Anexo Nº 01-A
TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIOS Y CONSULTORÍAS

Órgano y/o Unidad Orgánica:	UNIDAD FUNCIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN	
Actividad del POI/Acción Estratégica PEI:	AOI00106600087 GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	
Cuadro Multianual de Necesidades	Meta	18
	Código Siga	870500030019
Denominación de la Contratación:	Servicio de Internet Dedicado para el Programa de Empleo Temporal "Llamkasun Perú"	

I. FINALIDAD PÚBLICA

Brindar al Programa de Empleo Temporal "Llamkasun Perú", una herramienta de interconexión global, la misma que permita dar a conocer la gestión promotora del Programa.

II. OBJETIVO DE LA CONTRATACIÓN

Contratar a una persona jurídica que ofrezca las mejores condiciones técnico-económicas para brindar los servicios de internet para el Programa de Empleo Temporal "Llamkasun Perú", en la cual se seleccionará la oferta que cumpla con todas las especificaciones y requerimientos técnicos mínimos.

III. ALCANCES DEL SERVICIO

El acceso a internet deberá estar basado en la implementación de ancho de banda permanente asegurando una adecuada calidad de servicio para lo cual deberá adjuntar un diagrama indicando el tipo de red de comunicaciones propuestos.
El sistema estará constituido por hardware y software que permitan la transferencia de datos y/o aplicaciones de internet aprovechando los recursos de la red propuesta. Los protocolos de comunicación serán los estándares de TCP/IP.

➢ ALCANCES DEL SERVICIO DE INTERNET

a) Enlace de comunicación dedicada de transmisión de acceso dedicado a internet deberá ser de 750 Mbps de ancho de banda simétrico respectivamente.
b) Overbooking de 1:1 tanto a nivel local como internacional, sin utilizar esquemas de acceso compartido o acceso del tipo asimétrico. Aplica para todo el enlace (es decir el tramo local hasta el punto de salida internacional).
c) El medio de transmisión de última milla del enlace principal se debe realizar mediante la instalación de cable de fibra óptica, con el fin de ofrecer mayor ancho de banda por escalamiento, baja atenuación de señal, medio seguro frente a intrusiones e inmunidad electromagnética.
d) El servicio debe contar con un enlace de respaldo de la misma capacidad 750 Mbps, este enlace debe conservar ruta y nodo distinto al enlace principal. El servicio de internet debe ser provisto desde dos (02) nodos distintos, en donde deberá entenderse por Nodo o PoP o PE, un local propio o alquilado por el Postor, donde se encuentre equipos activos de los que salgan servicios a otros clientes, no se aceptaran buzones o mufas. El enlace de respaldo deberá entregarse mediante fibra óptica y debe ser configurado en pasivo/standby.
e) El proveedor deberá contar con una red propia y/o subarrendada a terceros.
f) El backbone deberá trabajar con tecnología MPLS o Metro EThernet y establecer un mínimo de 3 de QoS (opcional), también, la red permitirá el paso de todo tipo de tráfico como voz video y todo tráfico IP.
g) El protocolo de comunicaciones deberá ser TCP/IP.

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:48:34 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:25:54 -05:00

h) Herramientas de Gestión y estadísticas (nivel de uso, picos máximos y mínimos) del tráfico en el enlace las 24 horas del día con actualización permanente incluyendo reportes de tráfico diario, semanales y mensuales mediante interface Web. Dicha herramienta deberá ser utilizada durante la vigencia del contrato. Así mismo, el acceso deberá ser a través de un protocolo seguro SSH o HTTP o HTTPS mediante un usuario y contraseña y deberá cumplir con las siguientes capacidades y características:

