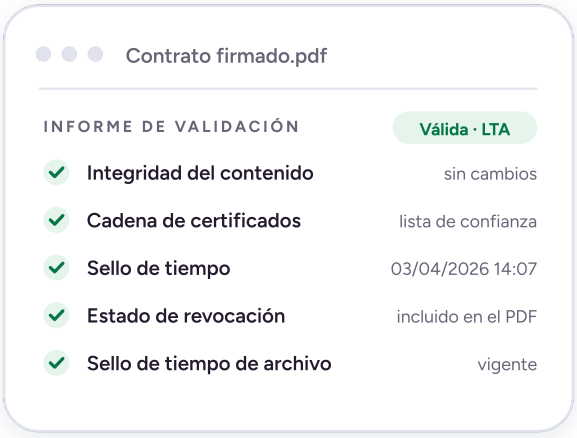
Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

TOMO 2

La prueba que perdura.

Formatos, niveles, sellos de tiempo, validación, listas de confianza y conservación: todo lo que hace falta para que una firma de hoy se pueda demostrar dentro de treinta años.





Primera edición · Montevideo, 2026

Interfase

Rúbrica. Cuadernos sobre firma, identidad y confianza digital
Tomo 2. La prueba que perdura

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 2

La prueba que perdura

Qué ocurre con una firma después de firmar, y cómo se conserva su valor a lo largo del tiempo.

CONTENIDO

Índice

	Prólogo	5
01	Cómo muere una firma	7
02	Los formatos	11
03	Los niveles de firma	15
04	La firma en el PDF	21
05	Los sellos de tiempo	25
06	La validación	29
07	Las listas de confianza	33
08	La conservación	37
09	El registro de evidencia	41
10	La firma ante el juez	45
	Glosario	49
	Para seguir leyendo	53

ANTES DE EMPEZAR

Firmar es un instante. Probar es para siempre.

El primer tomo de esta serie terminó en el momento en que alguien firma. Este empieza justo después, cuando la firma tiene que empezar a defenderse sola.

Una firma manuscrita envejece con su papel. Se destiñe, se mancha, se pierde en una mudanza, pero mientras el papel exista sigue siendo la misma firma y un perito puede examinarla. Con la firma digital ocurre algo paradójico: el documento puede conservarse intacto, bit por bit, durante décadas, y aun así la firma puede volverse imposible de verificar. Los certificados vencen, las autoridades que los emitieron cierran, los algoritmos se debilitan, los programas que sabían leer un formato desaparecen.

Este tomo trata de cómo evitar ese destino. Es el más técnico de la serie, y lo es por necesidad: la conservación de la prueba depende de detalles que no se ven en la pantalla del firmante pero que deciden, años después, si un documento vale o no. Hemos intentado explicar esos detalles sin perder de vista la pregunta práctica que los justifica: qué necesita una organización para poder demostrar, dentro de diez, veinte o treinta años, que un documento fue firmado por quien dice, cuando dice y sin cambios.

Los capítulos siguen el recorrido de una firma a lo largo de su vida. Empezamos por los riesgos que la amenazan con el paso del tiempo. Seguimos con los formatos y los niveles que se diseñaron para resistirlos, con especial atención al PDF, que es el soporte de la mayoría de los documentos firmados del mundo. Dedicamos luego capítulos a los sellos de tiempo, a la validación y a las listas de confianza, que son las tres piezas que permiten a un tercero verificar una firma sin depender de quien la produjo. Cerramos con la conservación a largo plazo, con el registro de evidencia del proceso de firma y con lo que ocurre cuando una firma llega a un tribunal.

SI NO LEYÓ EL TOMO 1

Este tomo supone conocidos algunos conceptos: la **huella** o resumen criptográfico, el **par de claves**, el **certificado** y la **cadena de confianza**, la **revocación** y el **sello de tiempo**, y los tres **niveles** de firma electrónica. Todos se explican en los capítulos tres y cuatro del primer tomo, y el glosario de este libro los resume.

01

CAPÍTULO UNO

Cómo muere una firma.

Una firma digital no se borra ni se destiñe. Se vuelve inverificable. Este capítulo enumera las seis causas por las que eso ocurre y la idea que permite enfrentarlas.

Imaginemos un contrato firmado digitalmente en 2026 que debe exhibirse ante un tribunal en 2046. El archivo se conservó sin un solo cambio. El juez, o el perito que lo asiste, abre el documento en un validador. ¿Qué puede salir mal? Mucho más de lo que parece. La firma depende de un conjunto de elementos externos al documento, y cada uno de ellos tiene su propio ciclo de vida.



FIGURA 1 Seis maneras en que una firma digital deja de poder verificarse, aunque el archivo se conserve intacto.

El certificado vence

Todo certificado tiene una fecha de vencimiento, habitualmente entre uno y cinco años después de su emisión. Pasada esa fecha, el certificado ya no sirve para firmar. Eso no invalida las firmas hechas mientras estaba vigente, pero obliga a demostrar que la firma se hizo antes del vencimiento. Sin una prueba fiable del momento de la firma, un validador en 2046 sólo verá un certificado vencido hace dieciocho años y no podrá concluir nada.

El certificado es revocado

Un certificado puede ser revocado antes de vencer, por ejemplo porque su titular denunció la pérdida de su tarjeta. Las firmas hechas antes de la revocación siguen siendo válidas; las posteriores, no. Otra vez, todo depende de saber cuándo se firmó y cuál era el estado del certificado en ese momento. Y hay un agravante: las autoridades de certificación no están obligadas a mantener para siempre la información sobre certificados vencidos. Una consulta hecha veinte años después puede no obtener respuesta.

La autoridad desaparece

Las autoridades de certificación son organizaciones, y las organizaciones cierran, se fusionan o pierden su acreditación. Cuando eso ocurre, sus servicios de consulta de revocación pueden dejar de funcionar y su certificado raíz puede ser retirado de las listas de confianza. Una firma que dependía de consultar en línea a esa autoridad queda huérfana.

El algoritmo se debilita

Como vimos en el primer tomo, los algoritmos criptográficos tienen una vida útil. Una firma hecha con una función de resumen que más tarde resulta vulnerable a colisiones pierde valor probatorio: alguien podría alegar que el documento firmado fue sustituido por otro con la misma huella. Los organismos de normalización publican periódicamente tablas con los algoritmos y longitudes de clave que consideran seguros, y las fechas a partir de las cuales dejan de serlo.

El formato se vuelve ilegible

Un documento firmado no sirve si no hay programas capaces de abrirlo y de interpretar su firma. Los formatos propietarios, o las variantes poco documentadas de formatos abiertos, son un riesgo de largo plazo. La historia de la informática está llena de archivos que nadie sabe leer.

La confianza cambia de manos

Por último, la decisión sobre qué autoridades merecen confianza no es fija. Las listas oficiales se actualizan, los lectores de PDF modifican sus listas propias, los sistemas operativos retiran raíces comprometidas. Una firma que hoy aparece como confiable en un programa puede aparecer mañana como «no verificada», sin que nada haya cambiado en el documento.

La idea que lo resuelve: congelar la prueba

Las seis amenazas tienen algo en común: dependen de información que vive fuera del documento y que cambia con el tiempo. La respuesta que la industria fue construyendo durante dos décadas es igualmente simple en su principio: **reunir esa información en el momento en que todavía está disponible, guardarla junto a la firma y protegerla a su vez con una prueba de tiempo**.

Concretamente, eso significa incorporar al documento, poco después de firmar, tres cosas: un sello de tiempo que fije cuándo se firmó, los certificados completos de la cadena de confianza y las respuestas de revocación obtenidas en ese momento. Con eso, un validador futuro no necesita consultar a nadie: tiene en el propio documento todo lo que necesita para reconstruir el estado del mundo el día de la firma. Y para que esa información no pueda ser alterada ni pierda valor cuando los algoritmos envejezcan, se la protege con sellos de tiempo sucesivos, renovados antes de que los anteriores se debiliten.

Esa idea, aplicada de manera sistemática, dio origen a los niveles de firma que estudiaremos en el capítulo tres. Antes conviene conocer los formatos que la hacen posible.

