

ANEXO N° 01

FORMATO DE CONTRATO MENOR DE SERVICIOS Y CONSULTORÍAS

DETALLE DEL REQUERIMIENTO	
Área usuaria (AU) o Área técnica estratégica (ATE)	Departamento de Soporte Técnico y Tecnologías de la información - GCPIT
Número de Cuadro Multianual de Necesidades	382
Objetivo estratégico	CS8. Modernizar la gestión institucional mediante la transformación del modelo operativo y la optimización de procesos clave, fortaleciendo la eficiencia, agilidad y capacidad de adaptación organizacional.
Denominación de la Contratación	Adquisición de Certificados para páginas Web SBS
Persona de contacto del AU o ATE	Luis Enrique Su Gonzales

1. FINALIDAD PÚBLICA

Garantizar la seguridad de la información, la autenticidad de los portales y servicios web institucionales, así como la continuidad operativa de los servicios digitales brindados por la SBS, en beneficio del público usuario, entidades supervisadas y personal interno, esto mediante la renovación de tres (03) certificados SSL para los portales web de la SBS, el servicio de correo electrónico y el software de inventario y despliegue de aplicaciones remotas en los equipos de cómputo.

2. OBJETIVO DE LA CONTRATACION

El presente proceso tiene como objeto contratar tres (03) certificados de seguridad SSL para los distintos servicios que brinda la SBS, incluyendo soporte técnico, para asegurar la vigencia de los mecanismos de seguridad implementados en los portales y servicios web institucionales de la SBS.

3. CARACTERÍSTICAS DEL SERVICIO

Los certificados SSL debe ser proporcionado digitalmente y tendrá las siguientes características

DESCRIPCIÓN DEL SERVICIO A CONTRATAR

a) Certificado Digital SSL tipo Wildcard, utilizado para los portales web institucionales bajo el dominio principal.

- Un (01) Certificado tipo Wildcard para el dominio *.sbs.gob.pe.
- Soportar la instalación en servidores Windows Server y Linux.
- Asegura subdominios ilimitados en un mismo servidor.
- Autenticación completa de la organización. Algoritmo de cifrado mínimo: SHA256.
- Compatible con: TLS 1.0, 1.1, 1.2 y 1.3
- Encriptación SSL de 2048-bits.
- Autenticación completa de la organización.
- Soporte ECC Algoritmo.



- Apoyo DSA Algoritmo.
 - Compatibilidad del navegador universal.
 - Licencias para varios servidores ilimitados.
 - Reemisiones gratuitas en caso sea necesario los primeros 30 días luego de emitido el certificado
 - Generación del archivo CSR gratuito.
 - Compatibilidad con el 99.9% de navegadores y dispositivos móviles
 - Compatibilidad con el 99.9% de servidores
 - Soporte para la exportación del certificado en diferentes plataformas soportadas (el certificado se instalará en varios servidores, el soporte deberá abarcar hasta en 2 servidores)
 - Asesoría y capacitación en la instalación de los certificados y las funciones adicionales, las cuales se darán como máximo hasta los 10 días posteriores a la entrega del certificado.
 - Soporte para cambios y consultas durante la vigencia del certificado.
 - Consola de gestión para la administración de los certificados (opcional)
 - Deberá tener activado el control de Revocación en línea.
 - El fabricante o emisor (compañía certificadora) debe de ser reconocida de manera nativa por los equipos de cómputo con Windows 10.
 - Opcional carta de garantía emitida por el fabricante
 - Opcional carta de soporte extendido emitida por el fabricante
- b) Certificado Digital SSL tipo EV (Extended Validation), utilizado para el servicio de correo electrónico institucional.**
- Un (01) Certificado SSL SAN Extended Validation.
 - Soportar la instalación en al menos dos servidores Windows Server 2012 o superior.
 - Compatible para la instalación con Microsoft Exchange 2013 o superior.
 - Válido para al menos tres nombres de dominio:
mailweb.sbs.gob.pe, autodiscover.sbs.gob.pe y outlook.sbs.gob.pe
 - Algoritmo de cifrado mínimo: SHA256.
 - Compatible con: TLS 1.0, 1.1, 1.2 y 1.3
 - Encriptación SSL de 2048-bits.
 - Autenticación completa de la organización.
 - Soporte ECC Algoritmo.
 - Apoyo DSA Algoritmo.
 - Compatibilidad del navegador universal.
 - Apoyo a la SAN (UC).
 - Soporte para IDN.
 - Licencias para varios servidores.
 - Reemisiones gratuitas en caso sea necesario los primeros 30 días luego de emitido el certificado.
 - Generación del archivo CSR gratuito.
 - Compatibilidad con el 99.9% de navegadores y dispositivos móviles
 - Compatibilidad con el 99.9% de servidores
 - Generación del archivo CSR gratuito.
 - Soporte para la exportación del certificado en diferentes plataformas soportadas (el certificado se instalará en hasta 2 servidores)
 - Asesoría en la instalación de los certificados y las funciones adicionales, las cuales se darán como máximo hasta los 9 días posteriores a la entrega del certificado.