- ✓ *Debe permitir la administración y monitoreo del desempeño de la red (monitoreo de los routers y sus enlaces). Para el router se debe mostrar gráficamente en una sola pantalla la salud del equipo: alarmas recientes, disponibilidad, tiempo de respuesta, pérdida de paquetes, utilización de CPU, utilización de memoria y temperatura. Asimismo, en una sola pantalla debe mostrar todas las interfaces con lo siguiente: el estado, nombre de la interface, tráfico de recepción (Kbps y porcentaje), tráfico de transmisión (Kbps y porcentaje), cantidad de errores.*
- ✓ *Deberá centrar la gestión a través de una consola web, que permita implementar políticas de monitoreo de múltiples dispositivos, así como deberá brindar una interfaz GUI para dispositivos Smartphone (iPhone, Android, Windows).*
- ✓ *Capacidad para seleccionar las interfaces físicas o virtuales a monitorear.*
- ✓ *Debe contener herramientas de diagnóstico y análisis en tiempo real, a través de gráficos en tiempo real, mapeo de puertos, análisis de MIBs.*
- ✓ *Deberá permitir la generación de alarmas que serán enviadas vía correo electrónico.*
- ✓ *Debe mostrar las alarmas, hasta de los últimos 90 días, con la siguiente información: origen, mensaje de la alarma, estado, categoría, hora y día.*
- ✓ *Debe permitir Reportes de Tráfico (Entrada y Salida): en Kbps y Paquetes por segundo, Errores y Descartes (Entrada y Salida).*
- ✓ *Capacidad de visualización de la red usando la integración de Google maps (Opcional).*
- ✓ *Almacenamiento de IP Flow en tiempo real y análisis histórico de todos los IP Flow. Se debe incluir base de datos con histórico de 6 meses.*
- ✓ *Capacidad de Geo-localización para identificar las IPs origen y destino (Opcional).*
- ✓ *Tráfico: Presentación del volumen, velocidad, utilización y paquetes, en presentación gráfica de tiempo y permita la generación del Informe de Planificación de Capacidad. Las mediciones deben actualizarse* como mínimo cada 5 minutos y las *cuales deben ser configurables por el usuario.*
- ✓ *Aplicaciones: Presentación de la distribución gráfica de las aplicaciones en el tiempo permitiendo tener la visibilidad de aplicaciones o mediante tabla y permitiendo filtrar por aplicación (Opcional).*
- ✓ *Conversaciones IP bidireccional mostrando: IP Origen, IP Destino, Aplicación, Puerto origen/destino, Protocolo, DSCP y tráfico. Permitir agruparlas por IP Origen, IP Destino, Aplicación, DSCP, Origen y Destino.*
- ✓ *Filtros configurables, personalización de reportes en archivos pdf, csv y creación de alarmas.*
- ✓ *Reportes ejecutivos personalizados y gráficos interactivos.*
- ✓ *Permite la configuración de reportes automáticos para ser generados mensualmente y a petición.*
- ✓ *Envió de notificaciones vía correo electrónico*

i) El proveedor del servicio deberá de brindar un (01) usuario al personal de la Unidad Funcional de Tecnología de la Información para acceder a la herramienta de sistema de monitoreo del servicio de internet.

j) El proveedor incluirá como parte del servicio todo el equipamiento de comunicaciones equipos, dispositivos y/o componentes necesarios para su funcionamiento sin que esto implique costo adicional para el Programa de Empleo Temporal "Llamkasun Perú", debiendo indicar marca, modelo y ficha técnica de los equipos (la ficha técnica se podrá presentar en idioma original). El servicio incluye lo(s) Router(s), terminales, que sean de tecnología vigente, con capacidad de soportar el requerimiento de ampliación de ancho de banda**,** todo el equipamiento deberá contar con vigencia tecnológica, no encontrase en End of life (se podrá comprobar a través de un enlace público del mismo fabricante, la comprobación de la vigencia tecnológica de los equipos router también podrá validarse mediante la entrega de una carta del fabricante y/o proveedor autorizado

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:49:01 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:07 -05:00

en el territorio nacional donde se indique que el equipamiento se encuentra vigente y no en estado de End of Life y End of Sale) ni en End of sale. El equipamiento debe soportar un crecimiento mínimo del 50% sin la necesidad de cambiar o reemplazar el equipo. La imputación de responsabilidades por la existencia de daños irreparables en los equipos, se evaluará previamente si esta deberá recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que el referido daño fue originado por el uso negligente imputable al usuario, será la Entidad quien asuma los costos adicionales por la mencionada contingencia. El término (tecnología vigente) se refiere a que los equipos deberán de contar con el soporte del fabricante durante el tiempo de ejecución del servicio.

k) En el caso que se necesite realizar obras civiles dentro o fuera del local del Programa de Empleo Temporal "Llamkasun Perú", deberán ser realizados por el proveedor asumiendo íntegramente su costo, el cual deberá cumplir con los protocolos sanitarios.

l) El Programa de Empleo Temporal "Llamkasun Perú" podrá solicitar cambios en la configuración de los enlaces cuando así lo considere necesario, durante el tiempo que dure el servicio, sin que ello implique algún costo adicional para el Programa de Empleo Temporal "Llamkasun Perú", el tiempo de atención a estas solicitudes por parte del proveedor no será mayor a ocho (8) horas, el mismo que se computara desde la generación del ticket. El cambio en la configuración también dependerá del impacto que pueda causar dicho cambio en la red del Programa, por lo que se deberá realizar si fuera necesario un tiempo para el análisis de una (1) hora. El proveedor deberá contar con un NOC propio y ubicado en Perú para gestión y monitoreo del servicio.

m) El proveedor deberá entregar 64 IPs públicas de internet que no se encuentren en blacklist, incluyendo dentro de estas las direcciones de IP de red, Broadcast y Gateway virtual, router principal y router contingencia, estas IP públicas de internet deben ser de Perú. Se debe instalar dos routers uno para el enlace principal (Activo) y un enlace de contingencia (Standby).

n) Acceso total a los servicios de Internet sin restricción de protocolo, puerto o aplicación.

o) El Proveedor será responsable de la adecuada integración del servicio de línea dedicada con acceso de internet a la red del Programa de Empleo Temporal "Llamkasun Perú". La configuración interna de la red será realizada por el Programa y se proporcionará las interfaces en los switch que sean necesarios para las conexiones con los equipos del Contratista.

