Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

TOMO 3

Orquestar la firma.

Procesos, identidad, integración y operación a escala: cómo se diseña, se conecta y se gobierna un servicio de firma, y qué cambian en él las carteras digitales, la inteligencia artificial y la criptografía poscuántica.



Primera edición · Montevideo, 2026

Interfase

Rúbrica. Cuadernos sobre firma, identidad y confianza digital
Tomo 3. Orquestar la firma

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. El epílogo describe una plataforma desarrollada por el editor y así se indica en él.

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

RÚBRICA · TOMO 3

Orquestar la firma

Cómo se diseñan, se integran y se operan los servicios que coordinan la firma entre personas, organizaciones y países.

CONTENIDO

Índice

	Prólogo	5
01	Diseñar un proceso de firma	7
02	La identidad de quien firma	13
03	Carteras y credenciales	17
04	Prestadores y mecanismos	21
05	Integrar	25
06	Operar a escala	29
07	Accesibilidad e idiomas	33
08	Inteligencia artificial y firma	37
09	La transición poscuántica	41
	Epílogo. Signing Flows	45
	Glosario	49
	Para seguir leyendo	53

ANTES DE EMPEZAR

De la firma al servicio

Los dos primeros tomos explicaron qué es una firma y cómo se conserva su prueba. Este se ocupa de lo que hace falta para que miles de firmas ocurran cada día, bien, en muchos lugares a la vez.

Una firma aislada es un problema resuelto. Un servicio de firma es otra cosa. Tiene que coordinar personas que no se conocen, en el orden correcto, con el nivel de identificación adecuado para cada una. Tiene que hablar con prestadores de confianza de distintos países, con los sistemas de las organizaciones que lo usan y con los dispositivos de quienes firman. Tiene que aislar los datos de cada cliente, rendir cuentas ante auditores y seguir funcionando cuando algún servicio externo falla. Y tiene que hacer todo eso de una manera que una persona sin formación técnica pueda entender en el momento de firmar.

Este tomo recorre esos desafíos. Empieza por el diseño de los procesos y por la identidad de quien firma, que es donde hoy se concentra buena parte del valor y del riesgo. Sigue con la elección de prestadores y mecanismos para cada acto, con la integración con otros sistemas y con la operación a escala, incluida la de quienes ofrecen el servicio a terceros. Dedica un capítulo a la accesibilidad y los idiomas, que suelen tratarse como detalles y no lo son. Termina con dos fuerzas que están cambiando la disciplina: la inteligencia artificial y la transición a la criptografía poscuántica.

Como los anteriores, este tomo no nombra productos en sus capítulos. La única excepción es el epílogo, donde, por primera y única vez en la serie, describimos la plataforma que desarrolla el editor de estos cuadernos y los problemas de este tomo a los que responde. Está separado del resto y señalado como tal, para que el lector pueda leerlo, o no, con esa información a la vista.

01

CAPÍTULO UNO

Diseñar un proceso de firma.

Antes de elegir tecnología hay que entender el acto: quién interviene, qué aporta cada uno, en qué orden y qué pasa cuando algo no sale como se esperaba.

La tentación al digitalizar un proceso de firma es copiar el proceso en papel. Se imprime mentalmente el documento, se recuerda quién lo firmaba y en qué orden, y se reproduce ese recorrido en una plataforma. El resultado suele funcionar, pero desaprovecha casi todo lo que el medio digital permite y arrastra pasos que sólo existían por las limitaciones del papel.

Un buen diseño empieza por otra pregunta: qué tiene que quedar probado al final. A partir de ahí se deduce quién debe intervenir, qué debe aportar cada uno y qué nivel de garantía necesita cada aporte.

Los roles

En casi todos los procesos aparecen los mismos papeles, aunque con nombres distintos.

ROL	QUÉ HACE	QUÉ DEBE QUEDAR PROBADO
Emisor	Prepara el documento, define participantes y reglas, y lo envía.	Qué versión envió y con qué instrucciones.
Completador	Aporta datos dentro del documento: un importe, una fecha, un número de cuenta.	Qué datos ingresó y cuándo.
Aprobador	Autoriza que el documento siga su curso, sin firmarlo.	Que aprobó esa versión, con su identidad.
Firmante	Expresa su voluntad sobre el contenido.	Identidad, autorización e integridad de lo firmado.
Destinatario de copia	Recibe el resultado para su conocimiento o archivo.	Que recibió el documento final.

Una misma persona puede tener más de un rol: un cliente completa sus datos y después firma. Lo importante es que el sistema distinga los actos, porque cada uno tiene consecuencias distintas.

Los patrones de recorrido

Las rutas en serie y en paralelo, presentadas en el primer tomo, se combinan en patrones que se repiten en todos los sectores.



FIGURA 1 Cinco patrones que se repiten en todos los sectores. Combinan rutas en serie, en paralelo y copias individuales.

- **Aprobación previa.** Un aprobador interno revisa antes de que el documento salga hacia los firmantes externos. Evita que un error llegue al cliente.
- **Completar antes de firmar.** Uno o más participantes aportan datos y el documento, ya completo, pasa a la firma. Es el patrón que más trabajo manual elimina.
- **Grupo con uno basta.** Cualquiera de los miembros de un grupo puede actuar, por ejemplo cualquiera de los apoderados de una empresa. El primero que firma cierra el paso.
- **Copias individuales.** El mismo documento se envía a muchas personas y cada una firma su propia copia, con su propio registro. Es el patrón de las políticas internas o los consentimientos masivos.
- **Contrafirma final.** La organización firma o aplica su sello de organización al final, cuando todas las otras partes ya lo hicieron, para no comprometerse antes.

Las excepciones son parte del diseño

Un proceso que sólo contempla el camino feliz falla en el primer imprevisto. Las preguntas que conviene responder antes de publicar un proceso son siempre las mismas.

- ¿Qué pasa si alguien rechaza? ¿Se anula todo, vuelve al emisor, se permite corregir y reenviar?
- ¿Puede un firmante delegar en otra persona? ¿Con qué control y qué constancia?
- ¿Qué pasa si nadie actúa? ¿Cuántos recordatorios, cada cuánto, y cuándo vence el envío?
- ¿Puede corregirse un dato después de que alguien firmó? Casi siempre la respuesta correcta es no: se anula y se envía de nuevo.
- ¿Qué pasa si un servicio externo, como el prestador de firma, no responde?

Las reglas viven en la persona, no en el documento

Una idea que simplifica mucho el diseño es asociar las reglas a cada participante y no al documento entero. Para cada persona se define cómo firma, con qué nivel de identificación, si puede descargar o imprimir, si su acceso exige un código. Así, en un mismo documento, un empleado interno puede aprobar con su cuenta corporativa, un cliente puede firmar con un código enviado a su teléfono y un apoderado puede firmar con su certificado cualificado. Y la plataforma puede comprobar antes del envío que cada requisito es alcanzable: un documento que exige a alguien un tipo de certificado que no está disponible no debería salir.

Plantillas y gobierno

Cuando un proceso funciona, se convierte en plantilla: el documento con sus campos, sus roles y sus reglas, listo para reutilizarse cambiando sólo los participantes. En organizaciones grandes, las plantillas se vuelven activos que hay que gobernar: quién puede crearlas, quién aprueba sus cambios, qué versión se usó en cada envío. Ese gobierno es, en sí mismo, parte de la evidencia: ante una disputa puede ser necesario demostrar con qué reglas se envió un documento hace cinco años.

PARA RECORDAR

Un buen proceso de firma se diseña desde la prueba que debe quedar, distingue los actos de cada participante, asigna las reglas a cada persona, contempla las excepciones antes de que ocurran y se gobierna como un activo de la organización.

02

CAPÍTULO DOS

¿Quién está del otro lado?

La criptografía garantiza que una clave firmó. La identidad responde a la pregunta que de verdad importa: quién usó esa clave. Es la capa donde hoy se concentran el valor, la innovación y el fraude.

