

I. DENOMINACIÓN DE LA CONTRATACIÓN

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

II. FINALIDAD PÚBLICA

Mantener la comunicación permanente, inmediata y sin interrupciones, entre los colaboradores del Servicio de Administración Tributaria (en adelante SAT), que permita el uso de sistemas de información y soluciones que conlleven a incrementar los niveles de eficiencia de la entidad y al logro de los objetivos y metas institucionales, en favor del ciudadano. Asimismo, implementar la mejora continua de nuestros procesos a través de la provisión de recursos tecnológicos adecuados.

III. OBJETIVOS DE LA CONTRATACIÓN

- Contar con el servicio de acceso dedicado a internet con un esquema de seguridad perimetral.
- Implementar una red de comunicación privada que permita establecer un canal de comunicación de datos entre la Sede Principal y las oficinas del SAT, ubicadas en la ciudad de Lima, para la transmisión de datos, voz y video sobre IP.
- Contar con el servicio de seguridad gestionada que permita ejecutar acciones preventivas y correctivas por parte del contratista, a fin de atender requerimientos e incidentes relacionados al servicio.
- Mantener y asegurar la continuidad de los servicios de tecnologías de la información que se brindan en diferentes sedes descentralizadas del SAT.

IV. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

A. ANTECEDENTES:

- El SAT, requiere la contratación de los servicios de interconexión con las sedes descentralizadas del SAT, servicios de Internet y seguridad perimetral gestionada, que permita garantizar el buen desarrollo de las funciones de los colaboradores del SAT y la operatividad de los servicios de tecnologías de la información.
- Para esto se requiere contar con una red WAN que interconecte sus sedes en Lima, a fin de dinamizar sus procesos internos y compartir la información que se genera entre todos sus grupos de trabajo, así también contar con una plataforma para la seguridad perimetral para el acceso a Internet.
- Como parte de sus planes de continuidad y mejora, la institución desea contar con los servicios de telecomunicaciones y seguridad perimetral con los que cuenta actualmente, así como prepararse para la implementación de nuevas aplicaciones que sirvan para el logro de sus objetivos estratégicos.

B. 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.
- El contratista deberá brindar el servicio de transmisión de datos entre las sedes del SAT, cuya relación de sedes están comprendidas en el presente documento que se detalla en el Anexo N.º 01, junto con el ancho de banda mínimo requerido.
- El contratista deberá brindar el servicio de Internet en la sede Principal del SAT.
- Toda la plataforma que el contratista brinde al SAT deberá estar preparada para una migración futura a IPv6.
- El contratista deberá facilitar la configuración de sus equipos en IPv6 o dual stack y brindará un pool de IPs públicas IPv6. En ese sentido, la entidad se encargará de las configuraciones en sus equipos.
- El SAT brindará tomas eléctricas NEMA5-15P para los equipos a instalar.

C. SERVICIO DE TRANSMISIÓN DE DATOS

- El servicio de transmisión de datos deberá estar basado en componentes tecnológicos que permitan el adecuado manejo de Clases de Servicio de extremo a extremo, y deberá soportar el ancho de banda establecido para la sede principal y todas las sedes remotas, indicadas en el Anexo N.º 01; dichas clases de servicio serán establecidas por el SAT antes del inicio de la implementación.
- El contratista no deberá emplear el Internet como medio de transporte para la interconexión de las sedes (ni en los enlaces principales ni en los de contingencia), no se aceptará una solución basada en túneles a través de Internet.
- El medio de acceso de última milla para el enlace principal de la sede central y sedes remotas, deberá ser en fibra óptica, el cual debe garantizar el ancho de banda al 100% dedicados, simétricos 1:1, asimismo, la topología implementada debe permitir la comunicación full mesh. La implementación de fibra óptica podrá ser aérea y/o canalizada, siempre y cuando el contratista cuente con los permisos municipales o de las entidades diferentes al SAT que correspondan.
- El contratista deberá instalar igualmente, enlaces de contingencia para la sede central y sedes remotas, 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 (Punto más cercano de presencia del operador) diferentes, o ruta y POP pasivos diferentes. El ancho de banda de los enlaces de contingencia se detalla en el Anexo N.º 01.
- Para la sede central (Jr. Camaná N° 370), el medio de acceso de última milla para el enlace de contingencia, debe ser en fibra óptica, siendo el POP (Punto más cercano de presencia del operador) de atención y recorrido de la fibra óptica diferente para el enlace de contingencia en comparación con el enlace principal.
- Para las sedes remotas, el medio de acceso de última milla para los enlaces de contingencia, podrán ser por medio alámbrico (fibra) o inalámbrico garantizando la misma confiabilidad y disponibilidad del servicio. Para el caso de enlaces inalámbricos, estos deberán ser bajo una banda licenciada, la misma que no deberá incurrir en trámites ni costos adicionales para la institución.
- 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, estos deberán ser realizados por el contratista, quien asumirá los costos de las obras a realizar.
- Para la instalación de fibra óptica al interior de las sedes (locales), el contratista deberá utilizar materiales como tuberías conduit, uso de los montantes disponibles, uso de las bandejas de metal instaladas sobre el falso techo, y en caso la fibra pase por las oficinas, deberá usarse canaletas.
- Es responsabilidad del contratista 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.
- El postor podrá realizar una visita técnica, en caso necesite dimensionar la longitud de la ruta o canalización a implementar, por lo que no se aceptarán costos adicionales en las tareas de implementación del servicio por desconocimiento de las condiciones existentes.
- Solo en la sede Principal (Jr. Camaná 370) el SAT proporcionará los gabinetes necesarios para la implementación de la solución, pero en el resto de las sedes, el contratista deberá provisionar e instalar los gabinetes necesarios (RU necesario) para la implementación de sus equipos. Los gabinetes del contratista serán solo para los equipos del contratista.
- 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 contratista.
- La infraestructura de red del contratista 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 contratista.

- Para la conexión de cada sede a la Red WAN debe garantizarse la priorización del tráfico de voz sobre el tráfico de datos.
- El contratista debe asegurar un nivel de disponibilidad del servicio de transmisión de datos de todas las sedes indicadas en el Anexo N° 01, por lo que la suma de indisponibilidad del servicio en todas las sedes, no deberá superar las 04 horas por cada periodo mensual, de no cumplir con la disponibilidad se aplicará la penalidad por indisponibilidad del servicio de transmisión de datos.
- No se aplicará penalidad al contratista en casos de desastres naturales o cuando éste demuestre no tener responsabilidad sobre la indisponibilidad del servicio, siempre y cuando el contratista emita, en un plazo no mayor a 24 horas contados a partir de solucionada la avería, un informe detallando las causas y análisis de la avería o problema y concluya no tener responsabilidad. El SAT evaluará y determinará la no penalización por el tiempo de indisponibilidad del servicio.
- El protocolo utilizado para el transporte de datos deber ser TCP/IP.
- En cada una de las sedes se deben instalar equipos de comunicación (routers) de tecnología vigente, es decir, que cuenten con soporte, upgrade y update de seguridad por el fabricante durante el tiempo de servicio; que soporten las velocidades mínimas solicitadas y las funcionalidades técnicas. Estos equipos deberán ser configurados inicialmente por el contratista 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 contratista del servicio deberá proporcionar una cuenta de monitoreo (Lectura) para acceder a todos los equipos routers del servicio brindado y poder ejecutar comandos "show".
- El contratista deberá instalar equipos de comunicación para los enlaces (routers, modem, Gateway, conversores, etc.) de contingencia, en cada sede central y remota, los cuales deberán ser independientes a los equipos de comunicación para los enlaces principales, dichos equipos deberán operar de manera automática en caso de caída del equipo principal, el tráfico deberá ser re direccionado automáticamente vía el enlace de contingencia (respaldo), y luego el tráfico deberá ser restablecido automáticamente al enlace principal cuando se solucione la caída del enlace principal (dicho requerimiento es solo para las sedes que cuentan con ambos enlaces - Principal y contingencia). Se precisa la contingencia de equipo solicitado, no incluye al equipo router, modem, Gateway de la sede (local) de Argentina.
- 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, firewalls y demás componentes que sean instalados en línea o que no dispongan de interfaces de bypass, deberán ser redundantes y no representar un único punto de falla. El postor deberá incorporar todos los componentes/accesorios necesarios para garantizar la alta disponibilidad solicitada.
- El servicio debe incluir el router, modem, Gateway, conversores y otros equipos propuestos por el contratista, en modalidad de alquiler sin incurrir en un costo alguno adicional a lo estrictamente presentado en la propuesta económica del postor.
- Los equipos de enrutamiento deben ser equipos de última generación, de tecnología vigente y con soporte del fabricante y 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.
- El router debe contar con alta 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
- Desde el mismo equipo o desde un sistema externo se debe verificar lógicamente la configuración antes de ser aplicada y con la capacidad de Rollback a la última configuración válida (opcional).
- El personal que realice la instalación de los equipos ruteadores, deberá estar certificado por el fabricante de los equipos. Dicha acreditación deberá ser presentada para la suscripción de contrato, con copia simple de la certificación.

