ESPECIFICACIONES TECNICAS ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL - FIREWALL

1. DENOMINACIÓN DE LA CONTRATACIÓN

El requerimiento consiste en la adquisición de un equipo (appliance) de Seguridad Perimetral – Firewall para el nuevo almacen central de SILSA.

2. AREA USUARIA

Departamento de Sistemas.

3. FINALIDAD PÚBLICA.

Fortalecer la seguridad de red de los Servicios Integrados de Limpieza S.A - SILSA mediante la implementación de un equipo de seguridad perimetral – firewall para la nueva sede del Almacén, el cual mejorará la seguridad de la red con la sede principal, protegiendo la red del acceso no autorizado, evitando que los actores maliciosos, piratas informáticos, bots y otras amenazas, sobrecarguen o se infiltren a la red privada de SILSA para robar datos sensibles.

4. OBJETIVO DE LA CONTRATACIÓN

Adquirir e implementar un equipo de Seguridad Perimetral – Firewall que permita proteger la red del acceso no autorizado, gestionar y aplicar políticas de seguridad de forma fácil y eficiente en todo su entorno de red.

5. CARACTERÍSTICAS Y CONDICIONES DEL BIEN A CONTRATAR

5.1. DESCRIPCIÓN DEL BIEN

Tipo	Descripción	Cantidad	Unidad de medida
1	Equipo (appliance) de Seguridad Perimetral – Firewall para proteger la red TI del almacén central de SILSA	01	Unidad
El servicio de soporte para la solución tendrá una duración de 1 año			

5.2. SUSTENTO TÉCNICO DE ESPECIFICACIONES TÉCNICAS MÍNIMAS

Para acreditar las características técnicas mínimas de los bienes requeridos, los postores deberán presentar brochures y/o catálogos y/o folletería y/o ficha técnica y/o otros documentos emitidos por el fabricante (copia simple u original).

5.3. CARACTERÍSTICAS TÉCNICAS MÍNIMAS DEL EQUIPO DE SEGURIDAD PERIMETRAL - FIREWALL

5.3.1. Características generales

- Un (01) equipo de propósito específico de firewall de siguiente

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas SILSA

generación.

- El fabricante de la tecnología adquirida debe haber sido evaluado y estar certificado por el estándar público de comparativa de rendimiento de productos de seguridad de red provisto por la agrupación NetSec OPEN, basada en los requerimientos de prueba internacionales definidos por la Internet Engineering Task Force (IETF).
- Estar licenciado como mínimo 1 año y habilitado en simultaneo las funcionalidades de: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios a través de directorio activo, prevención de Bots y Sandboxing cloud.
- La plataforma propuesta debe permitir utilizar las capacidades de Firewall e IPS en IPv4 e IPv6. Esto debe ser demostrado a través de la certificación USGv6/IPv6 tanto para firewall como para IPS.
- 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.
- Debe soportar redundancia de al menos tres enlaces de internet, permitiendo elegir el mejor enlace en función de la calidad de estos tomando como criterios: latencia, pérdida de paquetes y jitter, y balanceo de enlaces.
- Debe ser capaz de inspeccionar en tiempo real el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- Debe soportar inspección SSL profunda de tráfico HTTP3/QUIC.
- Reconocer por lo menos 6000 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.
- El equipo debe contar con todo el hardware soportado por el mismo: procesadores, memoria ram, disco interno, interfaces, entre otros componentes. El equipo debe estar habilitado a su máxima capacidad, no debe tener limitaciones de desempeño por software o licenciamiento.

