

En el marco de la III Asamblea Ordinaria del Consejo Federal, celebrada en la Ciudad de Buenos Aires, se brindó un Foro sobre Modernización y Firma Digital que estuvo a cargo de la Lic. Maria Paula Schiappapietra, de la Secretaría de Modernización del Estado, y los Nots. Néstor Lamber, Walter Schmidt y Martín Giralt Font y coordinado por el Secretario del CFNA Not. Diego Maximiliano Martí.

Modernización – Firma Digital – Trámites a distancia

Posicionamiento del Notariado.

El Foro tuvo como principal tema el de la implementación de la Firma Digital y las formas por las cuales los distintos actores de la sociedad civil pueden adentrarse en la era digital, resaltando especialmente el rol que el notariado debe cumplir en el proceso. Les acercamos un extracto de la información y documentación presentada por la expositora

Se entiende por Firma Digital, según lo establecido en el Artículo 2 de la Ley 25.506, al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Según el Artículo 9 de la citada norma, son requisitos para su validez y para que se presuma la autoría y la integridad de la firma digital: la vigencia del certificado digital válido del firmante, verificar que los datos del certificado sean correctos y que el certificado haya sido emitido por un certificador licenciado.

En este sentido respecto a LA AUTORÍA, se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital (Artículo 7, Ley 25.506).

En cuanto a la INTEGRIDAD, si la verificación de una firma digital aplicada a un documento digital es verdadera, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma (Artículo 8, Ley 25.506).

Cabe aclarar que cuando se habla de firma digital no nos estamos refiriendo ni a la FIRMA ELECTRÓNICA, que es un conjunto de datos electrónicos utilizados como identificación por el signatario, pero que carece de algunos de los requisitos de la firma digital, ni de FIRMA

OLÓGRAFA, que es la firma manual en soporte papel. La firma escaneada no es firma digital, como tampoco lo es la firma digital impresa.

En consecuencia, la firma digital es una firma personal cuyos efectos, salvo prueba en contramano y cada persona cuenta con una única firma utilizándola indistintamente para trámites personales y/o laborales.

Cuando una persona firma digitalmente en carácter profesional, para que su firma digital valga como tal no basta sólo con aplicarla, sino que deberá añadirse un sello dentro de un firmador con la acreditación del carácter invocado por quien esté autorizado a certificarlo (por ejemplo en el caso de ser notario, esta facultad corresponde a cada Colegio Notarial).

La firma digital puede utilizarse en trámites con entidades privadas y públicas, declaraciones impositivas y notificaciones judiciales, operaciones bancarias, contratos a distancia, documentos de comercio exterior, entre otros ejemplos.

Existen dos tipos de firma digital:

1. FIRMA DIGITAL POR TOKEN: así se firman documentos en cualquier aplicativo de firma con la utilización de un Token.

Para ello se requiere instalar drivers en la computadora desde donde se va a firmar.

La clave pública y privada se almacenan en el dispositivo USB Token, que se requiere para firmar. Las ventajas de ésta es que puede utilizarse en cualquier dispositivo que tenga instalados los programas, haya o no conexión a internet. La desventaja es que para instrumentarla se necesita necesariamente contar con un Token, lo que puede resultar oneroso.

2. FIRMA DIGITAL REMOTA: permite firman documentos desde una plataforma y sin Token. Se necesita contar solamente con un dispositivo móvil.

La clave pública se almacena en la Plataforma Digital Remota (PFDR) y sólo tiene validez con la Clave Privada, Pin y OTP (One Time Password) del suscriptor. Las



ventajas de ésta es que puede usarse desde cualquier dispositivo móvil, sin la utilización de Token, lo que facilita y abarata los costos de su implementación. La desventaja es que sólo puede usarse teniendo conectividad.

Para obtener la firma digital, debe contarse con un documento de identidad válido y presentarse ante la Oficina de Registro de AC (Autoridad Certificante) que corresponda, en donde se tomarán los datos biométricos del solicitante (foto y huella).

Si es firma digital con Token, el interesado deberá iniciar vía web en la página <https://pki.jgm.gov.ar> la solicitud del certificado. Una vez aceptada la misma, deberá acercarse con el Token y la solicitud impresa a la Oficina de Registro. El dispositivo Token debe ser FIPS 140-2 nivel 2 o superior y debe poder generar y almacenar pares de clave RSA de 2048 bits como mínimo.

Si es firma digital remota, para tramitarla el interesado debe solicitar un turno en <https://www.argentina.gob.ar/obtener-firma-digital-remota>, tener acceso a una cuenta de correo electrónico y poseer un teléfono inteligente que tenga una aplicación instalada para generar OTP, que sirve para autenticarse cada vez que se quiera firmar un documento.

Una vez obtenida la firma digital por el sistema de Token, podrá firmarse un documento digitalmente mediante la utilización del dispositivo en cualquier puerto USB de un ordenador que tenga los programas necesarios.

