ANEXO N° 1
FICHA TÉCNICA

<table>
<tr><td colspan="3">Objeto: OIS-191-Contratar la adquisición de certificados de firma digital tipo Token y la renovación de los certificados SSL para el dominio y Subdominios de la Entidad.</td></tr>
<tr><td colspan="2">Denominación del Bien:</td><td>Contratar la adquisición de certificados de firma digital tipo Token y la renovación de los certificados SSL para el dominio y Subdominios de la Entidad.</td></tr>
<tr><td colspan="2">Clasificación UNSPSC</td><td>El objeto contractual está codificado en el clasificador de bienes y servicios UNSPSC (The United Nations Standard Products and Services Code / Codificación de Bienes y Servicios de Acuerdo con el Código Estándar de Productos y Servicios de Naciones Unidas) como se indica a continuación:
<table>
<tr><th>Clasificación UNSPSC</th><th>Segmento</th><th>Familia</th><th>Clase</th><th>Producto</th></tr>
<tr><td>43233201
Software de servidor de autenticación</td><td>43000000
Difusión de Tecnologías de Información y Telecomunicaciones</td><td>43230000
Software</td><td>43233200
Software de seguridad y protección</td><td>43233201
Software de servidor de autenticación</td></tr>
<tr><td>43231503
Software para oficinas</td><td>43000000
Difusión de Tecnologías de Información y Telecomunicaciones</td><td>43230000
Software</td><td>43231500
Software funcional específico de la empresa</td><td>43231513
Software para oficinas</td></tr>
</table></td></tr>
<tr><td colspan="2">Denominación Técnica:</td><td>Adquirir la renovación de los certificados SSL, Wildcard para el dominio y Subdominios de la entidad y el certificado SSL/TSL para el pool de equipos de HA de FORTIGATE.</td></tr>
<tr><td colspan="2">Unidad de Medida:</td><td>Unidad</td></tr>
<tr><td colspan="3">CERTIFICADOS SSL</td></tr>
<tr><td>ITEM</td><td>CARATERISTICA</td><td>MINIMO REQUERDO</td></tr>
<tr><td>1.1</td><td>Cantidad</td><td>Un (1) certificado SSL – EV "para el dominio principal foncep.gov.co y www.foncep.gov.co" y Un (1) Certificado SSL Wildcard (DV) para los subdominios "*.foncep.gov.co".
Un (1) certificado SSL/TSL para el pool de equipos de HA de FORTIGATE, puesto que los equipos de seguridad perimetral usan un certificado auto firmado que el sistema no reconoce como seguro.</td></tr>
</table>

1.2	**Generalidades**	Las áreas de tecnología de la información se han convertido en actores de apoyo fundamentales a nivel estratégico, táctico y operativo, lo cual indica que las organizaciones dependen cada día más de estas áreas para alcanzar sus objetivos, generando una necesidad creciente de servicios informáticos disponibles y de calidad; tanto para la operatividad de los usuarios de las entidades como para la ciudadanía, a la cual se prestan servicios. Por ello debe garantizar disponibilidad, integridad, confidencialidad, oportunidad y mejora continua de los servicios de TI, proporcionando a los funcionarios y a la ciudadanía las herramientas necesarias para el desarrollo de sus actividades.
1.3	**Características del servicio**	• El contratista debe entregar un (1) Certificado digital de capa de conexión segura de preferencia, con validación extendida (SSL – EV) y un (1) Wildcard, un (1) Certificado SSL/TLS de dominio único (Single Domain) para el FQDN que se utilizará para el portal de la SSL-VPN, todos con vigencia de uso de doce (12) meses, de acuerdo con las exigencias jurídicas y técnicas previstas en la normatividad vigente, que permita legitimar la autenticidad de los servicios ofrecidos por la Entidad a través de la internet así como permitir el establecimiento de conexiones seguras entre los servicios ofrecidos y el navegador del usuario que accede a él. • Los certificados digitales deben ser compatible con todos los navegadores (Mozilla Firefox, Internet Explorer, Google Chrome, Opera, Safari.)
1.4.	**Instalación y Configuración**	• El contratista debe realizar el apoyo y asesoría técnica al personal de infraestructura de FONCEP para el proceso de instalación, configuración y pruebas de funcionalidad de los Certificados SSL adquiridos, en los servidores que la Entidad designe. • Se debe apoyar y asesorar a los ingenieros de FONCEP para garantizar que los Certificados SSL, Wildcard y Certificado SSL/TLS de dominio único (Single Domain) para el FQDN, queden funcionales y con licencia vigente por el periodo estipulado en la compra. • Se debe apoyar y asesorar a los ingenieros del FONCEP en el protocolo a realizar para revisión de los posibles casos que puedan ocurrir con los Certificados (SSL, Wildcard, Certificado SSL/TLS de dominio único (Single Domain) para el FQDN) durante la vigencia, con el objetivo de poder atender de forma inmediata los casos que puedan ocurrir, adicional se de asesorar a los ingenieros en el debido proceso de escalamiento de casos que se requieran realizar al proveedor de los Certificados.
1.5	**Certificaciones**	El proponente deberá presentar con la oferta económica el certificado de distribuidor autorizado y/o certificado de fabricante directo de certificados SSL.

