

ANEXO N° 01

DETALLE DEL REQUERIMIENTO	
Área usuaria / Área técnica estratégica	Gerencia Central de Planeamiento Innovación y Tecnología
Número de Cuadro Multianual de Necesidades	268
Objetivo estratégico	C1. Optimizar la infraestructura tecnológica institucional y el valor de los datos
Denominación de la Contratación	Servicio de Alquiler y licenciamiento de Firewall para Redes Inalámbricas
Persona de contacto del AU/ATE	Fernando Gabriel Chacchi Niño

FINALIDAD PUBLICA	El presente proceso tiene como finalidad contratar el servicio de Firewall para redes inalámbricas y el servicio de Web Scraping con el fin de brindar protección a los dispositivos y servidores de web scraping de la Superintendencia, contribuyendo con mejorar el desempeño de las funciones y metas a través de la adecuada gestión de seguridad en la Superintendencia.
OBJETIVO DE LA CONTRATACION	El objetivo es la contratación del alquiler y el licenciamiento de Firewall para las redes inalámbricas a fin de brindar la protección a los dispositivos que se conectan de forma inalámbrica y servicio de web scraping

CARACTERÍSTICAS DEL SERVICIO

CARACTERÍSTICAS TÉCNICAS

- Se solicita un (01) equipo Firewall con características de NGFW (Next Generation Firewall) y un Spare del mismo modelo como medida de contingencia. El equipo spare debe encontrarse disponible dentro de las instalaciones de la Superintendencia en el caso se presente algún problema de hardware y se necesite un reemplazo.
- El Firewall debe ser un appliance de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), consola de administración y monitoreo en un solo equipo.
- Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- El Firewall debe tener licencias para: IPS, VPN (GW to GW, Client to GW), Threat Protection, Antimalware o Antibot y/o Antispyware, el cual tiene que estar incluido en la propuesta enviada.
- El software deberá ser ofrecido en su versión más estable y/o más avanzada.
- Los equipos deben ser nuevos, sellados y sin uso.
- En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan anunciado su "End-of-life", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 4 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante.



SUPERINTENDENCIA

DE BANCA, SEGUROS Y AFP

República del Perú

- La solución debe ser capaz de operar en modalidad capa 3, modalidad in-line (bridge) y L2 (Port mirroring).
- El Firewall ofertado debe realizar inspección profunda en todos los niveles de la capa OSI.
- El Firewall debe permitir la creación de políticas con capacidad de seleccionar campos como direcciones y redes, identificador de usuarios y aplicaciones.
- La solución debe ser capaz de crear políticas basadas en aplicaciones y determinar el comportamiento de estas.
- El Firewall debe analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- El Firewall debe permitir filtro de tráfico VoIP, implementando filtraje de protocolos SIP, H.323, MGCP.
- El Firewall debe filtrar tráfico IP del tipo IPv4 e IPv6. Estas reglas deben ser configurables tanto por CLI (Command Line Interface), como por GUI (Graphical User Interface).
- El Firewall debe filtrar de manera optimizada protocolos P2P independiente de los puertos TCP utilizados para su comunicación.
- El Firewall debe filtrar de manera optimizada protocolos de comunicación instantánea como Yahoo, Messenger, Skype, Gtalk. El proveedor debe especificar cómo filtra y permite este tipo de protocolos.
- El Firewall debe implementar protecciones contra ataques XSS y/o SQL Injection. La solución debe ser compatible y certificada (USGV6 en Firewall e IPS) para trabajar en IPv6.
- El Firewall debe ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6.
- El Firewall debe soportar protocolos de enrutamiento RIP, OSPF (v2 y v3) y BGP.
- El Firewall debe soportar protocolo multicast y servidor multicast, implementando protocolos IGMP, PIM-SM, PIM-SSM o PIM-DM y otros que el proveedor indique.
- El Firewall debe soportar VLAN tagging y creación de zonas de seguridad en base a VLAN.
- El proveedor deberá tener disponibilidad de protocolo de ruteo IPv4 e IPv6, los cuales deberán estar habilitados para su uso.
- El Firewall va a tener un enlace de 100Mbps para la salida a internet conectado al firewall virtual.
- Sobre el equipo firewall, el contratista podrá brindar un equipo temporal mientras se culmina el proceso de importación e implementación del equipo solicitado en las bases. Así mismo el equipo temporal será retirado una vez que se culmine con la implementación final. El inicio de servicio no será condicionado a la implementación del equipo final.

