ANEXO N° 01

OECE – OAD - UABA	FORMATO DE TÉRMINOS DE REFERENCIA PARA SERVICIOS Y CONSULTORÍAS	Versión:	
		Fecha de aprobación:	

DETALLE DEL REQUERIMIENTO	
Área usuaria / Área técnica estratégica	Unidad de Infraestructura y Soporte Tecnológico (UIN)
Número de Cuadro Multianual de Necesidades	APROBACIÓN DE MODIFICACIONES AL CUADRO MULTIANUAL DE NECESIDADES N° 00000035.
Objetivo estratégico	C0286 – DISPONIBILIDAD DE LOS SERVICIOS DEL OECE QUE USAN TECNOLOGIAS DE LA INFORMACION.
Denominación de la Contratación	Servicio de Evaluación de Seguridad y Hardening de Base de Datos del SEACE.
Compatibilización del requerimiento	No aplica.

Firmado digitalmente por ADRIANZEN VALENCIA Angelo Josehp FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 10.07.2026 20:17:10 -05:00

En caso se trate de una consultoría, indicar lo siguiente:

Indicar tipo de consultoría	Servicio de Evaluación de Seguridad y Hardening de Base de Datos del SEACE.
Tipo de información de la consultoría	Este servicio tiene carácter confidencial debido a que se trabajará con información de los servidores y activos tecnológicos del ambiente de producción del OECE.

TÉRMINOS DE REFERENCIA:

FINALIDAD PÚBLICA	*La contratación de este servicio tiene como finalidad mejorar, fortalecer y controlar los mecanismos y medidas de seguridad digital en la capa de datos de la plataforma tecnológica de la entidad. Esto se realiza mediante la aplicación de controles técnicos que garanticen los principios de disponibilidad, confidencialidad e integridad de la información crítica del Sistema Electrónico de Contrataciones del Estado (SEACE), mitigando así riesgos informáticos, reduciendo la superficie de ataque y fortaleciendo la resiliencia institucional.*
OBJETIVO DE LA CONTRATACIÓN	*El objeto del presente servicio es realizar un diagnóstico integral de seguridad (Evaluación y Hardening) de la arquitectura de Base de Datos y del Sistema Operativo que hospeda la instancia de la base de datos del SEACE. El servicio consistirá en aplicar y contrastar el estándar internacional CIS Benchmark para Oracle Database, el CIS Benchmark para Oracle Linux, así como las mejores prácticas y recomendaciones oficiales de seguridad del fabricante Oracle. El servicio concluirá con la entrega de los informes técnicos de brechas (estado actual) que incluye un plan estimado de remediación, quedando excluida la ejecución física o implementación de las mejoras sugeridas.*

CARACTERÍSTICAS DEL SERVICIO

El servicio solicitado debe cumplir con lo siguiente:

1. Reunión de Inicio del Servicio:

   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, requisitos técnicos y el alcance.

2. Metodología para el Desarrollo del Servicio.

   Debido a las políticas estrictas de seguridad, el servicio se regirá bajo la modalidad de asistencia remota guiada, por lo que el postor no tendrá acceso directo, credenciales, ni conectividad a los servidores de base de datos ni de sistema operativo. El postor deberá suministrar el set de scripts (PL/SQL, Shell Scripts) o herramientas de análisis necesarios para la recopilación de datos de configuración. Todo script o herramienta será validada y ejecutada exclusivamente por el equipo técnico del OECE.

   El proceso se ejecutará de acuerdo con las siguientes fases obligatorias, alineadas con el estándar internacional CIS Benchmark para Oracle Database 19c, el CIS Benchmark para Oracle Linux 8, así como la guía oficial de seguridad del fabricante Oracle Database Security Guide 19c.

2.1. Recopilación de información:

Esta fase tiene como objetivo identificar la superficie de exposición y los vectores de riesgo dentro de las instancias de base de datos del OECE. Las actividades mínimas incluyen:

- ✓ identificación de la arquitectura actual, versiones exactas, componentes instalados y revisión del estado de los parches en el motor Oracle 19c que soporta a la plataforma del sistema SEACE.

