INICIATIVA CON PROYECTO DE DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DE LA LEY GENERAL DE TURISMO, LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, EL CÓDIGO PENAL FEDERAL, CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES Y LA LEY DE SISTEMA DE PAGOS EN MATERIA DE PREVENCIÓN, RESPUESTA RÁPIDA Y SANCIÓN FRENTE A PÁGINAS FALSAS Y FRAUDES EN RESERVAS DE HOSPEDAJE Y PAQUETES VACACIONALES A CARGO DEL SENADOR EUGENIO SEGURA VÁZQUEZ, DEL GRUPO PARLAMENTARIO DE MORENA.

HONORABLE ASAMBLEA:

Quien suscribe, Eugenio Segura Vázquez, Senador de la República de la LXVI Legislatura e integrante del Grupo Parlamentario de MORENA, con fundamento en lo dispuesto por los artículos 71, fracción II, 72 y 73, fracción XXXI de la Constitución Política de los Estados Unidos Mexicanos, así como por los artículos 8, numeral 1, fracción I, 164, numeral 1 y 171, numeral 2, del Reglamento del Senado de la República, someto a la consideración del Pleno, la presente **Iniciativa con proyecto de decreto que reforma y adiciona diversas disposiciones de la Ley General de Turismo, Ley Federal de Protección al Consumidor, el Código Penal Federal, Código Nacional de Procedimientos Penales y la Ley de Sistema de Pagos en materia de prevención, respuesta rápida y sanción frente a páginas falsas y fraudes en reservas de hospedaje y paquetes vacacionales, al tenor de las siguientes:**

CONSIDERACIONES

La economía mexicana vive una etapa de expansión sostenida de sus canales digitales de intercambio. La digitalización ha permitido ampliar el acceso a bienes y servicios, reducir costos de transacción, facilitar la contratación a distancia y abrir mercados a empresas de todos los tamaños, incluidas las micro, pequeñas y medianas. En 2024, México registró 100.2 millones de personas usuarias de internet, equivalentes a 83.1% de la población de 6 años y más; adicionalmente, 35.8% de las personas usuarias realizó compras por internet. Este dato no es accesorio: revela que el comercio digital dejó de ser un nicho y se convirtió en una dimensión ordinaria de la vida económica y social del país (Instituto Nacional de Estadística y Geografía [INEGI], 2025a, pp. 3, 8).

Esa expansión del entorno digital ha sido acompañada por un esfuerzo institucional relevante del Estado mexicano para construir capacidades de ciberseguridad, fortalecer la infraestructura pública digital y ordenar los ecosistemas tecnológicos. La Estrategia Digital Nacional 2021-2024 concibió la seguridad de la información

como un referente de estabilidad, protección y certidumbre de la información generada o resguardada en sistemas o plataformas digitales, dentro de una visión de transformación tecnológica orientada al bienestar. En paralelo, la Guardia Nacional ha desarrollado capacidades permanentes de alertamiento, análisis y gestión de incidentes cibernéticos; la CONDUSEF, el Banco de México y la CNBV han reforzado el monitoreo de riesgos y operaciones digitales; y la PROFECO ha consolidado instrumentos para la protección del consumidor en el comercio electrónico (Presidencia de la República, 2021, numeral 4.3, Eje I, objetivo específico 5; Guardia Nacional, 2025, p. 84).

Sin embargo, el crecimiento del comercio digital y de los medios de pago electrónicos ha venido acompañado por una sofisticación creciente de los fraudes basados en suplantación digital. Una de sus modalidades más lesivas es la creación y operación de sitios web apócrifos que imitan la identidad de empresas, hoteles, agencias, comercios o instituciones, inducen a error a las personas consumidoras, capturan pagos y, en numerosos casos, obtienen además datos personales y financieros. Se trata de un fenómeno que no sólo afecta patrimonialmente a quien sufre el engaño; también erosiona la reputación de los proveedores legítimos, afecta la confianza en los mercados digitales y deteriora un activo económico esencial: la certidumbre transaccional (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros [CONDUSEF], 2023, p. 1; Guardia Nacional, 2025, p. 84).

La presente iniciativa parte de una convicción sencilla, pero jurídicamente exigente: un entorno digital amplio y dinámico requiere un estándar igualmente robusto de protección, trazabilidad y respuesta institucional. No se propone una sobrerregulación casuística, ni un rediseño maximalista del ordenamiento. Se propone, por el contrario, una reforma acotada, técnicamente depurada y constitucionalmente cuidadosa, que fortalece el marco vigente allí donde hoy existen los cuellos de botella más evidentes: la prevención, la identificación de actores, la preservación oportuna de evidencia, la contención del daño y la articulación entre protección al consumidor, investigación penal y seguridad en pagos (Quechol Maciel & Aguilar Antonio, 2025, pp. 1, 36, 51).

Diagnóstico nacional

El primer dato estructural del problema es la masificación del universo potencialmente expuesto. Como ya se señaló, 100.2 millones de personas usan internet en México y más de una tercera parte de las personas usuarias compra por esa vía. A ello se suma la escala del propio canal de pago digital: al cierre del primer trimestre de 2025 se efectuaron 388.5 millones de operaciones en comercio electrónico por un monto superior a 285 mil millones de pesos; de ellas, 69.2% se realizaron con tarjeta de débito y 30.8% con tarjeta de crédito. La propia

CONDUSEF reporta que, desde el primer trimestre de 2015 hasta el primero de 2025, la tasa media de crecimiento de estas operaciones fue de 7.3% en tarjeta de crédito y 11.0% en tarjeta de débito. Es decir, el país enfrenta el problema en un mercado de gran escala, de crecimiento sostenido y de uso cotidiano (INEGI, 2025a, pp. 3, 8; CONDUSEF, 2025, p. 179).

La ENVIPE 2025 estimó que en 2024 ocurrieron 33.5 millones de delitos asociados con 23.1 millones de víctimas. Dentro de ellos, el fraude fue el delito más frecuente: registró una tasa de 7,574 delitos por cada 100 mil habitantes y representó 21.7% del total de delitos estimados. La misma encuesta precisa que esa categoría incluye fraude bancario y fraude al consumidor, lo que la convierte en una fuente especialmente pertinente para dimensionar los ilícitos cometidos mediante engaño patrimonial en entornos digitales (INEGI, 2025b, pp. 3, 5, 8).

En 2024, sólo 9.6% de los delitos se denunció y apenas en 70.5% de esas denuncias se abrió carpeta de investigación. Ello implica una cifra oculta de 93.2%. Este dato es decisivo para el diseño normativo: significa que el problema no puede abordarse únicamente desde una lógica reactiva basada en denuncia e investigación penal posterior. Una política legislativa seria tiene que combinar mecanismos ex post con medidas ex ante de reducción de riesgo, interrupción temprana y trazabilidad. De otro modo, el Estado llega demasiado tarde (INEGI, 2025b, p. 15).

