

Qué necesitas saber sobre la firma digital

Las firmas electrónicas son ampliamente aceptadas en todo el mundo como sustituto electrónico de la firma manuscrita. La mayoría de las leyes definen una firma electrónica como datos electrónicos asociados lógicamente a un documento y utilizados por el firmante para indicar su acuerdo. Para la mayoría de los casos de uso, clientes y ubicaciones, una firma electrónica simple es suficiente.

Sin embargo, algunas transacciones en ciertos países, en sectores altamente regulados o con entidades gubernamentales, pueden requerir o preferir la firma digital - un tipo de firma electrónica que ofrece un nivel aún mayor de garantía jurídica de identidad y seguridad.

En este eBook, exploramos a fondo el tema de la firma digital, en particular su validez legal en México, los requisitos legales y cómo DocuSign se posiciona como una solución confiable en este contexto.

Índice

- 1/ Validez legal de la firma electrónica en México
- 2/ Tipos de firma electrónica utilizadas en México
- 3/ ¿Qué es el Certificado Digital?
- 4/ DocuSign y la validación de identidad del firmante
- 5/ Conclusión

Validez legal de la firma electrónica en México

Las firmas electrónicas se han convertido en una herramienta fundamental para la realización de transacciones y acuerdos en línea, especialmente porque son prácticas, rápidas y seguras.

En México, la validez legal de una firma electrónica se encuentra respaldada por una serie de leyes y regulaciones.

Algunos de los marcos legales relevantes incluyen:

- **Código Civil Federal:** establece las bases para la legalidad de las firmas electrónicas en transacciones civiles.
- **Código de Comercio:** regula el uso de firmas electrónicas en transacciones comerciales.
- **Ley de Firma Electrónica Avanzada:** define y regula las firmas electrónicas avanzadas, conocidas también como firmas digitales.
- **Ley Federal de Protección al Consumidor:** aborda cuestiones de protección al consumidor relacionadas con transacciones electrónicas.
- **Acuerdo General 21/2007:** emitido por el Pleno del Consejo de la Judicatura Federal, establece directrices adicionales para la admisibilidad de evidencia electrónica en procesos judiciales.

En este entorno legal sólido, las empresas pueden aprovechar soluciones de terceros de confianza, como DocuSign, para garantizar la autenticidad y validez de las firmas electrónicas.

Tipos de firma electrónica utilizadas en México

La existencia de diferentes tipos de firma electrónica se debe a la diversidad de necesidades y contextos en los que se utilizan. Cada tipo de firma electrónica se adapta a distintos niveles de seguridad y requisitos legales, permitiendo su aplicación en una variedad de situaciones.

A continuación, se presentan dos tipos de firma electrónica utilizados en el país:

Firma electrónica simple (Estándar)

La firma electrónica simple, también conocida como “estándar”, está tipificada en el [artículo 89 del Código de Comercio de México](#).

La firma electrónica simple no utiliza certificados digitales para autenticar la identidad del firmante, cumple con los requisitos básicos de una firma electrónica válida y puede ser utilizada en una variedad de transacciones cotidianas.

Firma electrónica avanzada (Firma Digital)

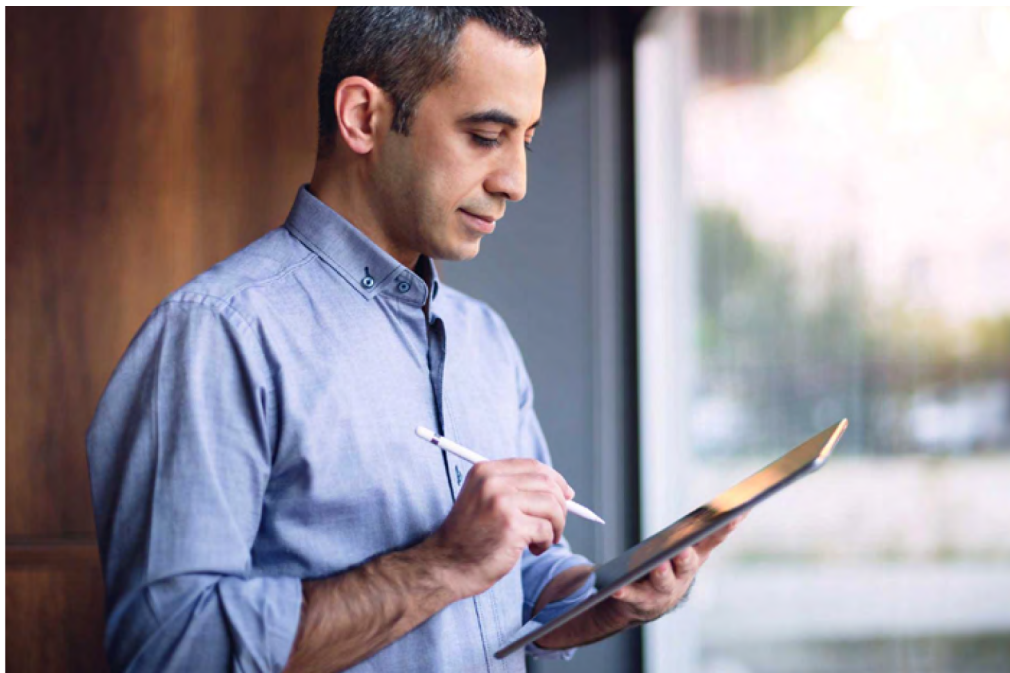
En México, la firma electrónica avanzada se define en la [Ley de Firma Electrónica Avanzada](#) y en el [artículo 97 del Código de Comercio](#).