PARA RECORDAR

Una firma digital no se conserva sólo conservando el archivo. Se conserva conservando la **prueba de cuándo se firmó**, la **cadena de certificados** y el **estado de revocación** de ese momento, protegidos a su vez contra el paso del tiempo.

02

CAPÍTULO DOS

Cuatro formatos y un contenedor.

Una firma digital tiene que vivir en algún lugar: dentro del documento, alrededor de él o a su lado. Las respuestas a esa pregunta dieron lugar a una familia de formatos normalizados en Europa y usados en todo el mundo.

Una firma, técnicamente, es un bloque de datos: el valor criptográfico de la firma, el certificado del firmante y un conjunto de atributos, como la hora declarada de la firma o el motivo. Ese bloque tiene que asociarse al documento firmado de alguna manera y con una estructura que cualquier programa pueda interpretar. Durante los años noventa cada fabricante resolvió esto a su modo. A partir del año 2000, el Instituto Europeo de Normas de Telecomunicaciones, conocido por su sigla ETSI, empezó a publicar especificaciones comunes que hoy forman la base de la firma avanzada en Europa y en buena parte del mundo.

Tres maneras de relacionar firma y documento

Antes de hablar de formatos conviene distinguir tres configuraciones básicas, que aparecen en todos ellos.

- **Firma envuelta.** La firma vive dentro del documento. Es el caso del PDF firmado: el archivo contiene a la vez el contenido y la firma, y un lector corriente puede mostrar ambos.
- **Firma envolvente.** La firma contiene al documento. El resultado es un nuevo archivo, con otra extensión, que hay que abrir con un programa capaz de extraer el contenido.

- **Firma separada.** La firma vive en un archivo aparte, que remite al documento por su huella. El documento original queda intacto, pero hay que conservar juntos los dos archivos.



FIGURA 2 Tres maneras de relacionar firma y documento. Todos los formatos de la familia europea admiten al menos una de ellas.

CAdES: la firma de cualquier cosa

CAdES deriva de un estándar más antiguo y muy difundido, la sintaxis de mensajes criptográficos conocida como CMS, heredera a su vez de especificaciones que una empresa de seguridad publicó en los noventa. Es un formato binario, compacto y agnóstico respecto del contenido: puede firmar un PDF, una imagen, un archivo comprimido o cualquier secuencia de bytes. Se usa mucho en firmas separadas y en sistemas que firman grandes volúmenes de datos, como la facturación electrónica de algunos países. Su norma actual es la EN 319 122.

XAdES: la firma de los documentos estructurados

XAdES se apoya en la firma XML definida por el consorcio W3C y está pensado para documentos estructurados en ese lenguaje. Permite firmar un documento entero o sólo algunas de sus partes, lo que lo hizo muy popular en el intercambio de datos entre sistemas, en la administración electrónica y en la factura electrónica de numerosos países latinoamericanos y europeos. Su norma actual es la EN 319 132.

PAdES: la firma que se ve

PAdES define cómo incorporar firmas avanzadas dentro de un PDF. Su gran ventaja es la experiencia: el documento firmado se abre con cualquier lector, la firma puede tener una representación visible en la página y el lector puede mostrar su estado. Por eso es el formato dominante en procesos donde intervienen personas. Se publicó por primera vez en 2009 y su norma actual es la EN 319 142. Le dedicamos el capítulo cuatro.

JAdES: la firma de las interfaces

JAdES es el miembro más joven de la familia, publicado en 2021. Se basa en las firmas para el formato JSON, el lenguaje en que hoy se comunican la mayoría de las aplicaciones web y las interfaces de programación. Está pensado para firmar mensajes entre sistemas y credenciales digitales, y es probable que gane peso con las carteras de identidad, que manejan credenciales en formatos de esa familia.

ASiC: el contenedor

ASiC no es un formato de firma sino un contenedor: un archivo comprimido con una estructura definida que reúne uno o varios documentos con sus firmas, sean CAdES o XAdES. Resuelve el problema de las firmas separadas, que obligan a conservar juntos varios archivos, y permite firmar en un solo acto un conjunto de documentos de cualquier tipo. Algunos países lo adoptaron como formato estándar para documentos firmados que no son PDF.

FORMATO	BASE TÉCNICA	USO TÍPICO	NORMA
CAdES	CMS, binario	Cualquier archivo, firmas separadas, grandes volúmenes	EN 319 122
XAdES	Firma XML	Documentos estructurados, intercambio entre sistemas, factura electrónica	EN 319 132
PAdES	PDF con firma CMS	Documentos que leen y firman personas	EN 319 142
JAdES	Firma JSON	Mensajes entre sistemas, credenciales	TS 119 182
ASiC	Contenedor comprimido	Conjuntos de documentos con sus firmas	EN 319 162

Por qué importan las normas

Estos formatos comparten un vocabulario de atributos y una lógica de niveles, de modo que una firma producida por un programa puede ser validada por otro de un fabricante distinto. Esa interoperabilidad es la garantía más importante contra la amenaza del formato ilegible que vimos en el capítulo anterior. Un documento firmado con un formato normalizado y abierto podrá leerse mientras exista alguien que implemente la norma, y las normas europeas cuentan con implementaciones de referencia de código abierto, mantenidas con apoyo público, que cualquiera puede usar.

La recomendación práctica es sencilla: ante cualquier solución de firma, preguntar qué formato produce y con qué norma cumple, y desconfiar de los formatos que sólo pueden validarse con las herramientas del propio proveedor.

03

CAPÍTULO TRES

Cuatro escalones hacia la permanencia.

Los formatos europeos definen niveles sucesivos que agregan, uno sobre otro, las pruebas que una firma necesita para sobrevivir al tiempo. Entenderlos es entender cuánto puede durar una firma.

No hay que confundir estos niveles con los niveles jurídicos del primer tomo. Aquellos, simple, avanzado y cualificado, describen cuánto confía la ley en una firma. Estos describen cuánta prueba técnica lleva consigo una firma para poder ser verificada en el futuro. Son dos ejes distintos: una firma cualificada puede tener un nivel técnico básico y quedar indefensa en pocos años, y una firma avanzada puede estar perfectamente preparada para durar décadas.

Las normas actuales de ETSI definen cuatro niveles, comunes a CAdES, XAdES, PAdES y JAdES. Se los designa con las letras B, T, LT y LTA, a menudo precedidas por el nombre del formato.

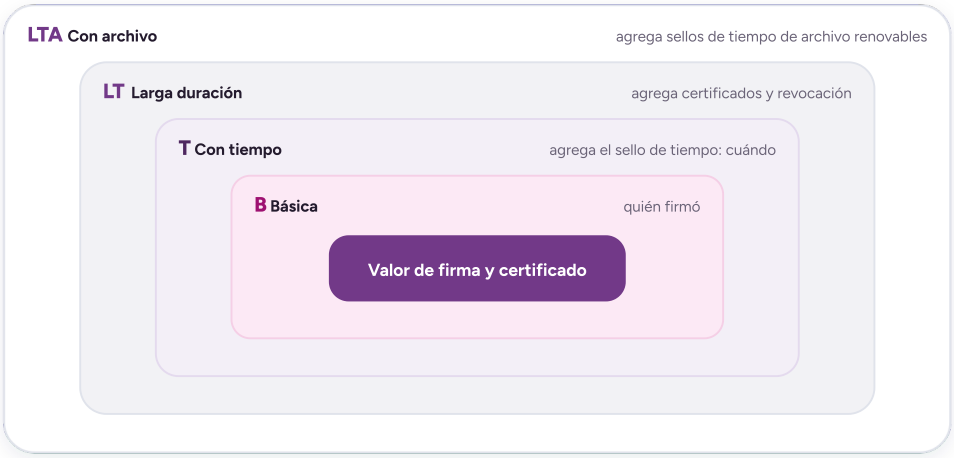


FIGURA 3 Los cuatro niveles técnicos de una firma avanzada. Cada capa envuelve a la anterior y agrega la prueba que le falta para durar.