La ENVIPE 2025 estimó en 269.6 mil millones de pesos el costo total del delito y la inseguridad en los hogares, equivalente a 1.07% del PIB. En promedio, cada persona afectada perdió 6,226 pesos. Del total, 177.8 mil millones correspondieron a medidas preventivas y 91.8 mil millones a pérdidas por victimización. Aunque esta cifra no se agota en fraudes digitales, sí muestra con claridad que la inseguridad y el delito no son sólo un problema de orden público: son también una fricción económica de gran escala que consume ingreso, desalienta consumo y obliga a hogares y empresas a desviar recursos hacia protección y mitigación (INEGI, 2025b, p. 13).

La CONDUSEF reportó que al cierre de 2023 las reclamaciones por fraudes cibernéticos ascendieron a 5,762,195, con un monto reclamado de 20,018 millones de pesos. El rubro "Comercio por Internet" por sí solo concentró 5,146,774 reclamaciones y 7,928 millones de pesos reclamados. Adicionalmente, la propia CONDUSEF reportó que los fraudes cibernéticos pasaron de representar 59% del total de fraudes en 2018 a 71% en 2023. Estos datos muestran una tendencia clara: el fraude se ha desplazado crecientemente hacia canales digitales y, dentro de ellos, el comercio por internet es un vector central (CONDUSEF, 2023, p. 1).

En su Informe Anual de Actividades 2024, la Guardia Nacional reportó, a través de su área de ciberseguridad, la emisión de 69 alertas, la publicación de 543 boletines, la identificación de 37,119 incidentes de seguridad notificados a instancias en riesgo y la gestión de desactivación de 4,407 sitios web que usurpaban identidad para fraudes, propagación de malware y obtención de datos personales y financieros. De esos sitios, 3,831 simulaban pertenecer al sector gubernamental, 402 al sector privado y 174 al sector financiero. Este dato acredita dos extremos: primero, que el fenómeno de los sitios apócrifos existe a gran escala; segundo, que el Estado mexicano ya cuenta con experiencia operativa real para detectarlo y actuar. La reforma, por tanto, no parte de cero: parte de capacidades existentes que deben recibir un andamiaje jurídico más preciso y eficaz (Guardia Nacional, 2025, p. 84).

En suma, el diagnóstico fáctico permite afirmar, con evidencia oficial, que México enfrenta un problema real, masivo y económicamente relevante de fraude digital basado en engaño y suplantación; que el comercio electrónico ya tiene una dimensión estructural en la economía nacional; que la cifra negra impide descansar exclusivamente en una respuesta penal tardía; y que existe base institucional suficiente para justificar una reforma orientada a prevención, cooperación y contención temprana (INEGI, 2025a, pp. 3, 8; INEGI, 2025b, pp. 3, 5, 13, 15; CONDUSEF, 2023, p. 1; Guardia Nacional, 2025, p. 84).

Impacto económico y afectación a la confianza

La confianza es una condición de funcionamiento del mercado. En el comercio presencial, esa confianza suele construirse a partir de señales tangibles: ubicación física, contacto directo, reputación local, entrega inmediata. En el comercio digital, en cambio, la confianza depende en gran medida de señales técnicas e institucionales: autenticidad del sitio, integridad de la identidad comercial, seguridad del canal de pago, trazabilidad del proveedor, capacidad de reclamación y expectativa razonable de respuesta. Cuando la suplantación digital se vuelve frecuente, se debilita precisamente esa arquitectura de confianza (INEGI, 2025a, pp. 3, 8; CONDUSEF, 2023, p. 1).

La relevancia macroeconómica del tema se entiende mejor si se observa la velocidad de expansión del ecosistema. El Banco de México reportó que las operaciones realizadas en comercio electrónico crecieron 27.2% de 2023 a 2024. La CONDUSEF, con base en información de Banco de México, registró 388.5 millones de operaciones de comercio electrónico en el primer trimestre de 2025 y un aumento anual de 33.1% en número de operaciones y de 30.5% en monto frente al primer trimestre de 2024. En un mercado de ese tamaño y dinamismo, la confianza no es una variable colateral: es una infraestructura económica. Su deterioro no sólo perjudica a víctimas individuales; eleva costos de transacción, desincentiva compras, desplaza demanda a canales menos eficientes y castiga

reputacionalmente a proveedores cumplidos (Banco de México, 2025, pp. 69-70; CONDUSEF, 2025, p. 179).

Además, el daño no recae de manera uniforme. Los sitios apócrifos afectan con mayor intensidad a quienes tienen menos herramientas para verificar señales técnicas o detectar patrones sofisticados de engaño. La política pública, por tanto, no sólo tiene una racionalidad económica, sino una dimensión de equidad. Proteger la autenticidad de las transacciones digitales es también proteger a personas consumidoras en posición de vulnerabilidad informativa frente a estructuras delictivas cada vez más profesionalizadas. INTERPOL ha advertido, justamente, que el uso de inteligencia artificial, criptomonedas y modelos de "fraude como servicio" ha profesionalizado y abaratado la ejecución de campañas fraudulentas a escala global (INTERPOL, 2024, pp. 4-7).

En ese contexto, la presente iniciativa busca preservar una trayectoria positiva de digitalización y expansión del comercio electrónico en México, reforzando la confianza mediante reglas generales y mecanismos operativos proporcionados. No se trata de "frenar" la economía digital, sino de hacerla más segura, más confiable y, por ello mismo, más sostenible (Banco de México, 2025, pp. 69-70; CONDUSEF, 2025, p. 179).

Esfuerzos institucionales previos y bases sobre las que se construye la reforma

Esta iniciativa reconoce expresamente los esfuerzos ya realizados por el Estado mexicano en los últimos años. La Estrategia Digital Nacional 2021-2024 configuró una hoja de ruta para orientar los esfuerzos tecnológicos y de seguridad de la información de la Administración Pública Federal, identificando a la seguridad de la información como un principio de estabilidad, protección y certidumbre. La Guardia Nacional, en el marco de esa arquitectura institucional, asumió la responsabilidad de establecer y operar el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y ha construido capacidades de alerta, monitoreo y desactivación de infraestructura maliciosa (Presidencia de la República, 2021, numeral 4.3, Eje I, objetivo específico 5; Guardia Nacional, 2025, p. 84).

