

MEMORANDO N° 00014-2026-DDS

A : Maria Elizabeth RODRIGUEZ PAJUELO
Subgerente de Logística

DE : Marco ROJAS AGUEDO
Jefe del Departamento de Desarrollo de Sistemas

ASUNTO : **REQUERIMIENTO - CONTRATACIÓN MENOR DE BIENES Y SERVICIOS**
Adquisición de Certificado Digital de Persona Jurídica para Agente Automatizado

REFERENCIA : Informe N° 009-2026 -DGED

FECHA : 13 de Julio de 2026

Por medio del presente, esta gerencia se dirige a usted para alcanzar a su despacho los términos de referencia para la adquisición de certificado digital de persona jurídica para el Agente Automatizado, con su respectivo servicio de soporte técnico y actualización, como resultado del informe N° 268 -2026 -SG remitido por Secretaría General sustentando dicha necesidad.

En el Anexo N° 01, se presentan los términos de referencia para la adquisición, con su respectivo servicio de soporte técnico y actualización del certificado digital de persona jurídica para el Agente Automatizado.

Cabe señalar que este proceso está incluido en el CMN N° 602

Para las coordinaciones relacionadas con este requerimiento, se ha designado al Sr. Juan Carlos Tovar, Arquitecto de Sistemas del Departamento de Desarrollo de Sistemas de la Gerencia de Tecnologías de la Información.

Finalmente, agradeciendo su atención al presente, esta gerencia queda a su disposición para cualquier consulta o coordinación adicional que considere conveniente.

Atentamente,

MARCO ANTONIO ROJAS AGUEDO
JEFE DE DESARROLLO DE SISTEMAS

JCT



ANEXO N° 01

FORMATO DE CONTRATO MENOR DE BIENES

DETALLE DEL REQUERIMIENTO	
Área usuaria / Área técnica estratégica	Departamento de Desarrollo de Sistemas - DDS (ATE) Departamento de Gestión Documental - DGED (AU)
Objetivo estratégico	P9. Ampliar la presencia, accesibilidad, calidad y el alcance de los servicios que brinda la SBS
Número de Cuadro Multianual de Necesidades	602
Denominación de la Contratación	Certificado digital de persona jurídica para firma mediante agente automatizado
Persona de contacto	Juan Carlos Tovar Ueda
FINALIDAD PUBLICA	La contratación busca garantizar la continuidad del servicio de firmado digital automatizado utilizado por la SBS para la emisión y validación de documentos electrónicos en el marco de sus funciones de supervisión, regulación y prestación de servicios al ciudadano, este servicio permite asegurar la emisión oportuna de las notificaciones derivadas de la Mesa de Partes Virtual, mediante el uso de firmas digitales automatizadas con plena validez jurídica, conforme a la Ley N.° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, contribuyendo a una gestión documental eficiente y a una adecuada atención de los ciudadanos.
OBJETIVO DE LA CONTRATACION	Garantizar la continuidad del servicio de firmado digital mediante agente automatizado, a través de la provisión del certificado digital correspondiente, a fin de asegurar la firma automatizada de documentos electrónicos generados por los sistemas institucionales, contribuyendo a la continuidad de los procesos de gestión documental y a la atención oportuna de los usuarios internos y ciudadanos.
CARACTERISTICAS TECNICAS	
La contratación comprende la adquisición de un (01) certificado digital de persona jurídica para su utilización por el agente automatizado de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS), incluyendo el servicio de soporte técnico y actualización por un período de doce (12) meses. El certificado digital será utilizado para la firma digital automatizada de documentos electrónicos generados por los sistemas institucionales, garantizando la continuidad del servicio de firmado digital implementado por la SBS.	



El certificado digital deberá cumplir, como mínimo, con las siguientes características:

