



Reconocimiento transfronterizo de la firma electrónica: comentarios al amparo del ordenamiento jurídico peruano y los principios de la CNUDMI

Cross-border recognition of electronic signatures: comments under the Peruvian legal framework

Ana Sofía Del Solar Figuerola*
García-Godos, Lindley-Russo & Adrianzén Abogados

Resumen:

La creciente digitalización del comercio transfronterizo demanda marcos jurídicos capaces de reconocer firmas electrónicas emitidas fuera del territorio nacional. Este artículo examina los estándares desarrollados por la CNUDMI y evalúa su compatibilidad con la normativa peruana, centrando el análisis en los principios del comercio digital y en la distinción entre enfoques prescriptivos, minimalistas e híbridos. Se analizan los mecanismos de reconocimiento adoptados por el Perú, basados en PKI, así como las barreras que este modelo genera para la interoperabilidad y el uso transfronterizo de firmas electrónicas. El artículo incorpora un análisis comparado de la regulación de los principales destinos de exportación del país y revisa disposiciones sobre firma electrónica incluidas en acuerdos comerciales e iniciativas de integración regional. Todo ello a fin de identificar oportunidades de mejora que permitan aprovechar plenamente los beneficios de la digitalización, fortalecer la confianza en el comercio digital y contribuir a la competitividad del país.

Abstract:

The growing digitalization of cross-border trade requires legal frameworks capable of recognizing electronic signatures issued outside national jurisdictions. This article examines the standards developed by UNCITRAL and assesses their alignment with the Peruvian regulatory framework, with particular attention to the core principles of digital commerce and the distinction between prescriptive, minimalist, and hybrid approaches. It analyzes the recognition mechanisms adopted in Peru, which rely on PKI-based models, as well as the barriers this structure poses for interoperability and the cross-border use of electronic signatures. The article also includes a comparative review of the regulation of Peru's main export destinations and examines relevant provisions on electronic signatures found in

* Especialista en Facilitación del Comercio. Universidad de Lima. Asociada en García-Godos, Lindley-Russo & Adrianzén Abogados. Asesora a empresas nacionales e internacionales, así como a organizaciones internacionales, en las áreas de comercio internacional y facilitación del comercio, life sciences & food law, y arbitraje comercial. Ha contribuido en proyectos de consultoría para organismos multilaterales como la Cooperación Económica Asia-Pacífico - APEC, Banco de desarrollo de América Latina y el Caribe - CAF, Organización de las Naciones Unidas para el Desarrollo Industrial - Onudi y el Banco Interamericano de Desarrollo - BID, así como entidades públicas como el Ministerio de Comercio Exterior y Turismo - Mincetur. Contacto: adelsolarf@glrabogados.com

trade agreements and regional integration initiatives. Overall, the analysis aims to identify opportunities for improvement that would enable Peru to better harness the benefits of digitalization, strengthen trust in digital commerce, and enhance national competitiveness.

Palabras clave:

Firma electrónica – firma digital – PKI – reconocimiento transfronterizo – CNUDMI – comercio digital

Keywords:

Electronic signature – digital signature – PKI – cross-border recognition – UNCITRAL – digital commerce.

1. Introducción

Contar con un marco jurídico adecuado para el comercio digital¹ es esencial para aprovechar los beneficios de la digitalización y facilitar el comercio transfronterizo. Este marco debe brindar un nivel suficiente de seguridad jurídica que permita generar confianza entre los actores de comercio, incentivando así el uso de herramientas digitales.

Para lograrlo, se requiere una regulación que i) reconozca la plena validez y efectos jurídicos de los elementos propios de una transacción digital, tales como documentos, firmas y sellos electrónicos; ii) precise los requisitos que permitan equiparlos a sus versiones en papel y, al mismo tiempo, iii) no imponga mayores exigencias que las necesarias para generar confianza, de modo que no se generen costos adicionales que encarezcan la digitalización o desincentiven su uso.

En este contexto, un desafío central para el comercio digital es el tratamiento de dichos elementos generados fuera del territorio nacional, especialmente cuando intervienen múltiples jurisdicciones con marcos normativos distintos. La validez de estos elementos emitidos en el extranjero depende, en gran medida, de los mecanismos de reconocimiento jurídico que cada país adopte.

Al respecto, la Comisión Económica y Social para Asia y el Pacífico - ESCAP (2019) ha señalado que, si bien más del 60 % de los países en esta región han desarrollado, al menos parcialmente, marcos legales para respaldar las transacciones electrónicas, dichos marcos siguen siendo incompletos y pueden resultar insuficientes para reconocer datos o documentos electrónicos emitidos en otros países.

Uno de los principales elementos de una transacción es la firma. Una firma no solo permite identificar al firmante, sino también atribuirle la autoría del contenido del instrumento y exteriorizar su voluntad de obligarse conforme a dicho contenido. En el entorno digital, generar confianza en el uso de la firma electrónica resulta especialmente relevante. El usuario debe tener la seguridad de que la firma realmente identifica a quien la utiliza, que dicha persona manifiesta efectivamente su voluntad de quedar vinculada y, además, que el mensaje no ha sido alterado.

En este contexto, su uso seguirá expandiéndose en los próximos años. Así, se prevé que en los próximos 3 a 5 años el uso de firmas electrónicas en el sector B2B continúe creciendo, impulsado por un mayor nivel de seguridad, privacidad e interoperabilidad. No obstante, persisten barreras para su adopción, tales como problemas de experiencia de usuario y la falta de un reconocimiento global uniforme (*Cloud Signature Consortium*, 2025).

Estas tendencias y desafíos refuerzan la necesidad de contar con un marco legal que regule adecuadamente la validez y requisitos de equivalencia de la firma electrónica, tanto a nivel nacional como en un contexto transfronterizo.

Así, la UNCTAD (2025) ha señalado que la adopción de reglas sobre reconocimiento de la firma electrónica, tanto en la legislación nacional como en acuerdos internacionales, permite garantizar la certeza jurídica necesaria para las transacciones digitales, reduciendo costos y demoras en el comercio transfronterizo. A su vez, juega un papel clave para estandarizar a nivel global estas prácticas, fortaleciendo la confianza y la eficiencia en el comercio digital.

1 Existe una diferencia entre comercio digital y comercio electrónico. La Organización Mundial del Comercio - OMC, en línea con el Fondo Monetario Internacional - FMI, la Organización para la Cooperación y el Desarrollo Económicos - OCDE y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo - UNCTAD (2023), define el comercio digital como todo intercambio internacional que es ordenado y/o entregado digitalmente, y el segundo como la compra o venta de bienes o servicios realizada a través de redes informáticas mediante métodos específicamente diseñados para recibir o efectuar órdenes (p. 14). Si bien el presente artículo se centrará en el primero de estos conceptos, tanto la doctrina como la normativa y leyes modelos suelen emplearlos de manera indistinta, prefiriendo el término comercio electrónico. En consecuencia, al desarrollar los aportes doctrinales, como los de la CNUDMI, o al analizar la regulación nacional, puede encontrarse el uso de dicho término, aun cuando el enfoque principal sea el comercio digital.

El presente artículo examina la problemática del reconocimiento transfronterizo de las firmas electrónicas² a partir de los estándares de la CNUDMI y de las mejores prácticas internacionales, así como su correlación con el ordenamiento jurídico peruano. A partir de los enfoques regulatorios identificados y evaluados por la doctrina y los organismos internacionales, se analiza la estructura normativa nacional para identificar los mecanismos disponibles para reconocer una firma electrónica emitida en el extranjero y evaluar su efectividad práctica. Con ello, se busca identificar oportunidades de mejora que permitan maximizar los beneficios de la digitalización del comercio en el país.

2. De los principios del comercio digital a la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas

En 1966, mediante Resolución 2205 (XXI), la Asamblea General de las Naciones Unidas estableció la CNUDMI como la comisión responsable de promover la armonización y unificación progresiva del derecho mercantil internacional (CNUDMI, 2013).

Conforme al artículo 7.c) de dicha resolución, la CNUDMI cumple este mandato mediante la elaboración y promoción de nuevas convenciones, leyes modelo³ y textos legislativos uniformes, entre otras iniciativas (CNUDMI, 2013).

Al respecto, la CNUDMI ha elaborado diversas leyes modelo en materias vinculadas al comercio internacional. Entre ellas, se encuentra la Ley Modelo sobre Arbitraje Comercial Internacional (1985), la Ley Modelo sobre Insolvencia de Grupos de Empresas (2019) y la Ley Modelo sobre Transferencias Internacionales de Crédito (1992); así como aquellas sobre comercio electrónico.

2.1. Principios del comercio electrónico

La primera ley modelo vinculada al comercio electrónico fue adoptada por la CNUDMI el 12 de junio de 1996. Así, según su Guía para la incorporación al derecho interno (CNUDMI, 1999), la Ley Modelo de la CNUDMI sobre Comercio Electrónico (en adelante, LMCE) buscaba

proporcionar al legislador nacional un conjunto de reglas destinadas a eliminar los obstáculos jurídicos al uso de mensajes electrónicos, así como establecer un marco normativo que permita el desarrollo seguro del comercio electrónico y dé certeza sobre su validez legal. Ello en respuesta al incremento de las operaciones comerciales internacionales que empleaban medios electrónicos de comunicación para su negociación.

En este instrumento se establecieron por primera vez los principios que hoy rigen el comercio electrónico: el principio de no discriminación, el de equivalencia funcional y el de neutralidad tecnológica (CNUDMI, s.f.).

El primer principio establece que “no se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por el mero hecho de estar en forma de un mensaje de datos” (CNUDMI, 2025, p. 3). Esto no implica que cualquier manifestación electrónica sea automáticamente válida, pues debe cumplir con los parámetros establecidos en el siguiente principio.

El segundo principio alude a los requisitos mínimos que debe cumplir un mensaje de datos para poder equipararse a su versión en papel. Conforme a la guía citada párrafos arriba (CNUDMI, 1999), este criterio parte de analizar los objetivos y funciones del soporte físico tradicional y evaluar cómo pueden ser satisfechos mediante las técnicas propias del comercio electrónico, considerando la distinta naturaleza de estos dos medios.

Finalmente, el principio de neutralidad tecnológica señala que todo texto legislativo debe evitar imponer una tecnología específica como obligatoria, considerando que la tecnología, por naturaleza, evoluciona con mayor rapidez que la norma. En consecuencia, una ley no debe quedar vinculada a un medio tecnológico concreto, pues correría el riesgo de volverse obsoleta con el tiempo.

2.2. Principales aspectos de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas

Cinco años después de la adopción de dicha ley modelo, en 2001, esta comisión adoptó la Ley

2 Cabe precisar que se emplea el término “firma electrónica” al referirse a aquella emitida en el extranjero, en lugar de “firma digital”, a fin de diferenciarla de la “firma digital” definida por el marco legal peruano, vinculada a una PKI, conforme se desarrollará en el artículo. Ello permitirá distinguirla de las firmas electrónicas sustentadas en certificados extranjeros, los cuales no necesariamente se encuentran basados en dicha infraestructura, atendiendo a los diversos estándares regulatorios existentes a nivel internacional.

3 Según la CNUDMI (2013), “[u]na ley modelo es un texto legislativo que se recomienda a los Estados para su adopción e incorporación a su derecho interno” (p. 16). Si bien la CNUDMI alienta a los Estados a adoptar estos instrumentos, su incorporación no es obligatoria, ni exige una transposición literal de su contenido. Los Estados pueden ajustarla a sus necesidades, sin perjuicio de que se recomienda que las modificaciones sean mínimas a fin de preservar el objetivo de armonización normativa (CNUDMI, 2013). De este modo, la ley modelo se concibe como un instrumento más flexible que las convenciones internacionales, diseñado para facilitar la negociación y promover una mayor tasa de adopción entre los Estados (CNUDMI, 2013).

