TÉRMINOS DE REFERENCIA

SERVICIO ESPECIALIZADO DE DIAGNOSTICO DE HARDENING A LOS SERVIDORES DE LA PLATAFORMA DE LOS SISTEMAS SEACE Y OCDS 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 mejorar la seguridad de la infraestructura tecnológica, mediante la implementación de prácticas de hardening que fortalezcan la configuración y protección de los servidores de red y los componentes de la infraestructura tecnológica de la plataforma de los sistemas SEACE y OCDS del OSCE.

3. OBJETIVO DEL SERVICIO

El objetivo del servicio consiste en identificar vulnerabilidades y ausencia de controles en los servidores y proponer mejoras para fortalecer la seguridad mediante la recomendación de configuraciones y prácticas seguras, con el fin de minimizar la superficie de ataque y garantizar la integridad, confidencialidad y disponibilidad de la información, cumpliendo con buenas prácticas de hardening y recomendaciones de las marcas que permita mitigar los riesgos frente a amenazas cibernéticas.

4. ACTIVIDAD DEL POI

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

5. CARACTERISTICAS Y/O CONDICIONES DEL SERVICIO

Ítem	Cantidad	Unidad de medida	Descripción
1	01	Servicio	Servicio especializado de diagnóstico de hardening a los servidores de la plataforma de los sistemas SEACE y OCDS del OSCE.

- La Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones proveerá al contratista 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:

- ✓ La reunión de inicio se llevará a cabo al día siguiente hábil de la notificación de la orden de servicio; donde se determinará la información necesaria y el alcance; así como la fecha exacta en que la Entidad deberá entregar la información al proveedor; para lo cual se suscribirá el Acta de Reunión de Inicio.
- ✓ El día que la Entidad entregue la información al proveedor, se suscribirá el Acta de inicio del servicio; lo que implica que el proveedor cumpla con la presentación del Entregable N° 1: cronograma de trabajo.
- ✓ Realizar el diagnóstico de hardening para la plataforma de los sistemas SEACE y OCDS del ambiente de producción (25 servidores virtuales - SO Oracle Linux), de acuerdo a la tabla N° 1 – Lista de Servidores:

- ✓ Realizar el análisis y diagnóstico del estado actual de la seguridad de los servidores virtuales, utilizando herramientas automatizadas como: Nmap, OpenVAS, Nessus, entre otras.
- ✓ Identificación, evaluación e inventario de los servicios, usuarios y puertos innecesarios que se encuentren en escucha o activos y generen riesgo.
- ✓ Evaluación e identificación de vulnerabilidades presentes en los servidores virtuales. Esta actividad debe abarcar el sistema operativo y su auditoria, servidores de aplicaciones (registro de logs y/o auditoria), servidores de base de datos (registro de logs y/o auditoria), a nivel de red (puertos y protocolos). Esta actividad se debe desarrollar considerando las recomendaciones de la marca y las mejores prácticas de seguridad y hardening de servidores.
- ✓ Revisión de parches de seguridad críticos en los servidores virtuales de la plataforma de los sistemas SEACE y OCDS del ambiente de producción. Esta actividad debe abarcar el sistema operativo y su auditoria, servidores de aplicaciones (registro de logs y/o auditoria), servidores de base de datos (registro de logs y/o auditoria), a nivel de red (puertos y protocolos). Esta actividad se debe desarrollar considerando las recomendaciones de la marca y las mejores prácticas de seguridad y hardening de servidores.
- ✓ Revisión de las configuraciones de seguridad de los servidores virtuales de la plataforma de los sistemas SEACE y OCDS del ambiente de producción. Esta actividad debe abarcar el sistema operativo y su auditoria, servidores de aplicaciones (registro de logs y/o auditoria), servidores de base de datos (registro de logs y/o auditoria), a nivel de red (puertos y protocolos). Esta actividad se debe desarrollar considerando las recomendaciones de la marca y las mejores prácticas de seguridad y hardening de servidores.
- ✓ Elaboración y presentación de los resultados obtenidos producto del servicio, así como la respectiva propuesta de solución considerando las recomendaciones de la marca y las mejores prácticas de seguridad y hardening de los servidores virtuales de la plataforma de los sistemas SEACE y OCDS del ambiente de producción.