Si la firma es digital remota, se contará con Usuario y Contraseña, y se tendrá OTP y PIN listos para firmar cualquier documento.

Ingresando al sistema mediante la página <https://firmar.gob.ar>, debe completarse número de CUIT y Contraseña (Clave Privada). Luego debe ingresarse el OTP (obteniendo el código del dispositivo móvil), seleccio-

nar la autoridad de registro que haya otorgado la firma digital y subir el documento que se desea firmar en formato PDF, completando con número de PIN, luego de lo cual el mismo estará firmado.

Una vez hecho esto, se podrá previsualizar el documento firmado que en caso de ser correcto se descargará para disponerlo. La plataforma no guarda el documento.

Se entiende por validación de la firma digital el proceso por el cual se chequea que la firma esté efectivamente aplicada y que la misma sea válida.

¿CÓMO VALIDAR UNA FIRMA DIGITAL?

Tanto para verificar la firma digital por Token y la remota, se necesita instalar y configurar el programa Adobe Reader RC, por única vez, debiendo además instalar los certificados para validar la firma:

1. Certificado de confianza de la AC- Raíz que aplica a todas las firmas;
2. Certificado intermedio por cada AC (AC-Modernización-PDFR para firma digital remota o AC-ONTI para firma digital por Token).

FIRMA DIGITAL REMOTA:

Abierto el programa Adobe, debe seleccionarse la pluma, donde se abren las firmas del documento, y se indica por quién está firmado, el origen de los elementos de confianza, si la identidad del firmante es válida y la marca de hora incrustada (hora de la firma).

Cabe aclarar que mientras que en la firma digital remota la hora es la que indica el ordenador donde se aplica, en la firma por Token la hora la determina el dispositivo.



FIRMA DIGITAL POR TOKEN:

También se verifica con el uso del programa Adobe, seleccionando la pluma donde aparecerá quien firmó el documento y la fecha y hora de la firma.

DOCUMENTOS QUE SE AGREGAN POR FUERA DEL DOCUMENTO MADRE. INTERVENCIÓN NOTARIAL.

Cuando con posterioridad a la firma digital se agregan otros instrumentos, como sería el caso de la certificación de esa firma por parte de un escribano y el agregado de un folio de certificación, el procedimiento se denomina "embeido".

En este caso no se modifica ni interviene el documento madre, sino que se le agrega un nuevo documento, que puede ser de origen notarial.

Para realizarlo, el interviniente puede recurrir al sistema de firma digital remota o por Token y seguir los mismos procedimientos antedichos para firmar el documento madre. El embebido podrá visualizarse también en el Adobe como un archivo adjunto en el margen izquierdo utilizando el dibujo del clip o gancho.

¿CÓMO DETECTAR CUANDO UN DOCUMENTO FIRMADO DIGITALMENTE FUE ALTERADO POSTERIORMENTE?

Si con posterioridad a la firma digital el documento fue modificado o alterado, al visualizarlo en el programa Adobe la información ya no aparecerá en color verde, sino en color rojo.

CASO DE FIRMA DIGITAL NO VÁLIDA

Ocurre cuando firma el documento quien no está autorizado por ONTI (Oficina Nacional de Tecnologías de la Información).

En ese caso, en el programa Adobe la información puede leerse en color amarillo, por lo que deberá chequearse si los certificados están correctamente emitidos.

En caso de no encontrarse la persona habilitada por

ONTI para firmar digitalmente, la firma no será válida.

FIRMA DIGITAL CONJUNTA

En los casos en que un mismo instrumento es firmado digitalmente por dos o más personas en distintos momentos, la fecha que valdrá como del documento es la de la última firma.

En este caso, cada vez que una de las partes firma el documento, el mismo aparecerá como alterado y en color amarillo en el programa Adobe, para poder chequear en qué parte fue modificado.

Cabe aclarar que las firmas serán válidas cuando la GDE (Gestión Documental Electrónica) incorpore los datos de localidad, fecha y número una vez que todas las partes hayan firmado.

DOCUMENTO CON CON FOLIO DIGITAL

Consta del documento firmado por las partes más el folio o foja de certificación del notario. Estamos frente a un documento embebido.

En este caso, para firmar como notario, no basta con la sola firma digital del escribano (que sirve solamente como firma de la persona como particular) sino que se necesita además de la validación de la firma por parte del Colegio de Escribanos que certifique la calidad de notario de la persona de manera online. La firma en este caso lleva sello del Colegio.

Para ello, los Colegios Notariales deberían contar con plataformas firmadoras online que habiliten al escribano a ingresar y solicitar el certificado.

Los trámites con intervención notarial que requieren de firma digital ya están activos. Por lo que se invita a los notarios a registrar su firma y a los Colegios de Escribanos del país a facilitar el procedimiento de firma digital a sus colegiados para cumplir el requerimiento social en este sentido.

Finalizado el foro, continuó el debate entre los presentes.