución debe evitar ataques de tipo cookie poisoning
- La solución debe ser capaz de crear una política de seguridad de forma automática, a través de un proceso de auto aprendizaje.

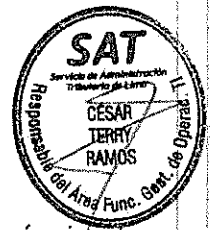
**14. Capa de mitigación de Ataques DDoS**

**Requerimientos generales:**

- La solución para mitigación de ataques DDoS debe constar de un (01) equipo de tecnología vigente y con fuente de poder redundante.
- Capacidad mitigación: La solución debe mitigar ataques DDoS al menos a una tasa mínima de 5 millones de paquetes por segundo, sin bloquear o afectar de manera grave el tráfico legítimo. De igual forma, se exige una capacidad mínima de mitigación de 6 Gbps
- La solución debe soportar un Throughput de al menos de 200 Mbps de tráfico legítimo y debe poder crecer a futuro, al menos 10 veces su capacidad inicial, sin cambiar el hardware, solo a través de licenciamiento.
- El equipo debe tener una latencia bajo ataque menor o igual a 80 micro segundos.
- La solución debe soportar mitigar ataques en IPv4 e IPv6.
- De manera opcional el equipo deberá contar con protección de puertos de cobre con bypass interno.

**Requerimientos específicos:**

- La solución debe proteger contra inundación de anomalías de paquetes. Al menos:
  - Unrecognized L2 Format
  - Incorrect IPv4 Checksum



- Invalid IPv4 Header or Total Length
- Invalid IP Header or Total Length
- Inconsistent IPv6 Headers
- Invalid L4 Header Length
- TTL Equal to 0
- IPv6 Hop Limit Reached
- Unsupported L4 Protocol
- Invalid TCP Flags
- Source or Dest. Address same as Local Host
- Source Address same as Dest Address (Land Attack)

- La solución debe proteger contra ataques DDoS en capa de red. Al menos:
- TCP-SYN floods
- TCP ACK + FIN Flood
- TCP-SYN + ACK floods
- TCP-RESET floods
- TCP fragments flood
- UDP Floods
- UDP Fragmented Floods
- ICMP Floods
- IGMP Floods

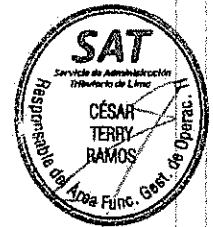


- La solución debe proteger contra ataques DDoS en capa de aplicación. Incluyendo al menos:
- Todo tipo de ataques de tipo reflection, independiente del protocolo capa 7 utilizado.
- Todo tipo de ataques de tipo Amplification, independiente del protocolo capa 7 utilizado.
- DNS Floods
- HTTP Floods
- Low and SLOW
- La solución debe tener protección DDoS originada desde atrás de CDN o proxies.
- La solución debe tener mecanismos de protección para ataques de tipo día cero y ataques conocidos.
- La solución debe tener mecanismo de prevención de falsos positivos DDoS a través de retos y respuestas.
- La solución debe tener protección TCP Out-of-State Flood Attack
- La solución debe tener protección granular para limitar por PPS y Kbps el tráfico hacia un destino con ciertos parámetros definidos.
- Debe proporcionar detección de ataques DoS/DDoS en tiempo real, basado en análisis de comportamiento o estadístico. No se admiten soluciones basadas en umbrales de ningún tipo.
- La solución debe prevenir falsos positivos en la detección causados por flash crowds o aumentos de tráfico súbito, a través de la correlación de parámetros que varíen con la tasa de tráfico con aquellos parámetros que no varían con la tasa de tráfico.
- En fase de protección, la solución debe actuar de forma automática, mitigando el ataque sin intervención humana.
- La solución no debe realizar mitigación a través de rate limits, únicamente se debe bloquear el tráfico que corresponda al ataque, dejando pasar el tráfico legítimo, aun cuando este sea lanzado desde el mismo direccionamiento IP.
- La solución debe detectar y bloquear comportamientos anómalos propios de escaneos de IP y puertos a la red, con el fin de prevenir la enumeración de recursos de la entidad.



**SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT**

- Debe soportar protección DDoS DNS basado en análisis de comportamiento de aplicación
- La solución debe soportar sistemas de protección de DNS Challenge para limitar el tráfico malicioso mediante mecanismos de descarte de paquetes que reduzcan los falsos positivos.
- La solución debe permitir crear listas blancas de subdominios de forma manual o automática.
- La protección de DNS debe ser completamente Stateless, Ingress-Only y no debe realizar conteos de NXDomains.
- La solución debe contar con un mecanismo de protección de ataques DDoS lanzados con herramientas conocidos o que utilicen exploits conocidos. Este mecanismo debe estar basado en una base de datos de firmas que contenga los parámetros necesarios para identificar estos ataques conocidos.
- Las firmas deben actualizarse de forma automática a través de internet durante la duración del soporte
- Al ser la primera línea de defensa, además de ataques DDoS conocidos se debe proteger al menos contra las siguientes vulnerabilidades
  - Web application vulnerabilities
  - Mail server vulnerabilities
  - FTP servers vulnerabilities
  - DNS Vulnerabilities
  - SQL Servers Vulnerabilities
  - VoIP (SIP) vulnerabilities
  - Buffer overflow
- Se debe incluir un servicio de inteligencia de amenazas directamente del equipo de investigación del fabricante, que provea información de los orígenes de ataques de denegación de servicio recientes y permita a la entidad prevenir que dichos orígenes analicen y obtengan información de la red.
- La solución debe contar con un sistema de administración centralizada del tipo virtual appliance que permita instalarse sobre VMware ESXi 5 o superior en la infraestructura de la entidad
- El sistema de administración debe incluir las licencias necesarias para poder tener capacidad completa de realizar cambios y configuraciones de la solución de mitigación de ataques
- El sistema de administración debe soportar Web User interface para toda la configuración del dispositivo
- El sistema de administración debe proveer la opción de personalizar "dashboards" por usuario y por política que muestren información en tiempo-real como: "top attacks view, traffic monitoring view, SLA reports (bandwidth consuming attack) view, etc"
- El sistema de administración debe soportar:
  - Accesos seguros HTTPS, SSH
  - Envío de eventos a través de SYSLOG y SNMP
  - Configuración de la solución a través de scripts
  - RBAC para los administradores de múltiples balanceadores
  - DAP, RADIUS, TACACS y autenticación local
  - Guardar toda la configuración en un servidor remoto
  - REST sobre HTTP
  - Realización de backups por SCP, FTP, SFTP
  - Diagnostic tools como core dumps, archivos de configuración, logs, etc
- El sistema de administración debe permitir la generación de reportes históricos, estos reportes podrán programarse y enviarse de forma automática.
- Debe contar con los siguientes protocolos para enviar los reportes programados: SFTP y SMTP.
- Los siguientes son los formatos de reportes que debe soportar el módulo de reportes históricos: PDF, HTML, CSV, TEXT



Los componentes de las capas solicitadas en I3, I4 y I5 deben ser configuradas por personal técnico del proveedor, certificado por el fabricante. En caso el contratista encuentre los equipos instalados y configurados, entonces no tendrá que configurarlos nuevamente.

#### J. Consideraciones para alta disponibilidad

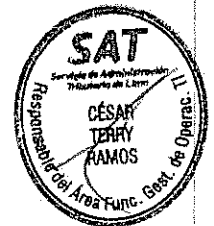
Con la finalidad de mantener la disponibilidad de los componentes solicitados para la solución de los sistemas de Internet, el postor deberá considerar al menos cuatro (04) switches de 24 puertos 10/100/1000BaseT y que incluyan las siguientes características:

- Deberán permitir la funcionalidad de ser agrupados bajo una redundancia del tipo activo-activo.
- Deberán ser equipos de capa 3 que incluya funcionalidades completas de NETFLOW o SFLOW o JFLOW o similar, para que sea incorporado a la herramienta de monitoreo solicitada.