2.2. Análisis de vulnerabilidades y configuraciones:

Evaluación de la configuración actual del motor de base de datos y del sistema operativo que lo hospeda frente al estándar CIS Benchmark:

- ✓ Recolección de datos e identificación de parámetros inseguros, configuraciones predeterminadas (default), debilidades en la autenticación y vulnerabilidades estructurales en la capa de datos.
- ✓ Identificación de cuentas con privilegios excesivos o asignación inapropiada de roles.
- ✓ Revisión y diagnóstico de la de auditoría de base de datos.
- ✓ Evaluación de cumplimiento de seguridad basándose:
  - CIS Benchmark Oracle Database 19c.
  - CIS Benchmark Oracle Linux 8.
  - Oracle Security Checklist / Recomendaciones del fabricante.

2.3. Elaboración del plan de Hardening

Elaboración del plan de hardening con tiempos estimados para la implementación por personal de la entidad:

- ✓ Identificación y priorización de hallazgos (Crítico, Alto, Medio, Bajo).
- ✓ Diseño de las recomendaciones técnicas específicas para subsanar cada brecha (comandos, parámetros a modificar, etc.).
- ✓ Elaboración de una matriz de esfuerzo estimado para la implementación y/o aplicación controlada del hardening para asegurar la correcta

continuidad operativa de la base de datos del sistema SEACE y el cierre efectivo de las brechas de seguridad identificadas por parte del equipo técnico del OECE.

3. Elaboración de informes:

   El contratista deberá entregar los siguientes documentos tras la finalización de las actividades:

   - ✓ Informe resumen: Orientado a la alta dirección, que contenga un resumen del estado de seguridad, medidas de mitigación de riesgo, principales hallazgos identificados y conclusiones generales sobre el impacto en la continuidad operativa de la entidad.
   - ✓ Informe técnico detallado: Documento de carácter confidencial que incluya la descripción técnica detallada del diagnóstico, detalle de las medidas de mitigación de riesgo, las configuraciones a aplicar y/o corregir, la justificación de los parámetros a aplicar bajo el estándar CIS Benchmark y recomendaciones de mantenimiento preventivo.

Nota: *Es pertinente recordarle que, conforme al artículo 3 de la Ley Nº 31227, las personas que participen en las actividades señaladas en dicho artículo se encuentran obligadas a presentar la declaración jurada de intereses; obligación que será exigible, de acuerdo a lo establecido en el Sistema de Declaraciones Juradas para la Gestión de Conflictos de Intereses de la Contraloría General de la República, de corresponder.*

REQUISITOS DEL PROVEEDOR

Experiencia del Proveedor

Empresa dedicada a brindar servicios de seguridad de la información, ciberseguridad, administración y aseguramiento de bases de datos, auditoría de sistemas o servicios similares.

El postor debe acreditar un monto facturado acumulado equivalente a S/ 35,000.00 (treinta y cinco mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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 consultorías o auditorías de seguridad y/o servicios de encriptación de bases de datos y/o análisis de vulnerabilidades y/o servicios de ofuscamiento de bases de datos y/o implantación, análisis o diagnóstico de hardening a los servidores o infraestructura tecnológica o bases de datos y/o implementación o análisis o diagnóstico de hardening de base de datos.

Acreditación:

La experiencia del postor en la especialidad se acredita con un máximo de veinte (20) contrataciones, mediante copia simple de: (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, o comprobantes de retención electrónico emitido por SUNAT por la retención del IGV. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de servicio con conformidad o constancia de prestación.

CAPACIDAD TÉCNICA Y PROFESIONAL

Experiencia del Personal Clave:

Especialista en Seguridad y Hardening de Bases de Datos (1)

Requisitos:
Tres (03) años de experiencia en labores de seguridad digital y/o ciberseguridad y/o seguridad de la información y/o seguridad informática y/o análisis de vulnerabilidades y/o aseguramiento o hardening de infraestructura, o administración de seguridad en bases de datos del personal clave requerido desempeñándose como Especialista en Seguridad y Hardening de Bases de Datos, Administrador de Base de Datos Oracle, Especialista de Seguridad de Base de Datos Oracle, Auditor de Base de Datos Oracle, Responsable de seguridad de Base de Datos, Coordinador de Seguridad de Base de datos, Analista de Seguridad de Base de Datos o similares en entidades públicas o privadas.