HARDWARE

- El Firewall debe ser un equipo de propósito específico. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PC's o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
- El Firewall debe ser provisto con al menos 6 interfaces de cobre 1GE RJ45, con capacidad de crecer hasta ocho (08) interfaces 1GE RJ45.
- El Firewall debe contar con 1 (una) interfaz de red 10/100/1000 dedicada para la administración o se podría utilizar una interfaz física del Firewall para este propósito.
- El Firewall debe soportar por lo menos un IPS Throughput de 3 Gbps
- El Firewall debe soportar como mínimo un Throughput de NGFW 2 Gbps.
- El Firewall debe soportar como mínimo en sesiones concurrente de 2 Millones.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

- El Firewall debe soportar como mínimo Threat Protection Throughput de 1.5Gbps.
- El Firewall debe soportar como mínimo dos (02) Firewalls virtuales, dentro del mismo appliance.
- El Firewall deberá estar listo para la configuración y habilitación del segundo firewall virtual.
- El Firewall debe soportar como mínimo la creación de 5000 políticas de Firewall.
- El Firewall debe soportar como mínimo la creación de 190 VPN Site to Site.
- El Firewall debe soportar como mínimo la cantidad de 100K nuevas conexiones por segundo.
- El Firewall debe soportar como mínimo una fuente de poder AC a 220v.
- El Firewall debe tener IPv6 habilitado.

THREAT PREVENTION

- El Firewall debe poseer módulo de IPS, Antivirus y Anti-Spyware y/o Antibot integrados en el propio appliance.
- Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware).
- Cuando se utilicen las funciones de IPS, Antivirus y Antibot y/o Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente.
- Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
- Debe permitir excepciones por dirección IP de origen o de destino deben ser posibles en las reglas, de forma general y firma a firma.
- Debe permitir el bloqueo de vulnerabilidades y exploits conocidos.
- Debe incluir seguridad contra ataques de negación de servicios.
- Deberá poseer los siguientes mecanismos de inspección de IPS.
- Análisis de patrones de estado de conexiones.

FIREWALL MANAGEMENT

- La Superintendencia debe tener la gestión con nivel administrador del Firewall ofertado, el cual se solicitará soporte local 24x7 al proveedor y soporte del fabricante 24x7 en el tiempo que dure el contrato de servicio.
- La administración de las políticas de seguridad debe realizarse sobre los mismos appliance de seguridad, sin necesidad de un servidor o appliance aparte. El Firewall debe contar con Interfaz gráfica de usuario (GUI), vía Web por HTTP y/o HTTPS compatible al menos con, Windows, Linux y Mac OS
- El Firewall debe contar con una interfaz gráfica de usuario (GUI) la cual se podrá elegir al menos entre los idiomas inglés y español.
- El Firewall debe poseer comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet).
- El Firewall debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales.
- La solución cuenta con la capacidad de asignar un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. (RBAC).



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

IMPLEMENTACIÓN DEL SERVICIO

Para el servicio de implementación del Firewall NGFW se va a requerir lo siguiente:

- Creación de un (01) FW virtual, con su correspondiente acceso a Internet.
- El Firewall virtual es para migrar las políticas de nuestro antiguo Firewall para accesos móviles.
- En este Firewall virtual debe configurarse cuatro (04) VLAN: tres (03) DMZ y una VLAN (01) para la salida a internet.
- Los Firewalls virtuales no se van a conectar entre sí.
- Se deberá habilitar la protección de url filtering.
- La Superintendencia proporcionará al proveedor, el ambiente adecuado para la instalación de sus servicios, tales como puntos de energía estabilizada con protección eléctrica, aire acondicionado de precisión, espacio en rack o gabinete para instalación de equipos y puntos de acceso a red LAN.
- La Superintendencia brindará las facilidades necesarias dentro de sus instalaciones para realizar los trabajos que requiera el servicio solicitado.
- El servicio solicitado se brindará en la sede la Superintendencia ubicada en calle Los Laureles 214, San Isidro. En el caso de que la entidad cambie de sede, se notificará al contratista oportunamente.
- El ingeniero implementador deberá estar certificado en la marca del equipo firewall ofertado, lo que acreditará de forma previa al inicio del servicio.
- Se deberá presentar el certificado a nivel profesional de administración y/o soporte y/o implementación en la marca de firewall ofertado, para el ingeniero implementador.