Tabla N°1 – Lista de servidores virtuales:

N°	Proyecto	Hostname	S.O	Versión	Servicio
1	OCDS	OSCEDSETL02	Oracle Linux	7.9	Servidor BackEnd ETL
2	OCDS	OSCEDSBEPROD02	Oracle Linux	7.9	Servidor Backend OCDS (ElasticSearch)
3	OCDS	OSCEDSFEPROD02	Oracle Linux	7.9	Servidor Frontend OCDS
4	OCDS	OSCEDSNFSPROD02	Oracle Linux	7.9	Servidor Storage NFS
5	SEACE	DBSEACE-NODO1	Oracle Linux	7.9	Oracle Base Database Service
6	SEACE	DBSEACE-NODO2	Oracle Linux	7.9	Oracle Base Database Service
7	SEACE	DBSEACEDG-NODO1	Oracle Linux	7.9	Oracle Base Database Service
8	SEACE	DBSEACEDG-NODO2	Oracle Linux	7.9	Oracle Base Database Service
9	SEACE	OSCEAFPROD01	Oracle Linux	7.9	Servicio Alfresco
10	SEACE	OCIPROID01	Oracle Linux	7.9	Servicio Oracle Internet Directory
11	SEACE	OCIPROID02	Oracle Linux	7.9	Servicio Oracle Internet Directory

N°	Proyecto	Hostname	S.O	Versión	Servicio
12	SEACE	OCIPRWL01	Oracle Linux	7.9	Servicio Oracle WebLogic Server
13	SEACE	OCIPRWL02	Oracle Linux	7.9	Servicio Oracle WebLogic Server
14	SEACE	OCIPRWL03	Oracle Linux	7.9	Servicio Oracle WebLogic Server
15	SEACE	OCIPRADMWL01	Oracle Linux	7.9	Servicio Oracle WebLogic Server
16	SEACE	OCIPRJB01	Oracle Linux	7.9	Servicio JBoss
17	SEACE	OCIPRJB02	Oracle Linux	7.9	Servicio JBoss
18	SEACE	OCIPRJB03	Oracle Linux	7.9	Servicio JBoss
19	SEACE	OCIPRJB04	Oracle Linux	7.9	Servicio JBoss
20	SEACE	OCIPRJB05	Oracle Linux	7.9	Servicio JBoss
21	SEACE	OCIPRJB06	Oracle Linux	7.9	Servicio JBoss
22	SEACE	OCIPRADMJB01	Oracle Linux	7.9	Servicio JBoss
23	SEACE	OCIPRADMJB02	Oracle Linux	7.9	Servicio JBoss
24	SEACE	OCIPRMS01	Oracle Linux	7.9	Servicio JBoss
25	SEACE	OCIPRADMMS01	Oracle Linux	7.9	Servicio JBoss

Fuente: Elaboración propia.

6. REQUISITOS DEL PROVEEDOR:

6.1 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, implementación o análisis o diagnóstico de hardening.

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.

6.2 EXPERIENCIA DEL PERSONAL CLAVE:

- ✓ **Consultor principal**

  Contar con una experiencia profesional mínima de cinco (05) años en proyectos de seguridad de la información, ciberseguridad o informática forense.

- ✓ **Consultor Técnico**

  Contar con una experiencia profesional mínima de cuatro años (04) años en proyectos de seguridad de la información, ciberseguridad o informática forense.

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.

6.3 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.

6.4 CAPACITACION:

- ✓ **Consultor Principal (jefe de proyecto)**

  Curso de Ethical Hacking, curso de administración Linux 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 administración Linux y 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.

7. LUGAR Y PLAZO DE EJECUCIÓN DEL SERVICIO:

7.1 Lugar:

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.

7.2 Plazo:

El plazo de ejecución del servicio, será de hasta cincuenta (50) días calendario contados a partir del día siguiente de la suscripción del Acta de Inicio del Servicio.

