CONTRATOS EMPRESARIALES
EN LA ERA DIGITAL

VALIDEZ Y EFICACIA JURÍDICA DE LAS FIRMAS ELECTRÓNICAS EN EL PERÚ.

Estudio sobre la ley de firmas y certificados digitales y su aplicación práctica en operaciones comerciales.

AUTORES

- Christian David Corrales Otazú
- Sarita Jessica Apaza Miranda
- Katia Scarlet Reyes Loaiza
- Andrea Coaguila Gómez
- Alexander Joao Peñaloza Mamani
- Jorge Luis Monje Téllez
- César Alejandro Nájar Becerra
- Nestor Raul Arredondo Perez

EDITORIAL
MUNDO INTERDISCIPLINARIO

ISBN 978-628-97574-4-6

Autores

Christian David Corrales Otazú

Universidad Católica de Santa María - **UCSM**

ccorraleso@ucsm.edu.pe

https://orcid.org/0000-0002-8774-4859

Sarita Jessica Apaza Miranda

Universidad Continental - Sede Arequipa

sapaza@continental.edu.pe

https://orcid.org/0000-0003-2358-2077

Katia Scarlet Reyes Loaiza

Universidad Continental - Sede Arequipa

kreyes@continental.edu.pe

https://orcid.org/0000-0002-2366-1958

Andrea Coaguila Gómez

Universidad Tecnológica del Perú **UTP**

c31403@utp.edu.pe

https://orcid.org/0000-0001-9118-1932

Alexander Joao Peñaloza Mamani

Universidad Católica de Santa María - **UCSM**

apenaloza@ucsm.edu.pe

https://orcid.org/0000-0003-0456-9221

Jorge Luis Monje Téllez

Universidad Nacional de San Agustín de Arequipa

jmonje@unsa.edu.pe

https://orcid.org/0000-0002-2114-3102

César Alejandro Nájar Becerra

Universidad Católica de Santa María – **UCSM**

cnajar@ucsm.edu.pe

https://orcid.org/ 0000-0001-8954-8918

Nestor Raul Arredondo Perez

Universidad Tecnológica del Perú **UTP**

C28406@utp.edu.pe

https://orcid.org/0009-0000-5049-1459

EDITORIAL
MUNDO INTERDISCIPLINARIO

Editor: Alain Castro Alfaro

Título: Contratos empresariales en la era digital. Validez y eficacia de las firmas electrónicas en el Perú. Estudio sobre la Ley de Firmas y Certificados Digitales y su aplicación práctica en operaciones comerciales

Autores: Christian David Corrales Otazú, Sarita Jessica Apaza Miranda, Katia Scarlet Reyes Loaiza, Andrea Coaguila Gómez, Alexander Joao Peñaloza Mamani, Jorge Luis Monje Téllez, César Alejandro Nájar Becerra, Nestor Raul Arredondo Perez

ISBN Versión Digital: 978-628-97574-4-6

Sello Editorial:
Editorial Mundo Interdisciplinario

Coordinadora: Nora González Pérez – Cartagena –Colombia

Diagramación: Linda Castro González

Portada: Linda Luz Castro González

Cartagena –Colombia, Abril 2026

CONTRATOS EMPRESARIALES EN LA ERA DIGITAL

Validez y eficacia jurídica de las firmas electrónicas en el Perú

Estudio sobre la Ley de Firmas y Certificados Digitales y su aplicación práctica en operaciones comerciales

Christian David Corrales Otazú

Sarita Jessica Apaza Miranda

Katia Scarlet Reyes Loaiza

Andrea Coaguila Gómez

Alexander Joao Peñaloza Mamani

Jorge Luis Monje Téllez

César Alejandro Nájar Becerra

Nestor Raul Arredondo Perez

Colombia

Latinoamérica

2026

INDICE

Contenido

INTRODUCCIÓN

1. El Nuevo Paradigma Contractual

La acelerada evolución de las tecnologías de la información y la comunicación ha dejado de ser una promesa de futuro para convertirse en la infraestructura operativa del presente. Este fenómeno ha generado un cambio de paradigma irreversible en las dinámicas económicas y jurídicas a nivel global. En particular, el ámbito de la contratación empresarial ha experimentado una transformación sustancial, transitando de esquemas tradicionales —basados en la ritualidad presencial, el papel físico y la firma manuscrita— hacia modelos digitales sustentados en plataformas en la nube, identidad biométrica y mecanismos de autenticación remota.

Este proceso de digitalización no es meramente técnico; ha redefinido la manera en que las empresas manifiestan su voluntad, perfeccionan acuerdos y buscan garantizar la seguridad jurídica de sus operaciones. La pandemia de COVID-19 actuó como un catalizador forzoso que eliminó la opción de "no ser digital", obligando al sistema jurídico a enfrentarse, sin preparación suficiente, a la validez de acuerdos cerrados por WhatsApp, correos electrónicos o plataformas de firma electrónica extranjeras.

2. El Problema de Investigación: La Asimetría Normativa

En este nuevo contexto, las firmas electrónicas se han consolidado como la piedra angular del comercio moderno, permitiendo superar barreras geográficas y optimizar costos. No obstante, esta eficiencia operativa plantea serios desafíos dogmáticos y probatorios.

En el Perú, la respuesta legislativa se centra en la Ley N.º 27269, Ley de Firmas y Certificados Digitales. Si bien esta norma fue pionera en el año 2000 al introducir el principio de equivalencia funcional, esta investigación parte de un diagnóstico crítico: a más de dos décadas de su promulgación, la regulación parece haber quedado estática frente a una realidad comercial líquida y veloz.

Hoy nos enfrentamos a una "zona de incertidumbre jurídica" provocada por la coexistencia de dos mundos:

- Por un lado, la Firma Digital (oficial, regulada por la IOFE, costosa y poco masiva).
- Por otro, las Firmas Electrónicas (ágiles, usadas en plataformas globales como DocuSign o Adobe, pero con un valor probatorio que muchos jueces aún desconocen cómo valorar).

¿Qué sucede cuando un contrato millonario se firma con un "click" y una de las partes lo desconoce? ¿Está preparado el juez peruano para auditar la "huella digital" o sigue exigiendo la pericia grafotécnica tradicional? Estas son las interrogantes que motivan esta obra.

3. Objetivos y Metodología

El presente libro tiene como objetivo general analizar la validez, eficacia y valoración probatoria de las firmas electrónicas en los contratos empresariales en el Perú, desmitificando su complejidad técnica para ofrecer respuestas jurídicas claras.

Para abordar esta problemática, la obra adopta un enfoque dogmático y funcional. No nos limitamos a la exégesis de la norma; utilizamos el método comparado como herramienta crítica, contrastando la rigidez de la norma peruana con las soluciones flexibles del Reglamento eIDAS (Europa) y los avances de la Alianza del Pacífico. Asimismo, la investigación se nutre de la realidad jurisprudencial, analizando cómo los tribunales nacionales están resolviendo (o complicando) las disputas sobre contratos digitales.

4. Estructura de la Obra

Para guiar al lector —sea juez, abogado corporativo, notario o investigador—, el libro se ha estructurado siguiendo la lógica del problema a la solución:

- En el Capítulo I, establecemos el Marco Teórico, definiendo qué es realmente un contrato electrónico y desmontando los mitos sobre su inseguridad.

- El Capítulo II se adentra en el Sistema Peruano, diseccionando la Ley 27269 para distinguir con claridad quirúrgica entre firma "electrónica" y "digital", una distinción que suele ser la causa de perder o ganar un juicio.
- Los Capítulos III y IV constituyen el núcleo dogmático y procesal. Aquí analizamos la validez contractual (consentimiento) y, crucialmente, la prueba electrónica: ¿quién debe probar la autenticidad de un correo? ¿Cómo se impugna una firma digital?
- Finalmente, en los Capítulos V y VI, la obra abandona el diagnóstico para ofrecer propuestas. Miramos hacia el Derecho Comparado y el futuro inmediato (Blockchain, Smart Contracts) para proponer reformas de *lege ferenda* que modernicen nuestro sistema, y ofrecemos pautas prácticas para la actuación judicial hoy.

En suma, este libro no pretende ser solo un texto descriptivo, sino una herramienta de consulta indispensable para navegar la inevitable digitalización del Derecho Contractual peruano.

Capítulo I

La contratación empresarial en la era digital

CAPÍTULO I

LA CONTRATACIÓN EMPRESARIAL EN LA ERA DIGITAL

La función del contrato dentro del derecho empresarial ha sido objeto de profundas transformaciones a lo largo de las últimas décadas, como consecuencia de los avances tecnológicos y el proceso de globalización de los mercados. Los contratos tradicionales, que dependían del soporte físico y de la firma manuscrita como expresión de la voluntad, han venido cediendo espacio a formas de celebración desmaterializadas y electrónicas, ajustadas a las exigencias del comercio digital contemporáneo. La contratación empresarial digital no solo responde a demandas de eficiencia y rapidez, sino también a la necesidad de sustituir prácticas convencionales por mecanismos tecnológicos que facilitan la interacción entre agentes económicos a distancia en tiempo real (Moreno Navarrete, 2017).

En Perú, la doctrina especializada ha subrayado que la contratación electrónica ha dejado de ser un simple supuesto teórico para convertirse en una realidad empresarial cotidiana, con implicancias directas en la validez jurídica de la manifestación de voluntad y en la seguridad jurídica de las transacciones (Cordero Mendoza, 2024). Esto exige un replanteamiento de las categorías clásicas del derecho contractual — como consentimiento, forma, perfeccionamiento y prueba — poniendo en el centro la fiabilidad de los mecanismos electrónicos que intervienen en la formación del contrato.

Una obra influyente en el ámbito peruano conceptualiza la contratación electrónica como un campo que abarca tanto los supuestos denominados "contratos informáticos" como los acuerdos celebrados por medios electrónicos, destacando que la distinción entre ambos resulta más histórica que dogmática frente a las nuevas formas de comercio digital (Soto Coaguila, 2002). Desde una perspectiva comparada, la literatura internacional reconoce que los contratos electrónicos son aquellos acuerdos formados, transmitidos y ejecutados íntegramente mediante sistemas informáticos y que responden a las mismas funciones jurídicas que los contratos celebrados en soporte analógico (Zhang, Ronggang & Gao, Xiayuan , 2025).

Este capítulo tiene por finalidad establecer el marco conceptual y contextual de la contratación empresarial digital, mediante el examen de su evolución, definición, características, principales tipos y los retos que esta modalidad contractual plantea desde una óptica jurídica y empresarial. La expansión de las plataformas tecnológicas obliga a repensar la contratación empresarial como un fenómeno híbrido que combina normas tradicionales del derecho de contratos con principios y técnicas propias del comercio electrónico global.

La contratación empresarial en la era digital no puede comprenderse únicamente como una adaptación instrumental de los medios tecnológicos al derecho de contratos, sino como una transformación estructural de la forma en que las organizaciones generan, gestionan y protegen valor jurídico y económico. En efecto, la digitalización ha modificado los procesos internos de toma de decisiones empresariales, la velocidad de negociación y la manera en que se configuran las relaciones contractuales, desplazando el énfasis desde el soporte material hacia la gestión estratégica de la información y de los riesgos jurídicos asociados. En este escenario, la contratación digital se integra a la estrategia empresarial como un componente esencial de la competitividad, exigiendo marcos normativos que aseguren previsibilidad y confianza en las transacciones electrónicas (Bharadwaj et al. , 2013).

Desde una perspectiva jurídica, esta evolución plantea la necesidad de reinterpretar los fundamentos clásicos del derecho contractual a la luz de entornos caracterizados por la automatización, la deslocalización y la interconexión permanente. La manifestación del consentimiento, la atribución de la autoría contractual y la conservación de la prueba adquieren nuevas dimensiones cuando los contratos se celebran mediante sistemas digitales, plataformas electrónicas o infraestructuras tecnológicas complejas. La doctrina contemporánea ha señalado que el derecho debe adaptarse a estos cambios sin sacrificar la seguridad jurídica, garantizando que las nuevas formas de contratación cumplan funciones equivalentes a las tradicionales en términos de validez, eficacia y protección de las partes (Teece, 2018).

Asimismo, la contratación empresarial digital se desarrolla en un contexto de asimetrías tecnológicas y organizacionales que pueden incidir en el equilibrio contractual. Las empresas que cuentan con mayores capacidades digitales tienden a

imponer estándares contractuales y plataformas de contratación que condicionan la forma de expresión del consentimiento y la aceptación de cláusulas predispuestas. Ello obliga a examinar críticamente el impacto de la digitalización en la autonomía privada y en la asignación de riesgos contractuales, especialmente cuando se utilizan mecanismos electrónicos de firma como elementos centrales de vinculación jurídica. La literatura especializada ha destacado que la adecuada estructuración de los recursos jurídicos y tecnológicos resulta determinante para sostener ventajas competitivas y garantizar relaciones contractuales estables en el largo plazo (Barney, 1991).

1.1. Evolución de la contratación empresarial

La contratación empresarial ha sido históricamente uno de los principales instrumentos jurídicos para la organización de la actividad económica, permitiendo a las empresas estructurar relaciones de intercambio, cooperación y financiamiento en función de sus objetivos estratégicos. En su configuración clásica, la contratación se desarrolló bajo un paradigma eminentemente presencial, sustentado en la negociación directa entre las partes, la documentación escrita en soporte físico y la firma manuscrita como medio privilegiado de manifestación del consentimiento y de atribución de responsabilidad jurídica. Este modelo respondió a una realidad económica caracterizada por mercados geográficamente delimitados, tiempos de negociación prolongados y una menor complejidad tecnológica en la gestión empresarial (Porter, 2001).

Durante gran parte del siglo XX, el derecho de contratos empresariales se consolidó sobre la base de los principios tradicionales del derecho civil y mercantil, en particular la autonomía privada, la libertad contractual y la fuerza obligatoria del contrato. Estos principios permitieron una notable flexibilidad en la estructuración de acuerdos empresariales, pero al mismo tiempo reforzaron la centralidad del documento escrito como elemento de prueba y seguridad jurídica. La firma autógrafa cumplía funciones esenciales: identificaba al firmante, evidenciaba su voluntad de obligarse y garantizaba la integridad del contenido contractual. En este contexto, la contratación empresarial se encontraba estrechamente vinculada al soporte material y a la presencia física de las partes.

La progresiva incorporación de tecnologías de comunicación en los procesos empresariales marcó una primera fase de transformación de la contratación. Herramientas como el fax, el correo electrónico y los sistemas de intercambio electrónico de datos (EDI) comenzaron a utilizarse como medios auxiliares para la negociación y formalización de contratos. Si bien en un inicio estos instrumentos generaron dudas respecto de su valor jurídico, la doctrina y la práctica comercial fueron reconociendo su utilidad y legitimidad, siempre que permitieran identificar razonablemente a las partes y conservar evidencia del acuerdo alcanzado. Esta etapa transicional evidenció la capacidad del derecho contractual para adaptarse funcionalmente a nuevos medios sin alterar su estructura esencial (Chang O'Campo, 2000).

Con la expansión de Internet y el desarrollo de plataformas digitales, la contratación empresarial ingresó en una fase de transformación más profunda. Los contratos comenzaron a celebrarse íntegramente en entornos electrónicos, prescindiendo del soporte físico y de la firma manuscrita. La noción de contrato como documento tangible dio paso a una concepción basada en registros electrónicos, bases de datos y sistemas de gestión contractual digital. Este proceso de desmaterialización contractual implicó una redefinición de los mecanismos de formación del consentimiento, de conservación de la prueba y de imputación de obligaciones, planteando nuevos retos para el derecho (Soto Coaguila, 2002).

En el ámbito empresarial, esta evolución se vio acelerada por la necesidad de optimizar procesos, reducir costos de transacción y operar en mercados cada vez más globalizados. La contratación digital permitió a las empresas celebrar un gran volumen de contratos de manera rápida y estandarizada, utilizando formularios electrónicos, condiciones generales predispuestas y mecanismos de aceptación automatizada. Estas prácticas, si bien incrementaron la eficiencia operativa, también generaron riesgos jurídicos asociados a la asimetría informativa, la falta de negociación real y la posible afectación del equilibrio contractual, lo que ha motivado un creciente interés doctrinal por el análisis de la validez y eficacia de estos contratos (Bharadwaj et al. , 2013).

La internacionalización de la actividad empresarial constituye otro factor clave en la evolución de la contratación. La contratación electrónica ha permitido a las empresas

establecer relaciones jurídicas con contrapartes ubicadas en distintas jurisdicciones, lo que ha intensificado la necesidad de contar con reglas claras sobre el reconocimiento transfronterizo de los contratos y de los mecanismos de firma utilizados. En este contexto, la armonización normativa y la adopción de estándares internacionales se han convertido en elementos esenciales para garantizar la seguridad jurídica y la previsibilidad de las relaciones comerciales digitales (Mohiuddin, 2025).

Un elemento central en esta evolución es la progresiva incorporación de la firma electrónica como sustituto funcional de la firma manuscrita. La firma electrónica surge como respuesta a la necesidad de garantizar, en el entorno digital, las mismas funciones jurídicas que tradicionalmente cumplía la firma autógrafa: identificación del firmante, manifestación de voluntad y garantía de integridad del documento. Su desarrollo ha estado estrechamente vinculado al avance de las tecnologías criptográficas y a la creación de infraestructuras de certificación digital que permiten verificar la autenticidad y fiabilidad de las transacciones electrónicas (Teece, 2018).

En el contexto peruano, la evolución de la contratación empresarial ha sido acompañada por un proceso de modernización normativa orientado a reconocer la validez jurídica de los contratos celebrados por medios electrónicos y de las firmas digitales. Este proceso refleja la toma de conciencia del legislador respecto de la necesidad de adecuar el derecho a las nuevas realidades económicas y tecnológicas, garantizando al mismo tiempo la protección de los intereses empresariales y la seguridad jurídica del tráfico comercial. Así, la evolución de la contratación empresarial no puede entenderse únicamente como un fenómeno tecnológico, sino como una transformación jurídica estructural que redefine las bases mismas del derecho contractual en la era digital.

1.2. Concepto y características de los contratos electrónicos

El contrato electrónico constituye una de las manifestaciones más relevantes de la transformación digital del derecho contractual contemporáneo, especialmente en el ámbito empresarial. Desde una perspectiva jurídica, el contrato electrónico no representa una nueva categoría autónoma de contrato, sino una modalidad de

celebración del contrato tradicional, caracterizada por el uso de medios electrónicos, digitales o telemáticos para la formación del consentimiento, la expresión de la voluntad y, en muchos casos, la ejecución y conservación del acuerdo. En este sentido, la doctrina mayoritaria coincide en que los contratos electrónicos se rigen por los principios generales del derecho contractual, sin perjuicio de las particularidades derivadas del entorno tecnológico en el que se desarrollan (Soto Coaguila, 2002).

En términos conceptuales, puede definirse el contrato electrónico como aquel acuerdo de voluntades en el que la oferta, la aceptación o ambas se realizan mediante sistemas electrónicos de información, tales como plataformas digitales, redes informáticas o aplicaciones tecnológicas, generando un vínculo jurídico válido y exigible entre las partes. Esta definición pone de relieve que el elemento distintivo del contrato electrónico no radica en su contenido, sino en el medio utilizado para su celebración, lo que obliga a replantear categorías clásicas como la forma contractual, la prueba y la manifestación del consentimiento (Chang O'Campo, 2000).

Desde una perspectiva funcional, el contrato electrónico debe cumplir las mismas finalidades jurídicas que el contrato celebrado por medios tradicionales. En particular, debe permitir identificar a las partes, expresar de manera inequívoca su voluntad de obligarse, determinar el contenido de las obligaciones asumidas y garantizar la posibilidad de prueba del acuerdo en caso de controversia. La doctrina internacional ha señalado que el desafío central del contrato electrónico consiste en asegurar la equivalencia funcional entre los medios electrónicos y los tradicionales, de modo que la digitalización no debilite la seguridad jurídica ni la confianza en el tráfico comercial (UNCITRAL, 1999).

Una de las características fundamentales de los contratos electrónicos es la desmaterialización del soporte contractual. A diferencia del contrato tradicional, que se plasma en un documento físico, el contrato electrónico se materializa en registros digitales almacenados en sistemas informáticos. Esta desmaterialización implica que el contrato puede existir simultáneamente en múltiples soportes electrónicos y ser reproducido indefinidamente sin pérdida de contenido, lo que plantea interrogantes relevantes sobre la autenticidad, la integridad y la conservación de la prueba contractual (Teece, 2018).

Otra característica esencial es la celebración a distancia, ya que los contratos electrónicos suelen celebrarse sin la presencia física simultánea de las partes. Esta circunstancia adquiere especial relevancia en el ámbito empresarial, donde las relaciones contractuales se desarrollan frecuentemente entre sujetos ubicados en distintas jurisdicciones. La contratación a distancia refuerza la necesidad de mecanismos tecnológicos confiables que permitan identificar a las partes y verificar la validez del consentimiento, función que en el entorno digital es asumida principalmente por las firmas electrónicas (Bharadwaj et al. , 2013).

Asimismo, los contratos electrónicos se caracterizan por un elevado grado de automatización y estandarización. En la práctica empresarial, muchos contratos electrónicos se celebran mediante sistemas automatizados, formularios digitales o plataformas que incorporan condiciones generales predispuestas. Esta realidad incrementa la eficiencia de las operaciones comerciales, pero también plantea desafíos jurídicos relacionados con la transparencia, la información precontractual y el equilibrio contractual, especialmente cuando una de las partes se limita a aceptar condiciones previamente establecidas sin posibilidad real de negociación (Porter, 2001).

Desde el punto de vista probatorio, los contratos electrónicos presentan particularidades relevantes. La prueba del contrato ya no se sustenta en un documento físico firmado, sino en registros electrónicos cuya validez depende de su integridad, trazabilidad y posibilidad de verificación. En este contexto, la utilización de tecnologías como la firma electrónica avanzada o la firma digital basada en certificados digitales adquiere una importancia central, al permitir garantizar la autenticidad del firmante y la inalterabilidad del contenido contractual (Barney, 1991).

Finalmente, debe destacarse que los contratos electrónicos se desarrollan en un entorno normativo en constante evolución. La regulación de esta modalidad contractual responde a la necesidad de equilibrar la innovación tecnológica con la protección de los principios fundamentales del derecho contractual. En el ámbito empresarial, este equilibrio resulta crucial para fomentar la confianza en las transacciones electrónicas y asegurar que los contratos electrónicos produzcan plenamente sus efectos jurídicos. Así, el estudio del concepto y las características de los contratos electrónicos constituye un paso indispensable para comprender la validez y

eficacia jurídica de las firmas electrónicas en las operaciones comerciales contemporáneas.

1.3. Tipos de contratos empresariales celebrados por medios digitales

La contratación empresarial celebrada por medios digitales no constituye un fenómeno homogéneo, sino que abarca una pluralidad de tipologías contractuales que responden a la diversidad de actividades económicas desarrolladas por las empresas en la era digital. La utilización de medios electrónicos para la celebración de contratos ha permitido trasladar al entorno digital prácticamente todas las categorías contractuales tradicionales, al mismo tiempo que ha dado lugar a nuevas modalidades contractuales directamente vinculadas a los modelos de negocio digitales. En este contexto, la clasificación de los contratos empresariales digitales resulta esencial para comprender los riesgos jurídicos asociados, el rol de las firmas electrónicas y la eficacia de los mecanismos de vinculación contractual (Bharadwaj et al. , 2013).

1.3.1. Contratos de compraventa y suministro celebrados electrónicamente

Uno de los tipos más frecuentes de contratos empresariales celebrados por medios digitales es el contrato de compraventa, particularmente en el ámbito del comercio electrónico entre empresas (B2B). En estos contratos, la oferta, la aceptación y la determinación de las condiciones esenciales —precio, cantidad, plazos de entrega— se realizan a través de plataformas electrónicas, portales empresariales o sistemas de gestión integrados. La digitalización de la compraventa permite automatizar procesos de aprovisionamiento, reducir costos de transacción y optimizar la cadena de suministro, pero exige mecanismos confiables de identificación de las partes y de prueba del consentimiento (Mohiuddin, 2025).

Una modalidad estrechamente relacionada es el contrato de suministro celebrado por medios digitales, utilizado de manera recurrente en relaciones comerciales de tracto sucesivo. En estos casos, las empresas emplean plataformas electrónicas para gestionar pedidos periódicos, modificar volúmenes de suministro y formalizar

renovaciones contractuales. Por ejemplo, una empresa industrial puede suscribir electrónicamente un contrato marco de suministro con un proveedor internacional, utilizando firmas electrónicas para validar cada orden de compra derivada del contrato principal. Este tipo de contratación evidencia la importancia de garantizar la integridad de los documentos electrónicos y la trazabilidad de las operaciones contractuales.

1.3.2. Contratos de prestación de servicios empresariales digitales

Otro grupo relevante lo constituyen los contratos de prestación de servicios celebrados por medios digitales. Estos abarcan desde servicios profesionales tradicionales —consultoría, asesoría legal o contable— hasta servicios altamente especializados vinculados a la economía digital, como desarrollo de software, análisis de datos o servicios en la nube. En estos contratos, la digitalización no solo afecta la forma de celebración, sino también la ejecución misma del contrato, que se realiza frecuentemente a través de plataformas tecnológicas (Teece, 2018).

Un ejemplo representativo es el contrato de servicios de computación en la nube (cloud computing), en el cual una empresa contrata electrónicamente el acceso a infraestructura, plataformas o software proporcionados por un tercero. Estos contratos suelen estructurarse mediante condiciones generales aceptadas digitalmente y complementadas por acuerdos de nivel de servicio (SLA). La utilización de medios digitales plantea desafíos jurídicos específicos, como la determinación de la ley aplicable, la protección de datos y la asignación de responsabilidades en caso de fallas del servicio, lo que refuerza la necesidad de mecanismos de firma electrónica robustos y confiables (Porter & Heppelmann, How Smart, Connected Products Are Transforming Competition, 2014).

1.3.3. Contratos de distribución, agencia y representación comercial digitales

La contratación empresarial digital también se extiende a contratos de distribución, agencia y representación comercial. En estos casos, las empresas utilizan medios electrónicos para formalizar relaciones de colaboración orientadas a la

comercialización de bienes o servicios en mercados determinados. La celebración digital de estos contratos facilita la expansión internacional de las empresas y la gestión centralizada de redes de distribución, pero introduce complejidades adicionales en materia de control contractual y cumplimiento normativo (Deng at al., 2018).

Por ejemplo, una empresa tecnológica puede celebrar electrónicamente contratos de distribución con socios comerciales ubicados en distintos países, utilizando plataformas digitales para la firma, modificación y renovación de los acuerdos. Esta práctica exige especial atención a la validez de las firmas electrónicas utilizadas y a su reconocimiento transfronterizo, dado que la eficacia jurídica del contrato dependerá de la aceptación de dichos mecanismos en las jurisdicciones involucradas.

1.3.4. Contratos marco y acuerdos empresariales complejos en entornos digitales

Los contratos marco y los acuerdos empresariales complejos constituyen otra categoría relevante dentro de la contratación digital. Estos contratos establecen las condiciones generales que regirán una serie de operaciones futuras, las cuales se concretan posteriormente mediante actos electrónicos específicos. La digitalización permite a las empresas gestionar estos acuerdos de manera dinámica, incorporando modificaciones, adendas y renovaciones sin necesidad de recurrir a documentación física (Barney, 1991).

Un ejemplo típico es el contrato marco de colaboración empresarial celebrado electrónicamente entre dos corporaciones para el desarrollo conjunto de proyectos tecnológicos. A partir de este contrato, las partes pueden formalizar electrónicamente acuerdos específicos, órdenes de servicio o anexos técnicos, utilizando firmas electrónicas para cada acto jurídico. Este tipo de contratación pone de relieve la importancia de la coherencia entre los distintos documentos electrónicos y la necesidad de sistemas de gestión contractual que garanticen la integridad y autenticidad de cada elemento del acuerdo.

1.3.5. Contratos empresariales propios de la economía digital

Finalmente, la contratación empresarial digital incluye contratos que no tienen un equivalente directo en el entorno tradicional, sino que surgen como consecuencia de los nuevos modelos de negocio digitales. Entre estos se encuentran los contratos de licenciamiento de software, los acuerdos de uso de plataformas digitales, los contratos de marketplace y los acuerdos de procesamiento de datos. Estos contratos suelen celebrarse de manera íntegramente electrónica y se caracterizan por un alto grado de estandarización y automatización (Westerman, G. et al., 2014)

Por ejemplo, una empresa que opera como marketplace digital suscribe electrónicamente contratos con vendedores y proveedores de servicios logísticos, estableciendo condiciones uniformes aceptadas mediante firma electrónica o mecanismos equivalentes. La eficacia jurídica de estos contratos resulta esencial para la sostenibilidad del modelo de negocio, lo que explica el creciente interés doctrinal y normativo en la regulación de la contratación digital empresarial y de las firmas electrónicas utilizadas en este contexto (Bharadwaj et al. , 2013).

En conjunto, la diversidad de contratos empresariales celebrados por medios digitales evidencia que la digitalización no se limita a reproducir esquemas contractuales tradicionales, sino que transforma profundamente la manera en que las empresas estructuran sus relaciones jurídicas. Esta realidad refuerza la necesidad de analizar la validez y eficacia jurídica de las firmas electrónicas como elemento central de la contratación empresarial en la era digital.

1.4. Ventajas y riesgos de la contratación digital

La contratación digital se ha consolidado como uno de los pilares fundamentales de la actividad empresarial contemporánea, al ofrecer soluciones eficientes frente a las exigencias de rapidez, escalabilidad y competitividad propias de la economía digital. Desde una perspectiva jurídica y económica, las ventajas de esta modalidad contractual son evidentes, aunque no exentas de riesgos que deben ser cuidadosamente gestionados para preservar la seguridad jurídica y la confianza en las relaciones comerciales. El análisis equilibrado de estas ventajas y riesgos resulta esencial para

comprender el alcance real de la contratación digital y el papel central que desempeñan las firmas electrónicas en la mitigación de las amenazas asociadas (Bharadwaj et al. , 2013).

1.4.1. Ventajas de la contratación digital en el ámbito empresarial

Una de las principales ventajas de la contratación digital es la reducción significativa de los costos de transacción. La eliminación del soporte físico, del traslado de documentos y de la necesidad de reuniones presenciales permite a las empresas optimizar recursos financieros y humanos. Por ejemplo, una corporación multinacional puede celebrar contratos de suministro con proveedores ubicados en distintos países mediante plataformas electrónicas, reduciendo drásticamente los tiempos y costos asociados a la formalización contractual tradicional (OCDE, 2019).

Asimismo, la contratación digital incrementa notablemente la rapidez y eficiencia en la celebración de contratos. Los procesos de oferta y aceptación pueden completarse en cuestión de minutos, lo que resulta especialmente relevante en mercados altamente dinámicos. Esta agilidad contractual permite a las empresas responder con mayor rapidez a oportunidades comerciales y adaptarse a cambios en las condiciones del mercado, integrando la contratación digital como un elemento estratégico de su modelo de negocio (Teece, 2018).

Otra ventaja relevante es la facilitación de la contratación transfronteriza. Los medios digitales eliminan barreras geográficas y temporales, permitiendo a las empresas operar en mercados globales sin necesidad de presencia física. Por ejemplo, una empresa peruana puede celebrar electrónicamente contratos de prestación de servicios tecnológicos con clientes europeos o asiáticos, utilizando firmas electrónicas reconocidas internacionalmente. Esta posibilidad amplía el alcance de las operaciones empresariales y fomenta la internacionalización, aunque exige un adecuado marco normativo para garantizar el reconocimiento jurídico de los contratos (Porter, Strategy and the Internet, 2001).

Desde el punto de vista organizacional, la contratación digital contribuye a una mejor gestión y trazabilidad documental. Los contratos electrónicos pueden almacenarse,

clasificarse y recuperarse fácilmente mediante sistemas de gestión documental, lo que facilita el cumplimiento normativo y la auditoría interna. Además, la digitalización permite integrar los contratos con otros sistemas empresariales, como los de contabilidad o logística, generando sinergias que incrementan la eficiencia operativa (Westerman, G. et al., 2014).

1.4.2. Riesgos jurídicos y tecnológicos de la contratación digital

Pese a sus ventajas, la contratación digital conlleva riesgos significativos que no pueden ser ignorados. Uno de los principales riesgos es la incertidumbre respecto de la identificación de las partes. En ausencia de mecanismos adecuados de autenticación, resulta posible que una de las partes cuestione la autoría de un contrato electrónico o alegue suplantación de identidad. Este riesgo adquiere especial relevancia en contratos empresariales de alto valor económico, donde la falta de certeza sobre el firmante puede generar litigios complejos (Barney, 1991).

Otro riesgo importante es la vulnerabilidad de la integridad del documento electrónico. A diferencia del documento físico, el documento digital puede ser alterado sin dejar huellas visibles si no se utilizan mecanismos tecnológicos adecuados. La posibilidad de modificaciones no autorizadas compromete la fuerza probatoria del contrato y la confianza en la contratación digital. En este contexto, el uso de firmas electrónicas avanzadas o digitales, basadas en criptografía y certificados digitales, resulta esencial para garantizar la inalterabilidad del contenido contractual (Teece, 2018).

La contratación digital también presenta riesgos asociados a la asimetría informativa y al desequilibrio contractual, especialmente cuando se utilizan contratos electrónicos predispuestos. En muchos casos, una de las partes —generalmente la empresa con mayor poder tecnológico— impone condiciones generales aceptadas mediante un simple clic, sin posibilidad real de negociación. Este fenómeno plantea interrogantes sobre la validez del consentimiento y la protección de la parte más débil, incluso en relaciones empresariales, lo que ha motivado un creciente interés doctrinal por el análisis del equilibrio contractual en entornos digitales (Bharadwaj et al. , 2013).