SOPORTE TÉCNICO

- El proveedor deberá brindar soporte técnico o similar, que opere en formato 24x7x365, las 24 horas del día durante los 365 días del año, incluyendo los domingos y feriados. El soporte debe contar con personal en la marca ofertada para la resolución de averías en los equipos y/o servicios ofrecidos. Para tal fin, se entenderá por avería una interrupción parcial, total y/o degradación del servicio bajo soporte técnico.
- La Superintendencia podrá reportar una avería telefónicamente o por correo electrónico, considerándose todas estas formas igualmente válidas. Finalizado el reporte de la avería, el centro de soporte deberá proporcionar un código de avería para el posterior seguimiento de esta. Posteriormente, a solicitud de la Superintendencia, el proveedor deberá proporcionar información del estado de la avería reportada. La Superintendencia deberá contar con acceso prioritario al centro de servicio, para la atención inmediata de las notificaciones de avería.
- Para la resolución de averías reportadas, el personal técnico del proveedor deberá apersonarse a las instalaciones de la Superintendencia, salvo que previamente y por mutuo acuerdo entre el personal técnico de ambas partes (proveedor y Superintendencia), se convenga que dicho soporte sea remoto.
- Las atenciones de averías deberán estar disponibles sin límite de horas por intervención, ni cantidad de intervenciones mensuales, dándose por atendido una avería cuando es solucionado en su totalidad y a satisfacción de la Superintendencia.
- No podrá modificarse el nivel, calidad, periodicidad, categoría o cualquier otra característica de estos servicios durante el período de duración del servicio, sin consentimiento de la Superintendencia.
- El proveedor deberá tomar las previsiones del caso, a fin de no perjudicar el inicio de las labores diarias en la Superintendencia en el momento de la implementación del servicio. La Superintendencia



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

proporcionará las facilidades necesarias para realizar los trabajos dentro de sus instalaciones y fuera de horarios laborales, de ser necesario.

- El proveedor deberá proporcionar la información de los contactos respectivos (número de teléfonos y correos electrónicos) y un cuadro de escalamiento comercial, de post-venta y atención de averías y/o asistencia técnica para el inicio del servicio.

REQUISITOS DEL PROVEEDOR

El proveedor debe ser un representante autorizado en el Perú para comercializar la solución ofertada la cual debe ser evidenciada con alguno de los siguientes documentos:

- a) Carta del fabricante, que acredite que el postor es representante y/o distribuidor y/o partner autorizado en el Perú, para brindar el servicio de la solución ofertada
- b) Carta del distribuidor autorizado por el fabricante para acreditar al postor como representante y/o distribuidor y/o partner autorizado en el Perú, para brindar el servicio de la solución ofertada

Sin perjuicio de lo anteriormente indicado, la Entidad se reserva el derecho de verificar los documentos presentados por el proveedor, verificando su condición de representante y/o distribuidor y/o partner autorizado por el fabricante.

LUGAR Y PLAZO DE EJECUCIÓN	<u>LUGAR DE EJECUCION DEL SERVICIO:</u> Calle Los Laureles 214, San Isidro. En el caso de que la entidad cambie de sede, se notificará al contratista oportunamente. <u>PLAZO DE IMPLEMENTACION:</u> El plazo de implementación iniciará con la firma del Acta de inicio de implementación y se ejecutará, como máximo, hasta un día antes del 21 de junio de 2026. Se solicitará la firma de las siguientes actas como constancia del servicio: • Acta de inicio de implementación. Se firmará en un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de la firma del contrato. • Acta de inicio de servicio. Realizada la implementación, el personal asignado por la Superintendencia verificará que el firewall cuenta con las configuraciones y servicios requeridos. <u>PLAZO DEL SERVICIO DE ALQUILER Y LICENCIAMIENTO:</u> El periodo efectivo del servicio de alquiler y licenciamiento será de 365 días calendarios y entrará en vigencia a partir del 21 de junio de 2026.
-----------------------------------	--

ENTREGABLES

1. Acta de inicio de servicio, suscrito por el proveedor y la entidad, y documento emitido por el fabricante, acreditando la activación del licenciamiento, señalando las fechas de inicio y de fin (incluir la información adicional que se requiera).



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

El acta de inicio de servicio y documento emitido por el fabricante debe enviarse en formato digital (PDF) a través de mesa de partes dirigido a la Gerencia de Tecnología de información.

CONFORMIDAD

1. El área responsable es el Departamento de Ciberseguridad
2. En el caso del primer mes, se deberán contar con los siguientes documentos:
 - Acta de inicio del servicio, suscrita por ambas partes
 - Documento que acredite la vigencia del servicio suscrito.

PENALIDADES

La Superintendencia aplicará otras penalidades diferentes a las de mora, de acuerdo con la siguiente tabla:

1. POR INCUMPLIMIENTO EN LOS TIEMPOS DE RESOLUCION DE AVERIAS EN EL EQUIPO FIREWALL	
Criterio: Incumplimiento en la atención	% Deducible del pago mensual
Hasta 30 minutos	0 %
De 31 a los 40 minutos	2 %
De 41 a los 60 minutos	5%
De 61 al más minuto	10 %

Las penalidades podrán ser acumulables en un mismo periodo.

