Gobierno de Colombia

# Contratar la renovación de dos (2) certificados digitales de sitio seguro (SSL/TLS) para los dominios institucionales de Computadores para Educar

## - ANEXO TÉCNICO -

**Computadores para Educar**

**BOGOTÁ D.C, SEPTIEMBRE DE 2026**

**Computadores para Educar**
Teléfono: (601) 313 77 77
Cra. 11 # 71-73, Bogotá, Colombia
Edif. Davivienda - Piso 10
Calle. 17a # 69f-49, Centros -
Zona Industrial de Montevideo

CERTIFICADO
ISO 9001:2015
ISO 14001:2015
CO26.05924
CO26.05925

Gobierno de Colombia

# FICHA TÉCNICA

Computadores para Educar es una asociación sin ánimo de lucro creada en el año 2000, a partir de los lineamientos de política del documento CONPES 3063 del 23 de diciembre de 1999, y lo establecido en el Decreto 2324 del 9 de noviembre del 2000. Sus asociados son: el Fondo de Tecnologías de la Información y las Comunicaciones, hoy Fondo Único de las Tecnologías de la Información y las Comunicaciones; el Ministerio de Educación Nacional y el Servicio Nacional de Aprendizaje (SENA). Es una entidad pública de segundo orden, autónoma, con personería jurídica, patrimonio independiente, con órganos de dirección y control propios, vigilada por la Contraloría General de la República.

Computadores para Educar fue creada bajo los lineamientos del CONPES 3063 de 1999 y tiene como objetivo fomentar la calidad de la educación bajo un modelo sostenible mediante el uso de las TIC, enmarcado en las competencias definidas para la prestación del servicio público educativo en sus niveles preescolar, básico y medio. De esta manera, enfoca sus esfuerzos en contribuir al cumplimiento de las metas del Gobierno relacionadas con el incremento de los niveles de educación a través de las TIC.

Computadores para Educar tiene como misión impulsar la innovación educativa con tecnologías digitales, contribuyendo al bienestar y desarrollo sostenible de la sociedad, promoviendo el acceso y la generación de conocimiento. Su gestión se desarrolla a través de cuatro líneas estratégicas: i) Acceso a TIC, ii) Apropiación pedagógica, iii) Sostenibilidad Ambiental y iv) Monitoreo & Evaluación. A través de estas líneas, entrega equipos a sedes educativas, casas de la cultura y bibliotecas públicas, y forma a los docentes para desarrollar competencias TIC, de manera que las soluciones tecnológicas se conviertan en herramientas que apoyen y fortalezcan la calidad educativa y contribuyan con nuevas oportunidades para los aprendizajes de los estudiantes.

De acuerdo con su naturaleza y misión, la asociación Computadores para Educar está estructurada administrativamente en una Dirección Ejecutiva, jefaturas y subdirecciones. Dentro de esta organización se encuentra la Subdirección de Tecnologías de la Información (TI), responsable de velar por el adecuado funcionamiento de la infraestructura tecnológica de la entidad y de brindar soluciones tecnológicas que generen valor, optimicen los procesos internos y garanticen la disponibilidad oportuna y segura de la información institucional.

A través de la gestión de sus servicios tecnológicos, esta subdirección contribuye de manera directa al cumplimiento de la misión institucional, fortaleciendo la capacidad operativa de las áreas misionales y facilitando la ejecución eficiente de los programas y proyectos orientados al cierre de brechas digitales en el país.

En este contexto, la Subdirección de Tecnologías de la Información (TI) ha implementado herramientas informáticas que le permiten a los usuarios internos y externos acceder a los diferentes servicios que ofrece la Entidad a través de mecanismos virtuales, apoyando de esta forma la consecución de los objetivos de esta y el cumplimiento de las políticas de gestión y desempeño.

Así, se hace necesario emplear instrumentos que permitan establecer un canal seguro entre el usuario y el servidor de manera que los datos viajen de manera íntegra y segura. Donde, es indispensable garantizar la autenticidad de la identidad del sitio de manera que se mitigue el riesgo de ataques de suplantación de identidad y certificar la confidencialidad de la información que se intercambia.

Por su parte la Política de Tratamiento de Información Personal de Computadores para Educar establece que se deben implementar los mecanismos necesarios para evitar el acceso no autorizado a terceros que puedan conocer o vulnerar, modificar, divulgar y/o destruir la información que allí reposa. De igual forma la Política Interna de Seguridad de la Información tiene como uno de sus principios minimizar el riesgo en el manejo de la información, en los procesos de la entidad.

