

Acta Admisión, Evaluación, Calificación y Otorgamiento de la Buena Pro	
Concurso Público N°	007-2024-COFIDE
Objeto	Servicio de Gestión y Operación de la Ciberseguridad
Fecha	14 de febrero de 2025

En el distrito de San Isidro, provincia y departamento de Lima, siendo las 09:00 horas del día 14 de febrero de 2025, el Comité de Selección designado en el Procedimiento de Selección Concurso Público N° 007-2024-COFIDE, para el “Servicio de Gestión y Operación de la Ciberseguridad”:

1. INTRODUCCIÓN:

Se dio a conocer los resultados de la evaluación y calificación de las ofertas presentadas en el procedimiento de selección Concurso Público N° 007-2024-COFIDE, para el “Servicio de Gestión y Operación de la Ciberseguridad”.

2. DETALLE DE LOS PARTICIPANTES:

De acuerdo al cronograma establecido en la plataforma del SEACE, se registraron como participantes los siguientes proveedores:

Nro.	Tipo proveedor	RUC/Código	Nombre o Razón Social	Fecha de registro en el procedimiento	Estado
1	Proveedor con RUC	99000035820	PASSWORD CONSULTING SERVICES SAS	31/01/2025	Válido
2	Proveedor con RUC	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	15/01/2025	Válido
3	Proveedor con RUC	20601317461	SECURESOFTE CORPORATION S.A.C	06/01/2025	Válido
4	Proveedor con RUC	20199144961	BAFING S.A.C.	03/01/2025	Válido
5	Proveedor con RUC	20521485702	IT DATUM S.A.C.	03/01/2025	Válido
6	Proveedor con RUC	20475805101	INNOVARE E-BUSINESS S.A.C.	29/12/2024	Válido

3. DETALLE DE LOS POSTORES:

En el día y horario señalado en el cronograma, los siguientes postores presentaron su oferta electrónica:

Nro.	RUC/Código	Nombre o Razón Social	Fecha de presentación	Hora de presentación	Estado de la propuesta	Estado
1	20601317461	SECURESOFTE CORPORATION S.A.C	04/02/2025	21:00:37	Enviado	Valido
2	99000035820	PASSWORD CONSULTING SERVICES SAS	04/02/2025	14:42:10	Enviado	Valido

4. REVISIÓN Y ADMISIÓN DE OFERTAS:

Se procedió con la revisión de los documentos requeridos para la admisión de ofertas, siendo el resultado siguiente:

DOCUMENTOS DE ADMISIÓN	SECURESOFT CORPORATION S.A.C	PASSWORD CONSULTING SERVICES SAS
Declaración jurada de datos del postor (Anexo N° 1)	Cumple	Cumple
Documento que acredite la representación de quien suscribe la oferta.	Cumple	Cumple
Declaración Jurada de acuerdo con el literal b) del art. 52 del Reglamento (Anexo N° 2)	Cumple	Cumple
Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 el Capítulo III de la presente sección. (Anexo N° 3)	Cumple	Cumple
Declaración jurada de plazo de prestación del servicio. (Anexo N° 4)	Cumple	Cumple
Promesa de consorcio con firmas legalizadas. (Anexo N° 5)	No corresponde	No corresponde
Precio de la Oferta en Soles. (Anexo N° 6)	Cumple	Cumple
CONDICIÓN	ADMITIDO	ADMITIDO (*)

(*) Respecto a la propuesta presentada por **PASSWORD CONSULTING SERVICES SAS**, mediante Acta de Solicitud de Subsanación de Oferta, de fecha 07 de febrero de 2025, se concedió al postor el plazo de un día hábil para subsanar (i) el visto y foliación de la propuesta, (ii) precisar los datos omitidos del poder otorgado en el Anexo N° 1 – Declaración Jurada de Datos del Postor y, (iii) presentar el Certificado de Vigencia de Poder; siendo que con fecha 10 de febrero de 2025, el postor cumplió con presentar la subsanación correspondiente.