No se aplicará penalidad por causas atribuibles a la SBS o por causas externas al contratista, debidamente acreditadas.

Una vez comunicado al contratista los motivos por los cuales está incurriendo en penalidad, éste tendrá como máximo cinco (05) días calendario para remitir sus descargos mediante un informe debidamente fundamentado y evidenciado, dicho documento será evaluado por la Gerencia de Tecnologías de Información de la Superintendencia. Se emitirá un informe con el resultado de dicha evaluación indicando si corresponde la aplicación de penalidades, adjuntando los documentos que lo acrediten.

FORMA Y CONDICIONES DE PAGO

El servicio se pagará, en doce (12) cuotas iguales mensuales, previa conformidad mensual del Departamento de Ciberseguridad de la Gerencia de Tecnologías de Información.

RESPONSABILIDAD POR VICIOS OCULTOS

2 años, contado a partir de la conformidad otorgada.

CLÁUSULAS ESPECIALES

a) RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas, y numeral 229.3 del artículo 229 de su Reglamento.

b) ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de LA SUPERINTENDENCIA en relación con el contrato. 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 SUPERINTENDENCIA, 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 SUPERINTENDENCIA.

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 SUPERINTENDENCIA el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

c) SOLUCIÓN DE CONTROVERSIAS:

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante conciliación.

NOMBRE COMPLETO DEL RESPONSABLE DEL AREA USUARIA / AREA TÉCNICA ESTRATEGICA
Robert Manuel Soto Manrique Jefe del Departamento de Ciberseguridad
FECHA: 17/04/2026

ANEXOS DE LA ORDEN DE SERVICIO/COMPRA (CLÁUSULAS DE ADHESIÓN)

CLÁUSULA PRIMERA.- ACEPTACIÓN DE LAS CONDICIONES DE LA CONTRATACIÓN

El CONTRATISTA conoce, acepta y se somete a las condiciones señaladas en los Términos de Referencia y/o Especificaciones Técnicas incluidas en la solicitud de cotización y es responsable de la veracidad de los documentos e información que presenta para la contratación.

CLÁUSULA SEGUNDA.- IMPEDIMENTOS PARA CONTRATAR CON EL ESTADO

El CONTRATISTA, conoce, acepta y confirma que no está impedido para Contratar con el Estado de acuerdo con el artículo 30, numeral 30.1 de la Ley General de Contrataciones Públicas N° 32069.

CLÁUSULA TERCERA.- PROHIBICIÓN DE NEPOTISMO

El CONTRATISTA conoce, acepta y confirma que no se encuentra inmerso en las prohibiciones establecidas en la Ley N° 26771, que establece la prohibición de ejercer la facultad de nombramiento y contratación de personal en el sector público, en caso de parentesco.

CLÁUSULA CUARTA.- SEGURIDAD DE LA INFORMACIÓN

EL CONTRATISTA conoce y acepta las condiciones sobre seguridad de la información establecidas por LA SUPERINTENDENCIA, que se detalla a continuación:

CONFIDENCIALIDAD

Se califica como confidencial toda la información obtenida, así como los informes y toda clase de documentos que produzca o tenga a su alcance EL CONTRATISTA para la ejecución del presente contrato.

Se entenderá como tal toda información de tipo económica, financiera, legal, contable, técnica, comercial, estratégica o de otro tipo, así como la información proveniente de la función de supervisión, que sea revelada por LA SUPERINTENDENCIA a EL CONTRATISTA, en forma oral, escrita, o por cualquier otro medio o soporte para la realización de la prestación contratada; así como cualquier análisis, recopilación, estudio, resumen, extracto o documentación de todo tipo que elabore o formule EL CONTRATISTA a partir de la Información Confidencial o documentación revelada por LA SUPERINTENDENCIA.

EL CONTRATISTA se obliga a cumplir con el deber de reserva respecto de dicha información, no pudiendo por tanto divulgarla sin autorización expresa de LA SUPERINTENDENCIA. Esta obligación subsistirá aún después de concluida la vigencia del presente contrato por un plazo mínimo de cinco (5) años.

EL CONTRATISTA se compromete a limitar el acceso a la información confidencial de forma tal que solo sea accesible a aquellas personas que necesariamente deban involucrarse en las conversaciones, tratativas y/o acuerdos mantenidos con LA SUPERINTENDENCIA.