Finalmente, deben considerarse los riesgos de seguridad informática y protección de datos. Los contratos electrónicos suelen contener información sensible, cuya

exposición o pérdida puede generar consecuencias económicas y legales significativas. Ataques informáticos, fallas de los sistemas o accesos no autorizados pueden comprometer la confidencialidad de los contratos y la responsabilidad de las empresas involucradas. Por ejemplo, una brecha de seguridad en una plataforma de contratación digital puede derivar en la divulgación de acuerdos comerciales estratégicos, afectando la competitividad empresarial y dando lugar a responsabilidades legales (OCDE, 2019).

En síntesis, la contratación digital ofrece ventajas sustanciales en términos de eficiencia, alcance y gestión empresarial, pero también introduce riesgos que exigen una respuesta jurídica y tecnológica adecuada. El equilibrio entre innovación y seguridad jurídica constituye el principal desafío de la contratación digital empresarial, y es en este punto donde la regulación de las firmas electrónicas adquiere una relevancia central como instrumento para garantizar la validez, eficacia y confianza en las relaciones contractuales digitales.

1.5. Uso de firmas electrónicas en la empresa privada

El uso de firmas electrónicas en la empresa privada peruana encuentra su fundamento jurídico directo en la Ley N.º 27269 – Ley de Firmas y Certificados Digitales, cuyo artículo 1 establece expresamente que su objeto es "regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que la firma manuscrita u otra análoga que conlleve manifestación de voluntad". Este reconocimiento legal constituye la base sobre la cual las empresas pueden sustituir válidamente la firma tradicional por mecanismos electrónicos en sus relaciones jurídicas internas y externas.

El artículo 2 de la Ley define la firma electrónica como cualquier símbolo basado en medios electrónicos que pueda vincular e identificar al firmante y garantizar la autenticación e integridad del documento electrónico. Esta definición amplia habilita a la empresa privada a emplear diversos tipos de firmas electrónicas, siempre que cumplan dichas funciones jurídicas esenciales: identificación, vinculación y preservación del contenido contractual.

Asimismo, el artículo 3 introduce la firma digital como una especie de firma electrónica que utiliza criptografía asimétrica, diferenciándola por su mayor nivel de seguridad

técnica y jurídica. Esta distinción es clave para la empresa privada, ya que permite seleccionar el tipo de firma adecuado según el nivel de riesgo de la operación contractual.

En el ámbito de la contratación interna, la empresa privada puede utilizar firmas electrónicas para formalizar contratos laborales, adendas, pactos de confidencialidad, reglamentos internos y resoluciones corporativas. Conforme al artículo 4 de la Ley N.º 27269, la firma digital tiene la misma eficacia jurídica que la firma manuscrita, por lo que los documentos internos firmados digitalmente producen efectos jurídicos plenos y obligatorios.

Por ejemplo, una empresa puede celebrar contratos de trabajo a distancia mediante firma digital, garantizando la identificación del trabajador y la integridad del contenido contractual. En estos casos, el consentimiento laboral se manifiesta electrónicamente sin afectar su validez, siempre que se respete el marco legal laboral y se garantice el acceso del trabajador al documento firmado.

El Reglamento de la Ley (D.S. N.º 052-2008-PCM) refuerza esta posibilidad al establecer que los documentos electrónicos firmados digitalmente pueden almacenarse y conservarse electrónicamente, siempre que se mantengan las condiciones de integridad, accesibilidad y disponibilidad (Perú, 2008, arts. 25–28). Esto permite a las empresas implementar sistemas de archivo digital corporativo con plena validez legal.

El uso de firmas electrónicas en la empresa privada también impacta directamente en el gobierno corporativo. Actas de directorio, acuerdos de junta general, decisiones del consejo de administración y autorizaciones internas pueden ser firmadas electrónicamente, reforzando la trazabilidad de las decisiones y la responsabilidad de los firmantes.

El artículo 6 de la Ley N.º 27269 dispone que la firma digital permite identificar al firmante y detectar cualquier modificación ulterior del documento. Esta característica resulta esencial en el ámbito corporativo, donde la integridad documental es

fundamental para auditorías, fiscalizaciones y eventuales procesos judiciales o arbitrales.

En las relaciones con proveedores, la empresa privada puede emplear firmas electrónicas para celebrar contratos de suministro, contratos de prestación de servicios, acuerdos marco y órdenes de compra. Conforme al artículo 7 de la Ley, los documentos electrónicos firmados digitalmente tienen valor probatorio, lo que permite acreditar la existencia del contrato, su contenido y la identidad del firmante.

Por ejemplo, una empresa industrial puede suscribir digitalmente contratos de abastecimiento con proveedores nacionales o extranjeros. En caso de controversia, el documento electrónico firmado digitalmente constituye prueba documental válida, equiparable a un contrato privado tradicional.

El artículo 11 de la Ley N.º 27269 reviste especial importancia en operaciones transfronterizas, al disponer que los certificados digitales emitidos por entidades extranjeras pueden ser reconocidos en el Perú, siempre que cumplan los requisitos establecidos por la autoridad administrativa competente. Esta disposición facilita la contratación internacional de las empresas peruanas.

En las relaciones con clientes, la firma electrónica permite formalizar contratos de adhesión, acuerdos de servicios, contratos financieros y suscripciones digitales. La validez de estos contratos se sustenta en el principio de equivalencia funcional recogido en el artículo 1 de la Ley, complementado por la exigencia de identificación y autenticación del firmante establecido en el artículo 2.

En sectores como el financiero, inmobiliario o de telecomunicaciones, la firma digital permite celebrar contratos sin presencia física, reduciendo costos operativos y mejorando la experiencia del cliente, sin sacrificar seguridad jurídica.

No obstante, el uso de firmas electrónicas en contratos con clientes exige respetar las normas de protección al consumidor y garantizar que el consentimiento sea informado, libre y verificable, lo cual se logra mediante interfaces claras y sistemas de auditoría electrónica.

La Ley N.º 27269 regula la Infraestructura Oficial de Firma Electrónica (IOFE), integrada por entidades de certificación y entidades de registro o verificación (arts. 12 y 13). Si bien estas entidades no forman parte de la empresa privada, su actuación es esencial para garantizar la validez de las firmas digitales utilizadas por las empresas.

El Reglamento detalla las obligaciones de estas entidades, incluyendo la emisión, suspensión y revocación de certificados digitales, así como la gestión segura de la información. La empresa privada, al utilizar firmas digitales, debe verificar que los certificados provengan de entidades debidamente acreditadas.

La Ley reconoce que los documentos electrónicos firmados digitalmente tienen eficacia probatoria, siempre que se garantice su integridad y autenticidad. El Reglamento establece reglas específicas sobre conservación, acceso y verificación, lo que permite a la empresa privada implementar sistemas de gestión documental plenamente válidos ante autoridades administrativas y judiciales.

Esta regulación refuerza la seguridad jurídica de la contratación empresarial digital, al reducir la posibilidad de impugnaciones basadas en la forma del contrato o en la supuesta inexistencia del consentimiento.

En conclusión, el uso de firmas electrónicas en la empresa privada peruana no solo es jurídicamente válido, sino expresamente promovido por la Ley N.º 27269 y su Reglamento. La normativa reconoce la equivalencia funcional de la firma electrónica y digital, regula su infraestructura técnica y atribuye valor probatorio pleno a los documentos electrónicos firmados conforme a ley.

1.6. Plataformas digitales y proveedores de firma electrónica

En la economía digital actual, las plataformas de firma electrónica y los proveedores tecnológicos se han convertido en elementos estructurales para la transformación de los procesos empresariales. En el Perú, esta transformación tiene un componente legal sólido, dado que la Ley N.º 27269 y su Reglamento reconocen la validez y eficacia jurídica de las firmas electrónicas y digitales, siempre que se generen bajo los estándares técnicos y de certificación establecidos por la norma.

La normativa peruana permite que empresas privadas utilicen tanto firmas electrónicas simples y avanzadas como firmas digitales con certificado digital cualificado. Este último tipo es el que actualmente ofrecen muchas de las soluciones tecnológicas que analizan a continuación, ya que garantiza integridad, autenticación y no repudio conformes a los requisitos técnicos aceptados en mercados globales.

La oferta de plataformas tecnológicas en el Perú converge en dos grandes modelos: soluciones locales adaptadas al contexto peruano, y plataformas globales con acreditación local. Ambos modelos responden a las necesidades de firmas en procesos empresariales internos (contratos, aprobaciones, autorizaciones) y externos (acuerdos con clientes y proveedores), bajo la regulación establecida en la Ley.

Acepta (Acepta.com) es una de las plataformas más conocidas en el mercado peruano para la provisión de certificados digitales y firma electrónica con valor legal. Ofrece la posibilidad de firmar documentos PDF y XML con certificados digitales aptos para contratos, boletas u otros instrumentos legales, totalmente compatibles con el marco legal peruano e incluso con sistemas de facturación electrónica integrados a SUNAT.

La solución de Acepta es particularmente útil para PYMEs que desean una experiencia self-service de firma digital, con certificados válidos por períodos de uno a tres años y compatibilidad con sistemas empresariales de gestión documental.

Intellisign, por su parte, representa otro caso de plataforma adoptada por organizaciones tanto medianas como grandes. Esta solución facilita la firma electrónica y digital de documentos en lotes, la gestión de flujos de trabajo con múltiples firmantes y la integración con múltiples perfiles de empresa, lo que resulta en una herramienta flexible para la contratación empresarial digital.

Intellisign ha sido adoptada por organizaciones como COVIPERÚ, lo que permite gestionar autorizaciones, acuerdos y contratos digitales en procesos internos y con terceros, reduciendo tiempos de aprobación y costos logísticos asociados a la gestión documental física.

Asimismo, EvidenSIGN ofrece una plataforma enfocada no solo en firma electrónica, sino también en validación de identidad y notificaciones certificadas por correo electrónico, funcionalidades que resultan estratégicas cuando una empresa busca

establecer flujos de contratación digital con clientes y proveedores sin intermediación física.

Algunas empresas globales han ingresado al mercado peruano mediante acreditación directa en Perú. Un ejemplo notable es GlobalSign, quien se convirtió en una Autoridad Certificadora acreditada por INDECOPI, permitiendo que empresas peruanas adquieran certificados con reconocimiento automático en herramientas de firma común (como Adobe Acrobat o Reader), lo cual facilita la interoperabilidad global y la confianza jurídica en documentos firmados digitalmente.

Esta opción internacional resulta atractiva para empresas con operaciones transfronterizas o con necesidad de interoperar con plataformas globales, pues los certificados se adhieren al Adobe Approved Trust List (AATL), lo que garantiza que las firmas digitales sean automáticamente válidas en entornos corporativos internacionales.

Plataformas globales ampliamente utilizadas, aunque no siempre específicas del mercado peruano, como DocuSign, también ofrecen soluciones de firma electrónica que pueden integrarse con sistemas empresariales y aplicaciones de gestión documental (ERP/CRM), facilitando la firma de contratos, acuerdos y órdenes de compra desde cualquier dispositivo.

En la práctica empresarial, la selección de una plataforma o proveedor de firma electrónica está estrechamente ligada a la capacidad de integración con sistemas existentes de la empresa. Esto incluye la integración con sistemas de gestión documental, flujos de aprobación automatizados, ERPs y herramientas de colaboración interna.

Para empresas que buscan automatizar procesos de múltiples pasos (ej. aprobación interna, firma de acuerdos con proveedores y luego con clientes), plataformas que soportan API, flujos de firma automatizados y firmantes múltiples son preferidas. Ejemplos de este enfoque son tanto soluciones locales como Intellisign o EvidenSIGN, que permiten la configuración de procesos complejos sin intervención manual constante.

La integración con plataformas de notificación y comunicación —por ejemplo, flujos que combinan firma electrónica y notificaciones certificadas— permite a las empresas disponer de trazabilidad completa del ciclo de vida de un documento, desde su emisión hasta su aceptación y archivo, eliminando puntos de falla tradicionales como el correo físico o las firmas presenciales.

Todas estas soluciones se apoyan en la legalidad de las firmas electrónicas y digitales en el Perú, la cual está consagrada en la Ley N.º 27269 y su Reglamento. De acuerdo con esta regulación, los documentos firmados digitalmente son válidos y exigibles legalmente siempre que se pueda demostrar la expresión de voluntad de las partes y que la ley no exige formalidad distinta para el contrato.

La existencia de proveedores acreditados por INDECOPI (como GlobalSign, Llama.pe o Bit4id como prestador de firma remota) permite que las empresas elijan entre soluciones con distintos niveles de integración, seguridad y reconocimiento internacional, según sus necesidades.

En algunos casos, las plataformas están adoptando avances tecnológicos como blockchain o sellado de tiempo distribuido, mecanismos que agregan valor para empresas que requieren niveles adicionales de trazabilidad o certificación temporal de documentos. Aunque estos mecanismos aún no son masivos en el Perú, se están incorporando gradualmente en soluciones avanzadas.

La integración con módulos móviles también responde a la demanda de trabajadores remotos y equipos dispersos geográficamente, permitiendo que un director o gerente firme documentos desde su dispositivo móvil sin pérdida de seguridad ni cumplimiento legal.

La elección de un proveedor o plataforma de firma electrónica no debe basarse únicamente en la facilidad de uso o costo, sino también en la seguridad jurídica y técnica que ofrece, especialmente en contextos empresariales en los que los documentos firmados pueden ser objeto de disputas judiciales o arbitrales.

La adhesión a estándares criptográficos sólidos (por ejemplo, X.509 para certificados digitales) y la gestión de claves privadas bajo políticas robustas de seguridad son aspectos clave para garantizar que las firmas sean admisibles como prueba ante terceros, conforme a la regulación local.

Como ejemplos de uso corporativo tenemos:

- Una empresa minera con operaciones nacionales e internacionales puede utilizar un proveedor global como GlobalSign para emitir certificados digitales que son igualmente válidos en Perú, Chile y otros países, facilitando la firma de contratos de suministro, ingeniería y servicios sin plazos ni locaciones físicas.
- Una firma de servicios profesionales puede implementar Intellisign para automatizar la firma de acuerdos de confidencialidad (NDAs), contratos con clientes y autorizaciones internas de proyectos, integrando la plataforma con su gestor de proyectos y CRM para lograr eficiencia y trazabilidad.
- Una empresa de retail puede adoptar EvidenSIGN para combinar firma electrónica con notificaciones certificadas, logrando que proveedores, clientes y auditores tengan acceso seguro y verificable a todos los documentos contractuales y operativos generados digitalmente.

A pesar de las herramientas disponibles, existen desafíos en la adopción plena de firmas electrónicas en el mercado peruano, como la interoperabilidad entre distintas soluciones tecnológicas o la unificación de estándares empresariales para firmas remotas en plataformas híbridas.

Sin embargo, la madurez regulatoria (Ley N.º 27269 y su Reglamento) y la entrada de jugadores globales acreditados incrementan la oferta tecnológica, permitiendo que las empresas peruanas seleccionen soluciones que se ajusten a su tamaño, sector y requerimientos de seguridad legal, funcionalidad técnica y escalabilidad.

Capítulo II

Marco conceptual: firma electrónica vs firma digital

CAPÍTULO II

MARCO CONCEPTUAL: FIRMA ELECTRÓNICA VS. FIRMA DIGITAL

La consolidación de la contratación empresarial en entornos digitales ha situado a la firma electrónica y a la firma digital en el centro del debate jurídico contemporáneo. En la medida en que los contratos electrónicos prescinden del soporte físico y de la presencia simultánea de las partes, surge la necesidad de contar con mecanismos jurídicos y tecnológicos capaces de garantizar la autenticidad del firmante, la integridad del documento y la manifestación válida del consentimiento. En este contexto, la firma electrónica se erige como el principal instrumento de vinculación jurídica en el tráfico comercial digital, cumpliendo funciones equivalentes —aunque no idénticas— a las tradicionalmente atribuidas a la firma manuscrita (Soto Coaguila, 2002).

Desde una perspectiva dogmática, la firma no constituye un mero elemento formal, sino un mecanismo jurídico de imputación de voluntad y de responsabilidad. En el derecho contractual clásico, la firma manuscrita permite identificar al autor del documento, exteriorizar su intención de obligarse y asegurar la integridad del contenido firmado. La transición hacia entornos digitales ha obligado a replantear estas funciones esenciales, adaptándolas a un contexto tecnológico caracterizado por la desmaterialización del documento, la automatización de los procesos y la celebración de contratos a distancia. En este proceso de adaptación, la doctrina ha desarrollado el principio de equivalencia funcional, según el cual los medios electrónicos pueden cumplir las mismas funciones jurídicas que los medios tradicionales, siempre que ofrezcan garantías equivalentes de fiabilidad y seguridad (UNCITRAL, 1999).

La firma electrónica, entendida en sentido amplio, engloba un conjunto heterogéneo de mecanismos tecnológicos utilizados para identificar al firmante y vincularlo con un documento electrónico. Esta amplitud conceptual ha dado lugar a diversas clasificaciones doctrinales y normativas, que distinguen entre firmas electrónicas simples, avanzadas y firmas digitales basadas en certificados digitales. Cada una de estas modalidades presenta distintos niveles de seguridad y confiabilidad, lo que incide directamente en su eficacia jurídica y en su valor probatorio en el ámbito empresarial

(Chang O'Campo, 2000). Así, no todas las firmas electrónicas ofrecen el mismo grado de protección frente a riesgos como la suplantación de identidad o la alteración del documento.

En el ámbito empresarial, la utilización de firmas electrónicas responde a necesidades prácticas concretas. Por ejemplo, una empresa que celebra contratos de suministro de manera recurrente puede optar por mecanismos de firma electrónica avanzada para agilizar sus operaciones, mientras que en contratos de alto valor económico o con implicancias transfronterizas puede resultar indispensable el uso de firmas digitales sustentadas en infraestructuras de certificación reconocidas. Estos ejemplos evidencian que la elección del tipo de firma electrónica no es una cuestión meramente técnica, sino una decisión estratégica con relevantes consecuencias jurídicas (Bharadwaj et al. , 2013).

La firma digital, como categoría específica dentro del género de la firma electrónica, merece un análisis particularizado. A diferencia de otras formas de firma electrónica, la firma digital se basa en técnicas criptográficas de clave pública y en el uso de certificados digitales emitidos por entidades de certificación acreditadas. Este modelo permite verificar de manera objetiva la identidad del firmante y detectar cualquier alteración posterior del documento firmado, lo que explica su especial reconocimiento jurídico en numerosos ordenamientos, incluido el peruano. Desde el punto de vista doctrinal, la firma digital representa el máximo nivel de seguridad técnica y jurídica disponible en la actualidad para la contratación electrónica (Teece, 2018).

La relevancia de la firma electrónica y digital se intensifica en un contexto de creciente internacionalización de las relaciones comerciales. Las empresas operan cada vez más en mercados globales, celebrando contratos con contrapartes sujetas a distintos sistemas jurídicos. En este escenario, la confianza en los mecanismos de firma electrónica se convierte en un factor determinante para la eficacia transfronteriza de los contratos. La armonización normativa y la adopción de estándares internacionales en materia de firma electrónica buscan precisamente facilitar el reconocimiento mutuo de estos mecanismos y reducir la incertidumbre jurídica asociada a la contratación digital (OCDE, 2019).

Finalmente, el análisis de la firma electrónica y la firma digital no puede limitarse a una dimensión puramente normativa o tecnológica. Resulta indispensable examinar su aplicación práctica en el ámbito empresarial, considerando los riesgos, beneficios y desafíos que plantea su utilización en operaciones comerciales concretas. La adecuada comprensión de estas figuras permitirá evaluar su capacidad real para garantizar la seguridad jurídica de los contratos empresariales digitales y servirá de base para el análisis del marco normativo peruano que regula su validez y eficacia. Este capítulo, por tanto, se orienta a establecer los fundamentos conceptuales necesarios para comprender el rol central de la firma electrónica y la firma digital en la contratación empresarial contemporánea.

2.1. Concepto de la firma electrónica

La firma electrónica constituye uno de los conceptos jurídicos más relevantes y complejos del derecho de la contratación digital contemporánea. Su importancia no radica únicamente en su función técnica como mecanismo de identificación, sino en su capacidad para cumplir las funciones jurídicas esenciales tradicionalmente atribuidas a la firma manuscrita: identificación del autor, manifestación de voluntad, vinculación jurídica y atribución de responsabilidad. En este sentido, la firma electrónica debe ser comprendida como una categoría jurídico-funcional antes que como un simple instrumento tecnológico (Cordero Mendoza, 2024).

Desde una perspectiva conceptual amplia, la firma electrónica puede definirse como cualquier conjunto de datos electrónicos asociados a un mensaje de datos que permiten identificar al firmante y expresar su intención de aprobar el contenido del documento. Esta definición, adoptada por numerosos instrumentos internacionales y legislaciones nacionales, evidencia el carácter tecnológicamente neutro del concepto, permitiendo su adaptación a distintas soluciones técnicas sin comprometer su eficacia jurídica (UNCITRAL, 1999). Así, la firma electrónica no se identifica con una tecnología específica, sino con la función jurídica que cumple dentro del acto contractual.

La doctrina especializada ha subrayado que el elemento central de la firma electrónica no es la forma, sino la función de imputación de voluntad. En efecto, una firma

electrónica será jurídicamente relevante en la medida en que permita atribuir razonablemente el acto a una persona determinada y demostrar que dicha persona consintió el contenido del documento electrónico. Esta concepción funcional supera visiones formalistas y resulta especialmente adecuada para entornos empresariales caracterizados por la automatización y la estandarización contractual (Moreno Navarrete, 2017).

Desde el punto de vista normativo comparado, el concepto de firma electrónica ha sido desarrollado bajo el principio de equivalencia funcional, conforme al cual los requisitos legales de una firma manuscrita pueden considerarse cumplidos mediante una firma electrónica si esta ofrece garantías equivalentes de fiabilidad. Este principio, recogido en instrumentos como la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, ha influido decisivamente en la regulación de la firma electrónica en América Latina y Europa, incluyendo el reconocimiento de distintos niveles de firma electrónica según su grado de seguridad (UNCITRAL, 1999).

En el ámbito empresarial, la firma electrónica cumple un rol estratégico al facilitar la celebración masiva de contratos sin sacrificar seguridad jurídica. Por ejemplo, una empresa que utiliza una plataforma digital para la contratación de servicios puede emplear mecanismos de firma electrónica basados en credenciales de acceso y registros de auditoría para vincular jurídicamente a sus clientes. Aunque estos mecanismos no siempre alcanzan el nivel de una firma digital criptográfica, pueden ser suficientes para acreditar el consentimiento en contratos de bajo riesgo económico, siempre que se cumplan estándares razonables de fiabilidad (Selvia, 2023).

No obstante, la amplitud conceptual de la firma electrónica también genera desafíos interpretativos. Uno de los principales debates doctrinales se centra en la distinción entre firma electrónica y otros mecanismos de autenticación, como contraseñas o códigos de verificación. Si bien estos mecanismos pueden cumplir funciones técnicas similares, no todos ellos alcanzan automáticamente la categoría de firma electrónica desde un punto de vista jurídico. La clave reside en determinar si el mecanismo utilizado permite identificar al firmante y vincularlo inequívocamente con el acto jurídico celebrado (Riega Virú et al., 2021).

Asimismo, la firma electrónica debe analizarse en relación con su valor probatorio. En procesos judiciales o arbitrales, la eficacia de una firma electrónica dependerá de su capacidad para demostrar autenticidad e integridad del documento. La doctrina ha señalado que, si bien toda firma electrónica puede ser válida como manifestación de voluntad, no todas ofrecen el mismo nivel de fuerza probatoria. Este aspecto resulta especialmente relevante en contratos empresariales complejos, donde la prueba del consentimiento y del contenido contractual adquiere una importancia decisiva (Mejía Fernández, 2023).

En síntesis, el concepto de firma electrónica se articula como una noción flexible y funcional, diseñada para responder a las exigencias de la contratación digital sin quedar obsoleta frente a la evolución tecnológica. Su correcta comprensión resulta indispensable para analizar posteriormente las distintas clases de firma electrónica, su regulación jurídica y, en particular, el rol de la firma digital como mecanismo reforzado de seguridad jurídica en la contratación empresarial.

2.2. Tipos de firmas electrónicas

La firma electrónica, como categoría jurídica amplia, no constituye una figura homogénea, sino que engloba diversas modalidades con distintos niveles de seguridad, fiabilidad técnica y eficacia jurídica. La necesidad de clasificar los tipos de firmas electrónicas surge de la constatación de que no todos los mecanismos utilizados para manifestar el consentimiento en entornos digitales ofrecen las mismas garantías desde el punto de vista de la autenticidad del firmante, la integridad del documento y la posibilidad de repudio. En consecuencia, tanto la doctrina como la normativa comparada han desarrollado tipologías que permiten diferenciar las firmas electrónicas según su grado de sofisticación tecnológica y su valor jurídico (Muñoz-Mendoza et al., 2017).

Desde una perspectiva funcional, esta clasificación responde a un criterio de gradualidad en la seguridad jurídica. A mayor nivel de garantías técnicas, mayor será la presunción de validez y eficacia jurídica de la firma electrónica. Esta lógica resulta especialmente relevante en el ámbito empresarial, donde la elección del tipo de firma

electrónica debe adecuarse al riesgo económico de la operación, al volumen de contratos celebrados y a la necesidad de contar con medios probatorios sólidos en caso de controversia (De Miguel Asensio, 2023).

2.2.1. Firma electrónica simple

La firma electrónica simple constituye la forma más básica de firma electrónica y se caracteriza por su mínimo nivel de exigencia técnica. En términos generales, se considera firma electrónica simple a cualquier dato electrónico que permita identificar, aunque sea de manera indirecta, a una persona y expresar su aceptación del contenido de un documento. Ejemplos típicos de esta modalidad son la inserción de un nombre al final de un correo electrónico, la aceptación de términos y condiciones mediante un clic ("clickwrap") o el uso de credenciales básicas de acceso a una plataforma digital (Lee Pérez, Oscar Iván, 2022).

En el ámbito empresarial, la firma electrónica simple es ampliamente utilizada en contratos de bajo riesgo, como acuerdos de confidencialidad preliminares, aceptaciones de políticas internas o contratos estandarizados de escasa cuantía económica. Por ejemplo, una empresa de comercio electrónico puede considerar suficiente la aceptación mediante clic para la celebración de contratos de compraventa con consumidores recurrentes. No obstante, desde un punto de vista jurídico, esta modalidad presenta limitaciones significativas en cuanto a su valor probatorio, ya que resulta más vulnerable a cuestionamientos sobre la identidad del firmante o la autenticidad del consentimiento (Jurado, 2023).

2.2.2. Firma electrónica avanzada

La firma electrónica avanzada representa un nivel intermedio de seguridad y fiabilidad. Se caracteriza por cumplir con requisitos adicionales que permiten vincularla de manera más sólida al firmante y detectar cualquier alteración posterior del documento firmado. Entre estos requisitos suelen incluirse la identificación unívoca del firmante, el control exclusivo de los medios de firma y la posibilidad de verificar la integridad del documento (Kostenko, 2023).

Desde una perspectiva empresarial, la firma electrónica avanzada es especialmente adecuada para contratos de mediana complejidad y valor económico, como contratos de prestación de servicios, acuerdos de distribución o contratos laborales celebrados a distancia. Por ejemplo, una empresa puede utilizar plataformas de firma electrónica avanzada que incorporan autenticación multifactor, sellos de tiempo y registros de auditoría, lo que permite reconstruir el proceso de firma en caso de disputa. Esta modalidad ofrece un equilibrio razonable entre eficiencia operativa y seguridad jurídica (De Miguel Asensio, 2023).

Sin embargo, a diferencia de la firma digital, la firma electrónica avanzada no siempre se basa en certificados digitales emitidos por entidades acreditadas. Ello implica que su reconocimiento jurídico puede variar según el ordenamiento aplicable y que su valor probatorio dependerá, en última instancia, de la apreciación judicial de las pruebas aportadas. Esta circunstancia obliga a las empresas a evaluar cuidadosamente su uso en operaciones de mayor riesgo (Cordero Mendoza, 2024).

2.2.3. Firma digital o firma electrónica cualificada

La firma digital —también denominada firma electrónica cualificada en algunos ordenamientos— constituye el máximo nivel de seguridad dentro de la tipología de firmas electrónicas. Se basa en técnicas criptográficas de clave pública y en el uso de certificados digitales emitidos por entidades de certificación debidamente acreditadas. Este modelo permite verificar con alto grado de certeza la identidad del firmante y garantiza la integridad del documento, ya que cualquier modificación posterior invalida automáticamente la firma (Asllani Ndreka, 2015).

En el ámbito empresarial, la firma digital es especialmente relevante para contratos de alto valor económico, operaciones financieras, contratos societarios y actos que requieren un elevado nivel de certeza jurídica. Por ejemplo, la celebración de contratos de financiamiento, fusiones y adquisiciones o acuerdos de inversión suele exigir el uso de firmas digitales para minimizar riesgos de impugnación. Desde el punto de vista probatorio, esta modalidad goza de una presunción reforzada de validez y eficacia, lo

que la convierte en un instrumento clave para la seguridad jurídica de la contratación digital (Gonzales Barrón, 2015).

La utilización de la firma digital también tiene implicancias en términos de cumplimiento normativo y gobernanza corporativa. Las empresas que adoptan este tipo de firma deben implementar políticas internas de gestión de certificados, capacitación del personal y medidas de ciberseguridad, lo que refuerza la cultura de cumplimiento y reduce la exposición a riesgos legales y reputacionales. En este sentido, la firma digital no solo es un mecanismo técnico, sino un componente integral de la estrategia jurídica y tecnológica de la empresa (Mohiuddin, 2025).

En conclusión, la clasificación de los tipos de firmas electrónicas permite comprender que no existe una solución única aplicable a todas las operaciones empresariales. La elección entre firma electrónica simple, avanzada o digital debe responder a un análisis contextual del riesgo, del marco normativo aplicable y de las necesidades probatorias de la empresa. Este enfoque gradual y estratégico resulta indispensable para garantizar la eficacia jurídica de la contratación digital y será clave para el análisis específico de la regulación peruana de la firma digital en los capítulos siguientes.

2.3. La firma digital y la criptografía

La firma digital constituye la manifestación más robusta y técnicamente sofisticada de la firma electrónica, al sustentarse en principios criptográficos que permiten garantizar, de manera objetiva y verificable, la autenticidad del firmante, la integridad del documento y el no repudio del acto jurídico. A diferencia de otras modalidades de firma electrónica, la firma digital no se apoya en simples mecanismos de identificación o autenticación, sino en algoritmos matemáticos que hacen prácticamente imposible la falsificación del proceso de firma sin el conocimiento de claves criptográficas específicas (Rivest et al., 1978).

Desde una perspectiva jurídico-funcional, la firma digital se erige como el instrumento que mejor satisface el principio de equivalencia funcional respecto de la firma manuscrita. En efecto, mediante el uso de criptografía asimétrica, la firma digital permite identificar de manera inequívoca al firmante, asegurar que el contenido del

documento no ha sido alterado y vincular jurídicamente a la persona con el acto celebrado. Estas características explican por qué numerosos ordenamientos jurídicos confieren a la firma digital una presunción reforzada de validez y eficacia jurídica, especialmente en el ámbito de la contratación empresarial (Diffie, W. & Hellman, M., 1976).

2.3.1. Fundamentos criptográficos de la firma digital

La base técnica de la firma digital se encuentra en la criptografía de clave pública, también conocida como criptografía asimétrica. Este sistema utiliza un par de claves matemáticamente relacionadas: una clave privada, que permanece bajo el control exclusivo del titular, y una clave pública, que puede ser conocida por terceros. El proceso de firma digital implica el uso de la clave privada para generar un valor criptográfico único asociado al documento, el cual puede ser verificado por cualquier receptor mediante la clave pública correspondiente (Stallings, 2011).

El carácter innovador de la criptografía asimétrica radica en que elimina la necesidad de compartir secretos entre las partes para verificar la autenticidad de una firma. Este avance, introducido inicialmente por Diffie y Hellman, revolucionó las comunicaciones seguras y sentó las bases para el desarrollo de sistemas de firma digital aplicables a gran escala. Desde el punto de vista jurídico, esta arquitectura técnica resulta especialmente valiosa, ya que permite a terceros —incluidos jueces y árbitros— verificar objetivamente la validez de una firma sin comprometer la seguridad del sistema (Diffie, W. & Hellman, M., 1976).

Un elemento adicional del proceso de firma digital es la utilización de funciones hash criptográficas, que transforman el contenido del documento en un resumen digital de longitud fija. Este resumen es el que se firma con la clave privada del firmante, de modo que cualquier alteración posterior del documento genera un hash diferente, invalidando automáticamente la firma. Esta característica asegura la integridad del documento y constituye una de las principales ventajas de la firma digital frente a otros mecanismos de firma electrónica (Stallings, 2011).

2.3.2. Firma digital y certificación de identidad

Para que la firma digital tenga plena eficacia jurídica, resulta indispensable vincular la clave pública utilizada en el proceso de verificación con la identidad real del firmante. Esta función es cumplida por los certificados digitales, emitidos por entidades de certificación que actúan como terceros de confianza. Un certificado digital contiene información sobre la identidad del titular, su clave pública y la firma digital de la entidad certificadora, lo que permite verificar la autenticidad del certificado y, por ende, del firmante (Adams, Carlisle & Lloyd, Steve, 1999).

En el ámbito empresarial, la intervención de entidades de certificación acreditadas resulta crucial para garantizar la confianza en los sistemas de firma digital. Por ejemplo, cuando una empresa celebra un contrato de financiamiento utilizando firmas digitales, la contraparte puede verificar el certificado digital del firmante y asegurarse de que la firma corresponde efectivamente a un representante autorizado. Este mecanismo reduce significativamente el riesgo de suplantación de identidad y fortalece la seguridad jurídica de las operaciones comerciales (Maurer, Ueli M. & Schmid, Pierre E., 2001).

