



**Ley 28612 – Ley que Norma el uso de Administración y adecuación del software de la administración pública.**

**INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE – OTI 009/2023**

Fecha de aprobación: 23/08/2023

Página 1 de 6

**Sustento Técnico para la Adquisición de Certificados Digitales SSL/TLS para aplicativos del Ministerio de Relaciones Exteriores**

**1. NOMBRE DEL ÁREA**

Oficina de Tecnologías de la Información.

**2. RESPONSABLE DE LA EVALUACIÓN**

Erick Manuel Bocanegra Villanueva

**Jefe de la Oficina de Tecnologías de la Información.**

Marco Antonio Tomy Baltazar

**Jefe de la Unidad de Redes e Infraestructura.**

Angelo Josehp Adrianzen Valencia

**Administrador de Base de Datos**

**3. FECHA**

23/08/2022

**4. JUSTIFICACIÓN**

El Ministerio de Relaciones Exteriores (MRE) con el fin de mantener la seguridad de los sistemas y/o aplicaciones implementadas en los servidores de la entidad necesita contar con certificados digitales que permitan tener un estándar de seguridad para las funcionalidades de los sistemas y/o aplicaciones que están publicados y brindan servicios en internet.

Por lo expuesto y en el marco de la Ley 28612 “Ley que norma el uso, adquisición y adecuación del software en la Administración Pública” se requiere la adquisición de certificados digitales.

**5. ALTERNATIVAS**

La evaluación técnica del software se ha realizado tomando como referencia productos similares existentes en el mercado con características parecidas que cumplan los requerimientos de la Entidad.

Las alternativas de evaluación consideradas para la adquisición de certificados digitales SSL/TLS para aplicativos de la entidad, son los productos de software de las marcas Entrust, Symantec y Sectigo:

- Entrust EV Multi-Domain SSL/TLS
- Symantec Secure Site Pro EV





- Sectigo EV Multi-Domain SSL/TLS

## 6. ANÁLISIS COMPARATIVO TÉCNICO

### a) Propósito de la evaluación:

Determinar el software apropiado para obtener una capa de seguridad con transferencia de datos de forma cifrada.

### b) Identificar el tipo de producto

Adquisición de certificados digitales multidominio EV SSL/TLS.

### c) Especificación del modelo de calidad:

Se aplicará el modelo de calidad de software descrito en la Parte I de la "Guía Técnica de Evaluación de Software para la Administración Pública" aprobado por Resolución de la Presidencia del Consejo de Ministros, N°139-2004-PCM.

### d) Selección de Métricas:

Las métricas fueron seleccionadas con base en el análisis de información técnica y a los antecedentes previos de evaluación para producto en la institución.

Se aplicó el modelo de calidad externa e interna, de acuerdo a la escala de calificación detallado en el cuadro de características, en base a la metodología establecida en la "Guía Técnica sobre Evaluación de Software para la Administración Pública" aprobada por Resolución Ministerial de la Presidencia del Consejo de Ministros, N° 139-2004-PCM.

Realizando las evaluaciones respectivas para los productos se obtiene la siguiente tabla comparativa:

| Atributo      | Características                                  | Puntaje máximo    | Puntaje mínimo   | Entrust (EV Multi Domain) | Symantec (Secure Site Pro EV) | Sectigo (EV Multi Domain) |
|---------------|--|-------------------|------------------|---------------------------|-------------------------------|---------------------------|
|               | <b>Puntaje total</b>                             | <b>100 puntos</b> | <b>90 puntos</b> | <b>96 puntos</b>          | <b>89 puntos</b>              | <b>97 puntos</b>          |
| Funcionalidad | Número de dominios protegidos                    | 10                | 5                | 9                         | 5                             | 10                        |
| Funcionalidad | Máximo SAN soportado                             | 2                 | 1                | 2                         | 2                             | 2                         |
| Funcionalidad | Trabaja con www.abc.com y abc.com                | 3                 | 2                | 3                         | 3                             | 3                         |
| Funcionalidad | Dominios adicionales                             | 10                | 5                | 9                         | 5                             | 10                        |
| Funcionalidad | Identidad de confianza (Validación organización) | 3                 | 2                | 3                         | 3                             | 3                         |
| Funcionalidad | Opciones de plazo (36 meses y 24 meses)          | 2                 | 1                | 2                         | 2                             | 2                         |
| Fiabilidad    | Soporte técnico 24x5x365                         | 10                | 5                | 10                        | 10                            | 10                        |
| Seguridad     | Sha-2 signing algorithm                          | 4                 | 3                | 4                         | 4                             | 4                         |
| Seguridad     | Rsa 2048 bit/3072 bit/4096 bit key               | 4                 | 2                | 4                         | 4                             | 4                         |
| Seguridad     | Dsa algorithm support                            | 2                 | 1                | 2                         | 2                             | 1                         |
| Seguridad     | Elliptic curve cryptography (ecc)                | 2                 | 2                | 2                         | 2                             | 2                         |
| Seguridad     | Website security bundle                          | 2                 | 2                | 2                         | 2                             | 2                         |