EL CONTRATISTA responderá legalmente por los daños y perjuicios causados por el incumplimiento al deber de reserva al que se refiere esta cláusula.

INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN

EL CONTRATISTA se compromete a respetar y aplicar en la prestación que brinde, según correspondan, las políticas, principios, procedimientos, manuales y controles de los sistemas de gestión, metodologías, estándares y otros, referidos a seguridad de la información, establecidos por LA SUPERINTENDENCIA.

Prevía evaluación y conformidad de las áreas competentes, LA SUPERINTENDENCIA autorizará los accesos a recursos o herramientas propias de la institución y que sean requeridos por EL CONTRATISTA para la ejecución de la prestación materia del presente contrato. Una vez finalizado el contrato, todos los accesos serán retirados.

EL CONTRATISTA debe tomar medidas de protección de la información de LA SUPERINTENDENCIA que se encuentre almacenada en los equipos y/o dispositivos que requieran mantenimiento fuera o dentro de las instalaciones de LA SUPERINTENDENCIA.

EL CONTRATISTA adoptará las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de la información involucrada. Las medidas de seguridad deben ser apropiadas y acordes con la naturaleza y envergadura de tal información, a fin de evitar cualquier manejo contrario a la prestación contratada, incluyéndose, entre otros, a la adulteración, la alteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

EL CONTRATISTA deberá reportar a LA SUPERINTENDENCIA dentro de las cuarenta y ocho (48) horas siguientes a su ocurrencia, cualquier incidente de seguridad de la información, hallazgo o situaciones sospechosas que puedan poner en riesgo la citada información, relacionada con vulneraciones a la Confidencialidad, Disponibilidad, Integridad o Privacidad de la información de LA SUPERINTENDENCIA, a fin de adoptar, de ser el caso, las coordinaciones y acciones necesarias que correspondan.

EL CONTRATISTA al inicio de la prestación deberá proporcionar al área usuaria la información de los canales de contactos respectivos (números de teléfonos y correos electrónicos) y un procedimiento para el reporte de incidentes de seguridad de la información y ciberseguridad que incluya un cuadro de escalamiento comercial, de post-venta y atención de averías y/o asistencia de soporte técnico.

EL CONTRATISTA exime de toda responsabilidad a LA SUPERINTENDENCIA, sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación o demanda que pudiera derivarse de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la ejecución de la prestación por parte de EL CONTRATISTA o el uso de la misma por parte de LA SUPERINTENDENCIA.

El incumplimiento de lo dispuesto en la presente cláusula de Seguridad de la Información por parte de EL CONTRATISTA podrá ser causal de resolución del presente contrato¹, y asimismo, podrá dar lugar a la indemnización por daños y perjuicios que le corresponda a LA SUPERINTENDENCIA conforme a ley.

CLÁUSULA QUINTA.- DE PROTECCIÓN DE DATOS PERSONALES

DEL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

EL CONTRATISTA declara que se somete a las disposiciones previstas por la Ley de Protección de Datos Personales, su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias; por lo que los datos personales que se proporcionen, así como aquellos generados o recopilados en el marco del presente contrato serán tratados en forma confidencial y estarán sujetos a estrictas medidas de seguridad, conforme lo dispone la referida normativa.

EL CONTRATISTA en caso corresponda, acepta y reconoce la responsabilidad de sus trabajadores y cualquier personal a su cargo, de mantener permanentemente una absoluta y total reserva y confidencialidad respecto de los datos personales a que tengan acceso en el marco del presente contrato, la que subsistirá en forma permanente e indefinida.

DEL ENCARGO DEL TRATAMIENTO

En caso EL CONTRATISTA deba proporcionar datos personales de sus colaboradores o terceros para el tratamiento de los datos personales, así como en caso deba generarlos o recopilarlos cuando estos resulten necesarios en el marco del cumplimiento del presente contrato, ello no implicará de modo alguno la transferencia de los mismos, debiendo EL CONTRATISTA asumir en dichos casos, la condición de encargado del tratamiento en el marco de la Ley de Protección de Datos Personales, y de su Reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias.

EL CONTRATISTA declara conocer que asume la condición de encargado del tratamiento cuando corresponda y por tanto se compromete a no utilizar o tratar los datos personales proporcionados, generados o recopilados con una finalidad

¹ Artículo 164.1° literal a) del Reglamento de la Ley de Contrataciones del Estado.

distinta a aquella por la que le fueron entregados o por la que son generados o recopilados así como a no transferirlos o divulgarlos a terceros, con excepción de entidades públicas, cuando estas lo soliciten en el marco del cumplimiento de sus funciones debidamente sustentadas o el poder judicial cuando sea solicitado mediante la orden judicial correspondiente, debiendo notificar de ello a la otra parte, según corresponda, dentro de las 24 horas de recibido el requerimiento.