En el ámbito de protección al consumidor, la LFPC ya reconoce desde hace tiempo un capítulo específico para transacciones efectuadas por medios electrónicos, ópticos o cualquier otra tecnología. En el ámbito financiero, el Banco de México y la CNBV han profundizado instrumentos de supervisión, gestión de riesgos y seguridad operacional. Incluso en el plano de la información al consumidor, la PROFECO cuenta con instrumentos como el Distintivo Digital, que buscan generar señales de confianza y cumplimiento en entornos de comercio electrónico (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis).

La lógica de la presente propuesta no es, por tanto, desconocer el marco construido ni sustituirlo con una regulación enteramente nueva. Su lógica es distinta: consolidar, articular y fortalecer ese marco para enfrentar una modalidad delictiva cuya peligrosidad deriva precisamente de operar en las intersecciones entre ramas normativas y entre sectores regulados. El sitio apócrifo se aprovecha del espacio entre consumidor, proveedor, infraestructura digital y pago. La respuesta legislativa debe cerrar ese espacio sin perder generalidad ni caer en hiperreformas de detalle (Quechol Maciel & Aguilar Antonio, 2025, pp. 1, 36, 51).

Mejores prácticas internacionales

La experiencia comparada muestra que los países con mejores resultados frente al fraude digital no descansan exclusivamente en aumentos de pena. Lo que hacen es distribuir deberes mínimos de diligencia a lo largo del ecosistema, acelerar la interrupción de la infraestructura fraudulenta y crear circuitos claros de reporte, trazabilidad y reparación (Australian Competition and Consumer Commission, 2024, p. 7; European Union, 2022, art. 30).

En el Reino Unido, el National Cyber Security Centre permite a cualquier persona reportar correos, mensajes y sitios sospechosos; el propio NCSC señala expresamente que tiene la facultad de investigar y retirar sitios fraudulentos. Este modelo de reporte simple y respuesta rápida disminuye la fricción entre detección ciudadana e intervención pública (National Cyber Security Centre, s. f.).

También en el Reino Unido, Nominet opera "Domain Watch", un mecanismo para identificar y suspender con rapidez dominios recién registrados que constituyen intentos evidentes de phishing. La lógica es clara: buena parte del daño puede evitarse si la infraestructura fraudulenta es detectada y suspendida antes de alcanzar masa crítica de víctimas (Nominet, s. f.).

A nivel del sistema de nombres de dominio, ICANN reforzó desde 2024 las obligaciones contractuales de mitigación de DNS abuse para registries y registrars, incluyendo phishing. La enseñanza regulatoria es importante: la infraestructura técnica no puede permanecer jurídicamente indiferente frente a usos manifiestamente abusivos cuando cuenta con señales suficientes para actuar y canales institucionales para cooperar (ICANN, 2024).

La Unión Europea, mediante el Digital Services Act, incorporó obligaciones de trazabilidad de comerciantes en marketplaces y plataformas que intermedian contratos a distancia con consumidores. El artículo 30 exige obtener información identificatoria, datos de contacto y, en su caso, cuenta de pago del comerciante, así como realizar esfuerzos razonables para verificar la fiabilidad de esa información. El valor de esta medida no es retórico: limita el anonimato funcional del oferente y

mejora la capacidad de respuesta pública y privada cuando aparece un fraude de suplantación o venta engañosa (European Union, 2022, art. 30).

Australia ha avanzado aún más hacia un modelo sistémico. El National Anti-Scam Centre publica reportes consolidados, integra información de varias fuentes y coordina acciones con bancos, telcos, plataformas y autoridades. En 2023, Australia registró más de 601 mil reportes de scam y pérdidas combinadas por 2.74 mil millones de dólares australianos; el propio reporte atribuye la reducción de pérdidas, pese al aumento de reportes, a esfuerzos concertados de gobierno, bancos, telecomunicaciones y plataformas digitales. Sobre esa base, el Scams Prevention Framework estableció obligaciones consistentes y exigibles para sectores clave donde operan los estafadores, y previó rutas claras de reporte y compensación cuando las obligaciones no se cumplen (Australian Competition and Consumer Commission, 2024, p. 7; Australian Treasury, 2025, pp. 4-5).

En materia de pagos, el Reino Unido ha impulsado la "Confirmation of Payee", un sistema de verificación del nombre del beneficiario antes de la transferencia, y el Payment Systems Regulator estableció en 2024 un régimen de reembolso para APP scams en Faster Payments. Más allá del detalle técnico británico, la lección normativa es nítida: los sistemas de pago deben incorporar controles específicos frente a transferencias inducidas por engaño, y las reglas de responsabilidad deben alinear incentivos para prevenir mejor (Payment Systems Regulator, 2024, pp. 1-3).

Por su parte, el Internet Crime Complaint Center de Estados Unidos no sólo consolida reportes de fraude y cibercrimen, sino que opera esquemas de recuperación y congelamiento de fondos coordinados con instituciones financieras. En su reporte 2024, el IC3 señaló pérdidas reportadas por 16.6 mil millones de dólares y destacó la operación de su Recovery Asset Team y de la Financial Fraud Kill Chain para intentar congelar recursos cuando la denuncia es oportuna (FBI Internet Crime Complaint Center, 2025, pp. 3, 12, 14).

Estas prácticas comparadas convergen en cinco principios: primero, reporte ciudadano simple y centralizado; segundo, trazabilidad mínima del oferente o comerciante; tercero, cooperación obligatoria y expedita de intermediarios técnicos; cuarto, preservación rápida de evidencia y desactivación proporcional de infraestructura fraudulenta; y quinto, controles de riesgo específicos en pagos. Son precisamente esos cinco principios los que orientan esta iniciativa (European Union, 2022, art. 30; Australian Competition and Consumer Commission, 2024, p. 7; Payment Systems Regulator, 2024, pp. 1-3).

Recomendaciones expertas nacionales

La literatura especializada mexicana ha sido consistente en advertir que una respuesta meramente penal o exclusivamente estado-céntrica resulta insuficiente. El estudio "¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023)" concluye que muchas iniciativas mexicanas han privilegiado enfoques centrados en seguridad nacional y seguridad pública, dejando en segundo plano derechos humanos, asociaciones público-privadas, cooperación institucional e internacional, protección de infraestructura crítica y adaptación tecnológica. El mismo trabajo destaca que la colaboración multisectorial, los estándares mínimos de responsabilidad cibernética y la claridad, adaptación y comprensión normativa son elementos frecuentemente omitidos (Quechol Maciel & Aguilar Antonio, 2025, pp. 1-2, 36, 51).