Nivel B: la firma básica

Es la firma tal como sale del acto de firmar: el valor criptográfico, el certificado del firmante y algunos atributos obligatorios, en particular una referencia protegida a ese certificado, que impide sustituirlo por otro con la misma clave. Una firma de nivel B prueba que alguien con la clave privada firmó ese contenido. No prueba cuándo, y su verificación depende de que, en el momento de validar, se pueda todavía consultar la cadena de certificados y su estado de revocación.

Una firma de nivel B es suficiente para una validación inmediata, pero empieza a perder fuerza en cuanto el certificado vence.

Nivel T: la firma con tiempo

Al nivel B se le agrega un sello de tiempo emitido por una autoridad de sellado de tiempo, aplicado sobre el valor de la firma. A partir de ese momento hay una prueba independiente de que la firma existía en una fecha y hora concretas. Esto resuelve el problema del certificado que vence o es revocado después de firmar: basta con comprobar que el sello de tiempo es anterior al vencimiento o a la revocación.

El nivel T es el mínimo razonable para cualquier documento que deba conservar valor más allá de unos pocos meses.

Nivel LT: la firma autosuficiente

Al nivel T se le agrega el material de validación: todos los certificados de la cadena, hasta la raíz, y las respuestas de revocación, sean listas o respuestas del protocolo OCSP, obtenidas después del sello de tiempo. Las siglas vienen del inglés *long term*, larga duración.

Con el nivel LT, la firma deja de depender de servicios externos. Un validador dentro de veinte años no necesitará consultar a la autoridad de certificación, que puede haber dejado de existir: encontrará en el documento la evidencia de que el certificado era válido cuando se firmó. Es la respuesta a las amenazas del certificado revocado y de la autoridad que desaparece.

Nivel LTA: la firma archivable

Queda una amenaza sin resolver: la del algoritmo que envejece. Todo lo que el nivel LT reunió está protegido por firmas y sellos de tiempo hechos con los algoritmos de hoy. Si dentro de quince años esos algoritmos se debilitan, alguien podría alegar que el material de validación fue fabricado después.

El nivel LTA, de *long term with archive*, agrega un sello de tiempo de archivo que cubre todo lo anterior: la firma, su sello de tiempo, los certificados y las respuestas de revocación. Ese sello de tiempo de archivo puede renovarse periódicamente, con algoritmos más robustos, antes de que el anterior se debilite. Cada renovación cubre todo lo que había antes, incluido el sello de tiempo previo, y así se forma una cadena de sellos de tiempo que extiende la vida de la firma de manera indefinida.

UNA IMAGEN ÚTIL

Pensemos en una carta guardada en una caja fuerte. El nivel B es la carta firmada. El nivel T agrega el matasellos del correo. El nivel LT agrega, dentro del sobre, copias certificadas de los documentos que prueban que el firmante era quien decía ser el día del matasellos. El nivel LTA guarda todo eso en una caja con un precinto fechado, y cada pocos años un escribano verifica el precinto y coloca encima uno nuevo, más resistente.

Quién agrega cada nivel

Los niveles no tienen por qué agregarse todos en el momento de firmar. El nivel B lo produce quien firma. El sello de tiempo del nivel T puede pedirlo quien firma o la plataforma inmediatamente después. El material de validación del nivel LT conviene incorporarlo lo antes posible, pero idealmente después de un breve período de gracia, para dar tiempo a que una eventual revocación hecha justo antes de la firma llegue a publicarse. El sello de tiempo de archivo del nivel LTA puede agregarlo la plataforma al cerrar el proceso o un servicio de conservación más adelante.

Esta distribución tiene consecuencias de diseño. Una plataforma que coordina procesos de firma está en una posición privilegiada para elevar el nivel de las firmas que recoge: conoce el momento de cada firma, puede pedir sellos de tiempo y respuestas de revocación a servicios de terceros y puede aplicar el sello de tiempo de archivo cuando el último firmante termina.

Cuando un servicio externo no responde

Elevar el nivel requiere contactar servicios externos: autoridades de sellado de tiempo, servicios de revocación. Esos servicios pueden fallar. Una buena práctica, que conviene exigir, es que la plataforma tenga alternativas configuradas para cada servicio y, si aun así no logra alcanzar el nivel previsto, que deje el documento en el nivel efectivamente alcanzado, lo informe con claridad y lo deje registrado, en lugar de fallar en silencio o de aparentar un nivel que no tiene. Un documento de nivel T declarado como tal es mucho más útil que uno que dice ser LTA y no lo es.

PARA RECORDAR

B prueba quién firmó. **T** agrega cuándo. **LT** guarda dentro del documento la prueba de que el certificado era válido en ese momento. **LTA** protege todo lo anterior con sellos de tiempo renovables contra el envejecimiento de los algoritmos.

04

CAPÍTULO CUATRO

Lo que pasa dentro de un PDF.

El PDF es el soporte de la mayoría de los documentos firmados del mundo. Su manera de alojar firmas tiene particularidades que explican muchos de los mensajes, a veces desconcertantes, que muestran los lectores.

Un archivo que crece por capas

La característica más importante del PDF para entender la firma es la actualización incremental. Cuando se modifica un PDF, el programa no tiene por qué reescribir el archivo: puede agregar al final una nueva sección que describe los cambios, dejando intacto todo lo anterior. El archivo crece como una cebolla, por capas, y cada capa es una *revisión* del documento.

La firma aprovecha este mecanismo. Cuando alguien firma un PDF, se agrega una revisión que contiene la firma, y la firma cubre todos los bytes del archivo hasta ese punto, salvo el espacio reservado para el propio valor de la firma. Si después firma otra persona, se agrega una nueva revisión que cubre todo lo anterior, incluida la primera firma. Cada firma protege la versión del documento que existía en el momento en que se hizo.



FIGURA 4 Un PDF firmado crece por revisiones. Cada firma cubre todo lo que había hasta ella; el sello de tiempo del documento cubre el archivo completo, incluido el material de validación.

Esto tiene una consecuencia importante: un PDF firmado puede seguir cambiando sin que las firmas anteriores se rompan, porque cada una sigue protegiendo su propia revisión. Un validador puede mostrar, para cada firma, exactamente qué versión del documento firmó esa persona y qué cambió después. La pregunta pasa a ser si esos cambios posteriores estaban permitidos.

Qué se puede cambiar después de firmar

El formato prevé dos mecanismos para declarar qué cambios se admiten después de una firma.

La certificación del documento

La primera firma de un documento puede ser una *firma de certificación*, que además de firmar declara qué cambios posteriores se aceptan. Hay tres opciones: ningún cambio; sólo completar formularios y agregar firmas; o, además, agregar anotaciones y comentarios. Un lector que respete la norma marcará como alterado un documento que recibió cambios fuera de lo permitido, aunque cada firma individual siga siendo matemáticamente válida. En la especificación este mecanismo se llama DocMDP.

El bloqueo de campos

El segundo mecanismo, llamado FieldMDP, permite que cada firma bloquee determinados campos del formulario. Así, cuando un firmante completa el importe y firma, puede impedir que el siguiente cambie ese importe, aunque el documento siga admitiendo que otros completen sus propios campos. Es la herramienta que hace posibles los procesos donde varias personas completan datos y firman sobre el mismo documento.

POR QUÉ UN LECTOR DICE «MODIFICADO»

Buena parte de los avisos que alarman a los usuarios se explican por estas reglas. Un documento que alguien abrió y guardó de nuevo con un programa que reescribe el archivo, o al que se le agregó un comentario cuando la certificación no lo permitía, puede aparecer como modificado aunque el contenido visible sea idéntico. La firma no miente: el archivo cambió.

La apariencia no es la firma

Una firma en un PDF puede tener una representación visible: un recuadro con el nombre del firmante, la fecha, un logotipo o la imagen de una rúbrica. Esa representación es sólo eso, una imagen. La firma real es el bloque criptográfico invisible asociado al campo. Copiar la imagen a otro documento no copia la firma, y un documento puede estar firmado sin ninguna representación visible.