En el primer tomo advertimos que la identidad es el eslabón débil de la firma electrónica. Este capítulo explica cómo se la refuerza. Conviene empezar por un vocabulario que distingue tres momentos que suelen confundirse.

- **Verificar la identidad** es comprobar, una vez, que una persona es quien dice ser, por ejemplo examinando su documento de identidad.
- **Autenticar** es comprobar, cada vez que la persona vuelve, que es la misma que fue verificada, por ejemplo con una contraseña y un segundo factor.
- **Autorizar la firma** es el acto concreto por el que la persona activa su firma sobre un documento, por ejemplo introduciendo un código o un PIN.

Una firma sólida necesita los tres, y la evidencia debe poder mostrar cada uno por separado.

Niveles de garantía

Las normas internacionales clasifican la fuerza de la identificación en niveles. El reglamento eIDAS define tres niveles de seguridad para los medios de identificación electrónica: bajo, sustancial y alto. Las guías de identidad digital del Instituto Nacional de Estándares y Tecnología de los Estados Unidos distinguen, por separado, la solidez de la verificación inicial y la del autenticador, cada una en tres niveles. Los nombres varían, pero la lógica es la misma: cuanto más grave el acto, más fuerte debe ser la prueba de que quien actúa es quien dice.

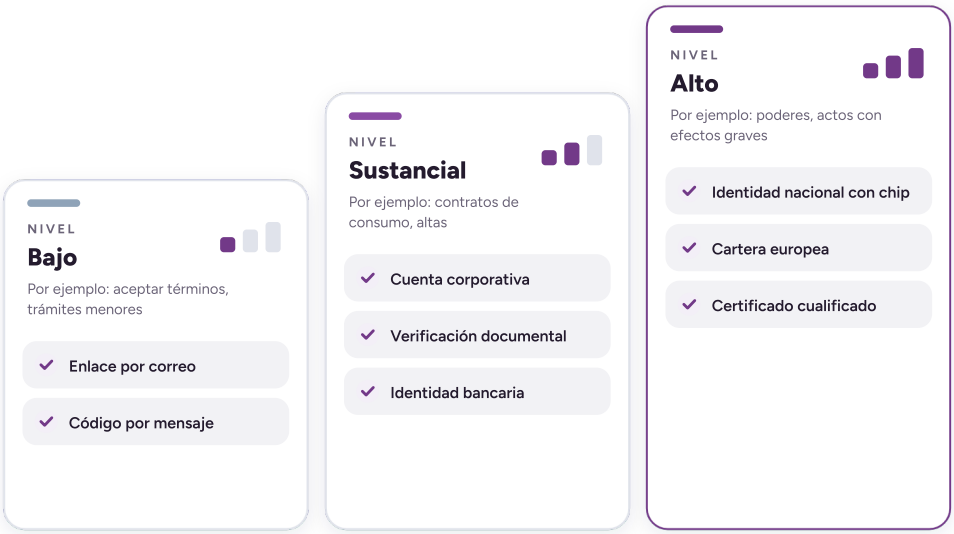


FIGURA 2 Niveles de garantía de la identificación y métodos que suelen alcanzarlos. La elección depende del acto, y conviene ofrecer más de un método por nivel.

Los métodos, del más liviano al más fuerte

Un enlace y un código

El método más difundido consiste en enviar a la persona un enlace por correo electrónico y, opcionalmente, un código por mensaje de texto o por una aplicación de mensajería. Prueba que la persona controla esa casilla o ese teléfono, no quién es. Para muchos actos es suficiente, sobre todo cuando la relación con la persona ya existe y sus datos de contacto fueron verificados antes.

Las identidades corporativas y sociales

Dentro de una organización, la identidad más natural es la cuenta corporativa, administrada por el proveedor de identidad de la empresa mediante protocolos estándar como SAML u OpenID Connect. Para relaciones con consumidores, algunos procesos aceptan identidades de proveedores de gran escala. Su fuerza depende de cómo se verificó la cuenta originalmente.

Las identidades digitales nacionales

Muchos países ofrecen a sus ciudadanos una identidad digital oficial, basada en el documento de identidad con chip, en aplicaciones gubernamentales o en credenciales bancarias reconocidas por el Estado. Suelen ser un medio fuerte y económico para identificar a una persona en su país, y su integración es cada vez más sencilla gracias a los protocolos estándar.

La verificación documental con prueba de vida

Cuando no hay identidad digital disponible, se puede verificar a distancia: la persona fotografía su documento de identidad, el sistema comprueba sus elementos de seguridad y lee el chip si lo tiene, y luego compara la foto del documento con la cara de la persona frente a la cámara, con pruebas de que es una persona viva y no una imagen. Es el método que permitió la banca digital a gran escala. Su desafío es la carrera con las técnicas de suplantación, que hoy incluyen imágenes y videos sintéticos de calidad creciente.

Los certificados

Finalmente, el propio certificado de firma, en tarjeta, en token o en la nube, identifica a su titular, porque su emisión exigió una verificación previa, a menudo presencial. Cuando la firma se hace con un certificado cualificado, la identificación viene incluida en la firma.

Elegir sin excluir

El error más frecuente es exigir a todos el método más fuerte. Un proceso que pide una identidad digital nacional a un cliente extranjero, o una tarjeta con lector a un usuario que firma desde el teléfono, no se completa. La práctica recomendable es definir, para cada acto, el nivel mínimo aceptable, ofrecer varios métodos que lo alcancen y dejar que cada persona use el que tiene.

El consentimiento también se prueba

Antes de firmar electrónicamente, muchas legislaciones exigen que la persona acepte hacerlo por ese medio, y las leyes de protección de datos exigen informar qué datos se recogen y para qué. Ese consentimiento es un acto en sí mismo y debe quedar

registrado con el texto exacto que la persona aceptó, en su idioma, y con la versión vigente de ese texto. Un recibo del consentimiento, entregado a la persona, refuerza la transparencia y la prueba.

UNA ADVERTENCIA

La identidad es también el terreno del fraude. Los ataques más comunes no rompen la criptografía: se apoderan de un correo, duplican una tarjeta SIM, engañan a la persona para que entregue un código o presentan una cara sintética. Ningún método es invulnerable. Por eso conviene combinar métodos según el riesgo, vigilar señales de fraude y registrar todo lo necesario para investigar después.

03

CAPÍTULO TRES

La identidad en el bolsillo.

Durante décadas, identificarse en línea fue pedirle a alguien que confirmara quiénes somos. Las carteras de identidad digital proponen otra cosa: que cada persona lleve sus credenciales consigo y decida qué mostrar.

Todos los métodos del capítulo anterior tienen algo en común: la persona depende de un intermediario que, en cada operación, confirma su identidad ante quien la pide. El proveedor de identidad corporativo, el banco, el sistema nacional de identificación o el servicio de verificación documental intervienen cada vez. Funciona, pero tiene costos: cada intermediario ve a qué servicios accede la persona, cada integración es distinta y la persona tiene poco control sobre qué datos se comparten.

Las carteras de identidad digital invierten ese esquema. Una autoridad confiable emite una credencial firmada, la persona la guarda en una aplicación de su teléfono y la presenta cuando la necesita. Quien la recibe verifica la firma del emisor sin tener que preguntarle nada en ese momento.

Tres papeles

El modelo se describe con tres papeles, que la literatura técnica suele llamar el triángulo de la confianza.



FIGURA 3 El triángulo de la confianza. El emisor no interviene en cada uso; el verificador confía en él a través de listas de confianza.

- **El emisor** es quien da fe de un atributo: el Estado que emite un documento de identidad, la universidad que otorga un título, el banco que confirma una cuenta. Firma la credencial con su clave.
- **El titular** es la persona que recibe la credencial y la guarda en su cartera. Decide cuándo presentarla y qué atributos revelar.
- **El verificador**, también llamado parte que confía, es quien recibe la presentación: un comercio, una administración pública, una plataforma de firma. Comprueba la firma del emisor y que la credencial no fue revocada.