La firma electrónica avanzada, conocida también como firma digital, **requiere el uso de un certificado digital**. Es generalmente, solicitada en transacciones online con sectores muy regulados o entidades gubernamentales.

Una firma digital es un tipo específico de firma electrónica que cumple con estrictas normas jurídicas, brinda un nivel más alto de garantía de identidad del firmante en comparación con la firma electrónica simple y mejora la seguridad de una transacción.

Con base en una tecnología llamada Public Key Infrastructure (PKI), una firma digital usa algoritmos y codificación para firmar y verificar la autenticidad de un documento. Un certificado digital anexado durante el proceso de firma, autentica la identidad del signatario y proporciona evidencia de prueba de manipulación.

Cabe mencionar que la responsabilidad de la obtención del certificado recae únicamente en el firmante, asegurando la no repudiación del proceso.



¿En qué casos es necesario utilizar firmas digitales?

La firma digital es una opción segura y eficiente para firmar documentos y transacciones requeridas en casos específicos, como por ejemplo, con entidades gubernamentales y/u organismos reguladores.

¿Qué es el Certificado Digital?

El certificado digital es un registro intransferible, una especie de credencial electrónica, que valida la autenticidad en línea de personas, empresas y entidades.

Básicamente es un archivo que reúne informaciones personales y datos sensibles. Estos datos son protegidos por el encriptado, garantizando la integridad de los documentos firmados electrónicamente.

Como hemos mencionado, la firma electrónica avanzada, o firma digital, utiliza un certificado digital para verificar la identidad del firmante.

Aquí hay una explicación general de cómo funciona:

- **Generación del par de claves:** un par de claves criptográficas es generado, una clave privada y una pública. La clave privada no se comparte y solo la utiliza el firmante para firmar documentos electrónicamente. La clave pública está disponible de forma abierta y es utilizada por cualquier persona que necesite verificar las firmas digitales generadas con la clave privada.
- **Solicitud y emisión:** la entidad o persona que desea obtener un certificado digital presenta una solicitud a una Autoridad de Certificación (AC) de confianza.
- **Instalación del certificado:** el certificado se asocia con la clave privada del titular y se utiliza para realizar operaciones seguras.
- **Verificación de la firma:** el destinatario del documento puede verificar la firma digital utilizando la clave pública del titular, que está contenida en el certificado digital del remitente.



e.Firma: el certificado digital del SAT

El Servicio de Administración Tributaria (SAT) es la autoridad fiscal de México encargada de administrar y supervisar el cumplimiento de las obligaciones fiscales en el país.

El órgano emite un certificado digital para identificar ciudadanos al realizar trámites y servicios por internet en el SAT, así como en otras Dependencias, Entidades Federativas, Municipios y la iniciativa privada.

Al igual que otros certificados digitales, la e.firma es un archivo cifrado, único e individual. Este conjunto único de datos autentica la identidad del emisor y valida documentos digitales, abriendo la puerta a más de 400 procedimientos en 20 dependencias.

DocuSign y la validación de identidad del firmante

Ahora que has conocido más sobre el escenario de la firma digital en México, es importante resaltar cómo DocuSign refuerza la seguridad y proporciona medios para identificar a los firmantes de documentos electrónicos, a través de su plataforma y una gama de soluciones robustas.

