OBJETO DE LA CONTRATACIÓN

Suministro, instalación y puesta en funcionamiento para firmar digitalmente documentos electrónicos de forma automática, individual y masiva del Departamento Administrativo Nacional de Estadística - DANE.

FICHA TÉCNICA – CONDICIONES CARACTERISTICAS TÉCNICAS

Certificado Virtual de Firma Digital Función Publica		
1	**Cantidad**	250 certificados virtuales de firma digital función pública.
2	**Descripción**	El certificado de Función Pública acredita su identidad y su condición como funcionario público o de particular en ejercicio de una función pública, y le permite firmar digitalmente sus documentos en la calidad que acredita su certificado de firma digital.
3	**Vigencia**	Los certificados deben tener una duración de 1 año a partir de la emisión del certificado virtual de firma digital
4	**Tipo**	Firma virtual digital Función pública
5	**Compatibilidad con sistemas operativos**	Garantizar que el certificado virtual de firma digital es compatible con mínimo sistemas operativos Windows, versiones Win10 y posteriores de 64 bits y sistemas operativos macOS mediante una aplicación de escritorio.
6	**Compatibilidad con estándares de seguridad**	Garantizar que el certificado virtual de firma digital es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) 7 ó superior.
7	**Autenticidad, Integridad y No Repudio**	Mecanismo de autenticación basado en el protocolo OAuth2 para la autenticación del usuario al momento de realizar la firma en el documento, que garantice la gestión segura de credenciales dentro del entorno del proveedor autorizado, impidiendo su manipulación externa. Este método debe asegurar la identidad del usuario, preservar la integridad de las transacciones y proporcionar trazabilidad confiable para efectos de no repudio.
8	**Características de centralización**	El certificado digital debe implementarse bajo un esquema de centralización en nube utilizando un token virtual. Estos certificados de firma digital deben se almacenarse de manera segura en un servicio en la nube, gestionado por la Entidad de Certificación Digital (ECD) debidamente acreditada.
9	**Firma digital función publica**	Garantizar que la Firma digital función pública permita acreditar la calidad de funcionario Público del DANE y en el marco de sus funciones firmar digitalmente de forma individual mensajes de datos y/o documentos en todos los formatos, PDF, WORD, XLSX, entre otros.
10	**Llaves criptográficas**	El tamaño de la llave de los certificados digitales de Función Pública debe ser de 2048 bits o tamaño superior con base en tecnología PKI (Public Key Infrastructure). El tamaño de las llaves certificadas de la CA (Certificate Authority), emisora de los certificados digitales de Función Pública debe ser de 4096 bits con base en tecnología PKI.
11	**Estándares criptográficos**	Cumplimiento de estándares criptográficos: El certificado debe cumplir con los más altos estándares de encriptación y seguridad informática (Entre otros RSA con longitud de 2048 Bits o superior, SHA-256).

12	**Consideraciones de reemisión**	Garantizar el derecho a una (1) reposición gratis del certificado digital dentro de los diez (10) meses posteriores a su emisión o hasta dos (2) meses antes de su vencimiento. La reposición se realizará por el tiempo restante de la vigencia original del certificado digital en los siguientes casos:
		1. Cambio de titular (el DANE cambia al funcionario Autorizado).
		2. Cambio de cargo y/o política (Institucionales legales).
		3. La reposición gratuita de cada firma digital aplicará de acuerdo con las necesidades de la entidad durante la vigencia de los certificados digitales
13	**Doble Factor de autenticación**	Implementación de mecanismos de autenticación robusta, que incluyan el uso de contraseñas y doble factor de autenticación, establecido como requisito obligatorio para todos los usuarios de la entidad que realizan procesos de firma de documentos.
14	**Custodia**	El proveedor será responsable de la administración y custodia de los certificados de firma digital, los cuales deberán ser entregados a la Entidad conforme a sus requerimientos. Esta administración y custodia incluirá la emisión, modificación, revocación y cualquier otra gestión necesaria para el uso adecuado de los certificados durante el período de un (1) año, correspondiente a su vigencia.
15	**Confidencialidad**	Mantener de manera permanente la confidencialidad sobre toda la información a la que se tenga acceso en el marco de la ejecución del contrato, obligación que permanecerá vigente incluso después de su terminación, liquidación o declaratoria de caducidad.
16	**Software de firmado**	El contratista debe suministrar una herramienta de gestión de firmado (Software para los equipos autorizados) que permita enviar, firmar y, almacenar documentos de manera electrónica en todos los formatos, que garantice su integridad y autenticidad mediante criptografía.
17	**Documentos Ilimitados**	Los usuarios pueden realizar firmas ilimitadas de documentos durante la vigencia del certificado. No habrá restricción de documentos a certificar por cada usuario.
18	**Atributo visual**	El certificado de firma digital deberá contar con una representación visual que permita su interpretación por parte de usuarios finales, con los siguientes atributos mínimos: Nombres y apellidos completos del titular, Correo electrónico asociado al certificado, Cargo o rol si aplica y en las propiedades de la firma: validez, fecha y hora en que ocurre la firma. Perfil PAdES (PDF Advanced Electronic Signatures)
19	**Revocación**	Posibilidad de revocar el certificado digital en caso de necesidad de la Entidad.
20	**Soporte técnico**	El contratista deberá prestar asistencia en la instalación, configuración y soporte de incidentes reportados por la entidad.
		Para corregir los incidentes reportados el Contratista deberá analizar la falla, identificar la causa, implementar mecanismos de corrección de errores y restaurar la disponibilidad del certificado digital durante toda su vigencia.

