# SERVICIO DE RENOVACIÓN DE CERTIFICADO DIGITAL SSL PARA SERVIDORES WEB DEL OSCE

1. ***AREA USUARIA:***

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

2. ***FINALIDAD PÚBLICA:***

   El presente proceso tiene como finalidad la renovación del Certificado Digital SSL de los servidores web del OSCE, que permitirá ser identificados en internet e intercambiar información de manera segura con otras instituciones con la garantía de que la identidad de los servidores o sitios protegidos puedan ser verificados.

3. ***OBJETIVO:***

   El objetivo del servicio es garantizar la seguridad y confianza a los usuarios internos y externos del Organismo Supervisor de las Contrataciones del Estado (OSCE).

4. ***ACTIVIDAD DEL POI:***

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

5. ***DESCRIPCIÓN DEL SERVICIO:***

| Ítem | Cantidad | Unidad de medida | Descripción |
|---|---|---|---|
| 1 | 01 | Servicio | Servicio de Renovación de Certificado Digital SSL para Servidores Web del OSCE |

***CARACTERÍSTICAS Y/O CONDICIONES DEL SERVICIO:***

***I. CARACTERÍSTICAS TÉCNICAS:***

El Certificado Digital SSL a renovar debe cumplir con los siguientes requerimientos técnicos mínimos:

- El Certificado Digital SSL debe proteger un **número ilimitado de subdominios.**
- El Certificado Digital SSL debe soportar hasta 10 nombres alternativos (SAN) del mismo dominio principal (CN).
- Emisión de certificados a subdominios ilimitados de cuatro (04) dominios.
- El Certificado Digital SSL debe tener una validez de **365 dias,** el cual tendrá como fecha de validez desde el 20/01/2025 hasta el **19/01/2026**.
- El Certificado Digital SSL debe tener un nivel de cifrado de 128 bits como mínimo hasta 256 bits de encriptación.

- El Certificado Digital SSL debe ser compatible con el 99.9% de navegadores: Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera, etc. (últimas versiones).
- El Certificado Digital SSL debe incluir verificación del dominio e identidad de la organización.
- El Certificado Digital SSL debe incluir sello de confianza online del proveedor.
- El Certificado Digital SSL debe ser emitido por Root Certificate Authority – CA Raíz reconocido mundialmente.
- El Certificado Digital SSL debe contar con Soporte IDN (International Domain names).
- El Certificado Digital SSL debe tener Soporte de OCSP (Online Certificate Status Protocol) y CRL.
- Estándar: x.509 v3.
- Remisiones gratuitas ilimitadas en todo el tiempo contratado.
- Opción para remisiones de nombre de los SANs específicos.
- Acceso a la Consola de gestión de Certificados SSL mediante credenciales que serán brindadas por el Proveedor al OSCE.
- ***Garantía:*** Durante la vigencia de validez del certificado digital SSL.
- ***Soporte técnico:***
    - Soporte telefónico / correo electrónico las 24 horas del día, por el periodo de validez del certificado digital SSL.
    - Soporte on-line con base de conocimiento y documentos de soporte.

## *6. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL:*

No aplica.

## *7. REQUISITOS DEL PROVEEDOR:*

### *7.1. Del Proveedor:*

- ✓ El proveedor deberá incluir dentro de su propuesta técnica una carta emitida por el fabricante, en donde indique que están autorizadas para comercializar certificados digitales.

## *8. PLAZO DE EJECUCIÓN*

La vigencia del Certificado Digital SSL será de **365 días** contados a partir del 20/01/2025 hasta el 19/01/2026.

Se deberá emitir el certificado digital hasta el 22/12/2024.

***9. PLAZO DE ENTREGA:***

***<u>ENTREGABLES</u>:***

| Entregable | DETALLE ENTREGABLES |
|---|---|
| ***<u>Entregable N° 01</u>***: Certificado Digital SSL por el periodo del servicio | ○ Certificado Digital SSL remitido al OSCE de manera electrónica para el primer año de servicio. La fecha de emisión del certificado digital SSL debe ser hasta el 22/12/2024 |
| ***<u>Entregable N° 02</u>***: Credenciales de Acceso | ○ Credenciales para poder acceder al portal web y realizar la gestión de los certificados digitales SSL propiedad del OSCE. La fecha para entregar las credenciales es hasta el 22/12/2024 |

Los entregables N° 01 y N° 02 deberá ser presentado a través de mesa de partes implementada por el OSCE y deberá estar dirigido a la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones en un plazo máximo de cinco (05) días calendarios luego de la emisión del certificado digital SSL.

***10. LUGAR DE LA PRESTACIÓN DEL SERVICIO:***

En el Centro de Cómputo de Contingencia (CCC) del OSCE (Edificio El Regidor, Av. Punta del Este cruce con Av. Cádiz, Residencial san Felipe - Jesús María) y/o en remoto previa coordinación con la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones.

**11. CONFORMIDAD DEL SERVICIO:**

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

***12. FORMA DE PAGO:***

Pago único, previa conformidad de la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones a los entregables N° 01 y N° 02.

***13. ADELANTOS:***

No aplica

***14. PENALIDADES APLICABLES:***

**14.1. Penalidades por mora:**

De acuerdo a lo establecido en la Ley de Contrataciones del estado y su reglamento.

**14.2. Otras Penalidades**

Asimismo, en aplicación de lo dispuesto en el Reglamento de la Ley de Contrataciones del estado se aplicarán las siguientes penalidades adicionales:

| SUPUESTO DE APLICACIÓN DE PENALIDAD | FORMA DE CALCULO | PROCEDIMIENTO DE VERIFICACIÓN |
|---|---|---|
| No cumplir con la entrega de los Entregables N°01 y N°02 | 5 % de la UIT vigente por cada día de retraso. | Informe del área usuaria. |
| No cumplir con la fecha máxima de emisión del certificado Digital SSL. | 5% de la UIT vigente por cada día de retraso | Informe del área usuaria |

Dichas penalidades serán aplicadas por la Unidad de Abastecimiento, previo informe de la Unidad de Arquitectura y Soporte de Tecnologías de la Información y Comunicaciones.

***15. CONFIDENCIALIDAD:***

- El contratista se comprometo 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 necesarias para resarcir del perjuicio y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

**16. 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-integrado-degestion-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/).

17. **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

## *18. RESPONSABILIDAD POR VICIOS OCULTOS:*

01 año a partir de culminada la prestación del servicio.

## *19. ANEXOS:*

No aplica

Firmado digitalmente por QUISPE RODRIGUEZ Ruben Raimond FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 28.10.2024 18:04:17 -05:00

Vº Bº Y SELLO
JEFE DEL ÁREA USUARIA

Firmado digitalmente por DIAZ ORTIZ Dan Hilber FAU 20419026809 hard
Motivo: Doy V° B°
Fecha: 28.10.2024 18:10:48 -05:00

Firmado digitalmente por VALDEZ RAMOS Julio Cesar FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 28.10.2024 17:28:36 -05:00