5. FACTORES DE EVALUACIÓN

Se procedió a evaluar la oferta admitida, siendo el resultado siguiente:

FACTOR DE EVALUACIÓN	SECURESOFT CORPORATION S.A.C	PASSWORD CONSULTING SERVICES SAS
<p>PRECIO 100 puntos</p> <p>La evaluación consistirá en otorgar el máximo puntaje de la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i = Oferta Pi = Puntaje de la oferta a evaluar Oi = Precio i Om = Precio de la oferta más baja PMP = Puntaje máximo del precio</p>	<p>S/ 1'805,000.00</p>	<p>S/ 2'658,926.00</p>
	100.00	67.88
PUNTAJE TOTAL	100.00	67.88
ORDEN DE PRELACIÓN	1	2

6. CALIFICACIÓN DE LAS OFERTAS:

Se procedió con la calificación del postor, siendo el resultado siguiente:

CRITERIO DE CALIFICACIÓN		SECURESOFT CORPORATION S.A.C	PASSWORD CONSULTING SERVICES SAS																
A.- CAPACIDAD TÉCNICA Y PROFESIONAL																			
A.1.- EQUIPAMIENTO ESTRATÉGICO Requisitos: El equipamiento estratégico requerido por cada servicio es como se detalla a continuación:		Cumple	No cumple																
<table><tr><th>Servicio</th><th>Facilidades Tecnológicas Mínimas</th></tr><tr><td>General</td><td><ul style="list-style-type: none">- El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE.</td></tr><tr><td>S1</td><td><ul style="list-style-type: none">- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Acceso a Internet.</td></tr><tr><td>S2</td><td><ul style="list-style-type: none">- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE</td></tr><tr><td>S3</td><td><ul style="list-style-type: none">- Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso).- Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs.- Conectividad para acceso al software y/o hardware de monitoreo.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.</td></tr><tr><td>S4</td><td><ul style="list-style-type: none">- Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.).- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.</td></tr><tr><td>S5</td><td><ul style="list-style-type: none">- Software especializado para el escaneo de las vulnerabilidades de las aplicaciones- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.</td></tr><tr><td>S6</td><td><ul style="list-style-type: none">- Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.</td></tr></table>				Servicio	Facilidades Tecnológicas Mínimas	General	<ul style="list-style-type: none">- El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE.	S1	<ul style="list-style-type: none">- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Acceso a Internet.	S2	<ul style="list-style-type: none">- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE	S3	<ul style="list-style-type: none">- Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso).- Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs.- Conectividad para acceso al software y/o hardware de monitoreo.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.	S4	<ul style="list-style-type: none">- Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.).- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.	S5	<ul style="list-style-type: none">- Software especializado para el escaneo de las vulnerabilidades de las aplicaciones- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.	S6	<ul style="list-style-type: none">- Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.
Servicio	Facilidades Tecnológicas Mínimas																		
General	<ul style="list-style-type: none">- El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE.																		
S1	<ul style="list-style-type: none">- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Acceso a Internet.																		
S2	<ul style="list-style-type: none">- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE																		
S3	<ul style="list-style-type: none">- Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso).- Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs.- Conectividad para acceso al software y/o hardware de monitoreo.- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.																		
S4	<ul style="list-style-type: none">- Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.).- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.																		
S5	<ul style="list-style-type: none">- Software especializado para el escaneo de las vulnerabilidades de las aplicaciones- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.																		
S6	<ul style="list-style-type: none">- Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.- Correo electrónico corporativo del Contratista para coordinaciones.- Sistemas de videoconferencia para realizar las coordinaciones.																		
A.2.- CALIFICACIONES DEL PERSONAL CLAVE																			
A.2.1.- FORMACIÓN ACADÉMICA Requisitos: Director del Proyecto: Titulado en las carreras de Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software		Cumple	Cumple																

<p>Líder del CSIRT: Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software</p> <p>Líder del CyberSOC: Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad.</p> <p>Service Manager: Profesional Titulado en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad.</p>		
<p>A.2.2.- CAPACITACIÓN</p> <p>Requisitos: Director del Proyecto: Por lo menos 01 de los siguientes cursos: Curso, diplomado o programa en gerencia y/o gestión de proyectos, de mínimo 100 horas.</p> <p>Líder del CSIRT: Por lo menos 03 de los siguientes cursos: -Curso, diplomado o programa de ITIL, de mínimo 20 horas. - Curso, diplomado o programa de ISO/IEC 27001 Auditor Líder, de mínimo 30 horas. -Curso, diplomado o programa de Transformación Digital, de mínimo 30 horas. - Curso, diplomado o programa de respuesta ante incidentes, de mínimo 50 horas. - Curso, diplomado o programa de atención de ciberamenazas, de mínimo 30 horas.</p> <p>Líder del CyberSOC: Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en gestión de servicio de SOC o CyberSOC, de mínimo 50 horas.</p> <p>Service Manager: Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en Gestión de Servicios de Tecnologías de la Información, de mínimo 40 horas. - Curso y/o Diplomado y/o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas.</p>	Cumple	Cumple
A.3.- EXPERIENCIA DEL PERSONAL CLAVE		