- Soporte para cambios y consultas durante la vigencia del certificado.
 - Consola de gestión para la administración de los certificados (opcional).
 - Deberá tener activado el control de Revocación en línea.
 - El fabricante o emisor (compañía certificadora) debe de ser reconocida de manera nativa por los equipos de cómputo con Windows 10 y Windows 11.
 - Opcional carta de garantía emitida por el fabricante
 - Opcional carta de soporte extendido emitida por el fabricante.
- c) Certificado Digital SSL tipo Multidominio, utilizado para plataformas institucionales que requieren asegurar múltiples nombres de dominio.
- Un (01) Certificado SSL individual para el nombre IVANTICL.SBS.GOB.PE con posibilidad de incorporar nombres adicionales en caso sea requerido.
 - Soportar la instalación en servidores Windows Server y Linux.
 - Algoritmo de cifrado SHA-2, con niveles de 256, 384 y 512 bits.
 - Compatible con: TLS 1.2 y 1.3
 - Longitud de clave pública de 2048-bits
 - Autenticación completa de la organización.
 - Soporte de algoritmo ECC (X25519)
 - Apoyo DSA Algoritmo.
 - Compatibilidad del navegador universal.
 - Licencias para varios servidores ilimitados.
 - Reemisiones gratuitas en caso sea necesario los primeros 30 días luego de emitido el certificado.
 - Generación del archivo CSR gratuito.
 - Asesoría en la instalación de los certificados.
 - Soporte para cambios (en caso se tenga que instalar en otro servidor) y consultas durante la vigencia del certificado.
 - Deberá tener activado el control de Revocación en línea.
 - El fabricante o emisor (compañía certificadora) debe de ser reconocida de manera nativa por los equipos de cómputo con Windows 10 y Windows 11.
 - Opcional carta de garantía emitida por el fabricante
 - Opcional carta de soporte extendido emitida por el fabricante

4. REQUISITOS DEL CONTRATISTA / PERFIL DEL CONSULTOR

- El contratista deberá acreditar experiencia comprobable mínima de tres (03) años, en la provisión de certificados digitales SSL y en la implementación de servicios de seguridad web.
- El contratista deberá ser fabricante o partner o distribuidor autorizado de una Autoridad Certificadora reconocida, con facultades para comercializar y brindar soporte.
- El contratista deberá contar con personal técnico con conocimientos en servidores web (IIS, Apache, Nginx) y administración de certificados digitales.
- El contratista deberá contar con la capacidad para brindar soporte remoto o presencial Durante el proceso de renovación, instalación, validación y durante la vigencia del certificado digital ante incidencias o requerimientos relacionados al servicio contratado.

Previo a la formalización de la contratación el contratista deberá presentar los documentos que acrediten:



- Documento que acredite la condición de fabricante, partner, distribuidor o canal autorizado para la comercialización y soporte de certificados digitales SSL, emitido por la Autoridad Certificadora, el fabricante o su representante autorizado, o declaración jurada del postor sustentada con documentación comercial vigente.
- Copia simple de contratos, ordenes de servicio, constancias o conformidades emitidas por entidades públicas o privadas, que acredite una experiencia mínima de tres (03) años en la provisión de certificados digitales SSL y en la implementación de servicios de seguridad web

5. LUGAR Y PLAZO DE EJECUCIÓN

El plazo máximo de entrega del nuevo certificado será de veinte (20) días calendario contados desde el día siguiente a la recepción de la formalización del contrato, incluyendo la instalación, validación y entrega de la conformidad técnica.

El plazo de vigencia de los certificados será de 12 meses contados a partir de la fecha de activación del certificado digital por parte de la Autoridad Certificadora correspondiente. Cabe señalar que la activación del certificado deberá ser comunicada en la misma fecha de producida mediante correo electrónico dirigido al Departamento de Soporte Técnico y Servicios de Tecnología de la Información.

6. CONFORMIDAD

El Departamento de Soporte Técnico y Servicios de Tecnología de la Información será el responsable de supervisar la ejecución del servicio y emitir el acta de conformidad una vez verificada la correcta instalaciones y funcionamiento de los certificados SSL.

7. FORMA Y CONDICIONES DE PAGO

El pago por el monto total contratado se realizará en único pago, luego de la recepción del documento que acredite la vigencia del periodo de tiempo del servicio de soporte técnico contratado con el fabricante y luego de la conformidad del Departamento de Soporte Técnico y Sistemas de Tecnologías de Información mediante el documento "Acta de Conformidad".

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

8. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados, conforme a lo indicado en el literal c) del Artículo 69° de la Ley General de Contrataciones Públicas, por un plazo de un (01) año contado a partir de ser emitida el "Acta de Conformidad"

9. 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.



Asimismo, puede resolverse de forma total o parcial el contrato por mutuo acuerdo entre las partes, previa opinión del área usuaria y/o área técnica estratégica.

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 Contratistas 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
MARCOS ERNESTO AZAÑEDO ALVA Jefe del Departamento Soporte Técnico y Servicios de Tecnologías de Información
FECHA: 02 de febrero de 2026

Nota: El presente formato deberá ser remitido con memorando suscrito por el Superintendente Adjunto, secretario general o Gerente, y registrado a través del SIGGED como requisito indispensable para su atención.