5.3.2. Requerimientos específicos

Capacidad

- Tener un rendimiento Threat Prevention o Threar Prevention (cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware) de 700 Mbps mínimo, medido en condiciones de prueba o mixtura empresariales o en transacciones HTTP de 64KB. No se aceptarán otro tipo de mediciones.
- Debe soportar al menos un rendimiento de 1 Gbps de NGFW, medido en condiciones de prueba o mixtura empresariales o en transacciones HTTP de 64KB. No se aceptarán otro tipo de mediciones.
- El equipo debe soportar como mínimo 700 mil sesiones concurrentes medido con transacciones TCP.
- Debe ofrecer al menos una capacidad de procesamiento de IPS de 1.4 Gbps en condiciones de tráfico mezclado, con el control de

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LABREZ LOZADA TORATO Jefe Dpto. de Ventas SILSA

aplicaciones, firewall de la nueva generación y protección de amenazas activados y con logeo de eventos
- El equipo debe soportar 35 mil nuevas sesiones por segundo medido con transacciones TCP.
- El Gateway debe incluir mínimo 10 interfaces 10/100/1000 Mbps RJ-45 que podrán ser utilizadas como interfaces WAN, LAN, DMZ, etc.

VPN
- La plataforma debe tener la capacidad y licenciamiento para soportar al menos 500 conexiones VPN IPSEC cliente servidor.
- La plataforma debe tener la capacidad de licenciamiento para al menos poder establecer 200 túneles VPN IPSEC punto a punto.
- La plataforma debe soportar un throughput mínimo de 6.5 Gbps de VPN Ipsec usando cifrado AES256-SHA256.
- El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad.

Identificación de Usuarios
- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local.
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad/controles basados en usuarios y grupos de usuarios.
- Debe poder integrarse con Azure AD para la autenticación de los usuarios vía SAML.
- Debe permitir el control de navegación sin necesidad de instalación de software de cliente, a través del uso portal cautivo.

QoS Traffic Shaping
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.

Prevención de amenazas
- La tecnología adquirida debe ser parte de la agrupación internacional Cyber Threat Alliance (CTA) para compartir indicadores de compromiso (IoC) con otros fabricantes líderes de ciberseguridad en base al framework de MITRE ATT&CK, con el fin de mejorar la protección de los clientes a través de la detección de contenido malicioso como: archivos, nombres de dominio, direcciones IP y URI's.
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ-LOZADA TORATO Jefe Dpto. de Sistemas SILSA

garantía del software con el fabricante.

- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets).
- Debe contar con un motor antimalware local basado en Machine Learning o IA (inteligencia artificial).
- Debe identificar y bloquear la comunicación con redes de botnet.
- Debe incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca.
- El fabricante del equipamiento de seguridad debe haber obtenido una efectividad de seguridad con calificación mínima de "A" en el último reporte de CyberRatings ENTERPRISE FIREWALL.
- Soportar Threat Feeds mediante cualquier de los siguientes métodos: STIX, servicios web, archivos o texto.
- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante provisto desde su nube.
- Tener habilitado la protección que al hacer una descarga por http/https, debe soportar modificar archivos (reconstruido durante su análisis) eliminando componentes riesgosos (código, link).

Filtro de Contenido

- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Debe tener capacidad de actualizar la base de datos de URLs y categorías desde el servicio de inteligencia del fabricante.
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL.
- Tener por lo menos 100 categorías de URL de al menos 500 millones de sitios y direcciones URL categorizadas.
- Permitir el bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón "Continuar" para que el usuario pueda seguir teniendo acceso al sitio).
- Debe permitir filtrar videos de Youtube por ID de canal, usuario o video.
- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Soportar la identificación de archivos comprimidos.
- Soportar la identificación de archivos cifrados.

Gestión en SDWAN

- Deberá ofrecer un Control de tráfico consciente de aplicaciones, con definición de políticas granulares de aplicación, selección de rutas basada en SLA de aplicaciones, medición dinámica de ancho de banda de rutas SD-WAN, reenvío activo/activo y activo/en espera, soporte superpuesto para transporte cifrado, dirección basada en sesiones de aplicaciones, mediciones SLA basadas en sonda.
- Deberá ofrecer un mecanismo de corrección de errores avanzada (FEC) Advanced SD-WAN (WAN remediación), Forward Error

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ AZABACHE TORATO Jefe Dpto. de Sistemas SILSA

Correction (FEC) para compensación de pérdidas de paquetes, duplicación de paquetes para el mejor rendimiento en tiempo real de las aplicaciones, integración con Active Directory para políticas de dirección SD-WAN basadas en usuarios, agregación de enlace por paquete con distribución de paquetes entre miembros agregados.