4 Según la última definición de “mensajes de datos”, planteada por la Ley Modelo de la CNUDMI sobre Contratación Automatizada, es toda “información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares” (CNUDMI, 2024)

Modelo de la CNUDMI sobre las Firmas Electrónicas (en adelante, LMFE)⁵. Con este instrumento, la comisión buscó reducir la incertidumbre respecto a las consecuencias jurídicas del uso cada vez más frecuente de técnicas de autenticación electrónicas en sustitución de la firma manuscrita, así como crear un marco normativo de referencia que permita uniformizar criterios entre los Estados, evitando la proliferación de reglas divergentes a nivel internacional (CNUDMI, 2002).

Tomando como referencia los principios del comercio electrónico, la LMFE establece lo siguiente. En relación con el principio de no discriminación, su artículo 6 equipara las firmas electrónicas⁶ a las firmas manuscritas, siempre que cumplan los requisitos de equivalencia funcional.

Sobre los requisitos de equivalencia funcional, el mismo artículo indica que la firma electrónica debe i) ser fiable y ii) resultar apropiada para los fines con los cuales se generó o comunicó el mensaje. Asimismo, establece los criterios para considerar una firma como fiable, los cuales se relacionan con la identificación del firmante en relación con los datos, el control exclusivo que éste ejerce sobre ellos, la capacidad para detectar alteraciones posteriores y la integridad de los datos.

Con relación al reconocimiento transfronterizo, dichos principios se materializan en el artículo 12 de la LMFE, el cual dispone que, para determinar los efectos jurídicos de una firma o certificado electrónico, no debe considerarse el lugar donde estos hayan sido emitidos, creados o utilizados, ni el lugar en el que se encuentre el establecimiento del firmante o del expedidor. Así, establece que no se le pueden negar los mismos efectos jurídicos a un certificado o firma electrónica extranjera si cumple con requisitos de fiabilidad equivalentes a los exigidos para los nacionales.

Por último, en línea con lo indicado por su guía explicativa (CNUDMI, 2002), la ley modelo “refleja” el principio de neutralidad tecnológica, al no discriminar alguna técnica de comunicación o archivo electrónico de información.

3. Marco jurídico peruano sobre firmas electrónicas

3.1. Marco jurídico general del comercio electrónico en el Perú

Si bien el Perú no cuenta con una regulación específica sobre comercio electrónico, sí dispone de un conjunto de normas que habilitan las transacciones realizadas mediante medios electrónicos. Dentro de este marco habilitante se encuentra la regulación que confiere validez jurídica a las firmas electrónicas.

En general, dicho marco está compuesto tanto por la Ley de Firmas Electrónicas como por su reglamento, así como por la modificación al Código Civil sobre formas de manifestación de la voluntad.

3.2. Ley de Firmas y Certificados Digitales

A inicios de este siglo, se publicó la Ley 27269, Ley de Firmas y Certificados Digitales, cuyo objetivo fue otorgar mayor seguridad jurídica a los actos realizados mediante medios informáticos, en respuesta al problema identificado sobre el uso indebido de los sistemas informáticos (Congreso de la República, 1999).

Esta norma representó un primer avance hacia el reconocimiento de la equivalencia jurídica de ciertos actos (i.e. acreditación de la identidad) realizados por medios digitales, avance que posteriormente fue acogido tanto en el Código Civil como en la Ley de Títulos Valores, entre otras disposiciones.

A su vez, conforme lo informado a la Secretaría de la CNUDMI, esta legislación se ha inspirado en la LMFE y sus principios (CNUDMI, s.f.)⁷. En este sentido, ahora cabe analizar los apartados de la ley bajo la óptica de este instrumento a fin de analizar su grado de compatibilidad.

Primero, el artículo 1 de la Ley 27269 acoge el principio de no discriminación, al establecer que la firma electrónica goza de la misma validez y eficacia jurídica que una manuscrita.

5 Esta ley modelo podría haberse aplicado como una versión ampliada del artículo 7 de la LMCE; sin embargo, la Comisión optó por presentarla como un instrumento independiente para evitar confusiones. Ello dado que, durante la última fase de elaboración de la LMFE, la Ley Modelo sobre Comercio Electrónico ya se encontraba en aplicación en determinados países, mientras que otros estaban evaluando su adopción (CNUDMI, 2002, págs. 36-37).

6 La LMFE define a la firma electrónica como aquellos datos electrónicos consignados, adjuntados o lógicamente asociados a un mensaje de datos que “puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos” (CNUDMI, 2002, p. 1).

7 A la fecha, el Perú no ha adoptado ni tomado como referencia las demás leyes modelo de la CNUDMI vinculadas a el comercio electrónico. Así, no ha adoptado la LMCE (CNUDMI, s.f.) ni la relacionada a los documentos transmisibles electrónicos (CNUDMI, s.f.). A su vez, según las Notas de Secretaría A/CN.9/1207 de 2025 (CNUDMI, 2025), A/CN.9/1172/Rev.1 de 2024 (CNUDMI, 2024), y A/CN.9/1136 de 2023 (CNUDMI, 2023), no se ha notificado ningún acto vinculado a las leyes modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza o sobre la contratación automatizada.

Asimismo, su artículo 11 (modificado por la Ley 27310) confiere a los certificados⁸ de firmas digitales emitidos por entidades extranjeras la misma validez y eficacia que los nacionales si son reconocidos por la autoridad competente; esto es, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Aunque el marco legal establece un mecanismo por el cual se pueden reconocer las firmas electrónicas emitidas en el extranjero, como se desarrollará en el presente artículo, existen problemas en su aplicación.

Segundo, en lo que respecta al principio de equivalencia funcional, si bien su artículo 1 indica que la firma electrónica debe cumplir total o parcialmente las funciones de una manuscrita, y su artículo 2 expresa que es aquella capaz de i) vincular e identificar al firmante y ii) garantizar la autenticación e integridad del documento electrónico, no presenta mayor desarrollo.

Finalmente, respecto al principio de neutralidad tecnológica, en principio se ampara en la definición de firma electrónica contenida en su artículo 1. Así, indica que esta alude a "cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita".

3.3. Manifestación de la voluntad por medios electrónicos y firma electrónica en el Código Civil

Casi un mes después de la publicación de la Ley 27269, se publicó la Ley 27291 que modificó los artículos 141 y 1374 del Código Civil a fin de habilitar el uso de medios electrónicos para manifestar la voluntad, así como la acreditación de la misma mediante una firma electrónica, conforme lo siguiente:

Artículo 141.- Manifestación de voluntad

La manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, **a través de cualquier medio** directo, manual, **mecánico, electrónico u otro análogo** [...] [Énfasis agregado].⁹ Asimismo, el numeral A de

este artículo reconoce que, cuando la ley establezca que la manifestación de voluntad debe realizarse mediante una formalidad específica o requiera una firma electrónica, esta puede generarse o comunicarse a través de medios electrónicos, ópticos o cualquier otro análogo.

Según su exposición de motivos (Congreso de la República, 2000), dicha modificación responde a los avances tecnológicos que han generado nuevos medios de comunicación por los cuales se puede manifestar la voluntad.

3.4. Reglamento de la Ley de Firmas y Certificados Digitales

El actual reglamento de la Ley 27269 fue aprobado en el 2008 mediante Decreto Supremo 052-2008-PCM (en adelante, el Reglamento). El artículo 1-A de esta norma distingue los tres tipos de firma electrónica: simple, avanzada y digital (también denominada cualificada), estableciendo que la única que es funcionalmente equivalente a la manuscrita es esta última:

Artículo 3.- De la validez y eficacia de la firma digital

La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica [...].Ello no implica que las firmas electrónicas, tanto simple como avanzada, no tengan efectos jurídicos, sino que se ha otorgado un grado de reconocimiento y presunción legal menor que el de la firma digital. Así, según los artículos 2 y 2.A del Reglamento, i) solo son válidas en consideración a los pactos o convenios que acuerden las partes ii) y, en caso de controversia, la carga de la prueba recae en quien la invoca como auténtica.

En consecuencia, estas firmas no gozan de las presunciones legales otorgadas a la firma digital, tales como la presunción de no repudio¹⁰ prevista en el artículo 8 del Reglamento. Adicionalmente, los artículos 42 y 43 del Reglamento establecen que únicamente se consideran seguros los procedimientos entre la administración pública y el administrado, o entre entidades públicas, cuando

8 Conforme al glosario del Reglamento, el certificado digital es el documento credencial electrónico generado y firmado digitalmente por la entidad de certificación, que vincula un par de claves con el titular y confirma su identidad. En otras palabras, el certificado es el instrumento que permite verificar la identidad de quien firma.

9 Ello sin perjuicio de la modificación introducida en 2008 mediante el Decreto Legislativo 1384, que reconoce y regula la capacidad jurídica de las personas con discapacidad en igualdad de condiciones. Dicha norma incorporó el término "digital" entre los medios de manifestación de voluntad, quedando la redacción actual como: "a través de cualquier medio directo, manual, mecánico, digital, electrónico, mediante la lengua de señas o algún medio alternativo de comunicación".

10 Conforme al glosario del Reglamento, el no repudio alude a la imposibilidad de una persona de desdecirse de sus actos cuando ha expresado su voluntad en un documento firmado, ya sea mediante firma manuscrita o firma digital. En el caso de la firma digital, este principio se refiere a la vinculación del firmante con el documento electrónico, de manera que no pueda negar su intervención ni alegar modificaciones o falsificaciones posteriores del documento.

se emplea firma digital. Del mismo modo, las entidades públicas solo están obligadas a aceptar documentos suscritos con este tipo de firma.

En este contexto, el Reglamento define a la firma electrónica simple como aquella que cumple con los mínimos requisitos para ser considerada como tal. Es decir, es un dato electrónico anexo o asociado de forma lógica con otros datos que un firmante utiliza para firmar.

Por su parte, establece que la firma electrónica avanzada es una forma de firma electrónica simple

que, además de identificar al firmante, cumple requisitos adicionales de seguridad y autenticidad. En cambio, indica que la firma electrónica cualificada o digital constituye una modalidad de firma electrónica avanzada que incorpora estándares adicionales.

A continuación, se analizarán las semejanzas y diferencias entre ambas figuras para determinar los criterios que permiten que la firma digital goce de pleno reconocimiento jurídico, en comparación con la firma electrónica avanzada.

Tabla 1. Comparación de las características de la firma electrónica avanzada y digital establecidas por el Reglamento

	Firma electrónica avanzada	Firma digital
Vinculación	Está vinculada al firmante de manera única. (Artículo 1-A del Reglamento)	Está vinculada únicamente al signatario y a los datos a los que refiere. (Artículo 6 del Reglamento) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste. (Artículo 7 del Reglamento)
Identificación	Permite la identificación del firmante. (Artículo 1-A del Reglamento)	Permite la identificación del signatario. (Artículo 6 del Reglamento)
Control	Ha sido creada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control. (Artículo 1-A del Reglamento)	Ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza . (Artículo 6 del Reglamento) Su generación está bajo el control exclusivo del suscriptor. (Artículo 7 del Reglamento)
Integridad	Está vinculada con los datos firmados de modo tal que cualquier modificación posterior de los mismos es detectable. (Artículo 1-A del Reglamento)	Está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. (Artículo 6 del Reglamento) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado. (Artículo 7 del Reglamento)
Tecnología	-	Usa una técnica de criptografía asimétrica (Artículo 6 del Reglamento) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado (Artículo 7 del Reglamento) Es susceptible de ser verificada usando la clave pública del suscriptor. (Artículo 7 del Reglamento)

	Firma electrónica avanzada	Firma digital
Entidad acre- ditada	-	Ha sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica - IOFE. (Artículo 6 del Reglamento)
Vicios de voluntad	No se excluye el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública. (Artículo 3 del Reglamento)	No se excluye el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública. (Artículo 3 del Reglamento) No medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil (Artículo 6 del Reglamento)

Fuente: Elaboración propia.

Como se puede apreciar, las diferencias entre la firma digital y la firma electrónica avanzada se sustentan en tres criterios:

- i) La firma digital debe garantizar con un “elevado grado de confianza” el control que posee el firmante sobre la creación de la firma.
- ii) La firma digital debe ser creada utilizando técnicas de criptografía asimétrica.
- iii) La firma digital debe ser creada por una entidad acreditada dentro del marco de la IOFE.