Ese diagnóstico académico es particularmente pertinente para el problema que atiende esta iniciativa. El fraude por sitios apócrifos no se agota en una agresión individual; es una conducta que explota, simultáneamente, reglas de identidad comercial, contratación electrónica, publicidad, protección de datos, procesamiento de pagos y capacidad de investigación digital. Por ello, la reforma debe ser intersectorial y, a la vez, contenida. Intersectorial, para conectar piezas hoy dispersas; contenida, para no convertir el ordenamiento en una suma caótica de microtipos o cargas imposibles de administrar (Quechol Maciel & Aguilar Antonio, 2025, pp. 19, 25, 36).

Otro trabajo relevante, "Delitos informáticos en México. Reconocimiento en los ordenamientos penales…", documenta que en México existe dispersión normativa y ausencia de un cuerpo suficientemente articulado para reconocer, investigar y mitigar conductas informáticas, a pesar de múltiples iniciativas legislativas. El artículo subraya que, aunque han existido esfuerzos, no se han hecho las reformas necesarias para implementar medidas y procedimientos suficientes para sancionar o mitigar de modo eficaz estas conductas (Alcalá Casillas, 2023, p. 5).

La iniciativa que ahora se propone toma muy en serio esas advertencias. Por ello evita dos errores frecuentes: el primero, creer que el problema se resuelve sólo "tipificando más"; el segundo, pretender una codificación total del ciberespacio. Lo que se plantea es una solución postdoctoral en el buen sentido del término: jurídicamente sobria, funcionalmente inteligente y normativamente armónica (Quechol Maciel & Aguilar Antonio, 2025, pp. 36, 51; Alcalá Casillas, 2023, p. 5).

Estado actual de la regulación en México

México no parte de un vacío normativo. Existe un conjunto valioso de disposiciones que hoy ya protegen, aunque de manera fragmentada, distintos componentes del problema.

La Ley Federal de Protección al Consumidor contiene, en su Capítulo VIII Bis, un régimen específico para transacciones efectuadas a través de medios electrónicos, ópticos o cualquier otra tecnología. Su artículo 76 Bis obliga al proveedor a usar la información del consumidor de forma confidencial; emplear elementos técnicos para brindar seguridad y confidencialidad; informar previamente las características generales de esos elementos; proporcionar domicilio físico, teléfonos y demás medios para reclamaciones o aclaraciones; y evitar prácticas comerciales engañosas respecto de las características de los productos. Es una base normativa correcta y valiosa, pero fue diseñada principalmente para una relación bilateral proveedor-consumidor, no para ecosistemas complejos de intermediación digital ni para suplantaciones a gran escala (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis).

El Código Penal Federal tipifica el fraude en su artículo 386 como la conducta de quien, engañando a alguien o aprovechándose del error en que éste se halla, se hace ilícitamente de una cosa o alcanza un lucro indebido. Esa fórmula es suficientemente amplia para abarcar numerosos fraudes digitales. Sin embargo, la práctica demuestra que la imputación y la investigación se dificultan cuando el engaño se despliega a través de sitios, dominios, perfiles, anuncios y pasarelas que fragmentan la conducta en varios intermediarios y que requieren reglas procedimentales específicas para preservar evidencia de forma útil y oportuna (Cámara de Diputados del H. Congreso de la Unión, 2025b, art. 386).

El Código Nacional de Procedimientos Penales ya prevé, en su artículo 303, la solicitud de localización geográfica en tiempo real y entrega de datos conservados a concesionarios de telecomunicaciones, autorizados y proveedores de servicios de aplicaciones y contenidos de equipos móviles. El artículo exige control judicial, expresión de motivos e indicios, y respuesta inmediata. Esa herramienta es muy importante, pero su diseño vigente está más claramente orientado a líneas y equipos de comunicación móvil que al conjunto de custodios de evidencia esencial en fraudes de sitios apócrifos, como registradores de dominios, hospedaje, plataformas de anuncios o intermediarios equivalentes (Cámara de Diputados del H. Congreso de la Unión, 2025a, art. 303).

La Ley de Sistemas de Pagos también ofrece una base útil. Su artículo 6 dispone que las normas internas de cualquier sistema de pagos deben propiciar eficiencia y seguridad, sujetarse a la autorización del Banco de México y prever, entre otras cuestiones, medios de control de riesgos y medidas de seguridad del sistema operativo, incluidas acciones correctivas y planes de contingencia. El problema no es la ausencia absoluta de mandato legal, sino que ese mandato aún no visibiliza de manera expresa los fraudes inducidos por suplantación digital como categoría de

riesgo que debe ser atendida con herramientas específicas (Cámara de Diputados del H. Congreso de la Unión, 2025g, art. 6).

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por su parte, tiene por objeto proteger los datos personales en posesión de particulares y regular su tratamiento legítimo, controlado e informado para garantizar la privacidad y la autodeterminación informativa. Esta ley es especialmente relevante porque buena parte del daño de un sitio apócrifo no se agota en el pago fraudulento; incluye también la captación ilegítima de nombres, correos, teléfonos, credenciales y datos financieros (Cámara de Diputados del H. Congreso de la Unión, 2025f, art. 1).

A su vez, la Ley Federal de Protección a la Propiedad Industrial ya reconoce como infracción usar, sin consentimiento del titular, una marca registrada o semejante en grado de confusión como elemento de un nombre de dominio o viceversa, cuando esos nombres estén relacionados con establecimientos que operen con los productos o servicios protegidos por la marca. Esto es particularmente pertinente para los supuestos en que el fraude opera mediante clonación de identidad comercial y uso indebido de marcas en dominios apócrifos (Cámara de Diputados del H. Congreso de la Unión, 2025e, art. 386, fr. XX).

Finalmente, el Código de Comercio reconoce la validez de los mensajes de datos y de la contratación electrónica, lo que resulta indispensable para la prueba y para la seguridad jurídica de las transacciones digitales. En otras palabras, el sistema jurídico mexicano sí ha incorporado progresivamente la dimensión digital del tráfico económico. Lo que hoy hace falta no es una refundación del sistema, sino una articulación mejor entre sus piezas (Cámara de Diputados del H. Congreso de la Unión, 2025c, arts. 89 y 89 bis).

Insuficiencias del marco vigente

La insuficiencia principal del marco actual no es conceptual, sino funcional. Hoy existen obligaciones del proveedor, tipos penales generales, facultades de investigación digital, reglas de seguridad en pagos y regímenes de protección de datos y propiedad industrial. Pero esos instrumentos operan en compartimentos relativamente aislados. El fraude por suplantación digital, en cambio, es transversal (Quechol Maciel & Aguilar Antonio, 2025, pp. 1-2, 36).