La certificación digital también desempeña un papel relevante en la gestión del ciclo de vida de las firmas digitales, incluyendo la revocación de certificados en caso de pérdida de la clave privada o cese de las facultades de representación. Desde una perspectiva jurídica, estos mecanismos permiten adaptar la firma digital a las dinámicas propias de la actividad empresarial, donde los roles y autorizaciones pueden cambiar con relativa frecuencia (Adams, Carlisle & Lloyd, Steve, 1999).

2.3.3. Ejemplos empresariales y relevancia jurídica

En la práctica empresarial, la firma digital se utiliza de manera preferente en operaciones de alto riesgo económico o con significativas implicancias legales. Un ejemplo típico es la celebración de contratos societarios, como acuerdos de accionistas o actas de juntas generales, mediante firmas digitales reconocidas. En estos casos, la posibilidad de verificar la identidad de los firmantes y la integridad del documento

resulta esencial para evitar controversias sobre la validez de los acuerdos adoptados (Stallings, 2011).

Otro ejemplo relevante se encuentra en el comercio electrónico B2B y en las operaciones financieras digitales. Las empresas que participan en licitaciones electrónicas o en plataformas de contratación pública suelen estar obligadas a utilizar firmas digitales para presentar ofertas y suscribir contratos. La utilización de criptografía avanzada y certificados digitales permite garantizar la transparencia del proceso y la igualdad de condiciones entre los participantes, reforzando la confianza en los mecanismos de contratación digital (Maurer, Ueli M. & Schmid, Pierre E., 2001).

En síntesis, la firma digital, sustentada en principios criptográficos sólidos, representa el instrumento más avanzado para garantizar la seguridad jurídica de la contratación electrónica empresarial. Su análisis integrado —tanto desde la perspectiva técnica como jurídica— resulta indispensable para comprender su rol central en los sistemas modernos de contratación y para evaluar adecuadamente su regulación y aplicación práctica en el ordenamiento jurídico peruano.

2.4. La firma electrónica como medio de manifestación de voluntad

La manifestación de voluntad constituye el núcleo esencial del negocio jurídico y, por ende, del contrato. En el derecho civil clásico, dicha manifestación se exterioriza a través de declaraciones verbales o escritas, siendo la firma manuscrita el signo paradigmático que permite atribuir la voluntad a una persona determinada. En el contexto digital, la firma electrónica emerge como el instrumento que permite exteriorizar, imputar y probar la voluntad contractual en ausencia de soporte físico. Desde esta perspectiva, la firma electrónica no es un simple requisito formal, sino un medio jurídico de expresión del consentimiento, cuyo análisis debe realizarse a la luz de la teoría general del acto jurídico (Caringella, 2011).

La doctrina contemporánea ha destacado que la voluntad contractual no se identifica con un estado psicológico interno, sino con su exteriorización jurídicamente relevante. En consecuencia, el problema central de la contratación electrónica no es la inexistencia de voluntad, sino la determinación de si los medios electrónicos utilizados permiten

exteriorizarla de manera válida, libre y consciente. La firma electrónica cumple precisamente esta función al operar como un signo objetivo que permite inferir la intención de obligarse del firmante, siempre que se inserte en un contexto tecnológico y normativo que garantice su fiabilidad (Roppo, 2009).

Desde el punto de vista funcional, la firma electrónica actúa como un acto concluyente de aceptación, equiparable a la firma manuscrita o incluso a ciertos comportamientos inequívocos reconocidos por el derecho civil. Por ejemplo, la aceptación de un contrato empresarial mediante una plataforma digital que exige la autenticación del usuario y la aplicación de una firma electrónica avanzada puede considerarse una manifestación válida de voluntad, en la medida en que el sistema permita atribuir el acto a una persona determinada y vincularla con el contenido contractual (Grundmann, 2018).

La equivalencia funcional entre la firma manuscrita y la firma electrónica no implica identidad absoluta, sino equivalencia en cuanto a resultados jurídicos. Mientras que la firma manuscrita se apoya en la grafía personal del firmante, la firma electrónica se sustenta en mecanismos tecnológicos que permiten cumplir las mismas funciones: identificación, imputación y prueba del consentimiento. Esta equivalencia ha sido ampliamente reconocida por la doctrina comparada, que subraya que el derecho no protege la forma en sí misma, sino la función que esta cumple en la estructura del negocio jurídico (Martinez-Cardenas, 2025).

En el ámbito empresarial, la firma electrónica como medio de manifestación de voluntad adquiere una relevancia particular debido a la automatización de los procesos contractuales. En muchos casos, la voluntad se expresa mediante interacciones hombre-máquina o incluso máquina-máquina, como ocurre en contratos celebrados a través de plataformas digitales con flujos predefinidos. Por ejemplo, un contrato de suministro puede activarse automáticamente cuando se cumplen ciertas condiciones programadas, siendo la firma electrónica el mecanismo que legitima jurídicamente esta manifestación anticipada de voluntad (Gulyaeva, Elena E. & Felix, Helen Grace D. , 2025).

Este fenómeno plantea interrogantes relevantes sobre la libertad y la conciencia del consentimiento. Sin embargo, la doctrina mayoritaria sostiene que la utilización de

medios electrónicos no vicia la voluntad per se, siempre que el sistema permita al usuario conocer el contenido del contrato y expresar su aceptación de manera informada. La firma electrónica, en este contexto, actúa como un sello de confirmación jurídica que cierra el proceso de formación del consentimiento, incluso cuando este se desarrolla de manera automatizada (Grundmann, 2018).

Desde una perspectiva probatoria, la firma electrónica también cumple una función esencial como medio de prueba de la manifestación de voluntad. En caso de controversia, el documento electrónico firmado permite reconstruir el proceso de formación del consentimiento y demostrar que una persona determinada aceptó el contenido contractual. Este aspecto resulta crucial en contratos empresariales complejos, donde la prueba del consentimiento puede ser determinante para la resolución del conflicto. La fiabilidad del sistema de firma electrónica utilizado incidirá directamente en la valoración judicial de dicha prueba (Gulyaeva, Elena E. & Felix, Helen Grace D. , 2025)

En conclusión, la firma electrónica debe ser entendida como un medio jurídicamente idóneo para la manifestación de voluntad en la contratación digital. Su validez no depende de la materialidad del soporte, sino de su capacidad para cumplir las funciones esenciales del consentimiento contractual. Este enfoque funcional y dogmático resulta indispensable para analizar, en los capítulos siguientes, la regulación específica de la firma electrónica y digital en el ordenamiento jurídico peruano y su aplicación práctica en las operaciones empresariales.

Capítulo III

Análisis exegético de la ley de firmas y certificados digitales

CAPÍTULO III

ANÁLISIS EXEGÉTICO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES

La incorporación de la firma electrónica en el ordenamiento jurídico peruano responde a un proceso de adaptación del derecho a las exigencias de la sociedad de la información y de la economía digital. La progresiva digitalización de las actividades empresariales, administrativas y financieras ha puesto en evidencia la necesidad de contar con un marco normativo que garantice la seguridad jurídica de los actos celebrados por medios electrónicos. En este contexto, el Perú ha desarrollado una regulación específica que reconoce la validez y eficacia jurídica de la firma electrónica y de la firma digital, alineándose con estándares internacionales y principios del derecho comparado (Ana Dobratinich, 2021).

El eje central de este marco normativo lo constituye la Ley N.º 27269, Ley de Firmas y Certificados Digitales, que establece los principios, requisitos y efectos jurídicos de la firma digital en el país. Esta norma introduce una distinción relevante entre firma electrónica en sentido amplio y firma digital como modalidad específica basada en certificados digitales. Dicha diferenciación no es meramente terminológica, sino que tiene implicancias directas en el valor probatorio de los documentos electrónicos y en el grado de confianza que el ordenamiento deposita en cada tipo de firma (Roel Alva, L. A.; Chocano Ravina, E. J. & Salazar Pariona, P. M., 2020).

Desde una perspectiva dogmática, la regulación peruana de la firma electrónica se apoya en el principio de equivalencia funcional, conforme al cual los actos jurídicos celebrados por medios electrónicos no pueden ser discriminados por el solo hecho de adoptar una forma distinta a la tradicional. Este principio se articula con el reconocimiento de la neutralidad tecnológica, permitiendo que la norma jurídica no quede atada a una tecnología específica y pueda adaptarse a la evolución constante de los mecanismos de firma electrónica (Calderón Puertas, 2024).

El marco jurídico peruano también se caracteriza por la incorporación de una infraestructura de confianza, sustentada en entidades de certificación y entidades de

registro acreditadas por el Estado. Este sistema busca garantizar la identidad de los firmantes y la integridad de los documentos electrónicos, especialmente en el uso de la firma digital. Por ejemplo, una empresa que celebra contratos electrónicos de alto valor puede utilizar certificados digitales emitidos por una entidad certificadora reconocida, lo que refuerza la seguridad jurídica de la operación y facilita la prueba del consentimiento en caso de controversia judicial.

Asimismo, la normativa peruana sobre firmas electrónicas no se limita al ámbito privado, sino que tiene una proyección significativa en la administración pública y la contratación estatal. La utilización obligatoria o preferente de firmas digitales en procedimientos administrativos y en sistemas de gobierno digital evidencia el rol estratégico que el Estado asigna a estos mecanismos como herramientas de modernización y transparencia. Este enfoque ha permitido agilizar trámites, reducir costos y mejorar la eficiencia administrativa, aunque también plantea desafíos en términos de interoperabilidad y acceso tecnológico (Presidencia del Consejo de Ministros.

Desde el punto de vista empresarial, el marco jurídico peruano ofrece un conjunto de oportunidades y desafíos. Por un lado, brinda certeza normativa para la celebración de contratos electrónicos, facilitando la adopción de modelos de negocio digitales. Por otro lado, impone obligaciones relacionadas con la gestión de certificados digitales, la protección de datos y la seguridad de la información. Por ejemplo, una empresa que implemente sistemas de firma digital debe establecer políticas internas de control y capacitación para evitar el uso indebido de certificados y prevenir riesgos legales (Castro, 2014)

La interacción entre la normativa sobre firmas electrónicas y otras ramas del derecho —como el derecho civil, el derecho probatorio y el derecho de la protección de datos personales— constituye otro aspecto central del análisis. La validez de la firma electrónica no puede evaluarse de manera aislada, sino en relación con normas sobre consentimiento, forma de los actos jurídicos y carga de la prueba. Esta interrelación normativa exige una interpretación sistemática que permita resolver conflictos y lagunas en la aplicación práctica de la ley (Nieto Melgarejo, 2016).

Finalmente, el estudio del marco jurídico de las firmas electrónicas en el Perú debe considerar su evolución y los retos futuros. La rápida transformación tecnológica plantea la necesidad de actualizar constantemente la regulación y de fortalecer las capacidades institucionales para su implementación efectiva. Este capítulo se propone, por tanto, analizar críticamente el régimen jurídico vigente, identificando sus fundamentos, alcances y limitaciones, como base para evaluar la eficacia real de las firmas electrónicas en la contratación empresarial peruana.

3.1. La Ley N° 27269 – Ley de Firmas y Certificados Digitales

La Ley N.º 27269, denominada Ley de Firmas y Certificados Digitales, constituye el instrumento legal fundamental en el Perú para regular la utilización de las firmas electrónicas y digitales en transacciones jurídicas y comerciales. La norma fue promulgada el 26 de mayo de 2000 y publicada el 28 de mayo de 2000, en respuesta a la necesidad de otorgar seguridad jurídica a la contratación digital y al desarrollo del comercio electrónico en el país.

El origen de esta ley se enmarca en el proceso de globalización de las economías y la expansión de las tecnologías de la información y comunicación (TIC) que, desde finales del siglo XX, transformaron radicalmente las prácticas contractuales. Antes de la Ley N.º 27269, el ordenamiento jurídico peruano carecía de una regulación específica que reconociera expresamente la validez de los actos celebrados por medios electrónicos, limitando la confianza de los agentes económicos en los contratos digitales y generando incertidumbre en materias como la firma, la autenticación y la integridad de los documentos digitales.

En sus antecedentes inmediatos se encuentra la discusión parlamentaria y técnica sobre la necesidad de equiparar la firma electrónica con la firma manuscrita, a fin de promover el desarrollo del comercio electrónico y la administración electrónica. La exposición de motivos del proyecto original señala que la ausencia de un marco legal adecuado dificultaba no solo la celebración de contratos electrónicos, sino también la defensa de derechos en procesos judiciales o administrativos, así como la

interoperabilidad con normas internacionales en materia de comercio y tecnología digital.

El objetivo principal de la Ley N.º 27269 es claro y se encuentra expresamente en su artículo 1: *"regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad"*. Esta formulación implica dos decisiones normativas estratégicas: primero, se reconoce la equivalencia funcional entre los mecanismos tradicionales de firma y los medios electrónicos; segundo, se habilita jurídicamente la utilización de tecnologías emergentes sin que el derecho deba exigir formalidades tradicionales del documento físico.

La ley define la firma electrónica como "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" (Artículo 1). Esta definición reconoce explícitamente el carácter tecnológico de la firma, sin limitarla a una determinada técnica, lo que permite la evolución normativa conforme avanzan las tecnologías.

El ámbito de aplicación de la ley abarca todas las firmas electrónicas que, al estar puestas sobre un mensaje de datos o asociadas lógicamente al mismo, permitan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos (Artículo 2). Este enfoque normativo sitúa la protección legal en torno a las funciones que la firma electrónica cumple —identificación, vinculación y autenticación— más que en la forma técnica específica que adopte.

Entre los principios rectores que se extraen del texto legal y de su finalidad se encuentran:

1. **Equivalencia funcional:** El legislador peruano reconoce que la forma no puede ser un obstáculo para la seguridad jurídica. Así, si una firma electrónica cumple las funciones esenciales de una firma manuscrita —identificar y vincular voluntades— debe gozar de la misma validez y eficacia. Esta concepción está

alineada con la Ley Modelo de la CNUDMI sobre comercio electrónico, que promueve la neutralidad tecnológica.

2. **Neutralidad tecnológica:** La norma no limita la firma electrónica a una tecnología específica, lo que le permite abarcar desde firmas simples hasta firmas digitales criptográficas basadas en certificados emitidos por entidades acreditadas. Esta neutralidad favorece la adaptabilidad del derecho frente a la innovación técnica y evita la obsolescencia normativa prematura.
3. **Seguridad jurídica:** Al equiparar la firma electrónica con la firma manuscrita, la ley busca ofrecer certeza a los agentes económicos y jurídicos sobre la eficacia de los actos y contratos celebrados digitalmente, reduciendo los riesgos de litigios basados en dudas sobre la autenticidad o integridad de los documentos electrónicos.
4. **Integración con otros marcos jurídicos:** La Ley N.º 27269 no opera de manera aislada; se inscribe dentro del corpus general del derecho, en diálogo con normas sobre derecho contractual, protección de datos personales y procedimientos administrativos, lo que exige interpretaciones sistemáticas cuando surgen conflictos normativos.
5. **Promoción del comercio electrónico y la modernización:** Implícitamente, la ley responde a la necesidad de fomentar el desarrollo del comercio electrónico, facilitando transacciones sin papel y agilizando procedimientos en el sector público y privado. En este sentido, la implementación de la norma ha sido un paso estratégico hacia la modernización del Estado y la reducción de costos de transacción, en línea con tendencias globales de digitalización.

La ley también incluye definiciones complementarias, como las de firma digital —entendida como firma electrónica que utiliza criptografía asimétrica con un par de claves pública y privada, de forma que la clave pública no permite derivar la clave privada—, y la de certificado digital, que es el documento emitido por una entidad certificadora que vincula un par de claves con la identidad de una persona (Artículos 3 y 6).

El desarrollo de la Ley N.º 27269 no estuvo exento de debates sobre su alcance y efectividad. Uno de los principales temas de discusión ha sido la regulación de los certificados digitales de entidades extranjeras, cuya validez estaba condicionada al reconocimiento por una entidad nacional, lo que generó tensiones con principios constitucionales de libre competencia y libertad de mercado.

Desde su entrada en vigencia, esta ley ha sido complementada con un reglamento específico y ha servido como base para múltiples instrumentos de gobierno electrónico y regulación del comercio digital en Perú. Su impacto ha sido particularmente visible en la administración pública, donde la obligación de utilizar firmas digitales en ciertos procedimientos ha facilitado la digitalización de servicios y trámites, contribuyendo a la eficiencia y transparencia.

Finalmente, la Ley N.º 27269 representa no solo una norma técnica sobre medios de firma, sino un verdadero marco estratégico para la inserción del Perú en la economía digital global, donde la confianza, la seguridad jurídica y la interoperabilidad normativa son condiciones necesarias para la competitividad empresarial y la protección de los derechos de los ciudadanos.

Respecto a los artículos correspondientes a la norma, se puede señalar:

3.1.1. Artículo 1: Objeto de la Ley

El artículo 1 establece de forma clara y programática el objeto de la Ley N.º 27269: *"regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad"*. Este precepto no solo reconoce el uso de medios electrónicos para la exteriorización de la voluntad contractual, sino que consagra el principio de equivalencia funcional entre los medios tradicionales y los electrónicos.

Conceptualmente, esto significa que el ordenamiento jurídico peruano no exige una forma determinada para la validez de los actos jurídicos, sino que reconoce que una firma electrónica puede producir los mismos efectos que una firma en papel si cumple con su función jurídica esencial. Este enfoque es coherente con las mejores prácticas

internacionales, como las planteadas en la *Ley Modelo de la CNUDMI sobre Comercio Electrónico*, que propugna la neutralidad tecnológica y la equivalencia jurídica de los medios digitales.

Un ejemplo práctico: si una empresa firma electrónicamente un contrato de suministro internacional mediante una plataforma certificada, esa firma tendrá la misma fuerza jurídica que si hubiera impreso y firmado manualmente el contrato, siempre que pueda probarse su identidad y voluntad. Esta equivalencia reduce la necesidad de pruebas adicionales sobre la forma misma del acto y facilita los procesos de contratación digital.

3.1.2. Artículo 2: Ámbito de aplicación

El artículo 2 define el ámbito de aplicación de la ley, señalando que se aplica "a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos".

Este artículo introduce tres elementos funcionales fundamentales que deben cumplirse para que una firma electrónica sea jurídicamente relevante:

1. **Vinculación con el firmante:** debe permitir identificar al autor del acto jurídico.
2. **Autenticación:** garantiza que la firma corresponde efectivamente a quien dice ser.
3. **Integridad del documento:** asegura que el contenido no ha sido alterado desde la firma.

Desde un punto de vista doctrinal, estos requisitos aseguran que la firma electrónica cumple las funciones tradicionalmente asociadas a la firma manuscrita sin depender del soporte físico. En la práctica empresarial, estos elementos son críticos, por ejemplo, cuando múltiples partes celebran un contrato de distribución a través de plataformas digitales: la firma vinculada al mensaje de datos permite verificar responsabilidad y cumplimiento. (Nieto Fernández, 2021).

3.1.3. Artículo 3: Firma digital

El artículo 3 define la firma digital como una modalidad específica de firma electrónica que utiliza técnicas de criptografía asimétrica mediante un par de claves (pública y privada).

Esta definición es doctrinalmente relevante porque distingue a la firma digital de otras formas de firma electrónica de menor nivel de seguridad. La firma digital, al depender de criptografía asimétrica, ofrece garantías de autenticidad, integridad y no repudio superiores. Por ejemplo, en operaciones financieras o de alto valor económico, la firma digital permite demostrar que solo el titular de la clave privada pudo haber generado la firma.

En términos prácticos, la firma digital se utiliza en transacciones que requieren un alto grado de certeza de identidad, como la suscripción de contratos de financiamiento, la presentación de ofertas en licitaciones electrónicas o actos notariales digitales que deben cumplir con requisitos estrictos de seguridad jurídica.

3.1.4. Artículo 4: Titular de la firma digital

El artículo 4 establece que el titular de la firma digital es la persona a la que se le atribuye exclusivamente un certificado digital que contiene una firma digital, identificándola objetivamente en relación con el mensaje de datos.

Este artículo refuerza un enfoque objetivo de la identidad digital: la persona identificada con un certificado digital emitido por una entidad certificadora acreditada es responsable de las firmas que genera. Este criterio objetivo es crucial en el derecho empresarial, donde las partes necesitan certeza sobre con quién están contratando.

3.1.5. Artículo 5: Obligaciones del titular de la firma digital

El artículo 5 impone obligaciones al titular de la firma digital, exigiendo que brinde a las entidades certificadoras y a terceros con quienes se relacione información exacta y completa sobre su identidad y uso de la firma digital.

Desde la óptica dogmática, este artículo introduce un deber de veracidad y diligencia para proteger la confianza en el sistema de firmas digitales. Si un titular proporcionara información falsa o incompleta, comprometería no solo su seguridad jurídica sino también la de terceros que confían en el certificado digital.

Por ejemplo, una empresa que mal declara su razón social o datos de representación al solicitar un certificado digital puede generar conflictos de responsabilidad si terceros actuaron confiando en esa identificación para celebrar contratos.

3.1.6. Artículo 6 y 7: Certificado digital y su contenido

Los artículos 6 y 7 regulan el certificado digital y su contenido mínimo, respectivamente. El certificado digital es el documento electrónico emitido por una entidad de certificación que vincula un par de claves con una persona determinada y confirma su identidad.

El artículo 7, por su parte, detalla los elementos que deben contener los certificados digitales: identificación del suscriptor, identificación de la entidad certificadora, clave pública, metodología de verificación, número de serie, vigencia y la firma digital de la entidad certificadora.

Esta regulación técnica normativiza los estándares mínimos que garantizan la fiabilidad y trazabilidad del sistema de firmas digitales. En la práctica, significa que empresas y autoridades pueden validar documentalmente la identidad y la vinculación de la firma digital a su titular, facilitando la prueba judicial o administrativa.

3.1.7. Artículos 8, 9 y 10: Confidencialidad, cancelación y revocación

Los artículos 8, 9 y 10 se refieren a la confidencialidad de la información, así como a los mecanismos de cancelación y revocación de certificados digitales.

El artículo 8 protege la privacidad de las claves privadas y datos personales del titular, permitiendo su levantamiento solo por orden judicial o solicitud del propio suscriptor.

Esto es un elemento clave de confianza para los usuarios de firmas digitales, ya que preserva la seguridad del sistema.

Los artículos 9 y 10 regulan causas y procedimientos para cancelar o revocar un certificado digital, incluyendo solicitudes del titular, revocación por inexactitudes, expiración de vigencia o cese de operaciones de la entidad certificadora. Estas reglas buscan proteger el sistema de certificados contra usos indebidos o desactualizados, reforzando la seguridad jurídica del contrato electrónico.

3.1.8. Artículo 11: Reconocimiento de certificados extranjeros

El artículo 11 establece que los certificados de firmas digitales emitidos por entidades extranjeras tienen la misma validez y eficacia jurídica si son reconocidos por la autoridad administrativa competente.

Este artículo tiene una importancia estratégica para la interoperabilidad jurídica internacional: permite que contratos transfronterizos, suscritos con firmas digitales emitidas en el extranjero, puedan ser reconocidos en el Perú si cumplen estándares equivalentes. Sin embargo, este reconocimiento está condicionado —según la ley— a que una entidad certificadora nacional valide a la entidad extranjera, lo que ha sido crítico en debates sobre libre competencia y competencia técnica internacional del sistema de certificación.

3.1.9. Artículos 12 a 15: Entidades de certificación y de registro

Los artículos 12 a 15 establecen el régimen de las entidades de certificación y de registro o verificación, así como el depósito de certificados digitales y su accesibilidad.

- **Artículo 12:** define la entidad de certificación, responsable de emitir o cancelar certificados digitales y brindar servicios relacionados.
- **Artículo 13:** regula la entidad de registro o verificación, que identifica y autentica al solicitante de un certificado digital.
- **Artículo 14:** crea la obligación de mantener un registro permanente de certificados digitales, accesible por medios telemáticos para consulta pública.

- **Artículo 15:** faculta al Poder Ejecutivo a determinar la autoridad administrativa competente para el registro de estas entidades y la exigencia de estándares técnicos internacionales.

Estos artículos son fundamentales para estructurar la infraestructura de confianza dentro del sistema peruano de firma electrónica, lo que va más allá de la norma individual para configurar un régimen institucional que promueve seguridad, transparencia y accesibilidad del sistema.

3.2. El Reglamento de la Ley de Firmas y Certificados Digitales

El Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N.º 052-2008-PCM, constituye la instrumentación operativa y técnica de la Ley N.º 27269, que reconoce la firma electrónica y digital como medio válido de manifestación de voluntad en los actos jurídicos, tanto en el sector privado como en el público.

La promulgación del Reglamento se produjo en un contexto de aceleración del uso de tecnologías de la información, con la finalidad de llenar los vacíos operativos que la Ley no podía resolver por sí sola, dado que la norma madre se limita a establecer principios generales y un marco conceptual. El Reglamento cumple la función de detallar procedimientos, roles, responsabilidades y herramientas técnicas necesarias para garantizar la seguridad jurídica de las firmas digitales en el Perú.

El artículo 1 del Reglamento declara su objeto normativo: regular, para los sectores público y privado, la utilización de firmas digitales y la infraestructura que las soporta, denominada Infraestructura Oficial de Firma Electrónica (IOFE), que comprende la acreditación y supervisión de diversas entidades como las de certificación y de registro o verificación.

Desde un punto de vista conceptual, el Reglamento reconoce la diversidad de modalidades de firmas electrónicas —con distintos niveles de seguridad y garantías— y establece que ninguna modalidad queda excluida siempre que cumpla con los requisitos de identificación, autenticación e integridad previstos en la Ley. Esta

amplitud permite la coexistencia de firmas electrónicas simples, avanzadas y cualificadas sin exclusión normativa automática.

Una de las funciones más relevantes del Reglamento es establecer la validez y eficacia jurídica de las firmas digitales generadas dentro del marco de la IOFE. Es decir, una firma digital que se genere utilizando un certificado emitido por una entidad certificadora acreditada y verificada bajo el marco regulatorio tiene igual efecto jurídico que una firma manuscrita, siempre que se cumplan los requisitos establecidos en la Ley y en el Reglamento.

Este aspecto es particularmente relevante en el ámbito probatorio: los documentos electrónicos firmados digitalmente deben ser admitidos como prueba válida en procesos judiciales o administrativos, lo que elimina la incertidumbre que generaciones anteriores de juristas enfrentaban sobre la fuerza probatoria de los documentos digitales.

El Reglamento también regula de manera detallada la conservación de documentos electrónicos firmados digitalmente. Esto significa que no basta con generar la firma digital; se deben cumplir requisitos técnicos para garantizar que el documento permanezca íntegro, accesible y verificable a lo largo del tiempo, lo cual es crucial para garantizar su valor probatorio cuando se requiere.

Otro punto normativo fundamental es la regulación del certificado digital: el Reglamento establece requisitos para su emisión, contenido mínimo, vigencia y proceso de cancelación. El certificado digital es el instrumento que vincula la identidad de una persona o empresa con su clave criptográfica, y su regulación opera como el soporte técnico que hace posible la verificación de la firma digital.

En este sentido, el Reglamento exige que para obtener un certificado digital se debe acreditar la identidad y la capacidad legal del solicitante, diferenciando entre personas naturales y jurídicas, y estableciendo reglas claras para la veracidad de la información proporcionada, lo que evita suplantaciones de identidad y fortalece la seguridad del sistema.

La regulación de la cancelación de certificados digitales es otro elemento esencial. El Reglamento prevé causales de cancelación voluntaria o forzada de certificados, con procedimientos específicos para proteger tanto los intereses del titular como los de terceros que puedan haber confiado en el certificado previo a su cancelación.

El Reglamento también contiene disposiciones sobre la validez de firmas digitales generadas fuera de la IOFE, reconociendo que, mediante pacto o convenio entre partes, firmas generadas fuera del marco oficial pueden tener validez. Esto introduce un elemento de autonomía de la voluntad contractual dentro del marco regulatorio.

De forma doctrinal, esta apertura facilita el comercio electrónico internacional, donde actores globales pueden validar firmas que no han sido emitidas dentro de la infraestructura nacional siempre que exista un acuerdo de reconocimiento previo entre las partes.

El Reglamento también regula la Infraestructura Oficial de Firma Electrónica (IOFE), que comprende a las entidades de certificación, de registro o verificación y a los prestadores de servicios de valor añadido. Estas entidades actúan como "terceros de confianza" y su acreditación ante la autoridad administrativa competente es obligatoria para poder operar legalmente.

Las entidades de certificación tienen competencias específicas: emitir, suspender, revocar y mantener certificados digitales, así como asegurar que la emisión se realice bajo parámetros técnicos y de seguridad previamente definidos.

Las entidades de registro o verificación son responsables de identificar y autenticar al solicitante de un certificado digital, asegurando que la identidad que se registra corresponde a una persona o entidad real con capacidad jurídica.

Los prestadores de servicios de valor añadido complementan la IOFE ofreciendo servicios como sellado de tiempo (timestamping), preservación del documento firmado o gestión de claves remotas, lo cual incrementa las capacidades de los sistemas empresariales de gestión documental.

El Reglamento también contempla la posibilidad de certificaciones cruzadas entre entidades certificadoras nacionales y extranjeras, lo que permite incorporar certificados emitidos en el exterior dentro de la IOFE, siempre que la autoridad competente determine que cumplen estándares equivalentes.

Esto representa una respuesta normativa al desafío de la interoperabilidad jurídica internacional, facilitando la contratación digital entre empresas peruanas y extranjeras sin exigir la duplicación de certificados.

En el sector público, el Reglamento detalla la estructura jerárquica de certificación digital, estableciendo que las entidades estatales que presten servicios de certificación digital en el marco de la IOFE deben estar acreditadas y cumplir con estándares técnicos, lo que fortalece la confianza de los ciudadanos y empresas en los trámites electrónicos del Estado.

Asimismo, el Reglamento regula la cooperación de información entre entidades públicas para facilitar el acceso a documentos electrónicos firmados, promoviendo que éstos sean interoperables entre las distintas plataformas del Estado.

Un impacto directo de este régimen en la práctica empresarial es la posibilidad de automatizar procesos contractuales complejos, como licitaciones, adjudicaciones o acuerdos de confidencialidad, sin acudir a documentación física, reduciendo costos y tiempos de operación.

Finalmente, el Reglamento ha sido objeto de modificaciones posteriores a fin de modernizar su alcance, como lo evidencian decretos supremos posteriores que actualizan disposiciones y plazos para implementar certificación nacional y políticas de gobierno digital.

El Reglamento de la Ley de Firmas y Certificados Digitales no es un mero texto técnico, sino una norma estructural del derecho contractual moderno peruano, que articula tecnología, prueba, autonomía privada y seguridad jurídica. Su correcta aplicación es indispensable para la eficacia de los contratos empresariales en la era digital.

Respecto a los artículos correspondientes a la norma, se puede señalar:

3.2.1. Disposiciones generales y objeto del Reglamento (contenido en Arts. 1–4)

El artículo 1 del Reglamento define su objeto: regular la aplicación de la Ley N.º 27269, precisando los aspectos técnicos, organizativos y procedimentales necesarios para la utilización de firmas digitales y certificados digitales. Desde una perspectiva dogmática, este artículo cumple la función de norma de cierre operativo, transformando los principios generales de la Ley en reglas aplicables y verificables.

El artículo 2 delimita el ámbito de aplicación, señalando que el Reglamento es aplicable tanto al sector público como al privado. Esta extensión normativa es fundamental, pues evita la fragmentación del sistema y garantiza la unidad del régimen jurídico de la firma digital, permitiendo que contratos empresariales, actos administrativos y trámites judiciales compartan una misma base de validez tecnológica y jurídica.

El artículo 3 establece definiciones técnicas esenciales (certificado digital, firma digital, entidad de certificación, etc.). Desde el punto de vista hermenéutico, este artículo cumple una función interpretativa clave, ya que fija el significado jurídico–técnico de conceptos que no pueden ser entendidos únicamente desde el derecho tradicional, sino desde la criptografía y la seguridad informática.

El artículo 4 consagra el principio de neutralidad tecnológica, al señalar que el Reglamento no impone una tecnología específica, sino estándares funcionales. Este principio es esencial para la vigencia futura de la norma, pues evita su obsolescencia frente a avances tecnológicos, permitiendo que nuevas soluciones criptográficas puedan ser incorporadas sin reforma normativa.

Ejemplo práctico: una empresa que migra de certificados almacenados en token físico a certificados en la nube puede hacerlo sin vulnerar el Reglamento, siempre que se mantengan los estándares de seguridad exigidos.

3.2.2. Infraestructura Oficial de Firma Electrónica – IOFE (Contenido en Arts. 5–13)

El artículo 5 crea la Infraestructura Oficial de Firma Electrónica (IOFE), concebida como un sistema jerárquico de confianza. Desde una visión institucionalista, la IOFE funciona como el "ecosistema jurídico-tecnológico" que permite que la firma digital sea confiable para terceros.

El artículo 6 establece los componentes de la IOFE: entidades de certificación, entidades de registro o verificación y prestadores de servicios de valor añadido. Este diseño reproduce el modelo internacional de Public Key Infrastructure (PKI), alineando al Perú con estándares globales.

El artículo 7 regula la acreditación de las entidades de certificación, exigiendo requisitos técnicos, financieros y organizativos. Jurídicamente, esta disposición protege el principio de seguridad jurídica preventiva, pues evita que entidades sin solvencia técnica comprometan la validez de miles de firmas digitales.

El artículo 8 asigna responsabilidades a las entidades certificadoras, incluyendo la emisión, suspensión y revocación de certificados. Aquí se introduce una forma moderna de responsabilidad profesional tecnológica, donde el error técnico puede generar consecuencias jurídicas relevantes.

El artículo 9 regula a las entidades de registro o verificación, encargadas de la identificación del titular. Este artículo conecta directamente con el principio civil de capacidad y legitimación, trasladándolo al entorno digital.

