Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

TOMO 1

De la rúbrica a la firma digital.

Historia, fundamentos, dispositivos y doctrinas de la firma electrónica, y cómo nacieron las plataformas que hoy coordinan quién firma, en qué orden y con qué prueba.



Primera edición · Montevideo, 2026

Interfase

Rúbrica. Cuadernos sobre firma, identidad y confianza digital
Tomo 1. De la rúbrica a la firma digital

Primera edición, octubre de 2026.
Montevideo, Uruguay.

Este libro es una obra de divulgación. Describe principios técnicos y jurídicos de alcance general y no constituye asesoramiento legal. La validez de una firma en un caso concreto depende de la legislación aplicable, del tipo de acto y de la prueba disponible; ante una decisión, consulte a un profesional habilitado en la jurisdicción que corresponda.

Las referencias a normas, organismos y empresas se hacen con fines históricos y didácticos. Las marcas mencionadas pertenecen a sus titulares.

Compuesto en Figtree y JetBrains Mono, ambas bajo licencia SIL Open Font License.

RÚBRICA · TOMO 1

De la rúbrica a la firma digital

Una introducción al mundo de la firma electrónica: de dónde viene, cómo funciona y hacia dónde va.

CONTENIDO

Índice

	Prólogo	5
01	Qué es firmar	7
02	Una historia breve	11
03	El vocabulario	17
04	Cómo funciona por dentro	23
05	Los dispositivos de firma	29
06	Las doctrinas	35
07	Usos y sectores	41
08	Ventajas y límites	45
09	Del documento al proceso	49
10	Anatomía de una plataforma	55
11	Lo que viene	63
	Glosario	67
	Para seguir leyendo	71

ANTES DE EMPEZAR

Por qué esta serie

Firmar es uno de los gestos más antiguos y más cargados de sentido que conocemos. Este libro cuenta cómo ese gesto se volvió matemática, ley e infraestructura sin perder su propósito.

Cada día se firman millones de documentos sin papel. Un préstamo se aprueba desde un teléfono, un contrato de trabajo se acepta en una pausa del almuerzo, un acta de directorio se cierra con firmantes repartidos en tres países. Para quien firma, la experiencia suele reducirse a un botón. Detrás de ese botón, sin embargo, hay cinco décadas de criptografía, tres décadas de legislación y una industria entera dedicada a que la firma valga lo mismo hoy que dentro de veinte años.

Esa industria tiene un vocabulario propio que confunde incluso a quienes trabajan en ella. Se habla de firma electrónica y de firma digital como si fueran lo mismo, y no lo son. Se habla de firma avanzada, de firma cualificada, de sello de tiempo, de prestador de servicios de confianza, de validación a largo plazo. Se mezclan conceptos jurídicos con conceptos técnicos, y conceptos de producto con ambos. El resultado es que muchas decisiones importantes, como qué tipo de firma exigir para un acto o cómo conservar la prueba de que alguien firmó, se toman sin un mapa claro.

Esta serie quiere ofrecer ese mapa. Está pensada para lectores con curiosidad y sin formación previa en criptografía ni en derecho: responsables de procesos, abogados que quieren entender la técnica, técnicos que quieren entender la ley, estudiantes y equipos que deben elegir, implantar u operar una solución de firma. Cuando un concepto exige precisión, lo explicamos con precisión; cuando una explicación exige fórmulas, preferimos una imagen.

Cómo está organizada

La serie se compone de tres tomos que pueden leerse por separado, aunque se apoyan entre sí.

- **Tomo 1. De la rúbrica a la firma digital.** El que tiene en sus manos. Recorre la historia de la firma, el vocabulario básico, el funcionamiento de la firma digital, los dispositivos que guardan las claves, las doctrinas jurídicas que la reconocen, sus usos, sus ventajas y sus límites, y el nacimiento de las plataformas que coordinan procesos de firma.
- **Tomo 2. La prueba que perdura.** Se ocupa de lo que pasa después de firmar: formatos y niveles de firma, sellos de tiempo, validación, listas de confianza, conservación a largo plazo y registros de evidencia.
- **Tomo 3. Orquestar la firma.** Trata del diseño de procesos de firma, de la identidad de quien firma, de la integración con otros sistemas y de la operación de estas plataformas a escala, con una mirada sobre la inteligencia artificial y la criptografía del futuro.

Una advertencia y una promesa

La advertencia: este no es un libro de derecho ni un manual de cumplimiento. Las leyes cambian y cada jurisdicción tiene sus matices. Citamos normas para explicar ideas, no para dar consejo sobre un caso concreto.

La promesa: al terminar este tomo, el lector podrá distinguir los tipos de firma, entender qué ocurre cuando alguien firma un documento electrónico, saber qué preguntas hacer ante una solución de firma y por qué esas preguntas importan. Si además encuentra en la historia de la firma algo de la fascinación que nos llevó a escribir sobre ella, mejor todavía.

SOBRE EL NOMBRE

La palabra *rúbrica* viene del latín *rubrica*, la tierra roja con que se escribían en rojo los títulos de las leyes. Con el tiempo pasó a nombrar el trazo personal que acompaña a una firma manuscrita y que la vuelve difícil de imitar. Nos pareció un buen nombre para una serie que habla de cómo ese trazo personal encontró su equivalente en el mundo digital.

01

CAPÍTULO UNO

Qué es firmar.

Antes de hablar de claves y certificados conviene detenerse en una pregunta simple: qué hace exactamente una firma. La respuesta explica casi todo lo que vendrá después.

Una firma no es un dibujo. Es un acto. Cuando alguien escribe su nombre al pie de un contrato, no está decorando el papel: está diciendo, frente a otros y frente a sí mismo, que ese texto lo compromete. La tinta es el soporte; el compromiso es lo que importa.

Esta distinción entre el soporte y el acto es la llave que permitió, a fines del siglo veinte, que el derecho aceptara firmas que no usan tinta. Si la firma vale por lo que hace y no por cómo se ve, cualquier mecanismo que haga lo mismo puede, en principio, valer lo mismo. A esa idea los juristas la llaman *equivalencia funcional*, y volveremos a ella en el capítulo seis. Para entenderla primero hay que precisar cuáles son esas funciones.

Las cinco funciones de una firma

La doctrina y los organismos internacionales que estudiaron el tema, en especial la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI, más conocida por su sigla inglesa UNCITRAL), coinciden en que una firma cumple varias funciones a la vez. Las agrupamos en cinco.



FIGURA 1 Las cinco funciones de una firma. Cualquier mecanismo, en papel o electrónico, puede evaluarse según cuánto cumple cada una.

Identificar a quien firma

La firma vincula el documento con una persona determinada. En el papel esa vinculación es indirecta: la firma manuscrita no dice quién es su autor, sino que permite compararla con otras firmas conocidas de esa persona. En el mundo electrónico la identificación puede ser mucho más fuerte, porque puede apoyarse en un documento de identidad verificado, en un certificado emitido por una entidad de confianza o en una combinación de factores.

Expresar la voluntad

Firmar significa aprobar, aceptar, reconocer o comprometerse. La firma es la manifestación de una voluntad sobre un contenido concreto. Por eso importa tanto que quien firma sepa qué está firmando, que haya podido leerlo y que el acto de firmar sea deliberado y no accidental. Un botón que dice «Aceptar» en letra pequeña no expresa la misma voluntad que una pantalla que muestra el documento completo y pide confirmación explícita.

Proteger la integridad del contenido

Una firma al pie de la última página no impide que alguien cambie la segunda. En el papel esa debilidad se compensa con iniciales en cada hoja, sellos de lacre, papel con marcas de agua o la intervención de un notario. La firma digital, como veremos, resuelve esto de raíz: cualquier cambio en el documento, aunque sea una coma, se detecta.

Darle solemnidad al acto

El gesto de firmar obliga a detenerse. Esa pausa tiene valor jurídico y psicológico: advierte a quien firma que está por asumir una obligación. Algunos actos especialmente graves, como un testamento o la compraventa de un inmueble en muchas jurisdicciones, exigen además formalidades adicionales precisamente para reforzar esa advertencia.

Dejar prueba

Finalmente, la firma sirve para demostrar después que el acto ocurrió. Esta es quizá la función que más ha cambiado con la tecnología. Una firma manuscrita prueba poco por sí sola: ante una disputa hace falta un perito calígrafo. Una firma electrónica bien construida puede venir acompañada de un registro detallado de quién accedió al documento, cuándo, desde dónde, cómo se identificó y qué versión exacta firmó.

PARA RECORDAR

Una firma **identifica**, **expresa voluntad**, **protege la integridad**, **advierte** y **prueba**. Cualquier mecanismo de firma, en papel o electrónico, puede evaluarse preguntando qué tan bien cumple cada una de estas cinco funciones.

Firmar no es lo mismo que autenticarse

Una confusión frecuente es pensar que iniciar sesión en un sistema equivale a firmar. No es así. Autenticarse es demostrar quién soy para obtener acceso; firmar es comprometerme con un contenido. Puedo autenticarme en mi banco cien veces por mes sin firmar nada, y puedo firmar un documento que me envían sin tener cuenta en ningún sistema.

La diferencia importa porque muchos procesos mezclan ambas cosas. Un sistema puede pedir al firmante que se autentique con un código enviado al teléfono y luego registrar su conformidad con un clic. En ese caso la autenticación aporta identificación, el clic aporta voluntad, y el sistema debe encargarse de aportar integridad y prueba. Cuando alguna de las piezas falta, la firma resultante es más débil, aunque la pantalla se vea igual.

Firmar no es lo mismo que sellar

En el papel, las organizaciones usan sellos: el sello de una oficina pública, el timbre de una empresa, el sello fechador de una mesa de entradas. Un sello no expresa la voluntad de una persona, sino que da fe de que un documento proviene de una organización o de que fue recibido en cierto momento.

El mundo electrónico conserva esa distinción. Existe la *firma electrónica*, que corresponde a una persona física, y existe el *sello de organización* (en el reglamento europeo, «sello electrónico»), que corresponde a una persona jurídica y garantiza el origen y la integridad de un documento emitido por ella. Existe además el *sello de tiempo*, que no identifica a nadie y sólo prueba que un documento existía en un momento determinado. Los tres usan técnicas parecidas y cumplen funciones distintas. Los iremos encontrando a lo largo de la serie.

Por qué la firma necesitó reinventarse

Durante siglos, la combinación de papel, tinta y testigos fue suficiente. El documento viajaba físicamente, las partes solían conocerse y las disputas se resolvían con peritos y declaraciones. Tres cambios rompieron ese equilibrio.

1. **La distancia.** El comercio a distancia, primero por correo, luego por telégrafo, fax y finalmente por redes, separó a las partes. Firmar en papel y enviar el original se volvió lento y caro.
2. **El volumen.** Bancos, aseguradoras, administraciones públicas y empleadores pasaron a gestionar millones de documentos. Cada firma en papel implica imprimir, enviar, recibir, escanear y archivar.
3. **La desmaterialización.** Cuando los documentos nacen, viven y se archivan en formato electrónico, imprimirlos sólo para firmarlos es un contrasentido. Y una firma escaneada pegada en un PDF no cumple casi ninguna de las cinco funciones: se copia con dos clics.

La firma electrónica nació para resolver esos tres problemas sin renunciar a las cinco funciones. Cómo lo logró, y cuánto le costó a la técnica y al derecho ponerse de acuerdo, es lo que cuentan los capítulos siguientes.