D. SERVICIO DE INTERNET

- El contratista debe brindar un enlace de comunicación dedicado, simétrico y 100% garantizado, con ancho de banda mínimo de 300 Mbps para el enlace principal y 90 Mbps para el enlace de contingencia.
- Los medios de acceso de última milla para el enlace principal y contingencia a ofertar deberán ser: Fibra Óptica, garantizando la confiabilidad y disponibilidad del servicio. La implementación de fibra óptica podrá ser aérea y/o canalizada, siempre y cuando el contratista cuente con los permisos municipales o de las entidades diferentes al SAT que correspondan.
- El contratista debe asegurar un nivel de disponibilidad del servicio de Internet, por lo que la indisponibilidad no deberá superar las 04 horas por cada periodo mensual, durante el tiempo de duración del contrato, de no cumplir con la disponibilidad, se aplicará la penalidad por indisponibilidad del servicio de internet.
- No se aplicará penalidad al contratista en casos de desastres naturales o cuando éste demuestre no tener responsabilidad sobre la indisponibilidad del servicio, siempre y cuando el contratista emita, en un plazo no mayor a 24 horas contados a partir de solucionada la avería, un informe detallando las causas y análisis de la avería o problema y concluya no tener responsabilidad. El SAT evaluará y determinará la no penalización por el tiempo de indisponibilidad del servicio.
- 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. Camaná 370 Lima.
- Nivel de compresión 1/1 (Overbooking 1:1) desde el router instalado en las oficinas del SAT, hasta el POP (Punto más cercano de presencia del operador) internacional (Incluye la última milla, el Backbone Local y el servicio de acceso a Internet hasta el Backbone).
- El contratista deberá instalar un enlace y equipo de contingencia (diferente al principal) a través de fibra óptica, con el mismo ancho de banda, cuyo POP (Punto más cercano de presencia del operador) de atención sea diferente al enlace principal y el recorrido de la fibra óptica en la vía pública sea diferente, también se aceptará contingencia con ruta y POP pasivos diferentes,
- Registro del DNS y asignación de las direcciones IP públicas necesarias (mínimo 32 en IPv4 y 32 en IPv6), así como, el respectivo acceso a Internet y la inscripción de dominios en los servidores del ISP. Como se está solicitando un enlace principal y uno de respaldo (contingencia) en activo pasivo, no es necesario que se brinden 02 rangos de 32



IPs públicas en v4.

- El SAT podrá solicitar la configuración de algunas de las IPs públicas en Dual Stack según se considere necesario. De las 32 IPs en IPv4, 29 son efectivas y las 3 restantes serán para la red, broadcast y equipo de red.
- 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 la mayor 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) con soporte del fabricante, los que deberán soportar los anchos de banda indicados. Las características mínimas de los equipos enrutadores, son las siguientes:
 - 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.
 - Alta 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.
 - 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.
 - Desde el mismo equipo o desde un sistema externo se debe verificar lógicamente la configuración antes de ser aplicada y con la capacidad de Rollback a la última configuración válida (Opcional).
 - El personal que realice la instalación de los equipos ruteadores, deberá estar certificado por el fabricante de los equipos. Dicha acreditación deberá ser presentada para la suscripción de contrato, con copia simple de la certificación.

E. SERVICIO DE MONITOREO DE CIRCUITOS

El contratista 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, poder diferenciar el tráfico http, ftp, ssl, entre otros. 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 contratista. El servicio de Monitoreo de Circuitos deberá ser una plataforma WEB implementada dentro de la infraestructura del contratista, sin la necesidad de instalar ningún componente (hardware) en el SAT.

La cantidad de usuarios con acceso a la plataforma deberá ser como mínimo dos (02) usuarios a la vez.

F. HERRAMIENTA PARA EL MONITOREO DE EQUIPOS DE RED

El contratista deberá entregar e implementar un software o suscripción para el monitoreo de equipos dentro de la plataforma tecnológica del SAT, el mismo que deberá ser instalado en el SAT (por el tiempo que dure el servicio) y podrá ser instalado en un ambiente virtual que el SAT podrá proveer. Dicha herramienta de monitoreo deberá contar con las siguientes características:

- Licencias activas durante todo el tiempo del servicio, para un mínimo de 250 interfaces o dispositivos de red de distintas marcas.
- 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.

El SAT proveerá un ambiente virtualizado en Windows server o Linux, con 8vCPU, 16 GB RAM y un tamaño máximo de 500 GB, donde se procederá a realizar la instalación del software. Asimismo, se indica que el uso de este software de monitoreo de equipos es de uso exclusivo para las actividades del SAT, sin algún otro fin para el contratista.

La solución para monitoreo será administrada y operada por el personal del SAT; sin embargo, en caso de incidentes y/o averías y/o problemas, el contratista deberá brindar el soporte y mantenimiento de la solución.

G. SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL DE INTERNET

La Solución integral de seguridad debe incluir lo siguiente:

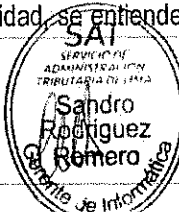
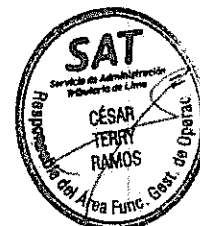
- Protección de la red perimetral con Next Generation Firewalls (NGFW), los cuales tienen funcionalidades de filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware conocido, así como desconocido o "Zero Day"
- Firewall perimetrales
- Balanceadores con WAF
- Capa de mitigación de ataques DDoS
- Protección anti DDoS en nube

G.1. Firewalls perimetrales

1. DESCRIPCIÓN

1.1. Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.

1.2. La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos 2

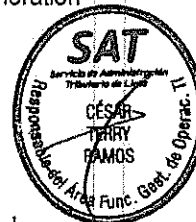


(dos) appliances con las mismas características mínimas mencionadas en estas especificaciones.

- 1.3. El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 8 reportes o en 5 reportes en los últimos 5 años.
- 1.4. El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls
- 1.5. El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
- 1.6. La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- 1.7. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- 1.8. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado. Dicha información se presentará para la firma de contrato.
- 1.9. Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware
- 1.10. Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones, dichos accesos se proporcionarán luego de finalizar la etapa de implementación.
- 1.11. Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución, dichos accesos se proporcionaran luego de finalizar la etapa de implementación.
- 1.12. La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- 1.13. La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.

2. CAPACIDAD

- 2.1. Throughput de Prevención de Amenazas de 2.2 Gbps medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7 o transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad avanzada en DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto



de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

2.2. El equipo debe soportar como mínimo 1 millón sesiones simultaneas y 46 mil nuevas sesiones por segundo, medidos con paquetes en capa 7.

2.3. Debe contar con fuente de poder redundante.

2.5. Disco interno de 120 GB o superior.

2.6. Mínimo 12 interfaces de red 1000 en cobre en formato RJ45. *Las 12 interfaces de red deberá ser auto-negotiation, el mismo que podrá ser seteado manualmente.*

2.7. *Opcional* 4 interfaces de red de 1Gbps en formato SFP para crecimiento, no es necesario incluir transceivers.

2.8. *Opcional* 4 interfaces de red de 10Gbps en formato SFP+ para crecimiento, no es necesario incluir transceivers.

2.9. *Opcional* 2 interfaces de red 1000 en cobre en formato RJ45 y 1 interface de red 10Gbps en formato SFP+ (no es necesario incluir transceiver), estas interfaces deben ser dedicadas para la función de alta disponibilidad.

3. CARACTERÍSTICAS GENERALES

3.1. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.

3.2. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).

3.3. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.

3.4. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.

3.5. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPsec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.

3.6. Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.

3.7. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.

4. ALTA DISPONIBILIDAD

4.1. Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).

4.2. La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.

4.3. Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.

SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	TÉRMINOS DE REFERENCIA	
	09/03/2023	
	SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT	

4.4. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

5. FUNCIONALIDADES DE FIREWALL

5.1. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.

5.2. Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.

5.3. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.

5.4. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).

5.5. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.

5.6. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.

5.7. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

6. DESCIFRADO DE TRÁFICO SSL/TLS

6.1. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.

6.2. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.

6.3. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.

6.4. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.

6.5. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS

6.6. Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).

6.7. Sebe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio

6.8. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.

6.9. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede



producir una falla en el descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

7. PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

7.1. Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.

7.2. Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa

7.3. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)

7.4. Opcional: La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS

7.5. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo

7.6. La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección.

7.7. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing (opcional), Loose Source Routing (opcional), Record Route (opcional).

7.8. Opcional: Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).

7.9. Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

8. CONTROL DE APLICACIONES

8.1. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.

8.2. Opcional: Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.

8.3. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado o deberá contar con una base de datos de reconocimiento de aplicaciones mayores a 8000.

8.4. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.

8.5. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de

expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.

- 8.6. Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- 8.7. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado o deberá contar con una base de datos de reconocimiento de aplicaciones mayores a 8000.
- 8.8. Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante y/o generar firmas para las aplicaciones propietarias a partir de una herramienta provista por el propio fabricante.
- 8.9. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- 8.10. Opcional: Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

9. PREVENCIÓN DE AMENAZAS

- 9.1. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- 9.2. Capacidad de realizar DNS Sinkhole y/o DNS traps para la identificación de equipos comprometidos por spyware en entornos corporativos
- 9.3. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente mientras dure el servicio.
- 9.4. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- 9.5. Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia y/o identificación de malware basadas en Deep Learning (En caso incluya Deep learning, este deberá estar licenciado y por el tiempo que dure el servicio).
- 9.6. Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos. Se precisa que los Sistemas Operativos son Windows y Linux. Asimismo, la plataforma de sandbox pueden ser en nube u on-premise.
- 9.7. Con el objetivo de tener la información de amenazas actualizada, la plataforma deberá ser capaz de actualizar su base de firmas en tiempo real sin afectar el performance del equipo.
- 9.8. Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de

usuarios y la combinación de todos esos ítems.

