TECNOLOGÍAS DE LA INFORMACIÓN. FIRMA DIGITAL
Dirección de Innovación Tecnológica - Oficina Nacional de Tecnologías de Información (ONTI)
Gestión

GERENCIA DE PLANIFICACIÓN Y PROYECTOS ESPECIALES
Departamento de Auditoría Informática

Normativa analizada / Marco normativo aplicable

Leyes. 25.506, de Firma Digital.
Decretos. 2628/02, 283/03, 1028/03.
Resoluciones. 227/10, de la Secretaría de la Gestión Pública.

Aclaraciones previas

Mientras el papel fue el soporte exclusivo de la documentación, el paradigma de la firma ológrafa (de puño y letra) se mantuvo inalterado, pero, con las nuevas tecnologías, resultó inadecuado para asegurar la validez de la información y su autoría. Para brindar seguridad y robustez, se desarrollaron métodos de validación actualmente conocidos como “firma digital”.

La firma digital es el “resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control”. Terceras partes deben poder “identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma”. *(Ley 25.506).*

No se consideran “firma digital”: la firma digitalizada (por ej., una firma escaneada), la firma electrónica (contraseña o password, firmas biométricas, etc.) ni los documentos encriptados, porque no permiten cumplir simultáneamente con los principios de autenticidad (de origen) e integridad (de contenido).

Se pueden firmar digitalmente los datos enviados a través de un formulario web, las imágenes, archivos de audio o video, bases de datos, páginas web y correos electrónicos, etc.

A nivel informático, la firma digital es un pequeño archivo denominado “código hash”, que se genera al aplicar una función hash al contenido del documento. El código hash se encripta y se adjunta al documento (como la firma ológrafa, la firma digital se suma al documento).

La **“cadena de confianza”.** Para asegurar que no haya habido sustitución de identidades–, se recurre a un marco institucional que, por medio de certificaciones, valida la identidad de los firmantes.

1) Entidades verifican la identidad del firmante confirmando datos (DNI, CUIL, CUIT, etc.) y expiden un Certificado Digital. Para garantizar la autenticidad e integridad del Certificado Digital expedido, este también debe estar firmado digitalmente por la entidad emisora.

2) Una entidad jerárquicamente superior certifica la identidad de la primera.

3) Las Autoridades Certificantes (AC) o Certificadores Licenciados emiten los Certificados de Clave Pública, que vinculan la clave pública con un titular determinado.

4) La Autoridad Certificante Raíz (AC Raíz) o Ente Licenciante expide los certificados de clave pública de las AC y certifica su identidad.

5) AC Raíz emite su clave pública en un Certificado Digital autofirmado.

MARCO LEGAL

Ley 25.506, de Firma Digital (2001).

Dto. 2628/02. Reglamenta la Ley de Firma Digital. Establece una infraestructura regulatoria y crea un Ente Administrador de firma digital.

Contacto
Av. Rivadavia 1745 - (C1033AAH) CABA - Argentina
Tel.: (54 11) 4124 - 3700
informacion@agn.gov.ar / www.agn.gov.ar

Dto. 283/03. Autoriza a la ONTI a emitir certificados digitales, "con carácter transitorio, y hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos por la Ley 25.506 y su Dto. Reglamentario".

Dto. 1028/03. Disuelve el Ente Administrador de firma digital creado en la reglamentación. Asigna competencias de AC-Raíz a la ONTI.

Res. 227/10, de la Secretaría de la Gestión Pública. Otorga a la ONTI la licencia para operar como Certificador Licenciado, es decir, como Autoridad Certificante o AC (art. 2º). Establece que la ONTI debe actuar como Autoridad Certificante para los organismos del Sector Público Nacional.

La ONTI ofrece los siguientes servicios:

- Publicación de Certificado Raíz y Certificado AC-ONTI.
- Publicación de CRL (Lista de Certificados Revocados).
- Sistema de Registro de firma digital.

CONCLUSIONES

La firma digital tiene validez jurídica y equivale a la firma ológrafa *(Dto. 427/98).*

La Ley 25.506, de Firma Digital (que deroga al Dto. 427/98 por subsumirlo en su objetivo), promueve su uso pero no le da carácter de obligatorio. Y si bien la Dirección de Innovación Tecnológica brinda cursos para promover la firma digital, no se ha logrado su uso masivo en el ámbito de la Administración Pública Nacional; de hecho, subsisten expedientes en soporte papel, con el consiguiente costo económico en concepto de almacenamiento. Por su parte, la Ley 19.549, de Procedimientos Administrativos, todavía mantiene vigente "el formalismo del acto administrativo": "…El acto administrativo se manifestará expresamente y por escrito…" *(art. 8°).*

La ONTI ejerce dos funciones contrapuestas:

-Como Autoridad Certificante, expide Certificados Digitales *(Dto. 283/03).*

-Como AC-Raíz, certifica y audita a las Autoridades Certificantes *(Dto. 1028/03).*

Se vulnera así el principio de control por oposición de intereses, lo que origina gran parte de las falencias detectadas:

Calidad y continuidad del servicio brindado por la ONTI. No se tuvieron a la vista los acuerdos de niveles de servicios formalizados con los organismos que brindan soporte a la plataforma tecnológica de firma digital, ni se realizan tareas de seguimiento y control periódico a la empresa que provee soluciones informáticas para la ONTI. El riesgo consecuente no es adecuadamente administrado: la ONTI carece de un plan de contingencia que determine los pasos a seguir ante una eventual caída de servicio.

-Falta un sistema de registro y seguimiento de pedidos de soporte. Esto pone en riesgo la resolución de las solicitudes de los usuarios y desaprovecha la posibilidad de realizar una adecuada gestión del conocimiento.

-Comisión Asesora para la Infraestructura de firma digital. Debe reunirse como mínimo cada tres meses (Ley 25.506). El Poder Ejecutivo designó a sus integrantes, pero la Comisión solo se reunió una vez.

-Recursos físicos y humanos asignados. Insuficientes para cumplir la normativa. Por ej., las auditorías sobre las Autoridades Certificantes y de Registro no se realizan con la periodicidad estipulada; el personal de la Dirección de Innovación Tecnológica que opera para la Autoridad Certificante ONTI es el mismo que controla su gestión, doble intervención que pone en riesgo la independencia del control realizado.

En síntesis. La ONTI cumple razonablemente con su tarea de gestionar la firma digital, pero es necesario compatibilizar el marco normativo institucional y los recursos asignados.

LA FUNCIÓN HASH. Aplicada a un documento, genera una cadena de caracteres (o código hash) a partir del propio contenido del documento. Algunas propiedades la hacen adecuada para su uso en firmas digitales:

-No es reversible: el contenido del documento puede generar un código hash, pero a partir de éste no se puede recuperar el contenido del documento.

-Pequeños cambios en el documento de origen provocan grandes cambios en el código hash. Así, una misma función hash aplicada dos veces sobre un mismo documento ofrecerá el mismo código hash sólo si no hubo modificaciones en el contenido.