En virtud de lo anterior, desde la Subdirección de Tecnologías de la Información (TI) se ha identificado la necesidad de adquirir dos (2) certificados digitales de sitio seguro (SSL - Secure Sockets Layer), con el propósito de mantener conexiones seguras mediante cifrado y proteger el tráfico de datos asociado a los servicios web y sistemas de información de Computadores para Educar.

Los certificados digitales de sitio seguro permiten autenticar los dominios asociados a los servicios institucionales y establecer conexiones seguras mediante HTTPS, utilizando protocolos de seguridad como TLS (Transport Layer Security) para proteger la información transmitida entre los usuarios y los servidores. De esta manera, contribuyen a preservar la confidencialidad e integridad de la información, así como a verificar la autenticidad del sitio web y mitigar riesgos asociados a la interceptación, modificación de la información o suplantación de los servicios institucionales.

## 1. OBJETO DEL CONTRATO

Contratar la renovación de dos (2) certificados digitales de sitio seguro (SSL/TLS) para los dominios institucionales de Computadores para Educar, con el propósito de mantener habilitadas las conexiones seguras mediante HTTPS/TLS y contribuir a la protección, autenticidad, confidencialidad e integridad de la información intercambiada a través de los servicios web de la Entidad.

## 2. JUSTIFICACIÓN DE LA NECESIDAD

Computadores para Educar, en cumplimiento de su misión institucional y de las funciones asignadas a la Subdirección de Tecnologías de la Información (TI), requiere disponer de una infraestructura tecnológica que permita garantizar la continuidad, disponibilidad, seguridad y adecuado funcionamiento de los servicios y sistemas de información utilizados por la Entidad.

En desarrollo de sus actividades, CPE cuenta con diferentes plataformas, aplicaciones y servicios web que permiten el acceso de usuarios internos y externos a información y funcionalidades institucionales. Estos servicios requieren mecanismos de seguridad que permitan establecer comunicaciones confiables entre los usuarios y los servidores de la

Entidad, especialmente cuando durante su utilización se intercambia información que debe ser protegida frente a riesgos de interceptación, alteración o acceso no autorizado.

En este contexto, los certificados digitales de sitio seguro constituyen un componente necesario para habilitar conexiones seguras mediante el protocolo HTTPS/TLS, permitiendo autenticar los dominios asociados a los servicios web institucionales y proteger mediante cifrado la información transmitida entre los usuarios y los servidores. De esta manera, contribuyen a preservar la confidencialidad e integridad de la información, así como a mitigar riesgos relacionados con la suplantación de los sitios y servicios institucionales.

Lo anterior guarda relación con las disposiciones internas de la Entidad en materia de protección de la información. En particular, en lo relacionado con la Política de Tratamiento de Información Personal establece la necesidad de implementar mecanismos orientados a prevenir el acceso no autorizado de terceros a la información que reposa en la Entidad, mientras que la Política Interna de Seguridad de la Información contempla dentro de sus principios la gestión y minimización de los riesgos asociados al manejo de la información institucional.

Por lo anterior, y teniendo en cuenta que los certificados digitales actualmente utilizados por la Entidad se encuentran sujetos a períodos determinados de vigencia, resulta necesario renovar dos (2) certificados digitales de sitio seguro, con el fin de mantener la operación de los servicios web institucionales bajo conexiones HTTPS/TLS y evitar afectaciones derivadas de su vencimiento, tales como alertas de seguridad en los navegadores, pérdida de confianza en los sitios, exposición de las comunicaciones y posibles interrupciones en el acceso a los servicios.

La renovación permitirá mantener las condiciones de seguridad requeridas para la prestación de los servicios tecnológicos de la Entidad, fortaleciendo la protección de la información intercambiada con los usuarios y contribuyendo a la continuidad y confiabilidad de las plataformas institucionales.

## 3. INFORMACIÓN GENERAL

### 3.1. TIPO DE SERVICIO REQUERIDO

Renovación de dos (2) certificados digitales de sitio seguro (SSL/TLS) para los dominios institucionales, con la finalidad de mantener la seguridad de las comunicaciones y reducir los riesgos que están asociados al acceso de los servicios web de la Entidad.

