SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP
República del Perú

ANEXO N° 01

FORMATO DE CONTRATO MENOR DE SERVICIOS Y CONSULTORÍAS

Área usuaria / Área Técnica:	Departamento de Riesgo Tecnológico (DSRIT) de la Gerencia de Riesgos (GER) / Departamento de Soporte Técnico (DST -GCPIT)
Número de Cuadro Multianual de Necesidades	CMN 285
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	Servicio de Infraestructura nube para la implementación de Herramienta Suptech para el análisis de autoevaluaciones de ciberseguridad
Persona de contacto del AU o ATE	Daniel Orlando Maguiña Cordova (DSRIT) / Rober Felipe Vidal Endara (GTI)

I. FINALIDAD PÚBLICA

Fortalecer la capacidad de la SBS para supervisar, de manera más oportuna, consistente y eficiente, el cumplimiento de las disposiciones sobre ciberseguridad por parte de las entidades bajo su ámbito de supervisión. Ello contribuirá a proteger la estabilidad, seguridad y confiabilidad del sistema financiero, de seguros y privado de pensiones, en resguardo de los intereses de los usuarios y de la ciudadanía.

II. OBJETIVO DE LA CONTRATACIÓN

Contar con un ambiente de pruebas en nube, operativo y seguro, con capacidades de inteligencia artificial habilitadas, que permita al equipo del DSRIT explorar, configurar, validar y evaluar una herramienta Suptech para el análisis de evidencias y autoevaluaciones de ciberseguridad, así como obtener las especificaciones técnicas y funcionales necesarias para sustentar su futura implementación institucional.

III. CARACTERÍSTICA DEL SERVICIO

La SBS requiere contratar un servicio que combine infraestructura tecnológica en nube con asesoría técnica especializada, capacitación y soporte reactivo. El alcance comprende los siguientes componentes:

Se deja constancia que el servicio solicitado corresponde a suscripciones destinadas a pruebas y no requerirá ni tendrá conexión, integración o interconexión alguna con los servicios institucionales de la SBS, ni con su infraestructura tecnológica (en nube o local) o redes internas.

Los objetivos específicos del servicio son los siguientes:

- Disponer de un entorno de nube funcional y escalable que soporte el procesamiento, análisis y evaluación de evidencias de ciberseguridad.
- Definir una arquitectura segura que permita anonimización, así como filtros y validaciones sobre la información de entrada y salida.
- Contar con asesoría técnica especializada que acompañe al equipo del DSRIT en la configuración, puesta en marcha y afinamiento iterativo de los componentes de la solución.
- Generar las especificaciones técnicas y funcionales necesarias para la formulación del TDR definitivo orientado a la integración de la solución en el Core institucional.
- Capacitar al equipo técnico del DSRIT en la administración y mantenimiento del entorno de nube aprovisionado.

A) Componente A: Infraestructura tecnológica en nube

El contratista proveerá y administrará el entorno de infraestructura en nube requerido para la operación del ambiente de pruebas durante los diez (10) meses de vigencia del contrato, bajo un modelo de consumo variable. El entorno deberá cubrir, como mínimo, los servicios indicados en el siguiente cuadro:

Para efectos de la ejecución del servicio, se estima un consumo referencial de servicios cloud por un monto de hasta USD 8,800 (ocho mil ochocientos y 00/100 dólares), durante la vigencia del contrato, bajo el modelo de consumo variable.

COMPONENTE DE SERVICIO EN NUBE	DESCRIPCIÓN FUNCIONAL REQUERIDA
Almacenamiento y gestión de documentos	Almacenamiento de evidencias (políticas, procedimientos, manuales, reportes) con control de versiones, protección contra borrado accidental y restricción de acceso público. Soporte a múltiples formatos: PDF, Word, Excel, imágenes, presentaciones y correos electrónicos, entre otros.
Extracción y procesamiento de datos	Extracción automatizada de texto y tablas desde documentos mediante reconocimiento óptico de caracteres (OCR). Segmentación inteligente de documentos extensos (chunking). Generación de vectores de texto (embeddings) para búsqueda semántica.
Búsqueda y recuperación de información	Motor de búsqueda con capacidades de búsqueda exacta, por similitud y semántica. Indexación vectorial para consultas en lenguaje natural. Recuperación aumentada por generación (RAG) que conecte los resultados de búsqueda con modelos de lenguaje.
Inteligencia artificial generativa	Acceso a modelos de lenguaje de alto rendimiento para análisis automatizado de evidencias. Generación de propuestas de hallazgos, observaciones y brechas identificadas. Trazabilidad y auditabilidad de los resultados generados. Interfaz conversacional en lenguaje natural.
Orquestación y procesamiento	Ejecución de funciones sin servidor para coordinar el procesamiento de documentos. Procesamiento en lote (batch) para análisis masivos de documentación. Orquestación de tareas en respuesta a eventos.

