



Colegio de Abogados
QUINTA CIRCUNSCRIPCIÓN JUDICIAL · SEDE RAFAELA · SANTA FE

Pautas para obtener firma digital:

1- **COMPLETAR** el formulario en

<https://pki.igj.gov.ar/app/Signature/Request/Hardware/CertificateRequest.aspx>

El correo electrónico ingresado al momento de completar el formulario debe ser personal (**únicamente del titular de la solicitud, sin excepción**)

Verificar los datos y luego seleccionar “Enviar Datos de Solicitud de Certificado”. En esta etapa sólo se precargan los datos necesarios para realizar el trámite. Aún NO se ha efectuado la generación de claves.

2- **CONFIRMAR**: El solicitante recibirá automáticamente un correo electrónico en la casilla consignada en el formulario. Este correo incluirá un link de verificación al que deberá acceder para continuar el trámite. El link tiene una vigencia de 24hs. Pasado ese lapso de tiempo, si el solicitante no **confirmó** el mail, deberá cargar nuevamente la solicitud (volver a completar el formulario).

3- **PRESENTARSE ANTE LA AUTORIDAD DE REGISTRO**: El próximo paso es presentarse personalmente ante el Oficial de Registro con el DNI y el TOKEN (dispositivo criptográfico)

El solicitante tiene veinte (20) días hábiles para presentarse ante el Oficial de Registro desde el momento en que completa y envía el formulario. Caso contrario, el formulario se rechazará automáticamente, debiendo completarse uno nuevo.

El oficial de registro realizará las validaciones correspondientes (verificará la identidad del solicitante y la toma de datos biométricos) y el soporte técnico de firma digital verificará los requisitos del dispositivo criptográfico (token)

El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada

del titular, informando la emisión del certificado en el cual figuran dos datos importantes (Número de serie del certificado y PIN de revocación), por lo que es recomendable conservarlo.

RECUERDE:

El trámite es personal y de modalidad presencial.

El certificado de firma digital tiene una validez de dos años. Se renueva el certificado, no el token.

Deberá solicitar la revocación y generar un nuevo certificado de firma digital:

- Si durante el plazo de validez del certificado se produce alguna modificación en los datos que fueron incluidos en el mismo (nombre, apellido, CUIL o correo electrónico),

-Ante cualquier circunstancia que pudiere comprometer la privacidad de sus datos de creación de firma.

-En caso de robo o extravío. Además de revocar el certificado deberá realizar la denuncia ante autoridad policial .

Los certificados que se otorgan son únicamente para personas físicas. (El certificado de firma digital se emitirá a nombre del suscriptor, no a nombre de empresas).

Requerimientos del token (dispositivo criptográfico)

Dispositivo criptográfico (token) que cumpla con el estándar FIPS 140-2 nivel 2 o superior, que soporte claves RSA de 2048 bits. Los mismos deberán estar homologados por NIST National Institute of Standards and Technology de acuerdo a lo establecido en la Política Única de Certificación de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI).

Requerimientos del software de su PC

Para empezar a operar con Firma Digital es necesario **instalar el Driver de su Token** y los **certificados de la AC-ONTI** (Autoridad Certificante de la ONTI) **y de la AC-Raíz** (Autoridad Certificante Raíz) en su equipo.

También la aplicación de escritorio **Acrobat o similares** que permite firmar cualquier documento en formato PDF.

IMPORTANTE: Es el proveedor del TOKEN quién también deberá suministrar todos los complementos requeridos en el puesto de trabajo (PC).

Aclaración importante: Para trámites judiciales sólo resulta válida la firma digital con token (no así la firma la firma digital remota sin token, aplicación que opera desde celulares)

GLOSARIO

Firma digital:

Es una herramienta tecnológica que nos permite asegurar la autoría de un documento o mensaje y verificar que su contenido no haya sido alterado. Es una secuencia única de letras y números que vincula al firmante con un documento electrónico.

Un documento electrónico firmado digitalmente posee la misma validez jurídica que un documento en papel firmado de puño y letra.

Se usa como identificación y autenticación en internet y sistemas informáticos.

Características de la firma digital:

Validez jurídica: tener tu firma digital te permite firmar documentos electrónicos digitalmente con la misma validez jurídica que una firma de puño y letra. La firma se encuentra bajo control del firmante en todo momento.

Autenticidad e integridad del documento: podrás identificar al autor fácilmente y verificar si ese documento fue alterado. Por lo cual se asegura la autoría e integridad del mismo.

Seguridad: se basa en la criptografía asimétrica.

Múltiples usos: para hacer trámites con entidades privadas y públicas, tales como declaraciones impositivas y notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior. Se puede firmar digitalmente cualquier tipo de archivo.

Token:

Es el dispositivo criptográfico donde se almacenan claves y certificados digitales necesarios para que se pueda firmar digitalmente.

Certificado digital:

Es un archivo digital que vincula datos de verificación de firma a un firmante (de forma que únicamente pueda firmar este firmante) y confirma su identidad.

ONTI:

Oficina Nacional de Tecnologías de Información encargada de crear, administrar y comunicar todos los procedimientos asociados al otorgamiento de Certificado digital.

Autoridad de Registro de Firma: El Poder Judicial de la Provincia de Santa Fe fue autorizado para cumplir la función de Autoridad de Registro de Firma Digital de la AC ONTI, por lo cual recepta y valida las solicitudes de certificados de firma digital. Existen en la provincia otras autoridades de registro además de la Corte, en las que también se puede tramitar el certificado.

Oficial de Registro:

Persona acreditada por la ONTI para controlar la documentación presentada, validar el proceso de registro, tomar datos biométricos y otorgar los tokens con certificado.