OBJETO DE LA CONTRATACIÓN: Adquisición de veinticinco (25) certificados digitales criptográficos tipo función pública, dos (2) certificados digitales (SSL) EV para los dominios www.chip.gov.co y www.contaduría.gov.co, y un (1) certificado digital (SSL) Wildcard OV para el subdominio *.contaduria.gov.co de la UAE Contaduría General de la Nación, con una vigencia de dos (2) años contados a partir de su instalación.

El proponente deberá conformar su propuesta de acuerdo con las siguientes especificaciones técnicas

Item	Requerimientos Mínimos Obligatorios	Cumple o No Cumple
1.	**ALCANCE**	
1.1.	Adquisición de veinticinco (25) certificados digitales criptográficos tipo función pública, dos (2) certificados digitales (SSL) EV para los dominios www.chip.gov.co y www.contaduria.gov.co, y un (1) certificado digital (SSL) Wildcard OV para el subdominio *.contaduria.gov.co de la UAE Contaduría General de la Nación, con una vigencia de dos (2) años contados a partir de su instalación.	
2.	**ESPECIFICACIÓN DE PRODUCTO Y/O SERVICIO CERTIFICADOS DIGITALES.**	
2.1.	**Veinticinco (25) certificados a utilizar en el SIIF Nación II** Para garantizar la compatibilidad con el aplicativo SIIF Nación II, los certificados deben cumplir estrictamente con los siguientes estándares:	
2.2.	**Estándar:** Los certificados deberán cumplir con el estándar UIT X.509 versión 3 (X.509 V3) en la modalidad de token virtual.	
2.3.	**Algoritmo de firma:** Algoritmo de firma: SHA-256 o superiores, que sean compatibles con SIIF Nación II, de conformidad con la Circular Externa No. 014 del 28 de marzo de 2025, donde se especifica que los	

Item	Requerimientos Mínimos Obligatorios	Cumple o No Cumple
	certificados digitales deberán ser expedidos por una Entidad de Certificación Digital Abierta acreditada por el Organismo Nacional de Acreditación de Colombia (ONAC) y homologada por la Administración del SIIF Nación para su utilización en el aplicativo SIIF Nación II,	
2.4	**Sistemas operativos compatibles:** Microsoft Windows 11, Windows 10 con soporte extendido, macOS soportado por Apple.	
2.5	**Compatibilidad: La solución deberá garantizar compatibilidad con SIIF Nación II y los componentes requeridos para su correcta operación.**	
2.6	**Mecanismo de almacenamiento seguro de claves:** los certificados podrán ser suministrados mediante token Virtual, certificado digital de software o servidor seguro tipo HSM, siempre que garanticen compatibilidad con SIIF Nación II y niveles adecuados de seguridad.	
2.7	**Entrega:** de PIN, credenciales de acceso, software, manuales técnicos y demás componentes necesarios para la instalación, configuración y operación de los certificados	
2.8	**Servicio de consulta CRL** (Lista de Certificados Revocados) con disponibilidad 7x24x365 vía web.	
2.9	**Soporte técnico:** durante la vigencia del certificado, mediante atención telefónica, correo electrónico y portal web (incluyendo chat, documentación técnica y preguntas frecuentes).	
2.10	**Notificación**: al usuario con al menos un (1) mes de anticipación al vencimiento del certificado digital, así como herramientas para la gestión de vigencias, emisión y uso de los certificados.	
3.	**ESPECIFICACIÓN DE PRODUCTO Y/O SERVICIO CERTIFICADOS DIGITALES (SSL)**	