Esta distinción, obvia para un técnico, no lo es para muchos usuarios, que confían en lo que ven. Por eso una buena práctica es que la representación visible remita a algo verificable, como un código que lleve a un validador, y que nunca se presente una imagen como si fuera la firma.

Dónde se guarda la prueba de largo plazo

Para alcanzar los niveles LT y LTA del capítulo anterior, el PDF necesita un lugar donde guardar los certificados y las respuestas de revocación. Las normas definen para ello un almacén de seguridad del documento, una estructura que se agrega en una revisión posterior a la firma y que reúne todo el material de validación. El sello de tiempo de

archivo, a su vez, toma la forma de un *sello de tiempo del documento*: una firma especial, emitida por una autoridad de sellado de tiempo, que cubre el archivo completo hasta ese punto, incluido el almacén.

Los lectores más difundidos identifican los documentos que tienen este material como «habilitados para validación a largo plazo».

PDF/A: el PDF para archivo

El formato PDF admite elementos que dificultan la conservación: fuentes no incrustadas, contenido que depende de recursos externos, código ejecutable. La familia de normas ISO 19005, conocida como PDF/A, define subconjuntos del PDF pensados para archivo a largo plazo, que exigen, entre otras cosas, incrustar todas las fuentes y prohíben el contenido dinámico.

Para documentos que deben conservarse durante décadas, conviene que el documento sea PDF/A antes de la primera firma. Convertirlo después no es posible sin romper las firmas, porque la conversión reescribe el archivo. Este detalle, que parece menor, es una de las causas más frecuentes de documentos firmados que no cumplen los requisitos de archivo de una organización.

Firmar no es aplanar

Una última advertencia práctica. Algunas herramientas, al terminar un proceso de firma, generan un PDF nuevo que reproduce el contenido y las firmas visibles, pero sin las firmas criptográficas, o con una sola firma de la plataforma que cubre todo. Ese documento puede ser útil para leer, pero no conserva la prueba individual de cada firmante. Ante cualquier solución conviene preguntar si el documento final contiene las firmas de cada participante, cada una sobre su revisión, o una reconstrucción.

05

CAPÍTULO CINCO

El reloj en el que todos confían.

La pregunta «¿cuándo?» atraviesa todo este tomo. Los sellos de tiempo son la respuesta técnica a esa pregunta, y su historia empieza con un problema de propiedad intelectual.

Un problema de laboratorio

En 1991, dos investigadores de un laboratorio de investigación en telecomunicaciones de los Estados Unidos, Stuart Haber y W. Scott Stornetta, publicaron un artículo cuyo título planteaba sin rodeos la pregunta: cómo sellar con tiempo un documento digital. El problema que les interesaba era el de los cuadernos de laboratorio: cómo probar que una idea o un resultado existía en cierta fecha, cuando los archivos digitales pueden modificarse sin dejar rastro y el reloj de una computadora puede ajustarse a voluntad.

Su propuesta tenía dos partes. La primera, confiar en un tercero que recibe la huella de un documento, le agrega la hora y firma el conjunto. La segunda, más original, encadenar los sellos de tiempo entre sí, de modo que cada uno incluya información de los anteriores. Así, ni siquiera el propio tercero podría fabricar un sello de tiempo con fecha pasada sin alterar toda la cadena posterior. Años después, una empresa fundada a partir de esas ideas empezó a publicar periódicamente una huella resumen de todos sus sellos de tiempo en los avisos clasificados de un diario de circulación masiva, un ancla que nadie podía alterar después de impresa. Esa idea de anclar una cadena en un medio público e inmutable reaparece hoy en muchos sistemas de evidencia.

El protocolo que se impuso

En 2001 se publicó el documento RFC 3161, que definió el protocolo de sellado de tiempo que hoy usan casi todos los sistemas de firma. Su funcionamiento es sencillo.

1. Quien necesita el sello de tiempo calcula la huella del dato a sellar, que puede ser un documento o, más a menudo, el valor de una firma. Sólo envía la huella: la autoridad nunca ve el contenido.
2. La autoridad de sellado de tiempo recibe la huella, toma la hora de un reloj confiable, arma una estructura con la huella, la hora, un número de serie y la precisión declarada, y la firma con su propia clave.
3. El sello de tiempo vuelve a quien lo pidió, que lo incorpora a la firma o lo guarda junto al documento.
4. Cualquiera puede verificar después que el sello de tiempo corresponde a esa huella y que lo firmó la autoridad, cuyo certificado tiene un uso específico para sellar tiempo.



FIGURA 5 Cómo se obtiene un sello de tiempo. La autoridad sólo recibe la huella, nunca el documento, y devuelve una estructura firmada con la hora de su reloj.

De dónde sale la hora

Un sello de tiempo vale lo que vale el reloj de la autoridad. Las autoridades serias sincronizan sus relojes con fuentes trazables al tiempo universal coordinado, como los laboratorios nacionales de metrología o señales satelitales, y vigilan permanentemente la desviación. Las normas europeas para autoridades de sellado de tiempo exigen una precisión de al menos un segundo respecto del tiempo universal y que la autoridad deje de emitir sellos de tiempo si pierde la sincronización.

El sello de tiempo cualificado

El reglamento eIDAS reconoce el sello de tiempo electrónico cualificado, emitido por un prestador supervisado que cumple esos requisitos. Su efecto jurídico es una presunción: se presume la exactitud de la fecha y hora que indica y la integridad de los

datos a los que se refiere. Como ocurre con la firma cualificada, esa presunción se reconoce en todos los Estados miembros. Fuera de Europa, varios países tienen esquemas de acreditación propios para autoridades de sellado de tiempo.

Qué prueba y qué no

Un sello de tiempo prueba que un dato existía **antes** de cierto momento. No prueba que no existiera antes, ni quién lo creó, ni que la hora declarada en la firma sea la verdadera. Si una firma dice haber sido hecha a las diez y el sello de tiempo es de las diez y cinco, lo único que sabemos con certeza es que existía a las diez y cinco. Para la mayoría de los usos eso es exactamente lo que importa: que la firma existía mientras el certificado era válido.

Redundancia y degradación

Depender de una sola autoridad de sellado de tiempo es un riesgo operativo: si no responde, no hay sello de tiempo, y la firma queda en nivel básico. Por eso las plataformas maduras configuran varias autoridades con un orden de preferencia, y documentan qué hacen si ninguna responde. Algunas reintentan más tarde y elevan el nivel en cuanto pueden; otras detienen el proceso. Lo que nunca debería ocurrir es que el sistema siga adelante como si hubiera obtenido el sello de tiempo.

Hay también una cuestión de costo. Los sellos de tiempo cualificados suelen cobrarse por unidad, y un proceso con muchas firmas puede requerir muchos sellos de tiempo. Por eso es habitual distinguir entre el sello de tiempo sobre cada firma, que da nivel T, y el sello de tiempo de archivo sobre el documento completo, que se aplica una sola vez al cerrar el proceso y da nivel LTA.

PARA RECORDAR

Un sello de tiempo es una firma de un tercero sobre una huella y una hora. Prueba que algo existía antes de ese momento, sin revelar su contenido. Su valor depende de la confianza en la autoridad y en su reloj, y por eso conviene que sea cualificado o acreditado, y que haya más de uno disponible.

06

CAPÍTULO SEIS

Válida, inválida o indeterminada.

Validar una firma parece una pregunta de sí o no. En realidad es un procedimiento con varias etapas, una política que decide qué se exige y tres respuestas posibles, una de las cuales es «todavía no se puede saber».

Cuando un lector de PDF muestra una marca verde junto a una firma, está resumiendo en un ícono un proceso bastante complejo. Ese proceso está normalizado en Europa por la norma EN 319 102, que describe paso a paso cómo debe validarse una firma avanzada y qué resultados puede producir. Conocerlo ayuda a interpretar lo que dicen los validadores y, sobre todo, lo que no dicen.