#### K. Equipos de Switch de Red

El proveedor deberá proporcionar Switches de Red Administrables en las oficinas externas del SAT; con el fin de poder gestionar las VLANs, accesos y seguridad respectiva que incluya las características de capa 2 con funcionalidades de NETFLOW o SFLOW o JFLOW o similar, para que sea incorporado a la herramienta de monitoreo del SAT.

Oficinas	Cant. puertos	PoE/PoE+
Agencia Jockey Plaza	48 puertos GE	No
Agencia San Juan de Miraflores	48 puertos GE	No
Deposito Comas1 Santa Ana	24 puertos GE	No
Deposito Ate2	24 puertos GE	No
Deposito de Villa El Salvador	24 puertos GE	No
Deposito de Argentina	144 puertos GE	No
	2 Switchs de 24 puertos GE	Si



En caso el contratista no pueda gestionar los Switches del local de Argentina, por no contar con un servicio de línea dedicada en dicho local, entonces dichos equipos (Argentina) solo contarán con el servicio de garantía y soporte de fábrica, que incluya atención ilimitada del TAC del fabricante 24x7, soporte en línea y el reemplazo de partes/equipo al día siguiente, considerando una vez identificada la necesidad del cambio por parte del fabricante y también del stock del fabricante.

#### L. Consideraciones Generales de toda la solución propuesta

- Con la finalidad de brindar un mejor servicio, El SAT requiere que la administración de los equipos ofrecidos sea de administración Compartida (Solo para el Caso de los equipos Router el proveedor deberá entregar las credenciales a nivel de consulta).
- El SAT podrá solicitar el cambio de la configuración de la Calidad y Servicio de los enlaces MPLS tres (03) veces, solo en caso se requiera, sin que este signifique un costo adicional para el SAT.
- Con la finalidad de poder mantener la administración remota por parte de los administradores de infraestructura de TI del SAT desde cualquier punto de la capital, se requiere de 4 dispositivos inalámbricos portátiles de internet con una capacidad de 8 Gb mensuales.

#### H. Atención por averías o problemas

- Para la atención de averías, problemas con el servicio y problemas con alguno de los equipos ofertados



en la solución, el personal del SAT, deberá comunicarse con el Call Center del Proveedor, con el fin de generar un ticket de atención. El tiempo máximo para que el proveedor entregue el ticket al personal del SAT, será de treinta (30) minutos de generada la llamada. El tiempo máximo mensual será de 4 horas, para dar solución a las averías y problemas ocurridos, los cual será contabilizado a partir de la generación del tickets de atención (Call Center). Dicho ticket será solicitado vía llamada telefónica, para lo cual el postor deberá dar la información sobre los puntos de contacto a la entidad.

- Soporte técnico 24 horas x 7 días a la semana los 365 días del año.
- Se entenderá por avería a una interrupción parcial (Un Circuito Digital o un equipo) o total del servicio, así como a una pérdida de la calidad del mismo.
- Toda actividad o provisión de bienes que tenga que ejecutar el postor para subsanar la avería será sin costo alguno para la Entidad, sólo en el caso sea imputable al postor.
- El postor deberá contar con un centro de servicio instalado de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con lo estipulado en este documento.
- La Entidad solamente reportará las averías técnicas en el servicio a un único número telefónico, el cual será el punto único de contacto con el Proveedor, permitiendo un adecuado control y seguimiento de dichos reportes, debiendo indicar el número telefónico en su propuesta.
- El tiempo de solución máximo para la atención de las averías, será de 4 horas mensuales, contadas desde que la Entidad genera el ticket de atención (reporta el o los incidentes al Centro de Call Center del proveedor).
- La Entidad podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas.
- Las llamadas de servicio se sujetaran a lo siguiente:
- Se podrán efectuar telefónicamente y por correo electrónico (considerándose todas estas formas igualmente válidas, con preferencia por la primera) a las direcciones acordadas entre la Entidad y el postor. En el caso del correo electrónico se enviará con la opción de acuse de recibido.
- Para el caso de la medición del tiempo de solución, solo será tomada como referencia las llamadas ingresadas por vía telefónica.
- La Entidad notificara las anomalías que se presenten incluyendo la siguiente información: fecha, hora, descripción del problema, nombre de la persona que reporta la avería y nombre de la persona que atiende la llamada.

