SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

ANEXO N° 01

FORMATO DE CONTRATO MENOR DE SERVICIOS Y CONSULTORÍAS

DETALLE DEL REQUERIMIENTO	
Área usuaria o Área técnica estratégica	Gerencia de Tecnología de Información
Número de Cuadro Multianual de Necesidades	356
Objetivo estratégico	Ampliar presencia, accesibilidad, calidad y al alcance de los servicios de brinda la SBS
Denominación de la Contratación	Contratación del servicio de soporte técnico, suscripción de hosting y administración para CHATBOT en Microsoft Azure
Persona de contacto del AU o ATE	Jorge Luis Cordova Torres
Compatibilización	Resolución N° 00541 - 2026

FINALIDAD PUBLICA	La finalidad la Contratación del servicio de soporte técnico, suscripción de hosting y administración para CHATBOT en Microsoft Azure, que va a permitir la atención ciudadano, brindando orientación y respuesta automatizada a consultas relacionadas con los temas de competencia de la SBS, por parte del Departamento de Servicios al ciudadano (DSC) de la Gerencia de Conducta de Mercado e Inclusión Financiera (GCMIF). Con el asistente virtual se busca un mayor acercamiento de la Superintendencia a los usuarios digitales y colocará a nuestra institución a la vanguardia en Latinoamérica en lo referente a gobierno electrónico, con un rol proactivo en la orientación al ciudadano.
OBJETIVO DE LA CONTRATACION	Contratación del servicio de soporte técnico, suscripción de hosting y administración para CHATBOT en Microsoft Azure
CARACTERISTICAS DEL SERVICIO	
1. Gestionar aplicaciones web, indispensable la gestión de aplicaciones ChatBot, construidas utilizando Microsoft Bot Framework. 2. Permitir la integración con el IDE Visual Studio para publicación y depuración de las aplicaciones web. 3. Ofrecer plantillas para la construcción de aplicaciones web compatibles con la plataforma, indispensable para la construcción de aplicaciones ChatBot con Microsoft Bot Framework. 4. Ofrecer la opción de almacenamiento a través del producto Cosmos DB. 5. Permitir la interpretación de texto. 6. Permitir la detección de anomalías y moderación de contenido. 7. Permitir crear una capa conversacional de preguntas y respuestas sobre los datos. 8. Exponer un API que pueda ser consumido desde aplicaciones tipo web y/o ChatBot. 9. Capacidad de administrar las aplicaciones de reconocimiento de lenguaje desde un ambiente web.	

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

REQUISITOS DEL PROVEEDOR / PERFIL DEL CONSULTOR

1. El proveedor deberá ser un agente autorizado de Microsoft en el Perú, para prestar servicios de administración sobre la nube Azure. Para acreditarlo, deberá presentar un documento emitido por Microsoft.

2. Disponer de un Acuerdo de Nivel de Servicio - ANS con el proveedor de servicios en la nube, en el que queden claramente definidas las responsabilidades de la SBS y el proveedor de servicios en la nube, definiendo como mínimo:
   - Descripción del servicio.
   - Tipo de servicio.
   - Disponibilidad y cantidad de tiempo de inactividad máxima (diario, mensual) o porcentaje de tiempo (diario, mensual) que el servicio estará disponible para su uso.
   - Capacidad del servicio.
   - Mantenimiento (planificado o no planificado, horarios, formas de comunicación).
   - Tiempos de respuesta y tiempos de solución.

3. El proveedor de servicios en la nube deberá contar como mínimo con un certificado vigente durante toda la ejecución del servicio de seguridad de la información, así como con el resultado de la revisión (reporte) de assessment y basado en estándares internacionales, el mismo que tiene que ser emitido por una organización de auditoría independiente y que sea certificador (no basta con un certificado del mismo Certified Security Provider - CSP), como:
   - Federal Risk and Authorization Management Program (FedRAMP).
   - ISO/IEC 27001 Seguridad de la información.
   - ISO/IEC 27017 Controles de seguridad de la información basada en ISO/IEC 27002 específicamente para los servicios en nube.
   - ISO/IEC 27018 Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud, entre otros.

4. La infraestructura que soportará el servicio en nube deberá contar con el reporte de revisión independiente SOC 2 TIPO II vigente y durante la ejecución del servicio. Asimismo, como requisito para la suscripción del contrato, el proveedor ganador de la buena pro deberá presentar el reporte de revisión independiente SOC 2 Tipo II vigente, el documento deberá permanecer vigente durante la ejecución del servicio.

5. Realizar el cifrado, tanto de los datos en tránsito como de los datos almacenados, para proteger su confidencialidad, así como la creación de copias de respaldo para proteger su disponibilidad e integridad.