Ejemplo práctico: cuando un gerente general solicita un certificado digital para firmar contratos empresariales, la entidad de registro verifica su identidad y poderes inscritos en SUNARP.

3.2.3. Certificados digitales: emisión, vigencia y cancelación (Arts. 14–24)

El artículo 14 define el contenido mínimo del certificado digital: identidad del titular, clave pública, vigencia y datos de la entidad emisora. Este artículo cumple una función probatoria, pues el certificado es el elemento que permite verificar la autoría de la firma.

El artículo 15 regula la vigencia del certificado digital, estableciendo límites temporales. Desde una perspectiva jurídica, esta limitación temporal protege a terceros frente a certificados obsoletos o comprometidos.

El artículo 16 introduce la figura de la suspensión del certificado, aplicable en casos de sospecha de compromiso de la clave privada. Este mecanismo refleja el principio de prevención del daño jurídico.

El artículo 17 regula la revocación definitiva del certificado, estableciendo causales y procedimientos. Este artículo es clave para determinar la validez temporal de los actos firmados.

Ejemplo práctico: si un certificado es revocado hoy, los contratos firmados antes de la revocación mantienen su validez, salvo prueba de fraude.

3.2.4. Validez jurídica y valor probatorio de la firma digital (Arts. 25–32)

El artículo 25 reafirma que la firma digital generada conforme al Reglamento tiene la misma validez jurídica que la firma manuscrita. Este es el núcleo dogmático del Reglamento, pues equipara el soporte digital al papel.

El artículo 26 reconoce expresamente el valor probatorio de los documentos electrónicos firmados digitalmente. Desde el derecho procesal, esto elimina cualquier presunción de inferioridad probatoria del documento electrónico.

El artículo 27 regula la conservación de documentos electrónicos firmados, exigiendo que se garantice su integridad y accesibilidad en el tiempo. Aquí se introduce el concepto de prueba digital duradera.

El artículo 28 permite el uso de sellado de tiempo, mecanismo técnico que acredita la fecha y hora exacta de la firma, reforzando la certeza jurídica.

Ejemplo práctico: un contrato de suministro firmado digitalmente y sellado en tiempo puede probar su existencia incluso años después ante un tribunal.

3.2.5. Firmas digitales fuera de la IOFE y autonomía privada (Arts. 33–36)

El artículo 33 reconoce la validez de firmas digitales generadas fuera de la IOFE, siempre que las partes así lo acuerden. Este artículo es una manifestación clara del principio de autonomía de la voluntad contractual.

El artículo 34 establece que dichas firmas tendrán validez inter partes, pero no necesariamente frente a terceros. Esta distinción es clave para la práctica empresarial.

El artículo 35 regula la prueba de este tipo de firmas, asignando la carga probatoria a quien las invoca.

Ejemplo práctico: dos empresas pueden usar una plataforma privada de firma electrónica para contratos internos, aunque para contratos con el Estado deban usar la IOFE.

3.2.6. Reconocimiento de certificados extranjeros (Arts. 37–41)

El artículo 37 permite el reconocimiento de certificados digitales emitidos en el extranjero, siempre que cumplan estándares equivalentes. Este artículo facilita el comercio electrónico internacional.

El artículo 38 introduce la certificación cruzada entre entidades nacionales y extranjeras, alineando al Perú con modelos de interoperabilidad global.

Ejemplo práctico: una empresa peruana puede aceptar contratos firmados digitalmente por su proveedor europeo sin exigir una nueva firma local.

3.2.7. Supervisión, infracciones y responsabilidad (Arts. 42–48)

El artículo 42 asigna a la autoridad competente la supervisión del sistema. Esta función de control es esencial para mantener la confianza en la IOFE.

El artículo 43 establece infracciones administrativas para entidades certificadoras que incumplan sus obligaciones.

El artículo 44 regula la responsabilidad civil por daños derivados de fallas en la certificación digital.

Desde una perspectiva de análisis económico del derecho, este régimen incentiva la inversión en seguridad tecnológica y cumplimiento normativo.

3.3. Entidades de Certificación y Entidades de Registro

3.3.1. La Infraestructura Oficial de Firma Digital como sistema de confianza institucional

La Infraestructura Oficial de Firma Digital (IOFD) constituye el eje central del modelo peruano de firma digital. Desde una perspectiva jurídica avanzada, no se trata únicamente de un conjunto de actores técnicos, sino de un sistema normativamente organizado de confianza institucional, diseñado para sustituir —en el entorno digital— las garantías que históricamente ofrecían la presencia física, la firma manuscrita y el notario. En este contexto, las entidades de certificación y las entidades de registro o verificación desempeñan funciones diferenciadas pero complementarias, sin las cuales la firma digital carecería de eficacia jurídica real.

El diseño de la IOFD responde a estándares internacionales de infraestructura de clave pública (PKI), adaptados al ordenamiento jurídico peruano. Este modelo asume que la confianza en un documento firmado digitalmente no surge de la tecnología en sí

misma, sino de la responsabilidad jurídica atribuida a terceros de confianza debidamente acreditados y supervisados por el Estado.

3.3.2. Entidades de certificación: concepto y función estructural

Las entidades de certificación son aquellas personas jurídicas, públicas o privadas, acreditadas para emitir, gestionar, suspender y revocar certificados digitales dentro del marco de la IOFD. Jurídicamente, estas entidades cumplen una función análoga a la de un fedatario tecnológico, pues garantizan que una determinada clave pública está vinculada de manera fiable a una persona natural o jurídica identificada.

Desde el punto de vista dogmático, la entidad de certificación es el núcleo del sistema de confianza, ya que sobre ella recae la presunción de veracidad del vínculo identidad–clave criptográfica. Sin esta presunción, la firma digital no podría equipararse a la firma manuscrita, ni mucho menos desplegar efectos probatorios plenos.

3.3.3. Funciones principales de las entidades de certificación

Entre las funciones esenciales de las entidades de certificación se encuentra, en primer lugar, la emisión de certificados digitales, proceso mediante el cual se crea un documento electrónico que vincula una clave pública con la identidad del titular. Este acto tiene naturaleza jurídica relevante, pues genera efectos frente a terceros que confían en la validez del certificado.

En segundo lugar, las entidades de certificación son responsables de la gestión del ciclo de vida del certificado, lo que incluye su vigencia temporal, renovación, suspensión temporal y revocación definitiva. Esta función resulta crucial para la seguridad jurídica, ya que un certificado comprometido o vencido no puede seguir produciendo efectos válidos.

Finalmente, estas entidades deben mantener registros accesibles y actualizados, como listas de certificados revocados (CRL) o servicios de verificación en línea (OCSP), que permitan a cualquier tercero comprobar la validez de una firma digital en tiempo real.

3.3.4. Obligaciones jurídicas de las entidades de certificación

Las obligaciones de las entidades de certificación no se limitan al plano técnico. Desde el punto de vista jurídico, están obligadas a cumplir estrictamente los estándares de seguridad, confidencialidad e integridad previstos en la normativa vigente y en sus políticas de certificación aprobadas por la autoridad competente.

Asimismo, tienen la obligación de verificar que el proceso de identificación del solicitante se haya realizado correctamente, aun cuando dicha función material sea ejecutada por una entidad de registro. La entidad certificadora no puede alegar desconocimiento o delegación para eximirse de responsabilidad frente a errores en la identificación.

Otra obligación esencial es la de informar oportunamente sobre la suspensión o revocación de certificados, pues la omisión o retraso en dicha comunicación puede generar daños a terceros que confían en un certificado que ya no es válido.

3.3.5. Responsabilidad civil y administrativa de las entidades de certificación

El régimen de responsabilidad de las entidades de certificación es particularmente riguroso. Desde una perspectiva de derecho civil, estas entidades pueden incurrir en responsabilidad por daños si, por negligencia o incumplimiento de sus obligaciones, causan perjuicios a titulares de certificados o a terceros que confían legítimamente en ellos.

Por ejemplo, si una entidad certificadora emite un certificado sin verificar adecuadamente la identidad del solicitante y este es utilizado para cometer fraude contractual, la entidad puede ser responsable por los daños derivados de esa falla de diligencia.

En el plano administrativo, las entidades de certificación están sujetas a supervisión y sanción por parte de la autoridad competente, pudiendo enfrentar multas, suspensión

o pérdida de la acreditación si incumplen el marco normativo. Este régimen sancionador refuerza la confianza sistémica en la IOFD.

3.3.6. Entidades de registro o verificación: rol y naturaleza jurídica

Las entidades de registro o verificación cumplen una función distinta pero igualmente esencial: son las encargadas de identificar y autenticar al solicitante de un certificado digital. Desde el punto de vista jurídico, su función se relaciona directamente con los principios de identidad, capacidad y legitimación, propios del derecho civil y mercantil.

Estas entidades actúan como el primer filtro del sistema, asegurando que la persona natural o jurídica que solicita un certificado es quien dice ser y tiene capacidad legal para los actos que pretende realizar mediante firma digital.

3.3.7. Funciones específicas de las entidades de registro

La función principal de la entidad de registro es la verificación de identidad, lo que implica comprobar documentos oficiales, poderes de representación y, en el caso de personas jurídicas, la existencia legal y vigencia de los cargos representativos.

Además, las entidades de registro deben documentar y conservar evidencia del proceso de identificación, ya que dicha información puede ser requerida posteriormente en procesos judiciales o administrativos para acreditar la validez de una firma digital.

En algunos casos, estas entidades también cumplen funciones de soporte y orientación al usuario, explicando las implicancias jurídicas del uso del certificado digital, lo que contribuye a la correcta utilización del sistema.

3.3.8. Obligaciones y estándares de diligencia de las entidades de registro

Las entidades de registro están obligadas a actuar con un alto estándar de diligencia profesional, dado que cualquier error en la identificación inicial puede comprometer la validez de toda la cadena de confianza.

Tienen la obligación de aplicar procedimientos estandarizados y auditables, evitando prácticas discrecionales que puedan generar riesgos de fraude o suplantación de identidad. Asimismo, deben proteger los datos personales del solicitante conforme a la normativa de protección de datos.

3.3.9. Régimen de responsabilidad de las entidades de registro

Desde el punto de vista jurídico, las entidades de registro pueden incurrir en responsabilidad solidaria con la entidad certificadora si se demuestra que una falla en la verificación de identidad contribuyó al daño causado.

Por ejemplo, si una entidad de registro valida incorrectamente a un falso representante de una empresa y firma contratos digitales en su nombre, la entidad de registro puede ser responsable por los daños ocasionados a la empresa y a terceros contratantes.

3.3.10. Interacción funcional entre entidades de certificación y de registro

La relación entre entidades de certificación y entidades de registro se basa en una división funcional de tareas, pero no en una fragmentación de responsabilidad. Ambas forman parte de una misma cadena de confianza, donde cada eslabón debe cumplir su función con rigor.

Desde una perspectiva sistémica, el correcto funcionamiento de la IOFD depende de la coordinación eficiente y transparente entre estas entidades, así como de la supervisión estatal efectiva.

3.3.11. Importancia práctica para la contratación empresarial digital

En el ámbito de los contratos empresariales, estas entidades permiten que actos jurídicos complejos —como contratos de suministro, acuerdos de confidencialidad, contratos de financiamiento o actos societarios— puedan celebrarse íntegramente en formato digital con plena validez jurídica y fuerza probatoria.

Por ejemplo, una empresa puede firmar digitalmente contratos con proveedores nacionales e internacionales sin desplazamientos físicos, confiando en que la identidad del firmante ha sido verificada por entidades acreditadas y supervisadas.

3.3.12. Valoración crítica y conclusiones

Desde una valoración doctrinal, el modelo peruano de entidades de certificación y registro ofrece un equilibrio adecuado entre seguridad jurídica y flexibilidad tecnológica. No obstante, su eficacia real depende del fortalecimiento continuo de la supervisión, la capacitación de operadores jurídicos y la actualización técnica del sistema.

En conclusión, las entidades de certificación y de registro no son simples intermediarios técnicos, sino actores jurídicos centrales en la contratación digital moderna, cuya actuación condiciona directamente la validez, eficacia y confiabilidad de los contratos empresariales en la era digital.

Cuadro comparativo: Entidades de certificación y registro

Perú vs. Unión Europea (eIDAS)

Criterio	Perú – Ley N.º 27269 y D.S. N.º 052-2008-PCM	Unión Europea – Reglamento (UE) N.º 910/2014 (eIDAS)
Marco normativo principal	Ley N.º 27269 – Ley de Firmas y Certificados Digitales y su Reglamento (D.S. N.º 052-2008-PCM).	Reglamento (UE) N.º 910/2014 (eIDAS), directamente aplicable en todos los Estados miembros.
Modelo de confianza	Infraestructura Oficial de Firma Digital (IOFD) basada en PKI nacional supervisada por el Estado.	Marco europeo de servicios de confianza cualificados, con reconocimiento transfronterizo obligatorio.
Entidad equivalente a certificación	Entidades de certificación acreditadas dentro de la IOFD.	Prestadores de servicios de confianza cualificados (QTSP – Qualified Trust Service Providers).
Entidad equivalente a registro	Entidades de registro o verificación de identidad.	Prestadores de servicios de identificación electrónica y mecanismos de identificación notificados.
Naturaleza jurídica	Personas jurídicas públicas o privadas acreditadas por autoridad nacional competente.	Entidades privadas o públicas acreditadas por organismos nacionales de supervisión.
Rol principal	Emitir, suspender, revocar certificados digitales y garantizar la vinculación identidad–clave.	Proveer servicios de confianza cualificados: firma electrónica, sellos electrónicos, sellado de tiempo, certificados.
Identificación del firmante	Realizada por entidades de registro mediante verificación documental y legal.	Identificación presencial o remota reforzada, conforme a niveles de garantía (bajo, sustancial, alto).

Criterio	Perú – Ley N.º 27269 y D.S. N.º 052-2008-PCM	Unión Europea – Reglamento (UE) N.º 910/2014 (eIDAS)
Tipos de firma reconocidos	Firma electrónica y firma digital (con mayor presunción jurídica).	Firma electrónica simple, avanzada y cualificada.
Equivalencia con firma manuscrita	Solo la firma digital emitida dentro de la IOFD tiene plena equivalencia jurídica.	La firma electrónica cualificada tiene efecto jurídico equivalente a la firma manuscrita en toda la UE.
Reconocimiento transfronterizo	Posible mediante certificación cruzada o acuerdos de reconocimiento.	Automático entre Estados miembros para firmas cualificadas.
Infraestructura técnica	PKI nacional con jerarquía definida.	Infraestructura europea interoperable con listas de confianza (EU Trusted Lists).
Supervisión estatal	Autoridad administrativa nacional supervisa, acredita y sanciona.	Autoridades nacionales supervisan; Comisión Europea coordina interoperabilidad.
Responsabilidad civil	Responsabilidad por negligencia o incumplimiento técnico-jurídico.	Responsabilidad estricta reforzada para servicios cualificados.
Carga probatoria	Presunción de validez para firmas digitales dentro de la IOFD.	Presunción legal fuerte para firmas electrónicas cualificadas.
Aplicación en el sector público	Obligatoria la IOFD para actos administrativos electrónicos.	Uso obligatorio de eIDAS en servicios públicos transfronterizos.
Flexibilidad contractual	Se admiten firmas fuera de la IOFD por acuerdo entre partes (inter partes).	Se admiten firmas simples y avanzadas, con menor presunción jurídica.
Protección de datos	Integrada con normativa nacional de protección de datos personales.	Integración directa con RGPD (GDPR).
Actualización tecnológica	Dependiente de reformas reglamentarias.	Marco tecnológicamente neutro con actualización continua.
Enfoque regulatorio	Predominio de control estatal previo (acreditación).	Predominio de control ex post y armonización supranacional.
Nivel de estandarización	Nacional, con aperturas a interoperabilidad internacional.	Alto nivel de estandarización europea obligatoria.
Orientación económica	Facilitación del comercio digital nacional y regional.	Mercado digital único europeo y comercio transfronterizo.

Fuente: Elaboración propia

El modelo peruano privilegia un enfoque de control estatal centralizado, adecuado para garantizar seguridad jurídica en una etapa de consolidación del comercio digital. En contraste, el modelo europeo eIDAS responde a una lógica de integración supranacional y libre circulación de servicios digitales, donde la interoperabilidad transfronteriza es prioritaria.

Mientras el sistema peruano otorga mayor rigidez formal a la firma digital emitida dentro de la IOFD, el sistema europeo ofrece gradaciones de confianza jurídica, permitiendo que distintas modalidades de firma convivan con efectos jurídicos diferenciados.

Desde una perspectiva evolutiva, el modelo peruano podría fortalecerse incorporando mecanismos similares a las listas de confianza europeas, lo que permitiría un

reconocimiento más ágil de certificados extranjeros y mayor integración con mercados digitales globales.

3.4. Relación con el Código Civil y la Legislación mercantil

3.4.1. Planteamiento general del problema de compatibilidad normativa

La incorporación de la firma electrónica y digital al ordenamiento jurídico peruano, a través de la Ley N.º 27269 y su Reglamento, plantea un desafío central: determinar su compatibilidad estructural y funcional con las normas generales del Código Civil y de la legislación mercantil, especialmente en materia de formación del contrato, manifestación de voluntad, forma contractual y prueba. Este análisis no puede abordarse desde una perspectiva meramente técnica, sino desde una lectura sistemática del ordenamiento jurídico como un todo coherente.

Desde una visión dogmática, la normativa de firmas electrónicas no constituye un subsistema aislado, sino una normativa especial de carácter instrumental, cuyo objetivo es permitir que los principios clásicos del derecho privado se proyecten eficazmente en el entorno digital, sin alterar su esencia.

3.4.2. La manifestación de voluntad contractual en el entorno digital

El Código Civil peruano consagra, en su artículo 140, que el contrato se perfecciona por el consentimiento de las partes, sin exigir una forma específica salvo disposición legal expresa. Esta regla general es plenamente compatible con la firma electrónica, en tanto esta constituye un medio de exteriorización de la voluntad, no un nuevo tipo de acto jurídico.

La firma electrónica, y especialmente la firma digital, cumple la función jurídica que históricamente ha desempeñado la firma manuscrita: identificar al autor del acto y vincularlo con el contenido del documento. Desde esta perspectiva, la normativa de

firmas electrónicas no modifica el concepto civil de consentimiento, sino que amplía los medios jurídicamente válidos para expresarlo.

Ejemplo práctico: un contrato de suministro celebrado mediante documento electrónico firmado digitalmente cumple con el requisito de consentimiento exigido por el Código Civil, siempre que exista acuerdo de voluntades verificable.

3.4.3. Principio de autonomía privada y contratación electrónica

El principio de autonomía privada, eje central del derecho civil y mercantil, encuentra una clara reafirmación en la normativa de firmas electrónicas. El Reglamento de la Ley N.º 27269 reconoce expresamente la validez de firmas electrónicas generadas fuera de la Infraestructura Oficial de Firma Digital cuando las partes así lo acuerdan.

Esta previsión es plenamente compatible con el artículo 1354 del Código Civil, que permite a las partes determinar libremente el contenido del contrato dentro de los límites de la ley. En consecuencia, la elección de un determinado mecanismo de firma electrónica constituye una manifestación legítima de la autonomía contractual.

Ejemplo práctico: dos empresas pueden acordar contractualmente el uso de una plataforma privada de firma electrónica para la celebración de contratos internos, sin necesidad de recurrir a certificados oficiales, siempre que no se trate de actos que la ley reserve a una forma especial.

3.4.4. La forma contractual y su reinterpretación digital

El Código Civil distingue entre contratos consensuales, formales y solemnes. La normativa de firmas electrónicas no altera esta clasificación, pero sí exige una reinterpretación funcional del concepto de forma. Allí donde la ley exige forma escrita, el documento electrónico firmado digitalmente cumple dicha exigencia, conforme al principio de equivalencia funcional.

Este principio, ampliamente aceptado en el derecho comparado, permite equiparar el documento electrónico al documento en papel, siempre que se garantice la

identificación del firmante y la integridad del contenido. En el ordenamiento peruano, esta equivalencia se encuentra expresamente reconocida para la firma digital.

Ejemplo práctico: un contrato que la ley exige conste por escrito puede celebrarse válidamente mediante documento electrónico firmado digitalmente, sin necesidad de soporte físico.

3.4.5. Compatibilidad con la legislación mercantil

En el ámbito mercantil, caracterizado por la celeridad, la masificación de operaciones y la desmaterialización de documentos, la firma electrónica se presenta como un instrumento plenamente coherente con los principios del derecho comercial. La legislación mercantil peruana, aunque no sistematizada en un solo cuerpo normativo, ha admitido históricamente medios ágiles de contratación, como la contratación por correspondencia y medios electrónicos.

La firma electrónica refuerza la seguridad jurídica en este contexto, al permitir la identificación del firmante y la trazabilidad de las operaciones, elementos esenciales en contratos empresariales de gran volumen o ejecución continuada.

Ejemplo práctico: contratos marco, órdenes de compra electrónicas y acuerdos de confidencialidad pueden celebrarse y ejecutarse íntegramente mediante firmas electrónicas, sin afectar su validez mercantil.

3.4.6. El documento electrónico como medio de prueba

Uno de los puntos más sensibles de la compatibilidad normativa se encuentra en el derecho probatorio. El Código Civil y el Código Procesal Civil reconocen el documento como medio de prueba, pero históricamente lo asociaron al soporte físico. La normativa de firmas electrónicas rompe con esta concepción materialista y reconoce expresamente el valor probatorio del documento electrónico firmado digitalmente.

Desde una perspectiva procesal, el documento electrónico firmado digitalmente goza de una presunción de autenticidad e integridad, equiparable a la del documento privado con firma manuscrita, lo que facilita su admisión y valoración en juicio.

3.4.7. Carga de la prueba y presunciones legales

La compatibilidad entre ambos regímenes también se manifiesta en la distribución de la carga de la prueba. Cuando un documento electrónico está firmado digitalmente conforme a la Ley N.º 27269, corresponde a quien lo impugna probar su falsedad o invalidez, y no al firmante acreditar su autenticidad.

Este régimen es coherente con los principios probatorios del Código Procesal Civil, que reconoce presunciones legales y traslada la carga probatoria a quien las cuestiona.

Ejemplo práctico: si una parte niega haber firmado un contrato digitalmente, deberá probar la invalidez de la firma o la existencia de un vicio técnico relevante.

3.4.8. Firma electrónica y contratos sujetos a formalidad especial

Un punto crítico en la compatibilidad normativa se presenta respecto de los contratos sujetos a formalidad solemne, como aquellos que requieren escritura pública. En estos casos, la firma electrónica no sustituye automáticamente al notario, salvo que exista una norma especial que así lo disponga.

No obstante, la firma electrónica puede integrarse como etapa previa o complementaria del proceso, por ejemplo, en la preparación del contrato o en actos accesorios, sin vulnerar las exigencias formales del Código Civil.

3.4.9. Seguridad jurídica y prevención de conflictos

La compatibilidad entre la normativa de firmas electrónicas y el derecho civil y mercantil contribuye a reforzar la seguridad jurídica preventiva, al reducir la incertidumbre sobre la autoría y el contenido de los contratos empresariales.

La trazabilidad digital, los sellos de tiempo y los registros de certificación permiten reconstruir con precisión el proceso de formación del contrato, lo que resulta particularmente valioso en litigios complejos.

Desde una perspectiva conclusiva, la normativa peruana sobre firmas electrónicas es compatible con el Código Civil y la legislación mercantil, pues no modifica los principios del derecho privado, sino que los adecua al entorno digital. El reto principal no es normativo, sino interpretativo y formativo, especialmente en la capacitación de los operadores jurídicos.

Capítulo IV

Impacto en el derecho civil y procesal peruano

CAPÍTULO IV

IMPACTO EN EL DERECHO CIVIL Y PROCESAL PERUANO

La validez jurídica de las firmas electrónicas en los contratos empresariales constituye uno de los ejes más relevantes del derecho contractual contemporáneo, en la medida en que pone en diálogo las categorías clásicas del derecho privado con los nuevos soportes tecnológicos de manifestación de la voluntad. Este capítulo se orienta a examinar cómo el ordenamiento jurídico peruano reconoce, delimita y garantiza la eficacia jurídica de las firmas electrónicas en el ámbito de las relaciones empresariales, caracterizadas por su dinamismo, complejidad y alto volumen de operaciones.

En el contexto de la economía digital, las empresas han migrado progresivamente de esquemas contractuales basados en el soporte físico a entornos desmaterializados, donde la contratación se realiza a través de plataformas electrónicas, sistemas automatizados y redes digitales. En este escenario, la firma electrónica deja de ser una innovación meramente tecnológica para convertirse en un instrumento jurídico esencial para la seguridad y previsibilidad de las transacciones comerciales.

El análisis de la validez jurídica de la firma electrónica exige partir de una premisa fundamental: el derecho de contratos no se define por el soporte material del documento, sino por la existencia de una manifestación de voluntad válida, libre e informada, atribuible a un sujeto determinado. En consecuencia, la firma electrónica debe evaluarse en función de su capacidad para cumplir las mismas funciones jurídicas que la firma manuscrita ha desempeñado históricamente.

Desde una perspectiva funcional, la firma —sea manuscrita o electrónica— cumple tres funciones esenciales: identificar al firmante, expresar su consentimiento respecto del contenido del documento y vincularlo jurídicamente con dicho contenido. La validez jurídica de la firma electrónica dependerá, por tanto, de su aptitud para satisfacer estas funciones de manera confiable y verificable en el entorno digital.

En el ámbito empresarial, esta cuestión adquiere especial relevancia debido a la necesidad de celeridad, estandarización y escalabilidad de los contratos. Operaciones

como contratos de suministro, acuerdos de confidencialidad, contratos marco, licencias de software o contratos de financiamiento requieren mecanismos de firma que permitan su celebración sin dilaciones innecesarias, pero sin sacrificar seguridad jurídica.

El ordenamiento jurídico peruano, a través de la Ley N.º 27269 y su Reglamento, ha optado por un modelo que reconoce expresamente la validez jurídica de la firma electrónica y, con mayor intensidad, de la firma digital, estableciendo un sistema de presunciones legales que fortalecen su eficacia en el tráfico jurídico empresarial. Este reconocimiento no supone una ruptura con el derecho civil clásico, sino una extensión funcional de sus principios al entorno digital.

Este capítulo analiza cómo la normativa especial sobre firmas electrónicas se articula con las reglas generales del Código Civil en materia de consentimiento, forma y prueba, demostrando que la firma electrónica no constituye un nuevo requisito de validez contractual, sino un medio alternativo y legítimo de exteriorización de la voluntad.

En particular, se examina la validez de la firma electrónica en contratos consensuales, que constituyen la regla general en el derecho peruano. En estos casos, la firma electrónica opera como un elemento probatorio reforzado, pero no como un requisito constitutivo del contrato, lo que resulta coherente con la tradición civilista.

Asimismo, se aborda la validez de la firma electrónica en contratos que requieren forma escrita, demostrando que el documento electrónico firmado digitalmente satisface dicha exigencia conforme al principio de equivalencia funcional. Este análisis resulta crucial para contratos empresariales que, por razones legales o de gestión de riesgos, deben constar por escrito.

Desde una perspectiva mercantil, la firma electrónica se presenta como un instrumento plenamente compatible con los principios de rapidez y eficiencia que caracterizan al derecho comercial. La contratación electrónica permite a las empresas reducir costos de transacción, eliminar barreras geográficas y mejorar la trazabilidad de sus relaciones contractuales.

El capítulo también introduce el análisis de la validez inter partes y frente a terceros de las firmas electrónicas, distinguiendo entre aquellas generadas dentro de la

Infraestructura Oficial de Firma Digital y aquellas utilizadas por acuerdo privado entre las partes. Esta distinción es clave para comprender los distintos niveles de seguridad jurídica que ofrece cada modalidad.

En el ámbito probatorio, la validez jurídica de la firma electrónica se proyecta directamente en su fuerza como medio de prueba. Los contratos empresariales firmados digitalmente gozan de presunción de autenticidad e integridad, lo que influye decisivamente en la carga de la prueba en eventuales controversias judiciales o arbitrales.

Un aspecto central que se desarrolla en este capítulo es el análisis de los riesgos jurídicos asociados al uso inadecuado de firmas electrónicas, especialmente cuando se emplean mecanismos sin certificación o sin adecuados controles de identidad. En el contexto empresarial, una mala elección del tipo de firma puede generar contingencias legales significativas.

A través de ejemplos prácticos, se demuestra cómo la firma electrónica puede ser utilizada válidamente en operaciones empresariales complejas, como contratos celebrados entre matrices y filiales, contratos transfronterizos o acuerdos celebrados mediante plataformas automatizadas de contratación.

El capítulo también reflexiona sobre el impacto de la firma electrónica en la gobernanza corporativa, particularmente en actos societarios como acuerdos de directorio, juntas de accionistas no presenciales o suscripción de documentos corporativos, donde la validez de la firma electrónica resulta determinante para la eficacia de las decisiones empresariales.

Desde una perspectiva de análisis económico del derecho, la firma electrónica contribuye a reducir los costos de transacción y a mejorar la eficiencia del mercado, siempre que exista un marco jurídico claro que garantice su validez y prevea mecanismos adecuados de resolución de controversias.

Este capítulo también se orienta a evaluar el grado de confianza institucional que el sistema jurídico peruano otorga a las firmas electrónicas, destacando el rol de las entidades de certificación y de registro como garantes de dicha confianza en el tráfico empresarial.

En términos comparados, la introducción sitúa el modelo peruano dentro de las tendencias internacionales, evidenciando su convergencia con estándares globales, aunque sin perder de vista las particularidades del contexto jurídico y económico nacional.

Finalmente, se plantea que la validez jurídica de la firma electrónica no es una cuestión meramente normativa, sino también cultural e institucional. Su eficacia real depende de la correcta comprensión y utilización por parte de empresarios, abogados, jueces y árbitros.

En conclusión, este capítulo sienta las bases teóricas y prácticas para el análisis detallado de los requisitos, alcances y límites de la validez jurídica de las firmas electrónicas en los contratos empresariales, demostrando que estas no solo son compatibles con el derecho privado peruano, sino que constituyen un elemento indispensable para la contratación moderna en la era digital.

4.1. Requisitos de validez de los contratos empresariales celebrados mediante firmas electrónicas

4.1.1. Consideraciones generales sobre la validez contractual en entornos digitales

La validez de los contratos empresariales celebrados mediante firmas electrónicas constituye uno de los aspectos más relevantes del derecho contractual contemporáneo, pues conecta los principios clásicos del derecho civil con las exigencias tecnológicas propias de la economía digital. La doctrina coincide en que la incorporación de medios electrónicos al proceso contractual no altera los elementos esenciales de validez, sino que exige su reinterpretación funcional a la luz de nuevos soportes de manifestación de la voluntad (Alnimer, 2021).

En este contexto, la validez contractual debe entenderse como la aptitud del contrato para producir efectos jurídicos obligatorios entre las partes y frente a terceros. En la contratación empresarial digital, esta aptitud se ve reforzada por la necesidad de

seguridad jurídica, trazabilidad y previsibilidad, especialmente en operaciones de alto valor económico o de ejecución continuada (Ranchordas, 2015).

4.1.2. El consentimiento válido en los contratos empresariales electrónicos

El consentimiento constituye el eje central de la validez contractual y se manifiesta a través de la coincidencia entre oferta y aceptación. En los contratos celebrados mediante firmas electrónicas, la doctrina sostiene que el consentimiento conserva plena validez siempre que pueda acreditarse de manera inequívoca la voluntad del contratante (Alqudah, Yassin Ahmad & Flieh Alnimer, Raed Mohammad, 2021).

Investigaciones sobre contratación electrónica destacan que la aceptación expresada mediante mecanismos digitales —como firmas electrónicas, plataformas contractuales o sistemas de autenticación— es jurídicamente válida cuando el proceso garantiza información suficiente, libertad de decisión y ausencia de vicios del consentimiento (Hayyunniarizka Wulandari, Asri & Agus Priyono, Ery, 2025). En el ámbito empresarial, estos requisitos suelen cumplirse mediante procedimientos estandarizados de contratación y auditorías digitales.

4.1.3. Ausencia de vicios del consentimiento en entornos digitales

La validez del consentimiento exige que este no esté afectado por error, dolo, violencia o intimidación. En el contexto digital, la doctrina ha identificado riesgos específicos, tales como interfaces engañosas, asimetrías informativas y automatización excesiva del proceso contractual, que pueden comprometer la libertad del consentimiento (B.M. Loos, Marco et al., 2025).

Estudios empíricos advierten que la transparencia contractual y la claridad de los términos son factores determinantes para evitar la invalidez del contrato electrónico por vicios del consentimiento (Miranzo-Díaz, 2019). En la contratación empresarial, el estándar de diligencia es más elevado, dado el carácter profesional de las partes.

4.1.4. Capacidad jurídica y legitimación de los contratantes

La capacidad para contratar es un requisito esencial de validez que se proyecta tanto en el plano jurídico como en el tecnológico. En la contratación empresarial digital, la capacidad implica no solo la aptitud legal para obligarse, sino también la posibilidad de acreditar identidad y representación mediante mecanismos electrónicos confiables (Arya, K. et al., 2025).

Investigaciones sobre contratos celebrados mediante agentes electrónicos y plataformas automatizadas resaltan la importancia de sistemas de identificación digital robustos para garantizar que el consentimiento proviene de un sujeto jurídicamente habilitado (De Miguel Asensio, 2023). La falta de estos mecanismos puede generar invalidez o inoponibilidad del contrato.

4.1.5. Objeto contractual lícito, posible y determinado en contratos digitales

El objeto del contrato debe ser lícito, posible y determinado o determinable. En el ámbito empresarial digital, este requisito se extiende a bienes y servicios intangibles, como licencias de software, servicios en la nube, bases de datos o soluciones tecnológicas, cuya validez ha sido ampliamente reconocida por la doctrina (De Franceschi, 2020).