p) El Proveedor deberá de incluir en su propuesta todos los componentes necesarios para el servicio de línea dedicada con acceso de internet (medios de enlace: Fibra Óptica, Antenas, Cables, Routers, etc.), los cuales deben ser de tecnología vigente que no hayan llegado al fin de su ciclo de vida. Igualmente deberá incluir la instalación y programación del equipo de acceso Router necesario para la prestación del servicio con la finalidad de que la Entidad obtenga información de forma detallada y en línea, que le permita detectar problemas de red, así como mejorar la utilización del ancho de banda y/o auditar el cumplimiento de los SLA del proveedor, así como verificar el correcto funcionamiento de los Routers. Los equipos deben de contar con soporte vigente del fabricante. El término (tecnología vigente) se refiere a que los equipos deberán de contar con el soporte del fabricante durante el tiempo de ejecución del servicio.

q) El Proveedor deberá reparar o reemplazar sin costo para el Programa de Empleo Temporal "Llamkasun Perú" los equipos o componentes que sean necesarios para asegurar la prestación del servicio en caso de falla de los equipos suministrados, los mismos que deberán tener iguales o mejores características.

r) El proveedor informará sobre cualquier mantenimiento físico o lógico que afecte el desempeño del servicio de Internet proporcionado (equipos de última milla, cableado, servidores, etc.). Para ello, elaborará cronogramas, que serán entregados a el Programa de Empleo Temporal "Llamkasun Perú", 48 horas previo al mantenimiento, con la debida anticipación. Deberá contar con un centro de gestión que atienda las 24 horas x 7 días de la semana, el cual garantice el monitoreo solicitado.

s) El Nivel del Servicio (SLA) mínimo debe ser de 99.50% de disponibilidad mensual para el servicio contratado.

t) El proveedor deberá ser miembro de la NAP PERÚ o de algún socio estratégico afiliado, por lo que deberá acreditar mediante constancia o captura de la página web del NAP Perú.

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:49:14 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:15 -05:00

u) El proveedor deberá contar con al menos 2 salidas internacionales a través de dos proveedores distintos los cuales deberán ser TIER-1, cada salida deberá tener una capacidad mínima de 10Gbps.

v) De los equipos, una vez finalizado el plazo contractual se procederá a la devolución del total de los equipos que le hayan sido entregados y/o instalados bajo cualquier modalidad distinta a la venta (incluyendo equipos, cargadores, baterías, accesorios, routers, switches y/o cualquier otro de propiedad del Contratista) sin más desgaste que el de su uso normal y diligente, aceptando que en caso de pérdida, deterioro o robo deberán asumir el costo de los mismos.

- **SOLUCIÓN DE SEGURIDAD GESTIONADA**

DESCRIPCIÓN

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

b) 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 (tecnología vigente).

c) El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 6 reportes.

d) El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

e) El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.

f) La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.

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

h) 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.

i) Los equipos NGFW deberán tener soporte vigente de fabrica 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.

j) Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.

k) 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

l) 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.

m) Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere que la propuesta incluya documentación pública sobre dicha herramienta explicando su alcance.

n) 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.

o) La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.

p) Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, la Entidad tendrá la potestad de contar con un servicio directo con el Fabricante,

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:49:28 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:23 -05:00

el cual incluye:

q) *Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas.*
r) *Análisis de logs e indicadores de compromiso*
s) *Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas*
t) *Recomendaciones de pasos siguientes a realizar*

CAPACIDAD

a) *Throughput de Next Generation Firewall de 2.4 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, y/o transacciones medidas en condiciones empresariales y/o transacciones HTTP 64KB de tamaño). 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.*
b) *Throughput de Prevención de Amenazas de 1 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, 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), 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.*
c) *No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.*
d) *El equipo debe soportar como mínimo 200.000 sesiones simultaneas y 38.000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte.*
e) El equipo debe soportar disco de estado sólido y/o almacenamiento de 120 GB o superior.
f) *Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red*
g) *Minimo una (01) interfaz de consola RJ45,*

CARACTERÍSTICAS GENERALES

a) *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.*
b) *Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).*
c) *Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.*
d) *Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.*
e) *Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.*
f) *Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.*
g) *Soportar túneles GRE como punto inicio o finalización del túnel.*
h) *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.*
i) *Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.*
j) *Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:49:40 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:32 -05:00

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.

ALTA DISPONIBILIDAD

a) *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).*
b) *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.*
c) *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.*
d) *Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.*

FUNCIONALIDADES DE FIREWALL

a) *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.*
b) *Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.*
c) *Permitir el agendamiento de las políticas de seguridad.*
d) *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.*
e) *Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.*
f) *Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.*
g) *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).*
h) *Debe mostrar la primera y última vez que se utilizó una regla de seguridad.*
i) *Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.*
j) *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.*

DESCIFRADO DE TRÁFICO SSL/TLS

a) *Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.*
b) *Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.*
c) *Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.*
d) *Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.*
e) *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*
f) *Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).*
g) *Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.*
h) *Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.*
i) *Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de*

MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:49:56 -05:00

MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:43 -05:00

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 la 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).

