



Videoconferencia

Infraestructura Oficial de la Firma Electrónica

Realizada el 14 de julio de 2025

Videoconferencia: Infraestructura Oficial de la Firma Electrónica

Editado por:

© Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Indecopi

Escuela Nacional de Defensa de la Competencia y de la Propiedad Intelectual

Calle De la Prosa N° 104, San Borja, Lima, Perú

Teléfono: (+51) 224-7800, anexo 4001

Correo electrónico: escuela@indecopi.gob.pe

Website de la Escuela: <https://escuela.indecopi.gob.pe/>

Website Indecopi: <https://www.gob.pe/indecopi/>

Director de la Escuela Nacional del Indecopi:

Fernando Lucio Cieza Paredes

Supervisión y edición:

Ingrid Romero Manco

Transcripción:

Abigail Soler Oré

Diseño y diagramación:

Valeria María Moreno Vásquez

Transcripción escrita literal del audio de la grabación de la videoconferencia
“Infraestructura Oficial de la Firma Electrónica”

Publicación electrónica. Primera edición. Lima, agosto de 2026

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2026-08472

ÍNDICE

LA FIRMA ELECTRÓNICA Y LA FIRMA DIGITAL (LEY 27269)	4
LA FIRMA DIGITAL: LA MÁS SEGURA	7
CRIPTOGRAFÍA DE PAR DE CLAVES	11
CERTIFICADO DIGITAL	14
¿QUÉ ES EL IOFE?	20
¿QUÉ ES LA ACREDITACIÓN?	23
PRESUNCIONES LEGALES EN FAVOR DE LA FIRMA DIGITAL ACREDITADA	25
APLICACIONES DE LOS SERVICIOS Y PRODUCTOS ACREDITADOS	26

LA FIRMA ELECTRÓNICA Y LA FIRMA DIGITAL (LEY 27269)

Exposición a cargo de Pedro Castillo del Carpio

Ejecutivo 1 de la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica (DGI) – Indecopi

En el lenguaje cotidiano suelen usarse indistintamente los términos firma electrónica y firma digital; sin embargo, legalmente no son exactamente lo mismo. La firma digital es una clase de firma electrónica, pero existen otras formas de firma electrónica. Por ello, el concepto de firma electrónica es más amplio y general.

Firma electrónica

Según la ley nacional, la firma electrónica es cualquier símbolo o dato creado mediante medios electrónicos, magnéticos u ópticos, que se utiliza con el propósito de autenticar un documento electrónico, es decir, vincular dicho documento con una persona determinada.

Este objetivo es equivalente al de la firma manuscrita en el mundo físico: cuando una persona firma un contrato, acta, resolución o declaración, busca establecer un vínculo entre el documento y la persona, comprometiéndose a respetar los derechos y obligaciones que nacen de ese documento.

Así, la firma electrónica viene a ser un correlativo de la firma manuscrita, trasladando esa lógica de la realidad tangible a la realidad electrónica. Por ejemplo, con el uso de Outlook, cuando una persona envía un correo electrónico y coloca su nombre al final — “Pedro Castilla del Carpio”—, ese nombre califica como firma electrónica, ya que es un símbolo creado por medios electrónicos y se utiliza con la finalidad de dar autenticidad al mensaje y comunicar que el remitente es quien dice ser.

Este tipo de firma electrónica suele ser suficiente para comunicaciones de mero trámite, como informar que un informe ya fue concluido. Sin embargo, presenta un alto margen de duda, pues cualquiera podría tipear el nombre del remitente. Si el contenido fuera más serio, por ejemplo, una oferta para comprar un inmueble por s/.200,000 soles, el destinatario razonablemente exigiría un medio más confiable, ya que el simple tipeo del nombre no garantiza suficientemente la identidad del firmante.

Otro ejemplo de firma electrónica es la firma escaneada. Esta consiste en capturar la imagen de una firma manuscrita y guardarla como archivo. Basta con copiarla y pegarla en documentos electrónicos. Tiene la ventaja de que visual y culturalmente reconocemos la firma gráfica como un medio de identificación. Sin embargo, es fácilmente falsificable, ya que basta copiar la imagen desde otro documento para reutilizarla. Por ello, aunque puede ser aceptable para trámites simples, resulta insegura para actos jurídicos relevantes, especialmente aquellos que implican obligaciones económicas. Aun así, legalmente sigue siendo una firma electrónica, porque encaja dentro de la definición legal.

Existe también la firma electrónica manuscrita, que se realiza firmando con un lapicero electrónico o el dedo sobre una pantalla o tablero digital, generando una imagen gráfica en tiempo real. Este tipo de firma ofrece mayor seguridad que la firma digitalizada, aunque sigue siendo una modalidad de firma electrónica, no una firma digital.

