SERVICIO DE ANÁLISIS Y AUDITORÍA DE LA BASE DE DATOS DEL REGISTRO NACIONAL DE PROVEEDORES DEL OSCE

1. AREA USUARIA:

Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones.

2. FINALIDAD PÚBLICA:

La contratación de este servicio tiene como finalidad supervisar los controles de acceso al sistema de información respecto de la base de datos del Registro Nacional de Proveedores (RNP), para garantizar la protección de la información y componentes del referido Sistema Informático.

3. OBJETIVO:

El objetivo del servicio es identificar el comportamiento de los usuarios y analizar patrones, desviaciones e inconsistencias sobre el acceso a los datos y la extracción de otro tipo de información útil de las auditorías que actualmente se están generando en la base de datos del sistema del RNP mediante el propio servicio de base de datos.

4. ACTIVIDAD DEL POI:

Aseguramiento de la Disponibilidad de los Servicios de Tecnologías de la Información.

5. DESCRIPCIÓN DEL SERVICIO:

Ítem	Cantidad	U. de medida	Descripción
1	01	Servicio	Servicio de análisis y auditoria de la base de datos del Registro Nacional de Proveedores del OSCE.

- ✓ La Oficina de Tecnologías de la Información (OTI) proveerá al contratista de las facilidades necesarias a fin de ejecutar satisfactoriamente el servicio.
- ✓ Todas las actividades que se desarrollen durante el servicio serán coordinadas y/o supervisadas por la UAST.
- ✓ El presente requerimiento del servicio no constituye un contrato de consultoría.

El servicio solicitado debe cumplir con lo siguiente:

a) Se llevará a cabo reunión de inicio del servicio, la misma que se dará al día siguiente de la notificación de la orden de servicio; donde se explicará la mecánica del mismo, fijándose como fecha de entrega de la información por parte de la Entidad al día siguiente de llevarse a cabo la presente reunión. Asimismo, finalizando la reunión se suscribirá el Acta de Reunión.
b) El día en que la Entidad entregue la información al proveedor (al día siguiente que se lleve a cabo la reunión, es decir al segundo día de la notificación de la Orden de Servicio).
c) Revisión y análisis forense de las pistas de auditoría de la base de datos del sistema RNP.
d) Identificar el acceso a los datos sensibles de acuerdo a las políticas de auditoría del OSCE.
e) Identificar actividades atípicas sobre los datos sensibles, excepciones de seguridad, modificaciones de acceso a los datos sensibles de acuerdo a las pistas de auditoría del OSCE.
f) Identificar la trazabilidad de la sentencia que accedió a los datos sensibles de acuerdo a

las políticas de auditoría del OSCE.

g) Clasificar los niveles de riesgos en las pistas de auditoría.

h) Recopilación de las operaciones que se han efectuado sobre los datos sensibles identificados previamente.

i) Elaborar un plan de acción para el afinamiento respecto a los hallazgos encontrados sobre las pistas de auditoría, de acuerdo a las buenas prácticas de seguridad.

j) Las pistas de auditoría serán suministradas en un ambiente del OSCE.

6. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL:

No aplica.

7. PLAN DE TRABAJO:

No aplica.

8. REQUISITOS DEL PROVEEDOR:

8.1. EXPERIENCIA DE EMPRESA

El postor debe acreditar un monto facturado acumulado equivalente a S/ 35,000 nuevos soles, por la prestación de servicios iguales o similares al objeto de la convocatoria, durante los dos (02) 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.

Se consideran servicios similares a los siguientes: servicios de seguridad de la información, ciberseguridad, informática forense, análisis forense, administración y monitoreo de equipo de seguridad perimetral, escaneo de vulnerabilidades, en implementación del Sistema de Gestión de Seguridad de la Información, consultoría o auditoría de seguridad de la información ISO27001, implementación o seguimiento de controles de seguridad de la información o ciberseguridad.

Se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

8.2. Experiencia del Personal:

Consultor Principal

Contar con una experiencia profesional mínima de cinco (05) años en proyectos de seguridad de la información, ciberseguridad o informática forense y/o análisis forense de base de datos SQL Server y/o Implementación de políticas y/o pistas de auditoría de base de datos SQL Server y/o auditoría de base de datos SQL Server y/o servicios de seguridad de base de datos SQL Server.

Consultor Técnico

Contar con una experiencia profesional mínima de cuatro años (04) años en proyectos de seguridad de la información, ciberseguridad o informática forense y/o análisis forense de base de datos SQL Server y/o Implementación de políticas y/o pistas de auditoría de base de datos SQL Server y/o auditoría de base de datos SQL Server y/o servicios de seguridad de base de datos SQL Server.