Primero, el régimen de consumo electrónico descansa sobre la figura del proveedor identificable. El sitio apócrifo justamente destruye esa premisa: se presenta como proveedor legítimo sin serlo. Por eso, si la norma sólo mira la conducta del proveedor final y no impone deberes mínimos de diligencia a ciertos intermediarios

digitales relevantes, deja sin tratar parte del problema (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis; European Union, 2022, art. 30).

Segundo, la respuesta penal llega tarde si antes no existe un circuito jurídicamente claro para preservar evidencia y suspender, con control judicial, la disponibilidad de infraestructura manifiestamente fraudulenta. En delitos que se consuman en horas y cuyos rastros técnicos pueden volatilizarse con rapidez, la oportunidad vale tanto como la tipificación (Cámara de Diputados del H. Congreso de la Unión, 2025a, art. 303).

Tercero, el sistema de pagos puede incorporar controles más explícitos frente a fraudes inducidos por engaño. La experiencia comparada demuestra que la sola existencia de una transferencia "autorizada" por el usuario no basta para desentender al sistema del problema si la autorización fue obtenida mediante una suplantación técnicamente sofisticada (Cámara de Diputados del H. Congreso de la Unión, 2025g, art. 6; Payment Systems Regulator, 2024, pp. 1-3).

Cuarto, la cooperación entre sector público y actores privados del ecosistema digital sigue dependiendo en buena medida de esquemas administrativos, prácticas institucionales o buenas voluntades, cuando la evidencia académica y comparada sugiere la necesidad de estándares mínimos más explícitos (Quechol Maciel & Aguilar Antonio, 2025, pp. 1-2, 36, 51).

Objeto y racionalidad de la iniciativa

La presente iniciativa tiene por objeto fortalecer la prevención, investigación y contención de fraudes por suplantación digital, especialmente aquellos cometidos mediante sitios web apócrifos u otros medios análogos de engaño digital, a través de una reforma mínima, general y tecnológicamente neutral de cuatro ordenamientos federales: la Ley Federal de Protección al Consumidor, el Código Penal Federal, el Código Nacional de Procedimientos Penales y la Ley de Sistemas de Pagos (Cámara de Diputados del H. Congreso de la Unión, 2025a, 2025b, 2025d, 2025g).

La racionalidad de este diseño es deliberadamente minimalista. No se crea una ley general nueva de servicios digitales. No se multiplica el catálogo de tipos penales. No se traslada al texto legal el detalle técnico que corresponde al regulador especializado. Lo que se hace es introducir, en los puntos correctos del ordenamiento, los mandatos generales que hoy faltan para cerrar los vacíos más costosos. Esa opción responde también a la crítica académica a iniciativas excesivamente fragmentarias o sobrerreguladas, y al principio de claridad y adaptación normativa (Quechol Maciel & Aguilar Antonio, 2025, pp. 6, 36, 51).

Contenido de la reforma propuesta

En la Ley Federal de Protección al Consumidor se incorpora una categoría funcional de intermediación digital para efectos del capítulo de transacciones electrónicas. No se trata de equiparar sin matices a todos los actores tecnológicos con el proveedor final, sino de reconocer que ciertos terceros facilitan de manera directa o indirecta la promoción, contratación, cobro o canalización hacia el proveedor y que, por ello, deben asumir obligaciones mínimas de diligencia. Entre ellas se encuentran la verificación razonable de identidad y medios de contacto del proveedor que usa sus servicios, la existencia de mecanismos accesibles para reportar suplantaciones y prácticas engañosas, la conservación inmediata de registros cuando exista requerimiento de autoridad competente y la colaboración con autoridades en la mitigación de prácticas que induzcan a error al consumidor. Esta solución toma la lógica de trazabilidad del DSA europeo, pero la adapta al contexto mexicano desde la LFPC, sin crear una legislación paralela (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis; European Union, 2022, art. 30).

Asimismo, en la LFPC se refuerza el deber del proveedor de identificar de manera clara sus canales oficiales de contratación y pago y de abstenerse de inducir a error respecto de la autenticidad de los medios electrónicos utilizados. Con ello se robustece el estándar informativo ya contenido en el artículo 76 Bis, se mejora la capacidad de verificación del consumidor y se dota a la PROFECO de una base más clara para actuar frente a la simulación de identidad comercial en entornos digitales (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis).

En el Código Penal Federal se incorpora una modalidad equiparada de fraude para los supuestos en que, con ánimo de lucro indebido, se utilicen sitios web, aplicaciones, dominios, perfiles digitales o cualquier medio tecnológico para suplantar o hacer aparecer como propia la identidad comercial o institucional de un tercero e inducir a error a consumidores o usuarios para realizar pagos, transferencias o entrega de datos. También se prevé un agravante cuando la conducta permita afectar a una pluralidad indeterminada de personas. La decisión dogmática es importante: no se crea un tipo casuístico hiperdescriptivo, sino una calificación del fraude coherente con el plus de antijuridicidad que representa la ingeniería masiva de confianza digital (Cámara de Diputados del H. Congreso de la Unión, 2025b, art. 386).

En el Código Nacional de Procedimientos Penales se fortalece el régimen de conservación y entrega de datos para que, cuando sea necesaria la investigación de estos hechos, el Ministerio Público pueda requerir judicialmente la preservación y entrega expedita de información relevante también a custodios tecnológicos que hoy no aparecen con la suficiente claridad en la regulación: prestadores de hospedaje, nombres de dominio, servicios de aplicaciones y contenidos, plataformas de

intermediación o publicidad digital y proveedores tecnológicos análogos. Adicionalmente, se habilita al juez de control para autorizar, de manera temporal, proporcional y revisable, la suspensión provisional del acceso o disponibilidad del recurso digital identificado cuando ello sea estrictamente necesario para impedir la continuación de la conducta delictiva o evitar un daño inminente a víctimas. Aquí el criterio rector es el debido proceso: rapidez sí, pero con control judicial, motivación, temporalidad y contradicción (Cámara de Diputados del H. Congreso de la Unión, 2025a, art. 303).

En la Ley de Sistemas de Pagos se incorpora de forma expresa el mandato para que las normas internas contemplen mecanismos de prevención, detección, contención y atención de fraudes inducidos por engaño o suplantación digital en órdenes de transferencia, incluyendo medidas de verificación y acciones correctivas. La reforma no impone en ley un diseño técnico cerrado. Deja ese detalle, correctamente, al Banco de México y a las disposiciones de carácter general que correspondan. Con ello se conserva flexibilidad regulatoria y se reconoce la competencia técnica del regulador, al tiempo que se envía una señal legal clara: los fraudes inducidos por suplantación digital son un riesgo propio de los sistemas de pago y deben ser tratados como tal (Cámara de Diputados del H. Congreso de la Unión, 2025g, art. 6).