02

CAPÍTULO DOS

De la arcilla al algoritmo.

Una historia breve de la firma: cinco mil años de sellos, trazos y testigos, y cincuenta años en que la matemática encontró la manera de reemplazarlos.

Sellos antes que nombres

Mucho antes de que la mayoría de las personas supiera escribir, ya existía la necesidad de marcar un objeto o un acuerdo como propio. En la Mesopotamia del cuarto milenio antes de nuestra era se usaban sellos cilíndricos de piedra tallada que, al rodar sobre la arcilla húmeda, dejaban una imagen única. Esos sellos cerraban recipientes, autenticaban tablillas con contratos y acompañaban a sus dueños hasta la tumba. La idea esencial ya estaba ahí: una marca difícil de reproducir, asociada a una persona, aplicada sobre el soporte del acuerdo.

Egipcios, griegos y romanos heredaron y refinaron la práctica. En Roma se difundió el anillo sigilar, con el que se imprimía un emblema personal sobre cera para cerrar cartas y documentos. Romper el sello era la prueba visible de que alguien había abierto el mensaje. Integridad y autoría, dos de las cinco funciones, resueltas con un objeto que cabía en un dedo.

La firma manuscrita y la rúbrica

La firma escrita con el propio nombre se generalizó mucho más tarde, a medida que se extendía la alfabetización. En la Europa medieval convivían varias formas: el sello de cera de nobles y obispos, la cruz trazada por quien no sabía escribir, a menudo

acompañada por testigos, y el signo de los notarios, un dibujo elaborado y personal que cada escribano registraba al recibir su oficio y que debía reproducir en cada documento que autorizaba.

De esa tradición proviene la rúbrica de los países hispanos: un trazo personal, a veces más importante que el nombre mismo, que vuelve a la firma difícil de imitar. La palabra conserva la memoria de su origen. Los títulos de las leyes y de los capítulos de los libros jurídicos se escribían con tinta roja, *rubrica* en latín, y el término pasó a designar primero el epígrafe y después el signo distintivo que se añade a la firma.

Con la imprenta y el crecimiento del comercio, la firma manuscrita se volvió el mecanismo dominante. Algunas normas la hicieron obligatoria para ciertos actos. El Estatuto de Fraudes inglés de 1677, por ejemplo, exigió que determinados contratos constaran por escrito y estuvieran firmados para poder reclamarse ante un tribunal. Muchos ordenamientos posteriores siguieron un camino parecido y reforzaron el binomio de documento escrito y firma manuscrita como prueba por excelencia.

El telégrafo pone a prueba al derecho

El primer gran desafío llegó en el siglo diecinueve con el telégrafo. Si un comerciante aceptaba una oferta por telegrama, ¿había firmado? El mensaje llegaba escrito por un operador desconocido, a cientos de kilómetros del autor. Los tribunales de varios países tuvieron que responder la pregunta. Uno de los razonamientos más citados es el de un tribunal de New Hampshire en 1869, que sostuvo, en sustancia, que no hacía diferencia si el operador escribía la aceptación con una pluma de acero de una pulgada o con un hilo de cobre de mil millas. Lo que importaba era la voluntad del autor, no el instrumento.

Ese argumento es, en germen, la equivalencia funcional que adoptaría el derecho más de un siglo después. Lo mismo ocurrió con el télex y con el fax: cada nueva tecnología obligó a los jueces a preguntarse si el mecanismo cumplía las funciones de la firma, y cada vez la respuesta dependió más de la prueba disponible que de la forma.

La revolución de la clave pública

El problema de fondo seguía sin resolverse. Un telegrama o un fax podían falsificarse con relativa facilidad, y nada en ellos permitía detectar una alteración. Hacía falta un mecanismo que vinculara de manera verificable un contenido con su autor. La

respuesta llegó desde la criptografía.

En 1976, los investigadores Whitfield Diffie y Martin Hellman publicaron un artículo titulado *New Directions in Cryptography* que cambió la disciplina. Propusieron la idea de la criptografía de clave pública: un sistema en el que cada persona tiene dos claves relacionadas, una privada que guarda en secreto y otra pública que puede compartir con cualquiera. Entre las aplicaciones que imaginaron estaba exactamente la que nos ocupa: una firma que sólo el titular de la clave privada podría producir y que cualquiera podría verificar con la clave pública.

Al año siguiente, Ron Rivest, Adi Shamir y Leonard Adleman, del Instituto Tecnológico de Massachusetts, presentaron el algoritmo RSA, que hizo práctica esa idea. Años más tarde se supo que investigadores de la agencia de inteligencia británica habían llegado a conclusiones similares a principios de los setenta, pero su trabajo permaneció en secreto hasta 1997. La firma digital, tal como la conocemos, nació en esos años.



FIGURA 2 Algunos hitos en la historia de la firma, presentados al modo de un registro de evidencia.

De la idea a la infraestructura

Una firma digital resuelve el vínculo entre un contenido y una clave. Pero ¿cómo saber a quién pertenece una clave pública? Si un impostor genera un par de claves y lo presenta como propio de otra persona, la matemática no lo detecta. Hacía falta una

manera confiable de asociar claves con identidades.

La solución fue el *certificado digital*: un documento electrónico, firmado por una entidad de confianza llamada autoridad de certificación, que declara que cierta clave pública pertenece a cierta persona. En 1988 la Unión Internacional de Telecomunicaciones publicó la norma X.509, que define el formato de esos certificados y que, con sucesivas revisiones, sigue siendo la base de la infraestructura de clave pública mundial. Cada vez que un navegador muestra un candado junto a una dirección web, está usando certificados X.509.

Durante los noventa se sumaron las piezas que faltaban: algoritmos estandarizados de firma, funciones de resumen criptográfico cada vez más robustas, protocolos para consultar si un certificado fue revocado y, hacia el final de la década, sellos de tiempo emitidos por terceros de confianza. También aparecieron los primeros formatos para firmar documentos de oficina. Hacia el año 2000 el formato PDF incorporó firmas digitales embebidas en el propio archivo, lo que permitió que un documento firmado pudiera verse, imprimirse y verificarse con un lector corriente.

Las leyes llegan a la cita

La técnica estaba lista antes que el derecho. La primera ley específica sobre firma digital fue la del estado de Utah, en los Estados Unidos, en 1995. Era una ley muy detallada, que regulaba la infraestructura de certificación casi como un reglamento técnico. Le siguieron normas en Alemania e Italia en 1997, también con un enfoque marcadamente tecnológico.

En 1996 la UNCITRAL aprobó su Ley Modelo sobre Comercio Electrónico, y en 2001 una Ley Modelo específica sobre Firmas Electrónicas. Su aporte fue conceptual: en lugar de prescribir una tecnología, establecieron principios generales, como la equivalencia funcional y la neutralidad tecnológica, que cualquier país podía adoptar. Esas leyes modelo inspiraron buena parte de la legislación latinoamericana.

La Unión Europea aprobó en 1999 una directiva sobre firma electrónica que introdujo la distinción entre firma electrónica y firma electrónica avanzada, y la idea de certificados reconocidos. En los Estados Unidos, la ley federal conocida como ESIGN, del año 2000, optó por un enfoque mínimo: declaró que no se puede negar validez a una firma o a un contrato por el solo hecho de ser electrónicos, sin exigir una tecnología concreta.

En América Latina el movimiento fue rápido. Colombia legisló en 1999, Argentina y Brasil en 2001, Chile en 2002. Uruguay aprobó en 2009 su ley de documento electrónico y firma electrónica, que creó además la unidad pública encargada de acreditar a los prestadores de servicios de certificación. Paraguay lo hizo en 2010 y modernizó su régimen en 2021. Cada país eligió su propia combinación de enfoques, y esa diversidad es uno de los desafíos que veremos en el capítulo seis.

De la directiva al reglamento, y del reglamento a la cartera

La experiencia europea mostró que una directiva, que cada país transpone a su manera, generaba fragmentación: una firma válida en un Estado podía tener dificultades para ser reconocida en otro. En 2014 la Unión Europea aprobó el Reglamento 910/2014, conocido como eIDAS, aplicable desde 2016 de manera uniforme en todos los Estados miembros. eIDAS consolidó tres niveles de firma, creó para las personas jurídicas el sello de organización, al que el texto llama «sello electrónico», reguló los servicios de confianza y estableció listas oficiales de prestadores cualificados.

En 2024 se aprobó su reforma, el Reglamento 2024/1183, que suele llamarse eIDAS 2. Su novedad principal es la cartera europea de identidad digital: una aplicación que cada ciudadano podrá llevar en su teléfono para identificarse, presentar credenciales y firmar con nivel cualificado. Los Estados miembros deben ofrecer al menos una de esas carteras hacia fines de 2026. Es un cambio de fondo en la manera de firmar.

Del documento al proceso

Mientras los legisladores debatían, el mercado encontró otra necesidad. Firmar un documento era posible; coordinar a varias personas que debían firmarlo, en cierto orden, con recordatorios y con un registro de todo lo ocurrido, era otra cosa. A comienzos de los dos mil surgieron empresas dedicadas precisamente a eso: enviar un documento a uno o más firmantes por correo electrónico, guiarlos para que firmaran en el lugar correcto y devolver al remitente el documento firmado con un certificado de lo ocurrido. Así nacieron los gestores de flujos de firma, a los que dedicamos el capítulo nueve.

> Cada tecnología de comunicación obligó a preguntarse de nuevo qué es una firma. La respuesta fue siempre la misma: lo que importa es la voluntad y la prueba, no el instrumento.

03

CAPÍTULO TRES

Electrónica, digital, avanzada.

Las palabras de la firma se usan con ligereza y casi nunca significan lo mismo para un abogado, un ingeniero y un vendedor. Este capítulo fija un vocabulario común.

Pocas áreas del conocimiento tienen tantos términos parecidos con significados distintos. Firma electrónica, firma digital, firma electrónica avanzada, firma cualificada, firma calificada, firma reconocida, certificado reconocido, certificado cualificado. Algunas diferencias son de fondo y otras son sólo de traducción o de país. Separarlas es el primer paso para no tomar decisiones equivocadas.

Firma electrónica: el concepto jurídico amplio

Firma electrónica es el término más general. En la mayoría de las legislaciones designa cualquier dato en formato electrónico que se asocia a otros datos electrónicos y que una persona usa para firmar. La definición es deliberadamente amplia. Entran en ella un nombre escrito al pie de un correo, una imagen de la firma manuscrita pegada en un documento, la marca de una casilla que dice «Acepto», un trazo hecho con el dedo sobre una pantalla, un código recibido por mensaje de texto y, por supuesto, una firma criptográfica con certificado.

Que todas esas formas sean firmas electrónicas no significa que todas valgan lo mismo. Significa que ninguna puede ser descartada por el solo hecho de ser electrónica. Su peso como prueba dependerá de cuánto cumplan las cinco funciones del capítulo uno, y eso es algo que, ante una disputa, evaluará un juez.

Firma digital: el concepto técnico

Firma digital, en sentido estricto, designa una técnica: la firma basada en criptografía de clave pública que describiremos en el capítulo cuatro. Es un mecanismo matemático que vincula un contenido con una clave privada y permite detectar cualquier alteración.

La confusión nace porque algunos países usan «firma digital» como categoría jurídica. En la legislación argentina, por ejemplo, la firma digital es la que cumple ciertos requisitos técnicos y se apoya en un certificado emitido por un certificador licenciado, y goza de presunciones que la firma electrónica común no tiene. En otros países la expresión no aparece en la ley y se usa sólo en el lenguaje técnico. Conviene, por eso, preguntar siempre en qué sentido se está usando.