Las preguntas que hace un validador

1. **¿El documento está intacto?** Se recalcula la huella del contenido firmado y se comprueba que la firma corresponde a esa huella con la clave pública del certificado.
2. **¿El certificado es el que dice ser?** Se comprueba que la referencia protegida al certificado dentro de la firma coincide con el certificado incluido.
3. **¿La cadena llega a una raíz confiable?** Se construye la cadena de certificados hasta una raíz y se comprueba que esa raíz figura entre las anclas de confianza que el validador acepta.
4. **¿Cuál es el momento de referencia?** Si hay un sello de tiempo válido, la firma se evalúa en el momento que fija ese sello de tiempo. Si no, sólo puede evaluarse en el momento presente.

5. **¿El certificado era válido en ese momento?** Se comprueba que no estaba vencido ni revocado, usando la información de revocación incluida en el documento o consultada en línea.
6. **¿Los algoritmos eran y siguen siendo aceptables?** Se comprueba que los algoritmos y longitudes de clave estaban permitidos en el momento de referencia, y que la protección de la firma no depende de algoritmos que hoy se consideran rotos.
7. **¿Se cumplen los requisitos de la política?** Por ejemplo, si la política exige un certificado cualificado, se comprueba que lo es.

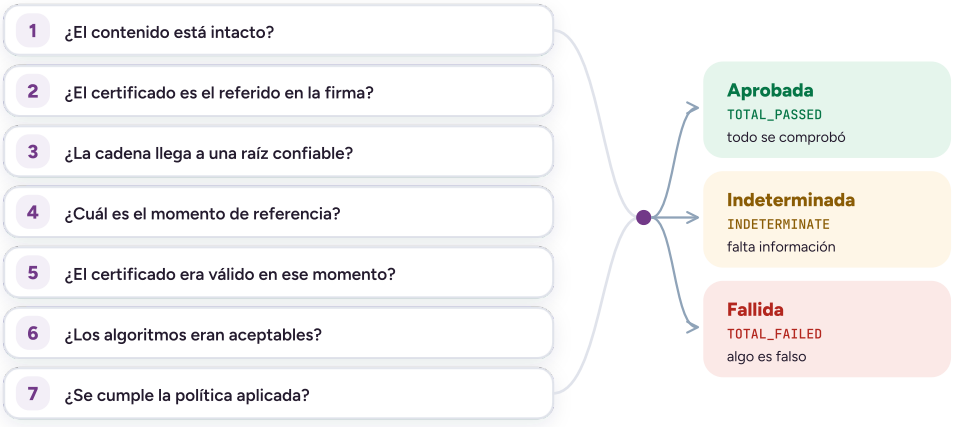


FIGURA 6 El recorrido de una validación y sus tres resultados posibles. Indeterminada no significa falsa: significa que falta información para decidir.

Tres resultados, no dos

La norma prevé tres conclusiones posibles, cuyos nombres técnicos se han vuelto habituales en los informes de validación.

- **Aprobada** (TOTAL_PASSED). Todas las comprobaciones resultaron positivas según la política aplicada.
- **Fallida** (TOTAL_FAILED). Alguna comprobación resultó negativa de manera definitiva: el documento fue alterado, la firma no corresponde, el certificado estaba revocado antes de firmar.

- **Indeterminada** (INDETERMINATE). Con la información disponible no es posible concluir. Puede faltar la información de revocación, la raíz puede no estar entre las confiables o puede no haber prueba de que la firma sea anterior a una revocación.

El resultado indeterminado es el más frecuente en la práctica y el más malinterpretado. No significa que la firma sea falsa. Significa que falta algo para decidir. Muchas veces ese algo puede conseguirse: incorporando una lista de confianza, obteniendo la información de revocación o encontrando un sello de tiempo. Un buen informe de validación dice exactamente qué faltó.

La política de validación

Validar siempre es validar *según algo*. La política de validación define qué anclas de confianza se aceptan, qué algoritmos se admiten y hasta cuándo, qué tipo de certificado se exige, si hace falta un sello de tiempo, qué tolerancia hay para la información de revocación. Dos validadores con políticas distintas pueden dar resultados distintos para el mismo documento, y ambos tener razón.

Esto explica muchas discrepancias entre programas. Un lector de PDF de uso general aplica una política pensada para la mayoría de sus usuarios, con su propia lista de raíces. Un validador oficial europeo aplica una política basada en las listas de confianza de los Estados miembros. Un validador nacional puede aceptar sólo los prestadores acreditados en su país. Cuando una firma aparece válida en uno e indeterminada en otro, lo primero es preguntar qué política aplicó cada uno.

UN CASO TÍPICO

Una firma cualificada emitida por un prestador de un país latinoamericano se abre en un lector europeo y aparece como «no verificada». La firma es perfectamente válida en su país. El lector simplemente no tiene esa raíz entre sus anclas. La solución no es desconfiar de la firma sino validar con la lista de confianza que corresponde.

Los validadores

Existen validadores de distintos tipos. Los lectores de PDF incluyen uno, cómodo pero limitado a su política. Los organismos públicos de varios países ofrecen validadores en línea basados en sus listas oficiales. La Comisión Europea mantiene una biblioteca de código abierto para crear y validar firmas según las normas europeas, que sirve de referencia para muchos productos y que cualquiera puede usar. Y las plataformas de firma suelen ofrecer validadores propios.

El reglamento eIDAS prevé además un servicio cualificado de validación, prestado por un tercero supervisado, cuyo resultado tiene especial valor probatorio. Para documentos de alto valor, conviene que la validación no dependa sólo de las herramientas de quien produjo la firma.

Lo que un buen validador debería mostrar

- El resultado global y, para cada firma, el resultado individual.
- La revisión del documento que cubre cada firma y los cambios posteriores, indicando si estaban permitidos.
- La cadena de certificados completa, con la raíz y la lista de confianza que la avala.
- El momento de referencia y la prueba en que se basa, como el sello de tiempo.
- La información de revocación usada, con su origen y fecha.
- El nivel técnico alcanzado, de B a LTA, y el nivel jurídico, si puede determinarse.
- Qué no pudo comprobar y por qué.

El último punto es el que más distingue a un validador honesto. En un dominio donde la confianza lo es todo, decir con claridad qué no se comprobó vale tanto como decir qué se comprobó.

07

CAPÍTULO SIETE

Quién decide en quién confiar.

Toda cadena de confianza termina en una decisión humana. Las listas de confianza convierten esa decisión en un documento público, firmado y verificable por máquinas.

En el primer tomo vimos que la cadena de certificados termina en una raíz en la que se confía por decisión explícita. La pregunta es quién toma esa decisión. Durante mucho tiempo la tomaron, de hecho, los fabricantes de software: cada sistema operativo, cada navegador y cada lector de PDF incluye una lista de raíces que considera confiables, elaborada con criterios propios. Para la navegación web ese modelo funciona razonablemente bien. Para la firma con efectos jurídicos tiene un problema evidente: la decisión sobre qué firmas valen ante la ley no debería depender de una empresa privada extranjera.

La respuesta europea

La Unión Europea resolvió el problema con un sistema de listas de confianza, cuyo formato está normalizado en la especificación TS 119 612 de ETSI. Cada Estado miembro publica una lista firmada con los prestadores de servicios de confianza que supervisa, los servicios que cada uno presta, su estado actual y la historia de ese estado. La Comisión Europea publica a su vez una lista de listas que indica dónde está la lista de cada país y con qué certificado está firmada.

Un validador que quiere saber si una firma es cualificada parte de la lista de listas, descarga la lista del país correspondiente, verifica su firma, busca al prestador, comprueba que el servicio que emitió el certificado estaba en estado cualificado en el momento de la firma y, sólo entonces, concluye. Todo el proceso es automático y no depende de ninguna lista privada.



FIGURA 7 El sistema europeo de listas de confianza. Una lista de listas señala las listas nacionales, que describen a cada prestador, sus servicios y su estado a lo largo del tiempo.

Más que una lista de raíces

Las listas de confianza contienen más información que una simple lista de certificados raíz. Describen cada servicio con su tipo, sea emisión de certificados, sellado de tiempo, validación o conservación, y su estado a lo largo del tiempo. Esto permite responder preguntas como «¿este prestador estaba acreditado para emitir certificados cualificados en marzo de 2024?», que es exactamente lo que necesita un validador que evalúa una firma en el momento en que se hizo.