Firma digital (como modalidad específica)

La firma digital no es un concepto opuesto a la firma electrónica, sino una especie dentro del género. Así como el apio o el espárrago son verduras, la firma digital es una forma particular de firma electrónica. La diferencia clave es que la firma digital no es un simple símbolo, sino que se basa en una tecnología específica de criptografía de doble clave.

La firma digital utiliza un par de claves criptográficas asignadas a cada persona:

- Clave privada: es exclusiva del titular, solo él puede usarla para firmar.
- Clave pública: sirve para que el receptor del documento verifique la autenticidad de la firma.

Cuando un documento es firmado digitalmente, el destinatario puede validar que el documento fue firmado por el titular del certificado, que el contenido no ha sido alterado ya que la firma es auténtica.

En consecuencia, toda firma digital es una firma electrónica, pero no toda firma electrónica es una firma digital.

Las firmas electrónicas incluyen, entre otras:

- Nombre tipeado
- Firma digitalizada o escaneada
- Firma manuscrita en dispositivos electrónicos
- Firmas biométricas (huella dactilar, iris, etc.)
- Firma digital (la más segura)

LA FIRMA DIGITAL: LA MÁS SEGURA

La firma digital es una modalidad de firma electrónica sustentada en mecanismos criptográficos. Si la firma digital se encuentra acreditada, se garantiza la autenticidad, la integridad y el carácter legalmente vinculante.

A partir de este punto, la mayor parte de la presentación se centrará en la firma digital. En la parte superior aparece un recuadro azul oscuro lleno de ceros y unos. Esto no es casual: las computadoras no procesan palabras en lenguajes humanos, sino que finalmente convierten todo el texto en números, y más específicamente, en ceros y unos, con los cuales construyen todos sus sistemas internos.

Vamos a adelantar un concepto clave: la acreditación. Lo desarrollaremos con mayor detalle más adelante, pero podemos ofrecer una explicación breve desde ahora. En esencia, la acreditación está directamente vinculada al tema central de esta presentación: la Infraestructura Oficial de la Firma Electrónica (IOFE).

La acreditación es un proceso —y también el resultado de ese proceso— mediante el cual la autoridad competente, en este caso el Indecopi, evalúa a los proveedores de servicios y productos de firma digital. Es importante precisar que no se evalúa a las personas que usan la firma digital, sino a:

- Los proveedores de certificados digitales.
- Los fabricantes o comercializadores de tokens criptográficos.
- Los proveedores de tarjetas inteligentes con microchip.
- Los desarrolladores de software de firma digital.

El Indecopi verifica que estos proveedores cumplan estándares técnicos y de seguridad óptimos, ya sea que produzcan directamente estos dispositivos o que actúen como socios locales de proveedores extranjeros, conforme a lo permitido por la ley. Una vez obtenida la acreditación —que implica el reconocimiento oficial de la autoridad—, los dispositivos y programas que ofrecen pueden considerarse productos acreditados.

Cuando los usuarios finales utilizan estos productos acreditados para generar una firma digital, se habla de una firma digital acreditada.

No siempre es necesario adquirir productos comerciales, ya que, por ejemplo:

- El RENIEC ofrece un software gratuito de firma digital, el cual está acreditado por el Indecopi.
- Las personas que cuentan con DNI electrónico ya poseen certificados digitales incorporados.

Si, mediante estos elementos, se genera una firma digital, dicha firma adquiere el carácter de firma digital acreditada, el uso de esta garantiza legalmente:

- La autenticidad del documento electrónico.
- La integridad del documento, es decir, que no ha sido alterado.
- El carácter legalmente vinculante entre la persona y el documento.

Este último aspecto es fundamental: sin carácter vinculante, un documento no puede producir efectos legales, ya sea que se trate de un documento en papel o de un documento electrónico. Estos tres efectos serán desarrollados con mayor detalle más adelante.

En ese punto ya es pertinente hacer referencia a la encriptación electrónica, específicamente a la encriptación de doble clave. Aunque pueda parecer un concepto complejo o misterioso, lo cierto es que esta misma tecnología se utiliza diariamente en aplicaciones ampliamente conocidas, como el WhatsApp, que usamos varias veces al día y Blockchain, conocido principalmente por su relación con las criptomonedas. La tecnología de encriptación de doble clave es el soporte de la seguridad y privacidad de los mensajes de WhatsApp y el fundamento tecnológico del sistema blockchain. Cuando WhatsApp indica que los mensajes están encriptados y que nadie, ni siquiera la propia plataforma, puede leerlos, ello es posible gracias a esta tecnología, que es extraordinariamente robusta. Entonces, no es casual que la firma digital tenga ventajas legales frente a otras firmas electrónicas. Estas ventajas se deben:

- A la robustez tecnológica de la criptografía de doble clave.
- A la facilidad para demostrar el vínculo entre el firmante y el documento.