ATENCIÓN CON LA TRADUCCIÓN

El reglamento europeo usa en castellano el término **cualificada**; buena parte de América Latina dice **calificada** o **reconocida**; el inglés dice **qualified**. Son la misma idea con distinto vestido. Lo que no es lo mismo es «digital» como técnica y «digital» como categoría legal.

Los tres niveles

El modelo que más se ha extendido en el mundo, consolidado por el reglamento europeo eIDAS, distingue tres niveles de firma electrónica, y cada uno incluye al anterior y le suma requisitos. Brasil adoptó esos mismos tres niveles; Uruguay, Paraguay y otros países adoptaron variantes con dos, una firma común y una de nivel superior basada en un certificado de un prestador acreditado.



FIGURA 3 Los tres niveles de firma electrónica del modelo europeo, adoptado con variantes en otros países. Cada nivel incluye los requisitos del anterior; en color, lo que agrega.

Firma electrónica simple

Es la categoría básica. No exige requisitos técnicos particulares. Su ventaja es la facilidad: cualquiera puede firmar sin dispositivos ni certificados. Su debilidad es probatoria: si la firma se impugna, quien la invoca debe demostrar que efectivamente la hizo la persona señalada y que el documento no cambió. Para muchos actos cotidianos, como aceptar un presupuesto, aprobar una orden de compra o confirmar una reserva, ese nivel es suficiente, sobre todo si viene acompañado de un buen registro de evidencia.

Firma electrónica avanzada

El reglamento eIDAS, en su artículo 26, le exige cuatro condiciones que conviene leer con atención porque se repiten, con palabras parecidas, en muchas leyes:

1. estar vinculada al firmante de manera única;
2. permitir la identificación del firmante;
3. haber sido creada con datos de creación de firma que el firmante puede usar, con un alto nivel de confianza, bajo su exclusivo control;

4. estar vinculada con los datos firmados de modo tal que cualquier modificación ulterior sea detectable.

La cuarta condición, en la práctica, sólo la cumple la criptografía. La tercera es la más debatida: qué significa «exclusivo control» cuando la clave no está en un objeto que el firmante tiene en la mano, sino en un servidor remoto. Volveremos sobre esto en el capítulo cinco.

Firma electrónica cualificada

Es una firma avanzada que además se crea con un dispositivo cualificado de creación de firma y se basa en un certificado cualificado, emitido por un prestador de servicios de confianza que fue evaluado y figura en una lista oficial. Su efecto jurídico es el más fuerte: en la Unión Europea, el artículo 25 de eIDAS le otorga un efecto equivalente al de la firma manuscrita, y una firma cualificada emitida en un Estado miembro debe ser reconocida en todos los demás.

En varios países latinoamericanos la categoría superior recibe otros nombres, como firma digital, firma electrónica avanzada con certificado reconocido o firma calificada, y los requisitos varían en el detalle. La lógica es la misma: un certificado emitido por un prestador acreditado ante una autoridad pública, una clave protegida por un dispositivo evaluado y un efecto jurídico reforzado, con frecuencia expresado como presunción de autoría e integridad.

Las otras piezas del vocabulario

TÉRMINO	QUÉ ES
Certificado digital	Documento electrónico, firmado por una autoridad de certificación, que vincula una clave pública con la identidad de su titular durante un período de validez.
Autoridad de certificación	Entidad que verifica identidades y emite certificados. Cuando está acreditada o supervisada por un organismo público, suele llamarse prestador de servicios de certificación o de confianza.
Prestador de servicios de confianza	Término del reglamento europeo, hoy adoptado en otras regiones, para quien presta servicios como emisión de certificados, sellos de tiempo, validación o conservación de firmas. Si cumple requisitos reforzados y figura en la lista oficial, es *cualificado*.
«Sello electrónico» (sello de organización)	Equivalente de la firma para una persona jurídica. Garantiza el origen y la integridad de un documento emitido por una organización, sin expresar la voluntad de una persona física.
Sello de tiempo	Prueba emitida por un tercero de confianza de que un dato existía en un momento determinado. No identifica a nadie; fija una fecha y hora verificables.
Validación	Proceso de comprobar que una firma es auténtica, que el documento no cambió y que el certificado era válido en el momento de firmar.
Lista de confianza	Lista oficial, publicada y firmada por una autoridad, de los prestadores de servicios de confianza supervisados y de los servicios que prestan.

Una regla práctica

Ante cualquier proceso que requiera firma conviene hacerse tres preguntas, en este orden. Primero, qué exige la ley para ese acto: algunos actos admiten cualquier firma electrónica, otros exigen el nivel superior y otros todavía requieren papel o intervención notarial. Segundo, qué riesgo de disputa tiene: un contrato de alto valor o con una

parte que podría negar haber firmado justifica un nivel más alto que una autorización interna. Tercero, qué experiencia puede soportar quien firma: exigir un dispositivo físico a un cliente ocasional puede hacer que el proceso no se complete nunca.

La respuesta casi nunca es «siempre el nivel más alto». Es el nivel adecuado para cada acto, combinado con la mejor evidencia posible. Las plataformas modernas, como veremos, permiten mezclar niveles dentro de un mismo proceso: un aprobador interno con firma simple, un cliente con firma avanzada y un apoderado con firma cualificada, todos sobre el mismo documento.

04

CAPÍTULO CUATRO

Cómo funciona por dentro.

La firma digital descansa sobre tres ideas: un resumen que cambia con cualquier alteración, un par de claves que sólo funcionan juntas y un certificado que dice a quién pertenecen. No hacen falta fórmulas para entenderlas.

Primera idea: la huella del documento

Una *función de resumen criptográfico*, llamada también función hash, toma un contenido de cualquier tamaño, sea una frase o un contrato de doscientas páginas, y produce una cadena corta de longitud fija. Esa cadena funciona como una huella digital del contenido. Las funciones que se usan hoy en firma, como SHA256, tienen tres propiedades que las hacen útiles.

- **Son deterministas.** El mismo contenido produce siempre la misma huella.
- **Son sensibles al mínimo cambio.** Alterar un solo carácter produce una huella completamente distinta, sin parecido alguno con la anterior.
- **Son de un solo sentido.** A partir de la huella no se puede reconstruir el contenido, y es prácticamente imposible encontrar dos contenidos distintos con la misma huella.

El siguiente ejemplo muestra la segunda propiedad. Las dos frases difieren en un solo cero.

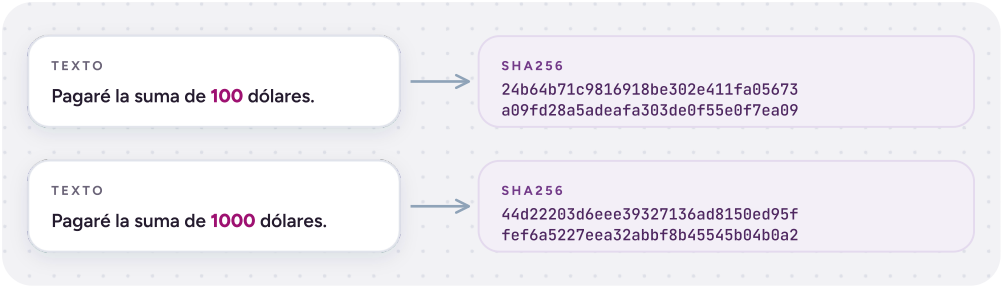


FIGURA 4 Un solo carácter de diferencia produce huellas sin ningún parecido. Los valores son reales: pueden recalcularse con cualquier herramienta SHA256.

La consecuencia es poderosa: para saber si un documento cambió no hace falta compararlo palabra por palabra con el original. Basta con comparar sus huellas.

Segunda idea: dos claves que se complementan

La criptografía de clave pública usa pares de claves matemáticamente relacionadas. Lo que una clave hace, sólo la otra puede comprobarlo. La clave privada queda en poder exclusivo de su titular y nunca se comparte. La clave pública puede publicarse sin riesgo, porque a partir de ella no es posible deducir la privada en un tiempo razonable.

Firmar un documento consiste, en términos simplificados, en dos pasos. Primero se calcula la huella del documento. Después se aplica a esa huella una operación que sólo puede realizar quien posee la clave privada. El resultado es la firma: un bloque de datos que se adjunta al documento.

Verificar la firma también tiene dos pasos. Quien recibe el documento calcula por su cuenta la huella del contenido que tiene delante. Luego usa la clave pública del firmante para comprobar que la firma corresponde exactamente a esa huella. Si el documento cambió, aunque sea una coma, las huellas no coinciden y la verificación falla. Si la firma se hizo con otra clave privada, también falla.

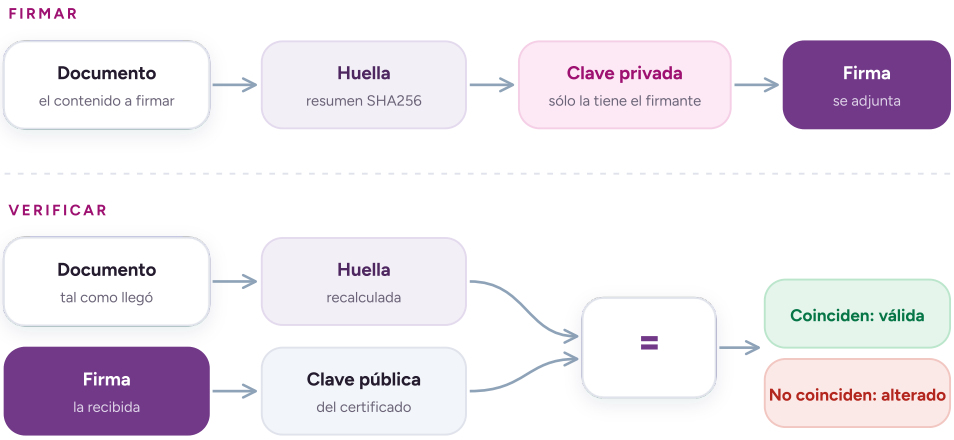


FIGURA 5 Firmar y verificar. Quien firma usa su clave privada sobre la huella; quien verifica recalcula la huella y la compara usando la clave pública.

UN MATIZ TÉCNICO

Suele explicarse la firma como «cifrar la huella con la clave privada». La imagen es útil y se ajusta bastante bien al algoritmo RSA, pero no describe con exactitud a otros algoritmos muy usados, como los basados en curvas elípticas, que producen la firma por otro camino. Lo que todos comparten es el resultado: sólo la clave privada produce la firma y cualquiera con la clave pública puede comprobarla.

Tercera idea: el certificado

La matemática garantiza que una firma fue producida por cierta clave privada. No dice de quién es esa clave. Para eso existe el certificado digital, que es, en esencia, una declaración firmada por una autoridad de certificación: «esta clave pública pertenece a esta persona, y esta declaración es válida entre tal y tal fecha».

Un certificado contiene, entre otros datos, el nombre del titular y a menudo un identificador como su número de documento, la clave pública, el nombre de la autoridad que lo emitió, las fechas de validez, los usos permitidos de la clave y las

direcciones donde consultar si fue revocado. Todo eso está firmado por la autoridad, de modo que nadie puede alterar el certificado sin que se note.