9.9. Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.

9.10. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.

9.11. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

9.12. Debe soportar la creación de firmas de IPS o Prevención de Amenazas basadas en el formato de Snort.

10. ANALISIS DE MALWARE DE DÍA CERO

10.1. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.

10.2. La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y MacOS como mínimo o también se aceptara la emulación x tipo de archivos o deberá incluir un appliance con dichas características solicitadas

10.3. Deberá ser capaz de analizar 1000 archivos por hora realizando análisis dinámico (es decir, no uso de firmas)

10.4. En caso de tratarse de una plataforma de Sandboxing Cloud, deberá cumplir con los siguientes requerimientos:

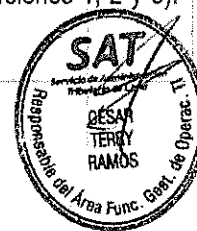
- Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
- Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, ISO 27001, ISO 27017 e ISO 27018.

10.5. En caso de tratarse de una plataforma de Sandboxing On-premise, deberá cumplir con los siguientes requerimientos:

- Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo), con el objetivo de mantener los controles de ciberseguridad en caso de falla de uno de los equipos.
- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows, MacOS, Linux y Android o también es podrá aceptar el análisis por tipos de archivos o también podrá incluir un appliance con dichas características solicitadas.
- Debe admitir topologías de implementación en modo sniffer o en línea (in-line)

10.6. Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.

10.7. El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.



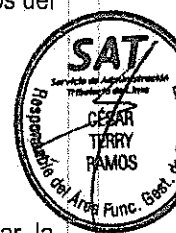
- 10.8. Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
- 10.9. Opcional: Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- 10.10. Permitir la subida de archivos al sandbox de forma manual y vía API.
- 10.11. Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- 10.12. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

11. FILTRO DE CONTENIDO WEB

- 11.1. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- 11.2. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
- 11.3. Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- 11.4. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing.
- 11.5. Debe contar con multi categorías de URL, que permita conocer si una web de una categoría determinada está catalogada como riesgo bajo, medio o alto.
- 11.6. Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder o que prevengan el ingreso de sitios maliciosos y eviten el robo de información personal.
- 11.7. El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing y otros tipos de contenido malicioso.
- 11.8. Debe permitir la creación de categorías personalizadas.
- 11.9. Debe permitir la customización de la página de bloqueo.
- 11.10. Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
- 11.11. Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.

12. IDENTIFICACION DE USUARIOS

- 12.1. Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory y base de datos local.



12.2. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.

12.3. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI para lo cual podrá usar un agente en los controladores de dominio.

12.4. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM u otro similar.

12.5. Opcional: Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.

12.6. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Así mismo deberá soportar añadir un segundo factor de autenticación a través de otros equipos.

12.7. Debe permitir la definición de grupos dinámicos de usuarios.

13. QOS

13.1. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.

13.2. Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.

13.3. El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.

13.4. Soportar marcación de paquetes DSCP.

13.5. Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.

14. VPN

14.1. Soportar VPN Site-to-Site en protocolo IPSec

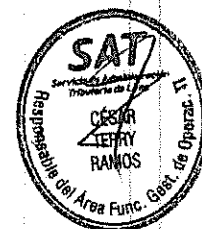
14.2. La VPN site to site debe soportar como mínimo:

- DES y 3DES; AES 128 y 256 (Advanced Encryption Standard)
- Autenticación MD5, SHA-1, SHA-2;
- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- La VPN site to site debe soportar como mínimo:

14.3. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

14.4. Permitir aplicar QoS dentro de los túneles VPN.

14.5. Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.



- 14.6. Permitir la conexión por medio de agente instalado en el sistema operativo.
- 14.7. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- 14.8. Debe permitir definir segmentos de red para ser agregadas de forma automática y/o manual en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- 14.9. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- 14.10. El Split Tunnel debe permitir elegir el tipo de tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio de encriptación (red). Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
- 14.11. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
- Antes del usuario se autentique en la estación;
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
 - Bajo demanda del usuario;
- 14.12. El agente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
- 14.13. La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada. La identificación de equipos colocados en cuarentena se debe basar en un ID inmutable del Cliente VPN, de tal forma que la restricción no pueda ser eludida (por ejemplo, si la cuarentena se hace a una IP, el malware puede modificar la IP del equipo para eludir la cuarentena)
- 14.14. Debe ser posible colocar equipos en cuarentena de forma manual y automática.
- 14.15. Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.
- 14.16 la Solución debe permitir una configuración mínima de 1000 usuario para la conexión VPN de manera básica del equipo.
- 14.17. 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:
- Opcional: Parches instalados en el cliente: según un número de parche determinado, según el nivel de criticidad del parche y proveedor del gestor de parches.
 - Antimalware instalado en el cliente: validar si se encuentra configurado con protección en tiempo real, si las firmas se encuentran actualizadas a la fecha o 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.
 - Firewall de host: validar si el Firewall del host se encuentra habilitado, validar el proveedor del gestor de firewall.
 - Opcional: Cifrado de disco: validar si el cliente tiene instalado un software de cifrado de disco y el proveedor de

la solución de cifrado.

- Opcional: Software DLP: validar si el cliente tiene instalado un software de DLP y el proveedor de la solución de DLP.
- Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro o validación de procesos o archivos específicos.
- Este control deberá estar disponible al menos para equipos Windows y MacOS, en al menos 1000 dispositivos.
- Todos los parámetros indicados deberán poder ser realizados desde la consola gráfica de la plataforma o a través de configuraciones a través de CLI.

15. DETECCIÓN DE DISPOSITIVOS IoT

15.1. La solución deberá contar con un módulo de monitoreo, descubrimiento, identificación y clasificación de dispositivos IoT (Internet de las Cosas) como teléfonos IP, cámaras de vigilancia, consolas de videojuegos, impresoras, dispositivos médicos, equipos industriales, entre otros.

15.2. Por cada dispositivo IoT identificado deberá mostrar la marca del fabricante, tipo de dispositivo, dirección IP, dirección MAC.

15.3. Debe descubrir y mantener un inventario de dispositivos IoT de forma automática, el cual deberá basarse en al menos dos mecanismos de descubrimiento como Firmas, Machine Learning u otro, con el objetivo de brindar mayor fiabilidad. No deberá depender únicamente de la dirección MAC, pues únicamente ese dato no garantiza la correcta identificación.

15.4. Debe identificar dispositivos que posean software o hardware desactualizado y vulnerable, junto con su respectivo identificador CVE.

15.5. Mostrar el nivel de riesgo de cada dispositivo IoT clasificando su severidad por nivel Bajo, Medio, Alto y Crítico o una clasificación equivalente.

15.6. Mostrar los ataques e intentos de ataques hacia los dispositivos IoT.

15.7. Mostrar la actividad en la red de los dispositivos IoT, a nivel de tráfico entrante y saliente. Adicionalmente deberá mostrar la aplicación, protocolo y puerto utilizado para dicha actividad de red.

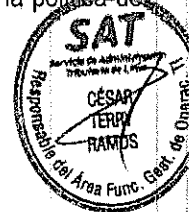
15.8. Opcional: Deberá contar con un mapa geográfico que facilite el monitoreo de la actividad de red del dispositivo IoT.

15.9. Deberá estar integrado nativamente a la plataforma Next Generation Firewall, con el objetivo de que la política de seguridad se pueda realizar directamente en base al Dispositivo IoT, en lugar de usar Direcciones IP.

15.10. Esta funcionalidad deberá poder ser ofrecida sin necesidad de instalar hardware adicional.

16. ADMINISTRACIÓN Y MONITOREO

16.1. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante. En caso, la solución del equipo dedicado a la protección perimetral no puede cumplir el requerimiento, el postor tiene la libertad de añadir un appliance y todo lo necesario (hardware y software) para cumplir con lo solicitado.



- 16.2. Permitir exportar las reglas de seguridad en formato CSV y/o PDF
- 16.3. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- 16.4. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- 16.5. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
- 16.6. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- 16.7. Contar con un módulo o vista que permita comparar y que indique específicamente que cambio se hizo a una política y/o los objetos de dicha política de seguridad respecto a una versión anterior de dicha política.
- 16.8. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- 16.9. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- 16.10. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- 16.11. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;
- 16.12. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- 16.13. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware y/o IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- 16.14. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

G.2 Balanceadores con WAF

Requerimientos generales:

- La solución debe estar compuesta por dos (02) equipos físicos, de tecnología vigente, con soporte del



- fabricante y con fuentes de poder redundantes c/u.
- Cada equipo debe tener las siguientes interfaces físicas:
 - o Un mínimo de dos (02) interfaces que soporten interfaces de fibra de 1 o 10 Gbps, para crecimiento futuro. No es mandatorio incluir los SFP+ de 10Gbps.
 - o De manera opcional puede contar con Interfaces de 1 GbE RJ45, en cuyo caso no deben ser menos de ocho (08)
- Los equipos deben tener al menos 32GB de memoria RAM cada uno.
- Los equipos deben tener al menos un disco SSD de 500 GB cada uno.
- 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 630,000 conexiones por segundo CPS por equipo
- Capacidad de soportar al menos 850,000 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 20,500 CPS por equipo.
- Capacidad de conexiones SSL con llave de 256 bit EC de al menos 12,000 CPS por equipo
- Capacidad de virtualización a través de un Hypervisor dedicado que permite el despliegue de al menos 2 instancias virtuales de ADC.