En el caso de otras firmas electrónicas, demostrar ese vínculo puede ser muy complejo. Por ejemplo, si alguien envía un mensaje firmándolo solo con su nombre y luego lo niega, probar que efectivamente fue esa persona quien lo envió resulta difícil y controvertido. En cambio, en la firma digital, la demostración del vínculo entre la persona y el documento es sencilla, inmediata y objetiva, como se explicará más adelante. Ya se ha introducido el concepto de criptografía de par de claves.

Dado que para algunos puede tratarse de ideas nuevas, estos conceptos serán reiterados, no por ser complicados, sino porque todo concepto novedoso requiere superar una primera barrera de comprensión.

CRIPTOGRAFÍA DE PAR DE CLAVES

La criptografía es el conjunto de técnicas matemáticas y semánticas mediante las cuales un texto legible —por ejemplo, un documento en castellano, inglés o alemán— es convertido en un texto ilegible, imposible de comprender para quien no esté autorizado. Este proceso transforma el texto en una secuencia aparentemente arbitraria de letras, números o símbolos, lo que comúnmente se percibe como una “sopa de caracteres”.

La transformación se realiza mediante procesos o algoritmos, es decir, secuencias ordenadas de pasos orientadas a un objetivo concreto: convertir información legible en información ilegible. Además, estos procesos pueden incorporar claves criptográficas, que constituyen datos de entrada específicos (números o combinaciones de números y letras) necesarios para ejecutar la transformación. Una característica esencial de la criptografía es que el proceso es reversible: aquello que fue convertido en ilegible puede posteriormente recuperar su forma original y legible, siempre que se utilicen los procesos y claves adecuados.

La criptografía no es una tecnología reciente. Ha sido utilizada desde hace aproximadamente dos mil años, especialmente en contextos militares.

En la antigüedad —por ejemplo, en la época romana— los mensajeros transportaban textos cifrados para evitar que, en caso de captura, el mensaje pudiera ser entendido por el enemigo. Por ello, es importante precisar que la criptografía no es necesariamente electrónica. Durante siglos existió una criptografía tradicional, aplicada sobre papel, mucho antes de la aparición de computadoras y medios digitales.

En la criptografía tradicional, se emplea un mismo proceso o clave secreta tanto para encriptar como para desencriptar un texto y esta clave debía mantenerse estrictamente en secreto y solo podía ser conocida por quienes participaban en la comunicación. Si el mensajero era capturado y el enemigo conocía el proceso o la clave, el sistema perdía totalmente su utilidad. Por ello, en este modelo existe una sola clave, esa clave es secreta y si deja de ser secreta, el sistema no sirve absolutamente para nada.

En la criptografía de clave pública o de doble clave se utilizan dos claves distintas:

- Clave privada: exclusiva del titular, conocida solo por él.
- Clave pública: se distribuye libremente y puede ser conocida por cualquier tercero.

Ambas claves mantienen una relación matemática compleja, no arbitraria. No se trata de números pequeños ni elegidos al azar, cabe mencionar que las claves modernas tienen aproximadamente 300 dígitos de longitud, lo que las hace inviables de procesar manualmente, pero perfectamente manejables por computadoras.

Un principio fundamental de este sistema es que cada clave descripta lo que la otra encripta. Sin embargo, debido a la naturaleza de los procesos matemáticos involucrados la misma clave que se usó para encriptar NO puede usarse para descriptar y esto no es una decisión legal ni convencional, sino una imposibilidad técnica y matemática. Si se utiliza la clave pública para encriptar un documento, solo la clave privada correspondiente podrá descriptarlo. Y si se encripta con la clave privada, únicamente la clave pública permitirá revertir el proceso. Por lo tanto, no es posible usar una sola clave en ambos sentidos y siempre se requiere la clave complementaria del par. Este principio es la base técnica de la firma digital.