La cadena de confianza

¿Y por qué confiar en la autoridad? Porque su propio certificado fue firmado por otra autoridad de nivel superior, y así sucesivamente hasta llegar a una *raíz*: un certificado que se firma a sí mismo y en el que se confía por una decisión explícita. Esa decisión la toma un sistema operativo, un navegador, un lector de PDF o, en el caso de la firma con efectos jurídicos, un organismo público que publica la lista de autoridades reconocidas.

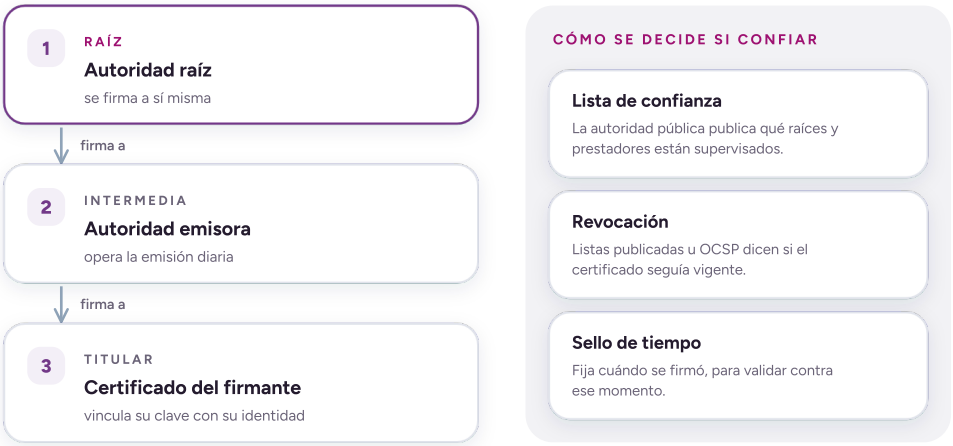


FIGURA 6 La cadena de confianza. Cada certificado está firmado por el de arriba; la raíz se acepta por decisión explícita, a menudo porque figura en una lista oficial.

Cuando un certificado deja de valer

Un certificado puede perder validez antes de su fecha de vencimiento. El titular puede haber perdido su tarjeta, la clave pudo verse comprometida o los datos del titular pudieron cambiar. En esos casos la autoridad revoca el certificado y lo informa por dos vías principales: listas de certificados revocados que se publican periódicamente, y un servicio de consulta en línea, el protocolo OCSP, que responde en el momento si un certificado concreto está vigente.

Para quien valida una firma, la pregunta relevante no es si el certificado está vigente hoy, sino si lo estaba en el momento de firmar. Responderla años después exige haber guardado la información de revocación de entonces y saber con certeza cuándo se firmó. De ahí la importancia de la cuarta pieza.

Cuarta pieza: el tiempo

La hora que marca el reloj de la computadora de quien firma no prueba nada: cualquiera puede cambiarla. Para fijar el momento de una firma de manera verificable se recurre a una *autoridad de sellado de tiempo*, un tercero de confianza que recibe la huella de un documento o de una firma, le añade la fecha y hora de un reloj confiable y firma el conjunto. El protocolo más difundido para esto se definió en 2001 en el documento RFC 3161 del organismo que estandariza los protocolos de internet.

Un sello de tiempo permite afirmar que la firma existía antes de cierto instante. Combinado con la información de revocación de ese instante, permite demostrar años después que el certificado era válido cuando se firmó, aunque haya vencido o sido revocado más tarde. Sobre esa combinación se construyen los formatos de firma de larga duración que estudiaremos en el tomo dos.

Los algoritmos envejecen

La seguridad de la firma digital depende de que ciertos problemas matemáticos sean muy difíciles de resolver con la capacidad de cálculo disponible. Esa capacidad crece, y los investigadores encuentran atajos. Por eso los algoritmos tienen una vida útil.

La historia ofrece ejemplos claros. La función de resumen MD5, muy usada en los noventa, quedó desacreditada cuando se demostró que se podían fabricar colisiones, y en 2008 un grupo de investigadores la explotó para crear un certificado de autoridad falso que los navegadores habrían aceptado. SHA1, su sucesora, cayó en 2017, cuando se publicó la primera colisión práctica. Las claves RSA de 1024 bits, habituales hace veinte años, hoy se consideran insuficientes y se usan claves de 2048 bits o más.

Este envejecimiento tiene una consecuencia práctica que suele pasarse por alto: una firma hecha hoy con algoritmos seguros puede volverse dudosa dentro de quince años. Los documentos que deben conservar su valor durante décadas necesitan mecanismos para renovar periódicamente su protección. El horizonte más visible de este problema es la computación cuántica, que amenaza a los algoritmos de clave pública actuales y ya motivó la publicación de nuevos estándares. Lo tratamos en el capítulo once y con más detalle en el tomo tres.

PARA RECORDAR

La **huella** detecta cualquier cambio. El **par de claves** vincula la firma con quien tiene la clave privada. El **certificado** vincula la clave con una identidad. El **sello de tiempo** fija cuándo ocurrió. Las cuatro piezas juntas cumplen las funciones de identificación, integridad y prueba que la firma manuscrita resolvía a medias.

05

CAPÍTULO CINCO

Dónde vive la clave.

Toda la seguridad de la firma digital depende de un secreto: la clave privada. Dónde se guarda ese secreto, y quién puede usarlo, es la pregunta que dio origen a toda una familia de dispositivos.

Si alguien copia una clave privada, puede firmar en nombre de su titular sin dejar rastro. Por eso la pregunta más importante de cualquier esquema de firma no es qué algoritmo usa, sino dónde se genera la clave, dónde se guarda y qué hace falta para usarla. A lo largo de treinta años la industria dio respuestas muy distintas a esa pregunta, y cada una supone un equilibrio diferente entre seguridad, costo y comodidad.

La clave en un archivo

La solución más simple es guardar la clave privada en un archivo protegido por contraseña, habitualmente en un formato estándar llamado PKCS #12, con extensiones como .p12 o .pfx. Es fácil de distribuir e instalar, y muchas organizaciones la usaron durante años.

Su debilidad es evidente: un archivo se puede copiar. Si alguien obtiene el archivo y adivina o roba la contraseña, tiene la clave. Además, el titular no puede saber si su clave fue copiada. Por eso la mayoría de las legislaciones no admite claves en archivo para los niveles superiores de firma, y las buenas prácticas las reservan para usos de bajo riesgo o para sellos de plataforma protegidos por otros medios.

La tarjeta inteligente

La respuesta clásica al problema de la copia es un chip. Una tarjeta inteligente contiene un pequeño procesador capaz de generar la clave privada en su interior y de realizar la operación de firma sin que la clave salga nunca del chip. La computadora le envía la huella del documento, la tarjeta pide un PIN y devuelve la firma. La clave no se puede exportar: si se pierde la tarjeta, se pierde la clave, y se revoca el certificado.

Las tarjetas inteligentes nacieron en los años setenta y se difundieron primero en la telefonía y la banca. Su uso para firma creció con los documentos nacionales de identidad electrónicos. Estonia, a partir de 2002, fue uno de los primeros países en entregar a toda su población una tarjeta de identidad con certificados de autenticación y firma, y hoy es el caso de referencia. Bélgica, España, Portugal, Alemania y muchos otros siguieron el camino. En América Latina, Uruguay incorporó en 2015 un chip con certificados a su cédula de identidad, y otros países avanzan en la misma dirección.

El precio de esa seguridad es la fricción. Para firmar hace falta un lector, un controlador instalado en la computadora y, a menudo, un componente intermedio que conecte el navegador con el lector. Cada actualización de sistema operativo o de navegador puede romper esa cadena. Para un usuario que firma una vez al año, el costo de aprendizaje suele ser mayor que el beneficio.

El token USB

El token criptográfico USB es, en esencia, una tarjeta inteligente y su lector en un solo objeto. Se popularizó entre profesionales que firman con frecuencia, como contadores, escribanos, despachantes de aduana o funcionarios públicos. Ofrece la misma protección que la tarjeta con menos piezas, aunque comparte su dependencia de controladores y componentes intermedios.

El módulo de seguridad de hardware

En el otro extremo de la escala está el HSM, sigla inglesa de módulo de seguridad de hardware. Es un equipo dedicado, del tamaño de un servidor o de una tarjeta que se inserta en uno, diseñado para generar, guardar y usar claves criptográficas con protecciones físicas y lógicas muy exigentes. Un HSM detecta intentos de apertura y

puede borrar sus claves si alguien intenta manipularlo. Se certifica según normas como FIPS 140, del gobierno de los Estados Unidos, o según perfiles de protección del esquema internacional Common Criteria.

Los HSM protegen las claves de las autoridades de certificación, las de los sellos de tiempo y las de los sellos de organización. Y desde hace una década protegen también las claves de personas, en lo que se conoce como firma remota.

La firma remota o en la nube

La firma remota invierte el modelo. En lugar de que cada persona tenga un dispositivo, el prestador de servicios de confianza guarda las claves de muchas personas en un HSM propio, y cada titular activa su clave a distancia, autenticándose con un segundo factor, como un código en el teléfono o una aplicación. La clave nunca sale del HSM y sólo se usa cuando su titular lo autoriza.

El reglamento eIDAS de 2014 reconoció expresamente que una firma cualificada puede crearse de este modo, siempre que el prestador gestione el dispositivo en nombre del firmante con garantías equivalentes. Las normas técnicas europeas definieron entonces los requisitos para los componentes que activan la firma remota y para los módulos que la ejecutan, y distinguieron niveles según cuánto control conserva el firmante.

Para conectar aplicaciones con servicios de firma remota de distintos prestadores se formó en 2016 el Cloud Signature Consortium, que publicó una interfaz de programación común. Gracias a ella, una aplicación puede pedir a cualquier prestador compatible que firme una huella en nombre de un usuario, siguiendo un mismo protocolo, sin integraciones a medida para cada uno. Esta interoperabilidad es uno de los factores que más contribuyó a que la firma de nivel superior dejara de depender de un objeto físico.



FIGURA 7 Dónde vive la clave privada. De izquierda a derecha, la clave pasa de estar en manos del firmante a estar en un servicio que él activa a distancia.

El teléfono como dispositivo de firma

Los teléfonos modernos incluyen zonas protegidas de hardware, como los enclaves seguros o los chips de seguridad dedicados, capaces de guardar claves que no pueden extraerse. Algunos países y operadores aprovecharon además la tarjeta SIM para alojar certificados. Estonia lanzó en 2007 un esquema de identidad móvil basado en la SIM y, años después, otro basado en una aplicación, y ambos se usan masivamente para identificarse y firmar.

La cartera europea de identidad digital que prevé el reglamento de 2024 sigue esta línea: una aplicación en el teléfono que, apoyada en un elemento seguro o en un servicio remoto, permitirá a cualquier ciudadano firmar con nivel cualificado sin costo para usos no profesionales. Si se cumple ese objetivo, la firma de nivel superior dejará de ser un trámite de especialistas y se volverá tan común como pagar con el teléfono.

Qué significa «control exclusivo»

Todas estas opciones intentan responder a la misma exigencia jurídica que vimos en el capítulo tres: que la clave esté bajo el control exclusivo del firmante. Con una tarjeta en la mano, la respuesta parece obvia. Con una clave en un servidor ajeno, el control se ejerce de otra manera: mediante la autenticación del titular cada vez que quiere firmar, y mediante garantías técnicas y auditorías que aseguran que ni el propio prestador puede usar la clave sin esa autorización.