8. ENTREGABLES:

El proveedor deberá PRESENTAR los siguientes entregables de acuerdo al detalle que se indica a continuación:

Entregables	Plazo
Entregable N° 1: Cronograma de trabajo	Hasta 5 días calendario, contados a partir del día siguiente de la suscripción del Acta de Inicio

	del Servicio. (cuando la entidad entregue la información)
Entregable N° 2: Informe final que incluya: ✓ Reporte de la identificación de servicios y puertos abiertos innecesariamente en los servidores de red, así como la respectiva propuesta de solución para cerrar los puertos identificados considerando las recomendaciones de la marca y las mejores prácticas de seguridad de servidores. ✓ Detalle de las vulnerabilidades identificadas y resultados obtenidos, así como la respectiva propuesta de solución para superar las vulnerabilidades identificadas y superficies de ataque considerando las recomendaciones de la marca y las mejores practicas de seguridad de servidores. ✓ Conclusiones y recomendaciones con propuesta de mejoras en los servidores virtuales del OSCE considerando las recomendaciones de la marca y las mejores prácticas de seguridad de servidores, las mismas que deben abarcar el sistema operativo y su auditoria, servidores de aplicaciones (registro de logs y/o auditoria), servidores de base de datos (registro de logs y/o auditoria), a nivel de red (puertos y protocolos).	Hasta los 45 días calendario contados a partir del día siguiente de la presentación del Entregable N° 1.

9. LUGAR DE PRESENTACIÓN DEL ENTREGABLE.

El entregable debe ser presentado, a través de la Mesa de Partes Digital del OSCE, disponible en https://apps.osce.gob.pe/mesa-partes-digital/, dirigida a la Unidad de Arquitectura y Soporte de Tecnología de la Información y Comunicaciones.

10. 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 (7) días calendario de recibido el entregable

11. GARANTÍA:

La garantía que el proveedor brinde al servicio realizado entrará en vigor a partir de la fecha de la firma del Acta de conformidad, y tendrá una duración mínima de (06) meses.

12. FORMA DE PAGO

Se hará un pago ÚNICO, y se efectuará previa conformidad del servicio por el área usuaria, el plazo para el pago no excederá los diez (10) días calendario siguientes de recibida la conformidad del Entregable N° 2. (Informe Final).

13. ADELANTOS:

No Aplica

14. PENALIDADES APLICABLES:

✓ **Penalidades por mora:**

De acuerdo a lo establecido en el artículo 162° del Reglamento de la Ley de Contrataciones del estado vigente.

✓ **Otras Penalidades:**

Se aplicará la siguiente penalidad:

N°	Condición	Penalidad	Procedimiento de Verificación
1	No cumplir con presentar el Cronograma de Trabajo al quinto día calendario posterior al acta de reunión de inicio del servicio.	2.5% de la UIT vigente por cada día de atraso	Informe del área usuaria

15. CONFIDENCIALIDAD DE LA INFORMACIÓN

- 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 de manera permanente.
- De igual manera se compromete a cumplir con: 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

16. DENUNCIAS POR PRESUNTOS ACTOS DE CORRUPCIÓN

En atención al numeral 8.1 referido a Disposiciones Complementarias de la Directiva N° 004- 2022-OSCE/SGE – "Directiva para la atención de denuncias por presuntos actos de corrupción, otorgamiento de medidas de protección al denunciante y gestión de las denuncias de mala fe" se anexa el material de orientación para denunciar actos de corrupción.

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.

17. PROPIEDAD INTELECTUAL

La información y material producido bajo los términos de este servicio, tales como escritos, medios magnéticos, digitales, y demás documentación generados por el servicio, pasará a propiedad del OSCE. El/La proveedor deberá mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

18. 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.

19. CLÁUSULA 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-integrado-de-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 o 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.

El contratista se compromete a denunciar, en base de una creencia razonable o de buena fe cualquier intento de soborno, supuesto o real, que tuviera conocimiento a través del canal de denuncias de soborno correspondiente.

20. 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.

21. CLÁUSULA DE CUMPLIMIENTO (LEY DE PREVENCIÓN Y MITIGACIÓN DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PÚBLICO, LEY N° 31564)

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

22. ANEXOS:

No aplica.

Firmado digitalmente por DIAZ ORTIZ Dan Hilber FAU 20419026809 hard
Motivo: Doy V° B°
Fecha: 29.10.2024 18:43:07 -05:00

Firmado digitalmente por QUISPE RODRIGUEZ Ruben Raimond FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 29.10.2024 18:16:58 -05:00

Vº Bº Y SELLO
JEFE DEL ÁREA USUARIA