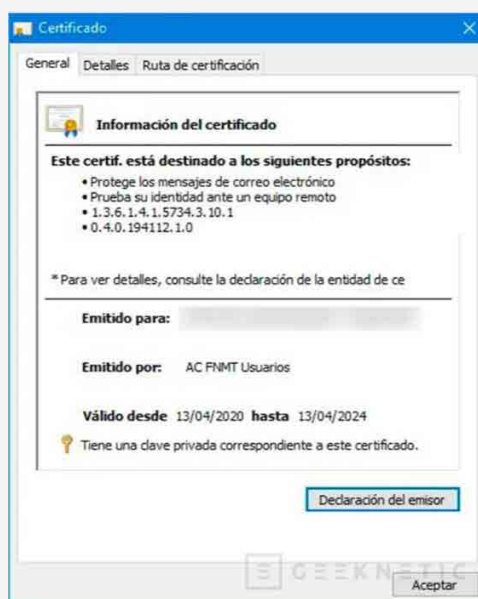
CERTIFICADO DIGITAL

Un certificado digital es un archivo electrónico que permite autenticar la identidad de una persona o entidad en entornos digitales. Este certificado se utiliza para garantizar la seguridad al firmar documentos digitalmente y proteger la información mediante mecanismos criptográficos. Contiene datos que vinculan la identidad del titular con una clave pública, asegurando que las comunicaciones y firmas sean válidas y confiables.

Para entender mejor, supongamos que una persona desea firmar digitalmente. En este proceso se generan dos claves: una clave privada y una clave pública. La clave privada puede almacenarse en un token criptográfico o en una tarjeta con microchip. En este dispositivo también se encuentra el certificado digital, que es un pequeño archivo electrónico donde se incluye la clave pública del titular.



Cuando descargamos o visualizamos un certificado digital en la computadora, aparece una pantalla con información relevante. En ella se muestran datos como el plazo de vigencia del certificado, la entidad emisora (por ejemplo, RENIEC), los usos permitidos del certificado (para qué funciones específicas puede utilizarse) y diversos datos técnicos adicionales.



Certificado digital



Documento electrónico

Emitido por una Entidad de Certificación Digital (por ejemplo, RENIEC).



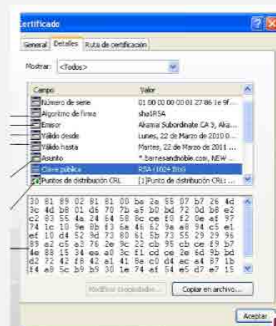
Clave pública

Certifica la asignación de una clave criptográfica pública a una persona específica.



Identidad digital

Funciona como un documento de identidad en entornos digitales. Cada vez que usted firma y envía un documento electrónico, también su certificado es enviado. Se usará su data para verificar la autenticidad de su firma.



Ahora bien, el certificado que se muestra en el ejemplo puede ser antiguo, pero es válido para fines explicativos. En la parte inferior del certificado digital suele aparecer un número extremadamente largo. Aunque visualmente parece estar formado por muchos grupos pequeños de números y letras, en realidad es un solo número y este número está expresado en sistema hexadecimal, que utiliza: Los dígitos del 0 al 9 y las letras A, B, C, D, E y F para representar valores mayores al 9. Por eso vemos letras mezcladas con números.

Ese número hexadecimal representa la clave pública completa. Incluso, si aparece una barra lateral de desplazamiento, significa que la clave pública continúa más abajo, confirmando que es un valor muy extenso. La clave pública está contenida íntegramente dentro del certificado digital.

Ambos ejemplos presentados son certificados digitales, el certificado digital tiene muchos campos, e como una pequeña arquitectura puesta en muchos campos que iré mostrando. El certificado digital (y, por tanto, las claves) puede estar almacenado en distintos soportes como en el microchip del DNI electrónico, en un token criptográfico, descargado en la computadora del usuario y en esquemas de firma remota (que no se abordan en esta explicación).

En el caso del DNI electrónico (documento electrónico) o del token, las dos claves (pública y privada) están físicamente almacenadas en dichos soportes. Aunque ambas claves estén almacenadas en el mismo soporte (por ejemplo, el microchip del DNI electrónico), su uso es distinto, la clave privada nunca se comparte, se utiliza únicamente para firmar digitalmente y solo la usa el titular, a través del software de firma.