La precisión del objeto contractual es particularmente relevante en contratos electrónicos empresariales, ya que la indeterminación puede generar disputas interpretativas y afectar la validez del contrato (Hayyunniarizka Wulandari, Asri & Agus Priyono, Ery, 2025).

4.1.6. Causa y finalidad económica del contrato empresarial

La causa, entendida como la función económica y social del contrato, sigue siendo un elemento relevante para el control de validez, incluso en contratos electrónicos. Estudios doctrinales sostienen que la causa permite evaluar la licitud y coherencia del acuerdo, especialmente en contratos automatizados o celebrados mediante plataformas digitales (Stone, R. & Devenney, J., 2022).

En el ámbito empresarial, la causa se vincula directamente con la finalidad económica del contrato, como la optimización de recursos, la distribución de riesgos o la generación de valor (Ranchordas, 2015).

4.1.7. Forma contractual y principio de equivalencia funcional

Si bien la libertad de forma es la regla general, determinados contratos requieren forma escrita como requisito de validez. La doctrina del principio de equivalencia funcional sostiene que el documento electrónico firmado digitalmente cumple con esta exigencia, siempre que garantice autenticidad, integridad y conservación del contenido (Alqudah, Yassin Ahmad & Flieh Alnimer, Raed Mohammad, 2021).

Las investigaciones comparadas confirman que la forma electrónica no solo satisface la exigencia legal, sino que refuerza la seguridad jurídica mediante mecanismos tecnológicos avanzados (De Franceschi, 2020).

4.1.8. Autenticidad, integridad y no repudio

La validez de los contratos empresariales firmados electrónicamente depende de la capacidad del sistema utilizado para garantizar la autenticidad del firmante, la integridad del documento y la imposibilidad de repudio injustificado (Arya, K. et al., 2025).

En este sentido, la firma digital certificada se presenta como el mecanismo más robusto, al generar presunciones legales de validez que facilitan la prueba del contrato en sede judicial o arbitral (De Miguel Asensio, 2023).

4.1.9. Legalidad, orden público y normas imperativas

Todo contrato válido debe respetar normas imperativas y el orden público. En la contratación empresarial digital, esta exigencia se amplía para incluir la normativa sobre protección de datos, ciberseguridad y comercio electrónico, cuya infracción puede afectar la validez del contrato (B.M. Loos, Marco et al., 2025).

4.1.10. Intención de crear relaciones jurídicas y exigibilidad

La intención de obligarse jurídicamente constituye un elemento implícito de validez (Hayyunniarizka Wulandari, Asri & Agus Priyono, Ery, 2025). En contratos empresariales electrónicos, esta intención se presume debido al carácter profesional y económico de la relación, salvo prueba en contrario

4.2. La equivalencia jurídica de la firma digital

El principio de equivalencia funcional constituye uno de los pilares dogmáticos más relevantes del derecho de la contratación electrónica contemporánea. Su finalidad es asegurar que los actos jurídicos realizados mediante medios electrónicos produzcan los mismos efectos jurídicos que aquellos celebrados por medios tradicionales, siempre que cumplan funciones jurídicas equivalentes. En el ordenamiento peruano, este principio encuentra reconocimiento implícito y explícito en la Ley N.º 27269 y su Reglamento, al equiparar la firma digital a la firma manuscrita en términos de validez y eficacia jurídica (UNCITRAL, 2001).

Desde una perspectiva teórica, la equivalencia funcional no implica identidad material entre los soportes, sino identidad funcional entre los efectos jurídicos que producen. La doctrina ha sostenido que el derecho no protege la forma en sí misma, sino la función que esta cumple dentro del acto jurídico, particularmente en lo referido a identificación del autor, integridad del contenido y expresión del consentimiento (Twigg-Flesner, 2025).

En el contexto peruano, la firma digital se define como un tipo cualificado de firma electrónica que utiliza criptografía asimétrica y certificados digitales emitidos por entidades acreditadas. Esta configuración técnica permite que la firma digital cumpla de manera reforzada las funciones tradicionales de la firma manuscrita, lo que justifica su equivalencia jurídica plena (Espinoza Cespedes, 2025).

El principio de equivalencia funcional tiene su origen en el derecho uniforme internacional, particularmente en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la cual influyó decisivamente en las legislaciones latinoamericanas, incluida la peruana. Este instrumento establece que los requisitos legales de forma

escrita, firma y original pueden satisfacerse mediante medios electrónicos que cumplan funciones equivalentes (UNCITRAL, 1999).

En la legislación peruana, la equivalencia funcional se manifiesta cuando la norma reconoce que la firma digital tiene la misma validez jurídica que la firma manuscrita, siempre que haya sido generada dentro de la Infraestructura Oficial de Firma Digital. Esta equiparación no es meramente declarativa, sino que produce efectos concretos en materia contractual y probatoria (Chang O'Campo, 2000).

Desde el derecho civil, la firma cumple una función esencial como medio de imputación del acto jurídico a su autor. La firma digital satisface esta función mediante mecanismos técnicos de autenticación que permiten identificar al firmante con un alto grado de certeza, superando incluso las limitaciones probatorias de la firma manuscrita tradicional (Castro, 2014).

En el ámbito de los contratos empresariales, la equivalencia funcional adquiere una dimensión práctica fundamental. La posibilidad de celebrar contratos con firma digital permite a las empresas operar sin restricciones geográficas, reducir costos de transacción y acelerar procesos decisionales, sin sacrificar seguridad jurídica (Negri, 2025).

Un ejemplo claro de aplicación del principio de equivalencia funcional se observa en los contratos que la ley exige consten por escrito. Conforme a la normativa peruana, un documento electrónico firmado digitalmente satisface dicho requisito formal, produciendo los mismos efectos que un documento en soporte papel firmado manuscritamente (De la Maza Gazmuri, 2005).

Desde la perspectiva probatoria, la equivalencia funcional se traduce en la presunción de autenticidad e integridad del documento electrónico firmado digitalmente. Esta presunción desplaza la carga de la prueba hacia quien impugna la validez del documento, reforzando su eficacia en procesos judiciales y arbitrales (Negri, 2025).

La doctrina comparada ha señalado que la equivalencia funcional no debe entenderse como una ficción jurídica, sino como una técnica normativa que permite adaptar las categorías clásicas del derecho a la realidad tecnológica, manteniendo la coherencia del sistema jurídico (González-Rivera, T. V. et al., 2024).

En el Perú, este principio también se proyecta sobre la actuación de la administración pública, donde la firma digital permite la emisión de actos administrativos electrónicos con plena validez jurídica, siempre que se respeten los requisitos técnicos y legales establecidos.

La equivalencia funcional no es absoluta ni irrestricta. Existen actos jurídicos que, por su naturaleza o por mandato legal expreso, requieren solemnidades específicas que aún no han sido plenamente digitalizadas, como ciertos actos notariales. No obstante, incluso en estos casos, la firma digital puede cumplir funciones preparatorias o complementarias (Castro, 2014).

Desde una perspectiva constitucional, el principio de equivalencia funcional se vincula con el derecho a la libertad de contratación y con el principio de neutralidad tecnológica, en la medida en que el Estado no debe privilegiar un soporte tecnológico sobre otro sin justificación objetiva (Twigg-Flesner, 2025).

En el comercio internacional, la equivalencia funcional de la firma digital facilita el reconocimiento transfronterizo de contratos electrónicos, siempre que exista interoperabilidad normativa y técnica entre los sistemas de certificación de los distintos Estados (Negri, 2025).

En el ámbito empresarial peruano, la correcta aplicación del principio de equivalencia funcional exige que las empresas comprendan la diferencia entre firma electrónica simple y firma digital, optando por esta última cuando se requiera un mayor nivel de seguridad jurídica (Espinoza Cespedes, 2025).

La jurisprudencia comparada ha resaltado que la equivalencia funcional no elimina la necesidad de valorar la prueba digital, sino que orienta al juez a reconocer su idoneidad jurídica, evitando prejuicios basados en la ausencia de soporte físico (Negri, 2025).

Desde el análisis económico del derecho, la equivalencia funcional reduce los costos de cumplimiento normativo y fomenta la eficiencia del mercado, al permitir que las transacciones se realicen de manera más ágil sin aumentar el riesgo jurídico (González-Rivera, T. V. et al., 2024).

En términos de política legislativa, el reconocimiento del principio de equivalencia funcional en la normativa peruana evidencia una clara intención de promover la digitalización de la economía y la modernización del derecho privado, alineándose con estándares internacionales (UNCITRAL, 2001).

No obstante, la eficacia real del principio depende de su correcta interpretación por jueces, árbitros y operadores jurídicos, quienes deben comprender que la firma digital no es una excepción, sino una manifestación moderna de categorías jurídicas tradicionales (De la Maza Gazmuri, 2005).

En conclusión, el principio de equivalencia funcional reconocido por la legislación peruana constituye el fundamento dogmático que permite afirmar la plena equivalencia jurídica de la firma digital respecto de la firma manuscrita, garantizando la validez, eficacia y seguridad jurídica de los contratos empresariales celebrados en la era digital.

4.3. Eficacia probatoria de la firma digital

La eficacia probatoria de la firma digital constituye uno de los aportes más significativos del derecho de las nuevas tecnologías al sistema probatorio tradicional. En el ámbito de los contratos empresariales, la prueba adquiere una función central, pues permite demostrar no solo la existencia del contrato, sino también su autoría, integridad y fecha cierta. La firma digital se inserta en este contexto como un mecanismo que refuerza la confianza jurídica en los documentos electrónicos (Vásquez Azuara, 2017).

Desde una perspectiva dogmática, la eficacia probatoria se refiere a la aptitud de un medio para generar convicción en el juez sobre los hechos que se pretenden acreditar. En el caso de la firma digital, esta eficacia no deriva únicamente de la voluntad de las partes, sino de un reconocimiento normativo expreso que le atribuye presunciones legales específicas (Ledesma Narváez, La prueba en el proceso civil, 2021).

El ordenamiento jurídico peruano, a través de la Ley N.º 27269 y su Reglamento, reconoce que el documento electrónico firmado digitalmente goza de la misma eficacia probatoria que el documento privado con firma manuscrita. Esta equiparación se

fundamenta en la confiabilidad técnica del sistema de criptografía asimétrica y en la intervención de entidades de certificación acreditadas (Becerra Lino, 2025).

La doctrina procesal contemporánea sostiene que la prueba digital no constituye un nuevo medio probatorio autónomo, sino una modalidad tecnológica del documento, cuyo valor debe evaluarse conforme a los principios generales de la prueba documental (Vásquez Azuara, 2017). En este sentido, la firma digital actúa como un elemento de autenticación reforzada.

Uno de los aspectos centrales de la eficacia probatoria de la firma digital es la presunción de autoría. Gracias al certificado digital, se presume que la firma ha sido generada por el titular del certificado, salvo prueba en contrario. Esta presunción desplaza la carga de la prueba hacia quien impugna el documento (Ledesma Narváez, La prueba en el proceso civil, 2021).

En los contratos empresariales, esta presunción resulta especialmente relevante, pues evita que una de las partes desconozca arbitrariamente su consentimiento alegando falsificación o suplantación, práctica frecuente en litigios comerciales tradicionales (Becerra Lino, 2025).

Otro elemento esencial es la presunción de integridad del documento electrónico firmado digitalmente. La criptografía garantiza que cualquier alteración posterior del contenido sea detectable, lo que otorga al documento un alto grado de fiabilidad probatoria (Hernández-García, M. E. & Hernández-Navarrete L. D., 2025).

Desde el punto de vista procesal, esta garantía de integridad facilita la labor del juez, quien puede verificar técnicamente si el documento ha sido modificado, reduciendo el margen de discrecionalidad y subjetividad en la valoración de la prueba (Vásquez Azuara, 2017).

La eficacia probatoria de la firma digital también se proyecta sobre la fecha cierta del documento. Mediante sellos de tiempo electrónicos, es posible acreditar con precisión el momento en que el documento fue firmado, lo que resulta crucial en conflictos empresariales vinculados a plazos, prioridades crediticias o cumplimiento de obligaciones (Hernández-García, M. E. & Hernández-Navarrete L. D., 2025).

En comparación con la firma manuscrita, la firma digital presenta ventajas probatorias significativas. Mientras que la autenticidad de una firma manuscrita suele requerir peritajes grafotécnicos complejos, la firma digital puede verificarse de manera objetiva mediante herramientas criptográficas (Ledesma Narváez, La prueba en el proceso civil, 2021).

La doctrina comparada ha destacado que esta objetivación de la prueba contribuye a una mayor racionalidad del proceso judicial, al reducir la dependencia de valoraciones subjetivas y de pruebas periciales contradictorias (Vásquez Azuara, 2017).

En el ámbito arbitral empresarial, la eficacia probatoria de la firma digital adquiere aún mayor relevancia, dado que los árbitros suelen privilegiar pruebas documentales claras, verificables y técnicamente confiables (Canga, 2005).

No obstante, la eficacia probatoria de la firma digital no es absoluta. Puede ser cuestionada si se demuestra la revocación del certificado, la vulneración del sistema de firma o la falta de correspondencia entre el titular del certificado y el firmante efectivo (Becerra Lino, 2025).

En estos casos, la impugnación de la firma digital exige una carga probatoria elevada, lo que refuerza su eficacia jurídica en comparación con otros medios de prueba electrónicos menos sofisticados (Hernández-García, M. E. & Hernández-Navarrete L. D., 2025).

Desde la perspectiva del derecho empresarial, esta fortaleza probatoria incentiva el uso de la firma digital en contratos de alto valor económico, operaciones financieras, contratos de suministro y acuerdos de confidencialidad, donde la prueba del consentimiento resulta crítica (Canga, 2005).

La eficacia probatoria de la firma digital también contribuye a la prevención de conflictos, al desalentar conductas oportunistas basadas en el desconocimiento del contrato o en la manipulación de documentos (Vásquez Azuara, 2017).

En el contexto peruano, el reconocimiento normativo de esta eficacia probatoria se alinea con estándares internacionales y con las mejores prácticas en materia de prueba

digital, fortaleciendo la confianza en el comercio electrónico y en la contratación empresarial digital (Ledesma Narváez, La prueba en el proceso civil, 2021).

Desde un enfoque constitucional, la eficacia probatoria de la firma digital se vincula con el derecho a la tutela jurisdiccional efectiva, en tanto garantiza que los contratos electrónicos puedan ser probados eficazmente ante los órganos jurisdiccionales (Becerra Lino, 2025).

En consecuencia, la firma digital no solo cumple una función técnica, sino que se erige como un instrumento jurídico de alto valor probatorio, capaz de integrarse armónicamente al sistema procesal civil y mercantil peruano (Canga, 2005).

En síntesis, la eficacia probatoria de la firma digital constituye uno de los principales argumentos a favor de su adopción masiva en los contratos empresariales, al ofrecer un nivel de certeza, seguridad y confiabilidad superior al de los mecanismos tradicionales de prueba documental.

4.4. La prueba en los contratos electrónicos

La prueba constituye un componente esencial de todo ordenamiento jurídico, en tanto habilita a las partes a acreditar hechos que generan, modifican o extinguen derechos y obligaciones. En los contratos electrónicos, el análisis probatorio exige articular la tradicional teoría de la prueba con las particularidades tecnológicas propias del soporte digital, sin desnaturalizar los principios procesales básicos del derecho probatorio (Ledesma Narváez, La prueba en el proceso civil, 2021).

El Código Procesal Civil peruano, comentado exhaustivamente por Gaceta Jurídica (2023), reconoce la admisibilidad de todo medio probatorio lícito dentro del proceso, sin exclusión de los documentos electrónicos. El juez debe ponderar la prueba documental digital bajo criterios objetivos de autenticidad e integridad, tal como lo haría con un documento físico tradicional, siempre que se garantice la identificación del autor y la inalterabilidad del contenido (Gaceta Jurídica, 2023).

El documento electrónico, definido normativamente como cualquier información generada o conservada en formato digital, ha dejado de ser un medio marginal para

convertirse en un eje probatorio central en la contratación moderna. La doctrina peruana sostiene que "la prueba documental debe ser valorada por el juzgador conforme a la credibilidad, fiabilidad y coherencia con el resto del acervo probatorio", lo cual se traslada al ámbito digital sin merma de efectos (Ledesma Narváez, La prueba en el proceso civil, 2021).

La Ley N.º 27269 – Ley de Firmas y Certificados Digitales expone en su artículo 1 que la firma electrónica y, en especial, la firma digital "tiene la misma validez y eficacia jurídica que la firma manuscrita u otra análoga que conlleve manifestación de voluntad". Esta equivalencia normativa se proyecta directamente al valor probatorio de los documentos electrónicos en sede judicial.

El artículo 2 de la misma ley exige que la firma electrónica asociada a un mensaje de datos permita vincular e identificar al firmante, así como garantizar la autenticación e integridad del documento electrónico. Este mandato legal coincide con la exigencia doctrinal de que el documento electrónico probatorio debe ser atribuible fehacientemente a una persona para que sea valorado como prueba.

En su comentario al Código Procesal Civil, la obra de Gaceta Jurídica (2023) enfatiza que la integridad del documento es un requisito probatorio esencial: "El juzgador debe evaluar si el documento presentado sufrió alteraciones", lo que en el ambiente electrónico se verifica a través de mecanismos criptográficos (Gaceta Jurídica, 2023).

En el ámbito de la prueba documental, Ledesma Narváez (2021) explica que la autenticidad, una de las condiciones para valorar un documento como prueba, exige certeza sobre la identidad del autor o firmante. En los documentos electrónicos, esta certeza se logra mediante firmas digitales amparadas por certificados emitidos en la Infraestructura Oficial de Firma Electrónica conforme al Reglamento de la Ley N.º 27269 (D.S. N.º 052-2008-PCM).

El principio de integridad, que forma parte de la valoración probatoria, adquiere especificidad técnica en los documentos electrónicos. A este respecto, Gaceta Jurídica (2023) indica que "los sellos de tiempo y las marcas de certificación digital aportan

elementos objetivos para verificar si el contenido ha sido modificado" (p. 395), lo cual refuerza el valor probatorio de dichos documentos.

El concepto de carga de la prueba, ampliamente desarrollado en la doctrina peruana, debe entenderse de manera dinámica en el entorno digital. Si una empresa presenta un contrato firmado digitalmente conforme a las exigencias legales, corresponde a la contraparte impugnar la autenticidad o integridad de la firma, no a quien la presenta demostrar su validez (Ledesma Narváez, La prueba en el proceso civil, 2021).

Este enfoque se alinea con la función de la prueba documental que subraya la obra de Gaceta Jurídica (2023): cuando un medio probatorio es presentado en su forma más confiable (como un documento electrónico con firma digital y sello de tiempo), su valor probatorio inicial goza de una presunción de veracidad que puede ser desvirtuada solo con prueba en contrario.

La integridad del documento electrónico, entendida como ausencia de alteraciones, constituye un valor probatorio crítico. Ledesma Narváez (2021) señala que "la integridad no solo es un atributo técnico, sino una garantía de que el contenido no ha sido alterado desde su emisión", lo cual en el contexto digital es verificado mediante algoritmos criptográficos.

El Reglamento de la Ley de Firmas y Certificados Digitales desarrolla la noción de certificado digital y su ciclo de vida, lo que permite a empresas y órganos jurisdiccionales verificar la vigencia y validez de las firmas digitales, elementos que consolidan la fuerza probatoria del documento firmado electrónicamente.

De acuerdo con la doctrina peruana, el documento electrónico firmado digitalmente se valora no de manera aislada, sino dentro de un conjunto probatorio coherente. La "probatio probatior" (prueba más fuerte) de un documento digital puede integrarse con otros medios probatorios como correos electrónicos, registros de sistema o comunicaciones, conformando un cuadro probatorio robusto y convincente (Gaceta Jurídica, 2023).

En casos de controversias contractuales, la fecha cierta del documento es un elemento crítico. Los sellos de tiempo electrónicos —mecanismos que acreditan el momento exacto de la firma— permiten que los jueces determinen con precisión la cronología contractual y, de ser necesario, resuelvan sobre prelación de obligaciones o cumplimiento de plazos (Ledesma Narváez, La prueba en el proceso civil, 2021).

La doctrina procesal civil peruana ha reconocido que, con la validación técnica adecuada, los documentos electrónicos pueden tener valor probatorio pleno, superando muchas limitaciones que tenían los documentos físicos ante la evidencia de falsificación, deterioro o pérdida (Gaceta Jurídica, 2023).

En consecuencia, la empresa que implementa sistemas de firma digital y almacenamiento seguro de documentos puede presentar estos como prueba documental primaria en procesos judiciales, administrativos o arbitrales, con la misma solvencia jurídica que un contrato tradicional en papel.

El valor probatorio de los documentos electrónicos también encuentra soporte en la normativa comparada. La Ley Modelo de la CNUDMI sobre Comercio Electrónico y otras normas internacionales consagran la neutralidad tecnológica, es decir, no discriminar los medios probatorios por su forma física o digital, siempre que cumplan sus funciones sociales y jurídicas.

En el ámbito peruano, ello implica que el juzgador debe valorar los documentos electrónicos atendiendo a su fiabilidad técnica, su relación con otros medios probatorios y su capacidad para reflejar con fidelidad la voluntad de las partes (Ledesma Narváez, La prueba en el proceso civil, 2021).

No obstante, el valor probatorio no se agota con la mera presentación de un documento electrónico. La parte que lo ofrece como prueba debe aportar —cuando sea necesario— los elementos que permitan su verificación técnica (por ejemplo, certificados digitales, sellos de tiempo y registros de auditoría de la plataforma utilizada).

Esto se vincula con la obligación de conservación documental: la empresa debe contar con políticas de archivo digital que garanticen el acceso, integridad y preservación de

los documentos electrónicos en el tiempo, de modo que puedan ser recuperados y verificados cuando se requiera su aporte probatorio en un proceso.

La jurisprudencia peruana, en línea con esta doctrina, ha admitido progresivamente la prueba electrónica en diversos ámbitos del derecho, reconociendo la validez de contratos electrónicos, correos con consentimiento manifiesto y documentos digitales firmados, cuando la parte demuestra que estos cumplen con los estándares de autenticidad, integridad y trazabilidad establecidos en la ley y en el reglamento.

Esta aceptación jurisprudencial otorga mayor certeza a las empresas al diseñar sus procesos de contratación digital, ya que la prueba documental no pierde eficacia por estar en formato electrónico, siempre que la firma digital haya sido aplicada conforme a la Ley N.º 27269 y su Reglamento.

Desde una perspectiva práctica, esto implica que el uso de herramientas tecnológicas de firma digital con certificados válidos, sellos de tiempo y registros de sistema robustos permite a las empresas consolidar su acervo probatorio sin depender exclusivamente de medios tradicionales, contribuyendo a una administración de justicia más eficiente y coherente con la realidad digital.

A nivel doctrinal y jurisprudencial, la prueba en los contratos electrónicos implica una evaluación técnico-jurídica híbrida: se ponderan tanto los aspectos normativos tradicionales del derecho procesal civil como los atributos técnicos que permiten acreditar la autenticidad e integridad del documento electrónico.

En suma, el valor probatorio del documento electrónico en los contratos electrónicos no solo está reconocido por el marco legal peruano (Ley N.º 27269 y su Reglamento), sino que se sustenta en una sólida doctrina procesal civil que concibe al documento documental digital como un medio probatorio robusto, confiable y plenamente integrable al sistema de prueba general, equiparable —cuando cumple los requisitos exigidos— al documento físico tradicional.

4.5. La firma digital como medio de prueba

La firma digital, entendida como un tipo cualificado de firma electrónica basado en criptografía de clave pública, ha adquirido en el derecho contemporáneo un rol epistemológico central en la configuración de la prueba documental electrónica, particularmente en el ámbito de los contratos celebrados por medios digitales. Esta función probatoria no se limita a una aptitud técnica, sino que posee efectos jurídicos objetivos mediante la atribución de presunciones legales, garantías de integridad y la mitigación del no repudio.

En el derecho peruano, la Ley N.º 27269 – Ley de Firmas y Certificados Digitales reconoce expresamente que la firma electrónica, y de manera más sólida la firma digital, tiene la misma validez jurídica que la firma manuscrita, lo que incluye su admisibilidad y eficacia como medio probatorio en sede judicial o arbitral siempre que cumpla los requisitos legales.

Para entender la eficacia probatoria de la firma digital, resulta necesario explorar tres nociones jurídicas claves: las presunciones legales, la integridad del documento y el principio de no repudio. Estas categorías actúan como pilares que hacen robusta a la firma digital dentro del sistema probatorio moderno.

El concepto de presunción legal se refiere a la atribución de una verdad provisional por mandato de la ley, hasta que se demuestre lo contrario por medios probatorios idóneos. En el contexto de la firma digital, esta presunción opera desde el momento de la validación técnica de la firma y del certificado digital que la respalda.

La obra *La prueba en el proceso civil* de Marianella Ledesma Narváez, referencia doctrinal imprescindible en el derecho procesal peruano, desarrolla la noción de presunción de veracidad de los documentos que cumplen con los requisitos de autenticidad e integridad, lo cual se extiende a los documentos electrónicos firmados digitalmente cuando están correctamente certificados y registrados.

Según Ledesma Narváez (2021), "la prueba documental que proporciona certeza sobre la identidad del autor y la integridad del documento goza de una presunción de

veracidad que solo puede ser desvirtuada con elementos probatorios que acrediten lo contrario", lo que en el ámbito digital se traduce en la confianza jurídica de la firma digital.

El Reglamento de la Ley N.º 27269 (D.S. N.º 052-2008-PCM) desarrolla cómo las entidades de certificación y registro de esta infraestructura oficial (IOFE) emiten certificados digitales que posibilitan la atribución de la firma a un sujeto identificado, lo que alimenta precisamente la presunción legal de validez del medio probatorio.

El segundo eje de análisis es la integridad del documento electrónico, que garantiza que el contenido del documento no ha sido alterado desde la fecha de su firma digital. Esta cualidad técnica es medible y verificable mediante algoritmos criptográficos que detectan cualquier modificación posterior.

La doctrina peruana sobre prueba documental tradicional, como *La prueba documental en el proceso civil* de Alberto Hinostroza Mínguez, subraya que la integridad constituye un criterio probatorio esencial, pues un documento alterado pierde su valor probatorio. Este principio se conserva y amplifica en el entorno de la prueba digital (Hinostroza Mínguez, 2018).

La obra enfatiza que "la integridad del documento es uno de los elementos que más influye en la valoración probatoria, especialmente cuando la verificación técnica permite detectar alteraciones que comprometen la fiabilidad de la prueba".

Aplicado a la firma digital, dicha integridad se logra mediante funciones hash, sellos de tiempo y certificados digitales que, combinados, aseguran que cualquier modificación del texto o metadatos del documento quede evidenciada, reforzando así su valor como prueba de hechos jurídicos.

El tercer eje, el principio de no repudio, hace referencia a la imposibilidad jurídica de negar la autoría de la firma digital realizada. En un documento firmado digitalmente según ley, quien niega haber firmado asume la carga de probar que la firma fue objeto de fraude, error técnico o suplantación.

En jurisprudencia procesal civil, recogida y analizada en obras como *La prueba en el derecho civil y procesal civil en la jurisprudencia casatoria*, la negación injustificada de la autoría de un documento firmado digitalmente debe enfrentarse no solo con presunciones legales, sino con evidencia técnica que demuestre fallas en el proceso de firma o compromiso de la clave privada.

El enfoque doctrinal peruano, apoyado en estos textos procesales, sostiene que la combinación del certificado digital, la infraestructura de registro y la propia tecnología criptográfica crea un entorno probatorio más sólido que la mera firma manuscrita sin soporte adicional.

Desde esta perspectiva, la firma digital se convierte en un medio probatorio superior en ciertos aspectos, porque permite reconstruir con precisión: (i) la identidad del firmante, (ii) el momento de la firma (sellos de tiempo), y (iii) la invariabilidad del documento, lo que favorece una valoración probatoria objetiva.

El profesor Hinostroza Mínguez observa que en los procesos civiles "el valor probatorio de un documento está en función de su credibilidad técnica y legal", lo cual en el entorno digital se traduce en una mayor confiabilidad cuando se emplean estándares criptográficos reconocidos (Hinostroza Mínguez, 2018).

Esta característica técnica y jurídica de la firma digital hace que, en la práctica judicial peruana, los jueces tiendan a otorgarle un peso probatorio elevado cuando se presentan como prueba en disputas contractuales, siempre que se acredite su correcta generación y conservación.

La presunción legal de validez de la firma digital puede ser desvirtuada, pero ello exige presentar evidencia técnica robusta, como peritajes forenses que demuestren compromisos en las claves criptográficas o vulneraciones de la infraestructura de certificación.

Esto contrasta con los documentos electrónicos simples (por ejemplo, correos electrónicos sin firma digital), cuya eficacia probatoria suele depender más de la

valoración discrecional del juez y de la corroboración con otras pruebas complementarias.

En el proceso civil peruano, el juez valora la prueba conforme a los principios de verdad material y sana crítica. La existencia de presunciones legales fuertes asociadas a la firma digital orienta esa valoración, otorgando mayor peso a documentos que cumplieron con estándares técnicos y legales.

El principio de no repudio se vincula también con la cadena de custodia del documento electrónico y del certificado digital. La preservación de estos elementos en sistemas seguros ayuda a que la parte demandante o demandada pueda demostrar que la firma no fue resultado de un artefacto fraudulento.

La literatura doctrinal peruana en derecho procesal resalta que, en ausencia de indicios claros de manipulación, la negación de la firma digital por un litigante obliga a un esfuerzo probatorio mayor por parte del impugnante, reforzando así la presunción de veracidad inicial.

Este enfoque procesal se complementa con reglas de admisibilidad probatoria que permiten al juzgador solicitar medios auxiliares de verificación técnica, como informes periciales de expertos en sistemas de firma digital.

La integración de elementos técnicos como sellos de tiempo, códigos de verificación y registros de auditoría no solo fortalece la integridad del documento, sino que también contribuye a la solidez de la valoración judicial en sede probatoria.

En consecuencia, la firma digital eleva la fiabilidad del documento electrónico como prueba, dado que incorpora mecanismos de autentificación que van más allá de la mera percepción subjetiva, introduciendo criterios técnicos verificables objetivamente.

Juristas peruanos señalan que esta evolución probatoria responde a la necesidad de adaptar el derecho de la prueba a la realidad digital, donde los medios electrónicos son cada vez más prevalentes para demostrar la realización de actos jurídicos.

Desde una perspectiva crítica, algunos autores procesales advierten que la eficacia probatoria de la firma digital debe acompañarse de protocolos de conservación adecuada, a fin de evitar la pérdida de accesibilidad o incompatibilidades tecnológicas que puedan comprometer su verificación futura.

La doctrina moderna coloca a la firma digital en el espectro de las pruebas preconstituidas de alta confiabilidad, lo que contribuye a una mayor predictibilidad en la valoración de la prueba y al fortalecimiento de la seguridad jurídica en litigios contractuales.

El contenido de estos libros de derecho procesal civil peruano, combinados con la regulación específica de la firma digital, ofrece una base teórica y práctica sólida para comprender por qué la firma digital ha trascendido su dimensión técnica para constituirse en un medio probatorio robusto y confiable.

En síntesis, la firma digital, mediante presunciones legales, mecanismos de integridad y principios de no repudio, se ubica como un medio de prueba de primer orden en los contratos electrónicos, aportando niveles de certeza, verificabilidad técnica y valor probatorio que permiten su integración armónica al sistema de prueba establecido por el derecho procesal civil peruano contemporáneo.

4.6. Carga de la prueba y controversias judiciales

La carga de la prueba constituye uno de los ejes estructurales del proceso judicial, al determinar qué parte asume las consecuencias jurídicas derivadas de la falta de acreditación de los hechos controvertidos. En el ámbito de los contratos electrónicos y del uso de la firma digital, este principio adquiere una complejidad singular, debido a la naturaleza técnica del medio probatorio y a la asimetría de información existente entre las partes. La doctrina procesal peruana ha señalado que la carga probatoria no solo cumple una función de distribución del riesgo procesal, sino también una función de orientación del juez en escenarios de incertidumbre fáctica (Ledesma Narváez, La prueba en el proceso civil, 2021). En este contexto, la firma digital introduce nuevos desafíos relacionados con la autenticidad, integridad y autoría del documento

electrónico, que inciden directamente en la determinación de quién debe probar qué hechos y bajo qué estándares.

Desde la perspectiva del Código Procesal Civil peruano, la carga de la prueba se rige por el principio general según el cual quien afirma un hecho relevante para su pretensión debe probarlo. Sin embargo, este criterio clásico se ve tensionado cuando el objeto probatorio es un documento electrónico firmado digitalmente, ya que su valoración exige conocimientos técnicos que superan el entendimiento ordinario del litigante promedio. Hinostroza Mínguez sostiene que, en estos casos, el juez debe adoptar una interpretación flexible de la carga probatoria, considerando la posibilidad de una carga dinámica de la prueba, especialmente cuando una de las partes se encuentra en mejor posición técnica o jurídica para acreditar la validez del documento digital (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). Esta postura resulta particularmente relevante en controversias empresariales, donde una de las partes suele controlar la infraestructura tecnológica.

La doctrina peruana ha resaltado que la carga de la prueba no puede analizarse de manera aislada, sino en relación con los principios de colaboración procesal y buena fe. Monroy Gálvez explica que el proceso civil moderno exige que las partes cooperen en la esclarecimiento de los hechos, evitando conductas obstructivas que dificulten la valoración probatoria (Monroy Gálvez, 2015). En el caso de la firma digital, esta colaboración se traduce en la obligación de facilitar información técnica sobre certificados digitales, proveedores de servicios de certificación y mecanismos de validación utilizados. La negativa injustificada a proporcionar tales elementos puede justificar una inversión o flexibilización de la carga probatoria, conforme a los criterios desarrollados por la jurisprudencia nacional y comparada.