COMPONENTE DE SERVICIO EN NUBE	DESCRIPCIÓN FUNCIONAL REQUERIDA
Almacenamiento de resultados estructurados	Base de datos para almacenar hallazgos, calificaciones y trazabilidad con consultas rápidas y eficientes. Soporte para modelos de datos flexibles. Capacidad de escalamiento automático.
Seguridad, accesos y auditoría	Gestión centralizada de identidades y permisos. Cifrado de datos en reposo y en tránsito (AES-256, TLS 1.2 o superior). Autenticación multifactor (MFA). Registro de auditoría de todas las acciones realizadas en la plataforma. Anonimización de información y controles de entrada y salida de información.

El contratista será responsable del aprovisionamiento, la configuración inicial de la infraestructura, el mantenimiento, las actualizaciones y la disponibilidad continua de los servicios incluidos. El entorno deberá restringir el acceso a las direcciones IP autorizadas por la SBS. Se aceptarán plataformas de nube de primer nivel con presencia de centros de datos en la región de América Latina, que cuenten con certificaciones de seguridad internacionales vigentes (ISO/IEC 27001, SOC 2 Type II u equivalentes).

B) Componente B: Asesoría técnica especializada

El DSRIT es la unidad responsable del desarrollo, configuración de las aplicaciones e implementación de la herramienta Suptech. El contratista pondrá a disposición de la SBS una bolsa de sesenta (60) horas de asesoría técnica especializada cuya finalidad es apoyar al equipo del DSRIT en la resolución de puntos de dolor, utilizables a lo largo de la vigencia del contrato conforme a la programación acordada entre el DSRIT y el contratista. Las horas cubren el acompañamiento directo al equipo del DSRIT en la configuración, puesta en marcha, afinamiento y validación de la solución, de acuerdo con los ámbitos detallados a continuación:

ÁMBITO DE ASESORÍA	ACTIVIDADES INCLUIDAS
Arquitectura y diseño técnico	Orientación técnica cuando el equipo del DSRIT encuentre decisiones sobre la arquitectura de la solución, selección de servicios del entorno de nube, diseño de flujos de procesamiento de evidencias y revisión de la integración entre componentes, considerando una arquitectura de seguridad que incluya criterios de anonimización y controles sobre la entrada y la salida de información.
Configuración y puesta en marcha de componentes	Asistencia técnica al equipo del DSRIT en la configuración de los servicios aprovisionados: conectores de almacenamiento, pipelines de extracción y transformación de datos, bases de datos vectoriales, parámetros de modelos de lenguaje, flujos RAG y lógica de orquestación.
Afinamiento de modelos y prompts	Apoyo para resolver problemas de precisión de prompts, estrategias de recuperación (RAG), parámetros de chunking y modelos de lenguaje para mejorar la precisión y relevancia de los resultados generados en el contexto de supervisión de ciberseguridad.

ÁMBITO DE ASESORÍA	ACTIVIDADES INCLUIDAS
Parametrización de frameworks de evaluación	Apoyo técnico en la configuración de los criterios de evaluación, controles y umbrales de calificación alineados a la normativa y procedimientos de supervisión de ciberseguridad de la SBS.
Validación y pruebas	Revisión conjunta a solicitud del DSRIT de resultados generados por la herramienta con documentos de prueba provistos. Identificación de errores, comportamientos inesperados y oportunidades de mejora.
Soporte para especificaciones del TDR definitivo	Apoyo técnico en la documentación de las especificaciones técnicas y funcionales derivadas del uso del ambiente de pruebas, orientadas a la formulación del TDR definitivo para la integración al Core institucional.