<p>Requisitos:</p> <p>Director del Proyecto: Mínimo 6 años en Gestión de Proyectos de TI y/o Seguridad Gestionada, como Jefe o Gestor o Coordinador o Encargado o Director o Gerente o Subgerente.</p> <p>Líder del CSIRT: Mínimo de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como jefe o Líder o Coordinador.</p> <p>Líder del CyberSOC: Mínimo de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o jefe o Líder</p> <p>Service Manager: Mínimo de seis (6) años en gestionar o liderar o supervisar servicios de ciberseguridad como Especialista o Analista Técnico o Jefe o Líder</p> <p>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</p>	Cumple	Cumple
<p>B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p>Requisitos:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 5'640,000.00 (Cinco millones seiscientos cuarenta mil con 00/100 Soles), por la contratación de servicios 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 los siguientes:</p> <ul style="list-style-type: none"> - Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad - Servicio de seguridad de red interna y perimetral - Servicio de Soporte, Monitoreo y Administración de red interna y perimetral - Consultoría, desarrollo, mantenimiento y/o soporte de soluciones tecnológicas de seguridad - Servicios de RedTeam - Servicio de monitoreo de eventos de seguridad (SOC) - Servicio de CyberSOC o Cyber Defense Center - Soporte, gestión, mantenimiento o monitoreo de equipamiento o plataformas de seguridad - Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad – SIEM - Servicio de soporte de plataforma de seguridad y correlación, servicio de protección de tráfico web, sistema de correlación de eventos-SIEM 	Cumple	No cumple
CONDICIÓN	CALIFICADO	DESCALIFICADO (*)

(*) Respecto a los documentos presentados por el postor **PASSWORD CONSULTING SERVICES SAS**, se advierte que:

- Del folio 11 al 18, presenta el Anexo Cumplimiento Equipamiento Estratégico, a partir del cual el representante del postor certifica que "... la firma cumple y cuenta con lo establecido en el anexo Equipamiento Estratégico..." y consigna un cuadro con los encabezados de: (i) Servicio, (ii)

Facilidades Técnicas Mínimas y (iii) Cumple, suscribiendo el mismo en la parte final del documento, según se advierte a continuación:

Así mismo, se adjuntan a continuación hojas de vida del equipo requerido. Adicionalmente, certificamos que en caso de resultar adjudicatarios nos comprometemos a aportar el equipo de trabajo en su totalidad encargado de ejecutar el proyecto, así como las certificaciones y acreditaciones que dan cuenta el cumplimiento de lo estipulado en el ítem 7.1. de las bases de concurso público.

Ciudad, 03 de febrero de 2025.


DAVID ENRIQUE BRAVO SHEEN
DNI N°: 09304274 – 9
Representante Legal
PASSWORD CONSULTING SERVICES SAS


Firmado digitalmente por:
BRAVO SHEEN DAVID ENRIQUE
Motivo: Soy el autor del documento
Fecha: 04/02/2025 12:44:12-0500

Ahora bien, conforme a lo señalado por el OSCE en la nota Importante de los Requisitos de Calificación de las Bases Integradas *“Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.”*; sin embargo, el postor no cumple con presentar documentos que acrediten fehacientemente contar con el Equipamiento Estratégico requerido, sino que presenta un documento denominado “Anexo Cumplimiento Equipamiento Estratégico” suscrito por el Sr. David Enrique Bravo Sheen, representante del postor PASSWORD CONSULTING SERVICES SAS, lo cual se considera una declaración jurada al ser suscrita por el propio postor. Por lo tanto, **el postor no cumple con acreditar que cuente con el Equipamiento Estratégico.**

