

DEPENDENCIA SOLICITANTE: DIRECCIÓN DE TECNOLOGÍAS E INFORMACIÓN

1. OBJETO DEL PROCESO

ADQUIRIR CERTIFICADOS DE FIRMA DIGITAL DE FUNCIONARIO PÚBLICO PARA LA FIRMA DE LOS DOCUMENTOS GENERADOS EN LA ENTIDAD POR LOS SISTEMAS DE INFORMACIÓN.

2. DESCRIPCIÓN DE LA NECESIDAD

La Dirección de Tecnologías e Información, como dependencia que articula todos los temas en materia de TIC (Tecnologías de la Información y las Comunicaciones), debe propender por suministrar y mantener soluciones que apoyen la gestión de información de los procesos misionales y de apoyo como insumo para la toma de decisiones, al igual que implementar y mantener mecanismos que permitan el intercambio de datos entre los sistemas de información de la entidad, a nivel interno y externo. Adicionalmente, dentro de sus actividades se encuentra la de garantizar el funcionamiento óptimo de los servicios tecnológicos que existen actualmente, desarrollados e implementados en la Entidad y fortalecer su funcionalidad teniendo en cuenta los requerimientos de los usuarios finales.

El fortalecimiento de la capacidad y gestión institucional de la Secretaría Distrital de Gobierno ha establecido orientaciones generales y protocolos que permitan la realización de trámites, prestación de servicios, entrega de información y respuesta a las quejas, reclamos y sugerencias de manera oportuna, eficiente y eficaz, garantizando una adecuada atención al ciudadano por los canales de atención existentes (presencial, virtual, escrito, buzón y telefónico).

El servicio al ciudadano se enmarca en los principios de información completa y clara, teniendo presente las necesidades, realidades y expectativas del ciudadano.

La Secretaría, los servidores públicos y los entes de control trabajan de manera coordinada para lograr dar cumplimiento a sus misionalidades y así tener un desarrollo de estrategias que permitan obtener resultados favorables de la gestión institucional garantizando la capacidad de la plataforma tecnológica de la Secretaría Distrital de Gobierno. Los principales participantes identificados son:

- Beneficiarios: Servidores públicos de la SDG, Ciudadanía.
- Cooperantes: SDG, Alcaldía Mayor, entes de control, MinTIC, DAFP.

El proceso de adquisición de certificados de firma digital busca garantizar el cumplimiento de forma efectiva de los procesos institucionales, seguridad de la información, transparencia y accesibilidad.

El literal C del artículo 2 de la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones), define la firma digital *“como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación”*.

En el marco del fortalecimiento de la infraestructura de confianza digital de la SDG, se requiere implementar mecanismos tecnológicos que garanticen la autenticidad, integridad, confidencialidad y no repudio de la información institucional, tanto en los procesos documentales como en los servicios digitales ofrecidos por la entidad.

Para tal fin, se identifica la necesidad de contratar el servicio de firmas digitales, los cuales constituyen componentes complementarios dentro de la arquitectura de seguridad de la información institucional y permiten asegurar la validez jurídica y la autenticidad de los documentos electrónicos generados y gestionados por la entidad, facilitando procesos administrativos y trámites digitales con plenas garantías de integridad y no repudio.

En este sentido, la contratación de este servicio responde a una estrategia integral de fortalecimiento de la infraestructura de confianza digital, orientada a mejorar los niveles de seguridad, confiabilidad y disponibilidad de los servicios digitales de la SDG.

3. DESCRIPCIÓN DEL BIEN O SERVICIO A CONTRATAR

CONDICIONES TÉCNICAS EXIGIDAS

Los productos a entregar para el presente proceso deben contar con las siguientes características técnicas:

Nombre del producto y/o servicio	Mecanismo de Firma Digital (Certificado de Titular de Función Pública)
-------------------------------------	---