La relación entre emisor y verificador ya no es directa. El emisor no se entera de cada uso de la credencial, y eso es una ganancia de privacidad. A cambio, el verificador necesita saber en qué emisores confiar, y ahí reaparecen las listas de confianza descritas en el segundo tomo.

Revelar sólo lo necesario

Una de las promesas más valiosas de las credenciales digitales es la divulgación selectiva. Quien necesita saber que una persona es mayor de edad no necesita su fecha de nacimiento, ni su dirección, ni su número de documento. Los formatos modernos permiten que la cartera presente sólo los atributos solicitados, o incluso una

afirmación derivada, como "mayor de dieciocho años", con la misma garantía criptográfica que la credencial completa. Para la firma electrónica esto significa que el registro de evidencia puede guardar exactamente lo que el acto exige, ni más ni menos, en línea con el principio de minimización.

La cartera europea

La reforma del reglamento eIDAS aprobada en 2024 convirtió esta idea en política pública. Cada Estado miembro debe poner a disposición de sus ciudadanos y residentes al menos una cartera europea de identidad digital, con plazos que el reglamento y sus actos de ejecución escalonan a partir de 2026. La cartera debe permitir identificarse, guardar y presentar credenciales de atributos emitidas por terceros, y crear firmas electrónicas cualificadas, gratuitas para usos no profesionales.

Hay tres consecuencias que importan a cualquier servicio de firma. La primera: la firma cualificada deja de ser un producto que hay que comprar y configurar, y pasa a estar en el bolsillo de cientos de millones de personas. La segunda: la identificación fuerte y la firma pueden ocurrir en un mismo gesto, desde la misma aplicación. La tercera: los verificadores deben registrarse y declarar qué datos piden y para qué, de modo que la cartera pueda advertir a la persona cuando se le solicita más de lo debido.

MÁS ALLÁ DE EUROPA

Las carteras no son un fenómeno exclusivamente europeo. Varios países de América Latina y de Asia tienen aplicaciones oficiales de identidad, los permisos de conducir móviles siguen una norma ISO publicada en 2021 y el consorcio que gobierna los estándares de la web aprobó en 2025 la segunda versión de su modelo de credenciales verificables. Los nombres y los formatos varían, pero la arquitectura del triángulo se repite.

Firmar con una cartera

Para un proceso de firma, la cartera puede intervenir de dos maneras. En la primera, sólo identifica: la persona presenta su credencial de identidad, la plataforma la verifica y registra el resultado, y la firma se hace por otro medio. En la segunda, la cartera también firma: la plataforma envía a la cartera la huella del documento, la persona la

autoriza con su biometría o su PIN, y la cartera devuelve una firma cualificada creada con una clave que la persona controla, sea en el propio teléfono o en un servicio remoto asociado.

En ambos casos la plataforma de firma cambia de papel. Ya no es la que identifica ni la que custodia claves: es la que orquesta. Pide lo necesario, verifica lo recibido, lo integra en el documento y lo deja registrado. Ese cambio de papel es una de las razones por las que la capa de orquestación gana importancia, y volveremos sobre ella al final del tomo.

Lo que todavía falta

Una tecnología que llega a escala masiva trae preguntas nuevas. ¿Qué pasa si la persona pierde el teléfono? ¿Cómo se recupera una cartera sin abrir una puerta al fraude? ¿Cómo se verifica una credencial emitida por un país cuyo sistema de confianza no se reconoce en el país del verificador? ¿Qué ocurre con quienes no tienen un teléfono compatible? Las normas dan respuestas parciales a cada una, y la experiencia de los primeros años completará el resto. Un servicio de firma prudente se prepara para aceptar carteras sin dejar de ofrecer alternativas.

PARA RECORDAR

Las carteras de identidad trasladan la confianza del intermediario a la credencial firmada. Permiten revelar sólo lo necesario, acercan la firma cualificada a millones de personas y convierten a la plataforma de firma en un orquestador que pide, verifica y registra.

04

CAPÍTULO CUATRO

Cada acto, su firma.

No existe una firma correcta para todo. Existe, para cada acto, en cada país, un mecanismo suficiente y un prestador capaz de ofrecerlo. Elegirlos bien, y decir con honestidad cuál se usó, es el oficio central de un servicio de firma.

En el primer tomo vimos que la ley reconoce varios tipos de firma y que su peso probatorio crece con la exigencia técnica. En el segundo, que la firma necesita de terceros para perdurar: autoridades de certificación, de sellado de tiempo, de validación. Un servicio de firma vive en la intersección de ambas cosas. Para cada documento debe decidir qué tipo de firma corresponde y quién la provee.

Una decisión en cuatro pasos

La decisión puede ordenarse en una secuencia de preguntas, que van de lo jurídico a lo operativo.



FIGURA 4 La elección del mecanismo de firma, de lo jurídico a lo operativo. Puede ser distinta para cada participante del mismo documento.

1. **¿Qué régimen se aplica?** El país donde surte efecto el acto, el de las partes y la naturaleza del documento determinan qué ley rige. Un contrato de consumo en un país europeo, una escritura en un país latinoamericano y un acuerdo comercial entre empresas de dos continentes no se rigen por las mismas reglas.
2. **¿Qué nivel exige el acto?** Algunos actos aceptan cualquier firma electrónica; otros requieren una firma avanzada; unos pocos, una firma cualificada o su equivalente local, o directamente la presencia de un fedatario. El nivel puede ser distinto para cada participante del mismo documento.
3. **¿Qué mecanismo lo alcanza?** Un mismo nivel puede lograrse por caminos diferentes: con un certificado en tarjeta, con un certificado remoto, con una cartera de identidad, o con el consentimiento de la persona y un sello de organización.
4. **¿Qué prestador lo ofrece?** Finalmente, hay que elegir un prestador de confianza reconocido en la jurisdicción correspondiente, que ofrezca ese mecanismo y esté disponible.

El catálogo de prestadores

Un servicio que opera en varios países necesita un catálogo de prestadores: qué autoridades de certificación, de sellado de tiempo y de firma remota puede usar, en qué jurisdicciones son reconocidas, qué mecanismos ofrecen, con qué niveles de

identificación y a qué costo. Ese catálogo cambia con el tiempo, porque los prestadores entran y salen de las listas de confianza, cambian sus condiciones o dejan de operar. Mantenerlo al día es parte del trabajo.

La firma remota facilitó mucho esta tarea. Gracias a interfaces normalizadas, en particular la especificación del Cloud Signature Consortium y los estándares europeos de firma en servidor, una plataforma puede integrarse una vez con un protocolo y trabajar con varios prestadores que lo implementan. El documento no viaja: la plataforma envía la huella, el prestador identifica a la persona, recibe su autorización y devuelve la firma.

Firma propia o firma por consentimiento

Entre los mecanismos disponibles hay una distinción que conviene entender bien, porque es fuente frecuente de confusión.

- **Firma con certificado propio.** La persona firma con un certificado emitido a su nombre, sea en una tarjeta, en un token, en la nube o en su cartera. La firma la identifica directamente, y su fuerza depende del tipo de certificado.
- **Firma por consentimiento.** La persona manifiesta su voluntad en la plataforma, tras identificarse con el método exigido, y la plataforma aplica al documento un sello de organización con un certificado de esa organización, dejando constancia de quién consintió y cómo se identificó. La prueba descansa en el registro de evidencia y en el sello de organización, no en un certificado personal.

Ambos son legítimos y tienen su lugar. La firma por consentimiento es muy común y basta para muchos actos. La firma con certificado propio es necesaria cuando la ley o el contrato la exigen. Lo que no es legítimo es presentar una como si fuera la otra.

La degradación declarada

Los servicios externos fallan. Una autoridad de sellado no responde, un servidor de revocación está caído, un prestador de firma remota tiene una interrupción. El servicio de firma debe decidir qué hacer en esos casos, y la decisión no es sólo técnica.