		Una vez emitido el certificado de firma digital, el contratista deberá garantizar la prestación del servicio de soporte durante toda su vigencia (un año), incluyendo la asistencia en la instalación, configuración y atención de incidentes en los equipos destinados para dicho propósito. Para ello, deberá disponer de un esquema de atención 5x10 (cinco días a la semana, diez horas al día), con un tiempo máximo de solución para incidentes mediante soporte remoto de dos (2) horas, contadas a partir del momento de su reporte.
		El tiempo de atención comenzará a contarse a partir del momento en que se realice la solicitud, siendo válidos como evidencia la fecha y hora de generación del número de servicio asignado, la fecha y hora de la llamada telefónica, o la fecha y hora del envío del correo electrónico, según el canal utilizado
		En caso de ser necesario, la Entidad determinará la modalidad de acceso o asistencia remota para el contratista de acuerdo con la infraestructura vigente en tecnología, seguridad y acceso en el DANE, la cual le será comunicada oportunamente al contratista. Si la falla no puede resolverse a través de esta modalidad remota, el contratista deberá asignar el personal necesario para solucionar dicha falla técnica en las instalaciones de la Entidad
		Por cada incidente atendido, el contratista debe generar un informe para la Entidad donde especifique la causa de la falla y la solución implementada; informe que deberá ser entregado a más tardar al quinto (5) día de culminación de las actividades ejecutadas con ocasión del reporte del incidente.
		El contratista deberá disponer de canales de soporte accesibles para la Entidad, tales como una plataforma web para el registro de casos, Mensajería instantánea, línea telefónica y correo electrónico, que permitan garantizar la trazabilidad de los requerimientos o incidentes reportados
21	**Certificación ONAC**	El contratista debe contar con Certificación expedida por el Organismo Nacional de Acreditación de Colombia - ONAC en la que conste que el mismo, como entidad certificadora abierta, está autorizado para expedir certificados digitales de función pública
22	**Costos adicionales**	Las actividades de activación, instalación, configuración y soporte están incluidas dentro del valor contratado, por lo tanto, no generarán costos adicionales para la Entidad.
23	**Transferencia de conocimiento**	El proveedor deberá realizar una jornada de transferencia de conocimiento, con una duración mínima de cuatro (4) horas, la cual podrá desarrollarse de manera virtual y deberá abordar el uso de los certificados de firma digital, así como la resolución de problemas asociados. Esta jornada deberá tener el alcance que la Entidad determine, incluyendo a los funcionarios o colaboradores que lo requieran.
24	**Auditoria**	La plataforma centralizada que administra las firmas digitales deberá contar con funcionalidades de auditoría, trazabilidad y generación de reportes sobre las firmas realizadas. En este sentido, cada acción de firma digital deberá quedar registrada en bitácoras seguras, incluyendo como mínimo información del usuario firmante, certificado utilizado, fecha y hora. Estos registros deberán ser inalterables y permitir su consulta y exportación para efectos de control interno y auditoría, garantizando la trazabilidad completa del proceso de firma.