|               |  |   |   |   |   |   |
|---------------|--|---|---|---|---|---|
| Seguridad     | Site seal w/real - time status check     | 2 | 2 | 2 | 2 | 2 |
| Usabilidad    | Licencia de servidor limitada            | 5 | 4 | 5 | 5 | 5 |
| Usabilidad    | Reediciones ilimitadas                   | 3 | 2 | 3 | 3 | 3 |
| Usabilidad    | Plataforma de gestión de certificados    | 3 | 2 | 3 | 3 | 3 |
| Usabilidad    | Auto installer                           | 2 | 2 | 2 | 2 | 2 |
| Usabilidad    | Compatibilidad de escritorio y móvil     | 2 | 2 | 2 | 2 | 2 |
| Seguridad     | Evaluación de vulnerabilidad             | 5 | 2 | 5 | 5 | 5 |
| Seguridad     | Autenticación de organización completa   | 2 | 2 | 2 | 2 | 2 |
| Seguridad     | Netsure garantía extendida               | 2 | 1 | 1 | 2 | 1 |
| Usabilidad    | Comprobador de instalación               | 2 | 2 | 2 | 2 | 2 |
| Seguridad     | Support to sgc                           | 2 | 1 | 1 | 2 | 1 |
| Adaptabilidad | Revocación y reemplazos gratuitos        | 3 | 2 | 3 | 3 | 3 |
| Adaptabilidad | Compatibilidad universal con navegadores | 3 | 2 | 3 | 3 | 3 |
| Adaptabilidad | Support for SAN                          | 4 | 3 | 4 | 4 | 4 |
| Adaptabilidad | Support for IDN                          | 3 | 2 | 3 | 3 | 3 |
| Usabilidad    | Licencia para varios servidores          | 3 | 2 | 3 | 2 | 3 |

## 7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO

En el presente informe técnico previo de evaluación de software, dos (02) alternativas alcanzaron el puntaje mínimo de 90 puntos, por lo que el análisis costo beneficio debe ser realizado considerando ambos productos:

### a) Licenciamiento

| Productos (Certificados Digitales) | Costos en soles (Anual)(*) |
|------------------------------------|----------------------------|
| Entrust EV Multi-Domain SSL/TLS    | s/ 1,318.296 (**)          |
| Sectigo EV Multi-Domain SSL/TLS    | s/ 1,226.020 (***)         |

(\*) Los precios indicados en el análisis de costo/beneficio son referenciales; la Oficina de Logística obtendrá en el estudio de mercado los costos reales.

(\*\*) Costo unitario de \$354/year (Ver anexo 1), tomado de la página oficial de la marca y convertido a soles con tipo de cambio de 3.724 tomado de la página de la SBS con fecha 22/08/2023 (Ver anexo 2).

(\*\*\*) Costo unitario tomado de la última orden de compra N° 0000309-2022 (Ver anexo 3).

### b) Hardware necesario para su funcionamiento:

Ambas marcas de certificados digitales pueden funcionar bajo la arquitectura informática con la que cuenta el Ministerio de Relaciones Exteriores. Para el uso de certificados digitales solo se necesitan adquirir las licencias de cada certificado digital SSL/TLS.

### c) Soporte y mantenimiento externo

No se requiere gastos adicionales con respecto a este componente, ya que cada una de las marcas brinda el soporte y mantenimiento para sus productos y servicios.

### d) Personal y mantenimiento interno.

El personal técnico del Ministerio de Relaciones Exteriores posee el conocimiento en la administración y operaciones de mantenimiento en los certificados digitales de ambos productos.



**e) Capacitación**

El personal técnico del Ministerio de Relaciones Exteriores posee el conocimiento necesario para el mantenimiento y uso de los certificados digitales de ambos productos.

**8. CONCLUSIONES**

Concretados los análisis correspondientes, los certificados Entrust EV Multi-Domain SSL/TLS y Sectigo EV Multi-Domain SSL/TLS cumplen con las especificaciones técnicas requeridas por la Institución, sin perjuicio de los otros productos de certificados digitales que puedan encontrarse en la indagación del mercado realizada por la Oficina de Logística.

**9. FIRMAS**

Erick Manuel Bocanegra Villanueva  
Jefe de la Oficina de Tecnologías  
de la Información



Marco Antonio Tomy Baltazar  
Jefe de la Unidad de Redes e  
Infraestructura



Angelo Adrián Valencia  
Administrador de Base de Datos



PERÚ

Ministerio de Relaciones Exteriores

Oficina General de Apoyo a la Gestión Institucional

Oficina de Tecnologías de la Información

ANEXOS:

Anexo 1: Costo del certificado digital Entrust EV Multi-Domain SSL/TLS al 22/08/2023.