Se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

8.3. Formación Académica:

Consultor Principal
Título profesional o bachiller en Ingeniería de Sistemas, Ingeniería Informática y/o Tecnologías de Información y/o Ingeniería de Sistemas e Informática y/o Computación y sistemas y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería de Seguridad y Auditoría Informática y/o afines.

Consultor Técnico
Título profesional o bachiller en Ingeniería de Sistemas, Ingeniería Informática y/o Tecnologías de Información y/o Ingeniería de Sistemas e Informática y/o Computación y Sistemas y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería de Seguridad y Auditoría Informática y/o afines.

Se acreditará con copia del documento al momento de la presentación de la cotización.

8.4. CAPACITACION:

Consultor Principal
Curso de Ethical Hacking, curso de SQL Server y deberá contar con al menos dos (02) certificaciones de entre las siguientes: CISA y/o CISM y/o CISSP y/o CGEIT y/o CRISC y/o Mile2 Certified Penetration Testing Consultant (CPTC) y/o EC Council Certified Security Analyst (ECSA) y/o Lead Auditor ISO 27001 y/o Lead Cybersecurity y/o Mile2 Certificación Profesional de Hacking Ético (CEHPC).

Consultor Técnico
Curso de SQL Server y deberá contar con al menos una (01) certificación de entre las siguientes: Certificación Profesional de Hacking Ético (CEHPC) y/o EC Council Certified Security Analyst (ECSA) y/o EC Council Licensed Penetration Tester (LPT) y/o Mile2 Certified Penetration Testing Consultant (CPTC) y/o Offensive Security Certified Professional (OSCP) y/o Mile2 Certificación Profesional de Hacking Ético (CEHPC) y/o Lead Auditor ISO 27001 y/o Lead Cybersecurity.

Cabe indicar que la experiencia se contabilizará a partir la obtención del grado de bachiller.

Se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

9. PLAZO DE EJECUCIÓN DEL SERVICIO:
Hasta cuarenta (40) días calendarios, contabilizados desde el día siguiente de la notificación de la orden de servicio.

10. LUGAR DE PRESTACIÓN DEL SERVICIO:
El servicio se desarrollará de manera presencial en las instalaciones del OSCE ubicada en la Av. Punta del Este S/N Edificio el Regidor Residencial San Felipe, Jesús María, Lima, y/o de marea remota de acuerdo a lo coordinado con la UAST.

11. PLAZO DE ENTREGA:

El contratista deberá presentar un informe final hasta los cinco (05) días calendario siguientes de culminado el plazo de ejecución del servicio.

12. ENTREGABLE:

El contratista deberá PRESENTAR el entregable de acuerdo al siguiente detalle:

Informe Final:

Al finalizar la prestación del servicio, el contratista deberá presentar un informe final, según el siguiente detalle:

1. Estado situacional de las pistas de auditoría.
2. Análisis forense realizado a las pistas de auditoría.
3. Detalle de los hallazgos encontrados.
4. Recomendación sobre políticas de respaldo de las pistas de auditoría.
5. Plan de acción de mejora y afinamiento respecto a los hallazgos encontrados sobre las pistas de auditoría, de acuerdo a las buenas prácticas de seguridad.

13. CONFORMIDAD DEL SERVICIO:

Será otorgada por la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones.

Dicha conformidad se otorgará dentro del plazo que no exceda los siete (07) días calendario de recibido el entregable.

14. FORMA DE PAGO:

Pago único: 100% del monto contratado previa conformidad del servicio y presentación del informe final.

En ese sentido, los plazos para los pagos serán según lo establecido en la Ley de Contrataciones del Estado y su Reglamento.

15. ADELANTOS:

No aplica

16. PENALIDADES APLICABLES:

Penalidades por mora: Se aplicará al contratista la penalidad establecida en el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

17. SEGURIDAD Y SALUD EN EL TRABAJO:

Resolución Ministerial N° 031-2023-MINSA, que aprueba la Directiva Administrativa N° 339-MINSA/DGIESP, Directiva Administrativa que establece las disposiciones para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-CoV-2, que como anexo forma parte integrante de la presente Resolución Ministerial y modificatorias.

18. CONFIDENCIALIDAD:

El contratista y su personal se obligan a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones del OSCE a los que tenga acceso en ejecución del presente contrato. En tal sentido, el contratista y su personal deberán abstenerse de divulgar tales documentos e informaciones, sea en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito del OSCE.