Uno de los principales problemas probatorios en controversias sobre firma digital es la dificultad de demostrar la autoría del acto electrónico cuando el titular del certificado niega haber suscrito el documento. En estos casos, la presunción de autoría derivada del uso del certificado digital juega un rol central. Ticona Postigo señala que las presunciones legales cumplen una función instrumental al aliviar la carga probatoria de la parte que invoca el documento, trasladando al impugnante la obligación de

demostrar la existencia de un uso indebido o comprometido del certificado (Ticona Postigo, 2014). No obstante, esta presunción no es absoluta y admite prueba en contrario, lo que abre un espacio significativo para controversias judiciales complejas.

La dificultad probatoria se intensifica cuando el cuestionamiento se centra en aspectos técnicos como la integridad del documento electrónico o la validez temporal de la firma digital. Varsi Rospigliosi advierte que, a diferencia de los documentos en soporte papel, los documentos electrónicos requieren de mecanismos adicionales de verificación, tales como sellos de tiempo y registros de auditoría. La ausencia o deficiencia de estos elementos puede debilitar la fuerza probatoria del documento, generando controversias que exigen la intervención de peritos informáticos. En este escenario, la carga de la prueba se ve fragmentada entre las partes y el órgano jurisdiccional, que debe evaluar la suficiencia de la prueba técnica aportada (Varsi Rospigliosi, 2016).

La jurisprudencia peruana ha empezado a desarrollar criterios específicos para la valoración de la prueba digital, reconociendo que la firma digital, cuando cumple los requisitos legales, goza de una presunción de validez similar a la firma manuscrita. Sin embargo, Castillo Freyre sostiene que esta equivalencia funcional no elimina la necesidad de un análisis crítico del contexto probatorio, especialmente cuando existen indicios de fraude o suplantación. En tales casos, la carga de la prueba puede desplazarse hacia quien se beneficia del documento, exigiéndole demostrar que el sistema de firma digital utilizado ofrecía garantías suficientes de seguridad y control (Castillo Freyre, 2013).

Otro aspecto relevante es la distribución de la carga probatoria en relación con los proveedores de servicios de certificación. Gaceta Jurídica destaca que, si bien estos proveedores no son parte directa del contrato, su actuación puede ser determinante para esclarecer controversias sobre la validez de la firma digital (Gaceta Jurídica, 2019). La información técnica que poseen —registros de emisión, suspensión o revocación de certificados— resulta esencial para la resolución del conflicto. En consecuencia, el juez puede ordenar la exhibición de dichos registros, atenuando la carga probatoria de las partes cuando se encuentren materialmente impedidas de acceder a esa información.

La carga de la prueba también se vincula estrechamente con el estándar de prueba aplicable en materia civil. Landa Arroyo señala que el juez debe alcanzar un grado de convicción suficiente basado en la preponderancia de la prueba, sin exigir una certeza absoluta. En el caso de la firma digital, este estándar se satisface cuando el conjunto de elementos técnicos y documentales permite inferir razonablemente la autenticidad del acto. La dificultad radica en traducir conceptos técnicos complejos a un lenguaje jurídico comprensible, lo que exige del juez una especial diligencia en la valoración probatoria (Landa Arroyo, 2018).

Desde una perspectiva comparada, diversos estudios científicos han resaltado la necesidad de capacitar a los jueces en materia de prueba digital. Autores como Varsi Rospigliosi sostienen que la falta de formación técnica puede generar decisiones inconsistentes o excesivamente formales. Esta problemática también se observa en el contexto peruano, donde la valoración de la firma digital depende en gran medida de la claridad de los informes periciales y de la capacidad del juez para integrarlos en su razonamiento jurídico. La carga de la prueba, en este sentido, se ve condicionada por factores institucionales que trascienden a las partes (Varsi Rospigliosi, 2016).

La doctrina nacional ha propuesto la adopción expresa de la carga dinámica de la prueba en controversias sobre firma digital. Ledesma Narváez sostiene que este enfoque permite asignar la carga probatoria a la parte que se encuentra en mejores condiciones de probar un hecho determinado, atendiendo a criterios de razonabilidad y equidad (Ledesma Narváez, La prueba en el proceso civil, 2021). En contratos empresariales, esta solución resulta especialmente adecuada cuando una de las partes administra la plataforma digital utilizada para la firma, mientras que la otra se limita a adherirse al sistema. En tales supuestos, exigir al adherente la prueba de un fallo técnico resultaría desproporcionado.

La carga de la prueba también se relaciona con el principio de igualdad procesal. Hinostroza Mínguez advierte que una aplicación rígida de las reglas tradicionales puede generar situaciones de desigualdad material, especialmente en litigios donde existe una brecha tecnológica significativa (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). La firma digital, al ser un instrumento altamente especializado,

puede convertirse en una barrera probatoria para sujetos sin conocimientos técnicos. Por ello, el juez debe interpretar las reglas probatorias a la luz de los principios constitucionales de tutela jurisdiccional efectiva y debido proceso.

En las controversias judiciales sobre contratos electrónicos, resulta frecuente que la discusión probatoria se centre en la existencia misma del consentimiento. Monroy Gálvez explica que el consentimiento electrónico debe analizarse considerando el diseño de la interfaz, los mecanismos de aceptación y la información proporcionada al usuario (Monroy Gálvez, 2015). La carga de probar que el consentimiento fue libre e informado recae, por lo general, en quien diseñó el sistema de contratación. Esta orientación resulta coherente con la doctrina científica que analiza la validez del consentimiento en entornos digitales.

La valoración judicial de la prueba digital exige un enfoque integral que combine elementos jurídicos y técnicos. Ticona Postigo señala que el juez no puede limitarse a verificar la existencia formal de la firma digital, sino que debe analizar su funcionamiento concreto en el caso específico (Ticona Postigo, 2014). Esto implica examinar la vigencia del certificado, la integridad del documento y la fiabilidad del proveedor de certificación. La carga de la prueba se distribuye, entonces, entre las partes y los terceros involucrados, configurando un escenario probatorio complejo y multidimensional.

Las controversias sobre firma digital también ponen de relieve la importancia de la prueba pericial informática. Varsi Rospigliosi sostiene que la pericia no solo cumple una función ilustrativa, sino que puede ser decisiva para la resolución del conflicto (Varsi Rospigliosi, 2016). Sin embargo, la carga de solicitar y sustentar adecuadamente la pericia recae en las partes, lo que puede generar desigualdades cuando una de ellas carece de recursos. Este problema ha sido señalado por la doctrina científica como uno de los principales obstáculos para la efectividad de la prueba digital en procesos civiles (Casey, 2018).

La jurisprudencia peruana ha mostrado una tendencia a otorgar un alto valor probatorio a la firma digital certificada, siempre que no existan indicios razonables de

irregularidad. Castillo Freyre explica que esta postura busca fomentar la seguridad jurídica y la confianza en los medios electrónicos (Castillo Freyre, 2013). No obstante, esta presunción favorable no exonera a la parte que invoca la firma de acreditar el cumplimiento de los requisitos legales, especialmente cuando la otra parte plantea una impugnación fundada. La carga de la prueba, en este sentido, se convierte en un instrumento de equilibrio entre eficiencia y garantía.

El análisis de la carga probatoria también debe considerar el rol del juez como director del proceso. Gaceta Jurídica señala que el juez tiene facultades para ordenar pruebas de oficio cuando lo considere necesario para esclarecer los hechos controvertidos (Gaceta Jurídica, 2019). En materia de firma digital, esta facultad resulta particularmente relevante, dado que la verdad técnica puede no emerger claramente de la prueba aportada por las partes. La intervención judicial, sin embargo, debe respetar el principio de imparcialidad y no sustituir indebidamente la iniciativa probatoria de los litigantes.

Desde una perspectiva teórica, la carga de la prueba cumple una función epistémica, al orientar la búsqueda de la verdad procesal. Landa Arroyo sostiene que el debido proceso exige que las reglas probatorias sean predecibles y razonables (Landa Arroyo, 2018). En el ámbito digital, esta exigencia se traduce en la necesidad de criterios claros sobre la valoración de la firma digital y la distribución de la carga probatoria. La ausencia de tales criterios puede generar inseguridad jurídica y desalentar el uso de tecnologías de firma electrónica en el ámbito empresarial.

La doctrina científica internacional ha propuesto modelos de valoración probatoria basados en el análisis de riesgos. Kessler sugiere que el juez evalúe la probabilidad de error del sistema de firma digital utilizado, considerando factores como el nivel de certificación y los mecanismos de control (Gary C., 2010). Este enfoque podría complementar las reglas tradicionales de carga de la prueba, permitiendo una valoración más contextualizada y técnica. Su adopción en el contexto peruano requeriría, no obstante, un desarrollo jurisprudencial y doctrinal más robusto.

Las controversias judiciales sobre firma digital también evidencian la necesidad de una adecuada conservación de la prueba electrónica. Hinostroza Mínguez destaca que la pérdida o alteración de registros digitales puede dificultar gravemente la acreditación de los hechos (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). La carga de preservar la prueba suele recaer en quien administra el sistema informático, lo que refuerza la idea de una carga probatoria diferenciada. Este criterio ha sido respaldado por estudios científicos sobre gestión de evidencia digital.

La interacción entre la carga de la prueba y las presunciones legales es particularmente relevante en materia de firma digital. Ticona Postigo explica que las presunciones operan como atajos probatorios, pero no deben aplicarse de manera automática (Ticona Postigo, 2014). El juez debe evaluar si las circunstancias del caso justifican mantener la presunción o permitir su desvirtuación. En controversias empresariales complejas, esta evaluación requiere un análisis detallado del funcionamiento del sistema de firma y de las conductas de las partes.

La doctrina peruana ha subrayado que la carga de la prueba no es estática, sino que puede variar a lo largo del proceso. Ledesma Narváez señala que, a medida que se incorporan nuevos elementos probatorios, la carga puede desplazarse de una parte a otra (Ledesma Narváez, La prueba en el proceso civil, 2021). En litigios sobre firma digital, este dinamismo es frecuente, especialmente cuando la pericia informática revela información que modifica el panorama probatorio. El juez debe estar atento a estos cambios para evitar decisiones injustas o desproporcionadas.

La valoración judicial de la prueba digital también se ve influida por el principio de inmediación. Monroy Gálvez advierte que, aunque el juez no percibe directamente el funcionamiento del sistema digital, debe interactuar activamente con los medios probatorios disponibles (Monroy Gálvez, 2015). La audiencia de actuación y explicación de la pericia informática se convierte, así, en un espacio clave para la formación de la convicción judicial. La carga de la prueba se articula, entonces, con la calidad de la exposición técnica realizada en sede judicial.

En el ámbito empresarial, las controversias sobre firma digital suelen involucrar altos montos y riesgos significativos. Varsi Rospigliosi sostiene que, en estos casos, el juez debe aplicar un estándar de valoración especialmente riguroso, sin caer en un formalismo excesivo (Varsi Rospigliosi, 2016). La carga de la prueba debe distribuirse de manera que incentive a las empresas a implementar sistemas de firma digital robustos y auditables. Este enfoque contribuye a la prevención de conflictos y al fortalecimiento de la confianza en el comercio electrónico.

La doctrina científica ha resaltado la importancia de la trazabilidad como elemento probatorio clave. Reedy indica que la capacidad de reconstruir el historial completo de un documento electrónico facilita la valoración judicial y reduce las controversias (Reedy, 2020). En este sentido, la carga de implementar sistemas de trazabilidad recae en quienes diseñan y gestionan las plataformas de firma digital. La ausencia de tales sistemas puede interpretarse en contra de la parte que tenía el control tecnológico.

La carga de la prueba también se vincula con la protección del derecho de defensa. Landa Arroyo señala que las reglas probatorias no deben impedir que una parte pueda cuestionar razonablemente la autenticidad de una firma digital (Landa Arroyo, 2018). El acceso a la información técnica y la posibilidad de contradecir la pericia son elementos esenciales del debido proceso. En este marco, el juez debe equilibrar la presunción de validez de la firma digital con el derecho a una defensa efectiva.

Las controversias judiciales han puesto de relieve la necesidad de criterios uniformes de valoración. Gaceta Jurídica destaca que la dispersión de criterios genera inseguridad jurídica y decisiones contradictorias (Gaceta Jurídica, 2019). La carga de la prueba, al depender en gran medida de la interpretación judicial, requiere una orientación doctrinal clara. El desarrollo de precedentes vinculantes podría contribuir a una mayor coherencia en la resolución de conflictos sobre firma digital.

Desde una perspectiva práctica, la carga de la prueba influye en la estrategia procesal de las partes. Castillo Freyre sostiene que quien invoca un contrato electrónico debe anticipar posibles impugnaciones y preparar un soporte probatorio sólido (Castillo Freyre, 2013). Esto incluye la conservación de registros, la identificación del proveedor

de certificación y la disponibilidad de peritos. La adecuada gestión probatoria puede marcar la diferencia entre el éxito y el fracaso de la pretensión.

La doctrina comparada ha señalado que la carga de la prueba en materia digital tiende a desplazarse hacia modelos más flexibles. Chang propone un enfoque basado en la razonabilidad y la proporcionalidad, que tenga en cuenta la complejidad técnica del medio probatorio (Chang O'Campo, 2000). Este enfoque resulta compatible con los principios del proceso civil peruano y podría enriquecer la práctica judicial en controversias sobre firma digital.

En definitiva, la carga de la prueba en controversias sobre firma digital exige una reinterpretación de las categorías tradicionales del derecho probatorio. Ticona Postigo advierte que el derecho procesal no puede permanecer ajeno a los cambios tecnológicos (Ticona Postigo, 2014). La firma digital no solo transforma la forma de contratar, sino también la manera de probar los hechos. La adaptación de las reglas probatorias es, por tanto, una condición necesaria para la efectividad del sistema jurídico.

Como conclusión, puede afirmarse que la carga de la prueba y la valoración judicial en materia de firma digital constituyen un campo en evolución, marcado por desafíos técnicos y jurídicos. La doctrina peruana y la literatura científica coinciden en la necesidad de un enfoque flexible, dinámico y garantista. La adecuada distribución de la carga probatoria, combinada con criterios de valoración razonables, permite resolver las controversias judiciales de manera justa y eficiente, fortaleciendo la confianza en los contratos electrónicos y en la firma digital como medio probatorio legítimo.

4.7. Límites legales al uso de firmas electrónicas

El reconocimiento jurídico de la firma electrónica y la firma digital no implica su aplicación irrestricta a todos los actos jurídicos. Tanto el derecho comparado como el ordenamiento peruano han establecido límites legales claros, orientados a preservar la seguridad jurídica en aquellos actos que, por su trascendencia personal, patrimonial o social, exigen formalidades reforzadas. Desde la perspectiva del derecho procesal, estos límites inciden directamente en la validez del acto y en su eventual eficacia

probatoria. Como señala Ledesma Narváez, la determinación de los actos excluidos del uso de medios electrónicos responde a criterios de protección del consentimiento y de prevención de fraudes, especialmente en contextos donde la tecnología aún no garantiza un control absoluto sobre la identidad del firmante (Ledesma Narváez, La prueba en el proceso civil, 2021).

En el ordenamiento peruano, la Ley N.º 27269 reconoce la equivalencia jurídica de la firma digital respecto de la manuscrita, pero lo hace bajo el presupuesto de que no exista una prohibición legal expresa. Esta cláusula de salvaguarda revela que el legislador ha optado por un modelo de habilitación condicionada. Hinostroza Mínguez sostiene que esta técnica legislativa evita una aplicación mecánica de la firma electrónica en ámbitos donde el riesgo jurídico es elevado, como ocurre con actos de disposición patrimonial de especial relevancia (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). Así, el límite legal no constituye una negación del valor de la tecnología, sino un mecanismo de equilibrio entre innovación y seguridad jurídica.

Uno de los principales grupos de actos jurídicos excluidos del uso de firmas electrónicas corresponde a aquellos que requieren forma solemne ad solemnitatem. Monroy Gálvez explica que la forma solemne no es un simple requisito probatorio, sino un elemento constitutivo del acto jurídico (Monroy Gálvez, 2015). En estos casos, la exigencia de escritura pública o intervención notarial cumple una función de control y asesoramiento que no puede ser sustituida íntegramente por medios electrónicos. La firma digital, aunque técnicamente segura, no reproduce por sí sola el conjunto de garantías que ofrece la actuación presencial del notario.

En el ámbito del derecho civil peruano, los actos de disposición sobre bienes inmuebles constituyen un ejemplo paradigmático de esta exclusión. Ticona Postigo señala que la transferencia de propiedad inmobiliaria exige escritura pública inscrita, lo que implica la intervención de un fedatario y el cumplimiento de una cadena de formalidades (Ticona Postigo, 2014). Aunque en otros ordenamientos se ha avanzado hacia la digitalización notarial, en el Perú la normativa vigente mantiene una postura conservadora. Este límite legal responde a la necesidad de proteger la seguridad del

tráfico jurídico inmobiliario y prevenir litigios derivados de suplantaciones o errores tecnológicos.

Las disposiciones testamentarias también se encuentran tradicionalmente excluidas del uso de firmas electrónicas. Varsi Rospigliosi destaca que el testamento es un acto personalísimo, cuya validez depende no solo de la autenticidad de la firma, sino también de la comprobación de la capacidad y libertad del testador (Varsi Rospigliosi, 2016). La presencia de testigos o del notario cumple una función de garantía que difícilmente puede ser replicada en entornos digitales. Este límite evidencia que la exclusión no se basa en la desconfianza hacia la tecnología, sino en la protección reforzada de la voluntad del otorgante.

Desde la óptica del derecho procesal, estos actos excluidos presentan consecuencias relevantes en materia probatoria. Castillo Freyre sostiene que un documento electrónico firmado digitalmente carecerá de eficacia probatoria plena si el acto que documenta está legalmente excluido del uso de firma electrónica (Castillo Freyre, 2013). En tales supuestos, el documento podrá tener un valor indiciario, pero no acreditará la validez del acto jurídico. Este criterio refuerza la idea de que los límites legales operan tanto en el plano sustantivo como en el procesal.

Otro ámbito de restricción lo constituyen las formalidades especiales impuestas por normas sectoriales. Gaceta Jurídica señala que determinadas operaciones societarias, como la constitución de sociedades o la modificación de estatutos, exigen formalidades específicas que pueden limitar el uso de firmas electrónicas (Gaceta Jurídica, 2019). Aunque la tendencia apunta hacia la digitalización registral, la normativa vigente aún exige, en muchos casos, la intervención notarial presencial. Esta situación genera tensiones entre la eficiencia empresarial y el respeto a las formalidades legales.

En materia de derecho de familia, los límites al uso de firmas electrónicas son aún más marcados. Landa Arroyo explica que actos como el matrimonio, el reconocimiento de hijos o la adopción involucran derechos fundamentales y requieren un control estatal reforzado (Landa Arroyo, 2018). La exclusión de la firma electrónica en estos supuestos se justifica por la necesidad de garantizar la autenticidad del consentimiento y la

protección de las personas en situación de vulnerabilidad. Desde el punto de vista constitucional, estas restricciones se alinean con el principio de tutela especial de la familia.

La doctrina científica internacional respalda la existencia de estos límites. Reedy señala que incluso en sistemas jurídicos altamente digitalizados se mantienen reservas respecto de ciertos actos solemnes (Reedy, 2020). La experiencia comparada demuestra que la digitalización total sin límites puede incrementar el riesgo de litigios y fraudes. En este sentido, los límites legales cumplen una función preventiva y contribuyen a la estabilidad del sistema jurídico.

Un aspecto particularmente relevante es la restricción vinculada a la protección de datos personales. Hinostroza Mínguez advierte que el uso de firmas electrónicas implica el tratamiento de información sensible, como datos biométricos o certificados digitales (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). En determinados actos, la ley puede restringir el uso de firmas electrónicas para evitar una exposición indebida de datos personales. Esta limitación se articula con la normativa de protección de datos y refuerza la idea de un uso responsable de la tecnología.

En el ámbito empresarial, los límites legales también se manifiestan en contratos regulados por normas especiales. Monroy Gálvez señala que ciertos contratos financieros o de seguros pueden exigir formalidades adicionales, como declaraciones presenciales o verificaciones específicas de identidad (Monroy Gálvez, 2015). La firma electrónica, en estos casos, puede ser utilizada de manera complementaria, pero no sustituir completamente las exigencias legales. Esta coexistencia de medios refleja un enfoque gradualista en la adopción de tecnologías jurídicas.

Desde la perspectiva de la prueba, la existencia de límites legales plantea desafíos interpretativos para el juez. Ticona Postigo explica que el órgano jurisdiccional debe distinguir entre la invalidez del acto y la invalidez del medio probatorio (Ticona Postigo, 2014). Un documento firmado electrónicamente puede ser auténtico, pero carecer de eficacia jurídica si el acto está excluido. Esta distinción resulta esencial para evitar decisiones erróneas que confundan la forma con el fondo del acto jurídico.

La jurisprudencia peruana ha sido cautelosa en la interpretación de estos límites. Varsi Rospigliosi señala que los jueces tienden a privilegiar la seguridad jurídica frente a la innovación tecnológica cuando existe duda razonable sobre la aplicabilidad de la firma electrónica (Varsi Rospigliosi, 2016). Este criterio conservador, aunque criticado por algunos sectores, busca evitar la generación de precedentes que puedan debilitar el sistema de formalidades legales.

Desde una perspectiva crítica, algunos autores sostienen que ciertos límites podrían ser revisados a la luz de los avances tecnológicos. Castillo Freyre reconoce que la firma digital ofrece niveles de seguridad superiores a la firma manuscrita, lo que justificaría una revisión progresiva de las exclusiones legales (Castillo Freyre, 2013). Sin embargo, esta revisión debe realizarse mediante reforma legislativa y no a través de interpretaciones judiciales extensivas que vulneren el principio de legalidad.

Los límites legales también cumplen una función pedagógica. Gaceta Jurídica indica que al establecer claramente los actos excluidos, el legislador orienta a los operadores jurídicos y a las empresas sobre el uso adecuado de la firma electrónica (Gaceta Jurídica, 2019). Esta claridad normativa reduce la litigiosidad y fomenta un uso responsable de la tecnología en el ámbito contractual.

En el contexto del comercio internacional, los límites nacionales pueden generar fricciones. Landa Arroyo señala que los contratos transfronterizos celebrados electrónicamente pueden enfrentar problemas de reconocimiento si involucran actos excluidos en uno de los ordenamientos (Landa Arroyo, 2018). Este escenario exige una coordinación normativa y una interpretación armónica de los principios de equivalencia funcional y autonomía de la voluntad.

La doctrina comparada ha propuesto el uso de listas taxativas de actos excluidos como mecanismo de certeza jurídica. Reedy destaca que este modelo reduce la discrecionalidad judicial y facilita la planificación contractual (Reedy, 2020). El ordenamiento peruano se aproxima a este enfoque, aunque aún subsisten zonas grises que requieren desarrollo jurisprudencial.

En materia probatoria, los límites legales influyen en la estrategia procesal de las partes. Hinostroza Mínguez sostiene que quien invoque un documento firmado electrónicamente debe verificar previamente que el acto no se encuentre excluido (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). De lo contrario, corre el riesgo de que su pretensión sea desestimada por un defecto formal insubsanable.

La exclusión de determinados actos también se vincula con la protección del orden público. Monroy Gálvez explica que ciertos actos tienen una dimensión social que trasciende la autonomía privada, lo que justifica la imposición de formalidades estrictas (Monroy Gálvez, 2015). La firma electrónica, en estos casos, no es suficiente para garantizar el interés público involucrado.

Desde el punto de vista constitucional, los límites legales deben ser razonables y proporcionales. Landa Arroyo advierte que una exclusión excesiva podría vulnerar la libertad de contratación y el derecho al desarrollo tecnológico (Landa Arroyo, 2018). Por ello, el análisis de los límites debe realizarse a la luz de los principios de necesidad y adecuación.

La doctrina científica ha señalado que los límites legales no son estáticos. Reedy sostiene que la evolución tecnológica puede justificar la revisión periódica de las exclusiones (Reedy, 2020). Esta visión dinámica resulta compatible con un derecho adaptativo que responda a los cambios sociales sin sacrificar la seguridad jurídica.

En el ámbito notarial, se discute activamente la posibilidad de ampliar el uso de firmas electrónicas. Varsi Rospigliosi indica que la digitalización notarial podría reducir costos y tiempos, pero requiere una infraestructura normativa y tecnológica robusta (Varsi Rospigliosi, 2016). Mientras ello no ocurra, los límites actuales seguirán siendo necesarios.

Las restricciones legales también afectan la eficacia internacional de los documentos electrónicos. Ticona Postigo señala que un acto válido electrónicamente en un país puede ser inválido en otro si se encuentra excluido (Ticona Postigo, 2014). Esta situación refuerza la importancia del análisis previo del marco legal aplicable.

Desde la perspectiva empresarial, los límites legales exigen una adecuada gestión de riesgos. Castillo Freyre sostiene que las empresas deben identificar claramente qué actos pueden celebrarse electrónicamente y cuáles requieren formalidades tradicionales (Castillo Freyre, 2013). Esta planificación reduce contingencias legales y fortalece la seguridad contractual.

La carga de la prueba también se ve influida por estos límites. Hinostroza Mínguez explica que, cuando un acto está excluido, no basta probar la autenticidad de la firma electrónica; es necesario acreditar el cumplimiento de la formalidad exigida (Hinostroza Mínguez, La prueba documental en el proceso civil, 2018). Este criterio refuerza la centralidad de la forma en determinados actos jurídicos.

La doctrina peruana coincide en que los límites legales no deben interpretarse extensivamente. Monroy Gálvez advierte que una interpretación expansiva podría frenar innecesariamente la innovación (Monroy Gálvez, 2015). Por ello, cualquier duda debe resolverse a favor de la validez del acto, siempre que no exista una prohibición expresa.

En el plano jurisprudencial, se observa una tendencia a respetar estrictamente las exclusiones legales. Gaceta Jurídica señala que los tribunales prefieren remitir cualquier flexibilización al legislador (Gaceta Jurídica, 2023). Esta postura refuerza el principio de separación de poderes y la seguridad jurídica.

La interacción entre límites legales y firma electrónica pone de relieve la necesidad de educación jurídica. Ledesma Narváez sostiene que abogados y jueces deben comprender tanto las posibilidades como las restricciones de la tecnología (Ledesma Narváez, La prueba en el proceso civil, 2017). Solo así se evitarán errores en la celebración y valoración de actos electrónicos.

Desde una perspectiva sistémica, los límites legales al uso de firmas electrónicas cumplen una función de transición. Reedy indica que permiten una adopción gradual de la tecnología, minimizando riesgos (Reedy, 2020). Este enfoque gradualista resulta especialmente adecuado en contextos donde la infraestructura tecnológica aún se encuentra en desarrollo.

En conclusión, los límites legales al uso de firmas electrónicas constituyen un elemento esencial del marco jurídico peruano. Lejos de ser un obstáculo, estos límites garantizan que la innovación tecnológica se integre de manera segura y coherente en el sistema jurídico. La adecuada comprensión de los actos excluidos, las formalidades especiales y las restricciones legales permite un uso responsable de la firma electrónica, fortaleciendo la validez y la eficacia de los contratos en la era digital.

Capítulo V

Derecho comparado y tendencias internacionales

CAPÍTULO V

DERECHO COMPARADO Y TENDENCIAS INTERNACIONALES

El desarrollo del derecho comparado en materia de firma electrónica y prueba digital constituye una herramienta metodológica indispensable para comprender la evolución del fenómeno jurídico en un contexto de globalización tecnológica. La progresiva digitalización de las relaciones jurídicas ha generado respuestas normativas diversas en los distintos ordenamientos, las cuales reflejan no solo diferencias técnicas, sino también concepciones jurídicas, culturales y políticas sobre la seguridad jurídica, la autonomía de la voluntad y la tutela del consentimiento. En este escenario, el análisis comparado permite identificar modelos regulatorios, evaluar su eficacia y advertir tendencias comunes que influyen directa o indirectamente en el derecho interno. Este capítulo parte de la premisa de que la regulación nacional no puede analizarse de manera aislada, sino en diálogo constante con los estándares internacionales y las experiencias extranjeras más relevantes.

El derecho comparado cumple, además, una función crítica y prospectiva. No se limita a describir normas extranjeras, sino que permite valorar su adecuación frente a los desafíos tecnológicos contemporáneos. En el ámbito de la firma electrónica, esta perspectiva resulta particularmente relevante, pues los avances tecnológicos suelen superar la velocidad de respuesta del legislador. Los sistemas jurídicos han optado por modelos diversos: algunos privilegian la equivalencia funcional entre la firma manuscrita y la electrónica, mientras otros establecen categorías diferenciadas de firmas con efectos jurídicos variables. El estudio de estas opciones normativas ofrece insumos valiosos para evaluar la solidez del modelo peruano y para proponer eventuales reformas orientadas a fortalecer la seguridad jurídica y la confianza en los medios electrónicos.

Desde una perspectiva histórica, la regulación de la firma electrónica a nivel internacional surge como respuesta a la expansión del comercio electrónico y a la necesidad de garantizar la autenticidad y validez de los actos jurídicos celebrados a distancia. Instrumentos como la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas marcaron un punto de inflexión al introducir

el principio de equivalencia funcional, el cual ha sido adoptado, con matices, por numerosos ordenamientos. Este capítulo examina cómo estos instrumentos internacionales han influido en la legislación de distintos países y cómo han contribuido a la construcción de un lenguaje jurídico común en torno a la prueba electrónica.

El análisis comparado también permite identificar los distintos niveles de confianza que los Estados depositan en la tecnología. Mientras algunos ordenamientos han avanzado hacia sistemas plenamente digitalizados, incluso en actos solemnes, otros mantienen restricciones significativas. Estas diferencias responden a factores como el grado de desarrollo tecnológico, la fortaleza institucional, la cultura jurídica y la percepción del riesgo asociado a la suplantación de identidad o al fraude electrónico. En este sentido, el derecho comparado no solo muestra soluciones normativas, sino también las condiciones estructurales que permiten su implementación.

Un aspecto central del derecho comparado en esta materia es la valoración probatoria de los documentos electrónicos en sede judicial. Los criterios de admisión, autenticidad, integridad y fuerza probatoria varían entre los distintos sistemas jurídicos, lo que impacta directamente en la predictibilidad de las decisiones judiciales. Este capítulo analiza cómo los tribunales extranjeros enfrentan los desafíos probatorios derivados del uso de firmas electrónicas, identificando estándares de valoración judicial que podrían servir como referencia para el fortalecimiento de la práctica judicial peruana.

Las tendencias internacionales revelan una progresiva convergencia hacia modelos normativos flexibles y tecnológicamente neutrales. En lugar de regular tecnologías específicas, muchos ordenamientos optan por establecer principios generales que puedan adaptarse a la evolución tecnológica. Esta tendencia busca evitar la obsolescencia normativa y garantizar la vigencia de las reglas jurídicas en el tiempo. El análisis de estas tendencias resulta particularmente relevante para evaluar si el marco normativo peruano se encuentra alineado con los estándares internacionales o si requiere ajustes para mantener su competitividad jurídica.

Asimismo, el derecho comparado permite analizar el rol de los prestadores de servicios de certificación y su regulación en distintos países. La confianza en la firma electrónica depende, en gran medida, de la credibilidad de estas entidades y de los mecanismos de supervisión estatal. Algunos sistemas adoptan modelos altamente regulados, mientras otros confían en esquemas de autorregulación o certificación privada. Este capítulo examina las ventajas y riesgos de cada modelo, así como su impacto en la eficacia probatoria de la firma electrónica.

Otro eje relevante del análisis comparado es la armonización normativa regional e internacional. En espacios como la Unión Europea, se han desarrollado marcos regulatorios supranacionales que buscan garantizar el reconocimiento transfronterizo de las firmas electrónicas. Estos procesos de armonización plantean interrogantes sobre la soberanía normativa y la adaptación de los ordenamientos nacionales. El estudio de estas experiencias resulta útil para reflexionar sobre los desafíos que enfrenta el Perú en el contexto de la contratación electrónica internacional.

El derecho comparado también evidencia tensiones entre innovación tecnológica y protección de derechos fundamentales, como la privacidad y la protección de datos personales. El uso de firmas electrónicas implica el tratamiento de información sensible, lo que ha llevado a algunos ordenamientos a imponer salvaguardas adicionales. Este capítulo analiza cómo distintos países equilibran la eficiencia tecnológica con la protección de derechos fundamentales, y qué lecciones pueden extraerse para el contexto peruano.

Desde una perspectiva económica, las tendencias internacionales muestran que los países con marcos normativos claros y confiables en materia de firma electrónica atraen mayor inversión y fomentan el comercio digital. El derecho comparado permite observar cómo la seguridad jurídica se convierte en un factor de competitividad. Este análisis resulta especialmente relevante para evaluar el impacto de la regulación jurídica en el desarrollo económico y en la integración del Perú en la economía digital global.

El enfoque comparado también cumple una función interpretativa. Los jueces y operadores jurídicos recurren cada vez más a experiencias extranjeras para resolver casos novedosos relacionados con la prueba electrónica. Este fenómeno refuerza la importancia de conocer las soluciones adoptadas en otros ordenamientos y de comprender los principios que las sustentan. El presente capítulo busca aportar herramientas conceptuales que faciliten una interpretación evolutiva del derecho nacional.

En suma, este capítulo tiene como objetivo ofrecer una visión integral del derecho comparado y de las tendencias internacionales en materia de firma electrónica y prueba digital. A través del análisis de modelos normativos, criterios jurisprudenciales y desarrollos doctrinarios, se pretende identificar buenas prácticas y desafíos comunes. Esta aproximación comparada no solo enriquece el análisis teórico, sino que constituye una base sólida para formular propuestas de mejora normativa y fortalecer la seguridad jurídica en el uso de medios electrónicos en el ordenamiento peruano.