Fortalecimiento sectorial en materia turística

De forma destacada, pues es el sector en donde la suplantación presenta mayor incidencia, la reforma fortalece al sector turísticos y se enfoca con detalle en él. La presente iniciativa también fortalece, de manera específica, la Ley General de Turismo, a partir de una premisa clara: en el sector turístico la autenticidad de la identidad comercial del prestador no es sólo un tema de información mercantil, sino una condición básica de protección al turista, de confianza en la contratación a distancia y de competitividad del mercado turístico nacional. La propia Ley General de Turismo reconoce, desde su artículo 1, que la materia turística comprende procesos derivados de viajes y estancias temporales y que éstos constituyen una actividad prioritaria nacional bajo un enfoque social y económico que genera desarrollo regional; asimismo, su artículo 2 establece como fines de la ley optimizar la calidad y competitividad de los servicios turísticos, impulsar la modernización de la actividad turística, regular a los prestadores de servicios turísticos y establecer bases para la orientación y asistencia a los turistas (Cámara de Diputados del H. Congreso de la Unión, 2025h, arts. 1 y 2). En esa lógica, incorporar medidas contra la suplantación digital de identidad de prestadores turísticos no desnaturaliza la ley: por el contrario, actualiza sus instrumentos para responder a un riesgo contemporáneo que afecta directamente la calidad, confiabilidad y seguridad del mercado turístico.

La reforma a la Ley General de Turismo se apoya, además, en una institución ya existente y plenamente congruente con el objeto de la ley: el Registro Nacional de Turismo. Conforme al artículo 46 de la Ley General de Turismo, el Registro es el catálogo público de prestadores de servicios turísticos en el país y constituye el mecanismo mediante el cual la Federación, las entidades federativas, los municipios y la Ciudad de México pueden contar con información sobre dichos prestadores; el artículo 49 dispone, además, que debe operar bajo el principio de máxima publicidad, y el artículo 50 ordena a la Secretaría difundir la información que derive de dicho Registro a través de su página web y otros medios que determine. En la práctica administrativa, la Secretaría de Turismo ya opera una consulta pública oficial del Registro Nacional de Turismo, accesible por nombre comercial o folio, y señala expresamente que los certificados de inscripción tienen una vigencia de dos años, lo cual confirma que el Registro ya cumple una función de identificación y verificación pública sectorial. En consecuencia, adicionar a esa arquitectura registral la posibilidad de verificar medios digitales oficiales de contacto, comercialización y atención no implica crear una institución nueva, sino fortalecer una herramienta existente para hacerla funcional frente a un riesgo emergente (Cámara de Diputados del H. Congreso de la Unión, 2025h, arts. 46, 49 y 50; Secretaría de Turismo, s. f.-a).

Por esa razón, la iniciativa adiciona un párrafo al artículo 46 de la Ley General de Turismo para que el Registro Nacional de Turismo constituya también un mecanismo de verificación pública de la identidad y, en su caso, de los medios digitales oficiales de contacto, comercialización y atención de los prestadores de servicios turísticos, en los términos que determinen las disposiciones reglamentarias. Esta modificación es consistente con el diseño vigente del propio Registro, ya que la ley actualmente remite al Reglamento para determinar tanto la información exigible como las personas obligadas a inscribirse, y el Reglamento ya prevé que los prestadores ratifiquen, rectifiquen o actualicen sus datos registrales, así como cambios de domicilio, denominación o razón social. La reforma, por tanto, no introduce una lógica ajena, sino que actualiza el contenido verificable del Registro conforme a la evolución digital del mercado turístico (Cámara de Diputados del H. Congreso de la Unión, 2025h, art. 46; Secretaría de Turismo, 2015, art. 94).

En la misma dirección, la adición de un párrafo al artículo 49 y de una oración al artículo 51 fortalece el valor preventivo del Registro Nacional de Turismo. Hoy la ley ya establece que el Registro debe operar bajo máxima publicidad y que corresponde a las autoridades locales constatar la veracidad de la información que proporcionen los prestadores de servicios turísticos. La reforma precisa que, como medida para prevenir la suplantación digital de identidad corporativa, la información relativa a la identidad del prestador, la vigencia de su inscripción y sus medios digitales oficiales de contacto, comercialización y atención deberá estar disponible al público, y que la

obligación de verificación por parte de las autoridades también comprenderá la información relativa a dichos medios digitales oficiales. Con ello, la ley traduce el principio general de publicidad registral en una función concreta de prevención del fraude digital: permitir al turista contrastar información auténtica y dotar a la autoridad de un parámetro verificable para actuar tempranamente (Cámara de Diputados del H. Congreso de la Unión, 2025h, arts. 49 y 51).

La reforma al artículo 58 también cumple una función esencial. La Ley General de Turismo ya impone a los prestadores obligaciones como informar precios y condiciones, implementar procedimientos alternativos para quejas, inscribirse en el Registro y actualizar oportunamente sus datos, así como cumplir con los servicios, precios, tarifas y promociones ofrecidos. Sobre esa base preexistente, la iniciativa agrega obligaciones estrechamente vinculadas con la realidad del mercado turístico digital: identificar de manera clara y verificable sus medios oficiales de contacto, comercialización, reservación, pago y atención; mantener actualizada en el Registro la información relativa a dichos medios; y dar aviso oportuno a la Secretaría y a las autoridades competentes cuando tengan conocimiento del uso indebido, falsificación o suplantación digital de su identidad comercial. Estas obligaciones no convierten al prestador en policía del ciberespacio ni le imponen cargas desproporcionadas; simplemente extienden al plano digital el deber ya existente de información veraz, actualización registral y colaboración con la autoridad, en congruencia con la propia estructura del artículo 58 (Cámara de Diputados del H. Congreso de la Unión, 2025h, art. 58).

Desde la perspectiva de los derechos del turista, la adición de una nueva fracción al artículo 61 también resulta plenamente consistente con la ley vigente. El artículo 61 reconoce hoy el derecho del turista a recibir información útil, precisa, veraz y detallada, a obtener los servicios en las condiciones contratadas y a recibir la documentación correspondiente. La incorporación del derecho a recibir orientación y canalización inmediata ante la autoridad competente cuando el turista sea víctima o probable víctima de fraude por suplantación digital vinculada con servicios turísticos no hace sino actualizar el alcance de ese estatuto de protección, trasladándolo a uno de los principales espacios de riesgo de la contratación contemporánea: el entorno digital. No se crea un derecho extraño al sistema; se fortalece el deber estatal de orientación y asistencia previsto en el propio objeto de la Ley General de Turismo (Cámara de Diputados del H. Congreso de la Unión, 2025h, arts. 2, fr. XIV, y 61).

