DocuWare

White Paper
Firmas Electrónicas con DocuWare

Procesos empresariales seguros gracias a la confianza en los documentos

Marzo 2021

DocuWare GmbH
Planegger Straße 1
D-82110 Germering
www.docuware.com

Contenido

1 Procesos empresariales seguros gracias a la confianza en los documentos

La confianza es la base de cualquier cooperación o intercambio de bienes e información, ya sea en el ámbito personal o en el comercial oficial. En los contratos u otros acuerdos, el símbolo vinculante de esta confianza es la firma de una persona.

Lo que antes era exclusivo del papel y el bolígrafo se consigue ahora con una firma electrónica, que crea un compromiso vinculante del mismo modo que lo hace la firma manuscrita, con socios comerciales de todo el mundo. Las firmas crean seguridad jurídica para sus documentos, incluso cuando los involucrados se encuentran lejos unos de otros.

Casi todos los sectores industriales se han adaptado a tener personal que colabora desde distintas ubicaciones, incluidos los empleados que trabajan desde casa o estando de viaje.

Las firmas en la nube contribuyen de forma significativa al éxito de su empresa, ya que proporcionan una verificación legal de los documentos al mismo tiempo que garantizan la continuidad y la productividad empresarial.

Demostrar la integridad y autenticidad de los documentos

Cada día escribimos o recibimos grandes volúmenes de documentos. Algunos de ellos no requieren ninguna prueba documental en un entorno empresarial u oficial. Otros, como determinados contratos, deben ser jurídicamente irreprochables para que un tribunal también los considere vinculantes. Según el sector industrial, el proceso, las preferencias, la ubicación de su empresa y con quién trabaja, las normas varían para establecer la seguridad jurídica.

Con las firmas electrónicas, se crea seguridad para tres factores esenciales:

- Autenticidad: El documento es genuino.
- Integridad: Los contenidos del documento no han cambiado.
- Origen: La persona que creó el documento puede ser identificada.

Firmas electrónicas para empresas en red y trabajo a distancia

Los documentos empresariales ya no son exclusivos de las oficinas corporativas físicas. También son utilizados por los empleados que trabajan desde casa o estando de viaje. Este entorno de trabajo dispersado exige la necesidad de contar con principios vinculantes y seguridad jurídica incluso cuando los involucrados se encuentran lejos unos de otros. Las firmas electrónicas ayudan a los empleados a cumplir con sus responsabilidades de forma inmediata y desde cualquier ubicación. Al fin y al cabo, un proceso no debería paralizarse porque un empleado no puede firmar un documento cuando se encuentra fuera de la oficina por trabajo debido a que no tiene la posibilidad de imprimir el documento.

Ejecutar transacciones independientemente de la ubicación y conforme a la ley

Aunque el rigor de los modelos legales varía de una región a otra, una cosa está clara: los módulos de seguridad de hardware para generar certificados digitales se pueden ubicar en infraestructuras de nube altamente seguras en cualquier lugar.

Mientras que antes era necesaria una tarjeta inteligente física y un lector de tarjetas, hoy se puede conectar a través de proveedores de firmas verificadas que están certificados de acuerdo con estándares de seguridad claros. De este modo, los datos intercambiados durante el proceso de firma también son seguros.

Firmar desde cualquier dispositivo

Mediante la integración de las firmas electrónicas en los flujos de trabajo automatizados, las empresas pueden completar todos los procesos de forma legalmente segura, independientemente del dispositivo utilizado. Esto incluye firmas proporcionadas en ordenadores, tabletas y dispositivos móviles tanto de la empresa como del cliente.

Los datos de la transacción son seguros y están protegidos. Con las firmas modernas, las empresas cumplen con los requisitos de cumplimiento normativo de sus respectivas regiones, tanto en términos de seguridad de la información como de protección de datos.

Autenticación y transmisión de la identidad

Muchos documentos, como los contratos, son creados y firmados por una persona dentro de una organización y luego refrendados por una persona ajena a la misma. En estos casos se utiliza muy a menudo la firma electrónica avanzada. Los procedimientos reconocidos para ello son la confirmación mediante código de acceso, teléfono, SMS o la autenticación basada en el conocimiento.