El debate sobre cuál modelo ofrece más control real sigue abierto. Una tarjeta puede prestarse junto con su PIN; un servicio remoto bien diseñado puede exigir una autenticación fuerte que es difícil de delegar. Lo que la experiencia muestra es que la seguridad no depende sólo del lugar donde está la clave, sino del proceso completo que rodea su uso.

DISPOSITIVO	DÓNDE ESTÁ LA CLAVE	FORTALEZA	FRICCIÓN
Archivo protegido	En el disco del usuario	Baja: puede copiarse	Muy baja
Tarjeta o token	En un chip que tiene el usuario	Alta: no se exporta	Alta: lector y controladores
Documento de identidad con chip	En la cédula o el documento nacional	Alta, y ya está en manos del ciudadano	Media o alta, según el país
Firma remota	En un HSM del prestador	Alta si la activación es fuerte	Baja: basta un teléfono
Teléfono o cartera	En el elemento seguro del teléfono o en un servicio remoto	Alta	Muy baja una vez configurada

Para quien diseña un proceso de firma, la consecuencia es clara: rara vez conviene atarse a un único dispositivo. Los firmantes de un mismo documento pueden tener herramientas distintas, y una buena plataforma debe poder aceptar a cada uno con la suya.

06

CAPÍTULO SEIS

Cómo el derecho aprendió a confiar.

La técnica estuvo lista antes que la ley. Este capítulo recorre los principios con los que los legisladores reconocieron la firma electrónica y los modelos que surgieron de combinarlos.

Cuando la firma digital estuvo disponible, el derecho enfrentó un dilema. Si exigía una tecnología concreta, corría el riesgo de quedar obsoleto en pocos años y de excluir alternativas válidas. Si no exigía nada, dejaba a jueces y ciudadanos sin criterios para saber qué firmas eran confiables. Las respuestas que se dieron a ese dilema se apoyan en un puñado de principios que hoy son patrimonio común.

Equivalencia funcional

Es el principio fundacional. Formulado con claridad por la UNCITRAL en sus leyes modelo, sostiene que un mecanismo electrónico satisface un requisito legal de firma si cumple las mismas funciones que la firma manuscrita cumple en ese contexto: identificar a la persona e indicar su aprobación del contenido, con un método tan fiable como sea apropiado para el fin del documento.

La equivalencia funcional no dice que toda firma electrónica equivalga a una manuscrita. Dice que la pregunta correcta no es «¿hay tinta?» sino «¿se cumplen las funciones?». Es la misma pregunta que se hizo aquel tribunal de New Hampshire ante el telégrafo, convertida en norma.

Neutralidad tecnológica

La ley no debe favorecer ni excluir una tecnología determinada. Debe describir requisitos y resultados, no algoritmos ni dispositivos. Este principio protege a la legislación del envejecimiento técnico y evita que una norma se convierta en una barrera de mercado a favor de un proveedor.

La neutralidad tiene límites prácticos. Cuando la ley exige que una modificación posterior sea detectable, en los hechos está exigiendo criptografía. Y los niveles superiores de firma se apoyan en normas técnicas detalladas que, sin nombrar productos, sí definen requisitos muy precisos. La neutralidad se mantiene en el texto de la ley y se concreta en las normas técnicas que la acompañan, que pueden actualizarse con más agilidad.

No discriminación

No puede negarse efecto jurídico ni admisibilidad como prueba a una firma por el solo hecho de ser electrónica o de no cumplir los requisitos del nivel superior. El reglamento eIDAS lo dice expresamente en su artículo 25, y la ley federal estadounidense de 2000 se construyó casi entera sobre esta idea.

El principio no obliga a aceptar cualquier firma como prueba plena. Obliga a evaluarla, en lugar de descartarla de antemano. Una firma simple puede ser perfectamente válida; lo que cambia es quién debe demostrar qué si se la discute.

Autonomía de la voluntad

En las relaciones privadas, las partes pueden acordar qué medios de firma aceptarán entre ellas. Un banco y su cliente pueden pactar que ciertas operaciones se confirmen con un código y una huella dactilar; dos empresas pueden acordar que sus órdenes de compra se firmen con un mecanismo determinado. Ese acuerdo previo refuerza el valor de las firmas que se hagan bajo sus términos.

La autonomía tiene límites cuando la ley exige una forma para ciertos actos o cuando una de las partes está en posición de debilidad, como ocurre con los consumidores. En esos casos las normas de protección suelen prevalecer sobre lo pactado.

La carga de la prueba y las presunciones

Aquí está, en buena medida, la diferencia práctica entre los niveles de firma. Ante una firma electrónica simple que se impugna, quien la invoca debe probar que es auténtica: que la hizo quien dice haberla hecho y que el documento no cambió. Ante una firma de nivel superior, muchas legislaciones invierten esa carga mediante presunciones: se presume que la firma pertenece al titular del certificado y que el documento no fue alterado, y es quien lo niega el que debe demostrar lo contrario.

Esta inversión explica por qué las organizaciones con alto riesgo de disputa, como los bancos ante ciertos préstamos o los empleadores ante ciertos acuerdos, prefieren firmas de nivel superior aunque cuesten más. No es que la firma simple «no valga»; es que, si alguien la niega, defenderla puede requerir peritajes, registros técnicos y tiempo.

EL NO REPUDIO, CON MATICES

En seguridad informática se llama *no repudio* a la propiedad que impide a alguien negar haber realizado una acción. La firma digital suele presentarse como garantía de no repudio. Jurídicamente conviene ser más cauto: siempre es posible alegar que la clave fue usada por otra persona, que hubo coacción o que el firmante no entendió lo que firmaba. Lo que una buena firma aporta no es la imposibilidad de negar, sino una prueba tan sólida que negar se vuelve muy difícil.

Tres modelos legislativos

De la combinación de estos principios surgieron, a grandes rasgos, tres modelos. Ningún país encaja exactamente en uno, pero la clasificación ayuda a entender por qué la misma firma puede tener efectos distintos según dónde se use.



FIGURA 8 Tres modelos legislativos. Ningún país encaja del todo en uno, pero la clasificación explica por qué la misma firma puede tener efectos distintos según la jurisdicción.

El modelo prescriptivo

Fue el de las primeras leyes, como la de Utah de 1995 y las europeas de fines de los noventa. Define una tecnología concreta, la firma digital con certificado emitido por una autoridad licenciada, y le reconoce efectos jurídicos. Lo que queda fuera de esa tecnología no recibe un tratamiento específico. Ofrece mucha seguridad jurídica para quien usa la tecnología prevista y poca flexibilidad para todo lo demás.

El modelo minimalista

Es el de la ley federal estadounidense de 2000 y de varias leyes inspiradas en la primera ley modelo de la UNCITRAL. Se limita a afirmar que la firma electrónica no puede ser rechazada por ser electrónica, y deja que la prueba de cada caso decida. Favorece la innovación y la adopción rápida, a cambio de trasladar la discusión sobre la fiabilidad a los tribunales.

El modelo de niveles

Combina los dos anteriores. Reconoce cualquier firma electrónica según el principio de no discriminación y, al mismo tiempo, define uno o más niveles superiores con requisitos técnicos y efectos reforzados. Es el modelo de la Unión Europea desde 1999, consolidado por eIDAS, y el que adoptaron con variantes muchos países latinoamericanos. Su fortaleza es que permite elegir el nivel adecuado para cada acto. Su desafío es la complejidad: hay que entender los niveles para aprovecharlos.

El reconocimiento entre países

Una firma válida en un país no es automáticamente válida en otro. Dentro de la Unión Europea, eIDAS resolvió el problema para las firmas cualificadas: deben ser reconocidas en todos los Estados miembros, y las listas de confianza de cada país permiten verificar a los prestadores de los demás. Fuera de ese espacio, el reconocimiento depende de acuerdos bilaterales o regionales, de la equivalencia de los regímenes y, en muchos casos, de la voluntad de las partes.

En América Latina existen iniciativas de reconocimiento mutuo, como los acuerdos entre países del Mercosur y los trabajos de la Red de Gobierno Electrónico de América Latina y el Caribe sobre el reconocimiento transfronterizo de la firma digital. Su avance es gradual. Para una organización que opera en varios países, esto significa que una misma plataforma de firma debe poder trabajar con prestadores y reglas distintos según la jurisdicción de cada acto.

Los actos que siguen pidiendo algo más

Casi todas las legislaciones mantienen excepciones. Los testamentos, ciertos actos de derecho de familia, la transmisión de inmuebles o los actos que requieren intervención notarial suelen quedar fuera del régimen general de firma electrónica o exigir requisitos adicionales. Las excepciones se van reduciendo con los años, a medida que aparecen mecanismos como la escritura pública electrónica o la comparecencia notarial a distancia, pero siguen existiendo y conviene verificarlas antes de diseñar cualquier proceso.

> La ley no le pregunta a la firma de qué está hecha. Le pregunta qué hace, y cuánta confianza merece para el acto que respalda.

07

CAPÍTULO SIETE

Para qué se firma.

La firma electrónica dejó de ser una curiosidad técnica para convertirse en infraestructura de bancos, gobiernos, hospitales y empresas. Un recorrido por sus usos muestra que cada sector le pide cosas distintas.

No hay un único caso de uso de la firma electrónica, sino una enorme variedad de actos que comparten la necesidad de dejar constancia de una voluntad. Lo interesante es que cada sector enfatiza funciones distintas: en unos importa sobre todo la identificación, en otros la velocidad, en otros la conservación durante décadas. Conocer esas diferencias ayuda a entender por qué las plataformas de firma se volvieron tan configurables.

Banca y finanzas

Fue uno de los primeros sectores en adoptar la firma electrónica de forma masiva. Apertura de cuentas, contratos de crédito, pagarés, autorizaciones de débito, actualizaciones de datos y consentimientos regulatorios se firman hoy, en muchos países, sin pisar una sucursal. La prioridad es doble: identificar con certeza al cliente, para cumplir con las normas de prevención de lavado de activos, y obtener una prueba sólida ante eventuales disputas. Por eso la banca combina verificación de identidad, a menudo con biometría, y firmas de nivel avanzado o superior, con registros de evidencia muy detallados.

Sector público

Los gobiernos firman y reciben firmas en volúmenes enormes: resoluciones, expedientes, certificados, declaraciones juradas, licitaciones. Muchos países construyeron sus estrategias de gobierno digital sobre la firma de nivel superior, a menudo apoyada en el documento nacional de identidad. La prioridad es la validez jurídica plena y la conservación a largo plazo, porque un acto administrativo puede tener que exhibirse décadas después. También importa la interoperabilidad: un expediente puede recorrer varios organismos, y cada uno debe poder verificar las firmas de los demás.

Recursos humanos

Contratos de trabajo, recibos de sueldo, políticas internas, acuerdos de confidencialidad y licencias. Los volúmenes son altos y los firmantes, muchas veces, no tienen dispositivos especiales. La prioridad es la facilidad de uso y la trazabilidad: saber quién recibió qué y cuándo aceptó. En algunos países, ciertos documentos laborales exigen nivel avanzado o superior, y la plataforma debe poder elevar el nivel sólo para ellos.

Salud

Consentimientos informados, recetas, historias clínicas, informes de estudios. La firma acredita la autoría del profesional y la voluntad del paciente. La prioridad es la integridad de documentos sensibles y la protección de datos personales. La receta electrónica, en particular, se convirtió en uno de los usos de mayor volumen de la firma de nivel superior en varios países.