Requerimientos generales	• Emitir y asignar 42 Certificados virtuales de firma digital de Titular de Función Pública compatible con el Sistema de Radicación ORFEO. • El plazo máximo de asignación y activación de la totalidad de los certificados digitales adquiridos será el plazo de ejecución del contrato, conforme a la programación acordada con el supervisor. • Firmado de documentos mediante el uso de servicios web. • Entregar los certificados de firma digital integrados con el sistema de información ORFEO y en funcionamiento. • Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la Ley 527 de 1999, y dar cumplimiento de los estándares vigentes RFC 5280 - internet X.509, ITU X-509 y lo establecido en el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014, los Criterios Específicos de Acreditación de Entidades de Certificación Digital del ONAC vigentes (CEA-3.0-07); y los reglamentos que los modifiquen o complementen. • Los Certificados de firma digital deben ser emitidos y activados en dispositivos criptográficos HSM (módulo de seguridad hardware) de la entidad certificadora.	
Vigencia	Dos (2) años a partir de la fecha de emisión del certificado.	
Reposición	La reposición es el mecanismo por el cual se emite un certificado digital a un usuario posterior a la revocación del certificado digital de un funcionario. Reposición del Certificado de firma digital emitido para la Entidad, se dará por los siguientes casos: • Pérdida del número de identificación personal (PIN) de acceso al certificado digital. • Compromiso de la llave privada. • Bloqueo del certificado digital. • Por renuncia o retiro del titular del certificado. • Por situaciones de carácter administrativo, como vacaciones o licencias del titular. En estos casos la Entidad Certificadora emitirá un nuevo Certificado de firma digital de Titular de Función Pública por el tiempo restante de su vigencia sin costo adicional para la Secretaría durante la vigencia del contrato. El término máximo para la renovación o reposición del certificado de firma digital será de dos (2) días hábiles contados a partir de la culminación satisfactoria del proceso de validación de identidad del nuevo titular. El contratista deberá habilitar y agendar dicha validación dentro del día hábil siguiente a la radicación de la solicitud en el sistema web de administración de certificados, de manera que el trámite integral no supere tres (3) días hábiles contados desde la radicación, salvo que la demora resulte imputable a la Entidad o al funcionario titular.	
Características técnicas del certificado	Se aclara que frente a cada ÍTEM (Requisito técnico) se debe cumplir con el estándar técnico y/o normativo mínimo indicado y descrito frente a cada característica.	
	<table> <tr> <td data-bbox="462 1638 682 1736">Algoritmo de firma</td><td data-bbox="682 1638 1430 1736"> • Función hash y RSA. • RSA 2048 o superior. • ECDSASHA-256 Tamaño de clave mínimo 2048 bits </td></tr> </table>	Algoritmo de firma
Algoritmo de firma	• Función hash y RSA. • RSA 2048 o superior. • ECDSASHA-256 Tamaño de clave mínimo 2048 bits	

	Contenido del Certificado Digital	• RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, o más recientes. • ITU-T Recommendation X.509 ISO/IEC 9594-8, Information technology - Open Systems Interconnection – The Directory: Public-key and attribute Certificate Frameworks. Los certificados deben cumplir con los requisitos exigidos en el artículo 35 de la Ley 527 de 1999 y demás normas que lo modifiquen, actualicen o deroguen y deben contener los requisitos del estándar ITU X-509 y como mínimo lo siguiente: • Nombre, cargo, dirección y domicilio del suscriptor. • Una Identificación única del suscriptor nombrado en el certificado. • Fecha de emisión y expiración del certificado.
	Ciclo de vida de los certificados	• RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.) • ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificate
	LDAP repositorio de certificados	• RFC 4523 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
	Generación de claves	• Los requisitos de seguridad deben ser de alto nivel de forma que generen confianza, además de cumplir con requisitos certificado FIPS 140-2 nivel 3 o superior.
	Formatos de Firma digital contemplados para el servicio	• Formato obligatorio – PAdES: ETSI TS (EN) 102 778 / EN 319 142 – PDF Advanced Electronic Signature Profiles, para los documentos PDF y PDF/A generados por la Entidad. • Formato obligatorio – CAdES: RFC 5126, RFC 5652 (Cryptographic Message Syntax – CMS) y ETSI TS 101 733 / EN 319 122, en sus modalidades adjunta o separada, para los demás tipos documentales. No se exigirá una extensión de archivo específica (.p7s, .p7m o .p7z), sino el cumplimiento del estándar y la posibilidad de verificar la firma con herramientas de validación de uso público. • Formato deseable – XAdES: W3C XML Advanced Electronic Signatures y ETSI TS (EN) 101 903 / EN 319 132. No será exigido como requisito habilitante y se mantendrá como capacidad deseable.