6. Requerir al proveedor de servicios en la nube, como mínimo el manejo de los siguientes protocolos de cifrado, los cuales se basan en estándares y algoritmos aceptados y probados por la industria:
   - AES (128 bits o superior).
   - TDES (Teclas de doble longitud).
   - RSA (1024 bits o superior).
   - ECC (160 bits o superior).

7. Permitir sincronizar el reloj del servicio en la nube con los relojes locales.

8. Disponer de registros de acceso que permitan monitorear, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

9. Los proveedores de servicios en la nube deberán proporcionar controles de identidad y acceso para restringir el acceso a la infraestructura y los datos de la SBS, cumpliendo para tal efecto con los estándares de cumplimiento, y observar las políticas de seguridad y cumplimiento de la nube, como: visibilidad, control y auditabilidad.

10. El proveedor de servicios en la nube deberá proporcionar información sobre todo cambio que pudiera afectar negativamente el servicio.

11. Otros que indiquen los "Lineamientos para el uso de Servicios en la Nube para las entidades de la Administración Pública del Estado Peruano" emitidos por la Secretaría de Gobierno Digital de la PCM.

12. El servicio que se provee en nube debe permitir la ejecución de revisión de vulnerabilidades por parte de la Superintendencia en forma coordinada. Asimismo, para contratar el servicio el proveedor debe presentar un reporte de ethical hacking de un tercero independiente realizado a la versión vigente del software ofertado, el mismo que no deberá tener vulnerabilidades con severidad media o superior. Sin perjuicio de lo anterior, antes de la salida de producción, la SBS deberá ejecutar una revisión de ethical hacking o test de penetración de los servicios expuestos o nuevos servicios que se han integrado a la plataforma de la SBS. Esta actividad deberá ser incluida en el plan de implementación de la plataforma si se encontraran hallazgos, se deberá realizar la remediación previa a la salida de producción y firma de la conformidad de la implementación, esta remediación deberá realizarse en el plazo siguiente:
    - CRÍTICA: 72 HORAS.
    - ALTA: 120 HORAS.
    - MEDIA: 240 HORAS.
    - BAJA: 360 HORAS.

13. El servicio deberá proveer informes de corte semestral o cuando libere una nueva versión de servicio de red team o test de penetración (de un tercero y no de la misma empresa) de caja negra y caja blanca. Asimismo, los plazos de remediación existentes de los hallazgos de estas pruebas son los siguientes:
    - CRÍTICA: 72 HORAS.
    - ALTA: 120 HORAS.
    - MEDIA: 240 HORAS.
    - BAJA: 360 HORAS.

14. En todos los casos, la métrica para evaluar la severidad es la del sistema CVSS (Common Vulnerability Scoring System) que comprende la evaluación de la gravedad y el riesgo de la seguridad del sistema informático.

15. El software ofertado debe tener usuarios de prueba para revisión o pruebas de vulnerabilidades, ethical hacking o test de penetración, para lo cual el proveedor de servicio en la nube deberá proporcionar a la Superintendencia las facilidades para realizar tal prueba.

16. La solución en nube debe contar con mecanismos de protección de amenazas y deberá incorporar controles de Web Application Firewall.

17. El gestor de la aplicación solo deberá estar alojado en un dominio que no debe tener un subdominio relacionado a sbs.gob.pe. El acceso solo deberá estar disponible para usuarios desde IP públicos desde la Superintendencia.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

LUGAR Y PLAZO DE EJECUCIÓN	El plazo de ejecución de la contratación del servicio será de un (01) año, del 19/03/2026 al 18/03/2027.

ENTREGABLES

Como parte de la prestación del servicio de hosting, administración, soporte técnico y actualización para el chatbot institucional "Sebas", el proveedor deberá entregar a la Superintendencia los siguientes entregables:

Entregable 1: Acta de inicio del servicio

- Contenido: Documento que formaliza el inicio del servicio, detallando el alcance, periodo de vigencia, datos de contacto del equipo de soporte, niveles de atención y condiciones generales del servicio.
- Forma de presentación: Documento digital en formato PDF.
- Área destinataria: Gerencia de Tecnologías de Información (GTI).
- Plazo de entrega: Dentro de los cinco (05) días hábiles posteriores a la suscripción del contrato.

Entregable 2: Informe de estado inicial del servicio

- Contenido: Informe que describa el estado operativo del chatbot y de la infraestructura administrada, incluyendo disponibilidad del servicio, componentes administrados, configuración general y validación de accesos a la plataforma.
- Forma de presentación: Documento digital en formato PDF.
- Área destinataria: Gerencia de Tecnologías de Información (GTI).
- Plazo de entrega: Dentro de los diez (10) días hábiles posteriores al inicio del servicio.