Inmobiliario y seguros

Contratos de alquiler con propietario, inquilino y garantes; pólizas, endosos y declaraciones de siniestros. Son procesos con varias partes que a menudo no se conocen, y donde cada una debe completar datos propios antes de firmar. La prioridad es la coordinación: que cada persona vea lo que le toca, complete sus campos y firme en el orden correcto.

Comercio internacional

Contratos de compraventa, cartas de crédito, certificados de origen, documentos de transporte. Las partes están en países distintos y regidas por leyes distintas. La prioridad es el reconocimiento transfronterizo y la posibilidad de verificar firmas emitidas bajo otros regímenes. La UNCITRAL aprobó en 2017 una ley modelo sobre documentos transmisibles electrónicos, pensada para títulos como el conocimiento de embarque, que extiende la lógica de la firma electrónica a documentos que representan mercaderías.

Profesiones y notariado

Escribanos, contadores, despachantes, abogados y arquitectos firman documentos que otros deben poder verificar con certeza. Fueron, en muchos países, los primeros usuarios de tokens y tarjetas. Hoy el notariado explora la escritura pública electrónica y la comparecencia a distancia, que exigen combinar firma, identificación por video y conservación con garantías especiales.

SECTOR	QUÉ ENFATIZA	NIVEL HABITUAL
Banca	Identificación del cliente y prueba ante disputas	Avanzado o superior, con biometría
Sector público	Validez plena, conservación, interoperabilidad	Superior, a menudo con el documento de identidad
Recursos humanos	Facilidad, volumen, trazabilidad	Simple o avanzado según el documento
Salud	Autoría profesional, integridad, privacidad	Superior para profesionales; simple o avanzado para pacientes
Inmobiliario y seguros	Coordinación de varias partes y datos propios	Simple o avanzado
Comercio exterior	Reconocimiento entre países	Avanzado o superior

El sello de organización

Junto a las firmas de personas, crece el uso del sello de organización, el «sello electrónico» de eIDAS. Facturas electrónicas, certificados emitidos en forma automática, constancias, extractos bancarios y diplomas universitarios reciben un sello de organización sin intervención humana, para garantizar que provienen de quien dicen y que no fueron alterados. En una organización que emite documentos en masa, el sello de organización automático puede superar con holgura en volumen a las firmas de personas, aunque sea mucho menos visible.

Documentos con muchas manos

Un rasgo común atraviesa casi todos estos usos: los documentos importantes rara vez los firma una sola persona. Un préstamo involucra al cliente, a sus garantes y al banco; un contrato de alquiler, al propietario, al inquilino, a los garantes y a la inmobiliaria; un acta, a todos los miembros de un órgano. Además, antes de firmar, alguien debe revisar, alguien debe aprobar y alguien debe completar datos. Esa realidad, más que la firma en sí, es la que dio origen a los gestores de flujos de firma.

08

CAPÍTULO OCHO

Ventajas, límites y malentendidos.

La firma electrónica tiene beneficios evidentes y otros que sólo aparecen con el tiempo. También tiene límites que conviene conocer antes de prometer lo que no puede dar.

Las ventajas evidentes

- **Tiempo.** Un contrato que en papel requería días de envíos y firmas sucesivas puede completarse en horas o minutos. Para procesos comerciales, esa diferencia se traduce directamente en ventas cerradas y clientes que no abandonan.
- **Costo.** Desaparecen la impresión, el transporte de originales, el escaneo y buena parte del archivo físico. El ahorro por documento puede parecer pequeño, pero se multiplica por el volumen.
- **Distancia.** Las partes pueden firmar desde cualquier lugar, en cualquier momento. Esto amplía el alcance de una organización sin abrir oficinas.
- **Ambiente.** Menos papel, menos tinta, menos traslados. El efecto es real, aunque conviene no exagerarlo: la infraestructura digital también consume recursos.

Las ventajas que se descubren después

- **Integridad verificable.** Una firma digital revela cualquier alteración posterior. En papel, detectar una página cambiada puede requerir un peritaje; en un documento firmado digitalmente, basta un validador.
- **Evidencia del proceso.** Una buena plataforma registra cada paso: el envío, la apertura, la identificación, la lectura, la firma. Esa traza suele ser más rica que cualquier prueba disponible en el mundo del papel.

- **Visibilidad.** Quien envía un documento sabe en todo momento quién firmó, quién lo abrió y quién todavía no. Los cuellos de botella se vuelven visibles y medibles.
- **Integración.** Un documento firmado puede alimentar automáticamente otros sistemas: el de gestión documental, el contable, el de recursos humanos. La firma deja de ser el final de un proceso manual para convertirse en un evento dentro de un proceso automatizado.
- **Accesibilidad.** Bien diseñada, la firma electrónica permite firmar a personas con discapacidad visual o motriz que en papel dependían de terceros, usando lectores de pantalla y la configuración de su propio dispositivo.

Los límites

La brecha digital

No todas las personas tienen un teléfono moderno, una conexión estable o la familiaridad necesaria para seguir un proceso digital. Un servicio que sólo acepta firma electrónica puede excluir a quienes más necesitan ese servicio. Las buenas prácticas recomiendan mantener alternativas y diseñar los procesos para el usuario menos experto, no para el promedio.

La identidad sigue siendo el eslabón débil

La criptografía garantiza que una firma fue hecha con cierta clave. No garantiza que la persona que activó esa clave sea quien dice ser. Si la verificación de identidad al emitir el certificado fue débil, o si el factor que activa la firma puede robarse, una firma técnicamente impecable puede quedar en manos equivocadas. Buena parte del fraude asociado a la firma electrónica no ataca la matemática: ataca la identificación.

La conservación no es automática

Un documento firmado hoy puede ser imposible de validar dentro de diez años si no se conservaron los certificados, la información de revocación y los sellos de tiempo, o si los algoritmos usados se debilitaron. Conservar la validez de una firma exige decisiones activas, que tratamos en el tomo dos.

La interoperabilidad tiene costuras

Una firma perfectamente válida puede aparecer como «no verificada» en un lector que no confía en la autoridad que emitió el certificado. Un formato de firma puede ser aceptado en un país y desconocido en otro. Estas fricciones no invalidan la firma, pero generan desconfianza en usuarios que no entienden por qué el mismo documento se ve distinto en dos programas.

Malentendidos frecuentes

SE DICE	LO QUE CONVIENE SABER
«Una firma escaneada es una firma electrónica.»	Lo es en el sentido más amplio, pero es la más débil de todas: se copia con facilidad y no protege la integridad del documento.
«La firma electrónica no tiene validez legal.»	En la gran mayoría de los países sí la tiene, con distintos efectos según el nivel. Lo que puede no tener es el efecto reforzado de la firma de nivel superior.
«Si el lector de PDF muestra un aviso, la firma es inválida.»	Muchas veces el aviso sólo indica que el lector no tiene configurada la autoridad que emitió el certificado. Hay que validar con la lista de confianza correcta.
«La firma digital no se puede falsificar.»	La matemática es muy robusta, pero la clave puede ser usada por otra persona si su protección falla. La seguridad es del proceso completo.
«Un documento firmado vale para siempre.»	Sólo si se conserva con las pruebas necesarias y se renueva su protección cuando los algoritmos envejecen.
«Siempre conviene el nivel más alto.»	No necesariamente. Un nivel excesivo para el riesgo del acto agrega fricción y puede hacer que el proceso no se complete.

PARA RECORDAR

La firma electrónica no elimina el riesgo; lo cambia de lugar. Del papel que se pierde o se altera, a la identidad que se suplanta o la prueba que no se conservó. Una buena solución se reconoce por cómo gestiona esos riesgos nuevos, no por la cantidad de funciones que ofrece.

09

CAPÍTULO NUEVE

Del documento firmado al proceso firmado.

Firmar un documento ya era posible. Lo difícil era coordinar a todas las personas que debían intervenir en él. De esa necesidad nacieron los gestores de flujos de firma.

A fines de los años noventa, firmar digitalmente un documento era técnicamente posible y, en varios países, jurídicamente válido. Sin embargo, casi nadie lo hacía. La razón no era la falta de confianza en la criptografía, sino la falta de un camino práctico. Quien quería que tres personas firmaran un contrato debía enviarles el archivo, explicarles cómo firmar con sus herramientas, esperar a que cada una lo devolviera, verificar que todas hubieran firmado la misma versión y archivar el resultado. Era más fácil imprimir.

Dos raíces

Los gestores de flujos de firma tienen dos raíces que se encontraron a comienzos de este siglo.

La primera es la de los sistemas de flujo de trabajo y gestión documental que las grandes organizaciones usaban desde los años ochenta y noventa. Esos sistemas ya sabían enrutar un documento por una serie de aprobaciones, registrar quién lo había visto y archivarlo. Las administraciones públicas, en particular, desarrollaron expedientes electrónicos con circuitos de firma internos. Pero eran sistemas cerrados, pensados para usuarios dentro de una misma organización.

La segunda raíz es la del correo electrónico y la web como canal universal. A comienzos de los dos mil, cualquier persona con una dirección de correo y un navegador podía recibir un enlace y abrir un documento. Bastaba con combinar ese canal con la lógica de los flujos de trabajo y con algún mecanismo de firma para que un documento pudiera recorrer, en minutos, el camino que en papel tomaba semanas.

Los pioneros

En 2003 se fundó en los Estados Unidos una de las primeras empresas del rubro, que popularizó la idea del «sobre» electrónico: un paquete con uno o más documentos, una lista de destinatarios y las instrucciones de qué debía hacer cada uno. En 2005 nació otra, que una empresa de software para documentos adquirió en 2011 y convirtió luego en la base de su servicio de firma. Hacia 2010 surgió una tercera, que un servicio de almacenamiento en la nube adquirió en 2019. A ellas se sumaron decenas de proveedores en Europa, América Latina y Asia, muchos surgidos de prestadores de servicios de certificación que vieron en el flujo la manera de llevar sus certificados a un público más amplio.

Los primeros servicios se apoyaron sobre todo en la firma electrónica simple: el firmante recibía un enlace por correo, revisaba el documento, hacía clic o dibujaba su firma, y la plataforma aplicaba un sello de plataforma al resultado y producía un certificado con el registro de lo ocurrido. Ese registro, más que la firma en sí, era la pieza que aportaba valor probatorio. Con el tiempo, las plataformas incorporaron la posibilidad de usar firmas avanzadas y cualificadas, verificación de identidad y prestadores de distintos países.

La adopción creció de manera sostenida durante la década de 2010 y se aceleró bruscamente en 2020, cuando la pandemia obligó a millones de organizaciones a firmar a distancia de un día para otro. Lo que hasta entonces era una mejora de eficiencia se volvió, durante meses, la única manera de seguir operando.

El vocabulario del flujo

Con los años se consolidó un vocabulario que hoy comparten casi todas las plataformas, aunque cada una le dé nombres propios.