Acreditación:

El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el Anexo N° 19, adjuntando en su oferta, copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.

Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.

Formación Académica:

Especialista en Seguridad y Hardening de Bases de Datos (1)

Requisitos:

Título profesional bachiller o titulado de las carreras de Ingeniería de Sistemas y/o 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 Ingeniería Industrial y/o Ingeniería Electrónica o afines del personal clave requerido como Especialista en Seguridad y Hardening de Bases de Datos, Administrador de Base de Datos Oracle, Especialista de Seguridad de Base de Datos Oracle, Auditor de Base de Datos Oracle, Responsable de seguridad de Base de Datos, Coordinador de Seguridad de Base de datos, Analista de Seguridad de Base de Datos o similares en entidades públicas o privadas.

Acreditación:

El postor debe señalar los nombres y apellidos, documento de identidad, el nombre de la universidad o institución educativa que expidió el grado bachiller o título profesional, y el grado o título profesional obtenido, adjuntando en su oferta copia del grado de bachiller o título profesional. En caso se acredite estudios en el extranjero del personal clave, debe presentarse, adicionalmente, copia simple de la revalidación o reconocimiento del grado o título ante la SUNEDU.

Los evaluadores o la DEC, según corresponda, verifican los grados o títulos profesionales en el Registro Nacional de Grados Académicos y Títulos Profesionales de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU, a través del

siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos del Ministerio de Educación, a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/ según corresponda.

Capacitación del personal clave:

Especialista en Seguridad y Hardening de Bases de Datos (1)

Requisitos:

1. Curso de Oracle Linux 8 o superior y/o RHEL 8 o superior.
2. Contar con certificación de base de datos Oracle: Oracle Database 11g Administrator Certified Professional y/o Oracle Certified Professional (OCP) en Oracle Database 12c y/o Oracle Certified Professional (OCP) en Oracle Database 19c.

Acreditación:

1. Se acredita con copia simple de certificado emitido por una institución pública o privada.

LUGAR Y PLAZO DE EJECUCIÓN *(expresar el plazo en días calendario*	**Lugar**: El servicio será brindado en modalidad presencial en las instalaciones del OECE, pudiendo ser en modalidad mixta es decir presencial y teletrabajo, previa coordinación con la UIN. Las actividades en modalidad presencial se realizarán en la sede del OECE ubicada en la Av. Punta del Este S/N Edificio el Regidor Residencial San Felipe, Jesús María, Lima. **Plazo:** La duración del servicio será de hasta cuarenta y cinco (45) días calendarios, contabilizados desde el día siguiente hábil de notificada la orden de servicio.

ENTREGABLES

Único entregable:

- ✓ Informe resumen: Deberá contener un resumen del estado de seguridad, métricas de riesgo, principales amenazas detectadas (sin detalle técnico de explotación) y conclusiones generales sobre el impacto en la continuidad operativa.
- ✓ Informe técnico detallado: El documento deberá contener la descripción de las herramientas y técnicas utilizadas, el detalle de las vulnerabilidades encontradas; con la descripción técnica y explicación de cada hallazgo, clasificado por criticidad, nivel de riesgo, evidencia de la explotación, guía para la mitigación del riesgo y recomendaciones.

El único entregable que contiene el informe resumen y el informe técnico detallado se debe presentar hasta los 45 días calendario contabilizados desde el día siguiente hábil de notificada la orden de servicio.

CONFORMIDAD

La conformidad del servicio estará a cargo de la UNIDAD DE INFRAESTRUCTURA Y SOPORTE TECNOLOGICO del OECE en donde indique que el servicio fue ejecutado correctamente y sin observaciones.

- El entregable, deberá presentarse a través de la Mesa de partes digital del OECE según el siguiente link: (https://apps.oece.gob.pe/mesa-partes-digital/) dirigido a la Unidad de Infraestructura y Soporte Tecnológico en un plazo de cinco (05) días calendarios.
- La emisión de la conformidad se dará dentro de los siete (7) días calendarios contados a partir del día siguiente de recibido el único entregable.

PENALIDADES

Penalidad por Mora en la ejecución de la prestación *(como referencia)*:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, el OECE le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F = 0.40.