Gestión y Reportes

- La gestión de los firewalls podrá realizarse desde los mismos equipos o desde una consola de gestión centralizada provista en appliance por el mismo fabricante de los firewalls.
- La interfaz de gestión debe permitir visualizar como mínimo el estado y consumo de: CPU, memoria, interfaces de red y estado del licenciamiento.
- La interfaz de gestión debe permitir crear, modificar o borrar: interfaces de red físicas y lógicas, objetos de red, configuraciones o perfiles de seguridad, políticas de seguridad, VPNs.
- Debe contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.
- La gestión de logs y reportes deberá ser realizada desde la nube del fabricante, y deberá cumplir con las siguientes características:
    - Debe poder mostrar los equipos o host comprometidos en función de las direcciones IP, URLs y/o dominios observados en el tráfico que pasó por el firewall.
    - Debe poder generar alertas de manera automática vía correo electrónico, SNMP y/o syslog.

5.4. CONDICIÓN DEL CONTRATISTA

La nube del fabricante deberá contar con las siguientes características:

- Debe contar con la certificación SOC2 y/o ISO 27001 a fin de garantizar la privacidad y seguridad del contenido de los archivos analizados, y deberán estar alineados a la Ley de Protección de Datos Personales Ley N°29733. Cualquiera de las certificaciones mencionadas o su equivalente debe ser presentado para la firma del contrato.

5.5. ENTRENAMIENTO SOBRE EL FUNCIONAMIENTO

a. El proveedor deberá brindar transferencia de conocimiento sobre el equipo implementado considerando las funcionalidades adquiridas de la solución para al menos 4 personas por un tiempo no menor a 6 horas.
b. El entrenamiento se deberá realizar dentro del rango de fechas de la implementación de la solución por un instructor certificado por el fabricante y de forma remota.

5.6. INSTALACIÓN

a. El postor deberá realizar la instalación de la solución ofertada en el centro de datos de SILSA, la cual deberá ser realizada por personal certificado por el fabricante de dicha solución o representante en el país de la marca ofertada (sustentada con carta original del fabricante o subsidiaria local), debiendo asignar por lo menos un ingeniero titulado o técnico especialista

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas SILSA

con certificación de la marca, adjuntando copia de su título profesional, copia de sus credenciales de certificación vigente en la marca del fabricante.

b. El proveedor deberá entregar un plan de trabajo detallado 5 días antes de la instalación, el cual será revisado y aprobado por la Oficina de Sistemas de SILSA.
c. El proveedor, al finalizar la puesta en producción, deberá entregar un informe detallado de todas las actividades para la puesta en producción según su plan de trabajo.
d. El postor deberá incluir una carta del fabricante o documento dirigido a la entidad en la que se especifique que es representante de la marca y que esta capacitado para brindar soporte del producto ofertado en el presente proceso.

5.7. MANTENIMIENTO

a. La solución debe incluir actualizaciones gratuitas de firmas, soporte técnico-operativo durante el tiempo de vigencia de la garantía en modo 24x7.
b. El SOC del proveedor se encargará de dar ayuda y/o apoyo al personal técnico de la entidad para cualquier configuración o habilitación de reglas que no haya sido posible realizar, siendo este trabajo dentro de los tiempos de respuesta establecidos.
c. Realizar actualizaciones de parches, nuevas versiones del Sistema Operativo del equipo, y funcionalidades que libere el fabricante por el plazo de vigencia de las licencias que será de 12 meses.
d. Tiempos de respuesta de atención no mayor a 2 horas.
e. Tiempo de resolución de incidentes no mayor a 4 horas.
f. Monitoreo de la plataforma a través del SOC 24x7x365.
g. Backup semanal de la configuración del equipo la cual deberá ser almacenada localmente.
h. Soporte remoto vía web o telefónica.
i. Soporte de hardware con reemplazo de equipo en un plazo no mayor de 3 días.

