Regulatory dispersion in information security for EMI in Mexico

DISPERSIÓN NORMATIVA EN LA SEGURIDAD DE LA INFORMACIÓN PARA LAS IFPE EN MÉXICO*

Por: Susana Cordova Ramos

Cordova Ramos, S. (2026). Dispersión normativa en la seguridad de la información para las IFPE en México. *Entorno UDLAP*, 25.
Recibido: 6 de octubre de 2025. **Aceptado:** 4 de febrero de 2026.

RESUMEN

En México la regulación de la seguridad de la información para las Instituciones de Fondo de Pago Electrónico (IFPE) se encuentra fragmentada en diversos instrumentos legales que conforman un marco legal integral, lo que genera retos respecto a la certeza jurídica y dificulta la implementación eficaz de mecanismos de cumplimiento, así como la prevención de riesgos operativos. Este artículo analiza la problemática derivada de dicha dispersión, identifica los instrumentos legales vigentes y propone un compendio consolidado como herramienta base estratégica para los operadores en el sector.

PALABRAS CLAVE

EMI • Seguridad de la información • Ley *fintech* • Marco legal

ABSTRACT

In Mexico, the regulation of information security for Electronic Money Institution (EMI) is fragmented across different legislations that make up a comprehensive legal framework, which generates challenges regarding legal certainty, and hinders the effective implementation of compliance mechanisms, as well as for the prevention of operational risks. This article analyzes the problems derived from such dispersion, identifies the legal instruments in force and proposes a consolidated compendium as a strategic tool for operators in the sector.

KEYWORDS

EMI • Information security • Fintech law • Legal framework

INTRODUCCIÓN

Las Instituciones de Fondos de Pago Electrónico (IFPE) han surgido como actores clave del ecosistema financiero digital en México. Al gestionar información y flujos de dinero en sus plataformas tecnológicas, enfrentan retos cada vez más complejos en materia de seguridad digital.

En México la regulación de seguridad de la información para las IFPE no se encuentra sus-

* Este artículo forma parte de un prontuario más detallado (próximo a publicarse) que profundiza en las obligaciones específicas y la continuidad operativa. Este servirá como base para facilitar auditoría y diseñar programas internos de cumplimiento.

tentada por un marco legal coherente y unificado, sino por una serie de disposiciones fragmentadas que abarcan desde protección de datos personales hasta regulación financiera y prevención de lavado de dinero. Esta dispersión provoca incertidumbre jurídica, dificulta su cumplimiento e incrementa costos y afectaciones en la supervisión efectiva por parte de las autoridades financieras.

Este artículo analiza dicha fragmentación, revisa distintas leyes y disposiciones, compara prácticas internacionales relevantes y presenta un compendio normativo organizado cronológicamente.

Evolución de las *fintech*

Durante la crisis de la COVID-19, las *fintech* tuvieron un alza a nivel mundial, que las convirtió en tendencia para descarga y uso de sus aplicaciones financieras (Martínez y López, 2022). La aceptación que han tenido en los últimos años ha provocado que las Instituciones de Fondos de Pago Electrónico (IFPE) se encuentren en constante crecimiento. De acuerdo con Finnovista (2025), este segmento ascendió en México en un 16 % en el último año.

El desarrollo de las IFPE ha sido parte fundamental en la inclusión financiera. Esto se debe a que sus productos y servicios son de fácil uso y acceso, lo que marca una diferencia con la banca tradicional. Sin embargo, su base tecnológica conlleva ciertos aspectos que pueden ser considerados como desventajas, ya que, además de los riesgos financieros tradicionales, las IFPE se enfrentan a desafíos propios de su entorno, como los riesgos tecnológicos, que a su vez mantienen subcategorías relacionadas con la seguridad de la información.

La seguridad de la información es parte fundamental de los servicios ofertados por las IFPE debido a la naturaleza de sus funciones y a la confianza que los usuarios depositan en las plataformas. Ello implica que estén conformadas por diversos elementos, dentro de los que se encuentran personas y procesos, así como la propia operación.

Comúnmente, la seguridad de la información es entendida como la preservación de su confidencialidad, integridad y disponibilidad, mediante la aplicación de procesos de gestión de riesgos (ISO/IEC, 2020). De acuerdo con Herrmann y Pridöhl (2020), el concepto de seguridad de la información hace referencia a la protección de datos (potencialmente aquellos procesados por los ordenadores). Sin embargo, desde una perspectiva original, la seguridad de la información tiene sus bases en los activos conformados por datos que pueden o no estar almacenados o ser transmitidos a través del uso de las tecnologías de la información y la comunicación (TIC).