Hay dos respuestas aceptables. La primera es esperar y reintentar hasta que el servicio vuelva, sin publicar un resultado incompleto. La segunda es continuar con un nivel menor, si el acto lo admite, y declararlo: el documento indica qué nivel alcanzó y por

qué no alcanzó el previsto. La respuesta inaceptable es continuar en silencio, entregando una firma de nivel inferior sin que nadie se entere. A esta práctica de bajar de nivel sólo cuando las reglas lo permiten, y dejando constancia, la llamamos degradación declarada.

UN EJEMPLO

Un documento debía alcanzar el nivel de archivo, con sello de tiempo y material de validación. Al cerrar, el servidor de revocación del prestador no respondió. Las reglas del proceso admitían completar con un nivel con tiempo y sin material de revocación. El documento se cerró, el certificado de finalización indicó el nivel obtenido y el motivo, y la plataforma programó un nuevo intento para completar el material cuando el servicio volviera.

Comprobar antes de enviar

Conviene evitar estos problemas detectándolos antes. Cuando las reglas viven en cada participante, como vimos en el primer capítulo, la plataforma puede comprobar antes del envío que cada una es alcanzable: que hay un prestador disponible para el mecanismo exigido, que el país del firmante está cubierto, que el nivel de identificación pedido puede lograrse. Un documento que no puede completarse no debería salir, y el emisor debería saber exactamente qué falta y para quién.

PARA RECORDAR

La elección del mecanismo de firma va del régimen al nivel, del nivel al mecanismo y del mecanismo al prestador. Un servicio maduro mantiene un catálogo de prestadores por país, distingue la firma propia de la firma por consentimiento, comprueba antes de enviar y, si algo falla, sólo baja de nivel cuando las reglas lo permiten y lo declara.

05

CAPÍTULO CINCO

La firma que no se ve.

Las firmas más eficientes son las que ocurren dentro de otros sistemas: el banco que abre una cuenta, el sistema de recursos humanos que incorpora a un empleado, el portal que contrata un seguro. Para eso, el servicio de firma tiene que saber conversar.

Una plataforma de firma usada sólo a través de su propia pantalla es útil, pero limitada. Alguien tiene que exportar el documento de otro sistema, subirlo, configurar los participantes, esperar, descargar el resultado y volver a cargarlo donde corresponde. Cada paso manual es una oportunidad de error y un costo. La integración elimina esos pasos: el sistema de origen pide la firma, la plataforma la gestiona y el resultado vuelve solo.

Las piezas de una integración

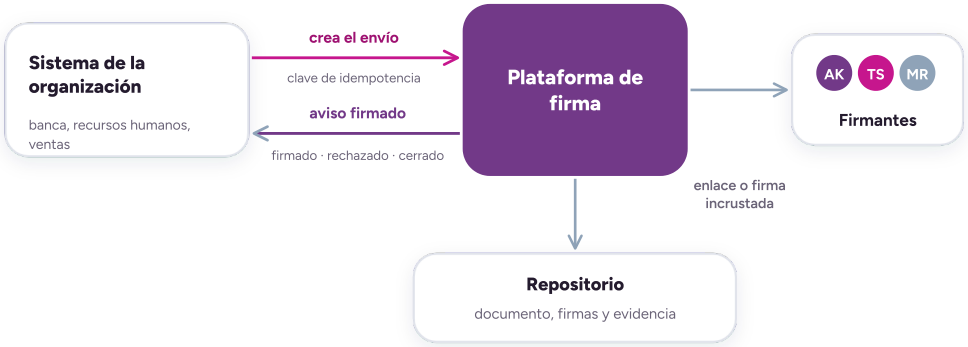


FIGURA 5 Las piezas de una integración. El sistema de origen pide la firma, recibe avisos firmados y obtiene el resultado completo para su archivo.

La interfaz de programación

La base es una interfaz de programación, casi siempre con el estilo REST sobre HTTPS, que permite crear envíos, consultar su estado, descargar documentos y evidencias, y administrar plantillas y usuarios. Una buena interfaz está documentada con una especificación legible por máquinas, como OpenAPI, que permite generar clientes en distintos lenguajes y probar las llamadas antes de escribir código.

Las notificaciones de eventos

Consultar una y otra vez si un documento ya se firmó es ineficiente. La alternativa es que la plataforma avise: cuando ocurre un evento relevante, como una firma, un rechazo o el cierre del proceso, envía un mensaje a una dirección que el sistema de origen indicó. Estos avisos, conocidos en la jerga como webhooks, deben estar firmados por la plataforma para que el receptor pueda comprobar que son auténticos, y deben reintentarse si el receptor no responde.

La firma incrustada

A veces el firmante no debe salir del sistema de origen. En lugar de recibir un correo con un enlace, firma dentro del portal del banco o de la aplicación del comercio, en una ventana que la plataforma de firma provee. La experiencia es continua y la evidencia sigue siendo la de la plataforma de firma, que sabe quién actuó y cómo se identificó.

Tres propiedades que separan una integración seria

- **Idempotencia.** En redes reales los mensajes se pierden y se repiten. Si un sistema envía dos veces la misma orden de crear un envío porque no recibió la primera respuesta, la plataforma debe reconocerla y no crear dos. La técnica habitual es que cada orden lleve una clave única elegida por quien la envía.
- **Orden y reintento.** Los avisos de eventos pueden llegar desordenados o repetidos. El receptor debe poder reconocerlos por su identificador y reconstruir el estado correcto, y la plataforma debe reintentar con pausas crecientes hasta que el receptor confirme.
- **Versiones.** Una interfaz que cambia sin aviso rompe a quienes dependen de ella. Las interfaces maduras declaran su versión, mantienen la anterior durante un período anunciado y documentan cada cambio.

Credenciales y permisos

Cada sistema que se conecta necesita una credencial, y esa credencial debe tener sólo los permisos necesarios: una aplicación que sólo envía documentos no debería poder borrar usuarios. Las credenciales deben poder rotarse sin interrumpir el servicio y revocarse de inmediato si se sospecha una filtración. Y toda acción hecha con ellas debe quedar registrada con el nombre del sistema que actuó, del mismo modo que se registra a las personas.

Integrar sin programar

No toda organización tiene programadores disponibles. Las plataformas de automatización sin código, que conectan aplicaciones mediante bloques visuales, permiten que una persona de negocio arme flujos como "cuando se aprueba una propuesta en el sistema comercial, enviarla a firmar y, al cerrarse, guardarla en el repositorio de contratos". Para que eso funcione, el servicio de firma debe ofrecer conectores para esas plataformas, con las mismas garantías que su interfaz.

El destino del documento firmado

El proceso no termina con la firma. El documento y su evidencia tienen que llegar al lugar donde la organización los conserva: un gestor documental, un repositorio de contratos, un sistema de archivo. La integración con esos repositorios, y la entrega de un paquete completo que incluya el documento, las firmas, el certificado de finalización y el registro de evidencia en un formato verificable, es lo que permite que la conservación a largo plazo descrita en el segundo tomo sea posible.

PARA RECORDAR

Integrar es lograr que la firma ocurra dentro de los procesos de la organización. Requiere una interfaz documentada, avisos firmados y reintentados, idempotencia, versiones estables, credenciales con permisos mínimos, conectores para quienes no programan y una entrega completa del resultado al lugar donde se conserva.

06

CAPÍTULO SEIS

Muchos clientes, una plataforma.

Un servicio de firma rara vez atiende a una sola organización. Atiende a muchas, a veces a través de distribuidores que a su vez tienen sus propios clientes. Operar así exige aislar, personalizar, medir y rendir cuentas.

Cuando una plataforma sirve a muchas organizaciones desde una misma instalación, cada una de ellas debe sentir que la plataforma es suya: con sus usuarios, sus plantillas, su marca y sus datos, invisibles para las demás. Este modelo, que en la industria del software se llama multiinquilino, es económico y permite mejorar el servicio para todos a la vez. Pero desplaza el riesgo: un error de aislamiento ya no afecta a un cliente, sino a todos.

