



SUPERINTENDENCIA

DE BANCA, SEGUROS Y AFP

República del Perú

ADJUDICACIÓN SIMPLIFICADA N° 57-2023-SBS

CONTRATACIÓN DE UNA SUSCRIPCIÓN DE SERVICIO DE RESPALDO DE CORREO ELECTRÓNICO EN NUBE

ACTA N° 05

Siendo las 14:30 horas del día 16 de enero del 2024, se reúnen bajo la presidencia de la Sra. Leyla Mercedes Fernández Pinillos, los miembros del Comité de Selección: la Sra. Nicida Frías Pérez y el Sr. Ramón Saavedra Viteri, para tratar los siguientes puntos:

1. Absolución de consultas
2. Integración de bases

El Comité de Selección procedió a dar respuesta a las consultas y observaciones presentadas por los participantes TCO Latam del Perú S.A.C., Daily Technology S.A.C., Grupo D2D Solutions S.A.C., Cloud Solutions and IT Management S.A.C. y Bigsecure S.A.C., de conformidad a lo indicado en el numeral 72.4 del artículo 72 del Reglamento de la Ley de Contrataciones.

Al finalizar, el Comité de Selección acordó publicar en el SEACE la absolución de consultas y observaciones de acuerdo al calendario del procedimiento de selección.

En seguida, el Comité de Selección revisó el proyecto de bases integradas con las modificaciones previstas en el pliego absolutorio. Al culminar con dicha revisión, el Comité de Selección acordó publicar las bases integradas en el SEACE de acuerdo al calendario del procedimiento de selección.

Siendo las 15:30 horas y no habiendo otro punto a tratar, se dio por concluida la sesión.

Firmado por:

Leyla Mercedes Fernández Pinillos
Presidente del Comité de Selección

Nicida Frías Pérez
Miembro del Comité de Selección

Ramón Saavedra Viteri
Miembro del Comité de Selección



SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

República del Perú

Nro. Orden	RUC/Código	Nombre o Razón Social	Formular	Sección	Numeral	Líral	Página	Consulta u Observación	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
1	2000573-4051	TCO LATAM DEL PERU S.A.C.	Consulta	General	2.2.1.1 e)		16	Considerando que debido a temas legales y de compliance, que tardaría mucho tiempo que el fabricante nos facilite copias de las certificaciones solicitadas, si vase confirmar que aceptarán carta del fabricante en la que se indique que se cumple con dichas certificaciones.	La área usaría, precisa a que no se aceptarían cartas del fabricante. Los postores deberán de presentar las copias de las certificaciones: Soc Type 2, Tier 3, ISO 27001, para el inicio del servicio. Los certificados: Safe Harbor y PCI serán retirados del requerimiento.	Con motivo de la integración se eliminará lo señalado inicialmente como numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requiera copia simple de certificaciones y reportes para la prestación de obra. Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente: • Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región de donde se provee el servicio con respecto a la conservación de datos y manejo de la información: Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III. • De forma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.
2	2000573-4051	TCO LATAM DEL PERU S.A.C.	Consulta	General	2.2.1.1 e)		16	Tomando en cuenta que en el año 2016 quedó sin efecto el acuerdo Safe Harbor entre los Estados Unidos y Europa y fue remplazada por Privacy Shield el cual fue invalidado en Julio del 2020 y hoy esta siendo remplazado por el framework de Privacidad de Datos UE: EEUU (DPF). Dado que ya no están vigentes si vase confirmar que no se será necesario incluirlos dentro de la propuesta.	La área usaría, precisa a que los certificados Safe Harbor y PCI serán retirados del requerimiento, por lo que no se será necesario incluirlos en la propuesta.	Con motivo de la integración se eliminará lo señalado inicialmente como numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requiera copia simple de certificaciones y reportes para la prestación de obra. Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente: • Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región de donde se provee el servicio con respecto a la conservación de datos y manejo de la información: Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III. • De forma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.
3	20593-40-4031	DAILY TECHNOLOGY S.A.C.	Consulta	Específico	5.1.	-	20	Al tratarse de res palidos de correo y productos Microsoft 365, favor de confirmar si los siguientes certificados: PCI y Safe Harbor, pueden ser tratados como opcionales, debido a que guardan poca relación con los productos principales de las bases. PCI corresponde a certificado en seguridad para datos de pago de tarjetas (utilizado mayormente en bancos) y Safe Harbor corresponde a la protección de datos personales para personas y región de la Unión Europea. Entiéndase de que dichos certificados solicitados no están relacionados con el requerimiento principal.	La área usaría, precisa a que los certificados Safe Harbor y PCI serán retirados del requerimiento, por lo que no se será necesario incluirlos en la propuesta.	Con motivo de la integración se eliminará lo señalado inicialmente como numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requiera copia simple de certificaciones y reportes para la prestación de obra. Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente: • Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región de donde se provee el servicio con respecto a la conservación de datos y manejo de la información: Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III. • De forma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.



SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

República del Perú

Nro. Orden	RUC/Código	Nombre o Razón Social	Formulario	Sección	Numeral	Literal	Página	Consulta u Observación	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
4	20553404631	DAILY TECHNOLOGY S.A.C.	Consulta	Específico	5.1.	-	20	En las bases se indica: "La solución ofertada deberá incluir una solución antivirus o podrá ser una solución diferente de antivirus integrada a la solución de backup en nube, que permitirá evitar, buscar, detectar y eliminar virus que pueda incluirse en la plataforma. Toda la solución de backup en nube, en donde se almacenarán la información respaldada debe de tener un sistema de antivirus. Deberá incluir la evidencia de la solución antivirus vigente." Al tratarse de una solución de respaldo del tipo SaaS ya se cuenta con los certificados que garantizan la seguridad y protección de los datos almacenados en sus nubes como el Soc Type 2, Tier 3, ISO 27001, por lo tanto, confirmar si este ítem sería opcional.	Considerando que la solución ofertada podrá incluir una solución antivirus, el área usuaria, precisa que los respaldos tipo SaaS, deberán contar con las certificaciones que garanticen la seguridad y protección de la información respaldada, por lo que, las certificaciones, Soc Type 2, Tier 3, ISO 27001, deberán presentarse para el inicio del servicio. La inclusión de una solución diferente de antivirus es opcional lo que deberá evidenciarse de forma previa al inicio del servicio.	Con motivo de la integración se modificará la viñeta siguiente del numeral 5.1 de los términos de referencia, quedando redactada de la siguiente forma: "• Podrá ser ofertada podrá incluir una solución antivirus o podrá ser una solución diferente de antivirus integrada a la solución de backup en nube, que permitirá evitar, buscar, detectar y eliminar virus que pueda incluirse en la plataforma. Toda la solución de backup en nube, en donde se almacenarán la información respaldada debe de tener un sistema de antivirus. Deberá incluir la evidencia de la solución antivirus vigente de forma previa al inicio del servicio."
5	20553404631	DAILY TECHNOLOGY S.A.C.	Consulta	Específico	5.1.	-	20	En las bases se indica: "Debe soportar capacidades de protección antimalware y ransomware SaaS, podrá ser realizado mediante la solución ofertada como antivirus integrado a la solución de backup en Nube." Confirmar si lo solicitado corresponde a una herramienta de detección y protección para los correos entrantes de la entidad en Exchange.	El área usuaria, precisa que lo solicitado no es para los correos entrantes, los respaldos deberán de contar con las certificaciones que garanticen la seguridad y protección de la información respaldada. Por lo que las copias de las certificaciones, Soc Type 2, Tier 3, ISO 27001, deberán presentarse de forma previa al inicio del servicio.	Con motivo de la integración se modificará la viñeta siguiente del numeral 5.1 de los términos de referencia, quedando redactada de la siguiente forma: "• Podrá ser soportar capacidades de protección antimalware y ransomware SaaS, mediante la solución ofertada como antivirus integrado a la solución de backup en Nube. Lo anterior se acredita con las copias de las certificaciones, Soc Type 2, Tier 3 e ISO 27001, que deberán presentarse de forma previa al inicio del servicio."
6	20553404631	DAILY TECHNOLOGY S.A.C.	Consulta	Específico	5.5.	-	22	Al tratarse de una solución de respaldo en nube de tipo SaaS, la consola de administración así como sus procedimientos, están diseñados para un uso intuitivo con una interfaz fácil de entender, lo cual permite reducir la curva de aprendizaje sustancialmente. Por lo tanto, confirmar si la cantidad de horas indicadas para la capacitación puede reducirse a 04 horas como máximo.	La área usuaria, precisa que la capacitación se reduce a 08 horas, como máximo.	Con motivo de la absorción se modificará el primer párrafo del numeral 5.5 quedando redactado de la siguiente forma: "El contratista deberá realizar una capacitación de ocho (8) horas como máximo, orientada a la administración del servicio de backup en nube para Microsoft 365, para un mínimo de seis (06) personas."
7	20607753602	GRUPO D2D SOLUTIONS S.A.C.	Consulta	Específico	2.2.1.1	e)	16	Solicitan en Documentos para la admisión de la oferta: e) Copia simple de las certificaciones y reportes requeridos, siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado: PCI, Safe Harbor, Certificación ISO 27001, SOC II Type 2, Centros de Datos Tier III. En vista que esos documentos el proveedor del Servicio lo proporciona cuando se contrata el servicio, sinase confirmar que los documentos: • Copia simple de las certificaciones y reportes requeridos, siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado: PCI, Safe Harbor, Certificación ISO 27001, SOC II Type 2, Centros de Datos Tier III. Se presentarán a la ejecución del servicio y no en la etapa de presentación de ofertas.	La área usuaria, precisa que las copias de las certificaciones Soc Type 2, Tier 3, ISO 27001, deberán presentarse de forma previa al inicio del servicio. El requerimiento de los certificados Safe Harbor y PCI serán retirados del requerimiento.	Con motivo de la integración se eliminará lo señalado inicialmente como numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requiera copia simple de certificaciones y reportes para la presentación de oferta. Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente: • Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región desde donde se provee el servicio con respecto a la conservación de datos y manejo de la información: Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III. • De forma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.



SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

República del Perú

Nro. Orden	RUC/Código	Nombre o Razón Social	Fórmula	Sección	Número	Líteral	Página	Consulta u Observación	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
8	20607753602	GRUPO D2D SOLUTIONS S.A.C.	Consulta	Específico	5.1	-	21	<p>Solicitan en Documentos para la admisión de la oferta:</p> <p>Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región desde donde se provee el servicio con respecto a la conservación de datos y manejo de la información:</p> <ul style="list-style-type: none">✓ PCI✓ Safe Harbor✓ Certificación ISO 27001✓ SOC II Type 2✓ Centros de Datos Tier III <p>Para la presentación de oferta, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba, siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.</p> <p>En vista que esos documentos el proveedor del Servicio lo proporciona cuando se contrata el servicio, sírvase confirmar que los documentos:</p> <ul style="list-style-type: none">-Copia simple de las certificaciones y reportes requeridos, siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado: PCI, Safe Harbor, Certificación ISO 27001, SOC II Type 2, Centros de Datos Tier III. <p>Se presentarán a la ejecución del servicio y no en la etapa de presentación de ofertas.</p>	<p>La área usuaria, precisa que las copias de las certificaciones Soc Type 2, Tier 3, ISO 27001, deberán presentarse para el inicio del servicio. El requerimiento de los certificados Safe Harbor y PCI serán retirados del requerimiento</p>	<p>Con motivo de la integración se eliminará lo señalado inicialmente como numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requiera copia simple de certificaciones y reportes para la presentación de oferta.</p> <p>Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente:</p> <ul style="list-style-type: none">• Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región desde donde se provee el servicio con respecto a la conservación de datos y manejo de la información: Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III.• De firma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenerlos vigentes durante todo el servicio contratado.
9	20607753602	GRUPO D2D SOLUTIONS S.A.C.	Consulta	Específico	5.1	-	22	<p>Solicitan:</p> <p>La solución deberá permitir la ejecución pruebas de vulnerabilidades automáticas o manuales (mediante herramientas o software de externos), las mismas que deberán realizarse en forma coordinada para determinar el alcance y tipo de pruebas a realizar, no debiéndose incluir en la solución o oferta</p> <p>Sírvase precisar que este requerimiento se refiere a que la ENTIDAD mediante sus propias herramientas o software externos ejecutarán pruebas de vulnerabilidad sin necesidad de instalar algún componente o agente o programa en los componentes de la nube del servicio propuesto; todo esto debido a que, nuestra solución a proponer, es una solución completa, segura, inmutable y cerrada que no permite la integración o instalación con otras herramientas o software por Compliance de seguridad.</p>	<p>El área usuaria, precisa, que se ejecutarán sin la necesidad de instalar algún componente o agente. La ejecución de prueba de vulnerabilidades será en coordinación con nuestro Departamento de Seguridad de Información (DSTI) de la Gerencia de Tecnologías de Información (GTI) y el contratista.</p>	<p>Con motivo de la integración se modificará la última viñeta del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente: • La solución deberá permitir la ejecución de pruebas de vulnerabilidades automáticas o manuales (mediante herramientas o software de externos) y que se ejecutarán sin la necesidad de instalar algún componente o agente. La ejecución de prueba de vulnerabilidades será en coordinación con el Departamento de Seguridad de Información (DSTI) de la Gerencia de Tecnologías de Información (GTI) y el contratista.</p>



SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

República del Perú

Nro. Orden	RUC/Código	Nombre o Razón Social	Formula	Sección	Numeral	Literal	Página	Consulta u Observación	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
10	20607017647	CLOUD SOLUTIONS AND IT MANAGEMENT S.A.C.	Consulta	Específico	5.1	--	21	<p>Solicitan: La solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región desde donde se provee el servicio con respecto a la conservación de datos y manejo de la información:</p> <ul style="list-style-type: none">¿ PCI¿ Safe Harbor¿ Certificación ISO 27001¿ SOC II Type 2¿ Centros de Datos Tier III <p>Para la presentación de oferta, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba, siendo obligación del proveedor mantenimientos vigentes durante todo el servicio contratado</p> <p>Dado que estos documentos el proveedor de servicio lo proporciona una vez se haya contratado el servicio por lo que solicitamos confirmar que dichas copias de certificaciones se presentaran en la ejecución del servicio.</p>	<p>La área usuaria, precisa que las copias de las certificaciones Soc Type 2, Tier 3, ISO 27001, deberán presentarse para el inicio del servicio. El requerimiento de los certificados Safe Harbor y PCI serán retirados del requerimiento</p>	<p>Con motivo de la integración se eliminará lo señalado inicialmente con numeral 2.2.1.1 e) del capítulo II de la sección específica de las bases que requería copia simple de certificaciones y reportes para la presentación de oferta.</p> <p>Con motivo de la integración se modificará viñetas del numeral 5.1 de los términos de referencia quedando redactado de la forma siguiente:</p> <ul style="list-style-type: none">Las copias de información deben estar protegidas por las medidas de necesidad de seguridad necesarias para garantizar la confidencialidad de toda la información almacenada, la solución deberá cumplir con los siguientes estándares de seguridad, relevantes a la zona o región desde donde se provee el servicio con respecto a la conservación de datos y manejo de la información: <p>Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III.</p> <ul style="list-style-type: none">De forma previa al inicio del servicio, el postor deberá presentar copia simple de las certificaciones y reportes requeridos líneas arriba (Certificación ISO 27001, SOC II Type 2 y Centros de Datos Tier III), siendo obligación del proveedor mantenimientos vigentes durante todo el servicio contratado.
11	20600981430	BIGSECURE S.A.C.	Consulta	Específico	3.2	B	29	<p>Dice : B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p>Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 150.000.00 (ciento cincuenta mil y 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a : ...</p> <p>Consulta : Con el objeto de lograr la mayor participación de postores, solicitamos se sirvan confirmar que también se aceptarán como servicios similares a los siguientes :</p> <ul style="list-style-type: none">¿ CONTRATACIÓN DE SERVICIO DE CORREO ELECTRÓNICO, MENSAJERÍA Y SITE COLABORATIVO A TRAVÉS DE LA NUBE DE INTERNET. INCLUYE: OFFICE 365 BUSINESS ESSENTIALS.¿ CONTRATACIÓN DEL SERVICIO DE MICROSOFT 365 (entregamente llamado OFFICE 365) PARA EL PROGRAMA NACIONAL CUNA MAS.¿ ADQUISICIÓN DE LICENCIAS DE SISTEMA OPERATIVO MICROSOFT WINDOWS SERVER O EQUIVALENTE PARA EL PROGRAMA PARA LA GENERACIÓN DE EMPLEO SOCIAL INCLUSIVO TRABAJA PERU.¿ CONTRATACIÓN DE SERVICIO DE SUITE DE HERRAMIENTAS DE PRODUCTIVIDAD Y COLABORACIÓN EN LA NUBE..	<p>La área usuaria, precisa que la experiencia solicitada es en backup SaaS, la experiencia solicitada a incorporar como servicio similar corresponde a O informática, no correspondiendo al fin del proceso al no ser servicios similares al servicio a contratar, backup SaaS. Por lo tanto no se acepta experiencia en informática.</p>	<p>No corresponde</p>