Item	Requerimientos Mínimos Obligatorios	Cumple o No Cumple
3.1	El proponente deberá ofertar a la U.A.E. Contaduría General de la Nación los certificados digitales para los dominios www.chip.gov.co, www.contaduría.gov.co y subdominios *.contaduria.gov.co, por el término de dos (2) años, a partir de su instalación.	
3.2.	Los certificados SSL/TLS OV y EV deberán ser certificados públicos X.509 v3, emitidos por una Autoridad de Certificación confiable y reconocida por los principales navegadores y sistemas operativos. Deberán cumplir los Baseline Requirements del CA/Browser Forum y, para certificados EV, las EV Guidelines vigentes. Los certificados deberán soportar autenticación de servidor TLS mediante serverAuth, utilizar algoritmos criptográficos seguros, firma SHA-256 o superior, llaves RSA de mínimo 2048 bits o ECC equivalente, incluir los nombres DNS protegidos en la extensión Subject Alternative Name — SAN — y suministrarse con la cadena de certificación completa. La solución deberá ser compatible con configuraciones de servidor bajo TLS 1.2 y TLS 1.3, y no deberá requerir el uso de protocolos obsoletos como SSL 2.0, SSL 3.0, TLS 1.0 o TLS 1.1. Teniendo en cuenta la reducción progresiva de la vigencia máxima de certificados TLS públicos, el proveedor deberá garantizar durante el plazo contractual la emisión, renovación y reemisión de los certificados requeridos sin sin afectar la continuidad del servicio, conforme a los límites de vigencia definidos por el CA/Browser Forum. Así mismo, cuando la entidad por necesidad técnica, operativa, o de seguridad requiera realizar un cambio en los sitios que implique ajuste en el certificado, el proveedor deberá garantizar durante el plazo contractual la emisión, renovación y reemisión de los certificados requeridos sin sin afectar la continuidad del servicio.	

<table>
<tr><th>Item</th><th>Requerimientos Mínimos Obligatorios</th><th>Cumple o No Cumple</th></tr>
<tr><td></td><td>Los certificados deben cumplir con la normatividad, estándares y lineamientos vigentes aplicables, incluyendo las disposiciones que emita el CA/Browser Forum respecto a los períodos máximos de validez de los certificados digitales.</td><td></td></tr>
<tr><td>3.3.</td><td>Formatos de entrega

El proveedor deberá entregar los certificados en formatos estándar, de acuerdo con la necesidad técnica de la entidad, se presentan algunos de los formatos requeridos, sin embargo, se puede requerir otro formato.

<table>
<tr><th>Formato</th><th>Uso</th></tr>
<tr><td>PEM .crt, .cer, .pem</td><td>Servidores Apache, Nginx, Linux, balanceadores, appliances.</td></tr>
<tr><td>P7B / PKCS#7 .p7b</td><td>Entrega de cadena de certificación.</td></tr>
<tr><td>PFX / PKCS#12 .pfx, .p12</td><td>Plataformas Windows/IIS, cuando la entidad lo requiera.</td></tr>
<tr><td>Intermedios</td><td>Certificados intermedios de la CA.</td></tr>
<tr><td>Root CA</td><td>Certificado raíz de referencia, si aplica.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Item</th><th>Requerimientos Mínimos Obligatorios</th><th>Cumple o No Cumple</th></tr>
<tr><td></td><td><table><tr><td>Bundle completo</td><td>Archivo con cadena completa para instalación.</td></tr></table></td><td></td></tr>
<tr><td>3.4.</td><td>Certificados requeridos<table><tr><th>Tipo</th><th>Característica mínima</th></tr><tr><td>Certificado SSL/TLS OV</td><td>Certificado con validación de organización. Debe identificar la entidad titular y permitir protección TLS para dominios institucionales.</td></tr><tr><td>Certificado SSL/TLS EV</td><td>Certificado con validación extendida de la organización, sujeto a verificación reforzada de identidad, existencia legal y autorización. Debe cumplir las EV Guidelines del CA/Browser Forum.</td></tr><tr><td>Certificado Single Domain</td><td>Debe cubrir un FQDN específico, por ejemplo www.entidad.gov.co.</td></tr><tr><td>Certificado Multi-Domain / SAN</td><td>Debe permitir incluir varios nombres DNS en el campo Subject Alternative Name.</td></tr><tr><td>Certificado Wildcard OV</td><td>Debe permitir proteger subdominios de un dominio, por ejemplo *.dominio.gov.co, cuando se requiera.</td></tr></table></td><td></td></tr>
</table>

<table>
<tr><th>Item</th><th>Requerimientos Mínimos Obligatorios</th><th>Cumple o No Cumple</th></tr>
<tr><td>3.5.</td><td>Compatibilidad requerida

El proveedor deberá garantizar que los certificados emitidos sean reconocidos como confiables por los principales navegadores y sistemas operativos, siempre que estos se encuentren actualizados y soportados por sus fabricantes.