Desde esta perspectiva, para las *fintech* es trascendental mantener una adecuada gestión de la seguridad que fomente la estabilidad financiera y una buena gestión de riesgos que proteja la confianza de sus usuarios, ya que se encuentran operando en un ambiente totalmente digital, por lo que están sujetas a ciberataques, fraudes electrónicos y fallas operativas que pueden culminar en nuevas formas de riesgo sistémico.

El riesgo sistémico ha sido abordado ya por diversos reguladores internacionales. Ejemplo de ello es la Unión Europea, que se ha ocupado de aumentar la resiliencia operativa digital en sus sistemas financieros mediante su Reglamento de Resiliencia Operativa Digital (DORA).

El reglamento, que es de observancia general a partir de enero de 2025, aborda aspectos clave relacionados con la ciberseguridad, la seguridad de la información y el riesgo tecnológico. Además, su objetivo principal es fomentar que todas las entidades financieras de la Unión Europea tengan una alta resiliencia operativa digital. Para lograrlo, establece requisitos uniformes de seguridad de sus sistemas y redes de información, los cuales son esenciales para sus operaciones (Gómez y Montilla, 2025).

Esta norma busca una armonización global de las obligaciones relacionadas con la gestión del riesgo de las TIC, lo que reduce la dispersión normativa de las diferentes legislaciones aplicables en la Unión Europea. Sin embargo, no es la única experiencia internacional que nos muestra cómo reducir dicha segmentación de marcos regulatorios basados en los riesgos tecnológicos. Dentro del mismo segmento, también se cuenta con el Reglamento General de Protección de Datos (GDPR) y la Directiva PSD2, que establecen obligaciones de seguridad para los proveedores de pagos electrónicos.

En el caso de Asia, Singapur destaca por la actualización en 2021 del Technology Risk Management Guidelines (MAS, 2021). Esta disposición establece principios y mejores prácticas que fortalecen la autogobernanza, y permite fincar marcos internos sólidos para la gestión de riesgos, incluyendo la responsabilidad del uso de tecnologías emergentes.

LA FALTA DE UN MARCO LEGAL COHERENTE PROVOCA INCERTIDUMBRE JURÍDICA, DIFICULTA SU CUMPLIMIENTO E INCREMENTA COSTOS Y AFECTACIONES EN LA SUPERVISIÓN EFECTIVA POR PARTE DE LAS AUTORIDADES FINANCIERAS.

En contraste, México carece de una norma específica de ciberseguridad que atienda estos riesgos relacionados con la tecnología y fomente la resiliencia operacional. Esta situación obliga a las IFPE a observar diversas legislaciones sin una dirección clara.

Contexto jurídico de la seguridad de la información en las IFPE

En el caso de México, el marco legal en materia de seguridad de la información aplicable a las IFPE se compone de múltiples leyes de carácter general, sectorial y técnico, que no se encuentran armonizadas entre sí.

Esta superposición normativa genera vacíos, duplicidades y retos de interpretación que dificultan la implementación de programas de seguridad de la información efectivos, robustos, consistentes y auditables. A continuación se enumeran los principales desafíos.

Pluralidad de autoridades reguladoras. Cada autoridad regulatoria involucrada, como la Comisión Nacional Bancaria y de Valores (CNBV), el Banco de México (Banxico) y la Secretaría de Hacienda y Crédito Público (SHCP), mantiene atribuciones específicas respecto a las obligaciones en materia de seguridad de la información. Esto puede provocar falta de claridad o coordinación en la aplicación y cumplimiento de las obligaciones.

Múltiples legislaciones generales, complementarias y secundarias. Aunque la ley *fintech* fue emitida para regular a las Instituciones de Tecnología Financiera, existen diversas disposiciones secundarias y complementarias que regulan aspectos específicos en materia de seguridad de la información. Esto dificulta el cumplimiento y aumenta la posibilidad de sanciones.

Transversalidad de la materia. Los riesgos asociados a la seguridad de la información abarcan no solo la operación financiera de las IFPE, sino también la protección de datos personales, prevención de lavado de dinero, protección al consumidor, etc. Cada uno de estos ámbitos se encuentra regulado por diversas legislaciones que a su vez establecen obligaciones específicas, lo que genera su fragmentación.