Estándares de red :

- Como mínimo el equipo debe soportar los siguientes estándares:
 - o Soporte VLAN 802.1q, Vlan tagging
 - o Soporte de 802.3ad para definición de múltiples troncales
 - o Soporte de NAT, SNAT
 - o Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
 - o Soporte de protocolos de enrutamiento BGP, RIP, OSPF

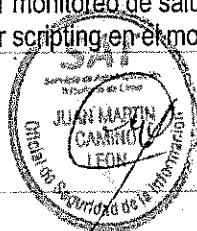
Requerimientos Específicos:

- Balanceo de carga:
 - o La solución debe soportar balanceo de carga de L4 a L7 con base en la dirección IP origen o la dirección IP destino
 - o La solución debe soportar balanceo de carga de L4 a L7 con base en el contenido de la aplicación
 - o La solución debe soportar balanceo de carga con base en pesos relativos asignados a servidores reales
 - o La solución debe soportar balanceo de carga con base en datos SNMP
 - o El balanceador debe soportar aceleración SSL en Hardware.

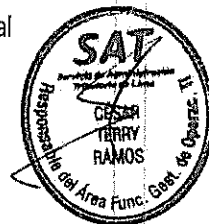
- Algoritmos de balanceo:

Round Robin, Fewest Number of Users (Optional), Least Amount of Connections, Minimum Misses (hash), Persistent Hash, Response Time, Hash, Server Bandwidth

- Monitoreo de salud
 - o Debe soportar monitoreo de salud TCP / UDP configurables
 - o Debe soportar monitoreo de salud HTTP / HTTPS
 - o La solución debe proveer monitoreo de salud de capa de aplicación predefinidos y configurables
 - o La solución debe soportar monitoreo de salud compuestos
 - o La solución debe soportar scripting en el monitoreo de salud



- Opcionalmente, además de lo anteriormente requerido se aceptaran soluciones que cumplan con:
 - ✓ Monitoreo de la salud de los servidores que gestione el equipo de balanceo de tráfico, por medio de:
 - a. Ping.
 - b. Chequeo a nivel de TCP y UDP a puertos específicos
 - c. Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.
 - d. Ejecución de scripts para determinar la respuesta emulando un cliente.
 - e. Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
 - f. Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma
 - g. Monitoreo de aplicaciones de mercado
- Persistencia. 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
 - Opcionalmente, además de lo anteriormente requerido se aceptaran soluciones que cumplan con:
 - ✓ Dirección IP destino
 - ✓ Cookies
 - ✓ Hash
 - ✓ SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
 - ✓ Sesiones SSL
 - ✓ Microsoft Remote Desktop"
- 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.
- La solución debe permitir modificar los códigos de respuesta del servidor al cliente, sin necesidad de scripting.
- La solución debe permitir modificar las URL de respuesta del servidor al cliente, 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.
- El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL)

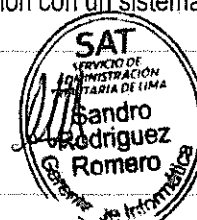
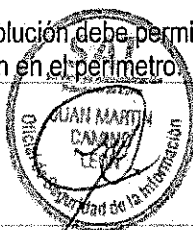
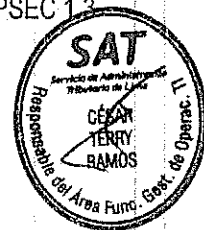
También se aceptarán soluciones que opcionalmente cumplan los siguientes requisitos, además de los anteriormente descritos:

- Permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
- Que tengan arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
- Soporte balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.
- Permita identificar fallos en servicios para redundancia de las aplicaciones.
- Cuenten con reglas que permitan el control de ancho de banda de manera dinámica
- Soporte e incluya Geolocalización, de manera que pueda tomar decisiones basadas en una base de datos de continentes, países y de direcciones IP.
- La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).
- Permita crear persistencia por cualquier valor del paquete por medio de reglas
- Capacidad de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.
- Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:
- Soporte de REST API
- Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.
- Debe soportar el protocolo TDS para balanceo de MSSQL
- Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT
- Debe soportar el protocolo NetFlow (v5)
- Permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código.
- El Equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3

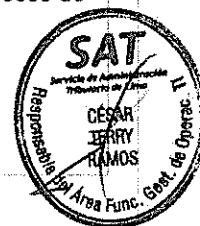
Funcionalidad Web Application Firewall

Requerimientos:

- La funcionalidad de Web Application Firewall debe estar embebida dentro de la solución Balanceadores con WAF.
- Como una funcionalidad opcional, 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 o mediante reverse proxy del tráfico correspondiente.
- La solución WAF, debe incluir el licenciamiento necesario para la obtención de reportes históricos.
- La solución WAF debe estar certificada por ICASA 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
- 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.
- 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 y/o políticas por países.
- La solución debe soportar aprendizaje sin manipulación del administrador.
- La solución debe registrar cambios en la configuración.
- El dispositivo debe permitir 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 Webscraping.
- 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.
- Adicionalmente a las características requeridas, de manera opcional se aceptaran las siguientes:
 - a. Restringir protocolo y versión utilizada
 - b. Multi-byte language encoding
 - c. Validar URL-encoded characters



- d. Restringir la longitud del método de request
- e. Restringir la longitud del URI solicitado
- f. Restringir el número de Encabezados (headers)
- g. Restringir la longitud del nombre de los encabezados
- h. Restringir la longitud del valor de los encabezados
- i. Restringir la longitud del cuerpo (body) de la solicitud
- j. Restringir la longitud del nombre y el valor de las cookies
- k. Restringir el número de cookies
- l. Restringir la longitud del nombre y valor de los parámetros
- m. Restringir el número de parámetros

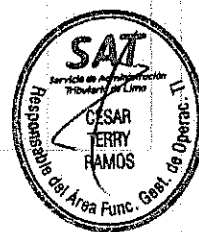
G.3 Capa de mitigación de Ataques DDoS

Requerimientos generales:

- La solución para la mitigación de ataques DDoS debe de constar de un (01) equipo físico, de tecnología vigente y con fuente de poder redundante. Opcionalmente, con el fin de eliminar puntos únicos de falla se aceptaran soluciones con dos (02) equipos físicos de tecnología vigente y con fuente de poder redundante.
- El dispositivo no debe tener límite de sesiones concurrentes al menos bajo condiciones de ataque.
- 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 10 Gbps.
- La solución debe soportar un Throughput de al menos 1 Gbps de tráfico legítimo y debe poder crecer a futuro, a por lo menos 5 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 microsegundos.
- 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.
- Como requerimiento opcional la solución debe tener una capacidad mínima de bulk encryption de 30 Gbps
- A nivel de puertos de conectividad, opcionalmente el equipo podrá contar con los siguiente:
 - o 4 puertos de conectividad de 10G SFP+ integrados
 - o Soporte para puertos de conectividad de 100G/40G/25G/10G QSFP+/QSFP/SFP28/SFP
- Opcionalmente se aceptaran los siguientes umbrales mínimos de gestión de conexiones y paquetes:
 - o Request por segundo Layer 7: un minimo de 2M
 - o Conexiones por segundo Layer 4: un minimo de 1M
 - o Request por Segundo Layer 4 HTTP: un minimo de 15M
 - o Conexiones concurrentes Layer 4: minimo 70M

Requerimientos específicos:

- La solución debe proteger contra inundación de anomalías de paquetes, como mínimo:
 - o Unrecognized L2 Format
 - o Incorrect IPv4 Checksum
 - o Invalid IPv4 Header or Total Length
 - o Invalid IP Header or Total Length
 - o Inconsistent IPv6 Headers
 - o Invalid L4 Header Length
 - o TTL Equal to 0
 - o IPv6 Hop Limit Reached
 - o Unsupported L4 Protocol
 - o 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, como mínimo:
 - 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 utilizado.
 - Todo tipo de ataques de tipo Amplification, independiente del protocolo 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.
- Debe proporcionar detección y mitigación basado en análisis del tráfico para lo cual se aceptara que la solución de anti DDoS debe contar con una segmentación y capacidad de protección segmentada por el Layer 4/7 sobre el cual pueden ocurrir los ataques.
- Como valor agregado a las características requeridas la solución podrá tener una capacidad mínima de procesamiento de tráfico de 90 Gbps en Layer 4 y 60 Gbps Layer 7
- No se admiten soluciones basadas en umbrales y rate-limit.
- Debe mitigar ataques DoS/DDoS de día cero en tiempo real, de forma automática sin intervención humana o a través de la elaboración de firmas por parte del centro de inteligencia del fabricante en base a capturas y análisis de tráfico de ataque generadas por el dispositivo.
- La solución debe prevenir falsos positivos en la detección causados por flash crowds o aumentos de tráfico súbito.
- 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.
- 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.
- De manera opcional debe contar con un sistema de protección basado en comportamiento (Behavioral) que permita la creación de firmas o vectores de ataque de manera dinámica
- 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.
- Se aceptará que la funcionalidad IPS se encuentre integrada en el equipo o también pueda ser atendido mediante un equipo adicional externo.
- Al ser la primera línea de defensa, además de ataques DDoS conocidos se debe proteger al menos contra las siguientes vulnerabilidades:
 - o Web application vulnerabilities
 - o Mail server vulnerabilities
 - o FTP servers vulnerabilities
 - o DNS Vulnerabilities
 - o SQL Servers Vulnerabilities
 - o VoIP (SIP) vulnerabilities
 - o 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.
- Opcionalmente se aceptara que el soporte de RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.
- También de manera opcional se aceptara que la solución soporte Port Misuse, evitando que servicios pasen a través de puertos conocidos que buscan saltar protecciones de Firewall