<table>
<tr><th>Componente</th><th>Compatibilidad mínima requerida</th></tr>
<tr><td>Navegadores</td><td>Google Chrome, Microsoft Edge, Mozilla Firefox y Apple Safari en versiones vigentes.</td></tr>
<tr><td>Sistemas operativos de escritorio</td><td>Microsoft Windows 11, Windows 10 con soporte extendido, macOS soportado por Apple y distribuciones Linux actualizadas.</td></tr>
<tr><td>Sistemas móviles</td><td>Android, iOS e iPadOS en versiones soportadas.</td></tr>
<tr><td>Almacenes de confianza</td><td>La cadena del certificado debe estar anclada en una CA raíz incluida en los programas de confianza de Google Chrome, Microsoft, Apple y Mozilla. Chrome, Microsoft, Apple y Mozilla mantienen programas/listas de raíces confiables para validar certificados TLS públicos.</td></tr>
</table>
</td><td></td></tr>
<tr><td>3.6</td><td>Requisitos criptográficos mínimos

<table>
<tr><th>Característica</th><th>Requisito técnico</th></tr>
</table>
</td><td></td></tr>
</table>

Item	Requerimientos Mínimos Obligatorios		Cumple o No Cumple
	Estándar del certificado	X.509 versión 3.	
	Algoritmo de firma	SHA-256 o superior. No se aceptarán certificados firmados con SHA-1, MD5 u otros algoritmos obsoletos.	
	Llave RSA	Mínimo RSA 2048 bits. Recomendado RSA 3072 o RSA 4096 cuando sea compatible con la plataforma.	
	Uso de clave	Debe incluir usos compatibles con autenticación de servidor TLS.	
	Extended Key Usage	Debe incluir serverAuth. No debe emitirse con usos ajenos al propósito de servidor web, salvo justificación técnica expresa.	
	SAN	Debe incluir obligatoriamente los nombres DNS protegidos en Subject Alternative Name.	
	CN	El Common Name no reemplaza el SAN. Los dominios deben declararse en SAN.	
	Cadena de certificación	El proveedor deberá entregar certificado de servidor, certificados	

<table>
<tr><th>Item</th><th>Requerimientos Mínimos Obligatorios</th><th>Cumple o No Cumple</th></tr>
<tr><td></td><td><table><tr><td></td><td>intermedios y cadena completa en formatos estándar.</td></tr></table></td><td></td></tr>
<tr><td>3.4</td><td>Requisitos de soporte técnico<table><tr><th>Característica</th><th>Requisito</th></tr><tr><td>Soporte de emisión y reemisión</td><td>Acompañamiento en validación OV/EV, generación de CSR, revisión de SAN y emisión.</td></tr><tr><td>Soporte de renovación</td><td>Alertas de vencimiento y acompañamiento en renovación.</td></tr><tr><td>Soporte de incidentes</td><td>Atención ante errores de cadena, revocación, incompatibilidad de navegador o fallas de instalación.</td></tr><tr><td>Mesa de ayuda</td><td>Disponer de un canal formal de soporte, correo, portal o teléfono.</td></tr><tr><td>SLA</td><td>Definir tiempos máximos de atención para incidentes críticos, altos, medios y bajos.</td></tr><tr><td>Idioma</td><td>Soporte en español.</td></tr></table></td><td></td></tr>
<tr><td>3.5</td><td>Herramienta de administración de certificados

La Herramienta en la nube que entregue el proveedor para gestión y administración de los certificados debe: generar, certificados, cadena de certificación completa, certificados intermedios, evidencia del tipo</td><td></td></tr>
</table>