Al respecto, conforme al artículo 8 del Reglamento, se presume que, cuando un documento electrónico es firmado mediante firma digital, el firmante mantiene el control de la clave privada asociada con un elevado grado de confianza. En otras palabras, el propio carácter de firma digital garantiza que se ejerce el control con un “elevado grado de confianza”.

En consecuencia, la firma digital se diferencia de la firma electrónica por el solo hecho de: i) haber sido creada con una tecnología específica, y ii) estar acreditada por la autoridad competente, siendo para estos efectos el INDECOPI.

3.5. Decreto Supremo 026-2016-PCM, que aprobó medidas para el fortalecimiento de la IOFE y la implementación progresiva de la firma digital en el Sector Público y Privado

Mediante los Decretos Supremos 070-2011-PCM y 105-2012-PCM se autorizó, excepcionalmente, que entidades de certificación no acreditadas pudieran

emitir certificados digitales. Si bien ambas normas están dirigidas al ámbito de la Administración Pública, la segunda permitió a personas naturales y jurídicas del sector privado usar certificados digitales de proveedores no acreditados que cuenten con certificación internacional *WebTrust*, hasta que el INDECOPI acredite o reconozca al menos a una entidad de certificación (privada, para el caso de personas jurídicas).

Esta situación excepcional se buscó remediar a través del Decreto Supremo 026-2016-PCM. Conforme su exposición de motivos (Gobierno del Perú, 2016), se buscó que dichas entidades de certificación autorizadas por los Decretos Supremos 070-2011-PCM y 105-2012-PCM vuelvan progresivamente a la regla establecida por la ley y su reglamento, mediante su acreditación o reconocimiento por parte del INDECOPI.

Así, esta norma estableció que se reconocerán las entidades de certificación que cumplan con determinados estándares técnicos o sellos de confianza internacionales¹¹ hasta que una empresa privada se acredite o se reconozca como entidad de certificación ante el INDECOPI. Estas entidades debían comunicar sus operaciones en el país para su incorporación en el Registro Oficial de Prestadores de Servicios de Certificación Digital - ROPS.

Luego que se acredite o reconozca una entidad privada, las demás entidades que se incorporaron en el ROPS debían iniciar el procedimiento de acreditación o de reconocimiento en un plazo máximo de un año. De lo contrario, se les retiraría del registro. Cabe indicar que, a la fecha, dicho plazo ya ha culminado y, en consecuencia, actualmente

11 Tales como ISO 21188, ETSI TS 101 456, ETSI TS 102 042 u otros con las mismas características, o que cuenten con el sello de confianza *Webtrust for Certification Authorities* vigente, obtenidos luego de haber sido auditados por un Auditor *Webtrust* autorizado

solo se consideran acreditadas las entidades que figuran en el ROPS publicado por el INDECOPI¹².

Asimismo, se facultó a las entidades públicas a permitir —cuando lo consideren apropiado y según una evaluación de riesgos basada en la naturaleza de cada trámite, proceso o procedimiento administrativo— el uso de mecanismos de firma distintos a la firma digital.

4. Limitaciones del enfoque prescriptivo

4.1. Definiciones

Conforme lo indicado en la sección anterior, nuestro marco jurídico ofrece un mayor nivel de reconocimiento jurídico a la firma digital, la cual se diferencia de la avanzada por: i) utilizar una técnica de criptografía asimétrica y ii) ser emitida por una entidad acreditada por el INDECOPI. La interrelación de ambos puntos configura la infraestructura de clave pública (PKI). En este punto, cabe definir ambos términos.

Primero, el glosario del Reglamento define a la criptografía asimétrica como aquella rama de las matemáticas aplicadas basada en el empleo de funciones algorítmicas para generar dos claves (una privada y una pública) diferentes, pero matemáticamente relacionadas entre sí. La clave privada es utilizada por el firmante para crear la firma, mientras que la pública se utiliza para verificarla. Si bien están vinculadas, no se puede acceder a la clave privada a través de la clave pública.

Por otro lado, según Albarqi *et al.* (2015), la PKI fue desarrollada como un soporte a la criptografía asimétrica, a fin de solucionar el problema vinculado a la verificación de la identidad del titular de una clave pública. Así, está compuesta por diversos elementos, entre ellos los certificados digitales, las autoridades de registro y las entidades certificadoras.

4.2. Enfoques regulatorios de firma electrónica

A nivel internacional, existen tres enfoques de regulación de firma electrónica: prescriptivo, minimalista e híbrido.

Así, según la ESCAP y la CNUDMI (2022), para determinar su validez, el marco legal puede:

- Exigir el uso de una tecnología específica para la creación de la firma, usualmente requiriendo además que esté certificada por una entidad acreditada. Este enfoque se justifica en la necesidad de garantizar la fiabilidad o la seguridad en la ejecución de las funciones de la firma. En esta línea, la validez puede

condicionarse a que la firma se emita dentro de una infraestructura PKI (**Enfoque prescriptivo**).

- Ser tecnológicamente neutral y reconocer todo tipo de firma electrónica, pudiendo establecer excepciones para ciertos documentos o transacciones específicas (**Enfoque minimalista o tecnológicamente neutral**).
- Adoptar un enfoque híbrido, en el que se reconocen todos los mecanismos de autenticación que cumplan los requisitos de equivalencia funcional, pero se otorga un estatus jurídico reforzado, tales como presunciones de origen e integridad, a aquellos que cumplen niveles superiores de seguridad (como las firmas digitales) (**Enfoque híbrido o de doble nivel “two-tier approach”**).

Al respecto, conforme lo indicado por Tasneem (2014), los defensores del enfoque prescriptivo sostienen que otorgarles un trato preferente promueve la estandarización tecnológica, impulsa la innovación (al permitir que la legislación se adapte rápidamente una vez que exista certeza sobre la tecnología) y proporciona mayor seguridad jurídica.

No obstante, continúa la autora, este enfoque es criticado porque solo sería viable si todos los gobiernos adoptaran exclusivamente este tipo de firma. Si los Estados aplican enfoques regulatorios diferentes para distintas tecnologías, no se facilitarían las transacciones transfronterizas, precisamente uno de los beneficios esperados. A su vez, puede interferir con la evolución natural del mercado al excluir el desarrollo de tecnologías alternativas que podrían superar a las firmas digitales (Tasneem, 2014).

Respecto al enfoque minimalista, la postura es que debe ser el mercado quien determine qué tecnologías deben usarse, pues una regulación excesiva podría limitar su desarrollo natural. En contraste, sus críticos advierten que puede afectar la protección del consumidor, ya que las firmas electrónicas simples suelen ser menos seguras que las firmas digitales e incluso pueden ofrecer menores garantías que las firmas manuscritas (Tasneem, 2014).

Finalmente, la autora indica que se favorece el enfoque híbrido por su flexibilidad, pues combina neutralidad tecnológica (al reconocer todo tipo de firma electrónica) con seguridad jurídica (al otorgar mayores beneficios legales a tecnologías que brindan mayor nivel de confianza). Sin embargo, también recibe críticas, pues se argumenta que no ofrece suficiente flexibilidad para el desarrollo del

12 Se puede acceder al ROPS a través del siguiente enlace: <https://www.gob.pe/institucion/indecopi/informes-publicaciones/5447866-registro-oficial-de-prestadores-de-servicios-de-certificacion-digital-rops>

mercado y puede limitar la innovación tecnológica al favorecer determinadas tecnologías sobre otras (Tasneem, 2014).

Con respecto a la CNUDMI, si bien esta comisión reconoce que el enfoque minimalista facilita el uso transfronterizo de la firma electrónica, al permitir cualquier método de firma siempre que su fiabilidad sea adecuada a la finalidad perseguida, dicho enfoque implica que las condiciones de fiabilidad solo se confirman a posteriori, sin garantías de que el tribunal acepte el método utilizado (CNUDMI, 2009).

Por otro lado, establece que el uso transfronterizo “de la autenticación y las firmas electrónicas se convierte en un verdadero problema en los sistemas que prescriben imperativamente o dan preferencia a una tecnología determinada” (CNUDMI, 2009, p. 70).

A su vez, establece que su complejidad aumenta directamente proporcional al grado de regulación y al grado de seguridad jurídica que la ley concede a un determinado método o tecnología. Si la legislación se limita a establecer la equivalencia general de las firmas electrónicas a las manuscritas, los riesgos serían similares entre ambas formas. Pero, si la ley reconoce más presunciones legales a ciertas firmas, todo método diferente puede considerarse, por defecto, poco fiable (CNUDMI, 2009).

Así, una regulación dependiente de una tecnología puede terminar obstaculizando, en lugar de fomentando, el uso de firmas electrónicas en el comercio internacional (CNUDMI, 2009).

Ello debido a que: i) cuando los ordenamientos imponen requisitos técnicos y jurídicos contradictorios, el uso de firmas electrónicas en operaciones transfronterizas se vuelve difícil o incluso imposible; y ii) una legislación excesivamente orientada a una tecnología específica —en especial aquella que privilegia las firmas digitales— genera un conjunto disperso y contradictorio de normas y autorizaciones que obstaculiza la interoperabilidad y el reconocimiento transfronterizo (CNUDMI, 2009).

4.3. Barreras del enfoque prescriptivo

Como señala el Comité de Comercio e Inversión del APEC (2025), muchos documentos de comercio exterior se firman con firmas electrónicas simples. Este comité continúa indicando que algunas economías han modificado el principio básico de equivalencia funcional contemplado tanto en la LMFE como en anteriores instrumentos como la LMCE y Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (en adelante, la Convención), al aceptar solo métodos basados en criptografía asimétrica de clave pública.

En esta línea, indica que este enfoque resulta restrictivo, ya que no es el método usado por varios actores del comercio internacional. Por ello, promueve la armonización y estandarización a nivel internacional de la legislación que establece los criterios de equivalencia funcional sobre firma electrónica, entre otros aspectos, para proporcionar certeza jurídica y uniformidad a las partes (APEC, 2025).

De forma similar, en un informe del Banco Mundial, se señala que el uso de este enfoque prescriptivo resulta innecesario y oneroso para muchas actividades, especialmente en los contratos entre particulares. A su vez, indica que exigir el uso exclusivo de firmas digitales genera más inconvenientes que beneficios, ya que implica recurrir a autoridades de certificación y asumir el pago de los certificados respectivos (Daza Jaller, Gaillard, & Molinuevo, 2020).

Por su parte, un informe de la ESCAP (Gregory, 2024) señala que exigir como criterio de equivalencia funcional, que la firma electrónica sea creada dentro de la PKI no solo puede resultar oneroso, sino que también puede ser difícil de cumplir para entidades proveedoras extranjeras. En este sentido, indica que este tipo de requisitos pueden constituir una barrera a la creación de métodos innovadores de autenticación, como las firmas electrónicas basadas en *blockchain*.

No obstante, el autor reconoce que la tendencia internacional ha sido abandonar este criterio en las transacciones B2B, reservándolo principalmente para las comunicaciones con entidades públicas.

Asimismo, el mismo autor señala que, en ciertos casos y para fines específicos, la ley puede exigir el uso de una tecnología determinada para garantizar mayor seguridad o fiabilidad. Sin embargo, advierte que no puede ser más específica de lo necesario, ya que puede generar mayores costos, rigidez y posibles inconsistencias con los métodos utilizados por los otros actores. A su vez, sostiene que esta especificación limita los tipos de mensajes de datos que pueden emplearse y constituye una barrera para su reconocimiento transfronterizo.

Como se desarrolló en la sección anterior, el enfoque prescriptivo se justifica en el mayor nivel de seguridad que otorga la PKI. Sin embargo, conforme Kim (2019), esta premisa: (i) es limitada frente al rápido avance tecnológico y (ii) no necesariamente es cierta. Ello se debe a que la PKI no garantiza plenamente la identidad del firmante, sino únicamente la posesión de un par de claves, lo que expone a los usuarios a riesgos si no cuentan con la capacidad técnica para mantenerlas seguras. Las claves pueden ser robadas o imitadas, y las autoridades de certificación también pueden ser vulneradas, emitiendo certificados erróneos.