CONFORMIDAD

1. Area Responsable: Gerencia de Tecnología de Información
2. Requisitos: Validación de continuidad operativa del CHATBOT por parte del Departamento de Servicios al ciudadano (DSC) de la Gerencia de Conducta de Mercado e Inclusión Financiera (GCMIF).

FORMA Y CONDICIONES DE PAGO

Forma:

El pago se realizará en un (01) único pago, por el monto total del servicio de suscripción, previa conformidad de la Gerencia de Tecnologías de Información (GTI), luego de la presentación y validación de la documentación que acredite la activación y vigencia del período contratado del servicio.

Condiciones:

Para efectos del pago, el proveedor deberá presentar la documentación correspondiente dentro de los (3) días hábiles posteriores al inicio de la vigencia del servicio, la cual deberá estar dirigida a la Gerencia de Tecnologías de Información (GTI) de la Superintendencia, quien emitirá la conformidad respectiva.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Para efectos del pago de las contraprestaciones ejecutadas por EL CONTRATISTA, LA SUPERINTENDENCIA debe contar con la siguiente documentación:

- Documento en el que conste la conformidad de la prestación suscrita por el servidor responsable de la Gerencia de Tecnologías de Información.

- Comprobante de pago.

El contratista deberá remitir su Comprobante de pago, conformidad u otros documentos exigidos en las bases y requerimiento, 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 dirigida a la Subgerencia de Logística con copia al correo: facturación_logistica@sbs.gob.pe

RESPONSABILIDAD POR VICIOS OCULTOS

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado, de acuerdo con lo dispuesto por el literal c) del numeral 69.2 del artículo 69 de la Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento, por un plazo de un (01) año contado a partir de la Conformidad otorgada por la Superintendencia.

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 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.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

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, participacioncitas, 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
MARCO ROJAS AGUEDO Jefe del Departamento de Desarrollo de Sistemas
FECHA: 02/03/2026

ANEXO N° 02

<table>
<tr><th colspan="7">FORMATO PARA IDENTIFICAR, EVALUAR Y ASIGNAR RIESGOS</th></tr>
<tr><td rowspan="3">1</td><td colspan="6">IDENTIFICACIÓN DE LOS RIESGOS</td></tr>
<tr><td>RIESGOS EN EL PROCESO DE CONTRATACIÓN (*)</td><td colspan="5">o Demora en la respuesta del mercado.
o Presentación incompleta o incorrecta de la documentación requerida por parte del proveedor autorizado
o Cambios o restricciones en los Términos de Servicio de Microsoft Azure durante el proceso de contratación</td></tr>
<tr><td>RIESGOS EN LA EJECUCIÓN DE LA PRESTACIÓN (**)</td><td colspan="5">- Vulnerabilidades que expongan información no autorizada
- Interrupciones temporales en el servicio de Microsoft Azure
- Cambios imprevistos en las funcionalidades del software SaaS por decisión del fabricante</td></tr>
<tr><td rowspan="11">2</td><td colspan="6">EVALUACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="2">RIESGO IDENTIFICADO</td><td colspan="2">PROBABILIDAD DE OCURRENCIA</td><td colspan="2">IMPACTO EN LA EJECUCIÓN DE LA PRESTACIÓN</td></tr>
<tr><td colspan="2" rowspan="3">Demora en la respuesta del mercado</td><td>Baja</td><td></td><td>Baja</td><td>X</td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td></td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td colspan="2" rowspan="3">Presentación incompleta o incorrecta de la documentación requerida por parte del proveedor autorizado</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td colspan="2" rowspan="3">Cambios o restricciones en los Términos de Servicio de Microsoft Azure durante el proceso de contratación</td><td>Baja</td><td>X</td><td>Baja</td><td>X</td></tr>
<tr><td>Media</td><td></td><td>Media</td><td></td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td rowspan="4">3</td><td colspan="6">ASIGNACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="3">Vulnerabilidades que expongan información no autorizada</td><td colspan="3">Proveedor/ Logística</td></tr>
<tr><td colspan="3">Interrupciones temporales en el servicio de Microsoft Azure</td><td colspan="3" rowspan="2">Proveedor</td></tr>
<tr><td colspan="3">Cambios imprevistos en las funcionalidades del software SaaS por decisión del fabricante</td></tr>
</table>

(*) A identificar por parte de la SL
(**) A identificar por parte del Área usuaria