5.8. OTRAS CONSIDERACIONES

a. Los equipos y componentes ofertados serán de últimas versiones.
b. Todos los componentes del hardware deben ser del mismo fabricante y tener número de parte para garantizar su completa compatibilidad en tecnología, funcionalidad y rendimiento.
c. Los equipos deben ser provistos con sus respectivos cables de alimentación eléctrica para los tomacorrientes de norma IEC C13, (200 VAC, 60 Hz).
d. El servicio debe comprender la instalación y puesta en producción hasta dejar la solución 100% operativa en la infraestructura de TI de la Oficina de Sistemas.
e. Deberá encontrarse activa la licencia y/o software que permita el uso de las funcionalidades del equipo ofertado, incluyendo los módulos y/o componentes contratados.

5.9. GARANTÍA COMERCIAL

a. La garantía comercial para el equipo de Seguridad Perimetral – Firewall es mínima 01 año contado a partir de la fecha de la culminación de la implementación o puesta en funcionamiento al 100%.
b. La garantía comercial incluye el servicio de soporte en la solución de

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas SILSA

incidentes que afecten el normal desempeño de la solución, las veinticuatro (24) horas del día, los siete (07) días de la semana incluyendo sábados, domingos y feriados (24x7x365), vía telefónica y/o remota.

c. La garantía cubre el soporte remoto, se dará con un tiempo de respuesta no mayor a dos (02) horas después de registrado el incidente a través de una mesa de ayuda y/o correo electrónico.
d. El diagnóstico y asistencia técnica remota para problemas, cuando se solicita atención a través de un número de teléfono asignado y/o mesa de ayuda y/o correo electrónico. La asistencia técnica cubrirá el período de cobertura para aislar el problema y remotamente diagnosticar, remediar y resolver el problema.

5.10. OBLIGACIONES DEL PROVEEDOR GANADOR

Brindar asistencia de forma remota en la implementación y poner en funcionamiento el equipo firewall, la misma que incluye lo siguiente:

- Configuración inicial del Firewall
- Configuración de SD-WAN y sus políticas
- Firewall / NAT
- VPN IPsec
- Pruebas y ajustes

6. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

El Contratista se compromete a guardar la más absoluta reserva, a fin de garantizar la seguridad e integridad de los procesos, programas, datos e información pertenecientes a la empresa SERVICIOS INTEGRADOS DE LIMPIEZA S.A. - SILSA. Así como, a no violar la confidencialidad, seguridad y propiedad de los datos, archivos, programas y sistemas de aplicación, sin la respectiva autorización por escrito por parte de la empresa SERVICIOS INTEGRADOS DE LIMPIEZA S.A.- SILSA, absteniéndose a efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, no pudiendo facilitar a terceros, bajo ningún concepto, información alguna.
El Contratista y los colaboradores contratados para la realización de la presente prestación, se encuentran obligados a mantener la confidencialidad de la información que reciban u obtenga como resultado de la ejecución del presente Contrato. El incumplimiento de esta obligación es causal de resolución de la Orden de Servicio, sin perjuicio de la indemnización por los daños y perjuicios ocasionados a la empresa SERVICIOS INTEGRADOS DE LIMPIEZA S.A. - SILSA.

Por lo antes expuesto, el Contratista del servicio NO podrá:

- Difundir, transmitir y/o relevar información a terceros
- Usar la información recopilada para ofrecer, promocionar o brindar información sobre productos y servicios
- Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por la empresa SERVICIOS INTEGRADOS DE LIMPIEZA S.A. - SILSA o como consecuencia del servicio brindado.
- Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias y/o eventos.

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas SILSA

El Contratista del servicio será responsable de todos los daños y perjuicios que para la empresa SERVICIOS INTEGRADOS DE LIMPIEZA S.A. - SILSA que se deriven como consecuencia del incumplimiento doloso o culposo de las obligaciones citadas.

7. MODALIDAD DE LA EJECUCIÓN

La modalidad de ejecución es llave en mano, la adquisición del bien debe cumplir con las especificaciones técnicas descritas, el cual incluye la entrega del equipo, soporte remoto en la instalación, puesta en funcionamiento y adiestramiento del funcionamiento.