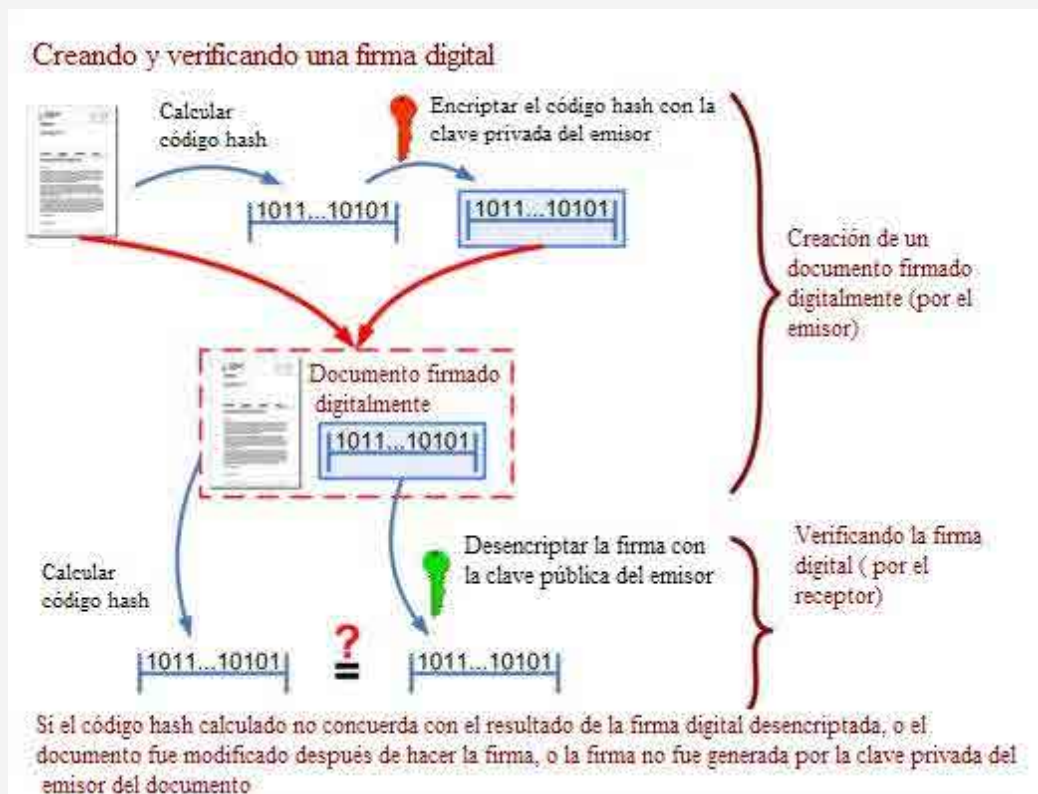
En cambio, la clave pública puede ser compartida libremente, se encuentra contenida dentro del certificado digital y sirve para verificar la firma digital. Cuando el titular firma un documento digital desde su computadora, el software de firma, de forma automática (sin intervención manual del usuario), accede al certificado digital almacenado en el DNI electrónico mediante un lector de tarjetas conectado a la computadora, puede extraer una copia del certificado digital y envía ese certificado junto con el documento electrónico firmado al destinatario. Esto no es ilegal ni encubierto: es parte normal del proceso de firma digital.

a. Respecto a la creación de la firma digital por parte del emisor tomemos como ejemplo un documento electrónico (un contrato, acta, declaración, etc.). Se daría de la siguiente forma:

1° Cálculo de hash: La computadora lee el documento (que internamente son números), luego lo comprime mediante un algoritmo matemático conocido como función hash y obtiene un resumen numérico único (el hash).

2° Firma del hash: Sobre el hash previamente obtenido se aplica algoritmos matemáticos - los algoritmos no son secretos-, luego se introduce la clave privada del firmante y el resultado de esta operación es la firma digital (llave roja).

3° Envío: Se envía por internet, el documento original, la firma digital y una copia del certificado digital (que contiene la clave pública).



b. Respecto a la creación de la firma digital por parte del receptor (por ejemplo, en otro país) no verifica nada manualmente; todo lo hace el software. Se realizan dos operaciones:

1° Hash del documento recibido: El software toma el documento recibido, aplica el mismo algoritmo y obtiene el mismo código hash.

2° Verificación de la firma: El software toma la firma digital recibida, usa la clave pública contenida en el certificado digital del firmante, realiza la operación inversa a la firma y obtiene el hash original generado por el emisor.

Actualmente existen dos valores hash: uno calculado directamente a partir del documento y otro obtenido al descryptar la firma digital. Si ambos coinciden, podemos afirmar que el documento no ha sido modificado, que la firma fue generada con la clave privada correspondiente y, por lo tanto, la identidad del firmante queda plenamente acreditada. En caso contrario, si no coinciden, significa que el documento fue alterado o que la firma no se generó con la clave privada del supuesto firmante.

Ahora bien, en un caso hipotético de conflicto, en vía judicial, el juez solo necesita la clave pública (contenida en el certificado digital) y repite la verificación sobre si los hashes coinciden, queda demostrado que solo el titular de la clave privada pudo firmar. A diferencia de la firma manuscrita, no existe margen razonable de negación. La firma digital ofrece una certeza técnica y jurídica superior.

En conclusión, el certificado digital es un elemento esencial, ya que en él se encuentra la clave pública del titular. Es importante destacar que sin un certificado digital no puede existir una firma digital con validez legal. Esta firma garantiza tanto la autenticidad como la integridad del documento, permitiendo verificar que el contenido no ha sido alterado y que efectivamente proviene del emisor autorizado.