CONTROL DE APLICACIONES

a) *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.*
b) *Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2*
c) *Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.*
d) *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.*
e) *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.*
f) *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.*
g) *Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.*
h) *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.*
i) *Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.*
j) *Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.*
k) *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.*

PREVENCION DE AMENAZAS CONOCIDAS

a) *Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.*
b) *Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos*
c) *Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.*
d) *El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.*
e) *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.*
f) *Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:50:10 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:26:53 -05:00

disponibilidad.

g) *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.*
h) *Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.*
i) *Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.*
j) *Los eventos deben identificar el país que origino la amenaza.*
k) *Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.*
l) *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.*
m) *Debe soportar la creación de firmas de IPS basadas en el formato de Snort.*

ANALISIS DE MALWARE DE DÍA CERO

a) *La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.*
b) *La plataforma de Sandboxing deberá ser ofrecido en Nube (Cloud). 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 Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye Firmas o Prefiltros)*
c) *Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.*
d) *Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.*
e) *El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.*
f) *Deberá garantiza 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, FedRAMP.*
g) *El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.*
h) *Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.*
i) *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.*
j) *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, tanto en IPv4 como en IPv6.*
k) *Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.*
l) *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.*
m) *Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.*
n) *Permitir la subida de archivos al sandbox de forma manual y vía API.*
o) *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.*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:50:23 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:27:05 -05:00

p) *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.*

FILTRO DE CONTENIDO WEB

a) *Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)*
b) *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.*
c) *Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs*
d) *Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.*
e) *Debe permitir la creación de categorías personalizadas.*
f) *Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.*
g) *Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.*
h) *Debe permitir la customización de la página de bloqueo.*
i) *Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.*
j) *Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.*
k) *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.*

IDENTIFICACION DE USUARIOS

a) *Debe incluir a 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, E- Novell Directory, Exchange y base de datos local.*
b) *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.*
c) *Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.*
d) *Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.*
e) *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.*
f) *Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.*
g) *Debe permitir la definición de grupos dinámicos de usuarios.*

QoS

a) *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.*
b) *Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.*
c) *El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.*
d) *Soportar marcación de paquetes DSCP, inclusive por aplicaciones;*
e) *Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.*

FILTRO DE DATOS

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:50:36 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:27:16 -05:00

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

VPN

a) *Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL para 500 usuarios como mínimo.*
b) *La VPN IPSec debe soportar como mínimo:*
   - *DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)*
   - *Autenticación MD5, SHA-1, SHA-2;*
   - *Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;*
   - *Algoritmo Internet Key Exchange (IKEv1 & IKEv2);*
c) *Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.*
d) *Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.*
e) *Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).*
f) *Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.*
g) *Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.*
h) *El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.*
i) *Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:*
j) *Antes del usuario se autentique en la estación;*
k) *Después de la autenticación del usuario en la estación usando Single Sign On (SSO);*
l) *Bajo demanda del usuario;*
m) *El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.*
n) *Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.*
o) *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)*
p) *Debe ser posible colocar equipos en cuarentena de forma manual o automática.*
q) *Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.*
r) *Debe permitir la conexión a la VPN sin necesidad de instalar el agente (clientless).*
s) *Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar ciertas características del equipo para controlar el acceso a la red, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que, si el equipo no cumple cierta condición basado en esas características, no permita el acceso a la VPN o le otorgue acceso de mayores restricciones. Este perfil de postura de seguridad debe poder ser personalizable desde la consola gráfica (GUI) del Firewall.*
t) *El perfilamiento y postura mencionado en el punto anterior tiene que poder efectuarse inclusive dentro de la red interna, entre dos o más segmentos de red que controle el firewall.*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:50:47 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:27:30 -05:00

CONSOLA DE ADMINISTRACION Y MONITOREO

a) *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*
b) *Permitir exportar las reglas de seguridad en formato CSV y PDF*
c) *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.*
d) *Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.*
e) *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)*
f) *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.*
g) *Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.*
h) *Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).*
i) *Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).*
j) *Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.*
k) *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).*
l) *Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;*
m) *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.*
n) *Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.*
o) *La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.*

➢ **SOLUCIÓN DE ADMINISTRADOR DE ANCHO DE BANDA**

DESCRIPCIÓN

a) *Un (01) administrador de ancho de banda de propósito específico de hardware tipo appliance (contar con vigencia tecnológica).*
b) *Un (01) equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras.*
c) *Deberá contar con al menos 3,000 aplicaciones identificadas.*
d) *Deberá contar con 2 bridges como mínimo, es decir, 4 puertos 1GE RJ45, con capacidad de adicionarle 2 bridges de 1GE (de cobre o de fibra) opcional, o un 1 bridge de 10GE (de cobre o fibra) opcional. Todos los bridges deberán contar con bypass interno que impida la*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:50:59 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:27:44 -05:00

interrupción ante eventos de falla por energía del equipo, no se aceptarán equipos con bypass externos.