8. ENTREGABLE

El proveedor deberá remitir el entregable dentro del plazo de ejecución detallado en el numeral 9 del presente documento, a través de la plataforma digital de SILSA (mesa de partes virtual) https://facilita.gob.pe/t/1485, o presencialmente por mesa de partes de SILSA, ubicado en calle Los Negocios 336, Surquillo – Lima, de lunes a viernes en el horario de 8:15 am - 5:15 pm.

El entregable consta de lo siguiente:

i. Copia de la guía de remisión por la entrega del equipo.
ii. Registro / reporte de la implementación de la solución
iii. Informe final del proyecto

9. LUGAR DE ENTREGA

Se deberá realizar la entrega del equipo de Seguridad Perimetral – Firewall en el almacén de SILSA ubicado en calle Nugget 145 – Lima, de lunes a viernes (días hábiles) en el horario de 8:15 am - 5:15 pm.

10. PLAZO DE ENTREGA

EL plazo total para la entrega e implementación del equipo es de máximo 20 días calendario, que inicia a partir del día siguiente de notificada la orden de compra.

11. REQUISITOS Y RECURSOS DEL PROVEEDOR

El postor deberá ser partner o representante del equipo de Seguridad Perimetral – Firewall ofertado, para lo cual deberá presentar una carta del fabricante, donde se acredite el nivel de partner o representante de la marca.

12. CONFORMIDAD DE LOS BIENES

La conformidad será otorgada por la Oficina de Sistemas de Información, la misma que deberá ser otorgada en un plazo máximo de siete (07) días calendario, luego de la entrega del bien y presentación del entregable.

13. FORMA DE PAGO.

El pago se efectuará en una (01) sola armada, una vez entregado el bien y los entregables, previa conformidad por parte del área usuaria.

14. PENALIDADES

Si el proveedor no cumple con las actividades encomendadas dentro del plazo estipulado, la Entidad le aplicará una penalidad por cada día de atraso hasta por un monto máximo equivalente al 10% del monto del contrato. La penalidad se aplicará automáticamente y se calculará de acuerdo con la siguiente fórmula:

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LANEZ-LOZADA FORATO Jefe Dpto. de Sistemas SILSA

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

- Para plazos menores o iguales a 60 días F=0.40
- Para plazos mayores a 60 días F=0.25

La Entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la Obligación.

15. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo de un (01) año, contado a partir de la conformidad otorgada por SILSA.

16. CLAUSULA ANTICORRUPCION

El proveedor deberá garantizar no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al objeto de la prestación. Asimismo, el proveedor se obliga a conducirse en todo momento, durante la ejecución de la prestación, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, el proveedor se compromete a comunicar a las autoridades competentes cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar las medidas apropiadas para evitar los referidos actos o prácticas; y comunicar el hecho a través del Canal de Denuncias disponibles en la página institucional de SILSA.

El proveedor afirma con carácter de declaración jurada que no ha cometido o cuenta con sentencia consentida o ejecutoriada por delitos de concusión, peculado, enriquecimiento ilícito, tráfico de influencias, corrupción, lavado de activos y financiamiento del terrorismo, así como delitos cometidos en remates o procedimientos de selección o delitos equivalentes en otros países.

El proveedor se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

El proveedor es consciente que, de no cumplir con lo anteriormente expuesto, SILSA podrá resolver el contrato e iniciar las acciones administrativas, civiles y/o penales que correspondan según la normativa vigente.

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas SILSA

17. REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/.120,000.00 (ciento veinte mil y 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 bienes similares a los siguientes: Equipos de Seguridad Perimetral UTM. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[1], correspondientes a un máximo de veinte (20) contrataciones . En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones. 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

[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".

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Licitaciones SILSA

	la documentación sustentatoria 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. **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".*

SERVICIOS INTEGRADOS DE LIMPIEZA S.A. SILSA V°B° CESAR JAVIER LAINEZ LOZADA TORATO Jefe Dpto. de Sistemas