2	TOKEN PARA FIRMA DIGITAL	
ITEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
2.1	**Tipo**	Certificado digital de función pública
2.2.	**Cantidad**	Doce (12) certificados digitales tipo token USB y/o token virtual (Según necesidad de la entidad).
2.3.	**Nombre**	Certificado digital función pública
2.4.	**Validez**	Cada certificado con validez de un (1) año a partir de su activación.
2.5.	**Referencia**	Certificado Digital de Función Pública
2.6.	**Sistemas operativos**	32bit and 64bit Windows XP SP3, Vista, 7, 8, 10, 11. Mac OS. Server2003, Server2008, Server2008 R2, Server 2012 R2.
2.7.	**Estándar**	X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
2.8.	**Funciones criptográficas**	Generación de par de claves Firma digital y verificación Cifrado y descifrado de datos
2.9.	**Conectividad**	Token USB y/o Token Virtual
	Almacenamiento	La entidad requiere que los certificados vayan almacenados en token físico y/o virtual dependiendo la necesidad de la entidad.
2.10.	**Bloqueo del Dispositivo**	**Se bloqueará al tercer intento de uso con clave incorrecta**
2.11.	**Algoritmo de firma**	Función Hash SHA256 con RSA Encryption Función de Cifrado RSA con longitud de clave de 4096 para CA RAIZ RSA con longitud de clave de 4096 para SUBORDINADA CA RSA con longitud de clave suscriptores / responsables de 4096.
2.12.	**Contenido de certificado digital**	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Mayo 2008. ITU-T-X509 octubre 2016 ETSI TS 102 042 - Policy requirements for certification authorities issuing public key. Dispositivo criptográfico (Token) dentro de un kit por usuario que contenga; el token, sobreflex con respectiva clave, manual del usuario y manual del software . **Alternativa:** Entrega del PIN a través de una notificación por correo electrónico

2.13.	**Ciclo de vida de los certificados**	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
2.14.	**Generación de claves**	Token FIPS 140-2 Nivel 3
2.15.	**Otras características**	Los certificados tienen que ser emitidos por una entidad certificadora de confianza reconocida por la ONAC.
2.16.	**Vigencia de los tokens para firma digital**	Los tokens de firma digital tipo token deberán contar con duración de uso de un (1) año para los usuarios de FONCEP. La activación de cada uno de los tokens se hará cuando el FONCEP lo determine y para la persona que la entidad designe en cada caso.
2.17.	**Revocación**	El token y/o firma digital debe tener al menos **una (1) revocación** para asignar a un nuevo funcionario durante su vigencia de activación.
2.18.	**Soporte**	El soporte deberá brindarse a través de correo electrónico y/o sesiones remotas cuando sea requerido por la entidad y durante la vigencia de los certificados, con un tiempo máximo de respuesta para incidentes por severidad críticos y altos de 8 a 48 horas y para incidentes por severidad medios y bajos de 48 a 72 horas. En caso de olvido de contraseña se deberá permitir hasta (3) intentos antes de que el Token quede bloqueado o inactivo.
2.19	**Instalación y Configuración**	El contratista debe realizar el apoyo y asesoría técnica al personal de infraestructura de FONCEP para el proceso de instalación, configuración y pruebas de funcionalidad de los Tokens adquiridos, en los servidores que la Entidad designe.

Aceptamos y nos obligamos a cumplir las especificaciones técnicas establecidas por la entidad.

NOMBRE PROPONENTE: CAMERFIRMA COLOMBIA S.A.S

NIT PROPONENTE:

Firmado por Jose Fernando Medina el 31/08/2026 a las 08:47:42 COT

FIRMA DEL REPRESENTANTE LEGAL DEL PROPONENTE.

Nombre: JOSE FERNANDO MEDINA TOLOSA

Documento de identidad: CC 79.421.621