CONCEPTO	QUÉ ES
Sobre o envío	La unidad de trabajo: uno o más documentos, los participantes y las reglas del recorrido.
Participante	Cada persona que interviene. Puede tener distintos *roles*: firmante, aprobador, revisor, quien completa datos o quien sólo recibe copia.
Ruta	El orden en que actúan los participantes: en serie, uno después de otro; en paralelo, todos a la vez; o mixto, con grupos que actúan en paralelo dentro de una secuencia.
Campos	Los lugares del documento donde cada participante firma, escribe una fecha, completa un importe o marca una opción, asignados a quien corresponde.
Autenticación de acceso	Lo que se pide al participante para abrir el documento: un código, un mensaje al teléfono, una identidad digital o un certificado.
Recordatorios y vencimiento	Avisos automáticos a quien todavía no actuó, y una fecha a partir de la cual el envío deja de estar disponible.
Rechazo y delegación	La posibilidad de negarse a firmar dejando un motivo, o de reasignar la tarea a otra persona cuando las reglas lo permiten.
Plantilla	Un documento con sus campos, roles y ruta ya definidos, que puede reutilizarse cambiando sólo los participantes.
Certificado de finalización	El informe que acompaña al documento firmado y resume quién hizo qué, cuándo y cómo se identificó.



FIGURA 9 Un recorrido de firma mixto: una firmante, dos garantes que actúan en paralelo, un propietario que firma al final y una inmobiliaria que sólo recibe copia.

Del gestor al tejido de la organización

A medida que maduraban, los gestores de flujos dejaron de ser una herramienta aislada para integrarse en los sistemas de cada organización. Las interfaces de programación permitieron que un sistema de gestión de clientes, de recursos humanos o de compras creara envíos automáticamente y recibiera aviso cuando un documento quedaba firmado. La firma embebida permitió que el firmante no saliera de la aplicación en la que estaba. Las integraciones con repositorios documentales hicieron que el documento firmado se archivara solo, en el lugar correcto.

Al mismo tiempo, el mercado se segmentó. Por un lado, plataformas generalistas de gran escala, orientadas a la facilidad de uso y a un ecosistema amplio de integraciones. Por otro, soluciones más especializadas, con foco en la firma de nivel superior, en el cumplimiento de regímenes nacionales o en la operación por parte de prestadores de servicios de confianza. Los analistas de la industria empezaron a evaluar no ya la firma en sí, que consideran una capacidad básica, sino el flujo completo y la identidad de quien firma.

Lo que cambió en la idea de firma

El aporte más profundo de los gestores de flujos no fue técnico, sino conceptual. Cambiaron la unidad de análisis. Antes, la pregunta era si una firma era válida. Ahora la pregunta es si un proceso de firma fue correcto: si cada persona vio la versión que debía ver, si completó lo que le tocaba, si se identificó con el nivel adecuado, si firmó en el orden previsto y si todo eso quedó registrado de manera que pueda demostrarse después.

Ese cambio de unidad, del documento al proceso, es el punto de partida del capítulo siguiente, donde describimos qué esperar hoy de una plataforma que coordina procesos de firma.

10

CAPÍTULO DIEZ

Anatomía de una plataforma.

Qué hace, por dentro, un sistema que coordina procesos de firma. Siete capas, lo que hoy se espera de cada una y lo que distingue a una solución madura de una que sólo lo parece.

Visto desde fuera, un gestor de flujos de firma parece simple: se sube un documento, se eligen los firmantes y se espera. Visto desde dentro, es un sistema con responsabilidades muy distintas que deben funcionar juntas. Para analizarlo conviene descomponerlo en capas. La descomposición que proponemos no corresponde a ningún producto en particular; es una manera de ordenar las preguntas que cualquier organización debería hacerse.



FIGURA 10 Siete capas de una plataforma de flujos de firma. En magenta, las dos capas que sostienen la prueba.

1. Preparación del documento

Todo empieza con un documento, casi siempre un PDF, aunque puede nacer de una plantilla o de otro sistema. En esta capa se decide qué hay que completar y quién lo completa. Una observación que el mercado tardó en incorporar es que la mayoría de los documentos no se firman primero: se completan primero. Un pagaré necesita el importe; un contrato de alquiler, la fecha de entrega; un consentimiento, el número de documento del paciente. Si esos datos se completan a mano antes de enviar, se pierde buena parte del beneficio.

Una plataforma madura permite asignar campos a cada participante, con reglas de obligatoriedad y validación, y garantiza que lo completado pase a formar parte de la versión que se firma. También convierte, cuando hace falta, el documento a un formato apto para conservación a largo plazo, como PDF/A, antes de la primera firma, porque convertirlo después invalidaría las firmas.

2. Ruta y participantes

Es la capa del flujo propiamente dicho: quién interviene, con qué rol y en qué orden. Las rutas en serie, en paralelo y mixtas son hoy lo básico, igual que los roles de firmante, aprobador y destinatario de copia. Lo que distingue a una solución madura es cómo resuelve los casos difíciles: un grupo donde basta con que firme uno de sus miembros, un participante que se define recién cuando el anterior actúa, un firmante que delega en un apoderado, un documento que debe volver atrás porque alguien lo rechazó.

También importa la experiencia de quien recibe. Cada participante debería ver sólo lo que le corresponde, en su idioma, desde cualquier dispositivo, con recordatorios oportunos y sin necesidad de crear una cuenta.

3. Identidad

Antes de firmar hay que saber quién firma. Las opciones van desde un código enviado por correo o al teléfono hasta la verificación de un documento de identidad con prueba de vida, pasando por las identidades digitales nacionales, los proveedores de identidad corporativos y los certificados en tarjeta o en la nube. Los analistas de la industria coinciden en que buena parte del valor de estas plataformas se trasladó a esta capa.

La pregunta clave no es cuántos métodos ofrece una plataforma, sino si permite elegir el método adecuado para cada participante y cada acto, y si registra en la evidencia, por separado, cómo se identificó cada persona y cómo autorizó su firma. Identificarse y autorizar son actos distintos, y una prueba sólida debe poder mostrar ambos.

4. Firma y servicios de confianza

En esta capa se produce la firma criptográfica. Una plataforma puede firmar con sus propias claves, aplicando un sello de plataforma sobre la firma simple de cada participante, o delegar la firma en prestadores externos, por ejemplo mediante la interfaz común de firma remota que vimos en el capítulo cinco. Puede además pedir sellos de tiempo y respuestas de revocación a terceros, e incorporarlos al documento.

Tres rasgos separan aquí lo maduro de lo aparente. El primero es la posibilidad de trabajar con varios prestadores y elegir, para cada acto, cuál corresponde según el país y el nivel exigido. El segundo es la resiliencia: qué ocurre si un servicio externo no

responde. Una buena práctica es definir un orden de preferencia y alternativas, y, si aun así algo falla, que el documento quede en el nivel que efectivamente alcanzó y lo declare, en lugar de fallar en silencio o de aparentar un nivel que no tiene. El tercero es el control de lo que puede cambiar después de cada firma: el formato PDF permite declarar si un documento firmado admite, por ejemplo, que otros completen campos o agreguen firmas, y una plataforma cuidadosa usa esas reglas para que cada firmante sepa exactamente qué protege su firma.

5. Evidencia

Durante todo el proceso, la plataforma registra eventos: el envío, cada apertura, cada identificación, cada campo completado, cada consentimiento, cada firma, cada rechazo. Ese registro es la columna vertebral de la prueba. Pero un registro sólo vale si puede demostrarse que nadie lo alteró, incluida la propia organización que opera la plataforma.

Las soluciones más cuidadosas encadenan los eventos mediante sus huellas, de modo que cada uno incluye la huella del anterior. Alterar o eliminar un evento rompe la cadena y se detecta. Un paso adicional, propio de los diseños más exigentes, es anclar periódicamente la huella del registro en un lugar externo que el operador no controla, como un servicio de sellado de tiempo o un almacenamiento inmutable de un tercero. Así, ni siquiera quien administra el sistema puede reescribir la historia sin dejar rastro.



FIGURA 11 Un registro de evidencia encadenado. Cada evento incluye la huella del anterior; modificar o borrar uno rompe la cadena desde ese punto.

6. Validación

Firmar es la mitad del trabajo. La otra mitad es permitir que cualquiera, en cualquier momento, compruebe que la firma es válida. Una plataforma madura entrega documentos que se validan con herramientas independientes, no sólo con las suyas, y en lo posible ofrece un validador abierto que explique qué comprobó y qué no. La transparencia es parte de la confianza: un validador que sólo dice «válido» o «inválido» enseña menos que uno que muestra la cadena de certificados, el sello de tiempo, la información de revocación y las reglas de modificación del documento.

La validación depende de la confianza que se deposite en las autoridades. Por eso las soluciones más completas leen las listas de confianza oficiales de cada país, en lugar de depender sólo de la lista de un lector o de un sistema operativo.

7. Integración y operación

La última capa es la que conecta la plataforma con el resto del mundo y la que permite operarla. Incluye las interfaces de programación, los avisos automáticos a otros sistemas cuando algo ocurre, las integraciones con repositorios y herramientas de

automatización, la personalización de marca y la administración de usuarios. También incluye aspectos que el usuario no ve y que un comprador exigente sí pregunta: el aislamiento entre los datos de distintas organizaciones, la residencia de los datos, el registro de actividad para auditoría, la conexión con los sistemas de monitoreo de seguridad del cliente, la posibilidad de desplegarse en la nube o en las instalaciones del propio cliente.

Una tendencia relevante es que estas plataformas dejan de ser sólo un servicio que una empresa contrata y pasan a ser una infraestructura que otros operan. Un prestador de servicios de confianza, un gobierno o un gran grupo empresarial pueden querer ofrecer el servicio con su propia marca a sus propios clientes, con una jerarquía de cuentas, medición de uso y precios propios. Diseñar para ese escenario exige pensar la plataforma desde el principio como un sistema con varios niveles de administración.

Preguntas para evaluar una solución

A modo de síntesis, estas son algunas preguntas que cualquier organización puede hacer a un proveedor, o a sí misma si construye su propia solución.

1. ¿Pueden los participantes completar datos dentro del documento antes de firmar, con reglas, y lo completado queda dentro de lo que se firma?
2. ¿Qué rutas admite, y cómo resuelve rechazos, delegaciones y grupos?
3. ¿Qué métodos de identificación ofrece, puede elegirse uno distinto por participante, y la evidencia distingue identificación de autorización?
4. ¿Con qué prestadores de firma, sello de tiempo y revocación puede trabajar, y qué pasa si uno no responde?
5. ¿Qué formato y nivel de firma produce, y alcanza para conservarse a largo plazo?
6. ¿Cómo se protege el registro de evidencia frente a alteraciones, incluidas las del propio operador?
7. ¿Los documentos se validan con herramientas independientes? ¿Qué dice su validador sobre lo que comprueba y lo que no?
8. ¿Cómo se aíslan los datos de cada organización, dónde residen y quién puede acceder a ellos?
9. ¿Qué funciones no están disponibles hoy, y la plataforma lo dice con claridad o lo disimula?

La última pregunta parece menor y no lo es. En un dominio donde la confianza es el producto, una plataforma que muestra con honestidad lo que todavía no hace, y por qué, merece más confianza que una que promete todo.

11

CAPÍTULO ONCE

Lo que viene.

La firma electrónica está entrando en una nueva etapa. Cinco fuerzas la empujan, y cada una abre preguntas que los tomos siguientes de esta serie retoman con más detalle.

La identidad en el bolsillo

La cartera europea de identidad digital es un cambio muy visible. Cuando cientos de millones de personas puedan identificarse y firmar con nivel cualificado desde su teléfono, sin costo para usos personales, la firma de nivel superior dejará de ser una excepción. Iniciativas parecidas avanzan en otras regiones, apoyadas en documentos de identidad con chip, en aplicaciones oficiales o en credenciales verificables emitidas por gobiernos y bancos.