e) *El equipo deberá poseer dos puertos 1GE RJ45 para la administración del sistema. El primero permitirá que la Entidad tenga acceso al equipo y la integración con el AD, y el segundo permitirá que el postor tenga acceso remoto del equipo sin tener que pasar por la red LAN de la Entidad. No se permitirá que la administración del sistema sea través de las interfaces que procesan el tráfico de red de la Entidad*
f) *Deberá estar licenciado para poder gestionar 500 Mbps de throughput simétrico inicialmente, con capacidad de poder incrementar (con licenciamiento adicional) a 1 Gbps como mínimo.*
g) *Deberá soportar como mínimo 750 mil de flujos concurrentes.*
h) *Deberá soportar como mínimo 350 mil de paquetes por segundo.*
i) *Deberá permitir la creación múltiple políticas o reglas de control de ancho de banda que realicen la priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo de ancho de banda permitido. Estas políticas también podrán ser basadas en tiempo.*
j) *Deberá permitir la creación de políticas de control de ancho de banda considerando el comportamiento de los flujos o sesiones. Es decir, políticas basadas en la duración de los flujos, la cantidad de paquetes, la velocidad de transferencia y por el total de transferencia.*
k) *La solución deberá integrarse con los Directorios Activos (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios. No se permitirá la instalación de ningún agente, conector o software adicional en los Directorio Activos (AD) de la Entidad.*
l) *La solución deberá tener capacidad de identificar y mostrar los sistemas operativos de los dispositivos que están que cursan tráfico a través del equipo*
m) *Deberá permitir la creación de los siguientes reportes históricos basados en gráficos para un periodo de tiempo configurable:*
n) *Tráfico de descarga y de subida*
o) *Top 10 de Host con mayor consumo*
p) *Top 10 de Usuarios con mayor consumo (cuando se haya integrado con el Directorio Activo).*
q) *Top 10 de Aplicaciones con mayor consumo*
r) *Deberá mostrar históricamente y en tiempo real (actualizado cada segundo), distintas métricas del desempeño a nivel de un usuario utilizando una aplicación específica, mínimamente:*
s) *Troughput (In / Out)*
t) *Bytes transmitidos (In / Out)*
u) *Número de Sesiones activas y nuevas sesiones por segundo*
v) *Número de Paquetes descartados y paquetes descartados por segundo*
w) *Desempeño de la calidad de la aplicación o soporte para TCP retransmisión, Session Time, TCP Pocket lost y TCP duplicate ACK.*
x) *Monitoreo en tiempo real con actualizaciones cada segundo a través de tablas con filtros y gráficos, que permitan realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.*
y) *El equipo deberá ser capaz de mostrar la geografía del tráfico, es decir contra que países se está realizando el intercambio de datos. Permitiendo limitar y bloquear desde o hacia uno o varios países.*
z) *El equipo a instalarse deberá enviar alarmas por medio de email y por traps*
aa) *El equipo deberá poder actualizarse automáticamente a la última versión de software publicado o la versión más reciente y estable recomendado por el fabricante.*
bb) *El equipo debe garantizar el almacenamiento de datos en su disco duro interno de por lo menos los últimos 24 meses, para la posterior generación de reportes y estadísticas.*
cc) *Deberá considerar una consola de administración web en el mismo equipo que permita, de forma gráfica, administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. La Entidad deberá contar con acceso de lectura al equipo para la obtención de reportes en cualquier momento.*
dd) *El Postor deberá presentar en su oferta una carta del fabricante de la solución indicando el*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:51:10 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:27:58 -05:00

cumplimiento de todas las características técnicas descritas y de la garantía del equipo a través de RMA

ee) *El Postor deberá reemplazar el equipo en caso de falla dentro de las 8 horas por un equipo similar o superior mientras se realiza el proceso del RMA con el fabricante.*

- **SOPORTE TÉCNICO**

a) *Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.*

b) *El postor deberá contar con un Centro de Operaciones de Seguridad (SOC) para el servicio de Soporte Técnico, con la finalidad de garantizar que se cuente con procesos de atención óptimos que asegure el cumplimiento de los tiempos de respuesta, la calidad de su atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y de la información de la entidad.*

c) *El soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio en internet, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".*

d) *El soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".*

e) *El Postor deberá brindar un servicio de pruebas de penetración continua, incluido el descubrimiento automático de activos, la identificación de la superficie de ataque, la minería y explotación de vulnerabilidades, que cumpla mínimamente con lo siguiente:*