### 3.2. NOMBRE REFERENCIA DEL PRODUCTO

El servicio objeto del presente Proceso de Contratación está codificada en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC) con el tercer nivel como se indica a continuación:

| Código y nombre del Segmento | Código y nombre de Familia | Código de nombre de clases |
|---|---|---|
| **43000000** Difusión de Tecnologías de Información y Telecomunicaciones | **43230000** Software | **43233200** Software de seguridad y protección. |

### 3.3. VIGENCIA MINIMA REQUERIDA

Las licencias deben tener una vigencia de 1 año contado a partir de la instalación.

Cabe aclarar que, en abril de 2025 el CA/Browser Forum acordó acortar la validez de los certificados para mejorar la seguridad: actualmente 200 días y en 2027 100 días hasta llegar a los 47 días de valides en el 2029.

Lo anterior, implica que si se instalan los nuevos certificados el día 28 de octubre de 2026 deberían ser renovados el día 16 de mayo de 2027 y posteriormente renovados a los 100 día es decir el día 24 de agosto de 2027 y así sucesivamente por el periodo de cobertura contratado (1 año).

La mayoría de los proveedores ofrecen el servicio de actualización automática en modalidades de 1, 2 y hasta seis años. Según esto, se requiere que el proveedor garantice las actualizaciones automáticas a que haya lugar durante la vigencia de un año.

### 3.4. FORMA DE PAGO

Un solo pago correspondiente al cien por ciento (100%) del valor total del contrato, contra la entrega de las certificaciones adquiridas.

## 4. CONDICIONES TÉCNICAS:

Los certificados digitales SSL/TLS con Validación de Organización (OV), destinados a los dominios institucionales cpe.gov.co y computadoresparaeducar.gov.co, deberán proteger las comunicaciones mediante conexiones HTTPS seguras. Como mínimo, deberán cumplir las condiciones establecidas sobre vigencia, cifrado, algoritmos, protocolos de seguridad, compatibilidad, cobertura, generación y custodia de la llave privada, y entrega del certificado.

### 4.1 CIFRADO Y ALGORITMO

Los certificados deberán utilizar mecanismos criptográficos vigentes que garanticen la confidencialidad, integridad y autenticidad de las comunicaciones. Deberán ser compatibles con algoritmos de clave pública RSA y admitir longitudes de clave y algoritmos seguros, conforme a los estándares y recomendaciones actuales de la industria. No se permitirá el uso de mecanismos criptográficos obsoletos, inseguros o vulnerables.

## 4.2 PROTOCOLOS DE SEGURIDAD

La solución deberá ser compatible con versiones vigentes y seguras del protocolo TLS, reconocidas por los principales navegadores, sistemas operativos y servidores web. Los protocolos y parámetros criptográficos utilizados deberán ajustarse a los estándares de seguridad aplicables durante la vigencia del certificado y excluir versiones o mecanismos obsoletos o con vulnerabilidades conocidas.

## 4.3 COMPATIBILIDAD

Los certificados deberán ser reconocidos por los principales navegadores, sistemas operativos y plataformas tecnológicas de uso habitual, y garantizar su interoperabilidad con los servicios web institucionales.

Asimismo, deberán contar con una cadena de confianza válida y reconocida, que permita establecer conexiones seguras sin generar advertencias, errores o alertas atribuibles al certificado, a su cadena de certificación o a la Autoridad de Certificación emisora.

## 4.4 COBERTURA

CPE utilizará la modalidad Wildcard, permitiendo proteger, mediante un único certificado, múltiples subdominios. Es decir, se tendrán dos certificados uno para **cpe.gov.co** y otro para **computadoresparaeducar.gov.co** con sus respectivos subdominios.

Esta modalidad deberá facilitar la administración y gestión de los certificados digitales utilizados en los diferentes servicios web institucionales, reduciendo la necesidad de disponer de certificados independientes para cada subdominio.

Esta solución garantizara la adecuada autenticación, cifrado y establecimiento de conexiones seguras mediante HTTPS en los dominios y subdominios protegidos.

## 4.5 COMPATIBILIDAD CON INFRAESTRUCTURA TECNOLÓGICA

Los certificados deberán ser compatibles con las plataformas utilizadas por CPE y con los ambientes que soporten SSL/TLS, incluidos servidores web, balanceadores de carga, infraestructura virtualizada, contenedores y demás componentes de los servicios web institucionales.

Su instalación, configuración y operación deberán ajustarse a las características de cada plataforma, sin exigir modificaciones que afecten el funcionamiento de la infraestructura existente.