Sin embargo, en función de los requisitos de la firma, es posible que sea necesario verificar la identidad del firmante sin dejar lugar a dudas. En estos casos se recomienda una firma electrónica cualificada. Esta verificación se realiza a través de un proveedor externo que autentifica al usuario y garantiza así su identidad al firmar.

Qué hay que tener en cuenta a la hora de tomar una decisión

Si quieren utilizar firmas electrónicas en su empresa, debe tener en cuenta estas cuestiones, entre otras:

- ¿La solución de firma es la adecuada para probar la integridad y autenticidad de los documentos?
- ¿El proceso de firma se realiza en flujos de trabajo automatizados en los que también se pueden incluir empleados con estaciones de trabajo remotas?
- ¿Ofrece la solución la posibilidad de firmar tanto en los dispositivos del cliente como en los de la empresa?
- ¿Permite la solución firmar con diferentes niveles de seguridad (firma electrónica avanzada o cualificada)?
- ¿Se almacenan los datos del proceso de firma cumpliendo la normativa aplicable en la región de protección de datos deseada?
- ¿Utiliza el proveedor de servicios de firmas módulos HSM altamente seguros con cumplimiento normativo probado?

2 Firma de documentos en el flujo de trabajo con DocuWare

Con el servicio de firmas DocuWare, puede aplicar una firma electrónica a sus documentos en un flujo de trabajo. Hay dos factores que garantizan la escalabilidad y la preparación de su empresa de cara al futuro:

- Con la firma de documentos dentro de los flujos de trabajo, se reduce al mínimo el tiempo y esfuerzo necesarios de sus empleados, a la vez que acelera los procesos en su totalidad.
- Utiliza firmas remotas, también conocidas como firmas en la nube por lo que son independientes de la ubicación de los implicados.

Con las firmas en la nube, el proceso de firma tiene lugar en la nube a través de Internet, independientemente de si se trabaja con DocuWare Cloud o con un sistema local de DocuWare. No es necesario instalar localmente ningún software ni hardware.

El servicio de firmas DocuWare garantiza que sus documentos sean firmados por un proveedor de firmas reconocido y verificado. El servicio le ofrece la máxima rapidez y flexibilidad en el uso de las firmas electrónicas:

- Integre sin problemas proveedores de firmas externos como Validated ID o DocuSign en sus flujos de trabajo de DocuWare. Los documentos se transmiten automáticamente al proveedor de servicios y el destinatario también recibe automáticamente una notificación cuando un documento está disponible para firmar.
- Recopilar las firmas de un documento de todos los firmantes pertinentes a tiempo.
- ¿Avanzada o cualificada? Usted elige el nivel de seguridad de la firma en función de sus necesidades. La principal diferencia es el procedimiento de autenticación. En el caso de una firma avanzada, por ejemplo, basta con una autenticación de dos factores del firmante (como el correo electrónico o el SMS). Para una firma cualificada, se requiere el certificado de un proveedor de servicios de confianza para la autenticación.
- Los certificados cualificados para una firma electrónica cualificada se almacenan de forma centralizada en un proveedor de servicios externo para que puedan ser utilizados en cualquier momento.
- Usted almacena el documento junto con la firma en el archivo para la auditoría.

3 Ventajas del uso de firmas electrónicas en sus procesos

La firma de documentos en los flujos de trabajo es necesaria en muchos procesos empresariales. Los siguientes escenarios son ejemplos de una gran variedad de áreas de negocio.

Tramitación de contratos sin papel

Introduzca los contratos de forma sencilla y sin demoras, por ejemplo, los contratos de arrendamiento de equipos.

Firma de contratos de trabajo

Con personal dispersado y trabajando remotamente, su departamento de RRHH puede solicitar la firma de diferentes tipos de contratos de trabajo sin demora y sin que el firmante esté físicamente presente. Esto no solo ahorra costes de papel y correo postal, sino que acorta enormemente el proceso. Si está invirtiendo mucho dinero en la contratación de empleados cualificados, no debe retrasarse la firma de contratos únicamente porque su empresa no dispone de un proceso de firma digital. Las firmas electrónicas también permiten que los nuevos empleados completen el proceso de contratación y de incorporación de forma 100% remota.