¿QUÉ ES EL IOFE?

La firma digital, basada en la encriptación electrónica de doble clave, se inserta dentro de un sistema denominado Infraestructura Oficial de la Firma Electrónica (IOFE), así denominado en el Reglamento de la Ley N.º 27269 – Ley de Firmas y Certificados Digitales. Si bien la Ley 27269 tiene aproximadamente 25 años de vigencia, la construcción efectiva de la IOFE no se remonta a ese tiempo, sino que se ha desarrollado progresivamente durante los últimos 12 años.

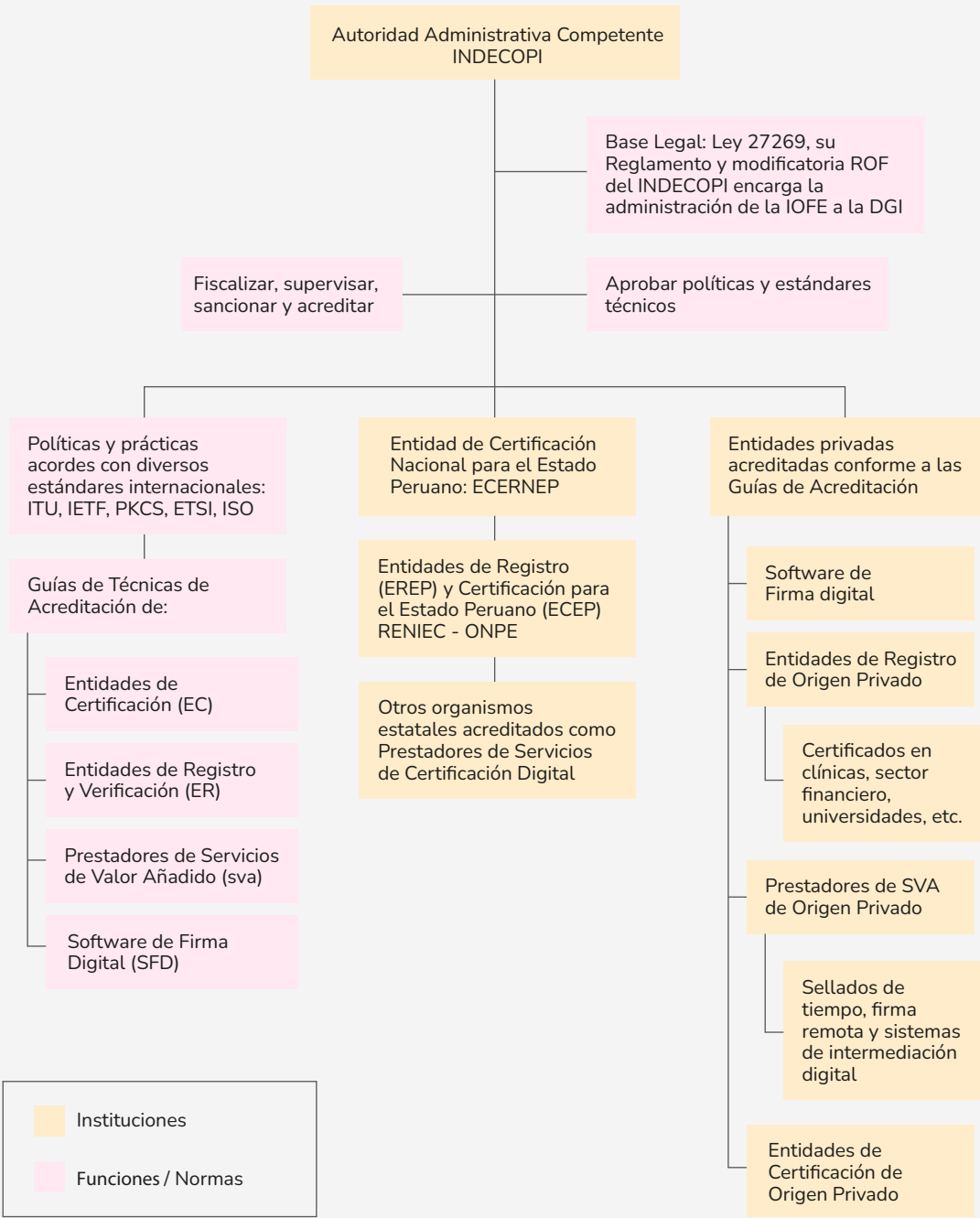
La IOFE no es un sistema aislado ni una entidad única, sino un ecosistema digital, en el que múltiples actores se encuentran interrelacionados jurídicamente, técnica y funcionalmente. No se trata de un ecosistema físico o biológico, sino un ecosistema digital normado por el Estado.