Sin perjuicio de ello, se hace presente que, conforme a lo señalado por el Tribunal de Contrataciones del Estado en su Resolución N° 03578-2023-TCE-S2, en sus considerandos 19 y 20:

*“19. (...) Además, no debe olvidarse que **cada postor debe ser diligente, y presentar ofertas claras y congruentes, de modo tal que el Comité de Selección pueda advertir lo que el postor oferta, sin recurrir a interpretaciones.** Así pues, toda información contenida en la oferta técnica o económica, debe ser objetiva, clara, precisa y congruente entre sí a fin de posibilitar al Comité de Selección la verificación directa de lo ofertado por los postores y, de esta forma, corroborar si lo descrito es concordante con lo requerido por la Entidad.*

*20. Por otro lado, debe aclararse **que la evaluación y revisión de la oferta se efectúa respecto de los documentos que la conforman y no de otros presentados con posterioridad que no formen parte de su oferta.**”*

Por lo que, respecto a las aclaraciones presentadas en el mencionado Anexo Cumplimiento Equipamiento Estratégico, si bien el postor consigna en su cuadro, para el Servicio General, S1, S2, S3 y S5, capturas de pantalla, links de acceso a publicaciones en LinkedIn y recortes de documentos, estos no pueden acreditar fehacientemente que el postor cuente con el Equipamiento señalado, mas aun si los mismos no fueron acreditados conforme la forma señalada en las bases integradas, asimismo se advierte que se desconoce de donde fue extraída la captura de pantalla de SOC PASSWORD, los links que derivarían a publicaciones realizadas por el propio postor y los documentos correspondientes al servicio S3 y S5 son recortes que ni siquiera contarían con destinatario y fecha;

- Que, del folio 6 al 9, el postor presenta el Anexo N° 8 Experiencia del Postor en la Especialidad, advirtiéndose que el tipo de cambio consignado no se ajusta a la realidad, así por ejemplo en la primer

experiencia consignada el postor señala como tipo de cambio venta: S/ 3,600 y de la publicación de la SBS se advierte como tipo de cambio S/ 0.001042

sbs.gob.pe/app/pp/SISTIP_PORTAL x +

https://www.sbs.gob.pe/app/pp/SISTIP_PORTAL/Paginas/Publicacion/TipoCambioContable.aspx

SISTEMA DE CONTR... Inspektor® LinkedIn Learning: c...

TIPO DE CAMBIO CONTABLE

Ingrese fecha: 30/07/2021 (dd/mm/aaaa) Consultar Exportar

Tipo de Cambio al 30/07/2021

Estados Unidos de América	Dólar de N.A.	4.04
PAIS	MONEDA	TIPO DE CAMBIO (En S/)
Unión Europea	Euro	4.790135
Argentina	Peso Argentino	0.041786
Australia	Dólar Australiano	2.963833
Bangladesh	Taka Bangladesí	0.047874
Bolivia, Estado Plurinacional de	Boliviano	0.592252
Brasil	Real	0.778629
Bulgaria	Lev	2.454433
Canadá	Dólar Canadiense	3.237696
Chile	Peso Chileno	0.005300
China	Yuan Chino Off-Shore	0.624847
China	Yuan	0.625299
Colombia	Peso Colombiano	0.001042
Congo	Franco Cfa de África Central	0.007300
Corea, República de (Sur)	Won Surcoreano	0.003515
Costa Rica	Colón de Costa Rica	0.006517
Dinamarca	Corona Danesa	0.643936

Siendo que, conforme a lo señalado en la mencionada Resolución N° 03578-2023-TCE-S2, el postor es responsable de que la información consignada sea clara, precisa y congruente entre sí, lo cual no fue consignado así en el Anexo N° 8.

DE OTRO LADO, conforme a lo establecido en el numeral 46.4 del artículo 46° del Reglamento de la Ley de Contrataciones del Estado, se solicitó el apoyo al área usuaria para determinar la valides de los servicios similares requeridos como Experiencia del Postor en la Especialidad, siendo que el área usuaria no validó como similares los servicios señalados en los numerales 1, 2, 3, 8, 9 y 10 del Anexo N° 8 Experiencia del Postor en la Especialidad, señalando que:

2. Respecto a la propuesta presentada por **PASSWORD CONSULTING SERVICES SAS**, se adjunta algunas observaciones a la facturación.