Recursos humanos

Para el cumplimiento corporativo, puede hacer que los empleados firmen electrónicamente los PNT (procedimientos normalizados de trabajo), las instrucciones de trabajo, los contratos de confidencialidad u otros acuerdos en el flujo de trabajo sencillamente y de inmediato. Si sus empleados trabajan en una oficina remota, las firmas electrónicas pueden ayudar a garantizar que todos apliquen el mismo estándar de confianza. Para las auditorías y las certificaciones, todas las pruebas están disponibles en el archivo de conformidad con la ley y se pueden presentar con tan solo pulsar un botón.

Aprovisionamiento de equipos informáticos

El aprovisionamiento de equipos es un componente clave del proceso de incorporación y supone una gran pérdida de tiempo y un aumento de los costes por las ineficiencias. Los flujos de trabajo automatizados permiten agilizar los procesos y las firmas electrónicas ayudan a los empleados a firmar de forma eficiente al recibir cualquier equipo informático. Esto también se puede aplicar cuando se proporcionan dispositivos para trabajar en casa.

Préstamos para clientes

Una empresa comercializadora o distribuidora concede a sus clientes líneas de crédito. La documentación relacionada y los acuerdos contractuales se envían automáticamente para su revisión por parte del cliente. Las firmas de los clientes se realizan electrónicamente en cualquier ordenador, tableta o dispositivo móvil disponible.

4 Proveedores de servicios de firmas de DocuWare

DocuWare trabaja con proveedores de servicios de firmas como Validated ID o DocuSign para firmar documentos en un flujo de trabajo de DocuWare. Ambos son proveedores de servicios de confianza (TSP, por sus siglas en inglés). Los procedimientos de firma de Validated ID y DocuSign ofrecen diferentes procedimientos de autenticación que puede especificar en función del método de firma que elija.

Los métodos de firma son la firma electrónica avanzada (AES, por sus siglas en inglés) y la firma electrónica cualificada (QES, por sus siglas en inglés), que se explican con más detalle en el capítulo Cumplimiento normativo mediante firmas electrónicas en todo el mundo (página 17).

Validated ID

Validated ID generalmente envía un correo electrónico al firmante con un enlace al documento. El firmante puede elegir entre los siguientes métodos de autenticación para firmar, dependiendo de cómo se haya enviado la solicitud y del método de firma AES o QES asociado:

- Remoto: autenticación por SMS (AES)
  Cuando se envía un documento a Validated ID para ser firmado, el destinatario recibe un mensaje SMS que le permite firmar el documento.
- Biométrico: autenticación in situ (AES)
  Un cliente firma en una tableta. Los datos biométricos, como la presión y la velocidad de escritura, se registran e integran en el documento con la firma. Los dispositivos utilizados deben estar registrados de antemano y, por lo tanto, son conocidos por el proveedor de servicios de firmas (dispositivos compatibles). Únicamente en el caso del método biométrico se enviará un documento directamente a un dispositivo registrado para su firma.
- Centralizado - autenticación única con el proveedor de servicios de firmas (AES/QES)
  Con esta firma, Validated ID almacena un certificado que confirma la identidad del usuario tras identificarlo. Esto permite que los usuarios se autentiquen y firmen documentos con una identificación validada desde cualquier lugar y en cualquier momento.

DocuSign

DocuSign envía un correo electrónico al firmante con un enlace al documento. La persona que inicia un proceso de firma puede elegir entre los siguientes métodos de autenticación para firmar, dependiendo de cómo se haya enviado la solicitud y del método de firma AES o QES asociado:

- Sin autenticación especial (AES)
- Autenticación por llamada telefónica (AES)
- Autenticación por código de acceso, por ejemplo, contraseña (AES)
- Autenticación por SMS (AES)

- Autenticación basada en el conocimiento (AES). En este método, disponible solo en los Estados Unidos, los firmantes responden a preguntas específicas sobre sí mismos, cuyas respuestas están disponibles en los registros públicos (por ejemplo, las direcciones actuales y anteriores).
- Comprobación de ID para eIDAS (AES/QES)

5 Cómo funciona la firma electrónica en DocuWare

Para firmar un documento con el servicio de firmas DocuWare (por ejemplo, un contrato), primero se debe almacenar el documento en un archivador. El servicio se inicia entonces dentro de una tarea de flujo de trabajo.

