Función Pública

LINEAMIENTOS PARA EL USO DE FIRMA DIGITAL

Proceso Gestión Documental

Versión 02
Enero 2025

Función Pública

Tabla de contenido

1. Objetivo

Determinar los lineamientos y pautas que permitan establecer el uso de la firma digital en las comunicaciones oficiales producidas por el Departamento Administrativo de la Función Pública.

2. Generalidades

Los certificados digitales son documentos digitales emitidos a una persona natural o jurídica, que contiene datos propios de la persona o empresa, que son validados por quien emite el certificado. En Colombia, la emisión del certificado digital está bajo la responsabilidad de una entidad de certificación debidamente acreditada por el Organismo Nacional de Acreditación de Colombia - ONAC (Ley 527 art. 29-34, Decreto 333 de 2014 art. 7). Así mismo, en dicha ley se establece el reconocimiento jurídico de los mensajes de datos y de la firma digital[1], teniendo la firma digital la misma fuerza y efectos que el uso de una firma manuscrita (Ley 527 art. 28).

El Departamento Administrativo de la Función Pública ha implementado el uso de la firma digital para la emisión de algunos documentos, comprometidos con la optimización y racionalización de trámites en la administración pública

En este documento se establecen los parámetros generales para la adquisición, administración, actualización y uso de las firmas adoptadas por la entidad dentro de la gestión documental institucional, convirtiéndose en un instrumento de apoyo, guía, orientación y consulta para los servidores autorizados para firmar las comunicaciones oficiales según lo establecido en la Guía para la elaboración o actualización de documentos

3. Glosario

Certificado en relación con las firmas: Mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide como al suscriptor, y contiene la clave pública de éste.

Certificado digital: Permite firmar documentos electrónicos digitalmente otorgándole al documento los atributos jurídicos contemplados en la ley para los mensajes de datos: autenticidad, integridad, fiabilidad y no repudio.

[1] La ley 527 de 1999, define en el artículo 2 numeral c), Firma digital: Se entenderá 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.

Comunicaciones Oficiales: Son todas aquellas recibidas o producidas en desarrollo de las funciones asignadas legalmente a una entidad, independientemente del medio utilizado para su creación o comunicación.

Correo electrónico certificado: Servicio que proporciona notificaciones electrónicas de los correos electrónicos enviados, con el cual se testifica su envío, entrega y lectura. Dicho servicio genera un registro de notificación, un acuse de recibo que es enviado automáticamente por email al remitente original en forma rápida, oportuna y segura, y que incluye fecha/hora oficial del envío, la entrega y el contenido transmitido, evidencia digital disponible de inmediato tanto para el remitente como para la Entidad.

Documento: Información registrada, cualquiera que sea su forma o el medio utilizado.

Documento electrónico de archivo: Es el registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

Entidad de Certificación: Es aquella persona, autorizada conforme a la Ley 527 de 1999, que está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Estampado cronológico: Es una estampa de tiempo que permite garantizar la existencia de un mensaje de datos, el instante de su creación, modificación y suscripción, por ende, lo vincula a un período de tiempo concreto evitando su alteración.

Firma Digital: Se entenderá 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.

Firma Mecánica: Consiste en una firma digitalizada implementada en el Sistema de Gestión Documental ORFEO, que bajo los parámetros de seguridad del sistema vincula a un suscriptor lo cual garantiza la identidad del firmante, la autenticidad y el no repudio del documento.

Firmas Masivas: Son aquellas agrupaciones de documentos o comunicaciones que por su volumen requieren ser suscritas en bloque a través de la firma mecánica o digital según sea el caso, implementadas en el Sistema de Gestión Documental Orfeo.

Mensaje de datos: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Radicación de comunicaciones oficiales: Es el procedimiento por medio del cual, las entidades asignan un número consecutivo, a las comunicaciones recibidas o producidas, dejando constancia de la fecha y hora de recibo o de envío, con el propósito de oficializar su trámite y cumplir con los términos de vencimiento que establezca la Ley. Estos términos, se empiezan a contar a partir del día siguiente de radicado el documento.

Token: Dispositivo de almacenamiento de certificados digitales (similar a una USB), utilizado para facilitar el proceso de autenticación de usuarios.