La organización como árbol

La forma más general de representar a los clientes es un árbol. En la raíz está quien opera la plataforma. Debajo pueden estar distribuidores o socios, que a su vez tienen clientes, que a su vez pueden tener filiales o departamentos. Cada nivel ve y administra lo suyo y lo que cuelga de él, y nada más.

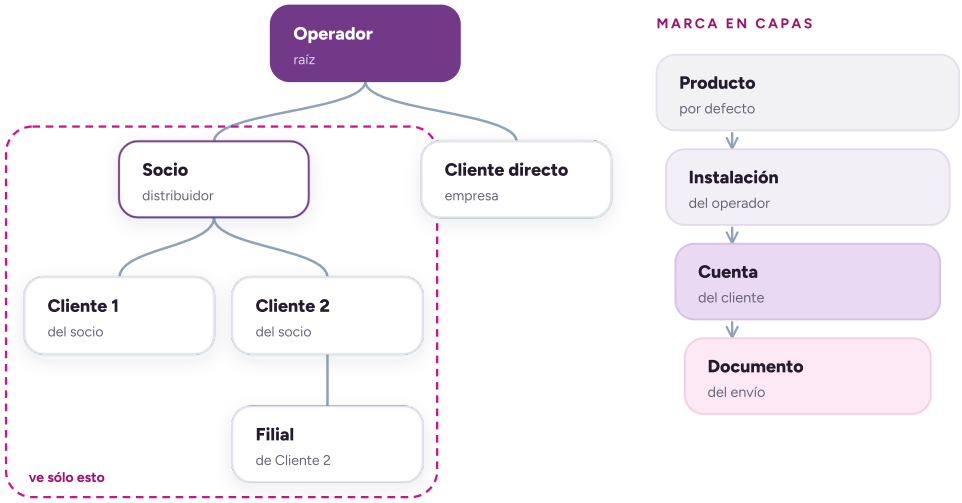


FIGURA 6 La organización como árbol. Cada nivel ve lo suyo y lo que cuelga de él; la marca se hereda de arriba hacia abajo y cada capa puede redefinirla.

El árbol resuelve con un mismo modelo situaciones muy diferentes: una empresa con una sola cuenta, un grupo con subsidiarias en varios países, un prestador de confianza que ofrece firma a sus clientes con su propia marca, un integrador que revende el servicio dentro de su software.

El aislamiento, en capas

Que una organización no vea los datos de otra no puede depender de que cada programador recuerde filtrar cada consulta. Las plataformas serias aplican el aislamiento en varias capas a la vez: en la aplicación, en la propia base de datos mediante reglas de seguridad por fila que la base hace cumplir aunque la aplicación se equivoque, y en el cifrado, a veces con claves distintas por cliente. Cuando el aislamiento lo garantiza la base de datos, un error en el código produce una consulta vacía, no una filtración.

La marca, también en capas

El firmante debe ver la marca de quien le envía el documento, no la de la plataforma. Eso exige una personalización en capas: la del producto, la de la instalación, la de cada cuenta y, a veces, la de cada documento, de modo que cada nivel hereda lo que no define. Los correos, las páginas de firma, el certificado de finalización y los avisos deben respetar esa jerarquía, y los dominios de envío de correo deben estar configurados para que los mensajes lleguen y no parezcan fraudulentos.

Medir el uso

Cada documento enviado, cada firma, cada sello de tiempo, cada verificación de identidad tiene un costo, a menudo pagado a terceros. La plataforma debe medir cada uso, asignarlo a la cuenta correcta del árbol y hacerlo visible para cada nivel. Esa medición sirve para facturar, pero también para detectar anomalías: un aumento brusco de envíos desde una cuenta puede ser un éxito comercial o una credencial robada.

Operar y vigilar

Quien opera la plataforma necesita una consola propia, separada de la de los clientes, para ver el estado de los servicios externos, los envíos detenidos, los errores y el consumo. Las acciones de los operadores también se registran, con la misma rigurosidad que las de los usuarios. Y los eventos de seguridad deben poder enviarse a los sistemas de monitoreo de cada cliente, para que sus equipos los vean junto con el resto de su actividad.

Dónde viven los datos

Muchas leyes de protección de datos, y muchas políticas de clientes públicos y financieros, exigen saber en qué país se almacenan los documentos y quién puede acceder a ellos. Algunas lo restringen. Un servicio que atiende a varios países necesita poder ubicar los datos de cada cliente en la región que corresponde, y en ciertos casos ofrecer la instalación en la infraestructura del propio cliente. La nube compartida, la nube dedicada y la instalación propia son tres respuestas a la misma pregunta, con distintos equilibrios de costo, control y responsabilidad.

Rendir cuentas

Los clientes de un servicio de firma no pueden auditarlo por sí mismos. Confían en certificaciones independientes. Las más comunes son la norma internacional ISO/IEC 27001 de gestión de la seguridad de la información, los informes de control conocidos como SOC 2 en el mercado estadounidense y, para los prestadores de servicios de confianza en Europa, la norma ETSI EN 319 401 y sus derivadas, que son la base de la supervisión bajo eIDAS. Cada certificación tiene un alcance: es importante leer qué cubre y qué no.

UNA DISTINCIÓN ÚTIL

Una plataforma de firma puede usar los servicios de un prestador de confianza cualificado sin ser ella misma un prestador cualificado. En ese caso, la confianza en los certificados, su emisión y su revocación es responsabilidad del prestador, y la plataforma responde por la orquestación, la evidencia y la custodia de los documentos. Confundir ambos papeles en la comunicación comercial es un error frecuente y engañoso.

PARA RECORDAR

Operar a escala es servir a muchos como si cada uno fuera el único: un árbol de organizaciones, aislamiento garantizado por la base de datos, marca en capas, medición de cada uso, una consola de operación vigilada, control sobre dónde viven los datos y certificaciones independientes cuyo alcance se conoce.

07

CAPÍTULO SIETE

Firmar es un acto para todos.

Una firma sólo expresa voluntad si quien firma pudo leer y entender lo que firmaba. La accesibilidad y el idioma no son detalles de diseño: son condiciones de validez del consentimiento.

Imaginemos a una persona ciega que recibe un contrato para firmar. Si la página de firma no funciona con su lector de pantalla, tiene dos opciones: pedir ayuda a otra persona, que verá el contenido y quizá actúe por ella, o renunciar. En ambos casos, la promesa de la firma electrónica, que cada persona exprese su voluntad por sí misma, se rompe. Lo mismo ocurre con quien no lee bien el idioma del documento o de las instrucciones, con quien tiene dificultades motrices para completar un campo pequeño, o con quien necesita más tiempo del que un código de un solo uso le concede.

El estándar de referencia

Las Pautas de Accesibilidad para el Contenido Web, conocidas por su sigla en inglés WCAG y publicadas por el consorcio que gobierna los estándares de la web, son la referencia mundial. Su versión 2.2, de 2023, organiza los requisitos en cuatro principios: el contenido debe ser perceptible, operable, comprensible y robusto. Cada requisito tiene un nivel, y el nivel intermedio, llamado AA, es el que suelen exigir las leyes.

En Europa, la Ley Europea de Accesibilidad se aplica desde junio de 2025 a una lista de productos y servicios que incluye la banca electrónica y el comercio electrónico, dos de los ámbitos donde más se firma. Muchos otros países tienen normas equivalentes para el sector público, y la tendencia es extenderlas.

Lo que significa en una firma

- Todo el recorrido, desde abrir el enlace hasta confirmar la firma, puede hacerse sólo con el teclado y con un lector de pantalla.
- Los campos del documento tienen nombres que se anuncian, y los errores se explican en texto, no sólo con un color.
- Los contrastes de color permiten leer a personas con baja visión, y la página se adapta cuando se amplía el texto.
- Los códigos y las sesiones dan tiempo suficiente, o permiten extenderlo, y no exigen resolver acertijos visuales.
- La autenticación no depende de recordar o transcribir información, una exigencia que la versión 2.2 de las pautas hizo explícita.
- El propio documento PDF, cuando se crea, es accesible: tiene estructura, orden de lectura y texto alternativo para las imágenes.