Tras esta activación, se llevan a cabo varios pasos entre la persona 1 que solicita una firma en un flujo de trabajo de DocuWare y la persona 2 que firma el documento. Ambos pueden ser también la misma persona.

En principio, el proceso de firma con el servicio de firmas DocuWare es siempre el mismo:

1. El flujo de trabajo envía información sobre el documento y la firma al servicio de firmas.
2. El servicio de firmas DocuWare carga el documento desde DocuWare y lo transfiere al proveedor de servicios de firmas.
3. El proveedor de servicios de firmas informa a la persona firmante por correo electrónico.
4. La persona que debe firmar abre el enlace enviado con el documento e inicia el proceso de firma.
5. El proveedor de servicios de firmas autentifica a la persona que firma el documento.
6. La firma está vinculada al documento.
7. El proveedor de servicios de firmas informa al servicio de firmas de que el documento está firmado.
8. El servicio de firmas DocuWare carga el documento desde el proveedor de servicios de firmas y lo almacena en DocuWare.

Un documento puede ser firmado por una sola persona o por varias. El proceso de firma es siempre el mismo para cada firmante, porque una firma electrónica está siempre vinculada a la persona que la ejecuta.

El tipo de firma que se elija, firma electrónica avanzada (AES) o cualificada (QES), depende siempre del tipo de documento, de los requisitos legales, de si deben firmar una o varias personas y del nivel de seguridad de la irma. Lea más sobre este tema en el capítulo Cumplimiento normativo mediante irmas electrónicas en todo el mundo (página 17).

Las diferentes opciones de firma

Los procedimientos de firma difieren principalmente en el método de autenticación. Las opciones de autenticación que se describen a continuación suponen que: La persona 1 (P1) trabaja en una empresa que utiliza DocuWare. La persona 2 (P2) puede ser un compañero interno o un socio comercial externo, pero no tiene por qué ser un usuario de DocuWare. Siempre es la persona 1 la que solicita la firma dentro de un flujo de trabajo y la persona 2 la que firma.

Validated ID: Remota (AES)

La persona 2 no necesita registrarse a Validated ID.

Pasos:

1. P2 indica a P1 su nombre, su dirección de correo electrónico y su número de teléfono con SMS.
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma de la Validated ID.
3. P2 recibe un correo electrónico con el enlace al documento y un SMS con un TAN, que utiliza para activar la firma.

Validated ID: Método biométrico (AES)

La persona 2 no necesita registrarse a Validated ID.

Pasos:

1. P1 trabaja en la recepción de una empresa y comprueba visualmente la identidad del visitante P2. P1 confirma la identidad de P2 e introduce su nombre en el formulario en una tarea de flujo de trabajo. La información se envía a una tableta de firmas.
2. P2 firma en la tableta, almacenándose así datos biométricos como la presión de la escritura para una posible verificación posterior.

Validated ID: Método centralizado (AES)

La persona 1 y la persona 2 trabajan en la misma empresa que tiene un contrato con Validated ID. P2 está registrado con Validated ID.

Pasos:

1. P2 indica a P1 su nombre, su dirección de correo electrónico y la ID de usuario que P2 ha recibido de Validated ID al autenticarse (que puede ser, por ejemplo, un número de pasaporte).
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma.
3. P2 firma el documento.

Validated ID: Método centralizado (QES)

La persona 1 y la persona 2 trabajan en la misma empresa que tiene un contrato con Validated ID. P2 está registrado en Validated ID y se ha sometido a una identificación independiente con Validated ID para obtener un certificado cualificado.

Pasos:

1. P2 indica a P1 su nombre, su dirección de correo electrónico y la ID de usuario que P2 ha recibido de Validated ID al autenticarse (que puede ser, por ejemplo, un número de pasaporte).
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma.
3. P2 firma el documento con el certificado cualificado.

DocuSign: Sin autenticación (AES)

La persona 2 no necesita registrarse a DocuSign.