La IOFE está constituida por empresas privadas, públicas y personas naturales, todas ellas acreditadas por el Indecopi, conforme al Reglamento de la Ley de Firmas Digitales y a las Guías Técnicas de Acreditación. Por ejemplo, una empresa que fabrica: tokens criptográficos, tarjetas con microchip o software de firma digital puede solicitar su acreditación ante el Indecopi. Esta acreditación no solo otorga una ventaja comercial, sino, principalmente, una ventaja legal, ya que solo la firma digital acreditada tiene equivalencia funcional inmediata con la firma manuscrita, según el Reglamento.

El legislador optó deliberadamente por este modelo, teniendo en cuenta que no toda firma digital es equivalente a la manuscrita, solo aquella generada con productos y servicios previamente evaluados y acreditados por la autoridad competente.



Infraestructura Oficial de la Firma Electrónica



Dentro de la Administración Pública se determinó la existencia de tres Actores públicos centrales de la IOFE:

- Indecopi: Es la Autoridad Administrativa Competente y sus funciones principales son otorgar la acreditación, supervisar a las entidades acreditadas. La acreditación tiene una vigencia de cinco años, pero existe una supervisión anual, destinada a verificar que los productos y servicios continúen cumpliendo los requisitos técnicos y legales. Esto evita que una entidad cumpla solo durante el proceso de acreditación y luego relaje sus estándares.
- Presidencia del Consejo de Ministros – PCM: A través de la Secretaría de Gobierno Digital, la PCM actúa como la Entidad de Certificación Nacional para el Estado peruano. La PCM emite los certificados raíz, que constituyen la base de confianza sobre la cual otras entidades estatales pueden emitir certificados digitales a ciudadanos y funcionarios públicos.
- RENIEC y ONPE: El RENIEC es una Entidad de Certificación del Estado. Con un certificado raíz emitido por la PCM, el RENIEC emite certificados digitales a ciudadanos mediante el DNI electrónico y certificados digitales a funcionarios públicos.

La ONPE también es una Entidad de Certificación del Estado, con la particularidad de que emite certificados digitales de muy corta duración (un día), destinados a los procedimientos electorales para miembros de mesa, personeros políticos. Esta característica es excepcional, ya que normalmente los certificados digitales tienen una vigencia de uno, dos o tres años.

¿QUÉ ES LA ACREDITACIÓN?

En cuanto a la acreditación, todas las empresas proveedoras de dispositivos, software o servicios asociados a la firma digital, pueden optar por acreditarse y las que se acreditan pasan a formar parte de la IOFE. Estas entidades deben cumplir con estándares técnicos, lineamientos operativos, políticas de seguridad y los documentos que generan deben de haber sido firmados con software de firma digital acreditado y haber sido validados con certificados digitales acreditados. El ecosistema digital de la IOFE es la suma de: i) las empresas, entidades públicas y personas naturales acreditadas por el Indecopi, ii) las políticas, estándares técnicos y lineamientos que ellas deben cumplir y iiiv) los servicios que prestan y los productos que ofrecen vinculados a la tecnología de firma digital.

Ahora bien, las guías técnicas de acreditación cuentan con las siguientes 4 categorías:

- **Entidades de Certificación (EC)**
Emiten certificados digitales.
- **Entidades de Registro y Verificación (ER)**
Verifican la identidad de las personas antes de la emisión del certificado.
- **Software de Firma Digital (SFD)**
Herramientas que permiten generar firmas digitales.

- **Prestadores de Servicios de Valor Añadido (SVA)**

Brindan servicios adicionales basados en la misma tecnología criptográfica, como: sellado de tiempo, firma remota y sistemas de intermediación digital.

Todos estos servicios utilizan la misma tecnología de criptografía de clave pública. Aunque la acreditación no es obligatoria, un proveedor puede operar sin acreditarse y comercializar productos de firma digital. Sin embargo, en caso de controversia judicial la firma digital acreditada goza de ventajas probatorias inmediatas y mientras que la no acreditada puede requerir una probanza más compleja. Por ello, el Reglamento establece que solo la firma digital acreditada tiene equivalencia funcional directa con la firma manuscrita.

PRESUNCIONES LEGALES EN FAVOR DE LA FIRMA DIGITAL ACREDITADA

El Reglamento de la Ley de Firmas Digitales establece las siguientes presunciones legales:

- 1° Se presume que el suscriptor tiene el control exclusivo de su clave privada, mientras no comunique su pérdida o compromiso.
- 2° Se presume que el documento fue firmado usando dicha clave privada.
- 3° Se presume que el documento no ha sido alterado después de la firma.