- Corresponder a un certificado digital de persona jurídica para firma digital de agente automatizado.
- Tener una vigencia de doce (12) meses.
- Emitirse en formato PKCS#12 (.PFX o P12).
- Soportar el algoritmo criptográfico SHA-256 o superior.
- El Nombre Común (Common Name) y el correo electrónico del certificado deberán emitirse a nombre de una cuenta genérica administrada por la SBS, la cual será definida durante las coordinaciones previas a la emisión del certificado.
- Contar con certificado raíz e intermedio reconocidos por los principales sistemas operativos (Windows, Linux, entre otros) o, en su defecto, poner a disposición pública los certificados raíz e intermedios correspondientes.
- Toda la cadena de confianza (certificado raíz, certificados intermedios y certificado final) deberá haber sido emitida por una Entidad de Certificación acreditada por el INDECOPI e inscrita en el Registro Oficial de Prestadores de Servicios de Certificación Digital (ROPS), conforme a la normativa vigente.
- Incluir la clave privada o permitir su generación posterior a la emisión del certificado.
- Ser de uso exclusivo para firma digital, con las extensiones y propósitos de uso correspondientes para autenticación y firma digital.
- Permitir la firma digital de contenido electrónico, garantizando la autenticidad, integridad y no repudio de los documentos firmados.
- La Entidad de Certificación deberá publicar y mantener disponibles los servicios de validación del estado del certificado mediante OCSP (Online Certificate Status Protocol) y CRL (Certificate Revocation List), de conformidad con los estándares X.509 e IETF aplicables.
- Los servicios de consulta OCSP y descarga de la CRL deberán estar disponibles las 24 horas del día, los 7 días de la semana (24x7) durante toda la vigencia del certificado.
- En caso de incidentes que afecten la disponibilidad de los servicios de validación CRL/OCSP, el proveedor deberá brindar atención inmediata y ejecutar las acciones necesarias para el restablecimiento del servicio.

Por otro lado, el contratista deberá garantizar los siguientes niveles mínimos de servicio (SLA) durante la vigencia del certificado digital:

- La disponibilidad mensual de los servicios de validación de certificados mediante OCSP y CRL no deberá ser menor al 99.9 %, excluyendo los mantenimientos programados previamente comunicados por el proveedor.
- El proveedor deberá garantizar la disponibilidad de los servicios de validación del certificado mediante OCSP y CRL las veinticuatro (24) horas del día, los siete (7) días de la semana (24x7), durante toda la vigencia del certificado.
- El proveedor deberá brindar soporte técnico especializado para la atención de incidentes relacionados con la emisión, instalación, configuración, funcionamiento, validación, renovación y revocación del certificado digital.
- El proveedor deberá brindar soporte técnico especializado durante el horario laboral de lunes a viernes, mediante correo electrónico y/o teléfono. Para incidentes críticos que afecten la continuidad del servicio de firmado digital, el proveedor deberá contar con un mecanismo de atención y escalamiento que permita iniciar las acciones correspondientes en el menor tiempo posible.
- El tiempo máximo para el inicio de la atención de un incidente crítico reportado dentro del horario de atención del proveedor, no deberá exceder de una (1) hora, contada desde la comunicación efectuada por la SBS a través de los canales de soporte establecidos, los incidentes reportados fuera del horario de atención serán registrados a través de los canales habilitados y su atención se iniciará al siguiente día hábil, salvo que el proveedor disponga de un esquema de atención fuera del horario laboral.





- El tiempo objetivo para la solución de incidentes críticos que sean atribuibles al proveedor no deberá exceder de cuatro (4) horas, salvo aquellos casos debidamente sustentados cuya atención dependa de terceros o de la autoridad certificadora.
- El proveedor deberá disponer, como mínimo, de un canal de atención mediante correo electrónico y un canal telefónico para el registro y atención de incidencias, pudiendo adicionalmente ofrecer otros mecanismos de atención.
- El proveedor deberá comunicar oportunamente a la SBS cualquier mantenimiento programado que pudiera afectar la disponibilidad de los servicios, con una anticipación no menor de cuarenta y ocho (48) horas.
- En caso de presentarse una indisponibilidad del servicio que afecte la continuidad del firmado digital, el proveedor deberá realizar las acciones necesarias para restablecer el servicio e informar a la SBS sobre la causa del incidente y las acciones correctivas implementadas.

Asimismo, el contratista deberá brindar, durante toda la vigencia del certificado:

- Servicio de soporte técnico especializado durante toda la vigencia del contrato.
- Se debe brindar asistencia para la instalación, configuración, renovación y solución de incidentes relacionados con el certificado digital.
- Para incidentes críticos que afecten la emisión, renovación, revocación o validación del certificado, el soporte deberá estar disponible 24x7, mediante teléfono, correo electrónico o portal de atención.
- El tiempo máximo para el inicio de la atención de incidentes críticos será de 1 hora desde el reporte realizado por la SBS.
- El proveedor deberá mantener un mecanismo de escalamiento para incidentes críticos que comprometan la continuidad del servicio.
- El proveedor deberá realizar las actualizaciones necesarias para garantizar el correcto funcionamiento del certificado durante el período contratado.

REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS, REGLAMENTOS Y DEMÁS NORMAS

- Ley N.º 27269, Ley de Firmas y Certificados Digitales, y sus modificatorias.
- Reglamento de la Ley N.º 27269, aprobado mediante Decreto Supremo N.º 052-2008-PCM, y sus modificatorias.
- Infraestructura Oficial de Firma Electrónica (IOFE) y las disposiciones emitidas por la autoridad administrativa competente.
- Guía de Acreditación de la Infraestructura Oficial de Firma Electrónica (IOFE) y demás disposiciones técnicas vigentes aplicables a las Entidades de Certificación, Entidades de Registro o Verificación y Prestadores de Servicios de Certificación Digital.

ACONDICIONAMIENTO, MONTAJE O INSTALACIÓN

La instalación y configuración del certificado digital será realizada por personal de la SBS, el contratista únicamente deberá proporcionar el certificado digital y brindar soporte técnico cuando sea requerido.

ENTREGABLES

1. Entregable N.º 1: Emisión y entrega de un (01) certificado digital de persona jurídica para agente automatizado, en formato PKCS#12 (.PFX o P12), junto con la documentación necesaria para su instalación y uso (*Plazo: Hasta 10 días calendario contados desde el día siguiente de la suscripción del contrato, o desde la notificación de la orden de compra, según corresponda*).



El contratista debe remitir sus entregables y cualquier documentación necesaria o adicional a través del correo gti@sbs.gob.pe y gti-arquitectura@sbs.gob.pe, con copia a la Mesa de Partes Virtual de LA SUPERINTENDENCIA ubicada en la página web: <https://www.sbs.gob.pe/mesa-de-partes-virtual>.

GARANTÍA COMERCIAL

El contratista garantizará el correcto funcionamiento del certificado digital suministrado durante toda su vigencia, así como la prestación del servicio de soporte técnico asociado, en caso de presentarse fallas atribuibles al certificado digital, errores en su emisión, problemas relacionados con la cadena de certificación, validación CRL/OCSP o cualquier otro inconveniente imputable al proveedor que afecte su utilización, el contratista deberá realizar las acciones necesarias para su corrección, reemisión o reemplazo, sin costo adicional para la SBS.

El periodo de garantía será de doce (12) meses, contados a partir de la conformidad de la entrega del certificado digital o desde su fecha de emisión, según corresponda.

PRESTACIONES ACCESORIAS

Como prestación accesoria, el contratista deberá brindar soporte técnico especializado durante toda la vigencia del certificado digital, el cual comprenderá la atención de consultas e incidencias relacionadas con la emisión, instalación, configuración, funcionamiento, validación (CRL/OCSP) y, de ser necesario, la reemisión del certificado digital.

Asimismo, el contratista deberá proporcionar las actualizaciones necesarias de la cadena de certificación (certificados raíz e intermedios), cuando corresponda, y brindar el acompañamiento técnico requerido para garantizar la continuidad del servicio de firmado digital del agente automatizado.

REQUISITOS DEL PROVEEDOR

1. Comercializar certificados digitales emitidos por una Entidad de Certificación acreditada por el INDECOPI e inscrita en el Registro Oficial de Prestadores de Servicios de Certificación Digital (ROPS), conforme a la normativa vigente.
2. Ser representante, distribuidor, partner o canal autorizado en el Perú para la comercialización de certificados digitales de persona jurídica de la Entidad de Certificación acreditada.
3. Acreditar lo señalado en el numeral anterior mediante cualquiera de los siguientes documentos:
 - a. Carta emitida por la Entidad de Certificación acreditada, que certifique la condición de representante, distribuidor, partner o canal autorizado del postor.
 - b. Carta emitida por un distribuidor autorizado por la Entidad de Certificación, mediante la cual se acredite la condición de representante, distribuidor, partner o canal autorizado del postor.
 - c. Declaración jurada del postor en la que manifieste ser representante, distribuidor, partner o canal autorizado en el Perú para la comercialización de certificados digitales de persona jurídica, indicando la Entidad de Certificación correspondiente.
4. Contar con capacidad para brindar soporte técnico especializado durante toda la vigencia del certificado digital, de conformidad con los niveles de servicio establecidos en los presentes Términos de Referencia.