Para las plataformas de firma, esto implica aceptar a firmantes que llegan con su propia identidad y su propio medio de firma, en lugar de imponerles uno. La plataforma deja de ser quien identifica para convertirse en quien orquesta identidades emitidas por otros.

La verificación de identidad a distancia

La combinación de lectura de documentos, reconocimiento facial y pruebas de vida permite verificar a una persona que nunca se presentó en una oficina. Es la puerta de entrada a muchos procesos de firma, especialmente en banca y en servicios para consumidores. Al mismo tiempo, las técnicas de suplantación por imágenes sintéticas crecen en sofisticación, y la verificación de identidad se convirtió en una carrera entre defensores y atacantes. Las normas técnicas europeas ya establecen requisitos para la identificación a distancia, y es probable que otras regiones las adopten o adapten.

La inteligencia artificial

La inteligencia artificial está entrando en las plataformas de firma por dos caminos. El primero es el de la asistencia: extraer automáticamente las partes, las fechas y los importes de un contrato, sugerir dónde debe firmar cada uno, resumir un documento largo para quien lo envía, detectar cláusulas inusuales. El segundo es el de los agentes: programas que actúan en nombre de una persona o una organización, preparan envíos, hacen seguimiento y, eventualmente, podrían firmar dentro de límites delegados.

Este segundo camino plantea preguntas de fondo. Si un agente firma, ¿quién expresa la voluntad? ¿Cómo se delimita lo que puede firmar y cómo se prueba después que actuó dentro de esos límites? Las respuestas probablemente se apoyen en figuras conocidas, como el sello de organización y los poderes de representación, pero todavía están en construcción. Lo que ya parece claro es que el registro de evidencia, que hoy documenta lo que hicieron las personas, deberá documentar también lo que hicieron las máquinas por ellas.

La criptografía poscuántica

Una computadora cuántica de gran escala podría romper los algoritmos de clave pública en los que se basan hoy casi todas las firmas digitales. No existe todavía, y las estimaciones sobre cuándo podría existir varían mucho. Pero el riesgo es suficiente para que el Instituto Nacional de Estándares y Tecnología de los Estados Unidos publicara en agosto de 2024 sus primeros estándares de criptografía poscuántica, incluidos dos algoritmos de firma, y para que las autoridades europeas recomienden planificar la transición.

Para la firma electrónica, la transición tiene una particularidad: los documentos firmados deben seguir siendo verificables durante décadas. Eso obliga a pensar desde ahora cómo proteger las firmas existentes, por ejemplo renovando sus sellos de tiempo de archivo con algoritmos nuevos, y cómo convivirán durante años firmas clásicas y poscuánticas en los mismos sistemas.

La confianza como infraestructura compartida

Finalmente, la tendencia de fondo es que la confianza digital se está convirtiendo en infraestructura, como la energía o las telecomunicaciones. Listas de confianza públicas, prestadores supervisados, interfaces comunes de firma remota, carteras de identidad, servicios de conservación cualificados. Las plataformas de firma ya no se distinguen por su criptografía, que es en gran medida estándar, sino por saber combinar esas piezas para resolver procesos reales, en distintos países, con distintas reglas, de manera comprensible para las personas.

EN LOS PRÓXIMOS TOMOS

El **tomo 2, *La prueba que perdura***, entra en el detalle de los formatos y niveles de firma, los sellos de tiempo, la validación, las listas de confianza y la conservación a largo plazo. El **tomo 3, *Orquestar la firma***, se ocupa del diseño de procesos, la identidad, la integración, la operación a escala, la inteligencia artificial y la transición poscuántica.

> Durante cinco mil años, firmar fue dejar una marca. En los próximos años será, cada vez más, demostrar un proceso.

REFERENCIA

Glosario

Los términos principales de este tomo, en el sentido en que se usan aquí.

Autoridad de certificación

Entidad que verifica la identidad de personas u organizaciones y emite certificados digitales que vinculan esa identidad con una clave pública.

Autoridad de sellado de tiempo

Tercero de confianza que emite sellos de tiempo: pruebas firmadas de que un dato existía en un momento determinado.

Cadena de confianza

Secuencia de certificados en la que cada uno está firmado por el siguiente, hasta llegar a una raíz en la que se confía por decisión explícita.

Cartera de identidad digital

Aplicación, normalmente en el teléfono, que guarda credenciales de identidad y permite presentarlas y firmar con ellas.

Certificado cualificado o reconocido

Certificado emitido por un prestador supervisado que cumple requisitos reforzados de verificación de identidad y operación.

Certificado digital

Documento electrónico firmado por una autoridad de certificación que declara que una clave pública pertenece a un titular durante un período.

Clave privada y clave pública

Par de claves matemáticamente relacionadas. La privada, secreta, produce la firma; la pública, compartible, permite verificarla.

Control exclusivo

Requisito jurídico según el cual sólo el firmante puede activar su clave de firma, ya sea porque la tiene en un dispositivo propio o porque su uso remoto exige su autenticación.

Equivalencia funcional

Principio según el cual un mecanismo electrónico satisface un requisito legal de firma si cumple las funciones que la firma manuscrita cumple en ese contexto.

Firma digital

Técnica de firma basada en criptografía de clave pública. En algunos países, también una categoría jurídica de nivel superior.

Firma electrónica

Cualquier dato electrónico que una persona asocia a otros datos electrónicos con la intención de firmarlos.

Firma electrónica avanzada

Firma vinculada de manera única al firmante, que permite identificarlo, creada con medios bajo su control exclusivo y que revela cualquier modificación posterior.

Firma electrónica cualificada

Firma avanzada creada con un dispositivo cualificado y basada en un certificado cualificado. En la Unión Europea, equivale a la firma manuscrita.

Firma remota

Firma en la que la clave del firmante se guarda en un módulo seguro de un prestador y se activa a distancia mediante la autenticación del titular.

Función de resumen (hash)

Función que transforma un contenido de cualquier tamaño en una huella de longitud fija, de modo que cualquier cambio en el contenido produce una huella distinta.

Gestor de flujos de firma

Sistema que coordina el recorrido de uno o más documentos entre varios participantes, con roles, orden, campos, identificación y registro de evidencia.

HSM

Módulo de seguridad de hardware: equipo dedicado a generar, guardar y usar claves criptográficas con protecciones físicas y lógicas certificadas.

Lista de confianza

Lista oficial, firmada por una autoridad pública, de los prestadores de servicios de confianza supervisados y de sus servicios.

Neutralidad tecnológica

Principio según el cual la ley describe requisitos y efectos sin favorecer ni excluir una tecnología determinada.

OCSP

Protocolo de consulta en línea que informa si un certificado concreto está vigente o fue revocado.

Prestador de servicios de confianza

Entidad que presta servicios como emisión de certificados, sellos de tiempo, validación o conservación. Es cualificado si cumple requisitos reforzados y figura en una lista oficial.

Registro de evidencia

Conjunto ordenado de eventos de un proceso de firma, protegido contra alteraciones, que permite demostrar después lo ocurrido.

Revocación

Anulación de un certificado antes de su vencimiento, informada mediante listas publicadas o mediante consulta en línea.

«Sello electrónico» (sello de organización)

Equivalente de la firma para una persona jurídica: garantiza el origen y la integridad de un documento emitido por una organización.

Sello de tiempo

Prueba firmada por un tercero de confianza de que un dato existía en un momento determinado.

Tarjeta inteligente

Tarjeta con un chip capaz de generar y guardar una clave privada y de firmar sin que la clave salga del chip.

Validación

Proceso de comprobar la autenticidad de una firma, la integridad del documento y la validez del certificado en el momento de firmar.

REFERENCIA

Para seguir leyendo

Las normas, artículos y estándares citados en este tomo, agrupados por tema. Todos son de acceso público o pueden consultarse en las bibliotecas especializadas.

Historia y fundamentos

Diffie, W. y Hellman, M. «New Directions in Cryptography». *IEEE Transactions on Information Theory*, vol. 22, n.º 6, 1976.

Rivest, R., Shamir, A. y Adleman, L. Artículo de presentación del algoritmo RSA. *Communications of the ACM*, vol. 21, n.º 2, 1978.

Howley v. Whipple, 48 N.H. 487. Tribunal Supremo de New Hampshire, 1869.

Statute of Frauds, Inglaterra, 1677.

Stevens, M. y otros. «Short Chosen Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate». *CRYPTO 2009*.

Stevens, M. y otros. Artículo sobre la primera colisión completa de SHA1. *CRYPTO 2017*.

Marcos internacionales

CNUDMI (UNCITRAL). Ley Modelo sobre Comercio Electrónico, 1996. Ley Modelo sobre Firmas Electrónicas, 2001. Ley Modelo sobre Documentos Transmisibles Electrónicos, 2017.

Unión Europea. Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica.

Unión Europea. Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza (eIDAS).

Unión Europea. Reglamento (UE) 2024/1183, que modifica el Reglamento 910/2014 en lo que respecta al marco europeo de identidad digital.

Estados Unidos. Electronic Signatures in Global and National Commerce Act (ESIGN), 2000. Uniform Electronic Transactions Act (UETA), 1999. Utah Digital Signature Act, 1995.

Legislación latinoamericana citada

Argentina, Ley 25.506 de Firma Digital, 2001. Brasil, Medida Provisoria 2.200 de 2001, que instituye la ICP Brasil, y Ley 14.063 de 2020. Chile, Ley 19.799, 2002. Colombia, Ley 527, 1999. Paraguay, Ley 4.017, 2010, y Ley 6.822 de los servicios de confianza, 2021. Uruguay, Ley 18.600 de Documento Electrónico y Firma Electrónica, 2009.

Estándares técnicos

UIT. Recomendación X.509, marco de certificados de clave pública, 1988 y revisiones posteriores.

IETF. RFC 3161, protocolo de sellado de tiempo, 2001. RFC 5280, perfil de certificados y listas de revocación, 2008. RFC 6960, protocolo OCSP, 2013.

ISO. ISO 32000, formato de documento portátil (PDF), 2008 y 2017.

ETSI. EN 319 142, firmas electrónicas avanzadas en PDF (PAdES). EN 319 102, procedimientos de creación y validación de firmas. EN 319 401, requisitos generales para prestadores de servicios de confianza.

CEN. EN 419 241, sistemas confiables de firma en servidor. EN 419 221, perfiles de protección para módulos criptográficos.

Cloud Signature Consortium. Especificación de la interfaz de firma remota, versión 2.

NIST. FIPS 140, requisitos de seguridad para módulos criptográficos. FIPS 204 y FIPS 205, estándares de firma poscuántica, 2024.

Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

Cinco mil años de firmar, explicados para quienes hoy tienen que decidir cómo hacerlo.

Del sello cilíndrico a la cartera de identidad en el teléfono, este primer tomo recorre la historia, los fundamentos técnicos, los dispositivos y las doctrinas jurídicas de la firma electrónica, y explica cómo nacieron las plataformas que hoy coordinan procesos de firma entre personas, organizaciones y países.

Tomo 1 · De la rúbrica a la firma digital

Historia, fundamentos, dispositivos, doctrinas, usos y plataformas.

Tomo 2 · La prueba que perdura

Formatos, niveles, sellos de tiempo, validación y conservación.

Tomo 3 · Orquestar la firma

Procesos, identidad, integración, operación a escala y futuro.

Interfase · Montevideo, 2026