Asimismo, exigir el uso exclusivo de firmas digitales no refleja las prácticas reales del mercado, donde su adopción continúa siendo baja debido a la complejidad técnica, los problemas de usabilidad y los elevados costos asociados al mantenimiento de la PKI y a la capacitación necesaria para su operatividad (Kim, 2019).

Por su parte, la LMFE promueve un enfoque híbrido. Su artículo 3 establece que ninguna disposición de la ley —salvo aquellas que permiten a las partes pactar excepciones o modificar efectos— puede aplicarse de manera que excluya, restrinja o prive de efectos jurídicos a cualquier método de firma electrónica que sea fiable y apropiado para el fin con el que fue generado.

Sin embargo, su artículo 7 permite que el Estado determine qué técnicas cumplen con dichos requisitos, siempre que ello se base en normas o criterios internacionales reconocidos.

La CNUDMI aclara que la facultad contenida en este artículo busca informar a los Estados que se puede otorgar certeza y previsibilidad al identificar técnicas que ofrecen altos niveles de fiabilidad y seguridad, permitiendo su evaluación y eventual reconocimiento. No obstante, también precisa que no debe interpretarse que este artículo prescribe efectos jurídicos imperativos para ciertos tipos de técnicas de firma o que limite el uso de otras tecnologías que también puedan ser fiables (2002).

A su vez, indica que es posible que las cuestiones de la PKI no se presten fácilmente a la armonización a nivel internacional (CNUDMI, 2002).

Por su parte, según Castellani (s.f.), si bien la aplicación de la PKI ofrece ventajas tales como un alto nivel de seguridad, así como velocidad, también presenta desventajas. Entre ellas, cita a los costos asociados, la participación de un tercero, su limitada disponibilidad en ciertos entornos —como dispositivos móviles— y, en algunos casos, niveles de seguridad que no son los esperados.

En este marco, está claro que la tendencia internacional es disuadir el acogimiento del enfoque prescriptivo en la regulación de firma electrónica, favoreciendo los enfoques minimalistas o híbridos.

Así, la adopción de este enfoque prescriptivo principalmente sustentado en el uso de la PKI genera los siguientes problemas:

- Constituye una barrera para el reconocimiento transfronterizo de la firma electrónica.
- Dificulta la armonización de la regulación a nivel internacional.
- Implica mayores costos de implementación y mantenimiento.
- Puede no funcionar en ciertos entornos, tales como en dispositivos móviles.
- Desincentiva la adopción de mecanismos tecnológicos más innovadores y que puedan presentar un mayor nivel de protección.

Si bien puede justificarse la imposición de determinadas técnicas o el otorgamiento de determinadas presunciones legales a favor de estas (como trasladar la carga de la prueba), con la finalidad de brindar un mayor nivel de seguridad a ciertas operaciones (tales como aquellas vinculadas al uso del DNI o al voto electrónico, también regulados por el Reglamento), su aplicación resulta menos razonable cuando se trata de operaciones entre privados dentro del ámbito comercial.

En el caso peruano, estudios como del Banco Mundial (Daza Jaller, Gaillard, & Molinuevo, 2020) y Kim (2019) han clasificado el marco legal nacional dentro del enfoque prescriptivo.

Si bien esta clasificación puede ser discutible, dado que el artículo 141 del Código Civil habilita expresamente el uso de medios electrónicos para la manifestación de la voluntad y el empleo de firmas electrónicas, y que el Reglamento reconoce la validez de las firmas electrónicas simples y avanzadas según los pactos o convenios de las partes, determinar si ello implica la adopción de un modelo híbrido —o si, por el contrario, la redacción del reglamento sugiere que solo la firma digital tiene plena validez y efectos jurídicos— no forma parte del presente análisis. No obstante, cabe señalar que existen posiciones contrarias a la conclusión de dichos estudios¹³.

Lo cierto es que la posibilidad de reconocer un certificado extranjero está, en general, condicionada a que dicho certificado haya sido emitido dentro de la PKI y, en consecuencia, corresponda a una firma digital. Ello en vista de que la IOFE opera exclusivamente con firmas digitales emitidas sobre la base de criptografía asimétrica por entidades acreditadas o reconocidas por el INDECOPI, conforme se desarrollará a continuación.

13 Al respecto, según la Exposición de Motivos del Decreto Supremo 026-2016-PCM (Gobierno del Perú, 2016), el Perú ha adoptado el enfoque de doble nivel. Asimismo, Espinoza (2017) señala que la Ley 27269 formuló una definición de firma electrónica con una redacción neutral, indicando que “la tecnología utilizada puede ser de cualquier tipo, lo importante es dar cumplimiento a los mínimos tecnológicos que exige la norma”. A su vez, según el Castilla (2025), “cualquier firma electrónica puede tener efecto legal ... en la medida en que usted demuestre con evidencias el vínculo entre la firma y el presunto firmante”.

5. Alcances y restricciones para el uso de firmas electrónicas extranjeras

5.1. Mecanismos de reconocimiento de firmas extranjeras en el Perú

Para que un certificado de firma digital emitido en el extranjero tenga la misma validez y eficacia jurídica reconocida en la Ley 27269, su artículo 11 exige que este sea reconocido por el INDECOPI¹⁴.

En este contexto, el Reglamento establece los siguientes mecanismos para poder reconocer un certificado extranjero, en línea con los artículos 6, 59, 71, 72 y 73:

- **Acreditación como entidad de certificación dentro de la IOFE.** Una empresa no domiciliada puede solicitar su acreditación como entidad de certificación ante el INDECOPI. Sin embargo, debe acreditar un establecimiento o domicilio en el territorio nacional.
- **Certificación cruzada.** Acto por el cual una entidad de certificación acreditada en el Perú reconoce la validez de un certificado emitido por otra, ya sea nacional o extranjera, previa autorización del INDECOPI, asumiendo la responsabilidad de tal certificado como si fuera suyo dentro de la IOFE.
- **Reconocimiento mutuo.** Parte de los acuerdos celebrados entre el INDECOPI con entidades extranjeras que cumplan funciones similares para reconocer la validez de los certificados extranjeros y extender la interoperabilidad de la IOFE. Este acuerdo debe garantizar en forma equivalente las funciones exigidas por la Ley 27269 y su reglamento.
- **Incorporación de entidades de certificación extranjeras por reconocimiento¹⁵.** El INDECOPI reconoce directamente los certificados emitidos por entidades de certificación extranjeras, conforme a las prácticas y políticas que apruebe por dicho efecto. A su vez, puede autorizar que entidades de certificación nacionales usen servicios de entidades extranjeras, asumiendo la responsabilidad correspondiente.

Estos cuatro enfoques se sustentan en la PKI. Toda acreditación ante el INDECOPI opera bajo

el modelo de firma digital y tiene como finalidad permitir la incorporación del prestador a la IOFE. Del mismo modo, los mecanismos de reconocimiento —certificación cruzada, reconocimiento mutuo e incorporación por reconocimiento— también funcionan dentro de la IOFE.

En otras palabras, para que una firma electrónica extranjera sea equiparable a la firma manuscrita, goce de las presunciones de no repudio y demás otorgadas por la ley y reglamento y, subsecuentemente, tenga un mayor nivel de seguridad jurídica, necesariamente debe ser una firma digital. Además, para que sus certificados emitidos en el extranjero puedan ser aceptados en el Perú, estos deben encontrarse dentro del marco de la IOFE, de modo que puedan ser reconocidos mediante los mecanismos previstos en la normativa peruana.

Como veremos en el siguiente apartado, y en línea con lo señalado por el Secretario Técnico de la Comisión para la Gestión de la IOFE, las firmas digitales generadas fuera del territorio peruano no tienen equivalencia funcional con la firma manuscrita (Castilla del Carpio, 2025).

5.2. Estado actual en el Perú

Corresponde ahora analizar qué entidades extranjeras se encuentran acreditadas o reconocidas en el Perú, a fin de determinar qué certificados pueden ser considerados válidos conforme a cada uno de los mecanismos previstos por el Reglamento.

- **Acuerdos de certificación cruzada y de reconocimiento mutuo.**

Conforme a la Carta 004163-2025-OAF/INDECOPI, a octubre 2025, el número de entidades de certificación extranjeras incorporadas bajo acuerdos de certificación cruzada, o de reconocimiento mutuo es cero.

- **Incorporación de entidades de certificación extranjeras por reconocimiento**

En línea con el Informe 000046-2025-DGI/INDECOPI, a septiembre 2025, “ninguna entidad extranjera¹⁶ de certificación digital ha solicitado formalmente el reconocimiento de la autoridad

14 Inicialmente, la norma condicionaba la validación de certificados extranjeros al reconocimiento previo por parte de una entidad de certificación nacional, quien debía garantizar su cumplimiento legal y vigencia en igualdad de condiciones con los certificados nacionales. Esta disposición fue modificada un mes después por la Ley 27310, que trasladó la función al INDECOPI. Según su exposición de motivos (Congreso de la República, 2000), la redacción inicial impedía a los usuarios el acceso a certificados extranjeros con un respaldo financiero y tecnológico reconocido internacionalmente, limitando también su libertad de elección en términos de calidad y costo. A su vez, advertía que, al depender la validación de esta entidad, esta no le interesaría reconocer certificados extranjeros al ser su competencia directa, ejerciendo un poder de mercado innecesario y generando desigualdad frente a la inversión extranjera y que la redacción final de la norma no reflejaba la intención debatida en el Pleno.

15 Mediante la Resolución de la Comisión de Reglamentos Técnicos y Comerciales 0103-2003-CRT-INDECOPI, se aprobaron disposiciones complementarias al Reglamento. Conforme a su novena disposición, el reconocimiento de certificaciones emitidas por entidades extranjeras exige su acreditación previa a través de una empresa que represente sus servicios en el país. No obstante, dichas disposiciones estaban vinculadas al reglamento anterior, aprobado por Decreto Supremo 019-2002-JUS.

16 Entendida como entidades cuya personería jurídica les ha sido conferida por el ordenamiento jurídico de un país extranjero.

administrativa de la Infraestructura Oficial de Firma Electrónica”.

En dicho informe, el INDECOPI señala que la demanda nacional de certificados aún no es elevada, por lo que las entidades acreditadas cubren adecuadamente la oferta existente. En esa línea, si el número de estas entidades fuese menor, existiría un mayor incentivo para que las entidades extranjeras soliciten su reconocimiento.

Al respecto, según el ROPS, a noviembre 2025, existen 16 entidades de certificación acreditadas, 3 de ellas entidades públicas y 13 privadas (INDECOPI, 2025).

- **Acreditación como entidad de certificación dentro de la IOFE.**

En el mismo informe, el INDECOPI precisó que algunas de las entidades acreditadas pertenecían a grupos económicos de origen extranjero, incluso pudiendo ser filiales de casas matrices extranjeras inscritas y domiciliadas en España, Chile y Brasil. No obstante, esas casas matrices no han solicitado su reconocimiento.

En este contexto, a la fecha, no se reconoce ningún certificado emitido por una entidad prestadora de servicios extranjera.

Ello sin perjuicio de que existen determinados supuestos dentro del marco normativo nacional que reconocen la validez de la firma electrónica en determinados sectores específicos.

Un ejemplo en el ámbito del comercio es que, tanto la Primera Disposición Complementaria Final del Decreto Legislativo 1147, que regula el fortalecimiento de las Fuerzas Armadas en las competencias de la Autoridad Marítima Nacional —Dirección General de Capitanías y Guardacostas (DICAPI)—, así como la Décimo Primera Disposición Transitoria y Final de la Ley del Sistema Portuario Nacional, Ley 27943, establecen que todo acto jurídico, administrativo o contractual exigido o derivado de dicha norma, su reglamento o normas complementarias puede realizarse por medios electrónicos.

En consecuencia, establece que los mensajes electrónicos de datos, los documentos electrónicos y la firma electrónica tienen plena validez dentro del ámbito de competencia de la DICAPI y del sistema portuario.