Las condiciones de uso de la bolsa de horas son las siguientes:

- El DSRIT es quien solicitará y programará las sesiones de asesoría con el contratista conforme a las necesidades que surjan durante el desarrollo.
- El DSRIT llevará un registro de consumo acumulado de horas, que se adjuntará a cada Informe Mensual (Entregable N.° 4).
- Los tiempos de respuesta para cada sesión de asesoría se acordarán entre las partes, con un plazo no mayor a dos (2) días hábiles para sesiones de soporte técnico y afinamiento, y de cinco (5) días hábiles para sesiones de diseño o documentación.
- La asesoría se prestará preferentemente de manera remota.
- El contratista deberá mantener vigente un canal oficial de atención (correo institucional o mesa de ayuda) y un punto de contacto formal designado desde el inicio del servicio.
- Las horas no consumidas al término del contrato no generan crédito ni devolución económica.

C) Componente C: Capacitación técnica

El contratista proveerá una capacitación técnica dirigida al equipo del DSRIT, orientada a habilitar la administración autónoma del entorno de nube. Los contenidos mínimos comprenden la arquitectura del entorno aprovisionado, la administración de usuarios y perfiles de acceso, el monitoreo del entorno y la respuesta ante incidencias básicas, y los procedimientos de carga de documentos y verificación del pipeline de procesamiento.

La capacitación tendrá una duración mínima de cuatro (4) horas cronológicas y podrá realizarse en forma remota, previa aprobación de la Superintendencia y contará con la entrega de material de capacitación en formato digital y se dictará hasta para un máximo de 5 personas. Para la capacitación y entrega del material el contratista tiene un plazo de treinta (30) días calendario de iniciado el contrato.

D) Soporte técnico reactivo

Durante la vigencia del contrato, el contratista proveerá soporte técnico reactivo en horario hábil (lunes a viernes, de 09:00 a 18:00 horas, hora de Lima), con los siguientes tiempos de atención:

- Severidad 1 – Incidentes críticos (el entorno no está operativo sin solución alternativa): respuesta máxima de cuatro (4) horas hábiles.

- Severidad 2 – Incidentes altos (degradación del servicio con solución alternativa temporal): respuesta máxima de veinticuatro (24) horas hábiles.
- Severidad 3 – Consultas y solicitudes de configuración: atención máxima de cuarenta y ocho (48) horas hábiles.

E) Modelo de responsabilidad compartida

ASPECTO	RESPONSABILIDAD DEL CONTRATISTA	RESPONSABILIDAD DE LA SBS
Infraestructura en nube	Aprovisionamiento, configuración inicial y mantenimiento de todos los servicios de nube requeridos. Actualizaciones, parches y disponibilidad de la plataforma.	No aplica.
Datos y acceso	Configuración de la infraestructura de almacenamiento. Cifrado en reposo y en tránsito. Gestión inicial de usuarios, roles y autenticación MFA. Eliminación certificada de datos al término del contrato.	Definición de usuarios y perfiles de acceso autorizados. Supervisión de actividad y logs de auditoría.
Configuración e implementación	Acompañamiento técnico al equipo del DSRIT durante la configuración de componentes y la puesta en marcha de la solución, en el marco de la bolsa de horas de asesoría.	El DSRIT es la unidad responsable del desarrollo, configuración e implementación de la herramienta. El contratista brinda soporte técnico especializado a solicitud del DSRIT.
Seguridad de aplicaciones	Configuración de controles de seguridad del entorno (WAF, IPS u equivalentes disponibles en la plataforma). Control de acceso por IP autorizada.	Definición de las direcciones IP autorizadas y políticas de acceso institucional.

COORDINACIONES:

El Departamento de Riesgo Tecnológico (DSRIT) de la Gerencia de Riesgos (GER) será la unidad responsable de la configuración e implementación, así como la coordinación con el contratista, la revisión de entregables y la emisión de conformidades. La Gerencia de Tecnologías de Información (GTI) brindará el apoyo técnico institucional necesario durante la ejecución del contrato.

El contratista es responsable exclusivamente de la provisión y mantenimiento de la infraestructura en nube, la bolsa de asesoría técnica especializada para soporte reactivo al DSRIT, la capacitación inicial sobre el entorno aprovisionado y el soporte técnico reactivo descrito en la sección III. Cualquier avance en el desarrollo de la herramienta corresponde al equipo del DSRIT.

