

# DOCUMENT TRUST MANAGER DE DIGICERT®

Firmas digitales, sellos electrónicos y marcas de fecha que protegerán las transacciones que lleve a cabo con documentos digitales en cualquier parte del mundo.

## Potencie los negocios internacionales

Document Trust Manager de DigiCert® permite a las empresas obtener firmas digitales, sellos electrónicos y marcas de fecha confiables que cumplen con las normativas y se aplican a una amplia gama de casos de uso internacionales. DigiCert ayuda a que las compañías tengan la seguridad de que cumplen con las regulaciones locales y específicas de su sector en Estados Unidos, la Unión Europea (UE), el Reino Unido, Suiza y otros países.

## Respete todas las normativas a nivel internacional

En muchos países, las leyes exigen firmas digitales de alta seguridad que cuenten con el respaldo de certificados emitidos por un proveedor de servicios de confianza que esté certificado en esa región. Por ejemplo, una firma electrónica calificada en la UE, el Reino Unido o Suiza solo puede ser emitida por un proveedor de servicios de confianza calificado, como DigiCert. Las firmas digitales de alta seguridad de DigiCert cumplen con la Lista de confianza aprobada por Adobe (AATL), el Reglamento de la UE (n.º 910/2014) en lo relativo a identificación electrónica y servicios de confianza para transacciones electrónicas (eIDAS), el eIDAS del Reino Unido y el ZertES de Suiza.

## Principales ventajas

- Agilice los procesos de firma de documentos de forma remota sin sacrificar la seguridad ni el cumplimiento de las normas.
- Utilice esta solución con las principales aplicaciones de firma electrónica de Adobe, Ascertia y DocuSign.
- Garantice que las firmas electrónicas ofrezcan los más altos niveles de seguridad en lo que concierne a la identidad.
- Cumpla con los reglamentos del sector, como Know Your Customer (KYC) o los requisitos contra el blanqueo de dinero (AML).
- Acceda a firmas electrónicas de confianza en Estados Unidos, la UE, el Reino Unido, Suiza y muchos países más.

## La ventaja de la confianza digital

Firme documentos en cualquier momento, lugar o dispositivo móvil moderno. Nuestra solución, que es sumamente flexible, incluye identidades digitales, certificados, tecnología y opciones de automatización que le permiten generar un elevado nivel de confianza en los documentos digitales. Document Trust Manager ofrece lo siguiente:



### Firmas digitales

Las firmas digitales son firmas electrónicas respaldadas por un certificado digital que está criptográficamente vinculado al campo de la firma por medio de la infraestructura de clave pública (PKI). Cada certificado digital, o identificación digital, como suele denominarse, está exclusivamente asociado a una persona específica y se obtiene tras la verificación de su identidad.



### Sellos electrónicos

Los sellos electrónicos son firmas digitales que ciertas entidades legales, como empresas u organizaciones, utilizan para certificar el origen, la autenticidad y la integridad de los documentos. Estos sellos pueden servir como una prueba legal contundente de que el documento proviene de una entidad específica y de que no ha sido manipulado y, por lo general, se utilizan en sistemas automatizados para gestionar procesos engorrosos, como tareas de facturación o pago masivo.



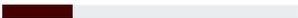
### Marcas de fecha

Las marcas de fecha son registros firmados de forma digital de la fecha y hora en que se produjo un evento y garantizan que un documento, firma digital o sello electrónico eran válidos en el momento en que se aplicó la marca y que no habían sido manipulados.

## Confianza integrada para las firmas electrónicas

No todas las firmas electrónicas son iguales. De hecho, la naturaleza de estas firmas es muy variada: desde simples casillas de verificación o garabatos en una tablet hasta firmas digitales de alta seguridad en la nube que cuentan con el respaldo de un riguroso proceso de verificación de identidad de parte de una autoridad acreditada, como DigiCert. Por este motivo, la incorporación de firmas digitales de alta seguridad que vinculen al signatario con un documento específico de modo definitivo ayuda a proteger las transacciones transfronterizas, las actividades de gran valor y otras operaciones electrónicas.

En el siguiente gráfico, se pueden apreciar la amplia gama de atributos de seguridad, el grado de cumplimiento normativo y el nivel de seguridad que caracterizan a los distintos tipos de firmas electrónicas:

| Tipo de firma                       | Firma electrónica   | Firma digital (AATL)  | Firma digital (regulada/calificada)   |
|-------------------------------------|---|---|---|
| Descripción                         | Este es un término amplio que abarca todos los procesos electrónicos que sirven para indicar la aceptación de un acuerdo o registro. La forma más básica de firma electrónica puede ser un nombre escrito por medio de una computadora o dispositivo móvil en una línea de firma o la selección de una casilla de verificación. | Esta es una firma electrónica más segura que requiere el uso de una identificación digital que haya sido emitida por un proveedor de servicios de confianza (TSP) que, a su vez, cumpla requisitos de seguridad y verificación de identidad específicos de la Lista de confianza aprobada por Adobe (AATL). | Esta es una firma electrónica sumamente segura que requiere el uso de una identificación digital regulada que haya sido emitida por un TSP que esté certificado en una región específica, como, por ejemplo, un proveedor de servicios de confianza calificado (QTSP) de la UE o Suiza. |
| Confianza pública                   | No es necesaria.  | Cuenta con la confianza de Adobe Acrobat y Reader.  | Cuenta con la confianza de Adobe Acrobat y Reader.*   |
| Identidad digital                   | No es necesario que esté exclusivamente vinculada al signatario.  | La prueba de la identificación digital exclusiva del signatario debe estar criptográficamente vinculada al campo de firma (PKI).  | La prueba de la identificación digital exclusiva del signatario debe estar criptográficamente vinculada al campo de firma (PKI).  |
| Nivel de seguridad                  | <b>Bajo</b><br>La verificación de identidad es limitada o escasa.    | <b>Considerable</b><br>La verificación de identidad es obligatoria.   | <b>Alto</b><br>La verificación de identidad es rigurosa y se lleva a cabo en persona o mediante un método similar.   |
| Autenticación de dos factores (2FA) | No es necesaria para firmar el documento.   | Es obligatoria para firmar el documento.  | Es obligatoria para firmar el documento.  |
| Validez a largo plazo               | No es necesaria; puede incluirse con una solución de firma.   | Se aplican un sello inviolable y una marca de fecha al documento firmado.   | Se aplican un sello inviolable y una marca de fecha al documento firmado.   |
| ¿Es equivalente a una firma manual? | No  | No  | Cumple los requisitos reglamentarios específicos de la UE, el Reino Unido y Suiza.*   |

## Características principales

### Prueba de firma

Constituye una prueba contundente de la identidad del signatario, la fecha y hora de la firma y la autenticidad del documento y, como tal, está criptográficamente vinculada a los acuerdos firmados.

### Integraciones escalables

Funciona con las principales soluciones de firma, como Adobe Acrobat Sign, Ascertia SigningHub y DocuSign.

### Verificación remota de la identidad

Identifica a clientes, ciudadanos y empleados por medio de dispositivos móviles modernos y documentos de identidad.

### Opciones de implementación flexibles

Implemente Document Trust Manager como una solución alojada, local o híbrida.

### Soluciones personalizadas

Cree una instancia privada de Document Trust Manager o use la API del Cloud Signature Consortium (CSC) para integrar este servicio con soluciones de firma personalizadas.

### Control centralizado

Simplifique la gestión de certificados e identificaciones digitales por medio de la plataforma DigiCert ONE.

### Claves de firma protegidas

Proteja las claves privadas que se utilizan para las firmas digitales en módulos de seguridad de hardware (HSM) acreditados y en dispositivos calificados de creación de firmas que se alojan en entornos seguros y certificados de Estados Unidos, la UE y Suiza.

## Proteja sus documentos digitales

Dado que los documentos digitales están reemplazando rápidamente a los procesos en papel, las empresas han comenzado a implementar soluciones de sellado electrónico para resguardar la autenticidad de los documentos. Cuando se la combina con firmas digitales de alta seguridad, la aplicación de sellos electrónicos en contratos, acuerdos y demás documentos digitales ayuda a proteger su empresa del costo que suponen los delitos cibernéticos o los fraudes que están relacionados con las transacciones electrónicas.

Document Trust Manager le permite garantizar que todos sus documentos estén protegidos con sellos electrónicos, marcas de fecha y firmas digitales que están respaldados por los más altos niveles de seguridad en materia de identidad.

## Plataforma DigiCert ONE: garantía de confianza digital

Document Trust Manager de DigiCert forma parte de la plataforma de confianza digital DigiCert ONE, que unifica las soluciones de confianza digital de DigiCert en una moderna arquitectura basada en contenedores que ofrece alta escalabilidad, flexibilidad de implementación, una rápida amortización y gestión unificada de la PKI.

## Ponga manos a la obra hoy mismo

Empiece a usar Document Trust Manager de DigiCert® ya mismo. Comuníquese con su gestor de cuenta de DigiCert o escriba a [sales@digicert.com](mailto:sales@digicert.com).

## Acerca de DigiCert, Inc.

DigiCert es el proveedor de confianza digital número uno del mundo. Gracias a él, tanto los usuarios individuales como las empresas pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida. La plataforma DigiCert® ONE, garantía de confianza digital, protege los sitios web, los accesos y comunicaciones empresariales, el software, las identidades, el contenido y los dispositivos para que las empresas respondan a toda una gama de necesidades en materia de confianza pública y privada con una visibilidad y un control centralizados. Su galardonado software y su liderazgo en el sector de los estándares, la asistencia y las operaciones convierten a DigiCert en el proveedor de confianza digital al que recurren grandes empresas de todo el mundo. Para obtener más información, visite [digicert.com/es](https://digicert.com/es) o siga a [@digicert](https://twitter.com/digicert).