4. Normatividad

Normativa consultada:

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"

Acuerdo 60 de 2001. "Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas".

Decreto-Ley 19 de 2012 art.34 y art.160. "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

Decreto 333 de 2014. Por el cual se reglamenta el artículo 160 del Decreto-Ley 019 de 2012

Decreto que tiene por objeto "definir el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en el artículo 160 del Decreto ley 19 de 2012"

5. Consideraciones generales para la adquisición, activación y utilización de firma digital

- ✓ Para la adquisición y/o activación de los certificados de firma digital se debe tener en cuenta lo señalado en la Guía para la elaboración o actualización de documentos,

donde se establecen los cargos de la Función Pública, autorizados para la firma de las comunicaciones oficiales producidas por la Entidad según el destinatario y el contenido.

- ✓ El Grupo de Gestión Documental será el encargado de realizar los trámites correspondientes para la adquisición y/o activación de los certificados de firma digital.

- ✓ El Grupo de Gestión Documental será el encargado de diligenciar el formato y recoger la firma mecánica (grafo manuscrito), el cual será incluido en el Sistema de Gestión Documental.

- ✓ El uso de la firma mecánica está dado como una representación visual de la firma manuscrita a los documentos firmados digitalmente, por ello no surte ningún efecto jurídico.

- ✓ El uso de la firma digital deberá ser para todas las comunicaciones emitidas como mensaje de datos (envío correo electrónico). Una vez firmadas digitalmente deberán conservarse en su estado electrónico para garantizar su validez. Aquellas que requieran enviarse físicamente serán impresas y enviadas a través de correo físico, y para verificar su validez se escaneará el código QR el cual direccionará al repositorio de evidencia digital de la Función Pública.

- ✓ No se requerirán copias para conformación de expedientes o para el consecutivo institucional para el caso de los documentos suscritos con firma digital, ya que estos se asociarán al expediente electrónico correspondiente dentro del sistema de gestión documental.

- ✓ Los documentos deben elaborarse en los formatos establecidos en el SIG y dando cumplimiento a lo establecido en la Guía para la elaboración o actualización de documentos.

- ✓ Una vez firmados los documentos con firma digital se convertirán en formato PDF/A y podrán visualizarse en el Sistema de Gestión Documental.

- ✓ En caso de requerirse, se podrá solicitar al Grupo de Gestión Documental la anulación de los documentos suscritos con firma digital que no surtieron trámite, a través del módulo de anulación del Sistema de Gestión Documental, generando la respectiva acta de anulación

- ✓ Las comunicaciones firmadas digitalmente quedarán en la bandeja de envíos del Sistema de Gestión Documental, para que se efectúe el envío respectivo a la dirección registrada en el destinatario.

- ✓ En el caso en el cual no pueda emplear la firma digital por alguna eventualidad, los documentos se firmarán de forma manuscritamente o autógrafa únicamente

5.1 Responsabilidades

5.1.1 Responsabilidad de quien firma el documento

- ✓ Recibir el token asignado por la Entidad certificadora para su administración y uso, siguiendo las instrucciones indicadas vía e-mail para la habilitación del mismo.

- ✓ Firmar el acta de los términos y condiciones de entrega del token suministrada por el Grupo de Gestión Documental

- ✓ El certificado digital emitido a nombre del usuario, el token criptográfico y su contraseña es de acceso personal y no debe ser transferida a terceros

- ✓ El usuario es responsable de solicitar a la Entidad certificadora a través del Grupo de Gestión Documental la revocación del certificado cuando deje de requerir su uso, en casos tales como: cuando se retire de la entidad, cuando se pierda, dañe o bloquee el token criptográfico, o por alguno de los motivos establecidos por la entidad de certificación.

- ✓ Devolver el token en caso de retiro definitivo de la Entidad o del cargo desempeñado al Grupo de Gestión Documental.
- ✓ Notificar con anterioridad a la fecha de caducidad del certificado digital, su renovación.