SEGURIDAD DE LA INFORMACIÓN:

El entorno de nube deberá contemplar, como mínimo, las siguientes medidas de seguridad:

- Cifrado de datos en reposo y en tránsito mediante estándares reconocidos (AES-256, TLS 1.2 o superior).
- Gestión centralizada de claves de cifrado con soporte para claves administradas por el cliente (Customer Managed Keys).
- Autenticación multifactor (MFA) obligatoria para todas las cuentas de administración y operativas.
- Registro y auditoría de todas las acciones realizadas en la plataforma, con retención mínima de noventa (90) días.
- Monitoreo en tiempo real de eventos de seguridad y métricas de rendimiento.
- Restricción de acceso por lista blanca de direcciones IP autorizadas por la SBS.
- Controles de protección de aplicaciones en el entorno (WAF, IPS u equivalentes disponibles en la plataforma).

Toda la información obtenida, procesada o generada en el marco del contrato se califica como confidencial. El contratista se obliga a guardar reserva durante la vigencia del contrato y por un mínimo de cinco (5) años adicionales. El contratista reportará a la SBS dentro de las cuarenta y ocho (48) horas siguientes a su ocurrencia cualquier incidente de seguridad de la información que pueda comprometer la confidencialidad, integridad o disponibilidad de la información institucional.

Al vencimiento del contrato, el contratista devolverá y eliminará de forma certificada toda la información de la SBS almacenada en el entorno de nube en un plazo máximo de cinco (5) días hábiles, proporcionando evidencia documental que acredite la eliminación completa e irreversible de los datos.

Los canales de reporte de incidentes de seguridad de la información son los siguientes:

- Incidentes de Seguridad Digital: mesa-ayuda@sbs.gob.pe o al número +51 1 630 9300.
- Incidentes de Seguridad Física: AA-seguridad@sbs.gob.pe o al +51 1 6309000, Anexo 1424 o 1425.

OTRAS CONDICIONES:

Todo bien tangible e intangible producido como consecuencia de la ejecución del presente contrato (documentación técnica, configuraciones, arquitecturas, materiales de capacitación y demás desarrollos) será transferido a la SBS de forma exclusiva y sin costo adicional. El contratista es responsable por la calidad de los servicios prestados y por los vicios ocultos por un plazo de un (01) año contado a partir de la conformidad otorgada por la SBS. Se encuentra prohibida la subcontratación de la totalidad de las prestaciones. Las controversias se resuelven mediante conciliación y/o arbitraje, conforme a la normativa de contrataciones del Estado vigente.

El contratista deberá observar, en la medida en que sea aplicable, la siguiente normativa: Resolución SBS N.° 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad; Resolución SBS N.° 2116-2009 – Reglamento para la Gestión del Riesgo Operacional (y modificatorias); Ley N.° 29733 – Ley de Protección de Datos Personales y su Reglamento; estándares internacionales ISO/IEC 27001, ISO/IEC 27017 y NIST CSF; y demás documentos normativos internos de la SBS que sean comunicados al contratista durante la ejecución del servicio.

REQUISITOS DEL PROVEEDOR:

A) Experiencia del proveedor en la especialidad

El proveedor deberá acreditar lo siguiente:

CRITERIO	DESCRIPCIÓN
Requisito	El postor debe acreditar un monto facturado acumulado equivalente a USD 50,000.00 (cincuenta mil y 00/100 dólares) o su equivalente en soles al tipo de cambio vigente, por la prestación de servicios iguales o similares, durante los tres (3) años anteriores a la fecha de presentación de ofertas.
Servicios similares	Se consideran servicios similares: (i) provisión de servicios de infraestructura en nube (IaaS, PaaS o SaaS); (ii) implementación o acompañamiento técnico en soluciones de inteligencia artificial generativa, procesamiento de lenguaje natural o analítica avanzada; (iii) consultoría o asesoría técnica especializada en arquitecturas de nube y/o soluciones de inteligencia artificial; (iv) desarrollo de soluciones con componentes de machine learning o IA para el sector público, financiero, de seguros o regulatorio.
Acreditación	Contratos u órdenes de servicio con su respectiva conformidad o constancia de prestación, o comprobantes de pago cancelados con documentación que acredite el abono. Esta acreditación deberá de ser presentada junto con la cotización del proveedor.