En caso EL CONTRATISTA asuma la condición de encargado del tratamiento de los datos personales que se le pudiera proporcionar, se compromete a conservarlos por el plazo de dos (2) años contados desde la culminación del presente contrato.

EL CONTRATISTA en caso corresponda, reconoce y acepta que podrá en cualquier momento, ser auditado por LA SUPERINTENDENCIA sobre las medidas aplicadas, en cumplimiento de la Ley de Protección de Datos Personales, su reglamento, y demás normas conexas. De comprobar LA SUPERINTENDENCIA el incumplimiento de esta cláusula podrá resolver el presente contrato e interponer las acciones legales a que hubiera lugar.

CLÁUSULA SEXTA.- OBLIGACIONES DEL CONTRATISTA

RESERVA Y USO DE LA INFORMACIÓN

EL CONTRATISTA acepta la obligación de guardar reserva sobre cualquier información de LA SUPERINTENDENCIA a la que haya tenido acceso con ocasión de la ejecución del presente contrato; a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros; a no utilizar la información vinculada al contrato con LA SUPERINTENDENCIA o el nombre, logo o cualquier medio que identifique a LA SUPERINTENDENCIA en cualquier promoción, publicidad o anuncio, sin previa autorización escrita de LA SUPERINTENDENCIA, a excepción de aquella información que LA SUPERINTENDENCIA o una autoridad judicial o arbitral autorice o disponga, o cuando se trate de información de dominio público, circunscrito para el uso que LA SUPERINTENDENCIA, autoridad respectiva o las normas vigentes permitan de manera expresa. El incumplimiento de esta obligación puede ser causal de resolución del presente contrato. Asimismo, esta obligación permanecerá vigente no obstante el vencimiento o la terminación del presente contrato, y su incumplimiento podrá conllevar a efectuar las acciones legales que correspondan.

La confidencialidad de la información, a que se refiere el párrafo precedente, alcanza a todo el personal y subcontratistas de EL CONTRATISTA, debiendo así constar en los correspondientes contratos que con estos se celebren.

FACILIDADES PARA LA INSPECCIÓN O VERIFICACIÓN

EL CONTRATISTA acepta y autoriza a LA SUPERINTENDENCIA para efectuar inspección o verificación en sitio, según la dirección indicada en su propuesta y/o contrato.

EL CONTRATISTA debe facilitar a LA SUPERINTENDENCIA, su(s) representante(s) y/u organismos reguladores o de fiscalización, el acceso a las instalaciones para la provisión de la prestación, en casos de auditorías, investigaciones e inspecciones de verificación de cumplimiento de las condiciones de la prestación. Estos accesos serán informados, autorizados y acordados con LA SUPERINTENDENCIA.

DEVOLUCIÓN Y ELIMINACIÓN DE LA INFORMACIÓN

Al vencimiento del presente contrato y mientras no se incumpla las condiciones de la prestación, EL CONTRATISTA debe devolver y eliminar toda la información que le haya sido proporcionada para el cumplimiento de las prestaciones materia del contrato, independientemente del soporte o formato en el que se encuentre almacenada; y, a mantener el compromiso de confidencialidad en forma indefinida, incluso luego de concluido el presente contrato.

EL CONTRATISTA está obligado a proveer evidencia de que dicha eliminación ha sido realizada, de acuerdo con las condiciones de la prestación a satisfacción de LA SUPERINTENDENCIA, en un plazo no mayor a cinco (5) días hábiles contados a partir de la fecha de culminación de contrato.

CLÁUSULA SÉTIMA.- CANALES DE COMUNICACIÓN DE LA SBS PARA RECIBIR REPORTES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los canales establecidos para tal fin son:

- ✓ Incidente de Seguridad Digital: A través del correo mesa-ayuda@sbs.gob.pe o en su defecto al número +51 1 630 9300.
- ✓ Incidentes relacionados a Seguridad Física: A través de la cuenta AA-seguridad@sbs.gob.pe o a través de una llamada telefónica al Departamento de Seguridad al anexo 1424 o 1425.

EL CONTRATISTA a solicitud de LA SUPERINTENDENCIA, debe proporcionar la información de los canales de contactos respectivos (números de teléfonos y correos electrónicos) y, de considerarlo necesario, un procedimiento para el reporte de incidentes de seguridad de la información y ciberseguridad que incluya un cuadro de escalamiento comercial, de post-venta y atención de averías y/o asistencia de soporte técnico.

