

FORMATO DE CONTRATO MENOR DE SERVICIOS Y CONSULTORÍAS

DETALLE DEL REQUERIMIENTO	
Área usuaria / Área técnica estratégica	Gerencia de tecnologías de información / Gerencia Central de Planeamiento Innovación y Tecnología
Número de Cuadro Multianual de Necesidades	256
Objetivo estratégico	N° 6: Contar con un diseño organizacional, procesos, tecnología e infraestructura que busquen la eficiencia y contribuyan al logro de las metas y la rendición de cuentas en la SBS.
Denominación de la Contratación	Suscripción del software Burp Suite Profesional para revisiones manuales de vulnerabilidades
Persona de contacto del AU/ATE	Bruno Paolo Guzmán Fonseca
Compatibilización	RESOLUCIÓN SBS N° 03550-2025
FINALIDAD PUBLICA	El proceso tiene como finalidad la suscripción de licencias de software Burp Suite Profesional y complementos de pruebas manuales de seguridad en aplicativos webs que permitan realizar la búsqueda, clasificación y generación de reportes de mitigación de vulnerabilidades encontradas en los aplicativos webs ya desplegados haciendo uso de las pruebas manuales de seguridad disponibles usando el software. De esta manera se contribuye con mejorar el desempeño, calidad, funcionalidad y seguridad de los aplicativos webs desarrollados por el Departamento de Desarrollo de Software, como parte de estrategia institucional para mejorar la seguridad de los aplicativos webs desarrollados.
OBJETIVO DE LA CONTRATACION	El objetivo del proceso es la suscripción de cuatro (04) licencias de Burp Suite Profesional y cuatro (04) licencias del complemento Burp Bounty Pro, para realizar pruebas manuales de seguridad en aplicaciones web. Esta herramienta permitirá identificar y reportar vulnerabilidades, verificar falsos positivos detectados y reducir el riesgo de explotación por parte de atacantes, fortaleciendo así la seguridad de los aplicativos webs desarrollados por la Superintendencia.
CARACTERISTICAS DEL SERVICIO	
CARACTERÍSTICAS TÉCNICAS	
<ul style="list-style-type: none"> • Cuatro (04) licencias del Software Burp Suite Profesional. • Cuatro (04) licencias del complemento Burp Bounty Pro. • El software deberá permitir a los clientes poder escanear desde el primer día de activada la licencia. • El software debe estar basada en una tecnología on premise. 	



- El software no debe tener limitante del número de targets que pueden escanearse.
- Deberá analizar rápidamente los aplicativos webs.
- Deberá disponer de opciones de personalización de los escaneos.
- Deberá de clasificar y puntuar las vulnerabilidades según estándares tales como CVSS, CVE, CWE.
- Deberá poder analizar aplicativos desarrollados en diferentes lenguajes de programación, entre estos .NET y JAVA.
- Deberá permitir generar reportes en diversos formatos, mínimo HTML y CSV.
- El software luego del análisis de vulnerabilidades deberá dar la ruta y/o payload usado para la comprobación de la vulnerabilidad.
- El software debe tener la opción de poder analizar aplicativos que contengan formularios de accesos.
- Posibilidad de transferir licencias entre computadoras.
- Deberá contar con actualizaciones automáticas.
- Deberá contar con plantillas preconfiguradas de escaneo.

SOPORTE TÉCNICO

- El servicio deberá incluir soporte técnico local bajo un esquema de atención 8x5 (lunes a viernes, de 08:00 a 17:00 horas), por un periodo de dos (02) años.
- El proveedor deberá contar con un centro de soporte técnico operativo en el mismo horario, con personal especializado para la atención y resolución de averías, entendidas como interrupciones totales, parciales o degradaciones del servicio.
- Los incidentes podrán ser reportados vía telefónica o correo electrónico, debiendo el proveedor asignar un código de avería para su seguimiento. A solicitud de la Superintendencia, se deberá informar el estado del incidente reportado. Asimismo, se deberá garantizar acceso prioritario al centro de atención para casos críticos.
- Tiempo de respuesta: máximo de 30 minutos desde el reporte hasta el primer contacto técnico.
- Tiempo de resolución: no mayor a ocho (08) horas desde el reporte.
- La atención podrá realizarse de forma remota mediante herramientas de conexión seguras por Internet, en coordinación con el personal de la Superintendencia. En caso necesario, se requerirá intervención presencial siguiendo los protocolos establecidos.
- El proveedor deberá entregar, al inicio del servicio, la siguiente información: Información de contacto (teléfonos y correos) del equipo de soporte. Cuadro de escalamiento técnico, comercial y postventa.
- El soporte técnico deberá garantizar la continuidad operativa y el acceso a actualizaciones del fabricante durante la vigencia del servicio. No se establecerá límite de intervenciones ni de horas por atención, considerándose cerrada una avería únicamente cuando haya sido resuelta en su totalidad y a satisfacción de la Superintendencia.