El idioma del consentimiento

El idioma es una forma de accesibilidad. Un servicio que opera en varios países debe ofrecer su interfaz, sus correos, sus avisos legales y su certificado de finalización en el idioma de cada participante, y el registro de evidencia debe guardar en qué idioma vio cada uno los textos que aceptó. Un mismo documento puede tener participantes que hablan lenguas distintas: el contrato es uno, pero la experiencia de cada uno debe ser la suya.

Traducir no es sólo cambiar palabras. Las fechas, los números, las monedas y los formatos de nombre cambian entre países. Los textos legales deben revisarse por profesionales de cada jurisdicción. Y la calidad de las traducciones automáticas, aunque útil, no basta para los textos que la persona acepta como parte del consentimiento.

Lenguaje claro

Un texto puede estar en el idioma correcto y ser incomprensible. Los movimientos de lenguaje claro, que varios gobiernos y una norma ISO de 2023 promueven, proponen escribir para que el lector encuentre, entienda y use la información a la primera. En un

proceso de firma, eso se traduce en instrucciones cortas, botones que dicen lo que hacen y avisos que explican la consecuencia de cada acto. Firmar no debería requerir saber qué es una firma avanzada.

PARA RECORDAR

Un consentimiento sólo vale si la persona pudo percibir, entender y actuar por sí misma. Las pautas WCAG en su nivel AA, el idioma de cada participante registrado en la evidencia y el lenguaje claro son parte de la validez de la firma, no un agregado.

08

CAPÍTULO OCHO

Cuando firma una máquina.

La inteligencia artificial ya prepara documentos, revisa cláusulas y completa formularios. Pronto actuará en nombre de personas y empresas. La pregunta no es si intervendrá en la firma, sino cómo se prueba lo que hizo y quién responde por ello.

La firma nació para atribuir un acto a una persona. Durante siglos, la pregunta fue si la persona era quien decía ser. Los sistemas de inteligencia artificial agregan una pregunta nueva: si fue la persona quien actuó o un sistema en su nombre, y con qué autorización. Este capítulo recorre los usos que ya existen, los que se están construyendo y los principios que permiten incorporarlos sin perder la prueba.

Ayudar a quien envía

El uso más inmediato está del lado del emisor. Un asistente puede leer un documento y proponer dónde van los campos de firma y de datos, quiénes deberían firmar y en qué orden, qué nivel de firma exige el tipo de acto en el país correspondiente. Puede detectar que falta una página, que dos importes no coinciden o que una cláusula contradice una plantilla aprobada. En todos estos casos la máquina propone y una persona decide, y conviene que el registro distinga qué fue sugerido y qué fue aceptado.

Ayudar a quien firma

Del otro lado, un asistente puede explicar al firmante, en su idioma y con lenguaje claro, qué está firmando: cuáles son sus obligaciones, plazos y costos. Es una promesa poderosa para la comprensión y la accesibilidad, y también un riesgo: si la explicación

es incorrecta, la persona puede consentir algo distinto de lo que creyó. Por eso la explicación debe presentarse como lo que es, una ayuda, y el registro debe guardar qué se le mostró, de la misma manera que guarda los textos legales que aceptó.

Los agentes

Un paso más allá están los agentes: sistemas que no sólo responden preguntas, sino que ejecutan acciones en otros sistemas. Protocolos abiertos publicados desde fines de 2024 permiten que un agente use las funciones de una plataforma de la misma manera en que lo haría una integración tradicional: crear un envío, consultar su estado, descargar la evidencia. En ese escenario, la persona dice "enviá este acuerdo a firmar a los tres socios" y el agente lo hace.



FIGURA 7 Un agente que actúa por una persona. La delegación fija el alcance, la plataforma lo comprueba en cada acto y el registro distingue a la máquina de la persona.

Que un agente prepare y envíe documentos plantea pocos problemas nuevos si se lo trata como cualquier otro sistema integrado: con una credencial propia, permisos mínimos y registro de cada acción. Que un agente firme en nombre de una persona es otra cosa. Exige resolver tres preguntas.

1. **¿Quién lo autorizó?** Debe existir una delegación explícita, de una persona identificada, con un alcance definido: qué tipo de documentos, hasta qué importe, durante cuánto tiempo.
2. **¿Actuó dentro de lo autorizado?** La plataforma debe comprobar el alcance en cada acto y rechazar lo que lo excede, no sólo confiar en el agente.

3. **¿Cómo se distingue en la prueba?** La firma y el registro deben dejar claro que actuó un agente, cuál, bajo qué delegación y con qué instrucción. Una firma hecha por una máquina que aparenta haber sido hecha por una persona es una falsificación, aunque la persona la haya autorizado.

El marco regulatorio

El reglamento europeo de inteligencia artificial, aprobado en 2024, establece obligaciones escalonadas según el riesgo de cada uso, incluidas obligaciones de transparencia cuando una persona interactúa con un sistema de inteligencia artificial. Otros países avanzan con leyes y guías propias. Al mismo tiempo, la figura del sello de organización (el «sello electrónico» de eIDAS), que en el primer tomo vimos como la firma de una organización, ofrece una herramienta existente para atribuir actos automatizados a la entidad responsable de ellos. Es probable que la práctica combine ambas cosas: sellos de organización para los actos de sus sistemas y delegaciones explícitas, registradas y limitadas, para los actos de agentes que representan a personas.

Principios para incorporar la inteligencia artificial

- **La máquina propone, la persona decide,** salvo delegación explícita, limitada y registrada.
- **Todo acto de una máquina queda registrado** como acto de una máquina, con su identidad, su versión y la instrucción que recibió.
- **Lo que se muestra se conserva:** resúmenes, explicaciones y sugerencias forman parte de la evidencia.
- **Los datos de los documentos se protegen** también frente a los modelos: qué se envía, a qué proveedor, en qué región, y si se usa para entrenar.
- **La responsabilidad tiene un nombre:** detrás de cada agente hay una persona o una organización que responde.

PARA RECORDAR

La inteligencia artificial puede preparar, explicar y ejecutar, y eso mejora los procesos de firma. Pero la firma sigue siendo atribución de voluntad. Cada acto de una máquina debe quedar registrado como tal, cada delegación debe ser explícita y limitada, y siempre debe haber alguien que responda.

09

CAPÍTULO NUEVE

Antes de que llegue la máquina.

Las computadoras cuánticas capaces de romper la criptografía actual todavía no existen. Pero las firmas que hacemos hoy deben poder verificarse dentro de treinta años. Por eso la transición ya empezó.

En el primer tomo vimos que la firma digital descansa sobre problemas matemáticos que las computadoras actuales no pueden resolver en un tiempo razonable: factorizar números enormes, en el caso de RSA, o calcular logaritmos discretos sobre curvas elípticas. En 1994, el matemático Peter Shor describió un algoritmo que, ejecutado en una computadora cuántica suficientemente grande, resolvería ambos problemas con eficiencia. Nadie ha construido todavía esa máquina, y los expertos discrepan sobre cuándo podría existir. Pero su posibilidad basta para cambiar la planificación.

Por qué importa a la firma

Para el cifrado, la amenaza es inmediata: un adversario puede guardar hoy comunicaciones cifradas y descifrarlas mañana. Para la firma, la amenaza es diferente. Una computadora cuántica permitiría falsificar firmas nuevas con claves actuales, pero no alteraría las firmas ya hechas. El riesgo, entonces, es que en el futuro no se pueda distinguir una firma auténtica de 2026 de una falsificación hecha en 2040 con la misma clave.

La respuesta ya la conocemos del segundo tomo: los sellos de tiempo de archivo. Si antes de que los algoritmos actuales se vuelvan inseguros se aplica sobre la firma un sello de tiempo con un algoritmo resistente, ese sello de tiempo prueba que la firma

existía cuando todavía no podía falsificarse. La renovación de sellos de tiempo, pensada para la obsolescencia gradual de los algoritmos, es también la defensa contra un salto brusco.