¿Qué diferencia a DocuSign del resto?

DocuSign es líder mundial en firmas electrónicas y ofrece gestión de transacciones digitales que ayudan a empresas de todos los tamaños a acelerar procesos, reducir costos y aumentar la eficiencia en diversos sectores.

Firma electrónica

El software de firma electrónica de DocuSign permite a los usuarios firmar documentos electrónicamente de forma legalmente vinculante.

Como presentamos anteriormente, la firma electrónica se considera tan válida como la firma autógrafa. DocuSign es una de las pocas empresas que ofrece firmas electrónicas que cumplen con las leyes de más de 180 países alrededor del mundo.

Firma digital

Documentos que requieren el uso de un certificado digital en el momento de la firma, también se pueden firmar a través de DocuSign.

A pesar de no ser una Autoridad de Certificación, DocuSign acepta diferentes certificados de varios países para la firma de documentos. En este material también mostraremos cómo utilizar los certificados digitales en DocuSign.

Verificación de identidad

DocuSign también ofrece una solución conectada de verificación de identidad:

[DocuSign Identify](#), una plataforma que brinda identificación digital de firmantes a través de métodos mejorados. La autenticación se puede realizar mediante diferentes métodos, como envío de código de acceso por SMS, Single Sign On (SSO), uso de claves de acceso, validación de credenciales, detección de vida mediante video, entre otros.



¿Qué es verificación de identidad?

La verificación de identidad es el método mediante el cual las personas demuestran que son quienes dicen ser. Es un elemento fundamental de seguridad para todo tipo de organizaciones, empleadores, clientes e individuos.

El método funciona mediante la recopilación de información y la comparación de lo que se recopila con lo que está en el archivo, para buscar una coincidencia que valide una identidad en diversos grados. Entre más puntos de coincidencia se recopilen, mayor será el grado de confianza en la verificación de identidad.

La verificación de identidad desempeña un papel importante en la prevención del fraude y el robo de identidad y en garantizar que los acuerdos que se completan digitalmente sean legalmente vinculantes. Pero autenticar la identidad puede ser complicado, especialmente cuando los contratos son de alto valor o vulnerables al fraude.

Para muchas transacciones comunes, un enlace a una dirección de correo electrónico validada es suficiente para certificar la identidad del firmante. Pero muchas organizaciones quieren una identificación de firmante mejorada para sus acuerdos de mayor valor, más allá del método de correo electrónico.



¿Cómo firmar documentos en DocuSign con certificado digital?

Puedes utilizar DocuSign para enviar y firmar documentos con certificados digitales.

Consulta una guía paso a paso para firmar con la e.firma del SAT:

- Alguien te envió un correo electrónico con documentos para revisar y firmar. Selecciona **Revisar Documento**
- Se abre la pantalla “Revise estos documentos y actúe en ellos”. Haz clic en **Iniciar**
- Selecciona las etiquetas de firma disponibles
- Selecciona **Continuar**
- Haz clic en el icono de firma, selecciona el tipo de firma deseado (predefinida, dibujo, imagen) y selecciona **Adoptar Firma**
- Una vez firmado el documento, haz clic en el botón **Finalizar**
- A continuación, DocuSign solicitará los archivos .cer y .key de tu e.firma
- Finalmente, introduce la contraseña de tu e.firma
- Luego, se abrirá la pantalla “Estamos aplicando su certificado”

¡Así se completó tu firma digital!

El documento quedará firmado y disponible en la plataforma de DocuSign.

Para verificar el archivo que ha sido firmado, haz clic en Bandeja de Entrada > Más > Historial > busca el documento en la lista.

¿Es seguro DocuSign?

DocuSign tiene seguridad y protección sólidas integradas en todas las áreas del negocio, incluyendo:

- Seguridad física: protección de sistemas y edificios donde residen los sistemas
- Seguridad de la plataforma: protección de los datos y procesos que se almacenan en los sistemas
- Certificaciones/procesos de seguridad: garantizan que los empleados y socios sigan las mejores prácticas de seguridad y privacidad

Seguridad física

- Centros de datos geográficamente dispersos con sistemas y redes activos y redundantes separados física y lógicamente
- Firewalls y enrutadores de calidad comercial para detectar ataques basados en la seguridad IP y denegación de servicio
- Protección contra malware
- Replicación de datos segura y en tiempo casi real
- Seguridad en sitio 24x7
- Estricto control de acceso físico con videovigilancia monitorizada