No obstante, cabe indicar que el artículo 139 del Reglamento de la Ley 27943, aprobado por Decreto Supremo 003-2004-MTC, indica que los usuarios portuarios podrán usar la firma digital o electrónica

en los actos administrativos ante la autoridad portuaria, siendo que esta firma debe estar registrada y cumplir con las normas de la Ley 27269.

Por su parte, el Decreto Supremo 005-2021-RE reguló el procedimiento de legalización de documentos extranjeros. Conforme a sus considerandos, la legalización elimina la incertidumbre jurídica respecto de los documentos emitidos por autoridades extranjeras y certificados por autoridades consulares peruanas o extranjeras en el Perú, otorgándoles valor legal probatorio.

En este sentido, su artículo 3 faculta al Ministerio de Relaciones Exteriores a utilizar el servicio de validación de firma digital para automatizar la verificación de la cadena de certificaciones de documentos públicos firmados digitalmente, en el marco de la IOFE u otros reconocidos por la Autoridad Administrativa. Al respecto, para legalizar el documento digital emitido en el extranjero, el funcionario público que lo firmó debe estar registrado ante dicho ministerio.

Como se advierte, si bien nuestra regulación reconoce el uso válido de la firma electrónica en determinados contextos sectoriales, como el portuario o marítimo, ello no implica necesariamente el reconocimiento automático de firmas electrónicas emitidas en el extranjero, ni extiende su validez a todas las relaciones jurídicas, especialmente aquellas de naturaleza privada.

En consecuencia, la ausencia de certificados emitidos por entidades de certificación extranjeras que sean considerados como válidos por el INDECOPI genera espacios de inseguridad jurídica y puede limitar los beneficios esperados del comercio digital.

Sea que ello responda a la aún baja demanda nacional de servicios de certificación digital o a los costos y exigencias asociados a los procedimientos de acreditación o reconocimiento de entidades extranjeras en el país que los disuaden, lo cierto es que la consecuencia práctica es la reducción del abanico de opciones disponibles para confiar en firmas digitales con pleno valor legal en transacciones transfronterizas.

5.3. Barreras en el reconocimiento de certificados digitales extranjeros

Si bien, en virtud del artículo 141 del Código Civil, en principio, toda manifestación de voluntad realizada mediante medios electrónicos es válida, este reconocimiento no incorpora las presunciones legales que solo respaldan a la firma digital. Es decir, se puede admitir la validez de toda firma electrónica, pero esta: (i) no goza de la presunción de no

repudio, (ii) las entidades administrativas no están obligadas a aceptarla¹⁷ y (iii) la carga de la prueba recae en quien afirma su autenticidad. En general, ello genera un entorno de menor seguridad jurídica que no favorece el uso de firmas electrónicas en el comercio, siendo la evaluación de su validez luego de su cuestionamiento.

Al respecto, la CNUDMI ha indicado que una de las dos principales barreras para el uso transfronterizo de métodos de firma y autenticación electrónica son las incompatibilidades jurídicas, las cuales se originan cuando los ordenamientos jurídicos establecen requisitos diferentes para el uso y la validez de dichos métodos (CNUDMI, 2009).

Señala que estas discrepancias, si bien pueden no restringir en principio su uso, pueden generar mayores costos e inconvenientes al obligar a los operadores a cumplir con exigencias de múltiples jurisdicciones, reduciendo así la rapidez y eficiencia esperadas de las comunicaciones electrónicas (CNUDMI, 2009).

Asimismo, la CNUDMI advierte que la tendencia a exigir algún tipo de verificación nacional como condición para otorgar validez a certificados electrónicos extranjeros conduce, en la práctica, a una discriminación basada en el origen geográfico del certificado. Ello se debe a que el proveedor extranjero debe cumplir tanto con los requisitos del régimen de su país de origen como con los del país receptor, a diferencia de los proveedores nacionales, que solo deben ajustarse a su propia normativa (CNUDMI, 2009).

Es por ello que, como se señala en la LMFE, la CNUDMI adopta el criterio de grado de fiabilidad técnica sustancialmente equivalente como parámetro para determinar la validez de los certificados y firmas electrónicas emitidos en el extranjero. Así, la comisión buscó establecer un “criterio general para el reconocimiento transfronterizo de certificados sin el cual los prestadores de servicios de certificación podrían verse enfrentados a la carga irracional de tener que obtener licencias en muchas jurisdicciones” (CNUDMI, 2002, p. 76).

A su vez, al exigir contrastar la fiabilidad del certificado extranjero con los requisitos establecidos por el Estado promulgante, se buscó evitar otorgar una ventaja indebida a las entidades de certificación extranjeras frente a las nacionales. Este criterio debe aplicarse “prescindiendo de la naturaleza del sistema de certificación utilizado en la jurisdicción

de donde emanó el certificado o la firma” (CNUDMI, 2002, p. 77).

No obstante, reconoce que pueden existir distintos grados de fiabilidad según el fin que los usuarios persigan al emplear el certificado. Señala que, en la práctica, será el tribunal judicial o arbitral quien evalúe cada certificado y lo equipare al grado de fiabilidad más cercano previsto en la normativa interna. Ello, sin perjuicio de que el Estado pueda, a priori, reconocer la fiabilidad otorgada por la legislación de un país extranjero (CNUDMI, 2002, p. 78).

Si bien la LMFE no especifica las técnicas mediante las cuales los Estados pueden reconocer por adelantado la fiabilidad de un certificado, la CNUDMI señala como ejemplos el reconocimiento automático de certificados emitidos por Estados que apliquen un nivel de fiabilidad equivalente al nacional, así como declaraciones unilaterales o tratados internacionales (CNUDMI, 2009, p. 79).

Posteriormente, este mismo criterio de fiabilidad fue recogido en la Ley Modelo sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza¹⁸ (en adelante, LMIC).

Adicionalmente, el artículo 13 de esta ley modelo establece que no se podrán negar los efectos jurídicos al resultado del uso de un servicio de confianza por la sola razón de que dicho servicio no ha sido designado por la autoridad competente. Así, otorga la misma validez tanto a aquellos servicios designados ex ante como aquellos sujetos a evaluación ex post (CNUDMI, 2023, pp. 58, 59, 73 y 74).

De forma similar que la LMFE, aunque la LMIC no prevé un mecanismo específico para el reconocimiento jurídico transfronterizo, su guía explicativa señala que la incorporación de sus disposiciones puede facilitar la aplicación de los principios de reconocimiento recíproco de los métodos de identificación electrónica, cada vez más presentes en los acuerdos de libre comercio (CNUDMI, 2023, pp. 46-47).

En este punto, corresponde identificar: i) si contamos con algún instrumento que reconozca la validez recíproca o automática de un certificado extranjero y, ii) el nivel de compatibilidad del marco normativo peruano con el de los principales países destino de las exportaciones peruanas, teniendo en

17 Ello sin perjuicio de la facultad de la Administración de aceptar documentos suscritos mediante firma electrónica. No obstante, existen determinados procedimientos en los que no se permite el uso de este tipo de firma, exigiéndose exclusivamente la firma digital. A modo de ejemplo, en el procedimiento de constitución de una Sociedad por Acciones Cerrada Simplificada (SACS) a través de la plataforma SID-SUNARP (régimen creado mediante Decreto Legislativo 1409), la suscripción del acto constitutivo solo puede realizarse mediante firma digital.

18 Un servicio de confianza es aquel que ofrece garantías de determinadas propiedades de un mensaje de dato. Incluyen métodos para la creación y gestión de firmas electrónicas, entre otros (CNUDMI, 2023, p. 12).

cuenta la necesidad de contar con una legislación armonizada que facilite el comercio transfronterizo.

A. Según los instrumentos internacionales suscritos por el Perú

Respecto al primer punto, se ha efectuado un análisis de los acuerdos comerciales suscritos a la

fecha de elaboración del presente artículo, con el fin de corroborar la existencia de disposiciones vinculadas con el uso y reconocimiento de la firma electrónica.

A continuación, se presenta una tabla que identifica los países cuyos acuerdos comerciales incluyen disposiciones relativas a ello.

Tabla 2. Disposiciones sobre firma electrónica en los acuerdos comerciales con el Perú

	Parte	No discriminación de firmas electrónicas	No restringir la libre elección del método de autenticación	No impedir la prueba de autenticación	Fomento de interoperabilidad
En vigor	Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico (el Protocolo de la AP) (Gobierno del Perú, 2020, pág. 4)	X	X	Artículo 13.10	
	Australia (Gobierno del Perú, 2019, pág. 4)	Artículo 13.6			
	CTPP (Gobierno del Perú, 2021, págs. 4-5)	Artículo 14.6			
	TLC Alianza del Pacífico y Singapur (Gobierno del Perú, 2022, pág. 7)	Artículo 13.13			
Por entrar en vigor	Optimización TLC con China	Artículo 18.5			
	Tratado de Asociación Transpacífico (Gobierno del Perú, 2016, págs. 4-5)	Artículo 14.6			
	Hong Kong (Gobierno del Perú, 2024, págs. 3-4)	Artículo 11.4			

Fuente: Elaboración propia.

En líneas generales, la redacción de dichos instrumentos es similar. El primer párrafo de dichos artículos (salvo el Protocolo de la AP) establece el principio de no discriminación de las firmas electrónicas, no pudiendo negar su validez solo por estar en formato electrónico, salvo que la normativa nacional disponga diferente para ciertas circunstancias.

Asimismo, salvo en el Protocolo de la AP, el segundo párrafo de estos acuerdos dispone que

ninguna Parte adoptará o mantendrá medidas que prohíban a las partes de una transacción electrónica determinar mutuamente los métodos de autenticación apropiados para dicha transacción.

Por su parte, todos los acuerdos establecen que no se puede impedir que las partes tengan la oportunidad de probar, ante las autoridades judiciales o administrativas, que la transacción electrónica cumple con los requisitos legales vinculados a la autenticación.

A su vez, todos (con excepción del Protocolo de la AP) señalan que la normativa nacional puede exigir, para determinadas categorías de transacciones, que el método de autenticación cumpla con ciertos estándares de desempeño o se encuentre certificado por una autoridad acreditada. El acuerdo entre la Alianza del Pacífico y Singapur precisa, adicionalmente, que se puede exigir que cumpla con ciertos estándares de seguridad.

Finalmente, todos los acuerdos disponen que las partes fomentarán la interoperabilidad de los mecanismos de autenticación electrónica. En el caso de los acuerdos de la Alianza del Pacífico, tanto el Protocolo de la AP como el suscrito con Singapur, se prevé que dicha interoperabilidad debe sustentarse en estándares internacionales o regionales. Particularmente, el Protocolo de la AP establece la obligación de desarrollar mecanismos y criterios de homologación que promuevan dicha interoperabilidad. En ese sentido, señala:

Con este propósito, podrán considerar el **reconocimiento de certificados de firma electrónica avanzada o digital** según corresponda, emitidos por prestadores de servicios de certificación, que operen en el territorio de cualquier Parte de acuerdo con el **procedimiento que determine su legislación**, con el fin de resguardar los estándares de seguridad e integridad [Gobierno del Perú, 2020, p. 4] [Énfasis agregado]. En esta línea, se ha establecido un mecanismo de reconocimiento mutuo y la futura interoperabilidad de la firma avanzada y/o digital. Así, conforme lo indicado por la Alianza del Pacífico, cada país miembro reconocerá la validez de dichos tipos de firma, siempre que cumplan con los estándares locales. Por ello, se posibilita “que cualquier documento electrónico que se suscriba mediante firma digital/electrónica avanzada no tenga que demostrar la validez dicha firma, sino que ésta será aceptada en cualquiera de los 4 países” (Alianza del Pacífico, s.f.).

Adicionalmente, conforme la Declaración de Cali, se ha establecido como mandato presidencial “[a]poyar el diseño, implementación, uso y reconocimiento de mecanismos de intercambio de información de firma electrónica avanzada o firma digital y la interoperabilidad transfronteriza para facilitar la prestación de los servicios de Gobierno Digital” (Alianza del Pacífico, 2017).