<https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates/ev-multi-domain-ssl>



Anexo 2: Tipo de cambio de la SBS al 22/08/2023

[https://www.sbs.gob.pe/app/pp/sistip\\_portal/paginas/publicacion/tipocambiopromedio.aspx](https://www.sbs.gob.pe/app/pp/sistip_portal/paginas/publicacion/tipocambiopromedio.aspx)

COTIZACIÓN DE OFERTA Y DEMANDA TIPO DE CAMBIO PROMEDIO PONDERADO

Ingrese fecha: 22/08/2023 (dd/mm/aaaa) Consultar Exportar

Tipo de Cambio al 22/08/2023

| MONEDA            | COMPRA (S/) | VENTA (S/) |
|-------------------|-------------|------------|
| Dólar de N.A.     | 3.724       | 3.729      |
| Dólar Australiano |             | 2.580      |
| Dólar Canadiense  | 2.681       | 2.999      |
| Peso Chileno      | 0.004       |            |
| Libra Esterlina   | 4.745       | 5.152      |
| Yen Japonés       | 0.026       | 0.028      |
| Peso Mexicano     | 0.220       | 0.256      |
| Franco Suizo      | 3.942       | 4.713      |
| Euro              | 3.891       | 4.255      |





PERÚ

Ministerio de Relaciones Exteriores

Oficina General de Apoyo a la Gestión Institucional

Oficina de Tecnologías de la Información

Anexo 3: Costo de certificado digital Sectigo con base a la orden de compra N° 0000309-2022.

Sistema Integrado de Gestión Administrativa  
Módulo de Logística  
Versión 22.02.01

Página: 1 de 4

**ORDEN DE COMPRA - GUÍA DE INTERNAMIENTO N° 0000309**

N° Exp. SIAF:

UNIDAD EJECUTORA : 001 MINISTERIO DE RELACIONES EXTERIORES  
NRO. IDENTIFICACIÓN : 000045

| 1 DATOS DEL PROVEEDOR   |  | 2. CONDICIONES GENERALES  |  |
|---|--|---|--|
| Señor(ee): PERU MEDIA SECURITY S.A.C.<br>Dirección: CAL 2 DE MAYO NRO. 516 INT. 201<br>LIMA / LIMA / MIRAFLORES<br>RUC: 20601709852 Teléfono: |  | N° Cuadro Adquisic: 000308<br>Tipo de Proceso: ASP<br>N° Contrato:<br>Moneda: S/ T/C: |  |
| CCI: 00219400238479907891<br>Fax:   |  |   |  |
| Concepto: ADQUISICIÓN DE CERTIFICADOS DIGITALES SSL/TLS PARA APLICATIVOS DEL MINISTERIO DE RELACIONES EXTERIORES                              |  |   |  |

| Código       | Cant. | Unid. Med. | Descripción  | Precio       |           |
|--------------|-------|------------|--|--------------|-----------|
|              |       |            |  | Unitario S/  | Total S/  |
| 140400040168 | 10    | UNIDAD     | CERTIFICADO DIGITAL SSL<br>ADQUISICIÓN DE CERTIFICADOS DIGITALES SSL/TLS PARA APLICATIVOS DEL MINISTERIO DE RELACIONES EXTERIORES, SOLICITADO POR LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN MEDIANTE MEMORANDUM (OTI) N° 01512/2022<br>PRESTACIÓN PRINCIPAL<br>*DIEZ UNIDADES DE CERTIFICADOS DIGITALES EV SSL/TLS QUE PERMITAN COMO MÍNIMO 3 NOMBRES ALTERNATIVOS.<br>*NOMBRES ALTERNATIVOS (SAN) ADICIONALES: SAN EV POR CADA CERTIFICADO DIGITAL<br>*CERTIFICADO DIGITAL SSL/TLS<br>*SOPORTA TLS 1.2; 2.0 Y EN SU ÚLTIMA VERSIÓN<br>*VALIDEZ DE UN AÑO A PARTIR DE SU ACTIVACIÓN<br>*ESTÁNDAR X.509 V3<br>*CERTIFICACION DE DOMINIO E IDENTIDAD DE ORGANIZACIÓN<br>*ALGORITMO DE CIFRADO MÍNIMO SHA256<br>*NIVEL DE CERTIFICADO 256 BITS COMO MÍNIMO<br>*EXTENDED VALIDATION (EV)<br>*SELLO DE CONFIANZA DEL PROVEEDOR<br>*SOPORTE DE OSCP<br>*CRYPTOGRAFÍA DE CURVA ELÍPTICA (ECC)<br>*SOPORTE IDN | 1,226.020000 | 12,260.20 |

| AFECTACION PRESUPUESTAL |                                  |        |               |       | Van ... S/ |
|-------------------------|----------------------------------|--------|---------------|-------|------------|
| Meta/Inemónico          | Cadena Funcional                 | FF/Rb  | Clasif. Gasto | Monto |            |
|                         |                                  |        |               |       | S/         |
| 0018                    | 02 006 0008 9001 3999999 5000003 | 1 - 00 | 2.6.6 1.3 99  |       | 12,260.20  |

|                |                  |
|----------------|------------------|
| Exonerado :    | 0.00             |
| V Venta :      | 10,390.00        |
| I.G.V :        | 1,870.20         |
| <b>Total</b> : | <b>12,260.20</b> |