B) Personal clave

El postor deberá acreditar la disponibilidad del siguiente personal clave durante la ejecución del servicio:

PERFIL	FORMACIÓN Y CERTIFICACIONES	EXPERIENCIA MÍNIMA REQUERIDA
Líder de Proyecto / Punto de Contacto	• Titulado o bachiller en Ingeniería de Sistemas, Informática, Software, Administración o afines. • Deseable: certificación en gestión de proyectos (PMP u equivalente) o metodologías ágiles.	Mínimo tres (3) años de experiencia **liderando** servicios de implementación o consultoría en soluciones de nube y/o inteligencia artificial.
Arquitecto / Especialista Técnico en Nube e IA	• Titulado o bachiller en Ingeniería de Sistemas, Informática, Software o afines. • Certificación vigente de arquitecto o especialista en nube emitida por el fabricante del servicio a proveer (mínimo 40 horas). • Deseable: certificación en IA/ML o procesamiento de lenguaje natural.	Mínimo tres (3) años de experiencia en diseño de arquitecturas en nube y/o implementación de soluciones de inteligencia artificial generativa, RAG o procesamiento de lenguaje natural.

PERFIL	FORMACIÓN Y CERTIFICACIONES	EXPERIENCIA MÍNIMA REQUERIDA
Especialista en Seguridad en Nube	• Titulado o bachiller en Ingeniería de Sistemas o afines. • Certificación en seguridad en nube (CCSK, certificación de seguridad del fabricante del servicio a proveer u equivalente) o en gestión de seguridad de la información (ISO/IEC 27001 LA).	Mínimo dos (2) años de experiencia en implementación de controles de seguridad en entornos de nube, incluyendo gestión de identidades, cifrado y registro de auditoría.

La acreditación del grado o título profesional se verificará en el Registro Nacional de Grados Académicos y Títulos Profesionales (SUNEDU) o en el Registro Nacional de Certificados, Grados y Títulos del Ministerio de Educación. En caso el grado o título no figure en los registros mencionados, el postor presentará copia del diploma respectivo

Para certificaciones, se presentará copia simple del certificado vigente.
.
La experiencia mínima requerida del personal clave se acreditará mediante currículum vitae documentado y/o declaración jurada simple suscrita por el representante legal del postor.

Los documentos de acreditación del personal clave deberán de ser presentados junto con la cotización del proveedor.

IV. LUGAR Y PLAZO DE EJECUCIÓN

LUGAR:
El servicio se prestará en forma remota en coordinación con el personal de Soporte Tecnico y personal del El Departamento de Riesgo Tecnológico de la GER.

PLAZO:
El servicio se prestará en un plazo de diez (10) meses calendario contados a partir del día siguiente de firmado el Acta de habilitación del entorno en nube, con sujeción a los plazos específicos de entrega establecidos en la sección entregables.

V. ENTREGABLES Y/O PRODUCTO FINAL

El proveedor deberá presentar los siguientes entregables:

N°	ENTREGABLE	DESCRIPCIÓN	PLAZO MÁXIMO
1	Plan de trabajo	Cronograma detallado de actividades de aprovisionamiento del entorno, calendario de uso de la bolsa de horas y mecanismos de coordinación con el DSRIT. Dentro de este plan también deberán de indicar el canal oficial de contacto, canal oficial de atención (correo institucional o mesa de ayuda).	5 días calendario desde la suscripción del contrato.

N°	ENTREGABLE	DESCRIPCIÓN	PLAZO MÁXIMO
2	Acta de habilitación del entorno en nube	Constancia de aprovisionamiento y configuración inicial del entorno, incluyendo verificación de servicios activos, gestión de accesos, cifrado y registro de auditoría.	20 días calendario desde la suscripción del contrato.
3	Acta de capacitación	Constancia de participación y entrega de material digital	30 días calendario desde la suscripción del contrato.
4	Informes mensuales de uso de la bolsa de horas y soporte	Informes mensuales acumulativos que sustenten el consumo de la bolsa de horas y el soporte brindado durante la ejecución del servicio, incluyendo las horas de asesoría consumidas, las actividades desarrolladas, el estado del entorno, las incidencias atendidas y el saldo de horas disponibles. Su presentación servirá de sustento para la conformidad del segundo pago.	Último día hábil de cada mes durante la vigencia del contrato.
5	Informe de cierre técnico y documentación del ambiente de pruebas	Documento técnico con la arquitectura implementada, componentes configurados, resultados de pruebas y especificaciones técnicas y funcionales útiles para la formulación del TDR definitivo.	Dentro de los últimos 15 días calendario antes de la finalización del contrato.
6	Acta de cierre y certificado de eliminación de datos	Acta de cierre del servicio y evidencia certificada de la eliminación total de la información de la SBS almacenada en el entorno de nube.	5 días hábiles posteriores a la finalización del contrato.