Consola de Gestión

- La solución debe contar con dos sistemas de administración para el WAF y la solución DDoS, del tipo virtual appliance que permita instalarse sobre VMware ESXi en un servidor provisto por el proveedor que cumpla los siguientes requerimientos mínimos de cómputo: Memoria de 32 GB, 8 vCPU y 500GB de disco SSD.
- La funcionalidad señalada se entiende como opcional, toda vez que en los TDRs se indica que: Para efectos de la gestión de la solución de mitigación de ataques DDoS y de los balanceadores con WAF, también se aceptara como valido soluciones que permitan el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, y por interfaz de administración gráfica basada en Web seguro (HTTPS). En concordancia con lo anterior, se aclara que se están solicitando "DOS SISTEMAS DE ADMINISTRACIÓN", UNO PARA EL WAF Y EL OTRO PARA LA SOLUCIÓN ANTI DDoS. No obstante, si el mismo fabricante tiene la capacidad de poder administrar las dos soluciones desde una sola consola, esto será aceptado puesto que representa un ahorro de recursos de cómputo y complejidad de despliegue para el SAT.
- 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 DDoS y de los balanceadores con WAF descritos en el punto G.2 de este documento.
- La funcionalidad señalada se entiende como opcional, toda vez que en los TDRs se indica que: Para efectos de la gestión de la solución de mitigación de ataques DDoS y de los balanceadores con WAF, también se aceptara como valido soluciones que permitan el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, y por interfaz de administración gráfica basada en Web seguro (HTTPS). En concordancia con lo anterior, se aclara que se están solicitando "DOS SISTEMAS DE ADMINISTRACIÓN", UNO PARA EL WAF Y EL OTRO PARA LA SOLUCIÓN ANTI DDoS. No obstante, si el mismo fabricante tiene la capacidad de poder administrar las dos soluciones desde una sola consola, esto será aceptado puesto que representa un ahorro de recursos de cómputo y complejidad de despliegue para el SAT.
- El sistema de administración debe soportar:
 - o Accesos seguros HTTPS, SSH
 - o Envío de eventos a través de SYSLOG y SNMP
 - o RBAC para los administradores de múltiples balanceadores
 - o RADIUS, y autenticación local



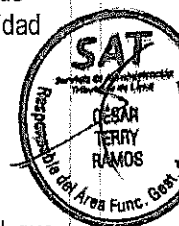
- Guardar toda la configuración en un servidor remoto
- REST sobre HTTP
- Realización de backups
- Para la solución de balanceadores con WAF, el sistema de administración debe permitir visualizar el tiempo de respuesta de peticiones HTTP (S), permitiendo diferenciar el tiempo de respuesta de la aplicación.
- Los siguientes son los formatos de reportes que debe soportar el módulo de reportes históricos, tanto para la solución de mitigación de ataques DDoS como para los Balanceadores con WAF: PDF, CSV.
- Los "DOS SISTEMAS DE ADMINISTRACIÓN", UNO PARA EL WAF Y EL OTRO PARA LA SOLUCIÓN ANTI DDoS, ambos deben permitir la generación de reportes en formatos PDF o CSV. Sin embargo, si el mismo fabricante tiene la capacidad de poder administrar las dos soluciones desde una sola consola, esto será aceptado puesto que representa un ahorro de recursos de cómputo y complejidad de despliegue para el SAT.

Para efectos de la gestión de la solución de mitigación de ataques DDoS y de los balanceadores con WAF también se aceptara como valido la siguiente solución:

- La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
- La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
- La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
- La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
- La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
 - Protocolo SysLog
 - Notificación vía SMTP
 - SNMP versión.2.0 o superior.
- El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
- El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
- La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
- Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
- Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
- Los "DOS SISTEMAS DE ADMINISTRACIÓN", UNO PARA EL WAF Y EL OTRO PARA LA SOLUCIÓN ANTI DDoS. No obstante, si el mismo fabricante tiene la capacidad de poder administrar las dos soluciones desde una sola consola, esto será aceptado puesto que representa un ahorro de recursos de cómputo y complejidad de despliegue para el SAT.

G.4. Servicio de Protección Anti DDoS en nube

El Postor deberá brindar un Servicio de Protección Anti DDoS para el servicio de Internet desde su nube local que proteja del tráfico entrante desde dentro y fuera de la NAP, dicho sistema debe contar con las siguientes características



mínimas:

- El sistema de protección Anti DDoS puede operar bajo una arquitectura en línea o Always-on o bajo una arquitectura de derivación de tráfico o demanda.
- El sistema debe proveer protección contra ataques de denegación de servicio distribuidos y no distribuidos a toda la infraestructura a través de los enlaces contratados.
- Opcionalmente se requiere que el sistema de protección AntiDDoS pueda mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos
- El sistema de protección Anti DDoS debe proteger mínimamente contra ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP.
- Opcionalmente el sistema de protección Anti DDoS debe proteger contra ataques cifrados (HTTPS).
- El sistema de protección Anti DDoS debe contar con firmas que permitan proteger contra ataques conocidos.
- Con el fin de garantizar una protección adecuada que no interrumpa el servicio de internet, aun cuando existan ataques en curso, se requiere que el sistema de protección Anti DDoS sea Stateless (sin límite de sesiones concurrentes).
- El postor debe garantizar la alta disponibilidad del sistema de protección Anti DDoS. En caso la propuesta del postor sea sistema AntiDDoS que opere bajo una arquitectura por derivación de tráfico, la alta disponibilidad sería garantizada por el postor mediante la infraestructura donde se aloje el sistema de protección AntiDDoS, siendo opcional considerar dos equipos en HA.
- El sistema de protección Anti DDoS debe permitir la generación de reportes en formato PDF por parte del postor.
- El sistema de protección Anti DDoS debe mitigar ataques de día cero bajo el despliegue de cualquiera de las dos arquitecturas (Always-on o derivación de tráfico)

Los componentes de las capas solicitadas en G.1, G.2 y G.3 deberán ser configurados por personal del contratista, siempre y cuando el personal este certificado por la marca de los equipos propuestos. Dicha certificación deberá ser presentada como requisito para la firma del contrato.

H. CONSIDERACIONES PARA ALTA DISPONIBILIDAD

Con la finalidad de mantener la alta disponibilidad de los componentes solicitados para la solución de los sistemas de Internet, el contratista deberá considerar al menos cuatro (04) switches nuevos de 24 puertos 10/100/1000BaseT, para el centro de datos principal, que cuenten con soporte vigente de la marca 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.
- Desde el mismo equipo switch o desde un sistema externo se debe verificar lógicamente la configuración antes de ser aplicada y con la capacidad de Rollback a la última configuración válida. En vez de esta característica, también se aceptará el cumplimiento la capacidad de mantener un backup de versiones que permitan realizar rollback a demanda.
- El personal que realice la instalación de los equipos switches, deberá estar certificado por el fabricante de los equipos. Dicha acreditación deberá ser presentada para la suscripción de contrato, con copia simple de la certificación.
- Los equipos a configurar deberán estar en una configuración de virtual chasis lo que permitirá la configuración de dos grupos y cada grupo estarán conformados por 2 switches en configuración activo activo.
- Toda la documentación técnica deberá estar en idioma original de acuerdo al artículo 59 del RLCE y otros documentos como certificados con su debida traducción.
- El personal que realice la instalación de los equipos switches, deberá estar certificado por el fabricante de los equipos. Se aceptará certificaciones a nivel profesional o especialista en la marca propuesta, así como otras certificaciones



emitidas por la marca propuesta. Dicha acreditación deberá ser presentada para la suscripción de contrato, con copia simple de la certificación.

I. EQUIPOS DE SWITCH DE RED

El contratista deberá proporcionar Switches nuevos de Red Administrables en las oficinas externas del SAT, de última generación y que cuenten con el soporte vigente de la marca; con el fin de poder gestionar las VLANs, accesos y seguridad respectiva que incluya las características de capa 3 con funcionalidades de NETFLOW o SFLOW o JFLOW o similar.