Item	Requerimientos Mínimos Obligatorios	Cumple o No Cumple
	de validación: OV o EV., fechas de emisión y vencimiento, dominios incluidos en SAN, algoritmo, tamaño de llave y huella digital del certificado. Registro, monitoreo e incidentes: Registro de eventos relacionados con certificados (emisión, renovación, revocación)	
3.6	**Documentación requerida** • Instrucciones de instalación • Procedimiento de renovación • Procedimiento de revocación • Garantía o responsabilidad del proveedor/CA.	
4.	**REQUERIMIENTOS TECNICOS**	
4.1	**Certificado Digital EV para el dominio www.chip.gov.co**	
4.1.1	El proponente deberá ofertar un certificado digital EV – Extended Validation para el dominio www.chip.gov.co por el término de dos (2) años a partir de su instalación.	
4.2	**Certificado Digital EV para el dominio www.contaduria.gov.co**	
4.2.1	El proponente deberá ofertar un certificado digital EV – Extended Validation para el dominio www.contaduria.gov.co por el término de dos (2) años a partir de su instalación.	
4.3	**Certificado Digital Wildcard OV para los subdominios *.contaduria.gov.co**	
4.3.1	El proponente deberá ofertar un certificado digital Wildcard OV para los subdominios *.contaduria.gov.co por el término de dos (2) años a partir de su instalación.	

Item	Requerimientos Mínimos Obligatorios	Cumple o No Cumple

5	**ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA DE PRODUCTO Y/O SERVICIO ISO 27001**	
5.1	El proveedor debe cumplir con los requerimientos establecidos en la política de seguridad informática de la Contaduría General de la Nación.	
5.2	El contratista debe garantizar, mediante documento anexo al contrato, y firmado por el representante legal de la empresa, estricta confidencialidad acerca de la información o demás activos propiedad de la U.A.E. Contaduría General de la Nación.	
5.3	El presente anexo define los requisitos de seguridad de la información aplicables al servicio a contratar, en alineación con el SGSI institucional y la norma ISO/IEC 27001:2022, considerando la criticidad de los activos involucrados.	
5.4	El contratista deberá tener en cuenta:	
5.5	**Gestión de Identidades** Aplicar validación de identidad para emisión de certificados	

5.6	**Protección de claves privadas**
	• Las claves privadas deben:
	  ○ Generarse en entornos seguros
	  ○ Almacenarse cifradas
	  ○ Tener acceso restringido
	• Prohibido compartir claves privadas	

5.7	**Cumplimiento legal y normativo**
	• Cumplimiento de:
	  ○ Legislación colombiana (protección de datos – Ley 1581)
	  ○ Políticas de seguridad de la entidad
	  ○ Certificados deben ser compatibles con:
	  ○ Navegadores estándar
	  ○ Plataformas tecnológicas institucionales	

5.8	**Soporte Tecnico- Acuerdos de nivel de servicio** Debe ser de acuerdo con los siguientes acuerdos de nivel de servicio.	

1. El proponente deberá atender y resolver cualquier inquietud, solicitud e incidencia, en un esquema de atención 8*5 (telefónico, email, acceso remoto o presencial en caso de que así se requiera).

Para ello debe contar con un centro de servicio que cumpla con mínimo:

● Software de Mesa de Servicio del proponente donde se puedan registrar casos o incidentes de forma web, correo o teléfono relacionado con el alcance del objeto del contrato

Con el objetivo de garantizar la correcta prestación del servicio, se establecen una serie de acuerdos de nivel de servicio.

La gravedad de una incidencia, problema técnico o solicitud realizada a través de los canales como mesa de servicios o llamada telefónica se determinará asignando un grado de prioridad en base al siguiente criterio.

Gravedad	Descripción
Crítica	Se han dejado de proveer totalmente los servicios, ocasionando un impacto crítico en la actividad de la CGN.
Grave	Eventos que causan impacto, pero no interrupción del servicio.
Leve	Eventos con impacto limitado, consultas sobre configuraciones o cualquier pregunta que no requiere respuesta inmediata.

Los acuerdos de nivel de servicio exigidos acorde a la gravedad de las incidencias son los siguientes

	Gravedad de la incidencia Tiempo de respuesta Tiempo de resolución Horario de Atención Crítica <= 1 hora <= 4 horas 8x5 Grave <= 4 horas <= 16 horas 8x5 Leve Siguiente día hábil 2 x Siguiente día hábil 8x5	

Elaboro: (Ferney Cuestas Mahecha.)
REVISIÓN (Martha Patricia Zornosa Guerra)
APROBÓ (Anuar Edilson Vargas Calderon)