**V. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL (\*)**

No aplica.

**VI. REQUERIMIENTOS DEL PROVEEDOR Y DE SU PERSONAL**

El postor deberá contar con experiencia en contratación de servicios de internet, servicio de línea dedicada, transmisión de datos y servicio de seguridad gestionada

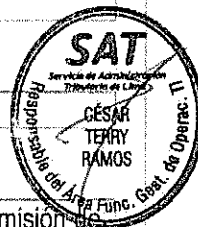
**VII. PLAZO Y LUGAR DE PRESTACIÓN DEL SERVICIO**

El servicio se brindará en los locales indicados en el cuadro N°1.

El servicio iniciará con un plazo de 40 días calendario como máximo, contabilizados a partir día siguiente de suscrito la contratación directa y deberá tener una duración de 6 meses.

**VIII. ENTREGABLES**

El contratista al finalizar el servicio, entregará por mesa de partes del SAT, el informe técnico final donde se pueda verificar la salud de todos los circuitos, consumo de ancho de banda (in Traffic y out Traffic) y un informe que reporte el nivel de todo el servicio propuesto, listando los tickets de avería/problema que se hayan generado durante cada mes, detallando el motivo de la avería, duración de avería y porcentaje de disponibilidad, y un informe mensual de los ataques cibernéticos. Dichos informes deberán ser entregado



como máximo a los 15 días calendario, contados a partir del día siguiente de culminado el mes anterior.

#### IX. CONFORMIDAD DEL SERVICIO

La conformidad de inicio del servicio será otorgada por la Gerencia de Informática, luego el contratista remita por mesa de partes del SAT, el informe técnico final donde se pueda verificar la salud de todos los circuitos, consumo de ancho de banda (in Traffic y out Traffic) y un informe que reporte el nivel de todo el servicio propuesto, listando los tickets de avería/problema que se hayan generado durante cada fin, detallando el motivo de la avería, duración de avería y porcentaje de disponibilidad, y un informe mensual de los ataques cibernéticos

#### X. PENALIDAD POR MORA

Penalidad: De acuerdo al artículo 162 del reglamento de la Ley de Contrataciones del Estado.

#### XI. OTRAS PENALIDADES DISTINTAS A LA PENALIDAD POR MORA

No aplica.

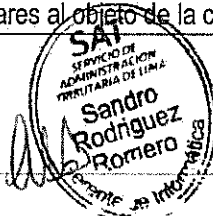
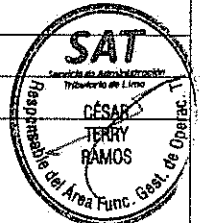
#### XII. FORMA DE PAGO

Pagos mensuales y de acuerdo al servicio brindado. Para gestionar los pagos, el contratista primero deberá remitir por mesa de partes del SAT, un informe mensual donde se pueda verificar la salud de todos los circuitos, consumo de ancho de banda (in Traffic y out Traffic) y un informe mensual que reporte el nivel de todo el servicio propuesto, listando los tickets de avería/problema que se hayan generado durante el periodo del servicio, detallando el motivo de la avería, duración de avería y porcentaje de disponibilidad, y un informe mensual de los ataques cibernéticos. Dichos informes serán revisado por personal de la Gerencia de Informática, quien remitirá (de ser el caso) las observaciones encontradas, para su corrección.