Las listas de los fabricantes

Los fabricantes de software no se quedaron al margen. El lector de PDF más difundido mantiene desde hace años un programa propio de raíces aprobadas para firma de documentos, y con el tiempo incorporó también la lista europea. Esto mejora mucho la experiencia de los usuarios europeos, pero deja una asimetría: una firma perfectamente válida emitida por un prestador acreditado en un país que no está en ninguna de esas listas puede aparecer como no verificada en millones de computadoras.

América Latina y el reconocimiento regional

Varios países latinoamericanos publican listas oficiales de sus prestadores acreditados, y algunos ya lo hacen en el formato normalizado europeo, lo que permite que los validadores las procesen automáticamente. La Red de Gobierno Electrónico de América Latina y el Caribe impulsó trabajos para armonizar esas listas y facilitar el reconocimiento mutuo, y en el Mercosur se firmaron acuerdos con el mismo objetivo. El camino hacia un reconocimiento transfronterizo automático, como el europeo, está en marcha pero no terminado.

Para una plataforma que opera en varios países, esto significa que no basta con confiar en las raíces del sistema operativo. Necesita leer y verificar las listas oficiales de cada jurisdicción en la que opera, mantenerlas actualizadas y aplicar, para cada firma, la lista que corresponde al país del acto.

Una lista también se firma y también envejece

Una lista de confianza es un documento firmado por la autoridad que la publica, y como tal debe validarse. Su firma usa certificados que a su vez vencen y se renuevan; la lista de listas europea indica qué certificados son válidos para firmar cada lista nacional. Además, las listas se actualizan con frecuencia y tienen una fecha prevista para la próxima publicación. Un validador riguroso verifica la firma de cada lista, rechaza las que están vencidas y guarda la versión usada para cada validación, de modo que el resultado pueda reproducirse años después.

PARA RECORDAR

Las listas de confianza trasladan la decisión de en quién confiar desde los fabricantes de software hacia las autoridades públicas, en un formato firmado y legible por máquinas. Son la base del reconocimiento transfronterizo de las firmas cualificadas y una pieza indispensable de cualquier validación rigurosa.

08

CAPÍTULO OCHO

Treinta años en una caja.

Conservar un documento firmado no es lo mismo que guardarlo. Este capítulo describe qué hace falta para que una firma siga siendo demostrable cuando ya nadie recuerda cómo se hizo.

Muchas organizaciones deben conservar documentos durante plazos muy largos: los contratos de crédito hipotecario, durante toda la vida del préstamo y algunos años más; las historias clínicas, durante décadas; ciertos actos administrativos, de manera permanente. Durante todo ese tiempo, la firma debe poder demostrarse. Los capítulos anteriores mostraron las piezas que lo hacen posible. Este las ordena en una estrategia.

Tres capas de conservación

Conservar los bits

Lo primero es que el archivo exista y no cambie. Esto exige copias en lugares distintos, comprobación periódica de su integridad mediante huellas, y migración a nuevos soportes cuando los anteriores envejecen. Es la disciplina clásica de la preservación digital, y la firma la hace más exigente: un solo bit alterado invalida la firma, aunque el documento siga viéndose igual. Los almacenamientos que impiden modificar o borrar un objeto durante un período definido, conocidos como almacenamientos de escritura única, son una herramienta habitual en esta capa.

Conservar la legibilidad

Lo segundo es que el archivo pueda leerse. Por eso se prefieren formatos abiertos y normalizados, como PDF/A para los documentos y los formatos europeos para las firmas, que cuentan con múltiples implementaciones independientes.

Conservar la prueba

Lo tercero, y propio de la firma, es que la prueba siga siendo demostrable. Esto exige que cada firma alcance al menos el nivel LT, con su material de validación incorporado, y que se proteja con sellos de tiempo de archivo renovados antes de que los algoritmos que los sostienen se debiliten.

La renovación de los sellos de tiempo de archivo

La renovación es el corazón de la conservación de largo plazo. Funciona así: periódicamente, o cuando las autoridades anuncian que un algoritmo o una longitud de clave dejará de considerarse segura, se aplica un nuevo sello de tiempo de archivo que cubre todo lo existente, incluidos los sellos de tiempo anteriores, usando algoritmos y claves más robustos. Antes de aplicarlo se incorpora el material de validación del sello de tiempo anterior, para que también ese sello de tiempo pueda verificarse en el futuro.

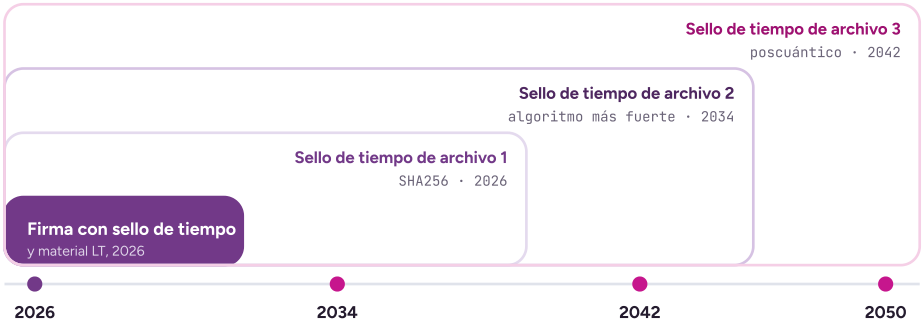


FIGURA 8 La renovación de los sellos de tiempo de archivo. Cada sello de tiempo nuevo, con algoritmos más robustos, cubre la firma y todos los sellos de tiempo anteriores.

El resultado es una cadena de sellos de tiempo en la que cada eslabón protege a los anteriores. Aunque el algoritmo del primer sello de tiempo se rompa, el segundo sello de tiempo prueba que todo lo que cubría existía antes de que eso ocurriera, y por lo tanto no pudo haber sido fabricado con el ataque. La cadena puede extenderse indefinidamente, siempre que se renueve a tiempo.

Los registros de evidencia

Renovar sellos de tiempo documento por documento es costoso cuando hay millones de documentos. Para resolverlo, el organismo de estandarización de internet publicó en 2007 la especificación de los registros de evidencia, conocida como RFC 4998. Su idea es agrupar las huellas de muchos documentos en una estructura de árbol, de modo que un solo sello de tiempo sobre la raíz del árbol proteja a todos. Cada documento conserva sólo el camino que lo une a la raíz, una prueba pequeña que permite demostrar que formaba parte del conjunto sellado. La renovación se hace sobre el árbol, no sobre cada documento.

Esta técnica, basada en los árboles que Ralph Merkle propuso a fines de los años setenta, es la misma que hoy usan los registros públicos de certificados y muchos sistemas de evidencia. Volveremos a ella en el capítulo siguiente.

El servicio cualificado de conservación

El reglamento eIDAS define un servicio cualificado de conservación de firmas cualificadas y de «sellos electrónicos» cualificados, prestado por un tercero supervisado que se compromete a prolongar la fiabilidad de las firmas más allá de su período de validez tecnológica. Las normas técnicas europeas describen distintos modelos: el servicio puede guardar los documentos, guardar sólo las pruebas o aumentar las firmas que el cliente sigue guardando. Para una organización, contratar un servicio de este tipo traslada la responsabilidad técnica de la renovación a un especialista auditado.

Una política escrita

Ninguna de estas técnicas sirve sin una política que diga qué documentos se conservan, durante cuánto tiempo, con qué nivel, dónde, quién vigila la obsolescencia de los algoritmos y quién decide cuándo renovar. Esa política debe revisarse periódicamente, porque el entorno cambia: aparecen nuevas normas, se anuncian nuevas debilidades, cambian los proveedores.