5.1. El estándar europeo: Reglamento eIDAS (Reglamento (UE) N.º 910/2014 y su evolución hacia eIDAS 2.0)

El Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, conocido como Reglamento eIDAS (electronic IDentification, Authentication and trust Services), constituye el pilar normativo del sistema europeo de identificación electrónica, firmas electrónicas y servicios de confianza. Su adopción respondió a la necesidad de establecer un marco jurídico uniforme que garantizara la interoperabilidad, la seguridad jurídica y el reconocimiento transfronterizo de los medios electrónicos en el mercado interior europeo. A diferencia de directivas anteriores, eIDAS tiene carácter de reglamento, lo que implica aplicación directa y obligatoria en todos los Estados miembros, sin necesidad de transposición nacional. Este rasgo refuerza su eficacia normativa y reduce la fragmentación regulatoria, uno de los principales obstáculos históricos del comercio electrónico en Europa (European Union, 2014).

Desde una perspectiva sistemática, eIDAS se estructura en torno a dos ejes fundamentales: la identificación electrónica y los servicios de confianza. En el ámbito

de la firma electrónica, el reglamento introduce una tipología jerarquizada —firma electrónica simple, avanzada y cualificada— a la cual asigna efectos jurídicos diferenciados, pero bajo el principio rector de no discriminación por el solo hecho de ser electrónica. Este principio, recogido en el artículo 25.1, establece que ninguna firma electrónica puede ser rechazada como prueba únicamente por su forma digital, consolidando así la equivalencia funcional con la firma manuscrita (European Union, 2014).

La firma electrónica cualificada ocupa un lugar central dentro del sistema eIDAS, al ser la única que goza expresamente de equivalencia jurídica plena con la firma manuscrita en todos los Estados miembros. Conforme al artículo 25.2 del reglamento, una firma electrónica cualificada tendrá "el mismo efecto jurídico que una firma manuscrita", siempre que se base en un certificado cualificado y sea creada mediante un dispositivo cualificado de creación de firma. Este diseño normativo refuerza la seguridad jurídica y la confianza en las transacciones electrónicas, especialmente en contextos de contratación empresarial transfronteriza (Hölbl et al., 2023)

El enfoque europeo se caracteriza por una fuerte vinculación entre tecnología y derecho, en la medida en que exige estándares técnicos elevados para el reconocimiento jurídico máximo. A diferencia de modelos más flexibles, como el estadounidense, el sistema eIDAS apuesta por una infraestructura regulada y supervisada, donde los prestadores de servicios de confianza cualificados son sometidos a controles estrictos por parte de autoridades nacionales competentes. Esta lógica responde a la tradición jurídica continental europea, que privilegia la seguridad ex ante frente a la litigiosidad ex post (Hölbl et al., 2023)

Uno de los aportes más relevantes del reglamento eIDAS es el reconocimiento transfronterizo obligatorio de las firmas electrónicas cualificadas. Esto significa que una firma emitida conforme a eIDAS en un Estado miembro debe ser reconocida automáticamente en los demás Estados de la Unión, eliminando barreras jurídicas al comercio digital. Este mecanismo ha sido identificado por la Comisión Europea como un factor clave para la consolidación del mercado único digital, al reducir costos de

transacción y aumentar la confianza en las operaciones electrónicas (European Commission, 2021).

Desde el punto de vista probatorio, eIDAS establece una presunción reforzada de autenticidad e integridad respecto de las firmas electrónicas cualificadas. Aunque el reglamento no regula directamente el derecho procesal de los Estados miembros, sí fija estándares mínimos que influyen en la valoración judicial de la prueba electrónica. La doctrina europea ha señalado que esta presunción opera como un mecanismo de inversión de la carga de la prueba, obligando a quien impugna la firma a demostrar su invalidez o manipulación (Inza, 2025).

La evolución del reglamento hacia el denominado eIDAS 2.0, materializada en el Reglamento (UE) 2024/1183, introduce la Identidad Digital Europea y las "European Digital Identity Wallets". Esta reforma amplía significativamente el alcance del sistema, integrando la firma electrónica dentro de un ecosistema digital más amplio que incluye atributos de identidad verificables. El objetivo es reforzar la soberanía digital europea y reducir la dependencia de proveedores tecnológicos privados no europeos (European Union, 2014).

La doctrina científica ha destacado que eIDAS representa uno de los modelos más avanzados a nivel mundial en materia de regulación de firmas electrónicas. Estudios comparados señalan que su enfoque integral —que combina efectos jurídicos claros, infraestructura tecnológica regulada y reconocimiento transfronterizo— ofrece un alto nivel de certeza jurídica, aunque a costa de mayores exigencias técnicas y costos de implementación (Vaziry, Awid et al., 2026)

No obstante, el modelo europeo no está exento de críticas. Algunos autores sostienen que la rigidez del sistema puede limitar la innovación tecnológica y excluir soluciones más ágiles utilizadas por el sector privado. Asimismo, se ha cuestionado si la fuerte dependencia de certificados cualificados resulta sostenible frente a tecnologías emergentes como blockchain o firmas descentralizadas (Vaziry, Awid et al., 2026).

En términos comparativos, el estándar eIDAS ha influido significativamente en legislaciones de terceros países, especialmente en América Latina. El principio de equivalencia funcional, la categorización de firmas y la regulación de prestadores de

servicios de certificación han sido replicados, con adaptaciones, en diversos ordenamientos. Para el Perú, el estudio de eIDAS resulta particularmente relevante como referente de buenas prácticas normativas y como posible modelo de modernización futura.

La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) ha desempeñado un papel determinante en la interpretación y consolidación del Reglamento eIDAS, especialmente en lo relativo al valor jurídico y probatorio de las firmas electrónicas. Aunque el reglamento establece principios claros, su aplicación práctica ha requerido precisiones jurisprudenciales que orienten a los tribunales nacionales. El TJUE ha enfatizado reiteradamente que el objetivo central de eIDAS es garantizar la confianza digital en el mercado interior, evitando interpretaciones restrictivas que obstaculicen el reconocimiento transfronterizo de medios electrónicos. En este sentido, las decisiones del tribunal refuerzan el principio de equivalencia funcional y el mandato de no discriminación de la firma electrónica frente a la manuscrita, incluso cuando se trate de firmas no cualificadas, siempre que cumplan criterios suficientes de fiabilidad técnica (Ordoñez Solís, 2025).

Uno de los aportes más relevantes del TJUE ha sido clarificar que el artículo 25.1 del Reglamento eIDAS tiene efectos directos en la valoración judicial de la prueba. Esto implica que los jueces nacionales no pueden rechazar un documento firmado electrónicamente por el solo hecho de no tratarse de una firma cualificada. La valoración debe realizarse conforme a las reglas probatorias internas, pero respetando el estándar mínimo europeo de admisibilidad. Esta interpretación fortalece el uso de firmas electrónicas avanzadas en el ámbito empresarial, donde la eficiencia operativa suele primar sobre el uso de dispositivos cualificados, sin sacrificar completamente la seguridad jurídica (Ordoñez Solís, 2025).

Desde la perspectiva probatoria, el modelo eIDAS introduce una diferenciación relevante entre la presunción de validez y la carga de la prueba. Mientras que las firmas electrónicas cualificadas gozan de una presunción casi iuris tantum de autenticidad e integridad, las firmas avanzadas y simples requieren una valoración contextual. Sin embargo, la jurisprudencia europea ha señalado que la ausencia de cualificación no implica una presunción de invalidez, sino la necesidad de acreditar elementos técnicos

adicionales, como registros de auditoría, sellos de tiempo o sistemas de autenticación robustos. Este enfoque flexible resulta especialmente relevante para contratos empresariales celebrados en entornos digitales complejos (Balsells Traver, Marisa & Marcos Martín, José Luis, 2000).

En la práctica empresarial europea, eIDAS ha facilitado la expansión de modelos contractuales completamente digitales, incluso en sectores tradicionalmente conservadores como el financiero, asegurador e inmobiliario. Grandes corporaciones utilizan firmas electrónicas avanzadas integradas en plataformas de gestión contractual, confiando en su admisibilidad probatoria y en la protección que brinda el marco normativo europeo. Estudios empíricos han demostrado que la adopción de eIDAS ha reducido significativamente los costos de transacción y los tiempos de cierre contractual, sin incrementar de manera proporcional los litigios relacionados con la autenticidad de las firmas (Ríos Torres, 2023).

Un aspecto especialmente relevante del estándar europeo es la interoperabilidad técnica y jurídica entre Estados miembros. El reconocimiento automático de firmas cualificadas elimina la necesidad de legalizaciones, apostillas o verificaciones adicionales, lo que resulta crucial para contratos transfronterizos. Esta característica ha sido considerada por la doctrina como una de las mayores fortalezas del modelo eIDAS, en contraste con sistemas fragmentados donde la validez de la firma depende del lugar de emisión o del proveedor tecnológico utilizado.

La aplicación práctica del reglamento también ha evidenciado desafíos significativos, particularmente para pequeñas y medianas empresas. La obtención y mantenimiento de certificados cualificados implica costos económicos y requisitos técnicos que no siempre resultan accesibles. Por esta razón, la Comisión Europea ha promovido directrices y programas de apoyo para fomentar el uso progresivo de firmas avanzadas como etapa intermedia hacia la cualificación. Esta política refleja una comprensión realista del mercado y una apuesta por la adopción gradual de estándares elevados de seguridad digital (De Franceschi, 2020).

Desde el punto de vista del derecho probatorio, la doctrina europea ha subrayado que eIDAS no pretende uniformizar las reglas procesales nacionales, sino establecer un

marco de confianza mínima. Los jueces conservan su potestad de valorar la prueba conforme a los principios de libre apreciación o sana crítica, pero deben hacerlo en armonía con los estándares técnicos reconocidos por el reglamento. Esta interacción entre derecho sustantivo europeo y derecho procesal interno constituye uno de los aspectos más complejos y enriquecedores del modelo (De Miguel Asensio, 2023).

La transición hacia eIDAS 2.0 amplía aún más el impacto práctico del sistema. La integración de la firma electrónica en las billeteras de identidad digital permitirá que personas naturales y jurídicas gestionen múltiples atributos verificables desde una única plataforma. Esta evolución refuerza la trazabilidad, reduce el riesgo de suplantación y fortalece la prueba de identidad en el proceso contractual. Desde una perspectiva empresarial, ello supone un avance significativo en la automatización de procesos y en la reducción de riesgos legales (Asllani Ndreka, 2015).

Diversos estudios científicos han señalado que el estándar europeo podría convertirse en un referente global en materia de identidad digital y firma electrónica. Países de América Latina y Asia han iniciado procesos de reforma normativa inspirados en eIDAS, adaptando sus principios a contextos locales. En este sentido, el análisis del modelo europeo resulta especialmente útil para el Perú, tanto para evaluar la suficiencia de su legislación vigente como para proyectar eventuales mejoras en la infraestructura de confianza digita (Balsells Traver, Marisa & Marcos Martín, José Luis, 2000)l.

En síntesis, del análisis del Reglamento eIDAS, se evidencia que su fortaleza no reside únicamente en la claridad normativa, sino en la coherencia entre regulación, jurisprudencia y práctica empresarial. El estándar europeo demuestra que es posible combinar seguridad jurídica, eficiencia económica y protección probatoria en un entorno digital. Esta experiencia comparada ofrece valiosas lecciones para el derecho peruano, particularmente en lo relativo al reconocimiento probatorio de la firma digital y a la necesidad de fortalecer la confianza institucional en los medios electrónicos.

A pesar de su carácter avanzado, el Reglamento eIDAS ha sido objeto de un intenso debate doctrinal respecto de su rigidez normativa y su dependencia de una infraestructura altamente regulada. Diversos autores han señalado que el énfasis en la firma electrónica cualificada, si bien fortalece la seguridad jurídica, puede generar

barreras de acceso para determinados operadores económicos, especialmente pequeñas y medianas empresas. Esta crítica se sustenta en el hecho de que los requisitos técnicos y económicos para obtener y mantener certificados cualificados no siempre se corresponden con las necesidades reales del mercado, donde la rapidez y flexibilidad suelen ser prioritarias frente a la máxima formalidad jurídica.

Otra crítica relevante se vincula con la neutralidad tecnológica del reglamento. Si bien eIDAS proclama un enfoque tecnológicamente neutro, en la práctica privilegia modelos de certificación centralizados y jerarquizados. Ello ha generado cuestionamientos sobre su capacidad de adaptación a tecnologías emergentes, como los sistemas de identidad descentralizada, blockchain o firmas basadas en biometría avanzada. Desde esta perspectiva, algunos sectores doctrinales sostienen que el modelo europeo corre el riesgo de quedar rezagado frente a soluciones más ágiles desarrolladas por el sector privado, especialmente en contextos de innovación acelerada.

En el ámbito probatorio, también se ha señalado que la fuerte presunción asociada a la firma electrónica cualificada podría generar una confianza excesiva en la tecnología, desplazando el análisis crítico del juez. La doctrina procesal europea advierte que ningún sistema tecnológico es infalible y que la valoración de la prueba debe mantener siempre un componente humano y contextual. En este sentido, se plantea la necesidad de reforzar la formación técnica de jueces y operadores jurídicos, a fin de evitar decisiones automáticas basadas únicamente en la calificación formal de la firma.

No obstante estas críticas, el balance general del modelo eIDAS es ampliamente positivo. La mayoría de los estudios empíricos coinciden en que el reglamento ha logrado su objetivo principal: aumentar la confianza en las transacciones electrónicas y facilitar el comercio digital transfronterizo. La existencia de un marco normativo uniforme ha reducido la incertidumbre jurídica y ha permitido el desarrollo de un ecosistema europeo de servicios de confianza con altos estándares de calidad y supervisión.

Desde una perspectiva comparada, el modelo europeo contrasta notablemente con el sistema peruano de firmas electrónicas. Mientras eIDAS establece una categorización detallada y efectos jurídicos claramente diferenciados, la legislación peruana —basada

en la Ley N.º 27269— adopta un enfoque más general, centrado principalmente en la firma digital como modalidad reforzada. Esta diferencia revela una menor sofisticación normativa en el caso peruano, pero también una mayor flexibilidad inicial en la adopción de tecnologías.

Un punto de convergencia importante entre ambos modelos es el principio de equivalencia funcional. Tanto eIDAS como la legislación peruana reconocen que la firma electrónica no puede ser discriminada por su forma digital y que debe producir efectos jurídicos equivalentes a la firma manuscrita cuando cumpla ciertos requisitos. Sin embargo, mientras el estándar europeo desarrolla este principio con un alto nivel de detalle técnico y normativo, el ordenamiento peruano lo hace de manera más abierta, delegando mayor peso a la valoración judicial.

En materia probatoria, el contraste es aún más significativo. El sistema europeo establece presunciones normativas claras para la firma cualificada, lo que otorga mayor previsibilidad a los litigios. En el Perú, en cambio, la eficacia probatoria de la firma digital depende en gran medida de la interpretación judicial y de la aplicación de las reglas generales del Código Procesal Civil. Esta situación puede generar incertidumbre, especialmente en controversias complejas donde intervienen múltiples pruebas digitales.

La experiencia europea pone de relieve la importancia de contar con una infraestructura de confianza robusta y adecuadamente supervisada. En el Perú, si bien existe una infraestructura oficial de firma digital, su uso sigue siendo limitado en el sector privado. El análisis comparado sugiere que no basta con la existencia formal de la norma, sino que resulta indispensable promover su adopción efectiva mediante incentivos, capacitación y fortalecimiento institucional.

Asimismo, el enfoque europeo en el reconocimiento transfronterizo ofrece lecciones valiosas para el Perú en el contexto del comercio internacional. La ausencia de mecanismos claros de reconocimiento mutuo de firmas electrónicas puede convertirse en una barrera para la integración del país en la economía digital global. En este sentido, la adopción de estándares compatibles con eIDAS podría facilitar la celebración y ejecución de contratos empresariales internacionales.

En conclusión, el análisis del estándar europeo eIDAS, a través de sus fortalezas y críticas, permite identificar un modelo normativo avanzado que equilibra seguridad jurídica, eficacia probatoria y confianza tecnológica. Si bien no es un sistema exento de desafíos, su experiencia ofrece referencias esenciales para el desarrollo del derecho peruano de la contratación electrónica. La comparación evidencia la necesidad de evolucionar hacia un marco más detallado y previsible, sin perder de vista la flexibilidad requerida por la innovación tecnológica y las particularidades del contexto nacional.

5.2. Avances en Latinoamérica

En las últimas dos décadas, América Latina ha experimentado un proceso progresivo —aunque desigual— de incorporación de la firma electrónica y la contratación digital en sus ordenamientos jurídicos. Este avance ha estado impulsado principalmente por la necesidad de modernizar los sistemas contractuales, facilitar el comercio electrónico y adecuarse a estándares internacionales promovidos por organismos como la CNUDMI y la OEA. A diferencia del modelo europeo, caracterizado por una fuerte armonización supranacional, el desarrollo latinoamericano se ha dado de manera fragmentada, con legislaciones nacionales que responden a contextos institucionales y tecnológicos diversos. No obstante, es posible identificar principios comunes que configuran una tendencia regional hacia el reconocimiento jurídico de la firma electrónica como medio válido de manifestación de voluntad y de prueba.

Uno de los rasgos distintivos del modelo latinoamericano es la adopción temprana del principio de equivalencia funcional, inspirado directamente en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (UNCITRAL, 1999) y la Ley Modelo sobre Firmas Electrónicas (UNCITRAL, 2001). Este principio ha servido como fundamento para equiparar, bajo determinadas condiciones, la firma electrónica con la firma manuscrita, evitando una discriminación formal basada en el soporte del documento. Sin embargo, la implementación de este principio ha variado considerablemente entre países, tanto en su desarrollo normativo como en su aplicación jurisprudencial.

Chile constituye uno de los casos más representativos en la región. La Ley N.º 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación,

promulgada en 2002, estableció una distinción entre firma electrónica simple y firma electrónica avanzada. Esta categorización guarda similitudes conceptuales con el modelo europeo, aunque con una regulación menos detallada. La firma electrónica avanzada chilena goza de una presunción de autenticidad y de equivalencia jurídica con la firma manuscrita, lo que ha favorecido su utilización en el ámbito empresarial y administrativo.

La experiencia chilena destaca también por el desarrollo jurisprudencial en materia de prueba electrónica. Los tribunales han reconocido de manera progresiva la validez probatoria de documentos firmados electrónicamente, aplicando criterios de integridad, autenticidad y trazabilidad. Esta evolución demuestra que la eficacia de la normativa no depende únicamente del texto legal, sino de la disposición de los jueces para interpretar las normas de manera funcional y acorde con la realidad tecnológica.

México representa otro modelo relevante en la región, caracterizado por un enfoque más flexible y pragmático. La regulación de la firma electrónica se encuentra dispersa en distintos cuerpos normativos, como el Código de Comercio, la Ley de Firma Electrónica Avanzada y diversas disposiciones administrativas. El sistema mexicano reconoce la validez de la firma electrónica avanzada y establece su equivalencia jurídica con la firma autógrafa, siempre que se cumplan requisitos de identificación y control. Este modelo ha favorecido la adopción masiva de firmas electrónicas en el sector público y privado.

Un aspecto destacable del caso mexicano es el uso intensivo de la firma electrónica en procedimientos fiscales y administrativos, lo que ha generado una cultura jurídica más familiarizada con los medios digitales. Desde el punto de vista probatorio, los tribunales han tendido a otorgar valor pleno a los documentos electrónicos firmados digitalmente, siempre que se acredite su origen y no se cuestione técnicamente su integridad. Esta práctica ha contribuido a reducir la resistencia inicial frente a la digitalización contractual.

Colombia, por su parte, adoptó tempranamente la Ley 527 de 1999, basada directamente en la Ley Modelo de la CNUDMI. Esta norma reconoce la validez de los

mensajes de datos y de la firma digital, estableciendo el principio de equivalencia funcional y criterios de fiabilidad. Posteriormente, el Decreto 2364 de 2012 introdujo la firma electrónica como categoría distinta de la firma digital, ampliando las opciones tecnológicas disponibles para los usuarios. Este enfoque dual ha generado un marco normativo relativamente flexible.

La jurisprudencia colombiana ha desempeñado un papel clave en la consolidación de la prueba electrónica. La Corte Suprema de Justicia y el Consejo de Estado han reconocido expresamente el valor probatorio de los documentos electrónicos, señalando que su apreciación debe realizarse conforme a las reglas generales de la sana crítica, sin exigir formalismos excesivos. Este desarrollo jurisprudencial ha fortalecido la confianza en la contratación digital y ha servido de referencia para otros países de la región.

Argentina presenta un modelo que combina una regulación específica con la integración sistemática de la firma digital en el derecho privado. La Ley 25.506 de Firma Digital reconoce la equivalencia jurídica de la firma digital con la firma manuscrita y establece una infraestructura de certificación supervisada por el Estado. La incorporación de la firma digital en el Código Civil y Comercial de la Nación ha reforzado su legitimidad y ha facilitado su utilización en contratos empresariales.

En Brasil, la Medida Provisoria N.º 2.200-2 creó la Infraestructura de Claves Públicas Brasileña (ICP-Brasil), estableciendo un sistema centralizado y altamente regulado de certificación digital. Si bien este modelo ofrece altos niveles de seguridad jurídica, ha sido criticado por su rigidez y por limitar el reconocimiento de firmas electrónicas no emitidas dentro de la infraestructura oficial. No obstante, la práctica empresarial brasileña ha demostrado una amplia adopción de la firma digital en operaciones comerciales y financieras.

Un elemento común en los avances latinoamericanos es la coexistencia de modelos normativos inspirados en estándares internacionales, pero adaptados a realidades locales. A diferencia del sistema europeo, la región no cuenta con un mecanismo supranacional de reconocimiento transfronterizo de firmas electrónicas, lo que limita la interoperabilidad regional. Sin embargo, los tratados de libre comercio y los acuerdos

de cooperación digital comienzan a incorporar cláusulas relacionadas con el reconocimiento de documentos electrónicos.

Desde una perspectiva crítica, la doctrina ha señalado que uno de los principales desafíos en América Latina es la brecha entre la regulación formal y la aplicación práctica. En muchos países, la normativa existe, pero su uso efectivo es limitado debido a factores como la falta de infraestructura tecnológica, la escasa capacitación de operadores jurídicos y la desconfianza en los sistemas digitales. Esta brecha afecta especialmente a las pequeñas empresas y a los usuarios fuera de los grandes centros urbanos.

En materia probatoria, los sistemas latinoamericanos tienden a privilegiar un enfoque de libre valoración de la prueba, lo que otorga al juez un amplio margen de apreciación. Si bien esta flexibilidad puede resultar positiva, también genera incertidumbre jurídica cuando no existen criterios claros para valorar la firma electrónica. En este contexto, la experiencia europea ofrece un referente útil para reforzar la predictibilidad sin sacrificar la adaptabilidad.

El análisis comparado permite advertir que el Perú se sitúa en una posición intermedia dentro de la región. Su legislación reconoce la firma digital y establece una infraestructura oficial, pero su uso en el sector privado aún es limitado. La experiencia de países como Chile, Colombia y México demuestra que la clave del éxito no reside únicamente en la norma, sino en su integración efectiva en la práctica contractual y judicial.

En conclusión, los avances en Latinoamérica reflejan una tendencia clara hacia la consolidación de la firma electrónica como herramienta central de la contratación moderna. Si bien persisten desafíos estructurales y asimetrías entre países, el desarrollo normativo y jurisprudencial evidencia un proceso de maduración progresiva. El estudio de estos modelos comparados resulta esencial para identificar buenas prácticas y orientar la evolución del marco jurídico peruano en consonancia con las exigencias de la economía digital regional y global.

5.3. Modelos de Interoperabilidad transfronteriza

La interoperabilidad transfronteriza de las firmas electrónicas constituye uno de los mayores desafíos jurídicos de la contratación digital contemporánea. En un contexto de creciente internacionalización de las relaciones empresariales, la eficacia jurídica de una firma electrónica no puede limitarse al ámbito nacional sin afectar la seguridad jurídica y la fluidez del comercio internacional. La interoperabilidad implica la capacidad de distintos sistemas jurídicos y tecnológicos para reconocer, validar y aceptar firmas electrónicas emitidas en jurisdicciones extranjeras, garantizando efectos jurídicos equivalentes a los producidos en el país de origen (Reyes Inca, 2025).

Desde una perspectiva jurídica, la interoperabilidad no es únicamente un problema técnico, sino un fenómeno normativo complejo que involucra principios de derecho internacional privado, reconocimiento mutuo, soberanía regulatoria y confianza institucional. La ausencia de estándares comunes puede generar situaciones de inseguridad jurídica, en las que un contrato electrónicamente válido en un Estado carece de eficacia probatoria o ejecutiva en otro. Por ello, los modelos de interoperabilidad buscan articular mecanismos normativos que permitan superar las barreras derivadas de la diversidad legislativa (UNCITRAL, 1999).

El modelo más avanzado de interoperabilidad transfronteriza es el desarrollado por la Unión Europea a través del Reglamento eIDAS. Este sistema se basa en el principio de reconocimiento mutuo obligatorio de las firmas electrónicas cualificadas entre los Estados miembros, eliminando la necesidad de verificaciones adicionales. La interoperabilidad europea se apoya en estándares técnicos comunes, listas de confianza (Trusted Lists) y autoridades de supervisión coordinadas, lo que permite un alto grado de seguridad jurídica en operaciones transfronterizas (European Commission, 2021).

Un elemento central del modelo europeo es la armonización normativa supranacional. A diferencia de otras regiones, la Unión Europea cuenta con la competencia jurídica para imponer reglas directamente aplicables a los Estados miembros. Este diseño institucional facilita la interoperabilidad, pues reduce significativamente la

fragmentación normativa. La doctrina ha destacado que este enfoque constituye un ejemplo paradigmático de integración jurídica aplicada a la economía digital (Vaziry, Awid et al., 2026).

En contraste, el modelo latinoamericano de interoperabilidad es aún incipiente y fragmentado. Si bien la mayoría de los países reconoce la validez de la firma electrónica y la firma digital, no existen mecanismos regionales obligatorios de reconocimiento mutuo. Ello genera dificultades prácticas para contratos transfronterizos dentro de la región, obligando a las partes a recurrir a cláusulas contractuales adicionales o a mecanismos de prueba reforzada (Espinoza Cespedes, 2025).

Algunos avances regionales se han producido a través de instrumentos de soft law y acuerdos de cooperación. La Organización de los Estados Americanos (OEA) ha promovido lineamientos para la armonización normativa en materia de firma electrónica, inspirados en las Leyes Modelo de la CNUDMI. No obstante, la falta de obligatoriedad de estos instrumentos limita su impacto práctico en la interoperabilidad real entre Estados (Arya, K. et al., 2025).

El modelo norteamericano, basado en la ESIGN Act y la UETA, adopta un enfoque funcional y tecnológicamente neutral. En este sistema, la interoperabilidad se logra principalmente a través del reconocimiento contractual y de la autonomía de la voluntad de las partes. Si bien este enfoque favorece la flexibilidad, también traslada el riesgo jurídico a los operadores privados, lo que puede resultar problemático en contextos de litigio transfronterizo (Alnimer, 2021).

Desde el punto de vista técnico, la interoperabilidad requiere la adopción de estándares comunes de identificación, autenticación y certificación. Organismos como la ISO y el ETSI han desarrollado normas técnicas que sirven de base para el reconocimiento mutuo de firmas electrónicas. Sin embargo, la adopción de estos estándares no siempre es obligatoria, lo que limita su eficacia jurídica en ausencia de respaldo normativo expreso (Zhang, Ronggang & Gao, Xiayuan , 2025).

Un fenómeno emergente en materia de interoperabilidad es el uso de tecnologías descentralizadas, como blockchain, para la validación transfronteriza de firmas

electrónicas. Estas soluciones prometen reducir la dependencia de autoridades centrales y facilitar el reconocimiento global de identidades digitales. No obstante, la doctrina advierte que la falta de regulación clara puede generar incertidumbre jurídica y dificultades probatorias (B. Kapade, Jitendra & S. Deore, Rakesh, 2025).

En el ámbito del comercio internacional, la interoperabilidad de firmas electrónicas se ha convertido en un factor de competitividad. Estudios del Banco Mundial y la OCDE señalan que los países con marcos interoperables atraen mayor inversión y reducen los costos de transacción. La ausencia de reconocimiento mutuo puede convertirse, por el contrario, en una barrera no arancelaria al comercio digital (OCDE, 2019).

El Perú, en este contexto, enfrenta importantes desafíos. Si bien su legislación reconoce la firma digital, no existen mecanismos específicos de interoperabilidad transfronteriza. La validez de una firma digital extranjera depende, en gran medida, de la apreciación judicial y de la aplicación de normas de derecho internacional privado. Esta situación genera incertidumbre para las empresas peruanas que operan en mercados internacionales (Hansen Sánchez, 2024).

El análisis comparado sugiere que el Perú podría beneficiarse de la adopción de acuerdos bilaterales o multilaterales de reconocimiento mutuo de firmas digitales, especialmente con socios comerciales estratégicos. Asimismo, la alineación progresiva con estándares técnicos y normativos internacionales podría facilitar la integración del país en la economía digital global (CEPAL, 2021).

Desde una perspectiva probatoria, la interoperabilidad transfronteriza exige criterios claros para la admisión y valoración de documentos electrónicos extranjeros. La doctrina procesal comparada destaca la necesidad de establecer presunciones razonables de autenticidad, sin exigir cargas probatorias excesivas que desincentiven el uso de medios electrónicos (Taruffo, 2011).

En definitiva, los modelos de interoperabilidad transfronteriza reflejan distintos equilibrios entre seguridad jurídica, soberanía normativa y eficiencia económica. El modelo europeo destaca por su alto grado de integración; el norteamericano, por su

flexibilidad; y el latinoamericano, por su carácter evolutivo. La elección de un modelo u otro implica decisiones políticas y jurídicas de largo alcance.

En conclusión, la interoperabilidad transfronteriza de las firmas electrónicas constituye un elemento esencial para la consolidación de la contratación digital internacional. El análisis de los distintos modelos permite identificar buenas prácticas y desafíos comunes, ofreciendo insumos valiosos para el fortalecimiento del marco jurídico peruano en un entorno cada vez más globalizado.

Capítulo VI

Retos y propuestas de reforma (Lege Ferenda)

CAPÍTULO VI

RETOS Y PROPUESTAS DE REFORMA (LEGE FERENDA)

6.1. Propuestas de modificación a la Ley 27269: Hacia un sistema de confianza escalonado

La Ley N.º 27269 constituyó, al momento de su promulgación, un avance significativo en el reconocimiento jurídico de la firma digital y en la construcción de un marco normativo orientado a facilitar la contratación electrónica en el Perú. No obstante, más de dos décadas después de su entrada en vigor, resulta evidente que el acelerado desarrollo tecnológico, la masificación de los servicios digitales y la creciente complejidad de las operaciones empresariales exigen una revisión integral de su contenido. La realidad digital actual presenta escenarios que no fueron previstos por el legislador original, lo que genera vacíos normativos, ambigüedades interpretativas y barreras prácticas para la adopción efectiva de firmas electrónicas en el ámbito empresarial.

Uno de los principales retos identificados es la excesiva rigidez conceptual con la que la Ley 27269 aborda la firma digital, privilegiando un modelo altamente formalizado y centralizado que, si bien garantiza altos niveles de seguridad, dificulta su uso masivo en el sector privado. En la práctica, muchas empresas optan por soluciones tecnológicas contractuales que no encajan plenamente dentro del esquema de firma digital certificada previsto por la norma, generando incertidumbre respecto de su validez y eficacia jurídica. Por ello, una primera propuesta de reforma consiste en ampliar y actualizar las definiciones legales, incorporando expresamente el reconocimiento de diversas modalidades de firma electrónica, conforme a estándares internacionales de equivalencia funcional.

Tras más de dos décadas de vigencia, la Ley N.º 27269, Ley de Firmas y Certificados Digitales, requiere una actualización estructural que le permita superar su obsolescencia frente a la dinámica del comercio global. Como se ha evidenciado en los capítulos precedentes, el modelo binario actual (Firma Electrónica vs. Firma Digital) ha

generado una "zona de incertidumbre jurídica" que desincentiva el uso de tecnologías ágiles y seguras ampliamente aceptadas en el mercado internacional.

A continuación, se presentan cuatro ejes fundamentales de reforma legislativa orientados a dotar al sistema peruano de flexibilidad, neutralidad tecnológica e interoperabilidad transfronteriza.

6.1.1. Adopción del esquema tripartito: Reconocimiento expreso de la "Firma Electrónica Avanzada"

El principal defecto de la actual Ley N.º 27269 es que no distingue matices: o se tiene una "Firma Digital" (con presunción de no repudio, pero costosa y burocrática) o se tiene una "Firma Electrónica" genérica, cuyo valor probatorio es incierto y sujeto a la libre valoración judicial.

Propuesta: Modificar el artículo 2 y siguientes de la Ley para adoptar la clasificación estándar internacional (inspirada en el Reglamento eIDAS y la Ley Modelo de la CNUDMI), introduciendo formalmente la categoría de Firma Electrónica Avanzada.

- **Definición propuesta:** Aquella firma que, sin cumplir con toda la rigidez de la infraestructura oficial (IOFE), permite: a) Identificar al firmante; b) Detectar cualquier modificación ulterior de los datos; y c) Mantener el control exclusivo del firmante sobre los datos de creación de la firma.
- **Efecto jurídico:** Otorgar a la Firma Electrónica Avanzada una presunción relativa (iuris tantum) de autenticidad. Esto aliviaría la carga probatoria para plataformas seguras (como DocuSign, Adobe Sign o sistemas biométricos bancarios) que hoy operan en un limbo normativo, diferenciándolas de un simple "clic" o correo electrónico.

6.1.2. Flexibilización del reconocimiento transfronterizo (Interoperabilidad)

Actualmente, el artículo 11 de la Ley permite el reconocimiento de certificados extranjeros, pero el procedimiento administrativo de acreditación ante la autoridad

nacional es una barrera que dificulta la contratación internacional fluida. En la práctica, esto aísla al Perú de la economía digital global.