Al respecto, en la Decisión 1 sobre el reconocimiento de documentos firmados electrónicamente en el marco de la interoperabilidad de las Ventanillas Únicas de Comercio Exterior (VUCE) de la Alianza del Pacífico, ejecutada mediante Decreto Supremo 003-2017-MINCETUR/SG, los Estados parte reconocen la validez de las firmas electrónicas utilizadas en los documentos que se transmitan

entre las VUCE a través de la plataforma de interoperabilidad (Alianza del Pacífico, 2024).

A su vez, en virtud del artículo 13.10 del Protocolo de la Alianza del Pacífico, la Hoja de Ruta para el mercado digital regional de la Alianza del Pacífico contempla como objetivo la “[c]ulminación de las acciones en curso para implementar la interoperabilidad de la firma electrónica entre los países miembros de la Alianza del Pacífico” (Subcomité de Economía Digital de la Alianza del Pacífico, 2021, p. 5).

Conforme a lo comunicado por el Estado Peruano, los países miembros de la alianza han venido trabajando para cumplir con este mandato. En este contexto, han proporcionado una lista de servicios digitales de confianza por cada país con el fin de interoperar entre ellos. Dicha lista incluye los archivos necesarios para validar la autenticidad de firmas electrónicas y digitales en los documentos intercambiados entre los países miembros. Dicha lista permite a los países miembros verificar la validez y autenticidad de las firmas electrónicas y digitales (Gobierno del Perú, 2020; 2023).

Adicionalmente, existen otras disposiciones similares en el marco de los distintos procesos de integración regional de los que el Perú forma parte.

Según la Decisión 929 de la Comunidad Andina - CAN, los Países Miembros deben reconocer como válidos los certificados de identificación digital o firma electrónica de los documentos digitales transmitidos o visualizados a través de plataforma de Interoperabilidad Comunitaria Andina - INTERCOM (Comunidad Andina, 2024).

A su vez, en el marco de la Organización de los Estados Americanos - OEA, en la VII Reunión Ministerial de Gobierno Digital de las Américas de la Red Interamericana de Gobierno Digital - Red GEALC, se presentó la lista de listas de confianza de esta red, así como se aprobó el Acuerdo regional de las Américas sobre Firma digital Transfronteriza (Red Gealc, 2022).

Conforme a dicho acuerdo, el cual ha sido suscrito por el Perú, la lista funciona como la base técnica de acuerdos regionales de firma digital transfronteriza. No obstante, precisa que la lista es un instrumento técnico, ya que la validez jurídica de las firmas digitales está condicionada a lo establecido en los acuerdos internacionales mutuos refrendados según su marco normativo nacional (Red Gealc, 2022).

Por otro lado, conforme la Resolución 87 (XIX) del Consejo de Ministros de la Asociación Latinoamericana de Integración - ALADI, se encomendó al Comité de Representantes la implementación de un mecanismo de

reconocimiento mutuo de la firma digital entre los países miembros (Consejo de Ministros de ALADI, 2023). Según lo comunicado, en la VIII Reunión de Expertos en Firma Digital del 17 de junio de 2025, se presentaron los avances sobre la Lista de Confianza Regional y el estado del servicio de verificación de las firmas digitales (ALADI, 2025).

En este contexto, el marco regulatorio peruano reconoce la validez general de las firmas electrónicas, no restringe el uso de firmas distintas a las emitidas por la IOFE en los pactos o convenios entre las partes, y no limita la oportunidad de probar la validez de la firma (precisando únicamente sobre quién recae la carga de la prueba). En consecuencia, el Perú cumple con las obligaciones asumidas en los diversos acuerdos comerciales suscritos. No obstante, dichos acuerdos (con excepción del de la Alianza del Pacífico) no incorporan disposiciones que permitan el reconocimiento mutuo de la validez de las firmas electrónicas entre las Partes.

Respecto a la Alianza del Pacífico, se ha establecido un mecanismo de reconocimiento mutuo por el cual se reconoce la validez de la firma avanzada y/o digital emitido en los países miembros, siempre que se cumpla con el procedimiento regulado por la normativa interna. En el caso peruano, solo la firma digital es equiparada a la firma manuscrita, y tiene la presunción legal de validez sin tener que demostrar su fiabilidad. En este sentido, la firma digital emitida en Chile, México y Colombia, para que sea válida en el Perú, debe estar creada en el marco de la PKI.

A su vez, sin perjuicio de lo indicado anteriormente, cabe indicar que no se ha regulado un procedimiento para el reconocimiento de las firmas electrónicas emitidas en el marco de la Alianza del Pacífico. Ello teniendo en cuenta que, conforme la Carta 004163-2025-OAF/INDECOPI, dicha autoridad ha indicado que aún no se ha incorporado alguna

entidad de certificación extranjera en virtud de un reconocimiento mutuo en el marco del Reglamento.

Finalmente, respecto a los demás instrumentos analizados, es importante señalar que el reconocimiento de firmas en el marco de la CAN opera únicamente para determinados documentos intercambiados entre autoridades a través del sistema Intercom¹⁹. Por su parte, el mecanismo promovido por la Red GEALC solo es aplicable cuando existe un acuerdo que lo operacionalice. De igual manera, el proyecto en el ámbito de ALADI se encuentra todavía sin un mecanismo de reconocimiento implementado.

B. Según la regulación de los principales países destino de las exportaciones peruanas

De acuerdo con lo expuesto previamente, uno de los principales objetivos de la armonización regulatoria es evitar la duplicación de requisitos, ya que esta incrementa los costos operativos y desincentiva el uso de la firma electrónica. En este contexto, resulta necesario evaluar el grado de compatibilidad entre la normativa peruana y la de los principales países de destino de las exportaciones nacionales.

Para identificar los dichos países, se tomó como insumo el Cuadro G6 de las Estadísticas y Estudios sobre Información Aduanera publicadas por la SUNAT (2025). Así, en el 2025 (hasta agosto), China concentró aproximadamente el 30.9 % del total exportado por el Perú. En segundo lugar, se ubicó Estados Unidos, con una participación del 11.76 %. Le siguieron India (6.6 %), Canadá (5.83 %) y Emiratos Árabes Unidos (4.55 %).

En este sentido, a continuación, se presenta el análisis del marco jurídico relativo al reconocimiento de la firma electrónica emitida en el extranjero en cada uno de dichos países.

Tabla 3. Análisis de la validez y eficacia jurídica de la firma electrónica extranjera en los principales países destino de las exportaciones peruanas

País	Norma	Detalle	Reconoci- miento
China	Ley de Firma Electrónica de 2019 (China Laws Portal, 2019)	Conforme su Artículo 26, los certificados de autenticación de firma electrónica emitidos por proveedores extranjeros tienen el mismo efecto legal que los emitidos por los proveedores establecidos según la ley. Se requiere de la aprobación de la autoridad competente, de conformidad con los acuerdos pertinentes o con el principio de reciprocidad.	Requiere aprobación de autoridad nacional competente

19 A la fecha, la INTERCOM solo prevé la gestión de los siguientes documentos de comercio exterior: certificado de origen, certificado fitosanitario, declaración andina de valor, declaración aduanera de mercancías, y notificación sanitaria obligatoria (Comunidad Andina, 2025).

País	Norma	Detalle	Reconoci- miento
Estados Unidos	Subcapítulo I del Capítulo 96 del Título 15 del Código de los Estados Unidos Firmas Electrónicas en el Comercio Global y Nacional del 2000 (Legal Information Institute, s.f.)	En línea con lo dispuesto en la sección § 7001, en toda transacción comercial interestatal o exterior no se podrán negar los efectos jurídicos, la validez ni la exigibilidad de una firma únicamente por encontrarse en formato electrónico. Asimismo, conforme a la sección § 7031, se promoverá la aceptación y el uso de las firmas electrónicas a nivel internacional, de acuerdo con lo señalado en la sección § 7001 y principios tales como adoptar un enfoque no discriminatorio respecto de las firmas electrónicas y de los métodos de autenticación de otras jurisdicciones. De este modo, se dispone que la Secretaría de Comercio deberá adoptar las medidas necesarias para eliminar o reducir, en la mayor medida posible, los impedimentos en materia de firmas electrónicas, a fin de facilitar el desarrollo del comercio interestatal y exterior.	Reconoce validez de firmas electrónicas extranjeras
	India	Ley de Tecnología de la Información de 2000 (India Code, s.f.)	Según su Artículo 19, para el reconocimiento de cualquier autoridad certificadora extranjera y, por ende, la validez del certificado de firma electrónica, se requiere la aprobación del gobierno y la notificación en el diario oficial.
Canadá	Ley de Protección de Información Personal y Documentos Electrónicos (Gobierno de Canadá, 2025)	No regula expresamente el reconocimiento de las firmas electrónicas emitidas en el extranjero. No obstante, reconoce la validez de la firma electrónica simple, pero exige el uso de una firma electrónica “segura” para determinados casos, como documentos utilizados como pruebas, sellos, documentos originales, declaraciones bajo juramento o de veracidad y firmas presenciadas. (Gobierno de Canadá, 2019). En este sentido, en línea con lo dispuesto en el Reglamento sobre Firmas Electrónicas Segura, se vincula la firma electrónica segura al uso de la PKI (Gobierno de Canadá, 2025)	No lo contempla
Emiratos Árabes Unidos	Decreto-Ley Federal 46 de 2021 (Gobierno de los Emiratos Árabes Unidos, 2021)	Su artículo 37 dispone que los servicios de confianza cualificados prestados por entidades extranjeras serán reconocidos cuando resulten equivalentes al nivel de los servicios prestados por las entidades nacionales, de conformidad con las disposiciones del decreto ley y las decisiones de la TDRA.	Requiere aprobación de autoridad nacional competente
	Decisión de la TDRA sobre la aprobación de los dispositivos de creación de firmas y sellos cualificados (TDRA, s.f.)	A raíz del número limitado de dispositivos que cumplen con los requisitos técnicos, la autoridad ha preaprobado aquellos que cuentan con certificaciones internacionales específicas (ISO/IEC y CEN EN) o que se encuentran listados por la Comisión Europea. Para su reconocimiento, el prestador debe notificar a dicha autoridad para su inclusión en el registro de organismos de certificación aprobados.	Reconocimiento unilateral
	Reglamento sobre Transacciones Electrónicas de 2021 del Abu Dhabi Global Market ²⁰ (ADGM, 2021)	Su artículo 30 dispone que las firmas electrónicas tienen efecto legal, validez y exigibilidad, aun cuando hayan sido creados, emitidos, utilizados o ejecutados fuera del Abu Dhabi Global Market o de los Emiratos Árabes Unidos.	

Fuente: Elaboración propia.

20 Es un centro financiero internacional del Emirato de Abu Dabi (uno de los siete territorios de Emiratos Árabes Unidos). Cuenta con su propia regulación civil y comercial basada en el *common law* inglés. (ADGM, s.f.)

Como se puede apreciar, en tres de los cinco principales países destino de las exportaciones peruanas se exige autorización por parte de la autoridad nacional competente.

Por otro lado, se ha verificado si estos países son parte de la Convención, dado que, aunque de alcance más limitado que la LMFE, también incorpora disposiciones relativas a la firma electrónica y el reconocimiento transfronterizo de las comunicaciones electrónicas.

En efecto, su artículo 9 recoge el principio de equivalencia funcional de las firmas electrónicas, al establecer que el requisito de firma se cumple cuando el método utilizado es suficientemente confiable y apropiado para los fines perseguidos, o cuando se demuestra que, por sí solo o con el respaldo de otras pruebas, dicho método cumple las funciones de identificar a la parte e indicar su voluntad respecto del contenido (CNUDMI, 2007, pp. 5-6).

Al respecto, la nota explicativa de dicha convención señala que la eficacia jurídica de una firma electrónica, o el grado en que pueda producirla, no puede depender del lugar donde se haya creado la firma electrónica ni del lugar en que se encuentre la infraestructura (jurídica o de otra índole) que la respalda, sino que debe basarse exclusivamente en su fiabilidad técnica (CNUDMI, 2007, p. 60).