	Mecanismos de validación del estado del certificado - Lista de Certificados Revocados	• RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. • ITU-T Recommendation X.509 ISO/IEC 9594-8 Information technology – Open Systems Interconnection - The Directory: Public-key and attribute Certificate Frameworks. • CRL (Certificate Revocation List)
	Mecanismos de validación del estado del certificado - Servicio del estado del certificado en línea	• RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. • RFC 2560 Protocolo OCSP (Protocolo de Estado de Certificado en Línea). • X.509 Internet PKI Online Certificate Status Protocol – OCSP. • RFC 6960.

Nombre del producto y/o servicio	Mecanismo de Firma Digital
Requerimientos generales	• El proponente debe ser una Entidad de Certificación Digital acreditada por el Organismo Nacional de Acreditación de Colombia (ONAC), con acreditación vigente a la fecha de cierre del proceso y alcance para la emisión de certificados de firma digital de función pública en dispositivo centralizado (requisito habilitante, numeral 6.1.2.3). El contratista deberá mantener vigente dicha acreditación durante el plazo de ejecución del contrato y hasta el vencimiento de los certificados emitidos. • Suministro de cuarenta y dos (42) certificados virtuales de firma digital tipo función pública, para firmado de documentos mediante el uso de servicios web. • Certificados de firma digital de función pública, con componente criptográfico de firmado / API sobre HASH, para firmado digital de documentos vía webservice. • Integración de servicios de firma digital mediante webservice para múltiples aplicaciones de la Entidad, incluyendo el sistema de radicación, permitiendo la automatización del firmado de documentos a través de una interfaz centralizada que garantiza la autenticidad, integridad y no repudio de los registros procesados. • Vigencia de dos (2) años para los certificados de firma digital a partir de su emisión en los dispositivos y equipos que defina la Entidad. • Reemisión sin costo durante la vigencia del certificado cada vez que se cambie al responsable de certificado o que se tengan problemas técnicos en los equipos en los cuales fueron instalados. • Firma de Documentos PDF/A, PDF y cualquier otro documento. • Función hash y RSA. • RSA 2048 o superior. • SHA-256 Tamaño de clave mínimo 2048 bits. • El mecanismo de firma digital debe vincular la identidad del titular con el

	contenido del documento electrónico producido en la Entidad o por el sistema de radicación ORFEO, obteniendo un documento PDF o PDF/A íntegro y firmado digitalmente desde la plataforma del proveedor del servicio. • La plataforma del servicio debe contar con mecanismos que permitan realizar la trazabilidad de cada operación de firma. • La gestión de los certificados de firma digital debe realizarse desde la plataforma del proveedor del servicio. • Los servicios ofertados deberán contar con interfaces de programación (API) que permitan la integración con el sistema de radicación ORFEO y demás aplicaciones de la Entidad para el procesamiento de documentos electrónicos. • El proveedor del servicio debe entregar al supervisor del contrato un reporte mensual de consumo y uso del servicio de firma digital dentro de los primeros cinco (5) días hábiles de cada mes o proporcionar una disponibilidad de consulta en línea o servicio web.	
Vigencia	Los certificados de firma digital tendrán una vigencia de dos (2) años contados a partir de la fecha de emisión de cada certificado. Las operaciones de firma asociadas a cada certificado no estarán sujetas a bolsa, cupo o límite de transacciones; el oferente deberá cotizar el certificado con operaciones de firma ilimitadas durante su vigencia y, en caso de que su modelo comercial contemple algún límite, deberá indicarlo expresamente en su cotización. Volumen estimado de referencia: para efectos exclusivos del dimensionamiento técnico, la Entidad estima un volumen aproximado de cuarenta y nueve mil (49.000) documentos firmados mensualmente a través del sistema ORFEO, distribuidos entre los cincuenta (50) titulares —promedio de novecientos ochenta (980) documentos mensuales por titular—, equivalentes a aproximadamente un millón ciento setenta y seis mil (1.176.000) operaciones de firma durante los veinticuatro (24) meses de vigencia. Se trata de una cifra estimada y de referencia que no constituye compromiso de consumo mínimo ni máximo.	
Características técnicas	Se aclara que frente a cada ÍTEM (Requisito técnico) se debe cumplir con el estándar técnico y/o normativo mínimo indicado y descrito frente a cada requisito.	
	Sistema operativo	Compatible con los sistemas operativos MacOS versión 14 y superiores, Windows 10 con soporte extendido del fabricante (LTSC o LTSCB), Windows 11 y/o superior.
	Acceso a la plataforma	La plataforma o portal de administración, consulta y firma del servicio debe ser accesible de manera responsiva desde navegadores web estándar (Google Chrome, Microsoft Edge, Mozilla Firefox y Safari, en sus versiones vigentes con soporte del fabricante), tanto en equipos de escritorio como en dispositivos móviles, con independencia de su sistema operativo base.
Nombre del producto y/o servicio	Servicios conexos Soporte en la implementación	