En el caso que el inicio del servicio se realice antes o después del ciclo asignado del contratista, se aceptará el prorrateo correspondiente, el cual se verá reflejado en el primer y último recibo del servicio contratado, sin modificar el importe total del mismo.

#### XIII. REQUISITOS DE CALIFICACIÓN

A	Capacidad Legal
A.1	Habilitación
	<u>Requisitos:</u>  Autorización del Ministerio de Transporte y Comunicaciones para la prestación de servicios de portadora o Acceso a Internet. (El documento debe estar vigente a la presentación de ofertas).  <u>Acreditación:</u>  Copia de la autorización del Ministerio de Transporte y Comunicaciones para la prestación de servicios de portadora o Acceso a Internet. (El documento debe estar vigente a la presentación de ofertas).
B	Experiencia del Postor en la Especialidad
B.1	Facturación
	<u>Requisitos:</u>  El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'000,000.00 (Un millón con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, por la contratación de servicios iguales



o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: Servicio de internet, servicio de línea dedicada, servicio de transmisión de datos y servicio de seguridad gestionada.

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<sup>1</sup>, 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 referido a la Experiencia del Postor en la Especialidad

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

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

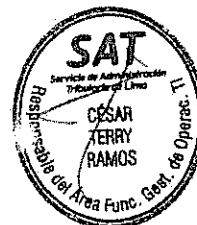
Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones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

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

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo.

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 publicada por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

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



ÁREA USUARIA SOLICITANTE:

GERENCIA DE INFORMÁTICA – ÁREA FUNCIONAL DE GESTIÓN DE OPERACIONES DE TI



NOMBRE: César Edilberto Terry Ramos

CARGO / ROL: Responsable del Área Funcional de Gestión de Operaciones de TI



NOMBRE: Sandro Iván Rodríguez Romero

CARGO / ROL: Gerente de Informática



SERVICIO DE  
ADMINISTRACIÓN  
TRIBUTARIA DE LIMA

## TÉRMINOS DE REFERENCIA

15.04.2023

SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED  
DEL SAT

Cuadro N° 1

ÍTEM	SEDE	Enlace Principal BW / Medio de Acceso	Enlace Secundario BW / Medio de Acceso	DIRECCIÓN DE LA SEDE
1	Sede Principal	30 Mbps / Fibra Óptica	15 Mbps / Fibra Óptica	Jr. Camana 370 Lima (Cercado)
2	Agencia Jockey Plaza	6 Mbps / Fibra Óptica	2 Mbps / Fibra Óptica, Inalámbrico	Av. Javier Prado Este 4200 Centro Financiero C.C. Jockey Plaza Tienda CF- B10A (Santiago de Surco)
3	Agencia San Juan de Miraflores	6 Mbps / Fibra Óptica	2 Mbps / Fibra Óptica, Inalámbrico	Av. De los Héroes 638 A (San Juan de Miraflores)
4	Depósito de Comas	6 Mbps / Fibra Óptica	2 Mbps / Fibra Óptica, Inalámbrico	Av. San Juan Lote 17 - Comas (Ref. Colinda con Urb. Alameda del Pilar)
5	Depósito de Ate	6 Mbps / Fibra Óptica	2 Mbps / Fibra Óptica, Inalámbrico	Lote 43B Lotización Parcelación La Estrella (Ate) (Ref. Colinda con Lidercom y Depósito Derco)
6	Deposito Villa El Salvador	6 Mbps / Fibra Óptica	2 Mbps / Fibra Óptica, Inalámbrico	Lote 4 Mz B Urbanización Pre Urbana tipo Huerta Panamericana Sur. Villa el Salvador
7	Agencia de Argentina	-----	-----	Av. Argentina N° 2926, Lima