Pasos:

1. P2 indica a P1 su nombre y su dirección de correo electrónico.
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma de DocuSign.
3. P2 recibe un correo electrónico con un enlace al documento en DocuSign, donde lo firma.

DocuSign: Autenticación vía SMS (AES)

La persona 2 no necesita registrarse a DocuSign.

Pasos:

1. P2 indica a P1 su nombre, su dirección de correo electrónico y su número de teléfono con SMS.
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma de DocuSign.
3. P2 recibe un correo electrónico con un enlace al documento en DocuSign. P2 recibe un TAN de DocuSign vía SMS, que utiliza para activar la firma.

DocuSign: Autenticación vía llamada telefónica (AES)

La persona 2 no necesita registrarse a DocuSign.

Pasos:

1. P2 indica a P1 su nombre, su dirección de correo electrónico y su número de teléfono.
2. P1 introduce los datos de P2 en el formulario del flujo de trabajo y así solicita la firma de DocuSign.
3. P2 recibe un correo electrónico de DocuSign con un enlace al documento, así como la información recibida por teléfono, por ejemplo, un código, con el que P2 activa la firma.

DocuSign: Autenticación vía código de acceso (AES)

La persona 2 no necesita registrarse a DocuSign.

Pasos:

1. P2 indica a P1 su nombre y su dirección de correo electrónico.
2. P1 introduce los datos de P2 y un código (p. ej. una contraseña) en el formulario del flujo de trabajo y así solicita la firma de DocuSign.
3. P2 recibe un correo electrónico con un enlace al documento en DocuSign.
4. P2 transfiere activamente el código a P1. Esto se puede hacer verbalmente (conversación cara a cara, llamada telefónica) o a través de un acuerdo previo (por ejemplo, la fecha de nacimiento o un número de socio siempre se pueden utilizar como código).
5. P2 utiliza el código para activar la firma.

DocuSign: Autenticación basada en el conocimiento (solo en EE. UU., AES)

La persona 2 no necesita registrarse a DocuSign.

Pasos:

1. P2 indica a P1 su nombre y su dirección de correo electrónico.
2. P1 solicita la firma y transmite el nombre y la dirección de correo electrónico de P2 a DocuSign.
3. El P2 recibe un correo electrónico con un enlace al documento y debe responder a una pregunta personalizada de opción múltiple basada en sus conocimientos formulada por DocuSign.

DocuSign: Autenticación vía comprobación de ID para eIDAS (AES/QES)

La persona 2 no necesita registrarse a DocuSign. Si se requiere una firma cualificada, la identificación por vídeo se realiza primero en el momento de la firma.

Pasos:

1. P2 indica a P1 su nombre y su dirección de correo electrónico.
2. P1 solicita la firma y transmite el nombre y la dirección de correo electrónico de P2 a DocuSign.
3. El P2 recibe un correo electrónico con un enlace al documento y se le pide que tome una foto de su documento de identidad emitido por el gobierno (es decir, licencia de conducir, pasaporte) o de su documento de identidad europeo, en el cuál se verifican las marcas de seguridad y marcas de agua y se verifica que el nombre en el documento de identidad coincida con el nombre en el contrato.

6 Licencia

Para utilizar el servicio de firmas DocuWare con Validated ID o DocuSign, debe firmar un contrato de servicio con uno de ellos. En función de si trabaja con DocuWare Cloud o con un sistema instalado localmente, necesita los siguientes elementos de licencia.

	DocuWare Cloud	Sistemas in situ
Servicio de firmas	Incluido	Se requiere licencia adicional *Electronic Signature Integration*
Licencias de clientes	El servicio de firmas requiere su propia licencia DocuWare Client	El servicio de firmas requiere su propia licencia DocuWare Client
Más licencias DocuWare	---	- Workflow Manager - Contrato de mantenimiento y asistencia válido
Volumen de firmas	Se debe adquirir adicionalmente del proveedor o, para ID validada, también de DocuWare	Se debe adquirir adicionalmente del proveedor o, para ID validada, también de DocuWare
Certificado de firma	Se debe adquirir adicionalmente	Se debe adquirir adicionalmente