Desafíos en la implementación. Si bien la ley *fintech* busca generar certidumbre jurídica para este sector, de acuerdo con BFA Global (2021), las obligaciones referentes a la seguridad de la información y ciberseguridad se consideran elevadas para las nuevas empresas. Por ello, algunas *fintech* se han asociado con empresas ya autorizadas.

Este último punto resulta relevante, porque el aumento de gastos operativos restringe la innovación financiera, ya que de acuerdo con la European Banking Authority (2019), las instituciones con reciente concesión consideran que el cumplimiento de la normativa vigente y futura constituye desafíos significativos, lo que ocasiona que decidan no adoptar innovaciones financieras basadas en tecnologías.

La interpretación de distintas normas, aunque aborden aspectos diversos, a menudo genera duplicidades y falta de claridad en su cumplimiento, lo que se traduce en costos legales y operativos, así como en un estancamiento en la adopción de nuevas tecnologías al no tener un rumbo preciso.

Por ejemplo, en el caso de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2010), se exigen estándares robustos respecto al tratamiento de datos personales. Sin embargo, la CNBV, mediante sus diversas disposiciones y circulares, establece parámetros más técnicos de infraestruc-

EN MÉXICO, EL MARCO LEGAL EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN APLICABLE A LAS IFPE SE COMPONE DE MÚLTIPLES LEYES DE CARÁCTER GENERAL, SECTORIAL Y TÉCNICO, QUE NO SE ENCUENTRAN ARMONIZADAS ENTRE SÍ.

tura sin integrar los criterios emitidos por la autoridad en materia de datos personales. La falta de armonización obliga a las instituciones a duplicar esfuerzos relacionados con el cumplimiento o, en el peor de los escenarios, a enfrentar sanciones ante la inobservancia de sus obligaciones.

Como consecuencia de esta dispersión en las normas aplicables a las IFPE, se analizó el marco legal para ubicar los principales instrumentos legales, disposiciones subsecuentes, circulares y reglamentos, que contemplan aspectos relacionados con la seguridad de la información.

Este compendio normativo que se presenta, se elaboró mediante una revisión documental de la legislación vigente, disposiciones de la CNBV, las circulares del Banco de México, así como lineamientos emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). El compendio, que se encuentra organizado de forma cronológica, nos permite evidenciar la evolución de las obligaciones aplicables.

En primer lugar, la Ley Federal de Derecho de Autor (LFDA) y la Ley Federal de Protección a la Propiedad Industrial (LFPI) constituyen el fundamento para la protección de los activos intangibles de las IFPE. Estos activos incluyen *software*, bases de datos y algoritmos, elementos clave para la seguridad de las operaciones de sus plataformas.

Aunque ambas leyes no ordenan directamente la implementación de medidas de seguridad de la información, sí obligan a las IFPE a respetar derechos de autor y patentes. Esto asegura la confidencialidad de la tecnología propia y de terceros, y evita la vulneración de licencias o marcas en entornos digitales.

Por su parte, la Ley de Protección y Defensa al Usuario de Servicios Financieros (LPDUSF, 1999) establece obligaciones específicas para garantizar los derechos de los usuarios de las IFPE frente a estas instituciones. Estas incluyen la confidencialidad y seguridad de la información proporcionada.

A esta base normativa le siguen la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2010) y su reglamento, que son un precedente al regular el tratamiento de datos personales dentro del sector privado. Ambas establecen obligaciones sobre medidas de seguridad administrativas, físicas y técnicas para salvaguardar la información personal de los usuarios. A su vez, el reglamento de la LFPDPPP complementa estas obligaciones, a través de la ampliación de los procedimientos, que incluyen el cumplimiento relacionado con avisos de privacidad y notificaciones de brechas de seguridad.

LA LEY DE PROTECCIÓN Y DEFENSA AL USUARIO DE SERVICIOS FINANCIEROS (LPDUSF, 1999) ESTABLECE OBLIGACIONES ESPECÍFICAS PARA GARANTIZAR LOS DERECHOS DE LOS USUARIOS DE LAS IFPE FRENTE A ESTAS INSTITUCIONES.

MÉXICO DIO UN PASO CLAVE AL PROMULGAR LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA (LEY FINTECH, 2018), LA CUAL ESTABLECE BASES NORMATIVAS EN EL SECTOR.