- *Debe realizar pruebas de caja negra y gris, formando automáticamente rutas de ataque basadas en el aprendizaje de la red y los sistemas.*
- *Las pruebas de penetración continua se deben realizar a 10 Host IP.*
- *Debe admitir un proceso completamente automatizado que pueda minimizar el comportamiento de un pirata informático real para escanear/descubrir las exposiciones de la superficie de ataque de la máquina objetivo, las vulnerabilidades del sistema y luego explotar automáticamente las vulnerabilidades del sistema para validar el riesgo real de las máquinas objetivo.*
- *Debe admitir al menos 4 niveles de control de nivel sigiloso para tareas de prueba de penetración, que incluyen: modo sigiloso, modo intermedio, modo normal y modo ruidoso.*
- *Debe ser compatible con una arquitectura escalable para realizar escaneos de redes/sistemas a gran escala y creación de perfiles de activos, descubrimiento de vulnerabilidades y minería de la base de conocimientos, autoexplotación de vulnerabilidades, postexplotación y priorización/informes de riesgos.*
- *Debe tener una base de conocimiento de complementos de vulnerabilidad/explotación con más de 36,000 complementos; cada complemento deberá incluir puntaje CVSS, vector CVSS, información de número CVE si está disponible; cada complemento tendrá un nivel de gravedad de vulnerabilidad y un nivel de control de riesgo de explotación asociado con él; el nivel de severidad del complemento debe tener Alto, Medio, Bajo e Informativo.*
- *Debe admitir complementos de vulnerabilidad/explotación desarrollados por el usuario*
- *Debe admitir el modo de intervención del usuario y tener registros de ataque para ataques de prueba de penetración de alto impacto.*
- *Debe admitir plantillas predefinidas para los siguientes casos de uso de pruebas de penetración.*
- *Debe admitir el caso de uso de prueba de penetración de Ransomware, puede simular técnicas populares de intrusión de ransomware para explotar y validar los riesgos de los sistemas de destino para posibles ataques de ransomware.*
- *Debe admitir la priorización de vulnerabilidades basada en el riesgo, proporcionar una tabla de riesgo simple de riesgo de alta prioridad que el usuario necesita mitigar lo antes posible.*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:51:21 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:28:15 -05:00

- *Debe admitir la explotación automática de vulnerabilidades y debe ser capaz de mostrar el progreso del exploit en tiempo real en su interfaz de usuario web.*
- *Debe permitir al administrador del sistema configurar la explotación en función del tipo de sistema operativo, los niveles de gravedad de la vulnerabilidad, los niveles de control del riesgo de explotación y las palabras clave definidas por el usuario.*
- *Debe ser capaz de mostrar la topología de ataque del entorno de destino con al menos 5 capas de información durante la explotación, incluidas, entre otras, la IP, el servicio, la superficie de ataque, la vulnerabilidad y el riesgo empresarial de la máquina de destino.*
- *Debe ser capaz de mostrar toda la información de la cadena de muerte de una vulnerabilidad explotada.*
- *Debe ser capaz de proporcionar pruebas de una explotación exitosa, incluyendo, entre otros, instantáneas de base de datos, salidas de webconsole, directorios de sistemas de archivos, credenciales*
- *Debe ser capaz de proporcionar validación con un solo clic para volver a validar la vulnerabilidad y la corrección.*
- *Debe ser capaz de proporcionar funcionalidad de limpieza de rastreo de ataques con un solo clicDebe soportar el movimiento lateral de la post-explotación y puede utilizar un activo comprometido como pivote para descubrir y explotar activos adicionales en redes adyacentes.*
- *Debe ser capaz de calcular el riesgo del sistema objetivo en función del impacto de la vulnerabilidad explotada y la información de la cadena de eliminación.*
- *Debe tener una plantilla de tarea dedicada para identificar y documentar la exposición de la superficie de ataque de las máquinas objetivo*
- *Debe admitir la priorización de vulnerabilidades basada en el riesgo, proporcionar una tabla de riesgos simple de alto riesgo prioritario que el usuario necesita mitigar lo antes posible.*
- *Debe proporcionar información detallada para cada vulnerabilidad descubierta, incluidos, entre otros, el tipo de vulnerabilidad, la gravedad, la puntuación CVSS (Common Vulnerability Scoring System), el vector CVSS, la descripción, la solución, el enlace de referencia, así como la máquina objetivo vulnerable, la superficie de ataque. y ruta de ataque para esta vulnerabilidad. La solución también debe proporcionar una herramienta de validación de vulnerabilidades que ayude al usuario a volver a validar la vulnerabilidad después de parchear el software.*
- *Debe tener una base de datos centralizada para gestionar los activos de TI para la validación de la seguridad. Los activos administrados incluirán hosts con información de la versión del sistema operativo, puertos abiertos del servidor e información de la aplicación activa, sitios web e información de la aplicación, nombres de dominio y direcciones IP, así como el estado del agente de prueba de evaluación de evaluación.*
- *El servicio debe ejecutarse mínimamente durante 10 días calendarios, emitir el informe de las remediaciones que deben ser solucionadas; y posteriormente a ello realizar un segundo escaeno durante el mismo periodo y emitir un informe final del servicio.*

f) *El soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.*

g) *El servicio de soporte técnico debe entregar en una recurrencia mensual informes sobre la solución implementada, a nivel de detalle de la totalidad de incidencias generadas en el periodo de tiempo.*

h) *Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.*

i) *El postor deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.*

j) *El soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:51:32 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:28:31 -05:00

disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.