En otras palabras, reconoce que no se puede negar la validez y eficacia de una firma electrónica por el solo hecho de ser emitida en el extranjero; sino que esta tiene que cumplir con los requisitos vinculados al uso de un método fiable.

En esta línea, se ha identificado que solo China ha firmado esta convención. No obstante, como aún no ha culminado su proceso de ratificación interna, aún no está vigente para este país (CNUDMI, 2025).

En consecuencia, únicamente en los Emiratos Árabes Unidos existe un mecanismo distinto de la acreditación de la entidad certificadora para reconocer la validez de firmas electrónicas extranjeras. Así, se reconocen aquellas que cumplan estándares internacionales y hayan sido notificadas para su inscripción en el registro nacional o, en el marco del Abu Dhabi Global Market, se aplica un reconocimiento unilateral de validez de firmas electrónicas creadas en el extranjero.

En los demás países analizados (con excepción de Canadá), dado que exigen acreditación por parte de la autoridad nacional y no existe un instrumento de reconocimiento mutuo u otro instrumento similar, sumado al propio requerimiento de la regulación peruana, los proveedores deben registrarse en ambas jurisdicciones.

6. Conclusiones y recomendaciones

- La digitalización se ha consolidado como un elemento estructural del comercio transfronterizo. En este contexto, la firma electrónica cumple una función central, al permitir acreditar la identidad del firmante, su voluntad de obligarse y la integridad de un mensaje de datos. Se estima que su uso a nivel internacional siga creciendo, especialmente en las transacciones B2B.

Para aprovechar plenamente los beneficios del comercio digital, se requiere contar con marcos jurídicos que reconozcan la validez de las firmas y certificados electrónicos emitidas en el extranjero y que establezcan criterios de reconocimiento armonizados con estándares internacionales. La ausencia de mecanismos claros y funcionales de reconocimiento genera fricciones, incrementa costos y desincentiva su uso.

- La doctrina internacional identifica tres enfoques regulatorios en materia de firma electrónica: prescriptivo, minimalista e híbrido. El enfoque prescriptivo, que condiciona la validez de la firma al uso de tecnologías específicas y, usualmente, exigiendo también que sean emitidas por entidades acreditadas por una autoridad nacional (PKI), tiende a convertirse en una barrera al comercio transfronterizo.

Ello debido a su elevada complejidad de implementación, a los costos asociados y a su limitada compatibilidad con las prácticas reales del mercado, donde gran parte de los documentos del comercio exterior se suscriben mediante firmas electrónicas simples.

- Frente a ello, la CNUDMI ha establecido determinados parámetros para superar estas barreras. Conforme lo dispuesto en la LMFE, esta comisión promueve un enfoque híbrido que vincula la validez de la firma electrónica no a la tecnología empleada, a la acreditación por una entidad nacional del proveedor o al lugar de emisión, sino al nivel de fiabilidad técnica en función al fin que se persigue.
- En el Perú, el marco legal que faculta el uso de firmas electrónicas está compuesto principalmente por el Código Civil, la Ley 27269 y su Reglamento. Estas normas permiten la manifestación de voluntad mediante medios electrónicos y reconocen, en términos generales, la validez de la firma electrónica.

Sin embargo, la plena validez de los certificados electrónicos emitidos en el extranjero está condicionada a su autorización por el INDECOPI.

En un escenario de creciente intercambio internacional, dicha disposición resulta insuficiente y se evidencia la necesidad de contar con mecanismos efectivos de armonización y reconocimiento mutuo.

- El Reglamento prevé dos vías para validar una firma electrónica extranjera: i) la acreditación de la entidad extranjera como proveedor y ii) el reconocimiento por parte del INDECOPI mediante reconocimiento mutuo, certificación cruzada o incorporación por reconocimiento. Todos estos mecanismos operan en el marco de la IOFE y exigen que el certificado corresponda a una firma digital basada en PKI. Esto supone el uso de criptografía asimétrica y la emisión del certificado por una entidad autorizada por el Indecopi.
- En consecuencia, si bien la normativa peruana no es incompatible con la LMFE ni con los principios del comercio electrónico, tampoco se encuentra plenamente alineada con ellos. En lugar de reconocer a la firma electrónica avanzada (sustentada en el uso de un mecanismo fiable) como equivalente a la firma manuscrita, dicha equivalencia se aplica exclusivamente a la firma digital basada en infraestructura PKI. A su vez, la validez de los certificados extranjeros se condiciona a la adopción de esta misma infraestructura, en contraposición a lo establecido por la CNUDMI.

En este punto, se evidencia la necesidad de alinear marco jurídico nacional con los estándares internacionales, a fin de fortalecer la seguridad jurídica al reconocer la plena validez del uso tanto de firma digital como de firma electrónica avanzada. De este modo, se busca que el centro de eventuales controversias contractuales se concentre en cuestiones sustantivas relativas al incumplimiento de las obligaciones asumidas, y no en debates preliminares sobre la validez y/o legitimidad del método de firma empleado.

- Actualmente, no existe en el Perú ninguna entidad extranjera reconocida bajo los mecanismos previstos. Los supuestos de reconocimiento vigentes se limitan a ámbitos específicos, tales como la CAN, la Alianza del Pacífico o en normas sectoriales, y algunos de ellos se limitan a documentos intercambiados entre autoridades. Asimismo, la mayoría de los acuerdos comerciales suscritos por el país no incluyen mecanismos de reconocimiento mutuo aplicables a firmas electrónicas.
- De manera similar, en los principales países destino de las exportaciones peruanas, el reconocimiento de firmas y certificados electrónicos extranjeros suele estar

condicionado a la aprobación de la autoridad nacional competente. Esto implica que los proveedores deban cumplir las exigencias regulatorias tanto del país de origen como del país receptor, lo cual incrementa los costos operativos y desincentiva su utilización.

- En este marco, se evidencia la necesidad de explorar en el Perú alternativas que faciliten el reconocimiento transfronterizo de las firmas y certificados electrónicos. Basado en la experiencia internacional, resulta pertinente promover mecanismos tales como:

- Sistemas de preaprobación basados en estándares internacionales, tal como ocurre en los Emiratos Árabes Unidos y como se aplicó temporalmente en el Perú mediante el Decreto Supremo 105-2012-PCM.
- Modelos de listas de confianza, como los implementados en la Unión Europea (Unión Europea, 2025).
- Plataformas regionales que permiten verificar la validez de firmas electrónicas emitidas en distintos países, como el sistema firma.gub.uy, aplicable para las firmas emitidas en Uruguay, Argentina, Brasil y Paraguay (Naciones Unidas, 2024); o
- Acuerdos de reconocimiento recíproco, como los desarrollados en la Alianza del Pacífico, entre otros.

- A su vez, hay que tener en consideración los nuevos instrumentos internacionales en proceso de negociación que el Perú tiene a la mira, tales como el Acuerdo sobre Comercio Electrónico de la OMC. Al respecto, el artículo 5.7 de su Texto Estabilizado establece que las partes deben promover el uso de mecanismos interoperables de autenticación electrónica. Asimismo, indica que las partes podrán voluntariamente cooperar para alentar el reconocimiento mutuo de las firmas electrónicas (OMC, 2024). De aprobarse este acuerdo, podría constituir un impulso adicional para la adecuación del marco normativo nacional a estándares internacionales, así como para el desarrollo de mecanismos de interoperabilidad y reconocimiento transfronterizo.

- En conjunto, la adopción de estos instrumentos permitiría reducir cargas regulatorias, promover la interoperabilidad y fortalecer la confianza en los sistemas de firma electrónica utilizados en el comercio internacional, contribuyendo a una mayor alineación del marco normativo peruano con los estándares internacionales y a una inserción más eficiente del país en el comercio digital transfronterizo.

7. Acrónimos

ADGM	Abu Dhabi Global Market
Aladi	Asociación Latinoamericana de Integración
APEC	Foro de Cooperación Asia-Pacífico
B2B	Business to Business
CAN	Comunidad Andina
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (Uncitral, en inglés)
CPTPP	Acuerdo Amplio y Progresista de Asociación Transpacífico
Dicapi	Dirección General de Capitanías y Guardacostas
Escap	Comisión Económica y Social para Asia y el Pacífico
Gealc	Red Interamericana de Gobierno Digital
Indecopi	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
IOFE	Infraestructura Oficial de Firma Electrónica
LMCE	Ley Modelo de la CNUDMI sobre Comercio Electrónico
LMFE	Ley Modelo de la CNUDMI sobre las Firmas Electrónicas
LMIC	Ley Modelo sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza
OEA	Organización de los Estados Americanos
OMC	Organización Mundial del Comercio
PKI	Infraestructura de Clave Pública (Public Key Infrastructure, en inglés)
ROPS	Registro Oficial de Prestadores de Servicios de Certificación Digital
Sunat	Superintendencia Nacional de Aduanas y de Administración Tributaria
TDRA	Telecommunications and Digital Government Regulatory Authority
Unctad	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
VUCE	Ventanilla Única de Comercio Exterior

Lista de referencias

ADGM. (2021). *Electronic Transactions Regulations 2021*. 30. *Cross-border recognition*. <https://adgmen.thomsonreuters.com/rulebook/30-cross-border-recognition>

ADGM. (s.f.). *Introduction to Abu Dhabi Global Market*. <https://en.adgm.thomsonreuters.com/rulebook/introduction-abu-dhabi-global-market-2>

Aladi. (2025). *Reuniones de expertos*. <https://www.aladi.org/agenda-digital/firma-digital/>

Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S. & Kar, J. (2015). Public Key Infrastructure: A Survey. *Journal of Information Security*, 6, 27-31. https://www.researchgate.net/publication/272955036_Public_Key_Infrastructure_A_Survey

Alianza del Pacífico. (2017). *Declaración de Cali*. https://www.acuerdoscomerciales.gob.pe/en_vigencia/alianza_pacifico/Documentos/docs/5_11_AP_20170630_Declaracion_de_Cali.pdf

Alianza del Pacífico. (2024). *Decisión N.º 1 de la Comisión de Libre Comercio del Protocolo*

Adicional al Acuerdo Marco de la Alianza del Pacífico. <https://alianzapacifico.net/download/decision-n1-reconocimiento-de-los-documentos-firmados-electronicamente-en-el-marco-de-la-interoperabilidad-de-las-ventanillas-unicas-de-comercio-exterior-en-la-alianza-del-pacifico/>

Alianza del Pacífico. (s.f.). *Comercio de servicios, inversiones y economía digital ante el Covid-19*. https://alianzapacifico.net/wp-content/uploads/OnePager_comercioap-infografia-actualizada_2.pdf

Castellani, L. (s.f.). *Introduction to the law of electronic signatures*. <https://www.carecprogram.org/uploads/Session-4-Introduction-to-the-Law-of-Electronic-Signatures.pdf>

Castilla del Carpio, P. (2025, 24 de julio). *Firma digital. Marco legal, usos y retos*. <https://isoc.pe/wp-content/uploads/2025/08/PPT-24-julio-2025.pdf>

China Laws Portal. (2019). *Electronic Signature Law of China (2019)*. <https://www.chinajusticeobserver.com/law/x/electronic-signature-law-of-china-20190423/chn>

Cloud Signature Consortium. (2025). *CSC Industry Market Report 2025. The Cloud Signature Market. EU & Global Perspective*. Cloud Signature Consortium. https://storage.uk.cloud.ovh.net/v1/AUTH_f3100dad5acd4df793f8778d19bcea24/CSC/5592012d-f6d3-42f4-845d-8b3f8c607c5d.pdf?temp_url_sig=d5e96a37bf44a805a985209a54906d702952c6ca&temp_url_expires=2059750745&filename=CSC%20Cloud%20Signature%20Market%20Report%2025

CNUDMI. (1999). *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998*. Naciones Unidas. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf

CNUDMI. (2013). *Guía de la CNUDMI*. Naciones Unidas. <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/12-57494-guide-to-uncitral-s.pdf>