Seguridad de la plataforma

- Cifrado de datos en tránsito y en reposo con conexiones TLS y cifrado AES 256 bits
- Acceso y transferencia de datos vía conexiones cifradas (HTTPS)
- Uso de Security Assertion Markup Language (SAML), ofreciendo a los usuarios la Funciones más recientes para autenticación y autorización basadas en web
- Sello a prueba de manipulaciones (Infraestructura de Claves Públicas - PKI)
- Certificado de conclusión del proceso de firma
- Verificación de firma y bitácora de auditoría inalterable de acciones y estados de conclusión
- Múltiples opciones de autenticación para firmantes



Certificaciones/procesos de seguridad

DocuSign implementa una serie de certificaciones y procesos de seguridad para garantizar la protección y la integridad de los documentos y datos almacenados en su plataforma, tales como:

- **ISO 27001**: un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. Esta certificación demuestra el compromiso de DocuSign con la seguridad de la información y la gestión de riesgos.
- **SSAE 16**: ahora conocida como SOC 1 (Service Organization Control 1), es una norma que evalúa los controles y procedimientos utilizados por una organización de servicios en la prestación de servicios a sus clientes. Esta certificación se enfoca en la evaluación de los controles relacionados con la seguridad y la integridad de los datos.
- **AES-256**: este es un estándar de cifrado ampliamente reconocido y seguro que garantiza la protección de la información sensible. Usado para cifrar los documentos y datos almacenados en la plataforma.
- **Transmisión de Documentos vía SSL**: la transmisión segura de documentos a través de SSL (Secure Sockets Layer) con cifrado de 256 bits, protege la transferencia de documentos entre los usuarios y la plataforma, garantizando que los datos no sean interceptados o manipulados durante la transmisión.
- **Centros de datos distribuidos**: DocuSign opera varios centros de datos geográficamente distribuidos. Esta distribución garantiza la disponibilidad y la redundancia.

Además, otra característica importante de DocuSign que contribuye a la seguridad es su escalabilidad y disponibilidad. Hay más de un millón de clientes y mil millones de usuarios en todo el mundo que utilizan nuestra plataforma.

Sumado a eso, DocuSign eSignature tiene un nivel de servicio con disponibilidad del 99,99%, lo que implica que no hay tiempo de inactividad por mantenimiento, cada día se procesan millones de transacciones.

DocuSign también ofrece atención al cliente de alta calidad. Los usuarios tienen acceso a un equipo de soporte telefónico en varios lenguajes, incluido español, listo para responder cualquier pregunta relacionada con el uso de las herramientas.

Conclusión

Como se ve, las firmas electrónicas son una forma rápida y sencilla de firmar documentos. Las firmas digitales, un tipo de firma electrónica, ofrecen un alto nivel de garantía de identidad, funcionando como huellas dactilares electrónicas, que se utilizan en casos específicos.

DocuSign admite firmas electrónicas y digitales en varios países del mundo, incluido México, permitiendo a empresas de todos los tamaños completar negocios, acuerdos y transacciones rápidamente sin dejar de cumplir con sus respectivos requisitos de la industria.

¿Quieres conocer más?

Descubre cómo funciona la firma electrónica de DocuSign:
[¡obtén una prueba gratuita de 30 días!](#)

Si quieres saber sobre los beneficios de un software de gestión de contratos digitales como [DocuSign CLM Essentials](#), [contacta con uno de nuestros expertos](#).

Acerca de DocuSign

DocuSign ayuda a las organizaciones a conectarse y automatizar la forma en que preparan, firman, ejecutan y gestionan los acuerdos. Como parte de su línea de productos líderes en la industria, DocuSign ofrece eSignature, la forma número 1 del mundo de firmar electrónicamente en prácticamente cualquier dispositivo, desde cualquier lugar y en cualquier momento. Hoy en día, más de un millón de clientes y más de mil millones de usuarios en más de 180 países utilizan productos y soluciones DocuSign para acelerar el proceso de hacer negocios y simplificar la vida de las personas.

DocuSign, Inc.

Av Javier Barros Sierra
495 Santa Fe, Zedec Sta
Fé, Álvaro Obregón 1219
Ciudad de México

Para obtener más información

contactomx@docusign.com
01-800-9531-662
docusign.com/es-mx

DocuSign®