Soporte técnico	• Resolver los problemas técnicos que surjan en la generación o emisión, activación, implementación y utilización de los productos y servicios adquiridos por la Entidad y prestar soporte técnico durante el término de vigencia de los certificados emitidos. El servicio de soporte será, como mínimo de lunes a viernes de 8:00 a 18:00 horas. • Niveles de servicio: los requerimientos se atenderán dentro de los siguientes tiempos máximos, contados desde su registro en cualquiera de los canales de atención: (i) prioridad alta —imposibilidad de firmar o indisponibilidad de la plataforma o de los servicios de validación OCSP/CRL—: respuesta en dos (2) horas y solución en ocho (8) horas hábiles; (ii) prioridad media —fallas que afecten a uno o varios titulares sin interrumpir el servicio—: respuesta en cuatro (4) horas hábiles y solución en dos (2) días hábiles; (iii) prioridad baja —consultas y solicitudes de información—: respuesta y solución en tres (3) días hábiles. La revocación por compromiso de la llave privada se atenderá de inmediato a través del canal 7x24x365. El supervisor verificará el cumplimiento de estos tiempos con el historial de requerimientos. • Contar con un sistema web de administración de cupo de certificados de firmas digitales a través de la cual el funcionario designado por la Entidad pueda llevar a cabo la gestión y control del cupo. El módulo debe permitir: • Radicar las solicitudes de emisión de los certificados digitales y hacer el cargue de los documentos soporte. • Visualizar las aprobaciones de solicitudes de emisión de certificados. • Solicitar revocación, reposición y reasignación de certificado digital. • Realizar seguimiento a la emisión y asignación de certificados digitales. • Controlar la cantidad de certificados digitales emitidos, activados, revocados, vigentes. • Consultar la trazabilidad del proceso de emisión y entrega de certificados. • Proveer el servicio de revocación de los certificados a través de una línea de atención a nivel nacional o servicio web con disponibilidad 7X24X365. • Contar con un centro de servicio que permita la atención y recepción de los requerimientos de la Entidad a través de: • Número telefónico de atención en Bogotá D.C. o línea telefónica con atributo de llamada local desde ciudad de Bogotá D.C. que cuente con un esquema de mesa de ayuda para la atención y solución de los requerimientos técnicos. • Chat en línea. • Correo electrónico. • Todo requerimiento o solicitud de soporte debe tener historial, desde su registro hasta la solución definitiva.
Instalación, configuración y puesta en funcionamiento de la suscripción del	• Facilitar la instalación y configuración de todos los componentes necesarios de software y el acompañamiento de los especialistas del proveedor. • Garantizar el correcto funcionamiento de las firmas con el Sistema de Radicación ORFEO.