Como complemento a la LFPDPPP y su reglamento, el INAI emitió las «Recomendaciones para el Tratamiento de Datos Personales y el Cumplimiento del Deber de Seguridad para las Instituciones de Tecnología Financiera», cuyo fin es orientar a las IFPE en la adopción de buenas prácticas en materia de protección de datos y establecer acciones concretas en políticas de seguridad, auditorías y protocolos de notificación de incidentes. Si bien estas recomendaciones no son de carácter obligatorio, brindan criterios que orientan y promueven la autorregulación.

También resulta relevante la observancia de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI, 2012), que refuerza el marco de prevención de lavado de dinero. Lo hace mediante la exigencia de controles para la identificación de operaciones financieras, los cuales incluyen almacenamiento seguro y auditable. Este marco demanda la implementación de procedimientos y tecnologías que aseguren la seguridad de la información en el monitoreo de operaciones consideradas como vulnerables.

Por su parte, el Banco de México ha publicado diversas circulares que establecen reglas de observancia obligatoria para las IFPE, como la Circular 14/2017, que introdujo lineamientos técnicos para la interconexión segura de sistemas de pago. Esta disposición contiene obligaciones enfocadas en garantizar estándares mínimos de seguridad para proteger la integridad de las operaciones electrónicas, la confidencialidad de los mensajes y la disponibilidad de las transacciones.

Con base en las normativas ya señaladas y la constante evolución tecnológica en el sector *fintech,* México dio un paso clave al promulgar la Ley para Regular las Instituciones de Tecnología Financiera (ley *fintech*, 2018), la cual establece bases normativas en

Tabla 1. Compendio normativo de la seguridad de la información para las IFPE en México.

INSTRUMENTO NORMATIVO
Ley Federal del Derecho de Autor (LFDA)
Ley Federal de Propiedad Industrial (LFPI)
Ley de Protección y Defensa al Usuario de Servicios Financieros (LPDUSF)
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI)
Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)
Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)
Recomendaciones para el tratamiento de datos personales y cumplimiento del deber de seguridad para las Instituciones de Tecnología Financiera
Circular 14/2017
Disposiciones de carácter general relativas a las interfases de programación de aplicaciones informáticas estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera
Ley para Regular las Instituciones de Tecnología Financiera (ley *fintech*)
Disposiciones aplicables a las Instituciones de Fondo de Pago Electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo, y 46, primer y segundo párrafos, de la Ley para Regular las Instituciones de Tecnología Financiera
Normas oficiales y estándares internacionales (ISO/IEC27001)

el sector. Dentro de esta, se encuentran disposiciones aplicables en materia de gestión de riesgos, resguardo de datos personales y controles de seguridad en plataformas electrónicas para las IFPE.

Además de la ley *fintech*, se expidieron diversas disposiciones, las de carácter general relativas a las interfaces de programación de aplicaciones informáticas estandarizadas (API). Estas regulan la forma en que las IFPE deben compartir datos con terceros a través de estas herramientas, obligándolas a establecer medidas de seguridad de la información para los datos intercambiados.

Finalmente, le siguen las disposiciones aplicables a las instituciones de fondos de pago electrónico. En estas últimas, con fundamento en los artículos 46, 48 y 54 de la ley *fintech*, se detallan lineamientos puntuales sobre controles de acceso, notificación de incidentes, respaldo de información y continuidad operativa, por mencionar algunos. Estas disposiciones proporcionan requisitos mínimos de seguridad para proteger la información bajo la administración de las IFPE.

Adicionalmente, la adopción de estándares internacionales reconocidos que complementan la regulación nacional beneficia la operación de las IFPE. Estos sirven como guías de buenas prácticas y de referencia técnica para robustecer políticas de seguridad, auditorías y control de incidentes, lo que es de gran utilidad para complementar o alinear lo establecido en el marco legal mexicano con estándares globales de resiliencia operativa.

Dentro de estos destaca la ISO/IEC/27001, que establece requisitos para la implementación un sistema de gestión de seguridad y privacidad. En la tabla 1, se presenta un compendio de los principales instrumentos normativos analizados, que muestran la dispersión del marco legal mexicano.

CONCLUSIÓN

La dispersión normativa en materia de seguridad de la información para las IFPE en México representa un desafío estructural: genera vulnerabilidades, compromete la certeza jurídica y eleva los costos de cumplimiento, además de limitar la capacidad de respuesta ante posibles incidentes de seguridad.

Mientras otros países han transitado en búsqueda de una regulación convergente, el sistema mexicano se mantiene fraccionado, con disposiciones distintas dependiendo de la autoridad que los emita y sin un órgano rector que unifique los criterios.

Finalmente, se recomienda que México avance en la adopción de estándares internacionales para elevar la confianza del usuario y fortalecer la posición, en complemento con la armonización de normas.