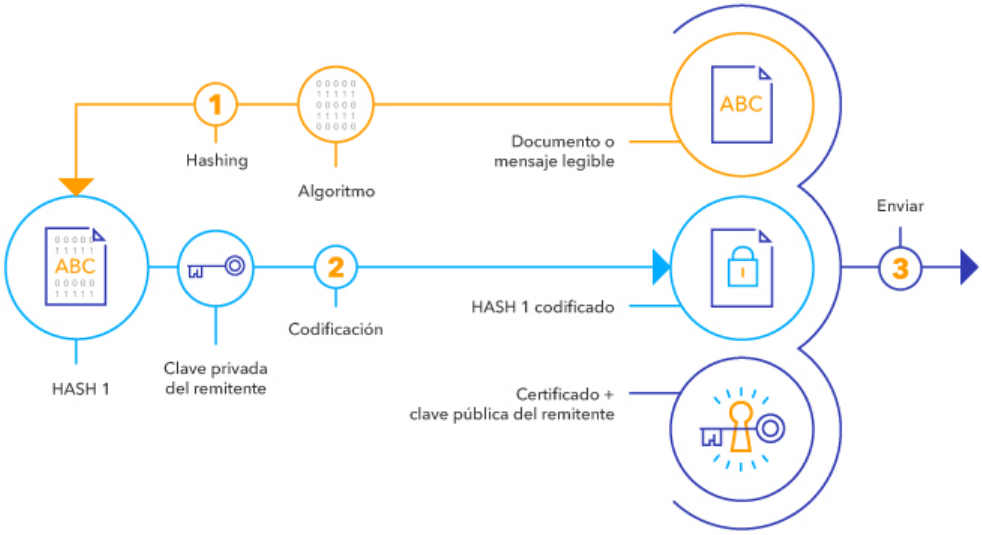
7 Qué ocurre técnicamente durante la firma electrónica

Cuando se añade una firma electrónica a un documento, el proceso implica algo más que añadir una firma al pie de un texto. La mayoría de los pasos tienen lugar entre bastidores, controlados por software.

En pocas palabras, toda tipo de firma electrónica consiste en datos que se añaden a un documento o archivo. Con la firma electrónica cualificada, estos datos añadidos son generados por módulos de seguridad de hardware (HSM) en un entorno técnico especialmente seguro. En las regiones con un sistema de regulación legal escalonado para las firmas entendidas como servicio de confianza, como en la UE, un organismo específicamente autorizado y cualificado para ello ha emitido también la prueba de identidad autentificada del firmante, el certificado digital.

La firma se lleva a cabo en lo que se conoce como infraestructura de clave pública, en la que se utiliza un procedimiento de cifrado con dos claves de software. Una es la privada, que solo conoce la autoridad responsable del cifrado, y otra es la pública. Esta última se proporciona junto con el documento en el certificado de firma para el destinatario.

El proceso consta de tres pasos:



1. **Cálculo del valor hash**
   Se utiliza una función matemática para calcular una suma de comprobación a partir de los datos del documento o archivo, que se denomina valor hash. Esto es como la huella digital del documento.
2. **Cifrado del valor hash**
   Este valor hash se cifra con la clave privada del firmante.
3. **Vínculo del valor hash cifrado + el certificado con el documento**
   El valor hash cifrado y el certificado se adjuntan al documento. El certificado contiene la clave pública para descifrar el valor hash, la información de que esta clave está asociada a la identidad del firmante y la validez del certificado.

8 Seguridad de los datos, protección de los datos y autenticación segura

Puede utilizar firmas en la nube como las que ofrece el servicio de firmas DocuWare con total independencia de si utiliza un sistema en la nube o in situ para su gestión de documentos y flujos de trabajo. El término «firma en la nube» solo describe que el servicio de firmas, al igual que DocuWare Cloud, está alojado en los centros de datos de Microsoft Azure. Tanto con las firmas en la nube como con el servicio de firmas DocuWare, trabajará con total seguridad y conforme a la ley con ambas soluciones.

Seguridad de los datos: proceso de firma en criptoprocesadores muy seguros

En el pasado, las empresas solo podían crear firmas electrónicas cualificadas si el hardware para ello (el dispositivo de creación de firmas) estaba bajo su control, es decir, el módulo criptográfico de hardware y la tarjeta inteligente y el lector de tarjetas necesarios.