Oficinas	Requerimiento de switches
Agencia Jockey Plaza	1 Switch de 48 puertos GE
Agencia San Juan de Miraflores	1 Switch de 48 puertos GE
Deposito Comas	1 Switch de 24 puertos GE
Deposito Ate	1 Switch de 24 puertos GE
Depósito de Villa El Salvador	1 Switch de 24 puertos GE
Depósito de Argentina	3 switches de 48 puertos GE
	2 switches de 48 puertos GE. 1 switch de 24 puertos GE.
	Cada switch debe poseer al menos un puerto de fibra de 1GB multimodo
	2 Switches de 48 puertos GE, PoE/PoE+

Tabla N° 01: cantidad y características de switches

- Los switches deben tener como mínimo la capacidad de packet switching de 126 Gbps y mínimo throughput de 94 Mpps.
- El personal que realice la instalación de los equipos switches, deberá estar certificado por el fabricante de los equipos. Se aceptará certificaciones a nivel profesional o especialista en la marca propuesta, así como otras certificaciones emitidas por la marca propuesta. Dicha acreditación deberá ser presentada para la suscripción de contrato, con copia simple de la certificación.

J. CAPACITACIÓN

- Teniendo en cuenta que los equipos pueden corresponder a diferentes tecnologías y marcas, es necesario que el postor presente un plan de capacitación, el cual deberá ser presentado hasta el día de finalizado el trabajo de implementación de la solución propuesta, previa coordinación con personal de la Gerencia de Informática, para establecer fechas, horarios y lugares de la capacitación.
- El plan deberá comprender la capacitación en la marca de los equipos a implementar, la misma que deberá tener un tiempo no menor de 60 horas en su conjunto, para 4 personas como mínimo, el cual deberá ser aprobado por el SAT, luego de la firma del contrato.
- La capacitación podrá ser en forma presencial y/o virtual. Se aceptará de forma virtual, siempre y cuando se cuente con toda la infraestructura necesaria para el desarrollo del mismo (Manuales, libros, ambientes virtuales para la parte teórica/práctica, entre otros). Dicha capacitación será para todos los equipos WAN, LAN y todos los demás equipos que el contratista incluya en su propuesta.
- La capacitación se coordinará entre el contratista y la entidad; para determinar un horario y fecha lo cual podrá ser en horario fuera de oficina. Además también será coordinados entre la entidad y el postor ganador los puntos a tratar en la capacitación.

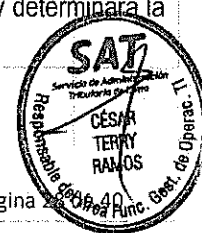
- La capacitación deberá culminar dentro de los primeros 30 días de iniciado el servicio, para lo cual el contratista y los participantes firmarán un Acta de Capacitación.

K. CONSIDERACIONES GENERALES DE TODA LA SOLUCIÓN

- Todos los equipos solicitados deberán ser nuevos, de primer uso y con vigencia tecnológica.
- 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 contratista 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 como mínimo (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 5 dispositivos inalámbricos portátiles de internet con una capacidad mínima de 12 Gb mensuales.
- Toda la documentación técnica deberá estar en idioma original de acuerdo al artículo 59 del RLCE y otros documentos como certificados con su debida traducción.
- Luego de culminado el servicio, el contratista deberá recoger todos los equipos instalados en las sedes (oficinas) del SAT. Dichos equipos no deberán tener más desgaste que el de su uso normal, aceptando que en caso de pérdida, deterioro o robo deberá ser asumido el SAT.
- El SAT brindará todas las facilidades de acceso a las sedes (locales) del SAT y facilidades para realizar los trabajos dentro de las instalaciones de las sedes (locales) del SAT. Dentro de las instalaciones del SAT, el SAT se encargará de gestionar las autorizaciones de ingreso necesarias, de desocupar los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación de los servicios y equipos parte de la propuesta.
- El momento que lo considere necesario durante el servicio, la entidad podrá solicitar la migración de IPv4 a IPv6, para los equipos WAN, LAN y en todos los demás equipos que el contratista incluya en su propuesta. La configuración podrá ser remota y/o presencial según sea el caso y no deberá generar un costo adicional para el SAT.

L. ATENCIÓN POR AVERÍAS O PROBLEMAS

- Para la atención de averías, problemas con el servicio y problemas con alguno de los equipos, el personal del SAT, deberá comunicarse con el Call Center del contratista, con el fin de generar un ticket de atención. El tiempo máximo para que el contratista entregue el ticket al personal del SAT, deberá ser de veinte (20) minutos, después de establecido la comunicación con el personal de soporte.
- El tiempo máximo mensual para dar solución a la suma de todas las averías y problemas ocurridos en dicho periodo mensual 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.
- El tiempo de solución deberá ser máximo de 12 horas cuando sólo un enlace (principal o contingencia) se encuentre sin servicio, de no contar el servicio en ambos enlaces, el tiempo de solución deberá ser máximo de 4 horas.
- Para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará si estas deberán recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que la referida contingencia fue originada por la Entidad o por un hecho ajeno a las partes (casos de desastres naturales y cuando éste demuestre no tener responsabilidad sobre la indisponibilidad del servicio), no se generará ningún tipo de penalidad en contra del contratista ni se le imputará ningún incumplimiento, siempre y cuando el contratista emita en un plazo no mayor a 24 horas contados a partir de solucionada la avería, un informe detallando las causas y análisis de la avería o problema y concluya no tener responsabilidad. El SAT evaluará y determinará la no penalización por el tiempo de indisponibilidad del servicio.



SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	TÉRMINOS DE REFERENCIA	09/03/2023
	SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT	

- 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 contratista, permitiendo un adecuado control y seguimiento de dichos reportes, debiendo indicar el número telefónico al finalizar la etapa de implementación.
- La Entidad podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas.
- En caso de requerir cambio de equipo, el tiempo de solución no deberá exceder las 24 horas para la sede central y 48 horas para las sedes remotas, y en caso de cambio de repuesto, no deberá exceder las 7 horas para la sede central y 48 horas para las sedes remotas. Los plazos de tiempo para el caso de cambio equipo y cambio de repuesto, serán efectivos siempre y cuando los servicios de contingencia (del servicio con avería o problema) este activado y funcionando de acuerdo a lo solicitado en los TDR. *Caso contrario, el tiempo de solución seguirá siendo de 4 horas.*
- Se aceptará un tiempo de solución máximo de 12 horas, para la solución de averías o problemas de degradación del servicio en todas las sedes.
- Se precisa que, 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.
- Las llamadas de servicio se sujetarán 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. En caso no se reciba el acuse recibo, entonces luego que el personal del SAT envíe el correo, el personal del contratista tendrá como máximo 30 minutos para contactarse con el personal del SAT y remitir el número del ticket.
- También se podrá reportar las averías mediante portal web del contratista, sin embargo, dicho portal deberá permitirle al personal del SAT, hacer seguimiento de los tickets, estado de las averías y verificar el tiempo transcurridos.
- La Entidad notificará 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.
- El postor deberá entregar a la Entidad, una nómina del personal técnico autorizado a realizar labores de mantenimiento en las sedes bajo contrato y dicha nómina será presentada a la entidad, siempre y cuando se tenga que realizar trabajos dentro de los locales del SAT. Dicha nómina deberá ser actualizada cuando se produzcan cambios.
- Toda la documentación técnica deberá estar en idioma original de acuerdo al artículo 59 del RLCE y otros documentos como certificados con su debida traducción.

M. INSPECCIÓN Y PRUEBAS

- El contratista y el personal correspondiente de la Entidad, una vez terminada la instalación, realizarán en forma conjunta los procedimientos de inspección y pruebas sobre la infraestructura y equipos instalados, de tal forma que le permita a la Entidad establecer que los servicios serán brindados de conformidad con lo requerido en este documento y en la propuesta del postor.



- Como parte de la inspección y pruebas, el contratista deberá presentar:
 - Plan del proyecto, con la relación de actividades involucradas será presentadas una vez terminada la instalación de los equipos.
 - El detalle de las pruebas a realizar para confirmar que cada uno de los elementos de la oferta cumpla con lo requerido.
 - El cronograma de pruebas y la puesta en operación del servicio.
 - Las pruebas se realizarán en los lugares de instalación. Los costos que demanden las mismas, no implicarán en ningún caso reconocimiento de gastos por parte de la Entidad y deberán ser provistos por el postor. La omisión en la oferta de algún producto que al momento de las pruebas resulte necesario para la provisión de los servicios, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al postor a proveerlo sin cargo alguno.
 - En esta etapa el postor deberá entregar los números de emergencias para reportar los servicios y averías 24x7x365 de su Call Center Técnico.
- Una vez realizados los procedimientos de inspección y pruebas a conformidad de la Entidad y el contratista presente los entregables solicitados, se levantará un Acta de culminación de la implementación del servicio y puesta en producción.

N. CONFIDENCIALIDAD

El postor deberá mantener un contrato de confidencialidad sobre toda la información del SAT, no pudiendo ser compartida bajo ninguna circunstancia sin la autorización previa por parte de la institución.

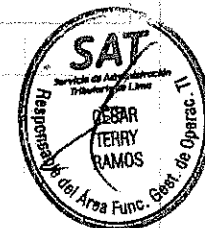
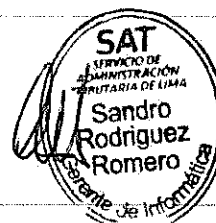
La obligación de confidencialidad no es aplicable en los siguientes supuestos:

- Cuando la información en cuestión haya sido de difusión o acceso público;
- Cuando la información en cuestión haya sido publicada antes de haber sido puesta a disposición del postor;
- Cuando la información en cuestión ya obre en poder del postor y no esté sujeta a cualquier otro impedimento o restricción que le haya sido puesto de manifiesto;
- Cuando la información en cuestión haya sido recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato;
- Cuando la información en cuestión haya sido independientemente desarrollada por el postor, siempre que no se hubiese utilizado para ello otra información confidencial; o
- Cuando la información en cuestión deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden.