Los nuevos estándares

En 2016, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos abrió un concurso internacional para seleccionar algoritmos resistentes a las computadoras cuánticas. Tras varias rondas de análisis público, en agosto de 2024 publicó los primeros estándares definitivos. Dos de ellos son de firma: FIPS 204, basado en problemas sobre retículos, y FIPS 205, basado únicamente en funciones de resumen. Un tercer algoritmo de firma, también basado en retículos y con firmas más compactas, está en proceso de normalización.

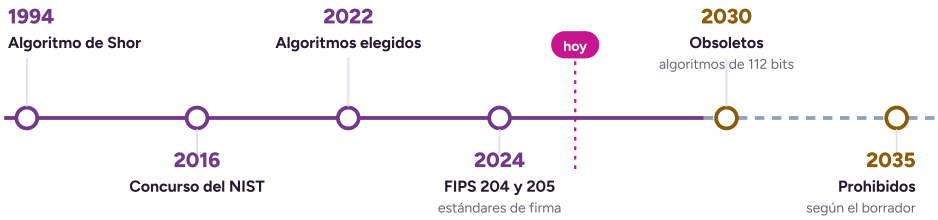


FIGURA 8 Hitos de la transición poscuántica. Las fechas de 2030 y 2035 provienen de un borrador y pueden cambiar.

Ese mismo año, el instituto publicó un borrador de calendario para la transición que propone considerar obsoletos los algoritmos de firma actuales de seguridad equivalente a 112 bits a partir de 2030 y prohibirlos a partir de 2035. Las agencias europeas de ciberseguridad han publicado hojas de ruta con horizontes similares. Las fechas pueden cambiar, pero la dirección es clara.

Lo que cambia en la práctica

Claves y firmas más grandes

Los algoritmos poscuánticos tienen claves y firmas bastante más grandes que las actuales: de unos pocos cientos de bytes se pasa a varios miles, y en algunos casos a decenas de miles. Para un PDF con varias firmas, cadenas de certificados y sellos de tiempo, eso significa archivos más pesados. Para los dispositivos con poca memoria, como algunas tarjetas, puede ser un límite real.

Toda la cadena debe migrar

Una firma poscuántica sólo es tan fuerte como su cadena de certificados, su sello de tiempo y su material de revocación. La transición involucra a autoridades de certificación, de sellado, de validación, a los fabricantes de dispositivos, a los lectores de PDF y a las listas de confianza. Ninguno puede hacerlo solo, y durante años convivirán ambos mundos.

Certificados híbridos

Para esa convivencia se estudian certificados y firmas híbridas, que combinan un algoritmo actual con uno poscuántico, de modo que la firma siga siendo verificable por los programas antiguos y protegida para el futuro. Los organismos de normalización trabajan en sus formatos, y es probable que las primeras implementaciones en firma de documentos adopten alguna de estas formas.

Agilidad criptográfica

La lección más importante de la transición no es un algoritmo, sino una propiedad: la agilidad criptográfica. Un sistema es ágil cuando puede cambiar de algoritmo sin rediseñarse, porque nunca dio por supuesto un algoritmo en particular. En un servicio de firma, eso implica saber qué algoritmos usa cada prestador, poder elegir entre varios, guardar en la evidencia qué algoritmo se usó en cada paso y tener un inventario que permita encontrar todos los documentos protegidos por un algoritmo que se debilita.

LISTA DE PREPARACIÓN

- Inventariar dónde se usa cada algoritmo: firmas, sellos de tiempo, cadenas, registros.
- Asegurar que los documentos de larga vida alcanzan el nivel de archivo y tienen sellos de tiempo renovables.
- Exigir a los prestadores un plan de transición con fechas.
- Probar formatos con firmas grandes antes de necesitarlos.
- Registrar el algoritmo en cada evento de la evidencia.

PARA RECORDAR

La computación cuántica amenaza la capacidad de distinguir firmas auténticas de falsificaciones futuras. La defensa combina sellos de tiempo de archivo renovados a tiempo, nuevos algoritmos ya normalizados y, sobre todo, sistemas ágiles que puedan cambiar de algoritmo sin rehacerse.

EPÍLOGO

Lo que construimos con estas ideas.

A lo largo de tres tomos evitamos nombrar productos. En estas páginas hacemos una excepción, la única de la serie: describimos la plataforma que desarrolla el editor de estos cuadernos y los problemas de este tomo a los que responde.

UNA NOTA ANTES DE LEER

Este epílogo no es neutral, y no pretende serlo. Lo escribe quien construye el producto que describe. Hemos procurado aplicarle el mismo criterio que al resto de la serie: afirmar sólo lo que puede comprobarse y decir también lo que el producto no hace.

Qué es Signing Flows

Signing Flows es un servicio de firma electrónica para documentos PDF. Quien envía sube un documento, elige quiénes deben actuar y en qué orden, ubica los campos y lo envía. Cada participante recibe un enlace, hace su parte en el navegador, y el servicio cierra el documento con la evidencia que lo acompaña.

Su unidad de trabajo es el circuito: un documento, sus personas, la manera en que circula y las reglas que lo gobiernan. Un circuito puede recorrerse en serie, en paralelo o en copias individuales, los patrones que describimos en el primer capítulo. Cada persona tiene un rol: firma, aprueba sin firmar, revisa sin firmar o sólo recibe una copia.

Tres ideas de este tomo están en su base. Las reglas pertenecen a la persona y no al documento: para cada participante se define cómo firma, con su propio certificado o por consentimiento con un sello de plataforma, qué nivel de identidad se le exige y qué puede hacer con el documento; y un documento que pide a alguien algo que la cuenta no puede ofrecer no se envía, e indica a quién y qué falta. La organización es un árbol,

con aislamiento aplicado en la propia base de datos y una marca en capas, para que quien firma vea la marca de quien le escribe. Y nada se afirma que la evidencia no respalde.

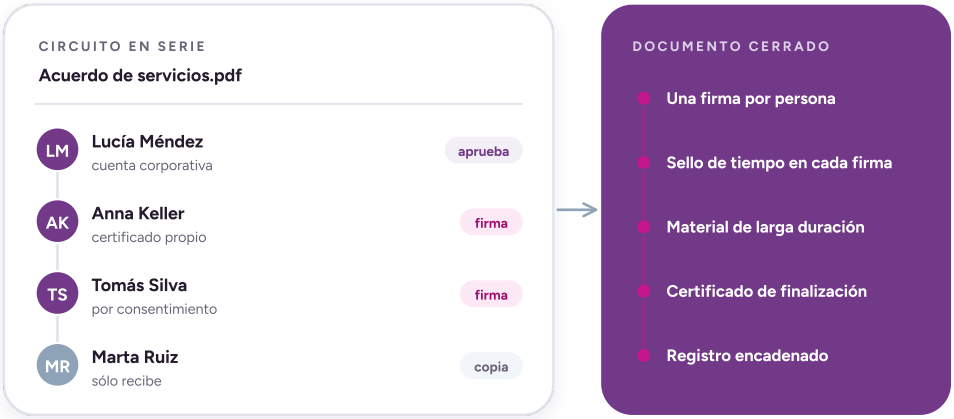


FIGURA 9 Un circuito de Signing Flows y lo que lleva el documento al cerrarse.

Lo que lleva un documento cerrado

- **Una firma por persona,** cada una sobre el estado del documento en el momento en que esa persona firmó.
- **Un sello de tiempo en cada firma,** pedido a la autoridad de sellado configurada.
- **Material de conservación a largo plazo:** la cadena de certificados y la información de revocación de cada firma, y un sello de tiempo sobre el archivo terminado. Con autoridad de sellado y revocación alcanzable, el documento llega al nivel de archivo de PAdES, según lo midió el validador de la Comisión Europea; sin ellas, queda en un nivel menor y lo declara.
- **Un certificado de finalización,** emitido una sola vez, con el sello de plataforma, en español e inglés.
- **Un registro de evidencia encadenado,** en el que cada evento se vincula con el anterior por su huella.