La SBS dispondrá de hasta tres (3) días hábiles posteriores a la presentación de cada entregable para formular observaciones. El contratista tendrá un plazo de dos (2) días hábiles para absolver dichas observaciones, y la SBS otorgará la conformidad en un plazo máximo de dos (2) días hábiles adicionales.

La presentación de los entregables se realizará mediante la Mesa de Partes Virtual https://www.sbs.gob.pe/mesa-de-partes-virtual, con copia a los analistas del DSRIT: jpolo@sbs.gob.pe y dmaguina@sbs.gob.pe.

VI. CONFORMIDAD

El Departamento de Riesgo Tecnológico de la GER y el Departamento de Soporte Técnico (DST) serán los encargados de brindar la conformidad del servicio.

VII. FORMA DE PAGO

El pago del servicio se realizará en dos (2) armadas, conforme al avance de ejecución, a la presentación y conformidad de los entregables asociados a cada hito y, en el caso de la bolsa de horas, al consumo efectivamente realizado durante la vigencia del contrato.

- Primer pago: contra la presentación y conformidad del Plan de trabajo (Entregable N.° 1), del Acta de habilitación del entorno en nube (Entregable N.° 2) y del Acta de capacitación (Entregable N.° 3), por el porcentaje del 50% del monto ofertado por el proveedor para los servicios cloud mencionados en el punto III, inciso A, así como por la totalidad de los servicios de habilitación del entorno en nube y capacitación.

- Segundo pago: contra la presentación y conformidad de los Informes mensuales de uso de la bolsa de horas y soporte (Entregable N.° 4), del Informe de cierre técnico y documentación del ambiente de pruebas (Entregable N.° 5) y del Acta de cierre y certificado de eliminación de datos (Entregable N.° 6). Este pago comprenderá el 50% restante del monto ofertado por el proveedor para los servicios cloud mencionados en el punto III, inciso A, así como las horas efectivamente consumidas de la bolsa de horas de asesoría técnica especializada, valorizadas al precio unitario ofertado.

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 del Departamento de Riesgo Tecnológico de la GER y el Departamento de Soporte Tecnico (DST).
- 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

VIII. PENALIDADES

N°	SUPUESTO DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	El contratista excede el tiempo de respuesta de cuatro (4) horas hábiles para incidentes de Severidad 1 (críticos: afectan la operatividad del entorno sin solución alternativa aceptable).	1.5% de 1 UIT por hora o fracción.	Informe del Departamento de Riesgo Tecnológico de la GER.
2	El contratista excede el tiempo de respuesta de veinticuatro (24) horas hábiles para incidentes de Severidad 2 (altos: degradan el servicio pero permiten continuidad operativa mediante solución alternativa temporal).	1.0% de 1 UIT por hora o fracción.	Informe del Departamento de Riesgo Tecnológico de la GER.
3	El contratista no entrega el Plan de Trabajo dentro del plazo de cinco (5) días calendario contados a partir de la suscripción del contrato.	5% de 1 UIT por día de atraso.	Informe del Departamento de Riesgo Tecnológico de la GER.

N°	SUPUESTO DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
4	Exfiltración o divulgación no autorizada de información confidencial de la SBS.	15 UIT por evento.	Informe del Departamento de Riesgo Tecnológico y/o del área de Seguridad de la Información.
5	El contratista no realiza la devolución y eliminación certificada de la información de la SBS dentro del plazo de cinco (5) días hábiles posteriores a la finalización del contrato.	20% de 1 UIT por día de atraso.	Informe del Departamento de Riesgo Tecnológico de la GER.

Las penalidades podrán acumularse. Una vez comunicado al contratista el motivo de la penalidad dispondrá de un plazo máximo de cinco (5) días hábiles para presentar descargos debidamente sustentados. No se aplicará penalidad por causas atribuibles a la SBS o a factores externos no imputables al contratista.

IX. 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 Publicas, por un plazo de un (01) año, contado a partir de la conformidad otorgada por la Superintendencia.

X. CLÁUSULAS OBLIGATORIAS

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.

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
MARCOS AZAÑEDO ALVA Jefe del Departamento de Soporte Técnico
Fecha: 01 de Junio de 2026

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

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.

Previa 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 contrato[1], 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] *Articulo 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° 30057[2], 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."