Documento: **Anexo 1 Experiencia.pdf**

Pag 2: El objeto no es similar

Contrato No:	1103 DE 2020
Tipo de Contrato:	Suministro
Objeto:	ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE ELEMENTOS TIC PARA EL FORTALECIMIENTO DEL MODELO Y LA PLATAFORMA DE CIBERSEGURIDAD DEL ÁREA METROPOLITANA DEL VALLE DE ABURRÁ, DE CONFORMIDAD CON LOS LINEAMIENTOS DE LA POLÍTICA NACIONAL DE SEGURIDAD DIGITAL
Fecha inicio:	23.01.2020

Documento: **Anexo 1 Experiencia.pdf**

Pag 27: El objeto no es similar

OBJETO: prestación del servicio para la realización de pruebas de vulnerabilidad acompañamiento asesoría para la definición y selección e implementación de las medidas de remediación corrección o atención de las vulnerabilidades detectadas para las direcciones IP externas (públicas) y para las aplicaciones del BANCO.

Documento: **Anexo 1 Experiencia.pdf**

Pag 45: El objeto no es similar

OBJETO: Realización de pruebas de vulnerabilidad, ingeniería social y de ethical hacking-penttesting a los aplicativos e infraestructura tecnológica que el BANCO determine, así como la asesoría y acompañamiento en la remediación de las vulnerabilidades detectadas.

Documento: **Anexo 1 Experiencia.pdf**

Pag 146: El objeto no es similar

900.175.316 – 8 ejecutó el siguiente contrato:

OBJETO DEL CONTRATO	Objeto del contrato: Prestación de servicios de consultoría, suministro de infraestructura tecnológica y capacitación para los diferentes proyectos que gestiona la organización.
VALOR TOTAL	\$ 2.923.580.000

Documento: **Anexo 1 Experiencia.pdf**

Pag 154: El objeto no es similar

CONTRATO ESTATAL DE PRESTACIÓN DE SERVICIOS PROFESIONALES No. 000923 DE 2020

OBJETO: Realizar análisis de seguridad informática mediante la aplicación de tres (3) instrumentos: gap análisis, análisis de vulnerabilidades y Ethical Hacking, teniendo en cuenta la norma ISO 27001 del 2013 con el fin de fortalecer y asegurar la disponibilidad de los servicios tecnológicos de información del Ministerio / Fondo Único TIC.

Documento: **Anexo 1 Experiencia.pdf**

Pag 189: El objeto no es similar

CONTRATO DE CONSULTORÍA N° 807 DE 2021

OBJETO: Realizar el análisis de seguridad informática mediante la aplicación de dos (2) instrumentos: análisis de vulnerabilidades y Ethical Hacking, teniendo en cuenta la norma ISO 27001- 2013 con el fin de fortalecer y asegurar la disponibilidad de los servicios tecnológicos de información del Ministerio / Fondo Único TIC.

En este sentido, descontando la mencionada experiencia no validada por el área usuaria, el postor acredita tener una experiencia similar a la requerida ascendente a S/ 2'711,068.19; por tanto no llega a acreditar la experiencia mínima requerida de S/ 5'640,000.00.

Por lo tanto; **no cumple con acreditar la experiencia del postor en la especialidad** requerida.

7. OTORGAMIENTO DE LA BUENA PRO:

Se procede a otorgar la **BUENA PRO** del procedimiento de selección Concurso Público N° 007-2024-COFIDE, para el "Servicio de Gestión y Operación de la Ciberseguridad", al postor **SECURESOFTE CORPORATION S.A.C.**, por el monto de **S/ 1'805,000.00 (Un millón ochocientos cinco mil con 00/100 Soles)**, incluido todos los impuestos de Ley.

A continuación, se suscribe la presente en señal de conformidad, siendo las 11:00 horas del día 14 de febrero de 2025.

.....
Juan Rodríguez Calderón
Presidente del Comité

.....
Mirtha Arrieta Calla
Miembro 1 del Comité

.....
Milagros Recabarren Medina
Miembro 2 del Comité