En su dimensión reactiva, las reformas a los artículos 68 y 69 también guardan plena armonía con la lógica vigente del ordenamiento. El artículo 68 ya prevé que las infracciones a la Ley, su Reglamento y las normas oficiales mexicanas, así como las derivadas de las quejas de los turistas, serán sancionadas por la Secretaría

mediante el procedimiento administrativo correspondiente; incluso, dispone ya que cuando una queja presentada ante la Procuraduría Federal del Consumidor revele un probable incumplimiento de la Ley General de Turismo, la Secretaría podrá iniciar procedimiento y requerir información al prestador. La iniciativa se limita a precisar que, cuando la queja o denuncia verse sobre probable suplantación digital de identidad de un prestador turístico o sobre medios digitales que aparenten corresponderle, la Secretaría podrá requerir información, emitir alertas preventivas al público y dar vista inmediata a las autoridades competentes. Se trata de una actualización puntual del mecanismo reactivo ya existente, no de una potestad extraordinaria o ajena al diseño legal actual (Cámara de Diputados del H. Congreso de la Unión, 2025h, art. 68).

Finalmente, la adición al artículo 69 es consistente con la estructura sancionatoria ya prevista para el Registro Nacional de Turismo. Actualmente, la ley sanciona tanto la falta de inscripción al Registro como la omisión o inexactitud de información proporcionada para dicho Registro, y prevé un requerimiento de cinco días hábiles para subsanar antes de imponer multa. La nueva regla simplemente extiende ese mismo patrón a la información relativa a los medios digitales oficiales: si el prestador omite registrarlos, actualizarlos o corregirlos, o proporciona información inexacta sobre ellos, será requerido para subsanar en el mismo plazo y, en caso de incumplimiento, se hará acreedor a la multa correspondiente. La reforma, por tanto, no crea una sanción disruptiva ni rompe la proporcionalidad interna del sistema; replica la lógica ya vigente para una categoría de información cuya relevancia práctica ha crecido de forma evidente en el mercado turístico contemporáneo (Cámara de Diputados del H. Congreso de la Unión, 2025h, art. 69).

Estas modificaciones a la Ley General de Turismo cumplen, en suma, una función complementaria de alto valor. Mientras la reforma a la Ley Federal de Protección al Consumidor establece deberes generales de identificación y diligencia en el comercio electrónico; la reforma penal tipifica con mayor precisión la suplantación digital con fin de lucro; la reforma al Código Nacional de Procedimientos Penales fortalece la preservación de evidencia y la reacción judicial temprana; y la reforma a la Ley de Sistemas de Pagos ordena incorporar mecanismos específicos de prevención y contención en las transferencias, la reforma sectorial turística añade una capa propia de prevención, verificación pública, orientación al turista y reacción administrativa temprana en uno de los sectores donde la contratación anticipada a distancia es parte esencial del modelo de negocio. De esta forma, la iniciativa articula una respuesta transversal, pero al mismo tiempo reconoce que en el turismo la confianza, la información verificable y la identidad del prestador constituyen bienes jurídicos y económicos particularmente sensibles (Cámara de Diputados del H. Congreso de la Unión, 2025d, art. 76 Bis; Cámara de Diputados del H. Congreso

de la Unión, 2025h, arts. 46, 49, 51, 58, 61, 68 y 69; Secretaría de Turismo, s. f.-a; Distintivo Digital PROFECO, 2025).

Qué problemas concretos busca resolver la iniciativa

La iniciativa busca resolver, de manera simultánea, cinco problemas.

Primero, la opacidad del oferente en entornos digitales. La trazabilidad mínima y la verificación razonable no eliminan todo fraude, pero sí reducen drásticamente la facilidad con la que un actor anónimo puede montar ofertas, cobrar y desaparecer (European Union, 2022, art. 30).

Segundo, la lentitud de la contención. En la práctica, el daño de un sitio apócrifo crece exponencialmente mientras el sitio sigue disponible. La suspensión provisional, judicialmente controlada, está pensada para acortar esa ventana de daño (National Cyber Security Centre, s. f.; Cámara de Diputados del H. Congreso de la Unión, 2025a, art. 303).

Tercero, la pérdida de evidencia digital. Sin preservación inmediata de datos de dominio, hospedaje, anuncios, pagos y comunicaciones, la investigación se vuelve frecuentemente estéril. Por ello la reforma procesal es tan importante como la penal (Cámara de Diputados del H. Congreso de la Unión, 2025a, art. 303).

Cuarto, la insuficiente alineación de incentivos en pagos. Si el sistema de pagos no incorpora controles explícitos para fraudes inducidos por engaño, parte del costo seguirá recayendo casi exclusivamente en la víctima. La reforma no define el instrumento técnico exacto, pero sí ordena que exista una respuesta regulatoria especializada (Cámara de Diputados del H. Congreso de la Unión, 2025g, art. 6; Payment Systems Regulator, 2024, pp. 1-3).

Quinto, la fragmentación institucional. Al distribuir deberes mínimos en consumo, penal, procedimiento y pagos, la iniciativa articula un circuito más coherente entre prevención, denuncia, investigación y mitigación (Quechol Maciel & Aguilar Antonio, 2025, pp. 36, 51).

Resultados esperados

La iniciativa persigue resultados concretos y verificables. En primer término, reducir el tiempo entre el reporte de una suplantación y la preservación útil de evidencia. En segundo lugar, disminuir el tiempo entre la identificación de una infraestructura fraudulenta y su suspensión provisional. En tercer término, elevar la trazabilidad de oferentes y canales de cobro en entornos de intermediación digital. En cuarto lugar, fortalecer la capacidad del sistema de pagos para prevenir y contener fraudes inducidos por engaño. Finalmente, proteger la confianza de las personas

consumidoras y de los proveedores legítimos en un mercado digital que, como muestran los datos oficiales, seguirá creciendo en escala y relevancia para la economía nacional (INEGI, 2025a, pp. 3, 8; CONDUSEF, 2025, p. 179; Guardia Nacional, 2025, p. 84).

No se promete, irresponsablemente, la erradicación del fraude digital. Ningún ordenamiento serio puede hacerlo. Lo que sí hace esta iniciativa es mover el punto de equilibrio a favor del consumidor, del proveedor legítimo y del interés público: aumenta la dificultad operativa del fraude, reduce su ventana de ejecución, mejora la posibilidad de atribución y fortalece la confianza en la economía digital mexicana. Esa es, precisamente, la función de una reforma bien hecha (Quechol Maciel & Aguilar Antonio, 2025, pp. 36, 51).