CAPACITACIÓN

El servicio de capacitación debe considerar lo siguiente:

- La duración mínima de la capacitación será de ocho (08) horas, e incluirá contenidos sobre instalación, administración, uso y configuración del software adquirido.
- La capacitación deberá contemplar la participación de al menos dos (02) personas de la Gerencia de Tecnologías de Información.
- La capacitación se realizará de forma virtual, a través de plataformas como Microsoft Teams, Webex, Zoom u otra equivalente, sin generar costo adicional para la Superintendencia.
- Se deberá proporcionar acceso a una plataforma de laboratorio en línea, disponible las 24 horas del día, que permita a los participantes practicar fuera del horario establecido para el taller.



- También se deberá incluir acceso a una plataforma de videos explicativos relacionados con temas de seguridad ofensiva, disponibles en todo momento para consulta posterior.
- El proveedor será responsable de proporcionar el contenido y material didáctico, incluyendo presentaciones, manuales y acceso a recursos adicionales.
- El proveedor deberá emitir certificados de capacitación por cada uno de los participantes.

Las fechas y horarios para el taller de capacitación, será validado previamente por el personal de la Superintendencia. La capacitación requerida, se debe llevar a cabo dentro de los primeros veinte (20) días calendario contado a partir de la suscripción del acta de inicio de servicio

REQUISITOS DEL PROVEEDOR

El proveedor debe ser un representante autorizado en el Perú, para brindar la comercialización de licencias de software Burp Suite Profesional; para lo cual se debe acreditar este requisito mediante 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 suscripción de software Burp Suite Profesional, o
- 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 suscripción de software Burp Suite Profesional.

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

El plazo de la suscripción y del soporte técnico local es de dos (02) años, contado a partir de la suscripción del acta de inicio de servicio.

La capacitación debe ejecutarse dentro de los primeros 20 días calendarios contado a partir de la suscripción del acta de inicio de servicio.

ENTREGABLES

1. Acta de inicio de servicio, suscrito por el proveedor y la entidad, y documento emitido por el fabricante, acreditando la activación de la suscripción, señalando las fechas de inicio y de fin (incluir la información adicional que se requiera).
Se presentará dentro de los cinco (5) días hábiles siguientes a la activación de la suscripción. El acta de inicio de servicio y documento emitido por el fabricante debe enviarse en formato digital (PDF) a través del correo electrónico segurinfo_sbs@sbs.gob.pe
2. Acta de conformidad de capacitación, suscrito por el proveedor y la entidad, y certificados de capacitación. Se presentará dentro de los diez (10) días hábiles siguientes a la finalización de las actividades de capacitación. El acta de conformidad deberá enviarse en formato digital (PDF) a través del correo electrónico segurinfo_sbs@sbs.gob.pe



CONFORMIDAD	<ol style="list-style-type: none">1. El área responsable es el Departamento de Ciberseguridad2. Para emitir la conformidad, se deberán contar con los siguientes documentos:<ul style="list-style-type: none">• Un (01) Acta de inicio del servicio, suscrita por ambas partes• Un (01) Acta de conformidad de capacitación, suscrita por ambas partes• Documento que acredite la vigencia del servicio suscrito con el fabricante.• Certificados de capacitación
FORMA Y CONDICIONES DE PAGO	Se realizará en un solo pago por el monto total contratado, luego de la activación del servicio de suscripción, la ejecución de la capacitación y la presentación de los entregables y posterior a la conformidad emitida por parte de la Gerencia de Tecnologías de la Información
RESPONSABILIDAD POR VICIOS OCULTOS	1 año, 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.

d) GESTIÓN DE RIESGOS:

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el 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. Los riesgos identificados se encuentran descritos en el Anexo A del presente requerimiento.

NOMBRE COMPLETO DEL RESPONSABLE DEL AREA USUARIA / AREA TÉCNICA ESTRATEGICA
ROBERT MANUEL SOTO MANRIQUE Jefe del Departamento de Ciberseguridad
FECHA: 10/10/2025

ANEXO A

Formato para identificar, evaluar y asignar riesgos					
IDENTIFICACIÓN DE LOS RIESGOS					
1	RIESGOS EN EL PROCESO DE CONTRATACIÓN (*)	Que el proveedor se encuentre impedido para contratar con el Estado			
	RIESGOS EN LA EJECUCIÓN DE LA PRESTACIÓN (**)	Incumplimiento, retrasos en los plazos de ejecución.			
EVALUACIÓN DE LOS RIESGOS					
2	RIESGO IDENTIFICADO	PROBABILIDAD DE OCURRENCIA		IMPACTO EN LA EJECUCIÓN DE LA PRESTACIÓN	
	Que el proveedor se encuentre impedido para contratar con el Estado	Baja	X	Baja	
		Media		Media	X
		Alta		Alta	
	Incumplimiento, retrasos en los plazos de ejecución	Baja	X	Baja	
		Media		Media	X
Alta			Alta		
ASIGNACIÓN DE LOS RIESGOS					
3	Que el proveedor se encuentre impedido para contratar con el Estado	Subgerencia de logística			
	Incumplimiento, retrasos en los plazos de ejecución	Contratista			

(*) A identificar por parte de la SL

(**) A identificar por parte del Área usuaria