k) *Para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará previamente si estas deberán recaer sobre el contratista o sobre la Entidad. No se contabilizará el tiempo de no disponibilidad de las interrupciones de servicio que pudieron producirse por causas imputables a la Entidad o Terceros, para ello deberá de presentar en un plazo no mayor a Tres (03) días hábiles un informe sustentando el hecho del evento acreditado fehacientemente lo ocurrido. Asimismo, se precisa que en caso se determine que dicho suceso es imputable al contratista se aplicara la penalidad por mora.*

➢ **CAPACITACIÓN**

a) *Se debe considerar capacitación en la administración y configuración de los equipos y/o servicios proveídos, para un máximo de 2 personas del Programa, con una duración de 8 horas como mínimo. La capacitación puede ser realizada de manera presencial y/o virtual previa coordinación con el personal de la* Unidad Funcional de Tecnologías de la Información *del Programa. Dicha capacitación deberá ser realizada en el primer mes de la ejecución del servicio.*

IV. REQUISITOS DEL PROVEEDOR

REQUISITOS DEL PROVEEDOR Y/O PERSONAL

- **REQUISITOS DEL POSTOR**
  - ✓ *Persona Jurídica con registro Único del Contribuyentes (RUC) Activo y habido.*
  - ✓ *Empresa dedicada al servicio de internet.*
  - ✓ *Contar con una mesa de ayuda propia para brindar el soporte 24x7x365 incluidos domingos y feriados. Se debe de acrediar mediante una declaración jurada al momento de presentar su oferta.*
  - ✓ *El postor deberá de poseer una experiencia mínima de dos (02) servicios en los últimos dos (02) años, relacionados al servicio, el mismo que debe estar acreditado con orden de servicio, contrato, con su respectiva conformidad u otro documento que lo acredite al momento de presentar su oferta.*
  - ✓ *Contar con un Centro de Operaciones de Seguridad propio o de terceros, Se debe de acrediar mediante una declaración jurada al momento de presentar su oferta.*

- **REQUISITOS DEL PERONAL CLAVE**

Un (01) Supervisor De Proyecto

- ✓ *Título Profesional de Ingeniero o Técnico en Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones o Administración de Tecnologías de Información o carreas afines. Solo para el caso del profesional titulado deberá estar colegiado y habilitado al momento de la presentación de la propuesta.*
- ✓ *Deberá contar con certificación "ITIL Foundation Certificate" y/o "Lead Cybersecurity Professional Certificate" y/o "Service Desk Leader Professional Certificate"*
- ✓ *Capacitación mínima de veinte (20) horas comprobadas en Gestion de servicios en la era digital basado en ITIL 4.*
- ✓ *Deberá contar con experiencia mínima de tres (03) años en supervisión de proyectos de seguridad informática o su puesto equivalente o similares al objeto de la convocatoria, del personal clave como Supervisor, la misma que debe estar acreditada con constancia o certificados y/o contratos y/o órdenes de servicio con sus respectivas conformidades.*

Un (01) Especialista en implementación

- ✓ *Título Profesional de Ingeniero o Técnico o Bachiller en Telecomunicaciones o Sistemas o Informática o Electrónica o Redes y Comunicaciones de Datos o Administración de*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:51:47 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:28:47 -05:00

Tecnologías de Información o carreras afines.

- ✓ Certificado oficial en la solución de seguridad perimetral y certificado en administrador de ancho de banda.
- ✓ *Capacitación mínima de dieciséis (16) horas comprobadas en redes WAN o Telecomunicaciones o afines de similar envergadura.*
- ✓ *Experiencia mínima de dos (02) años, implementando soluciones similares al objeto de la convocatoria, del personal clave como implementador, la misma que debe estar acreditada con constancia o certificados y/o contratos y/o órdenes de servicio con sus respectivas conformidades.*

V. REGLAMENTOSTÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS

No aplica

VI. SEGUROS

No aplica

VII. PRESTACIONES ACCESORIAS

No aplica

VIII. LUGAR Y PLAZO DE EJECUCIÓN

Lugar:

El servicio será configurado en las instalaciones del Programa de Empleo Temporal "Llamkasun Perú", ubicado en Av. Salaverry Nº 655- Piso 7, distrito de Jesús María.

Plazo:

El plazo de ejecución del servicio será computado desde la fecha de la firma de la respectiva acta de Activación del servicio, luego de culminada la instalación del servicio y será de cuarenta y dos (42) días calendarios.

El plazo para la instalación y/o implementación del servicio de internet de 750 Mbps en la sede central del Programa de Empleo Temporal "Llamkasun Perú será hasta cinco (05) días calendarios, desde el dia siguiente de notificada la orden de servicio.

IX. ENTREGABLES

El proveedor del servicio deberá de presentar los siguientes entregables a través de mesa de partes digital (https://mesadepartes.llamkasunperu.gob.pe/):

ENTREGABLE 1: PLAN DE TRABAJO

El proveedor deberá presentar dentro de los 2 días calendarios, contados desde el día siguiente recibida la orden de servicio.