LISTA DE VERIFICACIÓN

- [ ] Los documentos se convierten a PDF/A antes de la primera firma.
- [ ] Cada firma alcanza al menos nivel LT, y el documento cerrado lleva un sello de tiempo de archivo.
- [ ] Hay copias en al menos dos ubicaciones y se comprueba su integridad periódicamente.
- [ ] Alguien vigila los anuncios sobre algoritmos y tiene la tarea de renovar a tiempo los sellos de tiempo de archivo.
- [ ] Se conservan, junto a los documentos, las listas de confianza y la información usadas para validarlos.
- [ ] La política de conservación está escrita, aprobada y revisada.

09

CAPÍTULO NUEVE

La memoria del proceso.

La firma prueba que alguien firmó un contenido. El registro de evidencia prueba todo lo demás: cómo llegó el documento, quién lo vio, cómo se identificó, qué aceptó. Diseñarlo bien es un arte con reglas propias.

En el primer tomo vimos que los gestores de flujos de firma cambiaron la unidad de análisis: del documento firmado al proceso firmado. Si lo que importa es el proceso, la prueba del proceso es tan importante como la firma misma. Esa prueba es el registro de evidencia: la secuencia ordenada de eventos que la plataforma anota desde que se prepara el envío hasta que se cierra.

Para una firma electrónica simple, el registro es a menudo la prueba principal. Para una firma cualificada, complementa la firma con información que ésta no contiene: qué versión vio el firmante antes de firmar, qué consentimientos dio, qué datos completó, desde qué dispositivo actuó.

Qué registrar

Un buen registro responde, para cada participante, a las preguntas que haría un juez o un auditor. Entre los eventos habituales están:

- la creación y el despacho del envío, con la lista de participantes y sus roles;
- cada notificación enviada y por qué canal;
- cada acceso al documento, con la fecha, la hora y datos técnicos del acceso;
- cada paso de identificación, con el método usado y su resultado;

- la aceptación de los términos y de cualquier consentimiento, con el texto exacto que se aceptó;
- cada campo completado y su valor;
- cada firma, con el método, el prestador y el nivel alcanzado;
- los rechazos, las delegaciones y las anulaciones, con sus motivos;
- el cierre del proceso y la emisión del certificado de finalización.

Cada evento debe identificar a su autor, persona o sistema, y llevar una marca de tiempo tomada de un reloj sincronizado. Los eventos producidos por servicios externos, como un proveedor de identidad o un prestador de firma, deberían incluir la respuesta del servicio o una referencia verificable a ella.

Identificación y autorización, por separado

Una distinción sutil y muy importante: identificarse y autorizar una firma son actos distintos. Una persona puede identificarse al abrir el documento con un proveedor de identidad y, minutos después, autorizar su firma con un código enviado a su teléfono o con el PIN de su tarjeta. Si el registro mezcla ambos actos en un solo evento, se pierde la capacidad de demostrar que la persona que firmó es la misma que se identificó, y en qué momento ocurrió cada cosa.

Cómo proteger el registro

Un registro sólo vale si puede demostrarse que nadie lo alteró. Y la amenaza más seria no viene de afuera, sino de adentro: de quien opera la plataforma, de un administrador con acceso a la base de datos, de un error de software. Por eso las técnicas de protección apuntan a que ni siquiera el operador pueda modificar el registro sin dejar rastro.

El encadenamiento

La primera técnica es encadenar los eventos: cada uno incluye la huella del anterior, como los eslabones de una cadena. Modificar o eliminar un evento cambia su huella y rompe todos los eslabones posteriores. Verificar la cadena es tan simple como recalcular las huellas desde el principio.

Las restricciones en la base de datos

La segunda es impedir, en el propio almacenamiento, que los eventos se modifiquen o borren una vez escritos. Las bases de datos modernas permiten definir tablas en las que sólo se puede agregar, y reglas de aislamiento que impiden que una organización vea o toque los eventos de otra.

El anclaje externo

El encadenamiento tiene un límite: quien controla el sistema podría recalcular la cadena entera después de una modificación. La defensa contra esto es publicar periódicamente la huella del último eslabón, o la raíz de un árbol que resume muchos eventos, en un lugar que el operador no controla: un sello de tiempo de un tercero, un almacenamiento inmutable de otra organización o incluso un medio público. A partir de ese momento, reescribir la historia anterior exigiría falsificar también el ancla, lo que ya no está al alcance del operador.

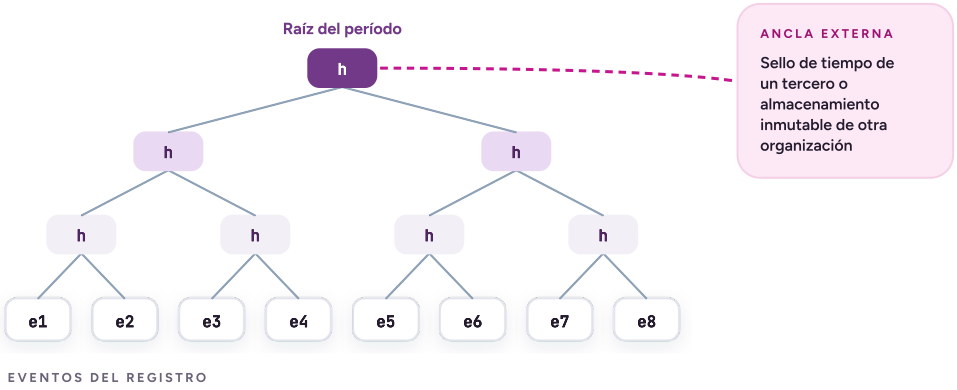


FIGURA 9 Anclar un registro de evidencia. Las huellas de los eventos se combinan de a pares hasta una raíz, y la raíz se publica fuera del control del operador.

Privacidad y minimización

Un registro de evidencia contiene datos personales: nombres, direcciones de correo, números de documento, direcciones de red, a veces datos biométricos. Las leyes de protección de datos exigen que se recojan sólo los necesarios, que se protejan y que se conserven sólo el tiempo justificado. Hay una tensión real entre la vocación de la evidencia por registrar todo y el principio de minimización. Las buenas prácticas

resuelven esa tensión registrando lo necesario para la prueba, guardando huellas en lugar de datos cuando la huella basta, y definiendo plazos de conservación coherentes con los del documento.

El certificado de finalización

El registro completo suele ser extenso y técnico. Por eso las plataformas producen un resumen legible, el certificado de finalización, que acompaña al documento y presenta, para cada participante, los hechos principales: cuándo recibió el documento, cómo se identificó, cuándo firmó. Para que ese resumen tenga valor debe estar firmado por la plataforma o llevar su sello de plataforma y ser coherente con el registro completo, que debe poder exportarse en un formato verificable.

PARA RECORDAR

Un registro de evidencia sólido registra cada hecho relevante con su autor y su hora, separa identificación de autorización, se protege con encadenamiento y con anclas externas que el operador no controla, y respeta la privacidad de quienes aparecen en él.

10

CAPÍTULO DIEZ

Cuando la firma llega a un tribunal.

Todo lo anterior existe para un momento que ojalá nunca llegue: alguien niega haber firmado. Este capítulo describe cómo se examina una firma disputada y qué conviene tener preparado.

La inmensa mayoría de los documentos firmados nunca se discute. Pero el valor de una firma se mide en el caso excepcional: el deudor que afirma no haber firmado el préstamo, el empleado que niega haber aceptado una política, la empresa que sostiene que el contrato fue alterado. En esos casos, la firma electrónica tiene que convencer a alguien que no es técnico, y hacerlo con pruebas que ese alguien pueda evaluar.

Qué se discute

Las disputas sobre firmas electrónicas suelen girar en torno a cuatro preguntas.

1. **¿Fue esta persona?** Es la pregunta de la identidad y la autoría. Se responde con la evidencia de identificación y de autorización: cómo se verificó quién era, qué factor activó la firma, si ese factor estaba bajo su control.
2. **¿Este es el documento?** Es la pregunta de la integridad. Se responde con la validación criptográfica, que muestra si el contenido cambió después de la firma.
3. **¿Cuándo?** Es la pregunta del momento. Se responde con los sellos de tiempo y, en su defecto, con el registro de eventos.
4. **¿Sabía lo que firmaba?** Es la pregunta de la voluntad. Se responde con la evidencia del proceso: qué se le mostró, qué aceptó, cuánto tiempo tuvo el documento a la vista, si pudo descargarlo.