- ✓ En caso de daño o pérdida del token deberá efectuar el pago de éste para su reposición, y entregar el comprobante al Grupo de Gestión Documental para realizar los trámites ante la Entidad Certificadora

- ✓ Mantener bajo su custodia el token criptográfico, y no dejarlo conectado al computador cuando esté ausente

- ✓ Es responsabilidad de cada servidor, el uso y manejo adecuado que se le dé al token utilizado para firmar digitalmente, el cual solo podrá ser empelado para trámites exclusivos de la Función Pública

- ✓ Dar el visto bueno a través del Sistema de Gestión Documental a todas las comunicaciones oficiales generadas por los servidores que las proyectan, y que serán firmadas con su certificado digital

- ✓ Asegurarse que todas las comunicaciones a firmar han pasado por su visto bueno, y tienen el respectivo número de radicado generado por el Sistema de Gestión Documental

5.1.2 Responsabilidad del Grupo de Gestión Documental

- ✓ Solicitar los documentos necesarios al Grupo de Gestión Humana para el respectivo trámite de solicitud de emisión de certificados de firma digital: Fotocopia de la cédula al 150% legible en texto, documentos donde se certifique que la persona está vinculada a la entidad y se acredite el Cargo que desempeña actualmente.

- ✓ Realizar la solicitud de emisión de certificados digitales (token) de manera masiva o individual siguiendo las instrucciones de la Entidad Certificadora.

- ✓ Realizar la entrega de los certificados de firma digital en los casos requeridos.

- ✓ Solicitar mediante oficio las reposiciones de los certificados (token) en caso de retiro de los funcionarios asignados, realizando la devolución a la Entidad certificadora del token que se debe reponer.

- ✓ Realizar el seguimiento de las solicitudes de emisión, uso de los certificados y fechas de renovación de los mismos.

- ✓ Solicitar al administrador del Sistema de Gestión Documental la inclusión de la (s) firma (s) mecánicas que se requieran

- ✓ Realizar el seguimiento al saldo disponible de estampas de tiempo utilizadas para la firma digital y garantizar su disponibilidad, así como la de los token utilizados para el firmado digital.

- ✓ Realizar capacitaciones en el uso de los certificados de firma digital y firma mecánica adoptados por la Entidad

5.1.3 Responsabilidad del Grupo de Gestión Humana

- ✓ Realizar la entrega de la documentación requerida por el Grupo de Gestión Documental, de los servidores que dentro de sus funciones requieran la utilización de firma digital

- ✓ Informar al Grupo de Gestión Documental cuando se presente alguna novedad en el cambio de funciones o retiro definitivo del funcionario que cuente con certificado firma digital

5.1.4 Responsabilidad del Grupo de Gestión Administrativa (Soporte primer nivel)

- ✓ Realizar las configuraciones requeridas para el uso y administración de los certificados de Firma digital
- ✓ Prestar soporte técnico para configuración de usuarios en el aplicativo, y para la solución de fallas en el sistema cuando de estas firmas se trate.

5.2 Recomendaciones generales

- ✓ El proceso de firma digital se puede realizar en cualquier navegador, sin embargo, se recomienda utilizar Mozilla para el uso del Sistema de Gestión Documental
- ✓ Se debe mantener habilitada en la configuración del navegador la opción de ventanas emergentes, o al menos para el dominio del certificador
- ✓ Antes de firmar digitalmente transacciones en el Sistema de Gestión Documental, es necesario que el administrador del aplicativo haya instalado y configurado en su equipo (s) los componentes necesarios para el uso de la firma digital (Elogic Monitor y los drivers del token)
- ✓ Para firmar digitalmente debe asegurarse que el dispositivo criptográfico (token) esté conectado en el puerto USB del computador desde el cual va a ingresar, de lo contrario se presentarán fallas cuando intente ingresar al sistema.
- ✓ Tener instalado en el PC el programa Adobe Acrobat para verificar la validez de la firma luego de ser firmado el documento
- ✓ Para la validación de la firma, que en un principio registra “Desconocida”, se deben desplegar las propiedades de la firma, y cambiar la configuración de confianza, de tal manera que, al aceptar las configuraciones, cambiará a un estado de “Firma válida”

6. Proceso de firma digital

El proceso de firma digital se encuentra descrito en la Guía tutorial ORFEO publicada en el SIG