O. DOCUMENTACIÓN ADICIONAL

- Información técnica de los equipos que forman parte de los servicios ofertados, que evidencien que los mismos cumplen totalmente con lo requerido. La información técnica solicitada es sobre los equipos ofertados por el postor (datasheets y/o guías de implementación y/o guías de diseños y/u otros documentos del fabricante y/o carta del fabricante). Dicha información deberá ser presentado para la firma del contrato.
- Descripción de otros componentes parte del servicio, como licencias, software y sub servicios necesarios para asegurar el nivel de servicio requerido en las especificaciones técnicas. Dicha documentación deberá ser presentada para la suscripción del contrato. Toda la documentación técnica deberá estar en idioma original de acuerdo al artículo 59 del RLCE y otros documentos como certificados con su debida traducción.

V. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL (*)



No aplica.

VI. REQUERIMIENTOS DEL PROVEEDOR Y DE SU PERSONAL

- El proveedor deberá contar con un centro de operación de red (NOC) local propio o tercerizado, esto será acreditado con tan solo la presentación del (Anexo 3 de las Bases – Cumplimiento de los Términos de Referencia), sin la necesidad de acreditar otro documento adicional.
- El proveedor y/o contratista deberá contar con un centro de operación de seguridad (SOC) local propio o tercerizado, esto será acreditado con tan solo la presentación del (Anexo 3 de las Bases– Cumplimiento de los Términos de Referencia), sin la necesidad de acreditar otro documento adicional.
- El proveedor y/o contratista deberá contar con un Call Center Técnico y con números de emergencia para reportar los servicios y averías (24x7x365), esto será acreditado para la suscripción del contrato mediante una carta; mencionado que cuenta con un Call Center Técnico con los respectivos números de emergencia para reportar los servicios y averías.
- Para el cumplimiento de performance del equipo firewall solicitado el punto Firewalls perimetrales (Capacidad), el contratista para la suscripción del contrato, deberá presentar una carta con el link (portal web) o presentar copia del datasheets o documento del fabricante en idioma original, con información del fabricante que respalde el cumplimiento del performance solicitado
- El contratista deberá cumplir con las disposiciones emitidas por el gobierno nacional en el ámbito del estado de la Emergencia Sanitaria a nivel nacional y medidas dictadas en prevención y control del COVID-19, protocolos y disposiciones del SAT, protocolos sanitarios y demás disposiciones que dicten los sectores y autoridades competentes.
- En caso que el personal del contratista necesite ingresar a lo locales del SAT, deberá remitir por correo electrónico el SCTR vigente y completar la ficha sintomatológica del SAT.

VII. PLAZO Y LUGAR DE PRESTACIÓN DEL SERVICIO

El plazo para la implementación e inicio del servicio, no debe exceder los cien (100) días calendario, contabilizados a partir del día siguiente de suscrito el contrato.

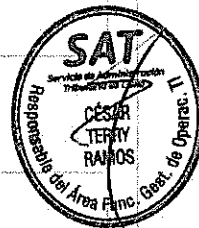
El servicio se brindará en los locales indicados en el Anexo N°1.

El servicio tendrá una duración de treinta y seis (36) meses y deberá de iniciar a partir del día siguiente de la firma del Acta de culminación de la implementación del servicio y puesta en producción.

VIII. ENTREGABLES

Por la implementación del servicio:

- Para el servicio de interconexión de datos, el contratista deberá entregar un plano en Autocad a escala, con todas las rutas y/o enlaces inalámbricos, de todos los accesos de última milla para cada sede que cuenta con principal y contingencia, con el recorrido desde cada POP (Punto más cercano de presencia del operador); la entrega de planos corresponde a todos los enlaces principales y de contingencia, los mismos que serán entregados al término de la implementación del servicio, con el Acta de Culminación de la Implementación del Servicio y Puesta en Producción. Toda información que se solicite como los planos y manuales debe ser por un CD, DVD o USB. Para el caso, que los



enlaces de contingencias sean con un medio inalámbrico, no será necesario presentar plano.

- Para el servicio de internet, el contratista deberá entregar un plano con todas las rutas los accesos de última milla (principal y contingencia), con el recorrido desde cada POP (Punto más cercano de presencia del operador); serán entregados al término de la implementación del servicio, con el Acta de Culminación de la Implementación del Servicio y Puesta en Producción. Toda información que se solicite como los planos y manuales debe ser por un CD, DVD o USB.
- Para el servicio de interconexión de datos, el contratista deberá presentar una topología de red, especificando cómo se administran las clases de servicio de su red. Dicha documentación deberá presentarse con al Acta de Culminación de la Implementación del Servicio y Puesta en Producción.
- Para el servicio de interconexión de datos e internet, el contratista deberá proporcionar información con respecto a la tecnología utilizada, así como también el diagrama respectivo del servicio a brindar. Dicha información deberá ser presentada conjuntamente con el Acta de Culminación de la Implementación del Servicio y Puesta en Producción.
- El contratista deberá entregar un informe final con los detalles técnicos y de infraestructura de telecomunicaciones implementados en el SAT. Dicha información deberá ser presentada conjuntamente con el Acta de Culminación de la Implementación del Servicio y Puesta en Producción.
- Diagrama de la arquitectura (interconexión, redes, protocolos, etc.) de la solución propuesta. Dicha información deberá ser presentada conjuntamente con el Acta de Culminación de la Implementación del Servicio y Puesta en Producción.

Por la ejecución del servicio y soporte técnico

El contratista deberá hacer la entrega por Mesa de Partes del SAT, una carta donde se sustente los informes mensuales. Los informes mensuales del contratista, deberán ser remitidos por mesa de partes del SAT, hasta diez (10) días calendario, luego de culminado cada periodo mensual.

IX. CONFORMIDAD DEL SERVICIO

- La conformidad de inicio del servicio será otorgada por la Gerencia de Informática, luego de firmada el acta de culminación de la implementación del servicio y puesta en producción.
- La conformidad para el primer mes de servicio, debe incluir el Acta de Capacitación.
- La conformidad mensual será otorgada, luego que el contratista remita por mesa de partes del SAT (hasta 10 días calendario, luego de culminado cada periodo mensual), un informe mensual donde se pueda verificar la salud de todos los circuitos instalados, consumo de ancho de banda (in Traffic y out Traffic), un informe que reporte el nivel de todo el servicio propuesto, listando los tickets de avería/problema que se hayan generado durante el mes, detallando el motivo de la avería, duración de avería y porcentaje de disponibilidad, y un informe de los ataques cibernéticos.
- Respecto a los switches, solo será necesario informar el detalle de los tickets de las averías o problemas reportados en el mes.
- Dicho informe será revisado por personal de la Gerencia de Informática, quien remitirá (de ser el caso) las observaciones encontradas, para su corrección.

X. PENALIDAD POR MORA

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



SATSERVICIO DE
ADMINISTRACIÓN
TRIBUTARIA DE LIMA**TÉRMINOS DE REFERENCIA**

09/03/2023

**SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED
DEL SAT****XI. OTRAS PENALIDADES DISTINTAS A LA PENALIDAD POR MORA****Penalidad por indisponibilidad del servicio y tiempo de solución soporte técnico.**

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	La penalidad será aplicable ante el incumplimiento de la disponibilidad mínima mensual de los servicios indicados en el Anexo N° 02; y por el incumplimiento del tiempo de solución de averías.	Las penalidades se aplicarán de acuerdo al incumplimiento indicado en la tabla de penalidad aplicable.	El Personal designado por la Gerencia de Informática del SAT al advertir el incumplimiento, levantará un Acta, el cual será comunicado vía correo electrónico al Contratista con copia al personal del Área Funcional de Logística, detallando los incumplimientos, a fin que se realice el cálculo de penalidades correspondiente.

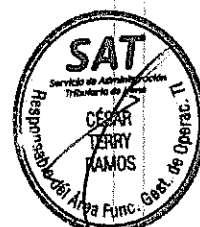
Tabla N° 02: Procedimiento de aplicación de penalidad

Estas penalidades serán aplicables después de la etapa de implementación del servicio citado.

El SAT realizará el respectivo Informe Técnico para el contratista, para que realice su descargo en un plazo máximo de 05 días calendario y determinará, de ser el caso, la imposición de la sanción.

Incumplimiento de los tiempos máximos de disponibilidad del servicio y solución de averías	% de la renta mensual del servicio involucrado
Menor o igual a 4 horas	2%
Mayor a 4 horas y menor o igual a 8 horas	4 %
Mayor a 8 horas y menor o igual a 24 horas	8%

Tabla N° 03: Penalidad aplicable.



El incumplimiento de los tiempos máximos de disponibilidad del servicio y solución de averías, se refiere al tiempo que el contratista excede en solucionar las averías o restablecer los servicios durante el periodo mensual, en comparación con los tiempos máximos estipulados para la solución de cada servicio. Dicho tiempo, corresponde a la sumatoria de todos los minutos durante los cuales la entidad no tuvo la disponibilidad del servicio de cualquier sede o la demora en la solución de averías, siendo estos minutos acumulables en forma mensual.