Hoy en día, el dispositivo de creación de firmas seguro (SSCD, por sus siglas en inglés) puede estar ubicado en un proveedor de servicios de firmas, que almacena y aplica el certificado y las claves para el creador de la firma. Estos proveedores ofrecen una plataforma de firma en la nube muy segura a través de Internet, dentro de la cual empresas, organismos oficiales o particulares pueden firmar sus documentos.

El proceso de firma propiamente dicho tiene lugar en módulos de seguridad de hardware que el proveedor de servicios de firmas opera en una infraestructura de servidor en la nube segura. Los módulos de seguridad de hardware (HSM, por sus siglas en inglés) son criptoprocesadores especiales que garantizan la protección de las firmas y las claves de software.

Los proveedores de servicios de firmas con los que trabaja DocuWare utilizan HSM que cumplen la norma estadounidense FIPS 140-2 Nivel 3 para módulos criptográficos.

Protección de datos: los datos permanecen en su región

Los datos de firmas contienen datos personales y confidenciales. Por lo tanto, se debe garantizar que estos datos permanezcan en la región de protección de datos donde la ley de protección de datos sea aplicable, incluso durante el proceso de firma. Esto lo garantizan los proveedores de servicios de firmas con los que trabaja DocuWare.

Validated ID utiliza centros de datos altamente seguros en Irlanda y los Países Bajos, que están sujetos al Reglamento General de Protección de Datos (RGPD) europeo, y un centro de datos adicional en el Reino Unido para los clientes de ese país.

DocuSign utiliza varios centros de datos de alta seguridad tanto en Estados Unidos como en la UE para el servicio de firmas.

9 Cumplimiento normativo mediante firmas electrónicas en todo el mundo

Las firmas electrónicas son un medio establecido para proteger legalmente los documentos en todo el mundo. Sin embargo, los requisitos legales varían según las regiones y los países. Cada empresa debe aclarar los requisitos legales aplicables para las transacciones protegidas con firmas electrónicas.

Es importante distinguir entre el lugar de jurisdicción y la ley aplicable de acuerdo con el principio de libertad contractual. El *lugar de jurisdicción* es el lugar al que se puede recurrir al tribunal en caso de duda. La *ley aplicable* se refiere a la ley nacional bajo la cual se decidiría el documento en caso de litigio. La ley aplicable rige tanto el contenido del documento como sus firmas electrónicas.

Modelos legales para las firmas

Los modelos legales para firmas electrónicas van de menos a más regulados. Los requisitos están menos regulados en Norteamérica, donde se aceptan como legalmente seguras una serie de soluciones tecnológicas y niveles de seguridad. Los países de la Unión Europea, para los que el reglamento eIDAS constituye el marco legal, tienen una regulación media o escalonada. Solo unos pocos países tienen una regulación especialmente estricta o restrictiva.

Escasa regulación	Regulación escalonada	Regulación restrictiva
Estados Unidos Canadá Australia Nueva Zelanda	UE Japón China Corea del Sur	Brasil India Israel Malasia

Merece la pena centrarse en los dos modelos legales más utilizados: la escasa regulación y la regulación escalonada.

Escasa regulación

En Estados Unidos, Canadá, Australia y Nueva Zelanda, las firmas electrónicas son generalmente aceptadas y tienen el mismo efecto legal que las firmas manuales. Todos los tipos de firmas electrónicas son legales y ejecutables y se consideran equivalentes.

Ejemplo de EE. UU.

En Estados Unidos, las firmas electrónicas están legalmente permitidas y bien establecidas. La Uniform Electronic Transactions Act (UETA, Ley uniforme de transacciones electrónicas) de 1999 y la Electronic Signatures in Global and National Commerce Act (ESIGN, Ley de firmas electrónicas en el comercio internacional y nacional) del 2000 reconocen la validez y aplicabilidad de las firmas electrónicas. Ambas leyes prevén expresamente que no se puede negar la validez legal de una firma, contrato u otro registro en relación con una transacción comercial únicamente porque esté en formato electrónico.