CLÁUSULA OCTAVA.- SOBRE EL COMPROMISO Y CUMPLIMIENTO DE SEGURIDAD Y SALUD EN EL TRABAJO

El contratista conoce y acepta las obligaciones y responsabilidades sobre SST las mismas que se encuentra especificadas en la **Ley N° 29783, Ley de Seguridad y Salud en el Trabajo y sus modificatorias y el Reglamento Interno de Seguridad y Salud en el Trabajo de la Superintendencia.**

FACULTADES DE LA SUPERINTENDENCIA

El CONTRATISTA acepta y autoriza que LA SUPERINTENDENCIA se reserva el derecho de supervisar en cualquier momento los equipos, elementos, sitios de trabajo, personal y documentos que sean necesarios para evaluar el cumplimiento y aplicación de las normas de Seguridad y Salud en el Trabajo.

El CONTRATISTA acepta y autoriza que LA SUPERINTENDENCIA se reserva el derecho de paralizar las labores o actividades del personal DEL CONTRATISTA que incumpla los citados procedimientos y normas.

El CONTRATISTA conoce que LA SUPERINTENDENCIA se reserva el derecho de comunicar a la Autoridad de Trabajo cualquier incumplimiento por parte DEL CONTRATISTA relacionado con las Normas de Seguridad y Salud en el Trabajo materia del presente contrato.

El CONTRATISTA reportará al Servicio de Seguridad y Salud en el Trabajo de la Superintendencia los incidentes o accidentes ocurridos durante la jornada laboral, de acuerdo con los plazos establecidos en el **Decreto Supremo N° 006-2022-TR**

CLÁUSULA NOVENA. - PROHIBICIÓN DE DOBLE PERCEPCIÓN DE INGRESOS EN CASO DE PERSONAS NATURALES

EL CONTRATISTA conoce, acepta y confirma que no se encuentra incurso en lo dispuesto en el Artículo 38 de la Ley del Servicio Civil, Ley N° 30057², sobre Prohibición de doble percepción de ingresos.

² Ley del Servicio Civil, Ley N° 30057:

“Artículo 38. Prohibición de doble percepción de ingresos

Los servidores del Servicio Civil no pueden percibir del Estado más de una compensación económica, remuneración, retribución, emolumento o cualquier tipo de ingreso. Es incompatible la percepción simultánea de dichos ingresos con la pensión por servicios prestados al Estado o por pensiones financiadas por el Estado, salvo excepción establecida por ley. Las únicas excepciones las constituyen la percepción de ingresos por función docente efectiva y la percepción de dietas por participación en uno (1) de los directorios de entidades o empresas estatales o en Tribunales Administrativos o en otros órganos colegiados. Queda prohibida la percepción de ingresos por dedicación de tiempo completo en más de una entidad pública a la vez.”



«TipoExpedienteSbs» N° «NumExpedienteSbs»

**CONTRATO DEL SERVICIO DE ALQUILER Y LICENCIAMIENTO DE FIREWALL PARA REDES
INALÁMBRICAS**

Conste por el presente documento, el contrato del servicio de alquiler y licenciamiento de Firewall para Redes Inalámbricas, que celebra de una parte, la SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES, en adelante LA SUPERINTENDENCIA, con RUC N° 20131370564, con domicilio legal en la Av. Guillermo Prescott N° 185, distrito de San Isidro, provincia y departamento de Lima, representada por la señora María Elizabeth Rodríguez Pajuelo, identificada con DNI N° 41585678, según facultades que constan en la Resolución Administrativa N° 401-2025-GGH del 14 de agosto de 2025 y en la Resolución SBS N° 4449-2025 del 23 de diciembre de 2025; y de otra parte, la empresa _____, en adelante EL CONTRATISTA, con RUC N° _____, con domicilio legal en la _____, distrito de _____, provincia y departamento de Lima, representada por _____, identificado con DNI N° _____, según poder inscrito en la Partida N° _____, Asiento N° _____ del Registro de Personas Jurídicas de la ciudad de Lima, en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: OBJETO

El presente documento tiene por objeto contratar el servicio de servicio de alquiler y licenciamiento de Firewall para Redes Inalámbricas.

CLÁUSULA SEGUNDA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a S/ _____ (_____ con __/100 Soles), incluido impuestos.