La consecuencia jurídica es que el suscriptor no puede repudiar ni desconocer un documento electrónico firmado digitalmente con su clave privada. Estas presunciones se justifican por el altísimo nivel de seguridad técnica de la criptografía de clave pública, es decir, la probabilidad de vulnerar una clave privada de cientos de dígitos es prácticamente nula. Gracias a estas presunciones las personas pueden contratar, transferir dinero y realizar actos jurídicos a distancia, con la certeza de que la firma digital acreditada no puede ser desconocida posteriormente. Esta misma tecnología se utiliza cotidianamente en portales bancarios, comunicaciones seguras (HTTPS), mensajería como WhatsApp, sistemas de inteligencia artificial, garantizando autenticidad, integridad y seguridad de la información.

APLICACIONES DE LOS SERVICIOS Y PRODUCTOS ACREDITADOS

Plataforma de Facturación Electrónica – Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT)

Entrando ya a las aplicaciones de la firma digital en el Perú, una de las más importantes es la facturación electrónica, que utiliza firma digital desde hace varios años. Todos los días se firman centenares de miles de documentos tributarios electrónicos, no solo en el Perú sino también en todo el mundo.

La tecnología que se emplea es exactamente la misma tecnología de criptografía de doble clave, aplicada al ámbito tributario, lo que permite garantizar la autenticidad e integridad de los comprobantes de pago electrónicos.

Ventanilla Única de Comercio Exterior (VUCE)- Ministerio de Comercio Exterior y Turismo

La Ventanilla Única de Comercio Exterior (VUCE) del Ministerio de Comercio Exterior y Turismo también utiliza firma digital en diversos procedimientos. En particular, se emplea en aquellos trámites vinculados a temas sanitarios, como permisos de la autoridad sanitaria, importación o exportación de frutas, semillas, animales, células animales y productos del mar.

A nivel mundial, los sistemas sanitarios están tendiendo a articularse mediante tecnología de firma digital, precisamente por los altos niveles de seguridad y trazabilidad que ofrece.

Sistema de Intermediación Digital (SID) - Superintendencia Nacional de los Registros Públicos (SUNARP)

En el ámbito registral, los Registros Públicos cuentan con una plataforma denominada Sistema de Intermediación Digital (SID). A través de esta plataforma, los notarios ingresan actualmente una gran cantidad de documentos electrónicos, que ya no se presentan en formato físico, sino que se tramitan íntegramente de manera digital mediante el uso de firma digital.

DNI electrónico - Registro Nacional de Identificación y Estado Civil (RENIEC)

El DNI electrónico es otra aplicación central de la firma digital y se utiliza en múltiples servicios del Estado, como programas sociales (por ejemplo, Pensión 65), programas de becas, obtención de certificados, como antecedentes, de manera remota. El certificado digital contenido en el DNI electrónico permite realizar estas operaciones a distancia, con seguridad jurídica y técnica.

Sistema de Notificaciones Electrónicas (SINOE) - Expediente Judicial Electrónico (EJE) – Poder Judicial

En el ámbito judicial, los abogados conocen bien que las notificaciones electrónicas llegan firmadas digitalmente a través del Sistema de Notificaciones Electrónicas (SINOE). Asimismo, el Expediente Judicial Electrónico (EJE) permite que los procesos judiciales se tramiten de manera digital, garantizando la autenticidad de los documentos y reduciendo significativamente el uso de papel.

Telemedicina – Sector Salud

Otro ámbito fundamental es el de la salud, particularmente las historias clínicas electrónicas. Estas permiten que una misma historia clínica pueda ser consultada, por ejemplo, en un hospital de Iquitos, uno de Lima o uno de Piura, manteniendo un solo registro integrado. Además, la telemedicina permite que un médico ubicado en Lima atienda a un paciente que se encuentra en Iquitos, firmando digitalmente la historia clínica.

Naturalmente, esto aplica a situaciones médicas que pueden ser tratadas a distancia, ya que los casos de mayor gravedad requieren atención presencial.

Acuerdo de Reconocimiento Mutuo

El Acuerdo de Reconocimiento Mutuo es un mecanismo mediante el cual los organismos de acreditación de dos países firman un documento reconociendo recíprocamente sus sistemas de acreditación. Sin este acuerdo, por ejemplo, un documento firmado digitalmente en el Perú, aunque esté acreditado por el Indecopi, no será aceptado en Argentina y viceversa. Con un acuerdo de reconocimiento mutuo, un documento acreditado en el Perú tendría el mismo valor legal en el otro país, y lo mismo ocurriría en sentido inverso. Actualmente, este tipo de acuerdos se encuentra en proceso de trabajo.