servicio de firmas de funcionario público modalidad SaaS	• El servicio de integración del Sistema de Radicación ORFEO de la Entidad con la plataforma del proveedor del servicio de firma digital se hará mediante interfaces de programación de aplicaciones que se ajusten a los límites de la arquitectura REST. • El proveedor deberá exponer, documentar y mantener disponibles los servicios web y las interfaces de programación (API REST) requeridas para la integración; entregar la documentación técnica de los mismos — especificación de métodos, esquemas de autenticación, códigos de error y ejemplos de consumo—; disponer de un ambiente de pruebas con las credenciales necesarias para la Entidad; y prestar el acompañamiento y soporte técnico requeridos durante las fases de pruebas, integración y puesta en producción, sin costo adicional para la Entidad. Los desarrollos, adecuaciones o configuraciones que deban efectuarse sobre el Sistema de Radicación ORFEO y demás sistemas de información de la Entidad estarán a cargo de la Secretaría Distrital de Gobierno, por tratarse de sistemas de su propiedad. • El contratista apoyará las actividades técnicas necesarias durante el proceso de transición de cambio de proveedor que se da por terminación del contrato e inicio de uno nuevo con un posible nuevo proveedor, lo anterior con el fin de mitigar cualquier riesgo de que la Entidad quede descubierto del servicio y esto afecta la operación. • En la actividad de transición el contratista debe mantener la disponibilidad de acceder a un certificado válido, este proceso puede tardar hasta el vencimiento de los certificados activos.
---	--

4. CLASIFICADOR DE BIENES Y SERVICIOS

El objeto del proceso está codificado en la clasificación que se describe a continuación:

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
43233201	43000000 – Difusión de Tecnologías de Información y Telecomunicaciones	43230000 - Software	43233200 - Software de Seguridad y Protección	43233201 - Software de Servidor de Autenticación

5. OBLIGACIONES ESPECÍFICAS

1. Establecer durante los primeros cinco (5) días hábiles de ejecución del contrato, en coordinación con el Supervisor de este, la programación de las actividades necesarias para la entrega, implementación y puesta en funcionamiento de los certificados digitales, de conformidad con los plazos y condiciones establecidos en la ficha técnica y demás documentos del proceso.
2. Entregar los certificados digitales en los tiempos establecidos en los documentos del proceso de conformidad con las cantidades definidas por la Entidad.
3. Cumplir con las fichas técnicas de los servicios prestados.
4. Realizar el cobro de los servicios prestados de acuerdo con las disposiciones definidas por la Entidad.
5. Abstenerse de utilizar la información entregada por la Entidad para cualquier fin distinto a la ejecución del contrato.
6. Cumplir con la legislación colombiana y a la normativa aplicable en la materia.
7. Suministrar el servicio objeto de adquisición en las cantidades y calidades acordadas con su implementación de acuerdo con los tiempos establecidos en el cronograma de trabajo.
8. Cumplir con la vigencia de los certificados requerida.
9. Mantener vigente la acreditación como Entidad de Certificación Digital ante el ONAC, con el alcance exigido, durante el plazo de ejecución del contrato y hasta el vencimiento de los certificados emitidos, e informar al supervisor, dentro de los dos (2) días hábiles siguientes, cualquier suspensión, reducción de alcance o retiro de la acreditación.
10. Ofrecer el acompañamiento por personal especializado en la implementación de los certificados digitales.
11. Garantizar el correcto funcionamiento de la operación de los componentes de hardware y software, en el momento de la integración de su plataforma con el sistema de radicación Orfeo de la Secretaría Distrital de Gobierno, sin que ello pueda incurrir en costos adicionales.
12. Brindar soporte técnico de acuerdo con lo establecido en la ficha técnica, dentro de los niveles de servicio allí previstos.
13. Proporcionar la transferencia de conocimiento de la integración de su plataforma con el sistema de radicación Orfeo.

6. PLAZO DE EJECUCIÓN

El plazo del contrato será de dos (2) meses, contado a partir de la fecha del acta de inicio, suscrita entre el supervisor del contrato designado por la SECRETARÍA DISTRITAL DE GOBIERNO Y EL CONTRATISTA, previo cumplimiento de los requisitos de ejecución.