El contratista deberá remitir los costos unitarios del servicio de acuerdo al formato indicado en el Anexo N° 02, para la firma del contrato.

No se contabilizará en el tiempo de no disponibilidad, las interrupciones de servicio que pudieran producirse por causas imputables a la entidad o terceros.

XII. FORMA DE PAGO

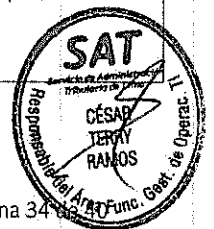
Pago mensual. Para gestionar el pago mensual, el contratista primero deberá remitir por mesa de partes del SAT, un



informe mensual donde se pueda verificar la salud de todos los circuitos instalados, 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 el mes, detallando el motivo de la avería, duración de avería y porcentaje de disponibilidad, y un informe de los ataques cibernéticos. Dicho informe será revisado por personal de la Gerencia de Informática, quien remitirá (de ser el caso) las observaciones encontradas, para su corrección.

XIII. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<p><u>Requisitos:</u></p> <p>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).</p> <p><u>Acreditación:</u></p> <p>Copia de la autorización del Ministerio de Transporte y Comunicaciones para la prestación de servicios de portadora o Acceso a Internet. También se aceptará copia del oficio emitido por el Ministerio de Transporte y Comunicaciones, donde se señale las concesiones y/o autorizaciones vigentes que mantiene la empresa de telecomunicaciones, así como el cuadro de Registro de Valor Añadido (registro para brindar servicio de conmutación por paquetes, denominación de internet), extraído de la web del MTC, donde se pueda evidenciar la habilitación para brindar el servicio solicitado (El documento debe estar vigente a la presentación de ofertas).</p>
B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	CALIFICACIONES DEL PERSONAL CLAVE
B.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u> 01 Jefe de Proyecto</p> <p>Titulado en Ingeniería de Sistemas o Ingeniería de Telecomunicaciones o Ingeniería Informática o Ingeniería Electrónica, del personal clave requerido como jefe de proyecto.</p> <p><u>Acreditación:</u></p> <p>El TÍTULO PROFESIONAL será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En caso el TÍTULO PROFESIONAL no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.1.2	CAPACITACIÓN
	<p><u>Requisitos:</u> 01 Jefe de Proyecto</p> <p>90 horas lectivas, en curso(s) o especialización(es) en gerencia de proyectos y/o dirección de proyectos del personal clave requerido como jefe de proyecto.</p>



SATSERVICIO DE
ADMINISTRACIÓN
TRIBUTARIA DE LIMA**TÉRMINOS DE REFERENCIA**

09/03/2023

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

Se acreditará con copia simple de constancias y/o certificados.

Importante

Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.

B.2**EXPERIENCIA DEL PERSONAL CLAVE**Requisitos: 01 Jefe de Proyecto

Mínimo 03 años en servicios de jefe de proyectos, en implementación de proyectos de internet y/o enlaces de datos y/o de ciberseguridad y/o transmisión de datos, del personal clave requerido como jefe de proyecto.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

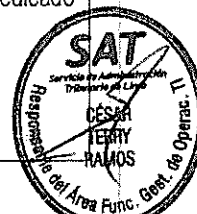
Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

C**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/. 3'000,000.00 (Tres millones con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: Servicio de internet, servicio de línea dedicada, servicio de transmisión de datos y servicio de seguridad gestionada, servicio de internet en general, servicio de Acceso a internet, Servicio de Red de transmisión de datos, Servicio de transmisión de datos por fibra óptica, servicio de Interconexión, servicio de Enlace de Datos, Servicio de ancho de Banda, Servicio de Interconexión de datos, Internet y Transmisión de Datos, Servicio de Acceso dedicado a internet, Servicio de Enlace dedicado a internet, Transmisión de voz y datos.



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 pago¹, 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 durante los ocho (8) años anteriores 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 otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo correspondiente.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 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".



SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	TÉRMINOS DE REFERENCIA	
	09/03/2023	
	SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT	

Importante

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

Importante

- Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.
- El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.
- Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.

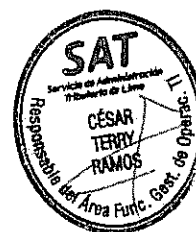


XIV. ANEXOS

ANEXO N° 01

Tabla N° 04

ITEM	SEDE	Enlace Principal BW / Medio de Acceso	Enlace contingencia BW / Medio de Acceso	DIRECCIÓN DE LA SEDE
1	Sede Principal	150 Mbps / Fibra Óptica	30 Mbps / Fibra Óptica	Jr. Camaná 370 Lima (Cercado)
2	Agencia Jockey Plaza	30 Mbps / Fibra Óptica	6 Mbps / Fibra Óptica o Inalámbrico	Av. Javier Prado Este 4200 Centro Financiero C.C. Jockey Plaza Tienda CF-B10A (Santiago de Surco)
3	Agencia San Juan de Miraflores	30 Mbps / Fibra Óptica	6 Mbps / Fibra Óptica o Inalámbrico	Av. De los Héroes 638 A (San Juan de Miraflores)
4	Depósito de Comas	30 Mbps / Fibra Óptica	6 Mbps / Fibra Óptica o Inalámbrico	Av. San Juan Lote 17 - Comas (Ref. Colinda con Urb. Alameda del Pilar)
5	Depósito de Ate	30 Mbps / Fibra Óptica	6 Mbps / Fibra Óptica o Inalámbrico	Lote 43B y 44B Lotización Parcelación La Estrella (Ate) (Ref. Colinda con Lidercom y Deposito Derco)
6	Deposito Villa El Salvador	30 Mbps / Fibra Óptica	6 Mbps / Fibra Óptica o Inalámbrico	Lote 4 Mz B Urbanización Pre Urbana tipo Huerta Panamericana Sur. Villa el Salvador
7	Agencia de Argentina	60 Mbps / Fibra Óptica	-----	Av. Argentina N° 2926, Lima

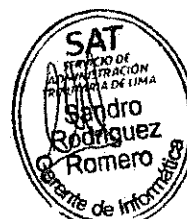


SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	TÉRMINOS DE REFERENCIA	09/03/2023
	SERVICIO DE TRANSMISIÓN DE DATOS, INTERNET Y SEGURIDAD GESTIONADA DE LA RED DEL SAT	

ANEXO N° 02

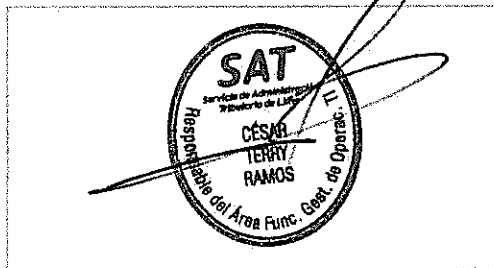
Listado de servicios a requerir costos unitarios

- Servicio de Internet Camaná - Enlace Principal
- Servicio de Internet Camaná - Enlace Contingencia
- Servicio de Firewalls Perimetral - Principal
- Servicio de Firewalls Perimetral - Contingencia
- Servicio de Balanceadores con WAF - Principal
- Servicio de Balanceadores con WAF - Contingencia
- Servicio de Capa de mitigación de ataques DDoS
- Servicio de Protección Anti DDoS en la nube
- Servicio de Transmisión de Datos Cabecera Camaná - Enlace Principal
- Servicio de Transmisión de Datos Cabecera Camaná - Enlace Contingencia
- Servicio de Transmisión de Datos Jockey Plaza - Enlace Principal
- Servicio de Transmisión de Datos Jockey Plaza - Enlace Contingencia
- Servicio de Transmisión de Datos San Juan de Miraflores - Enlace Principal
- Servicio de Transmisión de Datos San Juan de Miraflores - Enlace Contingencia
- Servicio de Transmisión de Datos Argentina
- Servicio de Transmisión de Datos Ate - Enlace Principal
- Servicio de Transmisión de Datos Ate - Enlace Contingencia
- Servicio de Transmisión de Datos Comas - Enlace Principal
- Servicio de Transmisión de Datos Comas - Enlace Contingencia
- Servicio de Transmisión de Datos Villa El Salvador - Enlace Principal
- Servicio de Transmisión de Datos Villa El Salvador - Enlace Contingencia
- Servicio de Switch de Red para el local de Camaná
- Servicio de Switch de Red para el local de Argentina
- Servicio de Switch de Red para el local de Jockey Plaza
- Servicio de Switch de Red para el local de San Juan de Miraflores
- Servicio de Switch de Red para el local de Ate
- Servicio de Switch de Red para el local de Comas
- Servicio de Switch de Red para el local de Villa El Salvador
- Servicio de Herramienta de Monitoreo de Circuitos
- Servicio de Herramienta de Monitoreo de equipos de Red
- Servicio de dispositivos inalámbricos portátiles de internet



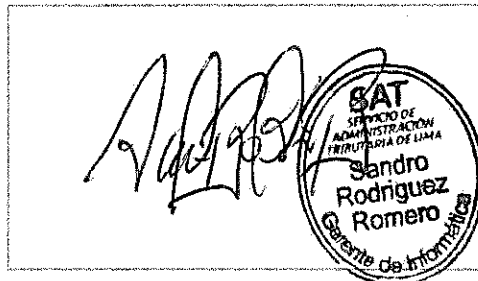
ÁREA USUARIA SOLICITANTE:

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



NOMBRE: Cesar 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