19. ACUERDO DE CONFIDENCIALIDAD

- El contratista se compromete a guardar reserva de la información privilegiada que conociera en el ejercicio de sus funciones, tareas y demás actividades como parte de la ejecución de la prestación, no revelando en forma oral, escrita, ni por cualquier otro medio, hechos, datos, procedimientos, documentación e información de acceso restringido (confidencial), a la que tuviera acceso a partir del inicio de las prestaciones relacionadas con el referido servicio, manteniendo la confidencialidad de la misma hasta por 01 año posterior a la culminación del vínculo contractual con el contratista.
- De igual manera se compromete a tomar conocimiento de: la Política Integrada de la Gestión de la Calidad ISO 9001, Gestión de Seguridad de la Información ISO 27001 y Gestión Antisoborno ISO 37001 del OSCE, las Políticas de Seguridad de la Información del OSCE, y demás normas y Leyes correspondientes a seguridad de la información, vigentes.
- En caso que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, el OSCE está autorizado a iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcir del perjuicio y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

20. COMPROMISO ANTISOBORNO:

- El contratista declara conocer los compromisos antisoborno del OSCE, el cual se establece en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del OSCE (https://www.gob.pe/institucion/osce/campa%C3%B1as/1861-politica-del-sistema-integradode-gestion-del-osce).
- El contratista declara no haber, directa o indirectamente, ofrecido, negociado o efectuado pago o, en general, entregado beneficio o incentivo ilegal en relación al servicio a prestarse bien a proporcionarse. En línea con ello, se compromete a actuar en todo momento con integridad, a abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio, percibido de manera directa o indirecta; a cualquier miembro del Consejo Directivo, funcionarios públicos, empleados de confianza, servidores públicos; así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor estimado, elaboración de documentos del procedimiento de selección, calificación y evaluación de ofertas, y la conformidad de los contratos derivados de dicho procedimiento.

MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCION EN LOS PROCESOS DE CONTRATACIÓN (ANEXO N° 4 DE LA DIRECTIVA N° 004-2022- OSCE/SGE)

En el Organismo Supervisor de las Contrataciones del Estado promovemos la ética e integridad de la función pública, por lo que, si conoces de algún acto de corrupción ejercido por un/a servidor/a del OSCE, comunícanos tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/).
Ejemplos:
1. Adecuación o manipulación de las especificaciones técnicas, expediente técnico o términos de referencia para favorecer a un proveedor específico.
2. Generación de falsas necesidades con la finalidad de contratar obras, bienes o servicios.
3. Otorgamiento de la buena pro obviando deliberadamente el procedimiento requerido conforme a ley.
4. Permisividad indebida frente a la presentación de documentación incompleta de parte del ganador de la buena pro.
5. Otorgamiento de la buena pro a postores de quienes se sabe han presentado documentación falsa o no vigente.
6. Otorgamiento de la buena pro de (o ejercicio de influencia para el mismo fin) a empresas ligadas a exfuncionarios, de quienes se sabe están incursos en algunos de los impedimentos para contratar con el Estado que prevé la ley.

7. Admisibilidad de postor (o ejercicio de influencia para el mismo fin) ligado a una misma empresa, grupo empresarial, familia o allegado/a, de quien está incurso en alguno de los impedimentos para contratar con el Estado que prevé la ley.
8. Pago indebido por obras, bienes o servicios no entregados o no prestados en su totalidad.
9. Sobrevaloración deliberada de obras, bienes o servicios y su consecuente pago en exceso a los proveedores que las entregan o brindan.
10. Negligencia en el manejo y/o mantenimiento de equipos y/o tecnología que impliquen la afectación de los servicios que brinda la institución.

¿Conoces de alguno de estos actos de corrupción, o de otros que pueden haberse cometido?, COMUNÍCANOS.

Notas:
(1) La denuncia puede ser anónima.
(2) Si el denunciante decide identificarse, se garantiza la reserva de su identidad y/o de los testigos que quieran corroborar la denuncia, y puede otorgar una garantía institucional de no perjudicar su posición en la relación contractual establecida con la Entidad o su posición como postor en el proceso de contratación en el que participa o en los que participe en el futuro.
(3) Es importante documentar la denuncia, pero si no es posible, se recomienda proporcionar información valiosa acerca de donde obtenerla o prestar colaboración con la entidad para dicho fin.
(4) La interposición de una denuncia no constituye impedimento para gestionar por otras vías que la ley prevé para cuestionar decisiones de la administración o sus agentes (OSCE, Contraloría General de la República, Ministerio Público, etc.).
(5) La interposición de una denuncia no servirá en ningún caso para paralizar un proceso de contratación del Estado.

Firmado digitalmente por ADRIANZEN VALENCIA Angelo Josehp FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.11.2024 13:44:58 -05:00

21. RESPONSABILIDAD POR VICIOS OCULTOS:

Según lo establecido en el artículo 40 de la Ley de Contrataciones del Estado, el plazo máximo de responsabilidad del contratista es de un año contado a partir de la conformidad otorgada por LA ENTIDAD.

22. ANEXOS:

No aplica.

Firmado digitalmente por QUISPE RODRIGUEZ Ruben Raimond FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 11.11.2024 12:50:49 -05:00

Vº Bº Y SELLO
JEFE DEL ÁREA USUARIA