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

OTRAS PENALIDADES (Opcional)

No aplica

FORMA Y CONDICIONES DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad contratante debe contar con la siguiente documentación:

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la UNIDAD DE INFRAESTRUCTURA Y SOPORTE TECNOLOGICO.
- Comprobante de pago y/o factura
- Orden de servicio.

El contratista debe presentar la documentación restante en Mesa de partes digital del OECE según el siguiente link: (https://apps.oece.gob.pe/mesa-partes-digital/).

RESPONSABILIDAD POR VICIOS OCULTOS (*La recepción conforme de la prestación por parte del OECE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas, y 144 de su Reglamento, aprobado por Decreto Supremo N° 009-2025-EF.*

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por el OECE.)

CLÁUSULAS ESPECIALES

a) RESOLUCIÓN CONTRACTUAL

El OECE puede resolver el contrato menor, en los siguientes casos:

i. Por acumulación del monto máximo de la penalidad por mora y/o por otras penalidades, en la ejecución de la prestación a su cargo.
ii. Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
iii. Incumplimiento de obligaciones contractuales, por causa atribuible al contratista.
iv. Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
v. Por incumplimiento de la cláusula anticorrupción y antisoborno.
vi. Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
vii. Por la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.
viii. Por mutuo acuerdo entre las partes, de forma parcial o total, previa opinión del área usuaria y/o área técnica estratégica, en los casos de contrataciones de servicios técnicos, profesionales y/o especializados realizados por personas naturales, bajo locación de servicios.

b) ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del contrato o de la formalización de la Orden, 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, al (los) evaluador (es) del proceso de contratación o cualquier servidor de OECE.

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 entidad contratante, 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 OECE.

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 este acápite, durante la ejecución contractual, otorga al OECE el derecho de resolver total o parcialmente el contrato.

Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

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 de la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/).

El contratista declara conocer los compromisos antisoborno del OECE, el cual se establece en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del OECE:
https://www.gob.pe/institucion/oece/campa%C3%B1as/1861-politica-del-sistemaintegrado-de-gestion-del-oece.

c) CONFIDENCIALIDAD Y 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, pasa a propiedad del OECE. El proveedor debe mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

d) 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 aplica la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

e) ACUERDO DE CONFIDENCIALIDAD

El contratista se compromete a mantener la reserva de toda información privilegiada a la que tenga acceso en el ejercicio de sus funciones, tareas y demás actividades derivadas de la ejecución del servicio contratado. En tal sentido, no puede revelar por ningún medio, ya sea oral, escrito o de cualquier otra forma, hechos, datos, procedimientos, documentación o información de acceso restringido (confidencial), obtenidos a partir del inicio de la prestación del servicio, debiendo preservar su carácter confidencial de manera permanente.

Asimismo, el contratista se compromete a cumplir con: la Política Integrada de la Gestión de la Calidad ISO 9001, Gestión de Seguridad de la Información ISO/IEC 27001 y Gestión Antisoborno ISO 37001 del OECE, las Políticas de Seguridad de la Información del OECE, y demás normas y Leyes correspondientes a seguridad de la información, vigentes.

En caso de incumplimiento de cualquiera de las obligaciones estipuladas en el presente acuerdo, el OECE queda facultado a iniciar las acciones judiciales o extrajudiciales que resulten necesarias a fin resarcir los perjuicios ocasionados. La obligación de confidencialidad permanecerá vigente mientras la información conserve su carácter confidencial.

f) SOLUCIÓN DE CONTROVERSIAS:

Los conflictos que se deriven de la ejecución e interpretación del contrato, orden de compra o de servicio, incluidos los que se refieran a su nulidad e invalidez, son resueltos mediante conciliación.

NOMBRE COMPLETO DEL TITULAR DEL ÁREA USUARIA / ÁREA TÉCNICA ESTRATÉGICA
Firmado digitalmente por VASQUEZ CASTILLO Arquimedes Alejandro FAU 20419026809 soft Motivo: Soy el autor del documento Fecha: 10.07.2026 20:28:48 -05:00 ALEJANDRO ARQUÍMEDES VASQUEZ CASTILLO / UNIDAD DE INFRAESTRUCTURA Y SOPORTE TECNOLÓGICO
FECHA: 10 de julio de 2026