La SBS se reserva el derecho de verificar, en cualquier etapa de la contratación, la condición del postor como representante, distribuidor, partner o canal autorizado, así como la vigencia de la acreditación de la Entidad de Certificación en el ROPS y ante el INDECOPI.



LUGAR DE ENTREGA Y PLAZO DE EJECUCIÓN	El plazo de ejecución de la prestación será de trescientos sesenta y cinco (365) días calendario, contados a partir del día siguiente de la fecha emisión del certificado digital. El contratista deberá poner a disposición de la SBS el certificado digital dentro del plazo máximo de diez (10) días calendario, contados a partir del día siguiente de la suscripción del contrato (u Orden de Compra, según corresponda), mediante una plataforma virtual segura para su descarga e instalación o, de ser necesario, mediante asistencia remota proporcionada por personal especializado del contratista, previa coordinación con la SBS. La documentación asociada a la entrega del certificado digital, así como cualquier comunicación relacionada con la prestación del servicio, será remitida a los correos electrónicos gti@sbs.gob.pe y gti-arquitectura@sbs.gob.pe y a través de la Mesa de Partes Virtual. La prestación del servicio se realizará de manera remota, el certificado digital será descargado e instalado en el servidor institucional donde opera el agente automatizado de la SBS, previa coordinación entre el contratista y el personal técnico designado por la Entidad.
CONFORMIDAD	
Área que brinda la conformidad: Departamento de Desarrollo de Sistemas (DDS) 1. Requisitos del Proveedor: - Entregar el certificado digital de persona jurídica conforme a las características técnicas establecidas en los presentes Términos de Referencia, junto con las credenciales. - Facilitar (o realizar, de ser el caso) a la SBS el proceso de instalación y configuración del certificado digital en el servidor donde opera el agente automatizado o brindar el acompañamiento técnico necesario para su instalación. - Remitir la documentación correspondiente (técnica, operativa, etc.) a la entrega del certificado a los medios de entrega indicados en los Términos de Referencia.	
FORMA Y CONDICIONES DE PAGO	
1. Forma: <i>Pago Único.</i> 2. Condiciones: <i>Al inicio del servicio.</i> 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 ATE. - 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: factura_logistica@sbs.gob.pe.	
RESPONSABILIDAD POR VICIOS OCULTOS	
1 año, contado a partir de la conformidad otorgada por la Entidad.	



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 al 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
Marco ROJAS AGUEDO Jefe del Departamento de Desarrollo de Sistemas
FECHA: 13/Julio/2026



ANEXOS DE LA ORDEN DE SERVICIO/COMPRA (CLÁUSULAS DE ADHESIÓN REFERIDAS A SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES)

1. CLÁUSULA DE 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:

1.1. 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.

1.2. 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 DE PROTECCIÓN DE DATOS PERSONALES

2.1. DEL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

EL CONTRATISTA declara que se somete a las disposiciones previstas por la Ley N° 29733, 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.

2.2. 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.

¹ Artículo 68.1° literal b) del Reglamento de la Ley General de Contrataciones Públicas.

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 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.

Asimismo, los Oficiales de Datos Personales de LAS PARTES o de quien haga de sus veces podrán efectuar las medidas necesarias cuando se presente un incidente de seguridad relacionado a los datos personales.

2. CLÁUSULA DE OBLIGACIONES DEL CONTRATISTA

3.1. 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.

3.2. FACILIDADES PARA LA INSPECCIÓN

EL CONTRATISTA brindará las facilidades necesarias para inspecciones o verificaciones por parte de LA SUPERINTENDENCIA y/o organismos reguladores, siempre que dichas acciones se efectúen bajo protocolos previamente acordados, que aseguren:

- Acceso controlado y seguro, limitado a información vinculada al servicio contratado.
- Exclusión de datos confidenciales o sensibles ajenos al objeto contractual, preservando la confidencialidad y el secreto empresarial.

- Cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, garantizando confidencialidad, integridad y disponibilidad mediante medidas técnicas y organizativas.
- Uso de mecanismos alternativos (revisión documental, evidencias técnicas, auditorías en entornos controlados) para verificar el cumplimiento sin comprometer la confidencialidad.

En caso el CONTRATISTA considere necesario proponer algún ajuste a los lineamientos establecidos, podrá remitir su propuesta para la evaluación correspondiente por parte de la Superintendencia, siempre que dichos ajustes se encuentren alineados con la normativa aplicable y no comprometan las obligaciones contractuales ni legales.

3.3. 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.

3.4. CLÁUSULA DE 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.