## 5. SITUACIÓN ACTUAL

CPE utiliza certificados SSL/TLS en controladores de dominio, múltiples subdominios, servidores web, firewalls y servicios WAF alojados en Microsoft Azure, entre otros componentes. Estos certificados son necesarios para prevenir riesgos de seguridad y

garantizar la continuidad de los servicios y aplicaciones que dependen de ellos. Los certificados actuales estarán vigentes hasta el 28 de octubre de 2026.

## 6. REQUERIMIENTO PARA EL CONTRATISTA

### 6.1 DOCUMENTACIÓN

El contratista deberá entregar la documentación que acredite el aprovisionamiento y la adquisición de las dos licencias de certificados SSL/TLS.

### 6.2 OBLIGACIONES ESPECIFICAS

- Entregar dos certificados digitales de sitio seguro con Validación de Organización y soporte para múltiples subdominios (Wildcard OV), en los formatos .key, .crt, .crt-ca-bundle, .pfx, .p7b y .pem.

- Atender de forma inmediata los requerimientos relacionados con la instalación, configuración y soporte técnico de los certificados digitales de la Entidad.

## 7. CONDICIONES LOGISTICAS

Las siguientes condiciones describen el proceso mínimo de activación, asignación de licencias y demás aspectos operativos que deberá contemplar el contratista.

### 7.1 ACTIVACIÓN DEL SERVICIO

Una vez emitida la orden de inicio por parte de Computadores para Educar, el contratista deberá entregar una constancia de puesta en operación, ya sea mediante acta o comunicación escrita, en la que se deje evidencia de la activación del servicio y de las licencias.

### 7.2 LUGAR DE EJECUCIÓN

Las actividades serán realizadas de manera virtual o presencial, en las sedes de Computadores para Educar, en los horarios que se definan desde la supervisión del contrato, y contemplando las necesidades del servicio:

Computadores para Educar
Carrera 11 # 71-73, Edificio Davivienda, Piso 10
Bogotá, D.C. – Colombia

Centro Nacional de Aprovechamiento de Residuos Electrónicos
Calle 17A No. 69F-49
Bogotá, D.C. – Colombia

Centro de Soluciones Tecnológicas
Calle 17A No. 69F-35

Bogotá, D.C. – Colombia

## 8. ENTREGABLES MÍNIMOS

- Entregar dos certificados digitales de sitio seguro con Validación de Organización y soporte para múltiples subdominios (Wildcard OV), en los formatos .key, .crt, .crt-ca-bundle, .pfx, .p7b y .pem, para los dominios:
  - Cpe.gov.co
  - Computadoresparaeducar.gov.co

- Atender de forma inmediata los requerimientos relacionados con la instalación, configuración y soporte técnico de los certificados digitales de la Entidad

## 9. CONDICIONES PARA LA COTIZACIÓN

La cotización deberá presentarse únicamente en pesos colombianos (COP) incluido el valor del IVA.

## 10. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de dos (02) mes, a partir de la suscripción del acta de inicio entre las partes, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. Además, las licencias deben tener una vigencia de 1 año y conforme a lo descrito en el subnumeral **3.3. VIGENCIA MINIMA REQUERIDA** del presente documento.

Gobierno de Colombia

| FORMATO DE COTIZACIÓN – LICENCIAMIENTO SSL/TLS tipo WILDCARD OV | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Razón social del proponente:** | | | | | | | | |
| **NIT:** | | | | | | | | |
| **Dirección:** | | | | | | | | |
| **Correo electrónico:** | | | | | | | | |
| **Teléfono de contacto:** | | | | | | | | |
| **¿Es MiPyME? (Sí/No):** | | | | | | | | |
| **Nota:** | | | | | | | | |
| **ÍTEM** | **ACCIÓN** | **TIPO** | **UNIDAD** | **CANTIDAD** | **VALOR UNITARIO** | **IVA** | **VALOR UNITARIO ANTES DE IVA** | **VALOR TOTAL CON IVA** |
| 1 | LICENCIAMIENTO SSL/TLS | WILDCARD OV | Licencia | 2 | **$** | **$** | **$** | **$** |
| **Nombre / Firma** | | | | | | | | |
| **Teléfono** | | | | | | | | |
| **Correo electrónico** | | | | | | | | |
| **Cargo** | | | | | | | | |

**Computadores para Educar**
Teléfono: (601) 313 77 77
Cra. 11 # 71-73, Bogotá, Colombia
Edif. Davivienda - Piso 10
Calle. 17a # 69f-49, Centros -
Zona Industrial de Montevideo

CERTIFICADO
ISO 9001:2015
ISO 14001:2015
CO26.05924
CO26.05925