ENTREGABLE 2: INFORME AL TERMINO DE LA IMPLEMENTACIÓN DEL SERVICIO

El proveedor deberá presentar dentro de los 2 días calendarios, contados desde el día siguiente de la implementación del servicio y/o firma del acta de instalación.

ENTREGABLE 3

El proveedor deberá entregar un informe al finalizar el servicio que contenga lo siguiente, el cual servirá para la emisión de la conformidad:

- Consumo de ancho de banda

MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:51:59 -05:00

MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:29:02 -05:00

NOTA:
En caso de que el día establecido para la presentación del producto fuera día inhábil, éste podrá presentarse el primer día hábil siguiente a la fecha prevista.

Asimismo, la presentación del producto podrá realizarse a través de Mesa de Partes Digital del Programa Llamkasun Perú, ingresando a la página web del Programa, o a través de Mesa de Partes Presencial ubicado en Av. Salaverry N° 655 - Piso 7.

X. CONFORMIDAD

La conformidad del servicio será otorgada por el jefe la Unidad Funcional de Tecnologías de la Información o quien haga de sus veces, quien verificará el estricto cumplimiento del término de referencia.

Asimismo, en caso de encontrar observaciones en el producto/entregable, la jefatura de la Unidad Territorial deberá comunicar a la Coordinación Funcional de Abastecimiento y Servicios Generales a fin de que este notifique al proveedor según Articulo 144. Del acápite 144.4 del Reglamento de la Ley 32069.

XI. FORMA Y CONDICIONES DE PAGO

Se realizará mediante abono en cuenta (CCI), en una (01) armada, la cual se cancelará previa presentación del entregable solicitado y conformidad respectiva a cargo de la Unidad Funcional de Tecnologías de la Información.

Documentos a presentar:

- Informe del servicio detallado (contenido entregable 1, 2 y 3)
- Conformidad emitida por por el jefe la Unidad Funcional de Tecnologías de la Información
- Factura electrónica o recibo electronico.
- Copia de orden de servicios (incluye TDR).

XII. GARANTÍAS

La garantía del servicio deberá de ser del total de dias que dure el servicio, ante cualquier falla debido al uso del mismo, contados a partir del acta de activación del servicio. Dicha garantía debe cubrir el mantenimiento en un plazo máximo de 48 horas de haberse notificado la falla al contratista. Se debe de acreditar mediante una carta de garantía.

XIII. CONFIDENCIALIDAD

El Contratista se obliga a guardar reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionado con la prestación, quedando expresamente prohibido revelar dicha información a terceros. El proveedor, deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información.

▪ Dicha obligación comprende la información que se entrega como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido con la prestación y/o entrega del bien y/o servicio.

▪ Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.

▪ El Contratista cederá en forma exclusiva al Programa los títulos de propiedad, derechos de autor y otro tipo de derecho de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones del presente Término de Referencia.

XIV. GASTOS POR DESPLAZAMIENTO

No aplica.

MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:52:16 -05:00

MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:29:19 -05:00

XV. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de cuarenta y dos (42) dias, emitidos a partir de la conformidad otorgada por la Entidad.

XVI. PENALIDADES POR MORA

Penalidad por Mora en la ejecución de la prestación:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se
calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde F tiene los siguientes valores:
Para bienes y Servicios: F = 0.40

Para obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40
b) Para plazos entre sesenta y uno a ciento veinte días: F = 0.25.
c) Para plazos mayores a ciento veinte días: F = 0.15

Para consultoría de Obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40.
b) Para plazos mayores a sesenta días: F = 0.25.

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

Nota:
Asimismo, es de indicar que cualquier tipo de penalidad a aplicar puede alcanzar como máximo un monto equivalente al diez por ciento (10%) por cada entregable, del monto total del contrato vigente y/o de la orden de servicio.

XVII. OTRO TIPO DE PENALIDADES

No aplica

XVIII. RESOLUCIÓN CONTRACTUAL

Son las establecidas en el Artículo 68 de la Ley General de Contrataciones N° 32069:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

XIX. CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:52:53 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:29:42 -05:00

entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

XX. APLICACIÓN SUPLETORIA

Según Ley Nº 32069, Ley General de Contrataciones Públicas y su Reglamento, Código Civil Peruano, entre otras normativas vigentes

XXI. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

No aplica.

XXII. GESTION DE RIESGOS

Según literal c) del Artículo 6 de la Ley de Contrataciones Públicas.

XXIII. SOLUCIÓN DE CONTROVERSIAS

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y/o acción judicial.

XXIV. CLÁUSULA DE CUMPLIMIENTO DE ACUERDO A LO ESTABLECIDO EN LA LEY N° 31564

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad".

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:52:25 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:29:54 -05:00

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Soy el autor del documento
Fecha: 10.07.2025 17:54:23 -05:00

Firma del solicitante

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Soy el autor del documento
Fecha: 10.07.2025 17:53:19 -05:00

Firma del Jefe del Área Usuaria

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:52:34 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 10.07.2025 17:30:14 -05:00