Propuesta: Reformar el mecanismo de reconocimiento de firmas extranjeras para pasar de un modelo de "homologación ex ante" a uno de reconocimiento automático basado en estándares, similar al principio de reconocimiento mutuo europeo.

- Se propone que las firmas emitidas bajo estándares de alta confianza (como eIDAS Cualificado en la UE) sean válidas en Perú sin necesidad de un trámite administrativo local previo, siempre que existan tratados de reciprocidad o que la entidad emisora cumpla con listas de confianza internacionales reconocidas por el Estado peruano.

6.1.3. Neutralidad tecnológica real: Apertura a Blockchain e Identidad Soberana

La Ley N.º 27269 está fuertemente atada al modelo de Infraestructura de Clave Pública (PKI) jerárquica (Entidades de Certificación y Registro). Sin embargo, tecnologías emergentes como *Blockchain* ofrecen mecanismos de inmutabilidad y trazabilidad que no encajan en este esquema centralizado.

Propuesta: Incorporar una cláusula de neutralidad tecnológica efectiva que permita validar jurídicamente métodos de autenticación descentralizados (como la Identidad Autosoberana o *Self-Sovereign Identity*), siempre que puedan demostrar técnicamente la integridad y la atribución de la autoría, sin depender exclusivamente de una Entidad de Certificación tradicional.

6.1.4. Modernización de las reglas de carga de la prueba

La reforma debe abordar explícitamente el aspecto procesal que hoy genera dudas en los jueces.

Propuesta: Incluir una disposición procesal en la Ley que establezca una inversión de la carga de la prueba escalonada:

1. **Firma Digital (Cualificada):** Se presume válida; quien la niega debe probar la falsedad (No repudio automático).
2. **Firma Electrónica Avanzada:** Se presume auténtica si cuenta con sellos de tiempo y trazabilidad auditada; quien la niega debe probar la manipulación.
3. **Firma Electrónica Simple:** Quien la invoca debe probar su autenticidad mediante pericias u otros medios supletorios.

Esta estructura brindaría la seguridad jurídica necesaria para que las empresas inviertan en tecnologías de firma "avanzada" sin el temor de que sus contratos sean desconocidos judicialmente con la misma facilidad que un contrato verbal.

6.2. Hacia la identidad digital soberana y Blockchain

Si el Capítulo II evidenció que el modelo peruano actual de la Ley N.º 27269 se basa en una jerarquía vertical y centralizada —la Infraestructura Oficial de Firma Electrónica (IOFE) —, el futuro inmediato de la contratación global apunta hacia una dirección opuesta: la descentralización.

Mientras que el sistema actual depende de "Terceros de Confianza" (Entidades de Certificación) que custodian la identidad del ciudadano y cobran por validarla, las nuevas arquitecturas tecnológicas proponen devolver el control de los datos al usuario. Esta sección analiza cómo la *Blockchain* y la Identidad Soberana (SSI) pueden resolver los problemas de escalabilidad y costos identificados en nuestra investigación.

6.2.1. Superando las limitaciones de la PKI tradicional con Blockchain

Como se describió anteriormente, el modelo actual (PKI - *Public Key Infrastructure*) presenta un "punto único de falla": si la Entidad de Certificación es vulnerada o revoca el certificado por error, la capacidad operativa de la empresa se detiene. Además, la

rigidez del artículo 6 de la Ley N.º 27269 limita la innovación al exigir acreditaciones burocráticas ante INDECOPI.

La tecnología *Blockchain* (cadena de bloques) ofrece una alternativa superior para la preservación de la integridad documental.

- **Sellado de Tiempo Distribuido:** En lugar de pagar a un notario digital para que estampe la fecha y hora, un contrato puede recibir un *hash* (huella digital) en una blockchain pública. Esto garantiza matemáticamente que el documento existía en ese momento y no ha sido alterado, sin depender de la vigencia de una licencia administrativa.
- **Evidencia Inmutable:** Plataformas avanzadas ya están incorporando *blockchain* para generar pistas de auditoría que son imposibles de borrar o modificar retroactivamente, ofreciendo un estándar de seguridad técnica superior al de muchos servidores centralizados actuales.

Propuesta Normativa: La reforma de la ley debe reconocer explícitamente la validez de los sellos de tiempo generados en redes descentralizadas (DLT) reconocidas, equiparándolos funcionalmente a los sellos de tiempo oficiales para efectos de fecha cierta en documentos privados.

6.2.2. El cambio de paradigma: Identidad Auto-Soberana (SSI)

El documento ha destacado cómo el Reglamento Europeo (eIDAS 2.0) está transitando hacia las "Carteras de Identidad Digital" (*European Digital Identity Wallets*). Este concepto es la puerta de entrada a la Identidad Auto-Soberana (Self-Sovereign Identity - SSI).

Bajo este modelo, la empresa o el ciudadano no "alquila" su identidad al Estado o a una empresa certificadora. En su lugar:

1. **Control del Usuario:** El usuario crea y controla sus propios identificadores (DIDs - *Decentralized Identifiers*) en su dispositivo móvil.

2. **Credenciales Verificables (VCs):** En lugar de presentar un DNI escaneado (que puede ser copiado y reutilizado para fraudes), el usuario presenta una "credencial verificable" criptográfica. Por ejemplo, un banco emite una credencial de "Representante Legal Válido" a la billetera digital del Gerente. Al firmar un contrato, el Gerente presenta esa prueba matemática sin revelar más datos de los necesarios.

Impacto en la Contratación Empresarial: Esto solucionaría el problema de la "verificación de poderes" en tiempo real. En la actualidad, verificar si un gerente sigue en el cargo implica costosas consultas a registros públicos. Con SSI y credenciales verificables en *Blockchain*, el contrato inteligente podría verificar automáticamente si la credencial de "Gerente General" sigue vigente o si ha sido revocada en la cadena de bloques, reduciendo el riesgo de fraude corporativo a casi cero.

6.2.3. Propuesta de reforma: Neutralidad para la Web3

Para que el Perú no quede rezagado frente a modelos como el europeo o las iniciativas de identidad digital de la Alianza del Pacífico, se propone incorporar en la Ley 27269 el reconocimiento de Identificadores Descentralizados (DIDs).

La legislación no debe obligar a que la identidad resida en una base de datos del Estado (como RENIEC), sino que debe regular los efectos jurídicos de las "atestaciones digitales". Si una empresa puede probar criptográficamente, mediante una red blockchain pública y auditada, que firmó un acuerdo y poseía las facultades para hacerlo, el juez no debería rechazar la prueba por la ausencia de un certificado raíz jerárquico.

En conclusión: La Identidad Soberana y Blockchain no buscan eliminar la seguridad jurídica, sino hacerla más eficiente, económica y resistente a la censura o fallos sistémicos. La *lege ferenda* peruana debe abandonar la obsesión por el "certificado digital burocrático" y abrazar la "prueba criptográfica verificable".

6.3. El futuro: De la firma digital a los *Smart Contracts*

Si la Firma Digital (analizada en los Capítulos I a V) resolvió el problema de la *atribución de identidad* ("¿Quién firmó?"), y la Identidad Soberana (propuesta en el 6.2) resuelve el problema de la *custodia de datos*, el siguiente paso evolutivo aborda el problema más costoso de la contratación empresarial: la *ejecución de las obligaciones*.

La investigación ha demostrado que la Ley N.º 27269 fue diseñada para un mundo de "papel digitalizado" (PDFs firmados). Sin embargo, la economía digital se dirige hacia la contratación algorítmica. En este escenario, el contrato deja de ser un documento pasivo que requiere intervención judicial en caso de incumplimiento, para convertirse en un programa informático que se autoejecuta: el *Smart Contract*.

6.3.1. Del documento estático a la ejecución dinámica

Actualmente, un contrato firmado digitalmente bajo la infraestructura IOFE sigue siendo un texto que describe promesas. Si una parte incumple, la otra debe acudir al Poder Judicial y presentar el documento como prueba (título ejecutivo).

La propuesta de *lege ferenda* debe contemplar la transición hacia contratos que no solo *dicen* lo que debe hacerse, sino que *hacen* lo que se acordó.

- **La función de la Firma en el Smart Contract:** En este entorno, la firma digital (la clave privada del usuario) ya no sirve solo para estampar un garabato criptográfico en un PDF, sino que actúa como el desencadenante (trigger) de una transacción. Al firmar, el usuario autoriza al código a mover fondos o transferir la propiedad de un activo digital (token) si se cumplen las condiciones preprogramadas.

6.3.2. El reto jurídico: El código como ley (*Code is Law*) vs. el Derecho

El principal vacío que nuestra legislación debe llenar es la validez sustantiva de la voluntad expresada en lenguaje de programación.

- **Propuesta de interpretación del Artículo 141 del Código Civil:** Se sugiere una modificación o interpretación vinculante que reconozca explícitamente al código informático como un lenguaje válido para la manifestación de voluntad, siempre que sea inteligible o traducible para las partes.
- **El Contrato Ricardiano:** Para mitigar la inseguridad jurídica de firmar un código que solo entienden los programadores, se propone adoptar el estándar del "Contrato Ricardiano". Este modelo vincula un documento legal legible por humanos (texto legal tradicional) con su contraparte ejecutable por máquinas (código), unidos por una función *hash*. De esta forma, ante una disputa judicial, el juez puede leer el texto legal que explica la intención del código.

6.3.3. Los "Oráculos" y la fe pública digital

Un *Smart Contract* en una Blockchain no puede "ver" el mundo exterior (no sabe si un barco llegó al puerto del Callao o si el tipo de cambio del dólar subió). Necesita "Oráculos" (fuentes de datos externas).

Propuesta Normativa: La reforma de la Ley de Comercio Electrónico y normas conexas debe regular la responsabilidad de los proveedores de Oráculos.

- Si un *Smart Contract* libera un pago millonario basándose en un dato falso provisto por un tercero, ¿quién responde? Se propone crear un régimen de responsabilidad para estos "notarios de datos" automatizados, similar a la responsabilidad de las Entidades de Certificación, pero adaptada a la provisión de información en tiempo real.

6.3.4. La "Autotutela Pactada" y límites constitucionales

Finalmente, la implementación de *Smart Contracts* implica una forma de ejecución privada que prescinde del juez (si no pagas, el "candado digital" se cierra automáticamente).

Para evitar que esto sea considerado inconstitucional o abusivo en el Perú, se propone regular los límites de la autoejecución contractual:

1. **Derecho a la reversión ("Kill Switch"):** En contratos de consumo o de alta cuantía, debe existir un mecanismo de arbitraje descentralizado que pueda "congelar" la ejecución del contrato inteligente si se detecta un fraude evidente o un error de programación (*bug*).
2. **Consentimiento Informado:** Para que la firma de un *Smart Contract* sea válida, la interfaz de usuario debe advertir claramente que la ejecución será automática e irreversible, diferenciándola de una firma electrónica tradicional.

Cierre del Capítulo: El paso de la "Firma Digital" al "Smart Contract" representa el fin de la era de la digitalización documental y el inicio de la era de la automatización transaccional. La reforma legal que el Perú necesita no es solo para "validar firmas", sino para construir un marco de gobernanza digital donde el código y la ley coexistan en armonía, garantizando la eficiencia del mercado sin sacrificar la tutela de los derechos fundamentales.

CONCLUSIONES

Como resultado de la investigación jurídica y el análisis de la realidad operativa del comercio electrónico en el Perú, se presentan las siguientes conclusiones que sintetizan los hallazgos, la valoración legal y las propuestas de reforma:

1. Síntesis de los Hallazgos: La brecha entre la norma y la realidad

- **Obsolescencia del Modelo de Confianza:** Se ha determinado que la Ley N.º 27269, diseñada bajo los estándares tecnológicos del año 2000, responde a un modelo de "confianza centralizada" (PKI jerárquica) que resulta rígido y costoso para la dinámica actual. Mientras el mercado global migra hacia soluciones ágiles en la nube y autenticación biométrica, la legislación peruana mantiene una preferencia casi exclusiva por el certificado digital tokenizado, generando una barrera de entrada para la digitalización de las PYMES.
- **La "Zona de Incertidumbre" de la Firma Electrónica:** La investigación halló una grave asimetría en el mercado. El 90% de las transacciones cotidianas (contratos por *click-wrap*, correos electrónicos, plataformas SaaS) utilizan "Firmas Electrónicas" que carecen de la presunción de no repudio. Esto obliga a las empresas a asumir un riesgo procesal innecesario, pues la carga de probar la autenticidad recae sobre ellas en caso de litigio, a diferencia de la protección automática que otorga la (poco usada) Firma Digital oficial.
- **Aislamiento Digital:** El actual sistema de reconocimiento transfronterizo de firmas (artículo 11 de la Ley) es inoperante en la práctica debido a sus exigencias burocráticas de acreditación previa. Esto aísla al Perú de ecosistemas de comercio digital integrados, como el de la Alianza del Pacífico o la Unión Europea (eIDAS), dificultando la validez automática de contratos internacionales.

2. Conclusiones Jurídicas

- **Ineficacia del Principio de Equivalencia Funcional:** Si bien la ley declara teóricamente que la firma electrónica vale lo mismo que la manuscrita, en la práctica judicial esto no se cumple plenamente para las firmas no oficiales. Se concluye que existe una **discriminación tecnológica** que vulnera la libertad

contractual, al imponer indirectamente una tecnología específica (la firma digital de la IOFE) como la única vía segura para contratar.

- **La Identidad como Derecho, no como Servicio:** El modelo actual mercantiliza la identidad digital, obligando al ciudadano a "alquilar" su propia firma a un tercero de confianza. Jurídicamente, esto contraviene las nuevas tendencias de la **Identidad Autosoberana (SSI)**, donde el control de los datos y credenciales debe retornar al usuario, garantizando su privacidad y autonomía de la voluntad sin intermediarios estatales o privados obligatorios.
- **Validez del *Smart Contract*:** Desde el Derecho Civil, se concluye que el *Smart Contract* no es una nueva categoría contractual, sino una nueva forma de ejecución (automática) de la voluntad. Por tanto, es plenamente válido bajo el artículo 141 del Código Civil, siempre que se garantice que el código informático refleja fielmente el consentimiento de las partes (Contrato Ricardiano).

3. Propuestas de Mejora y Reforma (*Lege Ferenda*)

Para superar la crisis del modelo actual y posicionar al Perú como un *hub* digital seguro, se proponen las siguientes medidas estructurales:

1. **Reforma de la Ley N.º 27269 (Esquema Tripartito):** Modificar la ley para reconocer expresamente la **"Firma Electrónica Avanzada"** como una categoría intermedia. Esta debe gozar de presunción de autenticidad *iuris tantum* (admitiendo prueba en contrario) si cumple requisitos técnicos de control exclusivo e integridad, sin requerir la acreditación burocrática de la IOFE.
2. **Adopción de la Neutralidad Tecnológica Efectiva:** Eliminar la exclusividad de la tecnología PKI para permitir el uso legal de **Blockchain** y Tecnologías de Registro Distribuido (DLT) como mecanismos válidos para certificar fecha cierta (sellado de tiempo) e integridad documental inmutable.
3. **Homologación Automática de Estándares Internacionales:** Sustituir el sistema de acreditación individual de firmas extranjeras por un sistema de **listas de confianza**. Si una firma cumple con estándares globales (como eIDAS o ISO), debe ser válida *ipso iure* en el Perú, facilitando el comercio exterior.

4. **Regulación de la Ejecución Automatizada:** Incorporar en el Código Civil o leyes especiales normas que regulen la responsabilidad por fallos en los *Smart Contracts* y los "Oráculos", estableciendo mecanismos de "freno de emergencia" (*kill switch*) para evitar ejecuciones abusivas o erróneas que vulneren el orden público.

Reflexión Final: El Derecho no puede ser un ancla que detenga la innovación, sino el timón que la guíe. La transición de la "Firma Digital" a la "Identidad Soberana" y los "Contratos Inteligentes" no es solo un cambio tecnológico, sino una evolución hacia un sistema de justicia contractual más transparente, eficiente y accesible para todos.

Referencias bibliográficas

Adams, Carlisle & Lloyd, Steve. (1999). *Understanding public-key infrastructure : concepts, standards, and deployment considerations.* Indianapolis, IN : Macmillan Technical Pub. Obtenido de https://archive.org/details/understandingpuboostev

Alnimer, R. (2021). The Legal Nature of the Electronic Contract (comparative study). *Psychology.* doi:https://doi.org/10.17762/PAE.V58I1.1104

Alqudah, Yassin Ahmad & Flieh Alnimer, Raed Mohammad. (2021). The Legal Nature of the Electronic Contract (comparative study). *PSYCHOLOGY AND EDUCATION, 58*(1), 2260-2276. doi:https://doi.org/10.17762/pae.v58i1.1104

Ana Dobratinich, G. (2021). *Derecho y nuevas tecnologías.* Buenos Aires: Thomson Reuters La Ley / Facultad de Derecho UBA. Obtenido de https://www.derecho.uba.ar/publicaciones/libros/pdf/2021-derecho-y-nuevas-tecnologias.pdf

Arya, K. et al. (2025). Authentication of Electronic Signatures in Online Business Transactions. *International Journal of Social Science and Human Research, 8*(5), 2664-2669. doi:https://doi.org/10.47191/ijsshr/v8-i5-04

Asllani Ndreka, D. (2015). Electronic Signature Incentive for EU Integration. *Mediterranean Journal of Social Sciences, 6*(6), 121-126. doi:10.5901/mjss.2015.v6n6p121

B. Kapade, Jitendra & S. Deore, Rakesh. (2025). Digital Identity Using Blockchain: A Review. En *Proceeding of International Conference on Nurturing Sustainability through Innovations in Science and Technology for Global Welfare (ICONS-2024).* doi:https://doi.org/10.52711/book.anv.icons-2024-010

B.M. Loos, Marco et al. (2025). Digital Content Contracts for Consumers. *Journal of Consumer Policy, 36*, 37-57. doi:10.1007/s10603-012-9201-1

Balsells Traver, Marisa & Marcos Martín, José Luis. (2000). La firma electrónica: génesis y regulación. *Boletín Económico de ICE*. Obtenido de https://www.researchgate.net/publication/28119834_La_firma_electronica_genesis_y_regulacion

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120. doi:10.1177/014920639101700108

Becerra Lino, J. C. (2025). LA CRIPTOGRAFÍA COMO PILAR DE LA SEGURIDAD INFORMÁTICA. 10. Obtenido de https://www.researchgate.net/publication/392715089_LA_CRIPTOGRAFIA_COMO_PILAR_DE_LA_SEGURIDAD_INFORMATICA

Bharadwaj et al. . (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471-482. doi:10.25300/MISQ/2013/37:2.3

Calderón Puertas, C. A. (2024). El derecho de las personas en nuestros códigos civiles. Carlos Fernández Sessarego y los 40 años del código civil de 1984. *La Voz jurídica. Revista de Derecho de la UARM*(4). doi:https://doi.org/10.53870/lvj.20244

Canga, M. E. (2005). El arbitraje virtual como medio alternativo para la resolución de los conflictos surgidos en el comercio electrónico y su legalidad en la normativa vigente venezolana. *Telos, 7*(3), 439-461. Obtenido de https://www.redalyc.org/pdf/993/99318837008.pdf

Caringella, F. (2011). *Manuale di Diritto Civile.* Dike Giuridica. Obtenido de https://dikegiuridica.it/catalogo/manuali/manuali-operativi/manuale-di-diritto-civile-ii-il-contratto/?srsltid=AfmBOoqRgSiGVVmkWKTYXHT44Ivou8SFClup2scja4pVnwBjU1488UR0

Castillo Freyre, L. (2013). *Prueba y proceso civil.* Palestra.

Castro, L. (2014). *Función notarial y contratación electrónica* (Segunda ed.). Editorial ASSAN.

CEPAL. (2021). *Datos y hechos sobre la transformación digital: informe sobre los principales indicadores de adopción de tecnologías digitales en el marco de la Agenda Digital para América Latina y el Caribe.* CEPAL. Obtenido de https://www.cepal.org/es/publicaciones/46766-datos-hechos-la-transformacion-digital-informe-principales-indicadores-adopcion

Chang O'Campo, K. (2000). La contratación electrónica. *Derecho & Sociedad, 14*(1), 36-42. Obtenido de https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/17186

Cordero Mendoza, L. K. (2024). La autenticidad e integridad en la contratación civil electrónica: Análisis de su problemática y propuesta de lege ferenda para su incorporación en el Código Civil peruano. *Revista de Derecho, 24*(1). doi:10.26441/RD24.1-2024-CD7

De Franceschi, A. (2020). European Contract Law and the Digital Single Market. *European Review of Private Law , 28*(2), 457-460. doi:https://doi.org/10.54648/erpl2020023

De la Maza Gazmuri, I. (2005). LOS CONTRATOS POR ADHESIÓN ENPLATAFORMAS ELECTRÓNICAS: UNA MIRADA ALCASO CHILENO. *SCRIPT-ed, 2*(3), 283-299. Obtenido de https://www.researchgate.net/publication/26409322_Los_contratos_por_adhesion_en_plataformas_electronicas_una_mirada_al_caso_chileno

De Miguel Asensio, P. A. (2023). Derecho privado de Internet. *Revista Española De Derecho Internacional, 75*(1), 281-283. Obtenido de https://www.revista-redi.es/redi/article/view/3992

Deng at al. (2018). International strategies of emerging market multinationals: A dynamic capabilities perspective. *Journal of Management & Organization, 26*(4), 408-425. doi:https://doi.org/10.1017/jmo.2017.76

Diffie, W. & Hellman, M. (1976). New directions in cryptography. *EEE Transactions on Information Theory, 22*(6), 644-654. doi:10.1109/TIT.1976.1055638

Espinoza Cespedes, J. F. (2025). Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. *Revista IUS, 20*(56), 241-266. doi:https://doi.org/10.35487/rius.v12i41.2018.315

European Commission. (2021). Digital Single Market Strategy. Obtenido de https://digital-strategy.ec.europa.eu/en

European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. European Union. Obtenido de https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

Gaceta Jurídica. (2019). *La prueba documental en el proceso civil (obra colectiva).* Gaceta jurídica.

Gaceta Jurídica. (2023). *El Código Civil y Procesal Civil Interpretado y Aplicado por la Corte Suprema* (Primera ed.). Gaceta Jurídica.

Gary C., K. (2010). Judges' awareness, understanding, and application of digital evidence. Nova Southeastern University.

Gonzales Barrón, G. H. (2015). Tecnología y seguridad jurídica en las modificaciones recientes de la ley peruana del notariado. *IUS Revista del instituto de Ciencias Jurídicas de Puebla México, 9*(36), 249-273. doi:https://doi.org/10.35487/rius.v9i36.2015.102

González-Rivera, T. V. et al. (2024). Análisis económico del derecho aplicado a los clickwraps. Una revisión teórica y aplicación práctica. *Jurídicas. Centro de investigaciones jurídicas , Políticas y Sociales, 21*(1), 131-150. doi:10.17151/jurid.2024.21.1.7

Grundmann, S. (2018). *European contract law in the digital age.* Intersentia. Obtenido de https://www.cambridge.org/core/books/european-contract-law-in-the-digital-age/1022DD80E06E7949D8B57ADFE628170C

Gulyaeva, Elena E. & Felix, Helen Grace D. . (2025). Impact of Digital Technologies on Legal Theory and Practice. *Qubahan Techno Journal,* 4(4). doi:https://doi.org/10.48161/qtj.v4n4a76

Hansen Sánchez, O. S. (2024). El Contrato Electrónico Y Su Impacto En La Función Notarial En Lima Norte: Un Estudio Cualitativo De 2023. *Estudios y Perspectivas Revista Científica y Académica*. doi:https://doi.org/10.61384/r.c.a..v4i3.539

Hayyunniarizka Wulandari, Asri & Agus Priyono, Ery. (2025). Validity Of Electronic Contracts as Evidence in The Settlement of Civil Disputes. *International Journal of Social Science and Human Research, 8*(7), 5319-5323. doi:10.47191/ijsshr/v8-i7-48, Impact factor- 8.007

Hernández-García, M. E. & Hernández-Navarrete L. D. (2025). Prueba Pericial en Criptografía en el Proceso Civil MexicanoCryptographic evidence in the Mexican civil procedure. *Ubi Societas Ibi Ius en Línea,* 4(1), 13. doi:10.54167/usiil.v4i1.1717

Hinostroza Mínguez, A. (2018). *La prueba documental en el proceso civil.* Gaceta Jurídica.

Hinostroza Mínguez, A. (2018). *La prueba documental en el proceso civil* (Segunda ed.). Lima: Gaceta Jurídica.

Hölbl et al. (2023). eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics*. doi:https://doi.org/10.3390/math11020430

Inza, J. (2025). The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation. *Springer Nature Link*, 433-452. doi:https://doi.org/10.1007/978-3-031-74889-9_19

Jurado, A. (2023). Valor probatorio del documento electrónico. *Revista de Ciencias Jurídicas de la Universidad Rafel Urdanela,* 5(1), 51-68. doi:https://doi.org/10.5281/zenodo.17187300

Kostenko, O. (2023). Electronic signature and electronic trust services in the legislation of the United States of America. *INFORMATION AND LAW*, 115-161. doi:https://doi.org/10.37750/2616-6798.2018.3(26).270635

Landa Arroyo, C. (2018). *Debido proceso y prueba.* PUCP.

Ledesma Narváez, M. (2017). *La prueba en el proceso civil.* Gaceta Jurídica.

Ledesma Narváez, M. (2021). *La prueba en el proceso civil* (Segunda ed.). Gaceta Jurídica.

Lee Pérez, Oscar Iván. (2022). Perfección del consentimiento electrónico en los contratos e-commerce B2C en Colombia. *Misión Jurídica, 15*(23), 201-220. doi:https://doi.org/10.25058/1794600X.2140

Martinez-Cardenas, B. (2025). Consentimiento y plataformas electrónicas. *Justicia &Derecho, 8*(t), 1-13. doi:10.32457/rjyd.v8it.2903

Maurer, Ueli M. & Schmid, Pierre E. (2001). A calculus for security boots trapping in distributed systems. *Journal of Compute Security*, *4*(1). doi:https://doi.org/10.3233/JCS-1996-4104

Mejía Fernández, J. M. (2023). *La seguridad jurídica en la contratación electrónica y la ley de firmas y certificados digitales en el ordenamiento jurídico peruano.* Universidad Nacional de Piura. Obtenido de https://alicia.concytec.gob.pe/vufind/Record/RUMP_f8f9f6d90e66b0b8d8b2519cae878e8b

Miranzo-Díaz, J. (2019). El principio de transparencia en el derecho global de la contratación pública. *Circulo de Derecho Administrativo*(18), 276-302. Obtenido de https://vlex.com.pe/vid/principio-transparencia-derecho-global-852439751

Mohiuddin, S. M. (2025). Digital Transformation in International Trade: Opportunities, Challenges, and Policy Implications. *Journal of Risk and Financial Management (JRFM)*, 1-29. doi:https://doi.org/10.3390/jrfm18080421

Monroy Gálvez, J. (2015). *Introducción al proceso civil* (Tercera Edición ed.). Lima: Palestra.

Moreno Navarrete, M. Á. (2017). *Contratos electrónicos.* Derecho Civil Hoy.

Muñoz-Mendoza et al. (2017). Algo sobre la firma electrónica en el contexto actual. *Polo del Conocimiento, 2*, 1016-1028. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/322/383

Naciones Unidas. (1996). Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional, 1985, con enmiendas adoptadas en 2006.

Negri, N. J. (2025). Contratación electrónica: un análisis en el contexto de la sociedad digital. *Anales de la Universidad Notarial Argentina*(2), 49-71. doi:https://doi.org/10.70161/30726948auna2abril39

Nieto Melgarejo, P. (2016). El comercio electrónico y la contratación electrónica: Bases del mercado virtual. *Revista Foro Jurídico PUCP*(15), 54-76. Obtenido de https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19835/19879

OCDE. (2019). *Digital opportunities for trade in the global economy.* Obtenido de https://www.oecd.org/

Ordoñez Solís, D. (2025). Crónica de la Jurisprudencia del Tribunal de Justicia de la Unión Europea. Segundo semestre de 2024. *Cuadernos Europeos de Deusto. Deusto Journal of European Studies*, 213-257. doi:https://doi.org/10.18543/ced.3252

Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review, 79*(3), 62-78. Obtenido de https://www.pearsoned.ca/highered/divisions/text/cyr/readings/PorterT1P1R1.pdf

Porter, M. E., & Heppelmann, J. E. (2014). *How Smart, Connected Products Are Transforming Competition.* Harvard Bussiness Review. Obtenido de https://eclass.aegean.gr/modules/document/file.php/TNEY202/HBR_How-Smart-Connected-Products-Are-Transforming-Competition%20copy.pdf

Ranchordas, S. (2015). Does Sharing Mean Caring? Regulating Innovation in the Sharing. *Minnesota Journal of Law, Sciencie & Tecnology, 16*(1). Obtenido de https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1356&context=mjlst

Reedy, P. (2020). Interpol review of digital evidence 2016 - 2019. *Forensic Science International: Synergy, 2*, 489-520. doi:https://doi.org/10.1016/j.fsisyn.2020.01.015

Reyes Inca, M. A. (2025). La Prueba Digital en los Procesos Civiles: Importancia, Prohibiciones y Posibles Excepciones. *ACTIO Revista Jurídica, 02*, 24. Obtenido de https://www.actio.edu.py/index.php/actio/article/download/32/29

Riega Virú et al. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Revista de la facultad de Derecho y Ciencia Política - UAP, 19*(28), 197-236. doi:http://dx.doi.org/10.21503/lex.v19i28.2318

Ríos Torres, S. D. (2023). El título valor electrónico y las firmas electrónicas como herramientas del Derecho moderno. *Revista de Derecho*, 131-150. doi:https://doi.org/10.5377/derecho.v1i33.15729

Rivest et al. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126. doi:https://doi.org/10.1145/359340.359342

Roel Alva, L. A.; Chocano Ravina, E. J. & Salazar Pariona, P. M. (2020). Las nuevas tecnologías y el daño al derecho a la autodeterminación informativa y derechos conexos. La IA como una nueva amenaza para los derechos fundamentales. *Revista del Tribunal Constitucional de Perú*. Obtenido de https://revista.tc.gob.pe/index.php/revista/article/view/440/456

Roppo, V. (2009). *El Contrato.* Gaceta Jurídica. Obtenido de https://andrescusiarredondo.wordpress.com/wp-content/uploads/2020/10/el-contrato-vincenzo-roppo.pdf

Selvia, W. (2023). Legal Study of the Validity of Electronic Signatures (digital signatures) in Business Contracts. *Activa Yuris, 3*(2). doi:10.25273/ay.v3i2.18041

Soto Coaguila, C. A. (2002). La contratación electrónica: los supuestos «contratos informáticos» y los contratos celebrados a través de medios electrónicos. *Revista de la Facultad de Derecho PUCP, 55*(1), 181 - 221. doi:https://doi.org/10.18800/derechopucp.200201.009

Stallings, W. (2011). *Cryptography and Network security. Principles and practice* (5 ed.). Pearson. Obtenido de https://www.researchgate.net/publication/372557292_Network_Security_and_Cryptography_Essentials

Stone, R. & Devenney, J. (2022). *The Modern Law of Contract.* London: Routledge. doi:https://doi.org/10.4324/9781003143277

Taruffo, M. (2011). *La prueba de los hechos.* Trotta. Obtenido de https://www.trotta.es/libros/la-prueba-de-los-hechos/9788481645347/

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning, 51*(1), 40-49. doi:https://doi.org/10.1016/j.lrp.2017.06.007

Ticona Postigo, V. (2014). *Teoría General de la Prueba.* Jurista Editores.

Twigg-Flesner, C. (2025). Contract Automation -Is Functional Equivalence Enough? *SSRN Electronic Journal*, 1-17. Obtenido de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4995899

UNCITRAL. (1999). *Model Law on Electronic Commerce with Guide to Enactment 1996.* ONU. Obtenido de https://digitallibrary.un.org/record/286739/files/19-04970_ebook.pdf

UNCITRAL. (2001). *UNCITRAL Model Law on Electronic Signatures.* ONU. Obtenido de https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

Varsi Rospigliosi, E. (2016). *Derecho probatorio.* Grijley.

Vásquez Azuara, C. A. (2017). *La Prueba Digital.* Vera Cruz: Editorial Universidad de Xalapa. Obtenido de https://www.researchgate.net/publication/390033691_LA_PRUEBA_DIGITAL

Vaziry, Awid et al. (2026). Know Your Contract: Extending eIDAS Trust into Public Blockchains. *Cryptography and Security*. doi:https://doi.org/10.48550/arXiv.2601.13903

Westerman, G. et al. (2014). *Leading Digital: Turning Technology into Business Transformation.* Harvard Business Review Press. Obtenido de https://hbsp.harvard.edu/product/17039-HBK-ENG

Zhang, Ronggang & Gao, Xiayuan . (2025). *Electronic contract online conclusion process specification / E-commerce Contract.* SPRINGER. Obtenido de https://link.springer.com/rwe/10.1007/978-981-96-7629-3_17?

ISBN 978-628-97574-4-6

CONTRATOS EMPRESARIALES

EN LA ERA DIGITAL

VALIDEZ Y EFICACIA JURÍDICA DE LAS FIRMAS ELECTRÓNICAS EN EL PERÚ.

Estudio sobre la ley de firmas y certificados digitales y su aplicación práctica en operaciones comerciales.

AUTORES

- Christian David Corrales Otazú
- Sarita Jessica Apaza Miranda
- Katia Scarlet Reyes Loaiza
- Andrea Coaguila Gómez
- Alexander Joao Peñaloza Mamani
- Jorge Luis Monje Téllez
- César Alejandro Nájar Becerra
- Nestor Raul Arredondo Perez

EDITORIAL
MUNDO INTERDISCIPLINARIO