Lo que no afirma

Pensamos que una lista de lo que un producto no promete es más útil que la de sus virtudes. Éstas son algunas frases que Signing Flows no dice de sí mismo, y por qué.

LA FRASE	POR QUÉ NO
"Una vez firmado, no puede modificarse"	Los cambios permitidos posteriores conviven con firmas anteriores válidas. Cada firma cubre el documento tal como estaba al firmarse.
"Somos un prestador de servicios de confianza"	Usa los servicios de uno. La confianza en el certificado, su acreditación y su revocación son responsabilidad del prestador.
"Nunca tenemos claves privadas"	Con prestadores de firma remota, la clave queda en el prestador. Con el motor local, la plataforma guarda una clave en un archivo.
"El validador dice válido, así que nadie lo alteró"	La política por defecto de un validador puede aprobar un archivo en el que se reescribió un campo bloqueado.

En su consola, las capacidades que una instalación no tiene habilitadas aparecen en gris, con el motivo a la vista y sin fechas.

Por qué ahora

Los capítulos de este tomo describen un cambio de fondo. Durante veinte años, la pregunta del sector fue cómo firmar. Hoy la firma está disponible en muchas formas y de muchos prestadores, y lo será todavía más cuando las carteras europeas pongan la firma cualificada en el bolsillo de cada ciudadano. La pregunta pasa a ser cómo orquestar: qué firma pedir a cada persona, a qué prestador, con qué identidad, y cómo probarlo después. Cinco fuerzas empujan en esa dirección.

- **La identidad se volvió portátil.** Carteras, identidades nacionales y credenciales verificables multiplican las maneras de identificar a una persona, y alguien tiene que elegir y registrar la adecuada para cada acto.

- **Los regímenes son nacionales, los procesos no.** Un mismo contrato atraviesa países con leyes y prestadores distintos, y la regla tiene que vivir en cada participante.
- **Los prestadores de confianza buscan distribución.** Necesitan plataformas que lleven sus servicios a organizaciones de todos los tamaños, con su marca y su propio árbol de clientes.
- **La inteligencia artificial entra en el proceso.** Una capa que registra cada acto y distingue personas de máquinas permite incorporarla sin perder la prueba.
- **La criptografía va a cambiar.** La transición poscuántica premia a quien guarda en la evidencia qué algoritmo usó en cada paso y puede renovar a tiempo sus sellos de tiempo de archivo.

Signing Flows se diseñó desde el principio para orquestar esas piezas, y no para firmar con un único mecanismo.

De dónde viene

Signing Flows es fruto de una larga evolución compartida. Miembros de Interfase, la empresa uruguaya que edita estos cuadernos, trabajan con certificados digitales e infraestructura de clave pública desde el año 2000. Un pionero de la infraestructura de clave pública, cuyos orígenes se remontan a los primeros productos comerciales del área, a mediados de la década de 1990, acompañó a Interfase en buena parte de la historia que relatan estos tomos, y Signing Flows se integra hoy en su propuesta de orquestación de identidad ciudadana.

Nos pareció justo cerrar la serie así: con la constancia de que las ideas descritas en estas páginas no son sólo teoría, y con la invitación a comprobarlas.

REFERENCIA

Glosario

Los términos principales de este tomo, en el sentido en que se usan aquí. Los conceptos básicos están en los glosarios de los tomos 1 y 2.

Agente

Sistema de inteligencia artificial que ejecuta acciones en otros sistemas en nombre de una persona u organización.

Agilidad criptográfica

Capacidad de un sistema para cambiar de algoritmo criptográfico sin rediseñarse.

Aislamiento por fila

Regla de seguridad que la base de datos aplica a cada fila, de modo que cada organización sólo pueda ver y modificar sus propios datos.

Cartera de identidad digital

Aplicación en la que una persona guarda credenciales emitidas por terceros y desde la que puede presentarlas y, en algunos casos, firmar.

Catálogo de prestadores

Inventario de los prestadores de confianza que un servicio puede usar, con sus jurisdicciones, mecanismos, niveles y condiciones.

Certificado híbrido

Certificado que combina un algoritmo actual con uno poscuántico para convivir con programas antiguos y resistir a las computadoras cuánticas.

Credencial verificable

Conjunto de afirmaciones sobre una persona, firmado por su emisor, que el titular guarda y presenta a quien la necesita.

Degradación declarada

Práctica de completar un proceso con un nivel de firma menor al previsto sólo cuando las reglas lo permiten, dejando constancia del nivel alcanzado y del motivo.

Delegación

Autorización explícita, limitada y registrada para que otra persona o un sistema actúe en nombre de alguien.

Divulgación selectiva

Capacidad de presentar sólo algunos atributos de una credencial, o una afirmación derivada de ellos, sin revelar el resto.

Firma incrustada

Firma que ocurre dentro de la aplicación de otra organización, en una ventana provista por la plataforma de firma.

Firma por consentimiento

Mecanismo en el que la persona manifiesta su voluntad tras identificarse y la plataforma aplica al documento un sello de organización, registrando quién consintió y cómo.

Idempotencia

Propiedad de una operación que produce el mismo resultado aunque se repita varias veces.

Multiinquilino

Modelo en el que una misma instalación de software atiende a muchas organizaciones, con sus datos aislados entre sí.

Niveles de garantía

Escalas que clasifican la fuerza de la identificación de una persona, como los niveles bajo, sustancial y alto de eIDAS.

Orquestación

Coordinación de personas, prestadores, mecanismos y sistemas para que un proceso de firma se complete y quede probado.

Webhook

Aviso que una plataforma envía a otro sistema cuando ocurre un evento, firmado para probar su origen y reintentado si no se confirma.

REFERENCIA

Para seguir leyendo

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

Identidad y carteras

Unión Europea. Reglamento (UE) 2024/1183, que modifica el Reglamento (UE) 910/2014 y establece el marco europeo de identidad digital.

NIST. Special Publication 800 63, guías de identidad digital, revisión 4.

W3C. Verifiable Credentials Data Model, versión 2.0, 2025.

ISO/IEC 18013 5, permisos de conducir móviles, 2021.

Firma remota y prestadores

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

ETSI. TS 119 431 y TS 119 432, firma en servidor. CEN. EN 419 241, sistemas confiables para firma en servidor.

Integración

OpenAPI Initiative. OpenAPI Specification, versión 3.

Operación y seguridad

ISO/IEC 27001, sistemas de gestión de la seguridad de la información, 2022.

AICPA. Criterios de servicios de confianza para informes SOC 2.

ETSI. EN 319 401, requisitos generales de política para prestadores de servicios de confianza.

Accesibilidad y lenguaje

W3C. Web Content Accessibility Guidelines (WCAG) 2.2, 2023.

Unión Europea. Directiva (UE) 2019/882, Ley Europea de Accesibilidad.

ISO 24495 1, lenguaje claro, 2023.

Inteligencia artificial

Unión Europea. Reglamento (UE) 2024/1689, de inteligencia artificial.

Criptografía poscuántica

Shor, P. Algoritmos para la computación cuántica: logaritmos discretos y factorización. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

NIST. FIPS 204 y FIPS 205, estándares de firma digital poscuántica, agosto de 2024.

NIST. IR 8547, borrador sobre la transición a la criptografía poscuántica, 2024.

Rúbrica.

CUADERNOS SOBRE FIRMA, IDENTIDAD Y CONFIANZA DIGITAL

Una firma es un instante. Un servicio de firma es todo lo que la hace posible.

Este tercer tomo explica cómo se diseña, se integra y se opera un servicio de firma: los procesos, la identidad de quien firma, las carteras digitales, la elección de prestadores, la integración con otros sistemas, la operación a escala, la accesibilidad, y lo que cambian la inteligencia artificial y la criptografía poscuántica.

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