Susana Cordova Ramos

Licenciada en Derecho. Especialista en derecho digital, enfocada en el análisis normativo de tecnologías emergentes. Graduada de la Maestría en Derecho de las Nuevas Tecnologías de la Información y Comunicación por el Centro de Investigación e Innovación en TIC (INFOTEC).

scordova612@gmail.com

REFERENCIAS

• Banco de México. (2017). Circular 14/2017, dirigida a las Instituciones de Crédito y Empresas que presten Servicios de Transferencia de Fondos. *Diario Oficial de la Federación*, 22 de noviembre de 2017.

• BFA Global. (2021). Regulación de Fintechs en México. https://bfaglobal.com/wp-content/uploads/2021/11/ES-Regulacio%CC%81n-de-Fintechs-en-Me%CC%81xico.pdf

• Disposiciones de carácter general relativas a las interfases de programación de aplicaciones informáticas estandarizadas. (2018). Comisión Nacional Bancaria y de Valores (CNBV). *Diario Oficial de la Federación*, 10 de septiembre de 2018.

• Disposiciones de carácter general aplicables a las Instituciones de Fondo de Pago Electrónico de la Ley para Regular las Instituciones de Tecnología Financiera. (2019). Comisión Nacional Bancaria y de Valores (CNBV). *Diario Oficial de la Federación*, 10 de septiembre de 2019.

• European Banking Authority. (2019). *EBA Report on the Impact of FinTech on Payment Institutions' and E-Money Institutions' Business Models.* https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/32ff1cbb-a6c3-4a01-94f2-4d129386fa0a/EBA%20thematic%20report%20on%20the%20impact%20of%20FinTech%20on%20PIs%27%20and%20EMIs%27%20business%20models.pdf

• Finnovista. (2025). *Finnovista Fintech Radar México 2025.* https://www.finnosummit.com/radar/fintechmexico2025/

• Gómez, R. y Montilla, L. (2025). Reglamento DORA: un nuevo paradigma de resiliencia operativa a digital en el sector financiero. *Actualidad Jurídica Uría Menendez*, (67), 133-141. https://www.uria.com/documentos/publicaciones/9340/documento/AJUM_67-2025.pdf?id=14024&forceDownload=true

• Herrman, D. y Pridöhl, H. (2020). Basic Concepts and Models of Cibersecurity. En M. Christen *et al*. (eds.), *The Ethics of Cybersecurity* (pp. 11-13). Spinger. https://doi.org/10.1007/978-3-030-29053-5_2

• Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2017). *Recomendaciones para el Tratamiento de Datos Personales y el Cumplimiento del Deber de Seguridad para las Instituciones de Tecnología Financiera.* México: INAI.

• ISO/IEC. (2020). ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts. International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en

• Ley de la Propiedad Industrial. (1991). Congreso de la Unión. *Diario Oficial de la Federación*, 27 de junio de 1991 (última reforma publicada el 1 de julio de 2020).

• Ley de Protección y Defensa al Usuario de Servicios Financieros. (1999). Congreso de la Unión. *Diario Oficial de la Federación*, 18 de enero de 1999 (última reforma publicada el 27 de diciembre de 2022).

• Ley Federal del Derecho de Autor. (1996). Congreso de la Unión. *Diario Oficial de la Federación*, 24 de diciembre de 1996 (última reforma publicada el 1 de julio de 2020).

• Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Congreso de la Unión. *Diario Oficial de la Federación*, 5 de julio de 2010.

• Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. (2012). Congreso de la Unión. *Diario Oficial de la Federación*, 17 de octubre de 2012.

• Ley para regular las Instituciones de Inteligencia Financiera (ley *fintech*). (2018). *Diario Oficial de la Federación*, 9 de marzo de 2018.

• Martínez Restrepo, J. y Lopez Restrepo, J. (2022). *Fintech: la revolución financiera en el siglo XXI.* Universidad Libre. https://repository.unilibre.edu.co/bitstream/handle/10901/26422/MD0607.pdf?sequence=1&isAllowed=y

• Monetary Authority of Singapore (MAS). (2021). *Technology Risk Management Guidelines.* https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

• Secretaría de Gobernación. (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*, 21 de diciembre de 2011.

• Uría Menéndez. (2025). *Actualidad Jurídica*, (67). https://www.uria.com/documentos/publicaciones/9340/documento/AJUM_67-2025.pdf?id=14024&forceDownload=true