CNUDMI. (2023). *Situación actual de los convenios, convenciones y leyes modelo y del funcionamiento del Registro de Transparencia. Nota de la Secretaría*. Naciones Unidas. <https://docs.un.org/es/a/cn.9/1136>

CNUDMI. (2024). *Situación actual de los convenios, convenciones, leyes modelo y otros textos de la CNUDMI. Nota de la Secretaría*. Naciones Unidas. Obtenido de <https://docs.un.org/es/A/CN.9/1172/Rev.1>

CNUDMI. (2025). *Examen de los textos de la CNUDMI relativos a aspectos electrónicos. Nota de la Secretaría*. Naciones Unidas. <https://docs.un.org/es/A/CN.9/1226>

CNUDMI. (2025). *Situación de las convenciones y leyes modelo y otros textos de la CNUDMI. Nota de la Secretaría*. Naciones Unidas. <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/1207-s.pdf>

CNUDMI. (s.f.). *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998*. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce

CNUDMI. (s.f.). *Ley Modelo de la CNUDMI sobre documentos transmisibles electrónicos (2017) - Situación Actual*. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_transferable_records/status

CNUDMI. (s.f.). *Situación actual: Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996)*. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce/status

CNUDMI. (s.f.). *Situación actual: ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)*. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_signatures/status

CNUDMI. (2002). *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, con su Guía para su incorporación al derecho interno*. Naciones Unidas. <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf>

CNUDMI. (2007). *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*. Naciones Unidas. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/06-57455_ebook.pdf

CNUDMI. (2009). *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas*. Naciones Unidas. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/08-55701_ebook.pdf

CNUDMI. (2023). *Ley Modelo de la CNUDMI sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza*. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/mlit_sp.pdf

CNUDMI. (2024). *Ley Modelo de la CNUDMI sobre Contratación Automatizada*. Naciones Unidas. https://uncitral.un.org/sites/uncitral.un.org/files/mlac_es.pdf

CNUDMI. (2025). *Situación actual: Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales* (Nueva York, 2005). https://uncitral.un.org/es/texts/ecommerce/conventions/electronic_communications/status

Comité de Comercio e Inversión del APEC. (2025). *A Path to Paperless Trade: Analysing the Legal Gaps and Economic Benefit of Adopting or Maintaining a Legal Framework that Takes into Account the UNCITRAL Model Law on Electronic Transferable Records (MLETR)*. APEC Secretariat. https://www.apec.org/docs/default-source/publications/2025/2/225_cti_paperless-trade.pdf?sfvrsn=d5779b94_1

Comunidad Andina. (2024, 5 de setiembre). *Decisión 929*. <https://www.comunidadandina.org/DocOficialesFiles/Gacetas/Gaceta%205547.pdf>

Comunidad Andina. (2025, 27 de octubre). *INTERCOM impulsará la facilitación del comercio exterior en la Comunidad Andina*. <https://www.comunidadandina.org/notas-de-prensa/intercom-impulsara-la-facilitacion-del-comercio-exterior-en-la-comunidad-andina/>

Congreso de la República. (1999, 18 de agosto). *Proyecto de Ley 5070/99-CP*. [https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/0/9f8c16c81bd57a6205257e5e007e44e7/\\$FILE/PL0507019990818.pdf](https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/0/9f8c16c81bd57a6205257e5e007e44e7/$FILE/PL0507019990818.pdf)

Congreso de la República. (2000, 4 de mayo). *Proyecto de Ley 5650/99-CR*. [https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/d99575da99ebfbfe305256f2e006d1cf0/9b0bcd2b8209ec5b05257f1e00719f51/\\$FILE/PL0565020000504.pdf](https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/d99575da99ebfbfe305256f2e006d1cf0/9b0bcd2b8209ec5b05257f1e00719f51/$FILE/PL0565020000504.pdf)

Congreso de la República. (2000, 14 de junio). *Proyecto de Ley 5762/99-CR*. [https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/0/f355ed074179cfaf05257f2b004d09b9/\\$FILE/PL0576220000614.pdf](https://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/0/f355ed074179cfaf05257f2b004d09b9/$FILE/PL0576220000614.pdf)

Consejo de Ministros de Aladi. (2023). *Resolución 87 (XIX). Agenda Digital*. Aladi. [https://www2.aladi.org/nsfaladi/Juridica.nsf/vresolucionesconsejo/8B072DB4EED788F03258A1C0067B794/\\$FILE/CM_019_Resolucion_087.pdf](https://www2.aladi.org/nsfaladi/Juridica.nsf/vresolucionesconsejo/8B072DB4EED788F03258A1C0067B794/$FILE/CM_019_Resolucion_087.pdf)

Daza Jaller, L., Gaillard, S. & Molinuevo, M. (2020). *The Regulation of Digital Trade: Key Policies and International Trends*. Banco Mundial. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/998881578289921641>

ESCAP. (2019). *Selected issues in cross-border e-commerce development in Asia and the Pacific*. United Nations publication. <https://digitallibrary.un.org/record/3928507?v=pdf>

ESCAP & CNUDMI. (2022). *Electronic signatures and trust services*. En *Legal Readiness Assessment Guide for Cross-Border Paperless Trade*. <https://readiness.digitalizetrade.org/legal-guide/ib-electronic-signatures-and-trust-services?>

Espinoza Céspedes, J. F. (2017). Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla*, 41, 241-266. Revista IUS: <https://revistaius.com/index.php/ius/article/view/315/623>

FMI, OCDE, UNCTAD & OMC. (2023). *Handbook on Measuring Digital Trade. Second Edition*. OMC. https://www.wto.org/english/res_e/booksp_e/digital_trade_2023_e.pdf

Gobierno de Canadá. (2019, 15 de julio). *Government of Canada Guidance on Using Electronic Signatures*. <https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html>

Gobierno de Canadá. (2025). *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*. <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>

Gobierno de Canadá. (2025). *Secure Electronic Signature Regulations*. <https://laws-lois.justice.gc.ca/eng/regulations/sor-2005-30/page-1.html>

Gobierno de los Emiratos Árabes Unidos. (2021). *Federal Decree Law No. (46) of 2021 on Electronic Transactions and Trust Services*. <https://uaelegislation.gov.ae/en/legislations/1539/download>

Gobierno del Perú. (2016). *Exposición de Motivos del Decreto Supremo 026-2016-PCM*. <https://spij.minjus.gob.pe/Graficos/Peru/2016/Abril/29/EXP-DS-026-2016-PCM.pdf>

Gobierno del Perú. (2016). *Textos negociados del TPP. Capítulo 14. Comercio Electrónico*. https://www.acuerdoscomerciales.gob.pe/Por_entrar_Vigencia/TPP/Documentos/Acuerdo/ES/14_Comercio_Electronico.pdf

Gobierno del Perú. (2019). *ALC Perú-Australia. Capítulo 13. Comercio Electrónico*. https://www.acuerdoscomerciales.gob.pe/En_Vigencia/Australia/Documentos/Capitulos/13_Comercio_Electronico.pdf

Gobierno del Perú. (2020). *Lista de servicios de confianza de la Alianza del Pacífico*. <https://www.gob.pe/institucion/rree/informes-publicaciones/455264-lista-de-servicios-de-confianza-de-la-alianza-del-pacifico>

- Gobierno del Perú. (2020). *Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico. Capítulo 13. Comercio Electrónico*. https://www.acuerdoscomerciales.gob.pe/En_Vigencia/Alianza_Pacifico/Documentos/espanol/13_CE_FINAL.pdf
- Gobierno del Perú. (2021). *CPTPP. Capítulo 14. Comercio Electrónico*. https://www.acuerdoscomerciales.gob.pe/En_Vigencia/CPTPP/Documentos/tpp/Acuerdo/ES/14_Comercio_Electronico.pdf
- Gobierno del Perú. (2022). *TLC entre la Alianza del Pacífico y Singapur. Capítulo 13. Comercio Electrónico*. https://www.acuerdoscomerciales.gob.pe/En_Vigencia/AlianzaPacifico_Singapur/Documentos/VERSION_ESPA%C3%91OL/13_PASFTA_Comercio_electronico.pdf
- Gobierno del Perú. (2023). *Interoperabilidad transfronteriza*. <https://www.gob.pe/8655-presidencia-del-consejo-de-ministros-interoperabilidad-transfronteriza>
- Gobierno del Perú. (2024). *ALC Perú-Hong Kong. Capítulo 11. Comercio Electrónico*. [https://www.acuerdoscomerciales.gob.pe/Por_entrar_Vigencia/Hong_Kong/Documentos/TLC%20HK%20SPANISH/11_Electronic_Commerce_\(SPANISH\).pdf](https://www.acuerdoscomerciales.gob.pe/Por_entrar_Vigencia/Hong_Kong/Documentos/TLC%20HK%20SPANISH/11_Electronic_Commerce_(SPANISH).pdf)
- Gregory, J. (2024). *Legal Implementation Guide For Cross-border Paperless Trade. UNNExT Working Paper Series No. 12. ESCAP*. <https://repository.unescap.org/server/api/core/bitstreams/8c2576f8-1898-4409-997e-ff9fd8e6b23a/content>
- Indecopi. (2025, 27 de noviembre). *Registro Oficial de Prestadores de Servicios de Certificación Digital (ROPS)*. <https://www.gob.pe/institucion/indecopi/informes-publicaciones/5447866-registro-oficial-de-prestadores-de-servicios-de-certificacion-digital-rops>
- India Code. (s.f.). *The Information Technology Act, 2000*. <https://www.indiacode.nic.in/handle/123456789/1999>
- Kim, H. (2019). Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. *Computer Law & Security Review*, 35(5).
- Legal Information Institute. (s.f.). *15 U.S. Code Chapter 96 Subchapter I - Electronic Signatures in Global and National Commerce Act*. <https://www.law.cornell.edu/uscode/text/15/chapter-96/subchapter-I>
- Naciones Unidas. (2024). *E-Government. Survey 2024. Accelerating Digital Transformation for Sustainable Development. With the addendum on Artificial Intelligence*. Naciones Unidas.
- OMC. (2024). *Iniciativa relativa a la Declaración Conjunta sobre el Comercio Electrónico*. https://www.wto.org/spanish/tratop_s/ecom_s/joint_statement_s.htm
- Red Gealc. (2022). *Acuerdo regional de las Américas sobre Firma digital Transfronteriza*. https://www.redgealc.org/site/assets/files/15613/doc_03_acuerdo_firma.pdf
- Red Gealc. (2022, 15 de noviembre). *Se presentó la lista de listas de confianza y otros hitos para la firma digital entre países*. <https://www.redgealc.org/contenido-general/noticias/se-presento-la-lista-de-listas-de-confianza-para-la-firma-digital-entre-paises/>
- Subcomité de Economía Digital de la Alianza del Pacífico. (2021). *Hoja de ruta para el mercado digital regional de la Alianza del Pacífico*. <https://alianzapacifico.net/wp-content/uploads/2021/06/HOJA-DE-RUTA-PARA-EL-MERCADO-DIGITAL-REGIONAL-DE-LA-ALIANZA-DEL-PACIFICO.pdf>
- Sunat. (2025). *Nota Tributaria y Aduanera. Información Aduanera - Exportaciones*. <https://www.sunat.gob.pe/estadisticasestudios/exportaciones.html>
- Tasneem, F. (Febrero de 2014). Legal Effect of Electronic Contracts: A Comparative Study. *Global Advanced Research Journal of Management and Business Studies*, 3(2), 74-81.
- TDRA. (s.f.). *QSCDs certification bodies approved by TDRA*. <https://tdra.gov.ae/en/About/tdra-sectors/information-and-digital-government/policy-and-programs-department/trust-services/qscds-certification-bodies-approved-by-tdra>
- UNCTAD. (2025). *Digital Economy Report Pacific Edition 2024. Promoting Digital Entrepreneurship and Trade*. Naciones Unidas. https://unctad.org/system/files/official-document/dtlecdc2025d1_en.pdf
- Unión Europea. (2025). *EU/EEA Trusted List Browser*. <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>