Este monto comprende el costo total del servicio, incluyendo, de ser aplicable, todos los impuestos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA TERCERA: DEL PAGO

LA SUPERINTENDENCIA se obliga a efectuar el pago a EL CONTRATISTA en Soles, mediante doce (12) cuotas iguales mensuales, previa conformidad mensual del Departamento de Ciberseguridad de la Gerencia de Tecnologías de Información, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley General de Contrataciones Públicas.

Para efectos del pago a EL CONTRATISTA, LA SUPERINTENDENCIA debe contar con la siguiente documentación:

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el responsable del Departamento de Ciberseguridad de la Gerencia de Tecnologías de Información de LA SUPERINTENDENCIA.
- Comprobante de pago.

EL CONTRATISTA debe remitir su comprobante de pago, conformidad, entregables establecidos en los Términos de Referencia y cualquier documentación necesaria o adicional a través de la mesa de partes



o mesa de partes virtual de LA SUPERINTENDENCIA: <https://www.sbs.gob.pe/mesa-de-partes-virtual> con copia electrónica al siguiente correo: factura_logistica@sbs.gob.pe.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días contabilizados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

LA SUPERINTENDENCIA debe efectuar el pago dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

En caso de retraso en el pago por parte de LA SUPERINTENDENCIA, salvo caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley General de Contrataciones Públicas.

CLÁUSULA CUARTA: DEL PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

Plazo de Implementación: El plazo iniciará con la firma del Acta de inicio de implementación y se ejecutará, como máximo, hasta un día antes del 21 de junio de 2026.

Se solicitará la firma de las siguientes actas como constancia del servicio:

- Acta de inicio de implementación. Se firmará en un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de la firma del contrato.
- Acta de inicio de servicio. Realizada la implementación, el personal asignado por la Superintendencia verificará que el firewall cuenta con las configuraciones y servicios requeridos.

Plazo del servicio de alquiler y licenciamiento: trescientos sesenta y cinco (365) días calendarios y entrará en vigencia a partir del 21 de junio de 2026.

CLÁUSULA QUINTA: OTRAS PENALIDADES

La Superintendencia aplicará otras penalidades diferentes a las de mora, de acuerdo con la siguiente tabla:

1. POR INCUMPLIMIENTO EN LOS TIEMPOS DE RESOLUCION DE AVERIAS EN EL EQUIPO FIREWALL	
Criterio: Incumplimiento en la atención	% Deducible del pago mensual
Hasta 30 minutos	0 %
De 31 a los 40 minutos	2 %
De 41 a los 60 minutos	5%
De 61 al más minuto	10 %

Las penalidades podrán ser acumulables en un mismo periodo. No se aplicará penalidad por causas atribuibles a LA SUPERINTENDENCIA o por causas externas al contratista debidamente acreditadas.

Una vez comunicado al contratista los motivos por los cuales está incurriendo en penalidad, éste tendrá como máximo cinco (05) días calendario para remitir sus descargos mediante un informe debidamente fundamentado y evidenciado, dicho documento será evaluado por la Gerencia de Tecnologías de Información de la Superintendencia. Se emitirá un informe con el resultado de dicha evaluación indicando si corresponde la aplicación de penalidades, adjuntando los documentos que lo acrediten.



SUPERINTENDENCIA

DE BANCA, SEGUROS Y AFP

República del Perú

CM 186-2026-SBS

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por el requerimiento y sus anexos, la oferta de EL CONTRATISTA, así como los documentos derivados del proceso de contratación que establezcan obligaciones para las partes, incluyendo las modificaciones contractuales y adendas aprobadas por LA SUPERINTENDENCIA, de ser el caso.

CLÁUSULA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, conforme a lo dispuesto en el numeral 81.3 del artículo 81 de la Ley General de Contrataciones Públicas, y el artículo 330 de su Reglamento.

CLÁUSULA OCTAVA: GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

CLÁUSULA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA SUPERINTENDENCIA: Av. Guillermo Prescott N° 185, distrito de San Isidro, provincia y departamento de Lima y/o a la Mesa de Partes Virtual (<https://servicios.sbs.gob.pe/mpv>).

DOMICILIO DEL CONTRATISTA: _____

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

EL CONTRATISTA señala el siguiente correo electrónico para efectos de las notificaciones que se realicen durante la ejecución del presente contrato, que no se realicen a través del SEACE: _____

La variación del correo electrónico aquí declarado debe ser comunicada a LA SUPERINTENDENCIA, formalmente y por escrito, con una anticipación no menor de cinco (5) días calendario.

Las partes lo firman en señal de conformidad en la ciudad de Lima, «Día» de «Mes» de «Año»

"LA SUPERINTENDENCIA"

"EL CONTRATISTA"

«NombreCompleto»

«Puesto»