El papel de los niveles

Como vimos en el primer tomo, en muchas jurisdicciones la firma cualificada o su equivalente goza de presunciones que trasladan la carga de la prueba a quien la impugna. Eso no la vuelve indiscutible: quien la niega puede demostrar, por ejemplo, que su tarjeta le fue robada o que fue engañado para activar la firma. Pero sí cambia la dinámica del proceso. Con una firma simple, en cambio, quien la invoca debe probar su autenticidad, y en ese esfuerzo el registro de evidencia se vuelve decisivo.

El perito

En una disputa compleja suele intervenir un perito informático. Su tarea es validar las firmas con herramientas independientes, examinar el registro de evidencia, verificar su integridad y explicar al tribunal, en lenguaje comprensible, qué demuestran y qué no. Un perito trabaja mucho mejor cuando la plataforma puede entregarle:

- el documento firmado original, con todas sus revisiones y firmas individuales;
- el registro de evidencia completo, exportado en un formato que pueda verificarse sin acceso a la plataforma;
- la descripción técnica de cómo se protege el registro y cómo se verifica su cadena;
- las anclas externas que permiten comprobar que el registro no fue reescrito;
- las respuestas de los servicios externos de identidad, firma, sello de tiempo y revocación;
- la documentación de la configuración vigente en el momento de los hechos.

Lo que la experiencia enseña

Sin pretender resumir la jurisprudencia de ningún país, algunas lecciones se repiten. Los tribunales tienden a valorar más la evidencia de proceso coherente y completa que las afirmaciones genéricas sobre la seguridad de un sistema. Una firma criptográficamente impecable puede perder fuerza si el proceso de identificación previo fue débil. Y una firma simple respaldada por un registro sólido, con identificación razonable y aceptación explícita, puede ser plenamente eficaz.

También se repite una lección menos técnica: la claridad. Un certificado de finalización comprensible, un validador que explica lo que comprobó, una plataforma que puede describir en pocas páginas cómo funciona su evidencia, todo eso facilita la tarea de quien tiene que decidir.

LO QUE CONVIENE EXIGIR A UNA SOLUCIÓN

Firmas en formatos normalizados que se validen con herramientas independientes. Niveles LT o LTA para documentos de largo plazo. Un registro de evidencia encadenado y anclado fuera del control del operador, exportable y verificable. Identificación y autorización registradas por separado. Un validador que diga qué comprobó y qué no. Y la capacidad de entregar todo eso, años después, a un perito que nunca vio la plataforma.

> Una firma no se demuestra con una marca verde en una pantalla. Se demuestra con un expediente que alguien ajeno al sistema pueda revisar y entender.

REFERENCIA

Glosario

Los términos principales de este tomo, en el sentido en que se usan aquí. Los conceptos básicos están en el glosario del tomo 1.

Actualización incremental

Mecanismo del PDF por el que los cambios se agregan al final del archivo sin reescribir lo anterior, formando revisiones sucesivas.

Ancla externa

Publicación de la huella de un registro en un lugar que su operador no controla, para impedir que la historia anterior se reescriba sin ser detectada.

Árbol de huellas (árbol de Merkle)

Estructura en la que las huellas de muchos datos se combinan de a pares hasta una única raíz, de modo que cualquier dato puede probarse parte del conjunto con un camino corto.

ASiC

Contenedor normalizado que reúne uno o varios documentos con sus firmas CAdES o XAdES en un solo archivo.

Bloqueo de campos (FieldMDP)

Mecanismo del PDF que permite que una firma impida modificar determinados campos del formulario.

CAdES

Formato de firma avanzada basado en la sintaxis CMS, binario y aplicable a cualquier tipo de archivo.

Certificación del documento (DocMDP)

Firma de un PDF que declara qué cambios posteriores se admiten: ninguno, completar formularios y firmar, o además anotar.

Certificado de finalización

Resumen legible del registro de evidencia que acompaña al documento firmado.

Conservación cualificada

Servicio de confianza, previsto en eIDAS, que prolonga la fiabilidad de firmas cualificadas y de «sellos electrónicos» cualificados más allá de su validez tecnológica.

Firma envuelta, envolvente y separada

Las tres formas de relacionar firma y documento: la firma dentro del documento, el documento dentro de la firma, o ambos en archivos distintos.

JAdES

Formato de firma avanzada basado en las firmas para JSON, pensado para mensajes entre sistemas y credenciales.

Lista de listas

Lista publicada por la Comisión Europea que indica dónde se encuentra la lista de confianza de cada Estado miembro y con qué certificado está firmada.

Material de validación

Certificados de la cadena y respuestas de revocación que permiten validar una firma sin consultar servicios externos.

Momento de referencia

Instante en el que se evalúa la validez de una firma, normalmente el que fija su sello de tiempo.

Niveles B, T, LT y LTA

Niveles técnicos de las firmas avanzadas europeas: básica, con tiempo, de larga duración y de larga duración con archivo.

PAdES

Formato de firma avanzada para documentos PDF.

PDF/A

Familia de normas ISO 19005 que define subconjuntos del PDF aptos para archivo a largo plazo.

Política de validación

Conjunto de reglas que define qué anclas, algoritmos, certificados y pruebas exige un validador.

Registro de evidencia (RFC 4998)

Estructura que protege muchos documentos con un solo sello de tiempo sobre la raíz de un árbol de huellas, y que se renueva periódicamente.

Renovación del sello de tiempo de archivo

Aplicación periódica de un nuevo sello de tiempo, con algoritmos más robustos, sobre una firma y todas sus pruebas anteriores.

Resultado indeterminado

Conclusión de una validación en la que la información disponible no permite decidir si la firma es válida o no.

Sello de tiempo del documento

Firma especial de una autoridad de sellado de tiempo que cubre un PDF completo hasta ese punto.

XAdES

Formato de firma avanzada basado en la firma XML, usado en documentos estructurados.

REFERENCIA

Para seguir leyendo

Las normas, artículos y estándares citados en este tomo, agrupados por tema.

Historia y fundamentos

Haber, S. y Stornetta, W. S. Artículo sobre el sellado de tiempo de documentos digitales. *Journal of Cryptology*, vol. 3, n.º 2, 1991.

Merkle, R. Trabajos sobre árboles de huellas y firmas, Universidad de Stanford, 1979.

Formatos y niveles

ETSI. EN 319 122, CAdES. EN 319 132, XAdES. EN 319 142, PAdES. TS 119 182, JAdES. EN 319 162, ASiC.

ISO. ISO 32000, formato de documento portátil (PDF). ISO 19005, PDF/A.

Sellado de tiempo

IETF. RFC 3161, protocolo de sellado de tiempo, 2001.

ETSI. EN 319 421 y EN 319 422, requisitos y perfiles para autoridades de sellado de tiempo.

Validación y confianza

ETSI. EN 319 102, procedimientos de creación y validación de firmas. TS 119 612, listas de confianza. TS 119 441, servicios de validación.

Comisión Europea. Biblioteca de código abierto para servicios de firma digital (DSS) y lista de listas de confianza.

Unión Europea. Reglamento (UE) 910/2014 (eIDAS), artículos 32, 33, 34, 41 y 42, y Reglamento (UE) 2024/1183.

Conservación y evidencia

IETF. RFC 4998, sintaxis de registros de evidencia, 2007. RFC 6283, su versión XML, 2011. RFC 6962, registros públicos de certificados, 2013.

ETSI. TS 119 511 y TS 119 512, servicios de conservación de firmas.

Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

Firmar es un instante. Probar que se firmó puede llevar décadas.

Este segundo tomo explica qué ocurre con una firma después de firmar: los formatos y niveles que la preparan para durar, los sellos de tiempo, la validación, las listas de confianza, la conservación a largo plazo, el registro de evidencia del proceso y lo que sucede cuando una firma se discute ante un tribunal.

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