Regulación escalonada

Ejemplo de la Unión Europea

El marco jurídico de las firmas electrónicas en la UE es el Reglamento eIDAS. Las siglas significan «Electronic IDentification, Authentication and Trust Services» (Servicios de identificación, autenticación y confianza electrónica»), en el mercado único europeo. El reglamento está en vigor desde 2016.

eIDAS ofrece un modelo jurídico escalonado para que las transacciones electrónicas sean más seguras, fiables y sencillas. Como reglamento de la UE, es una especie de ley europea y sustituye a las legislaciones nacionales de los Estados miembros de la UE. Cada Estado miembro de la UE tuvo que adaptar su legislación al contenido del reglamento. En Alemania, por ejemplo, el eIDAS se implementó, entre otras cosas, en la Ley alemana de servicios fiduciarios.

El eIDAS se aplica en todo el Espacio Económico Europeo (EEE), que incluye a Noruega, Islandia y Liechtenstein. Sin embargo, las empresas no europeas que hacen negocios con empresas de la UE también deberían considerar el eIDAS. Por ejemplo, muchas empresas estadounidenses tienen sucursales o clientes en la UE y, en este caso, también deben cumplir los requisitos del eIDAS.

El eIDAS distingue entre tres niveles de firma electrónica, que tienen diferentes pruebas documentales: la firma electrónica simple, la avanzada y la cualificada.

- **Simple: informal con bajo riesgo legal**
  Para muchos documentos utilizamos la firma electrónica simple. En un correo electrónico y en muchos contratos, basta con el nombre mecanografiado o la imagen de mapa de bits del nombre escrito a mano. No hay una forma específica exigida por la ley para estos documentos y hay poco riesgo de que se cuestione su validez legal. Con DocuWare, puede proporcionar una firma electrónica simple con un sello.
- **Avanzada: riesgo jurídico medio**
  En caso de litigio en el que deba ser posible identificar al firmante de un documento o al creador de la firma, necesita una firma electrónica avanzada. Se utiliza mucho para los contratos comerciales en el sector B2B. El eIDAS prescribe ciertas normas para este nivel de firma, como que el creador de la firma se debe identificar mediante un certificado de firma electrónica. La firma avanzada tiene un nivel de prueba documental medio.
- **Cualificada: máxima seguridad**
  Por ejemplo, para algunos documentos, como determinados contratos, la legislación alemana exige una firma manuscrita. En estos casos, se utiliza la firma electrónica cualificada, que, salvo excepciones, equivale a la firma manuscrita en los tribunales y tiene el máximo nivel de prueba documental.

Las firmas electrónicas avanzadas pueden ser aceptadas por otros Estados miembros de la UE, mientras que las cualificadas deben ser aceptadas en toda la UE. Sin embargo, cada Estado miembro regula por sí mismo si una transacción comercial u oficial requiere una firma electrónica y el nivel en que debe proporcionarse.

Los certificados cualificados los proporcionan los proveedores de servicios de confianza (VDA), que deben cumplir requisitos de seguridad especiales para este fin. Estos proveedores han recibido el estatus de cualificados tras una auditoría oficial por parte de

una autoridad nacional y están incluidos en la lista de la UE de Listas de Confianza eIDAS (LOTL).

Ejemplo de Japón

Japón también tiene un modelo legal escalonado para la regulación de las firmas electrónicas. Desde abril de 2001 está en vigor la Ley japonesa de firmas electrónicas y negocios de certificación (Ley n.º 102 de 31 de mayo del 2000), según la cual una firma electrónica cualificada se considera una firma electrónica legalmente válida. La firma electrónica avanzada es posible, pero por sí sola tiene un menor nivel de prueba documental.

DocuWare es compatible con todos los escenarios y requisitos legales

Con el servicio de firmas DocuWare, puede utilizar las firmas electrónicas de forma eficiente en su empresa y garantizar un mayor cumplimiento normativo. En colaboración con los proveedores de servicios de firmas Validated ID y DocuSign, DocuWare le ofrece una amplia gama de procedimientos seguros para este fin.

Compruebe qué documentos necesitan un nivel de cumplimiento normativo y cuál es este nivel de acuerdo con los requisitos legales. A partir de ahí, decida cuál de las muchas opciones de firma quiere utilizar.