México ha avanzado de manera importante en la construcción de capacidades digitales, en la protección del consumidor y en la seguridad de su infraestructura tecnológica y financiera. La presente iniciativa se inscribe en esa trayectoria de fortalecimiento institucional. No parte de una lógica de ruptura, sino de consolidación. Reconoce lo construido, identifica con precisión un problema cuya magnitud ya es inocultable y propone una respuesta jurídicamente sobria, comparativamente informada y operacionalmente útil (Presidencia de la República, 2021, numeral 4.3, Eje I, objetivo específico 5; Guardia Nacional, 2025, p. 84).

En un país con más de cien millones de personas conectadas, con cientos de millones de operaciones trimestrales de comercio electrónico y con una economía cada vez más integrada a canales digitales, proteger la autenticidad de las transacciones y la confianza de los usuarios no es un asunto marginal. Es una condición del desarrollo. Esta iniciativa busca, precisamente, reforzar esa condición mediante un marco normativo más articulado, más rápido y más eficaz frente a los fraudes por suplantación digital (INEGI, 2025a, pp. 3, 8; CONDUSEF, 2025, p. 179).

Referencias

- Banco de México. (2025). Informe anual sobre las infraestructuras de los mercados financieros 2024.
- Cámara de Diputados del H. Congreso de la Unión. (2025a). Código Nacional de Procedimientos Penales.
- Cámara de Diputados del H. Congreso de la Unión. (2025b). Código Penal Federal.
- Cámara de Diputados del H. Congreso de la Unión. (2025c). Código de Comercio.
- Cámara de Diputados del H. Congreso de la Unión. (2025d). Ley Federal de Protección al Consumidor.

- Cámara de Diputados del H. Congreso de la Unión. (2025e). Ley Federal de Protección a la Propiedad Industrial.
- Cámara de Diputados del H. Congreso de la Unión. (2025f). Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Cámara de Diputados del H. Congreso de la Unión. (2025g). Ley de Sistemas de Pagos.
- Cámara de Diputados del H. Congreso de la Unión. (2025h). *Ley General de Turismo*.
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2023). Fraudes cibernéticos y tradicionales: 4.º trimestre de 2023.
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2025). Informe de autoevaluación enero-junio 2025.
- European Union. (2022). Regulation (EU) 2022/2065 (Digital Services Act).
- Guardia Nacional. (2025). Informe anual de actividades 2024.
- ICANN. (2024). Advisory: Compliance with DNS Abuse obligations in the Registrar Accreditation Agreement and the Registry Agreement.
- Instituto Nacional de Estadística y Geografía. (2025a). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2024: Reporte de resultados.
- Instituto Nacional de Estadística y Geografía. (2025b). Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2025: Reporte de resultados.
- Nacional Cyber Security Centre. (s. f.). Report a scam website; Spot and report scam emails, texts, websites and calls.
- Nominet. (s. f.). Domain Watch.
- Payment Systems Regulator. (2024). Faster Payments APP scams reimbursement requirement.
- Presidencia de la República. (2021). Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024.
- Secretaría de Turismo. (2015). *Reglamento de la Ley General de Turismo*.
- Secretaría de Turismo. (s. f.-a). *Registro Nacional de Turismo: consulta pública de prestadores de servicios turísticos*.
- Secretaría de Turismo. (s. f.-b). *Trámites ante el Registro Nacional de Turismo*.
- Procuraduría Federal del Consumidor. (2021). *Distintivo Digital Profeco*.
- Distintivo Digital PROFECO. (2025). *Padrón de proveedores responsables en comercio electrónico*.
- Quechol Maciel, K., & Aguilar Antonio, J. M. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023). PAAKAT: Revista de Tecnología y Sociedad.

- Alcalá Casillas, M. G. I. M. G. A. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades federativas, delito y bien jurídico tutelado. PAAKAT: Revista de Tecnología y Sociedad.
- Australian Competition and Consumer Commission. (2024). Targeting scams: Report of the National Anti-Scam Centre on scams activity 2023.
- Australian Treasury. (2025). Scams Prevention Framework – Protecting Australians from scams.
- Council of Europe. (2026). Parties/Observers to the Budapest Convention and Observer States to T-CY.
- FBI Internet Crime Complaint Center. (2025). 2024 IC3 Annual Report.

Para mayor referencia, a continuación se integra un cuadro comparativo detallando la propuesta de la presente iniciativa.

Texto vigente	Propuesta
Ley General de Turismo	
Artículo 7. Para el cumplimiento de la presente Ley, corresponde a la Secretaría: … Sin correlativo ….	**Artículo 7.** Para el cumplimiento de la presente Ley, corresponde a la Secretaría: … **XIV Bis. Coordinarse con la Procuraduría Federal del Consumidor y las demás autoridades competentes para la orientación, prevención, atención y canalización de reportes relacionados con la suplantación digital de identidad de prestadores de servicios turísticos;** **XIV Ter. Emitir alertas y recomendaciones al público, en los términos que establezca el Reglamento, cuando existan elementos suficientes sobre medios digitales que aparenten corresponder a prestadores de servicios turísticos y puedan inducir a error o engaño a los turistas;** ….
Artículo 46. El Registro Nacional de Turismo, es el catálogo público de prestadores de servicios turísticos en el país, el cual constituye el mecanismo por el que el Ejecutivo Federal, los Estados, Municipios y	**Artículo 46.** El Registro Nacional de Turismo, es el catálogo público de prestadores de servicios turísticos en el país, el cual constituye el mecanismo por el que el Ejecutivo Federal, los Estados, Municipios y la

la Ciudad de México, podrán contar con información sobre los prestadores de servicios turísticos a nivel nacional, con objeto de conocer mejor el mercado turístico y establecer comunicación con las empresas cuando se requiera. En las disposiciones reglamentarias se establecerán todas aquellas personas físicas y morales obligadas a inscribirse en el Registro Nacional de Turismo.	Ciudad de México, podrán contar con información sobre los prestadores de servicios turísticos a nivel nacional, con objeto de conocer mejor el mercado turístico y establecer comunicación con las empresas cuando se requiera. **Asimismo, constituirá un mecanismo de verificación pública de la identidad y, en su caso, de los medios digitales oficiales de contacto, comercialización y atención de los prestadores de servicios turísticos, en los términos que determinen las disposiciones reglamentarias.** En las disposiciones reglamentarias se establecerán todas aquellas personas físicas y morales obligadas a inscribirse en el Registro Nacional de Turismo.
Artículo 49. El Registro Nacional de Turismo deberá operar bajo el principio de máxima publicidad, por lo que la información contenida o que se desprenda del mismo deberá estar disponible al público en general, en la forma y términos que determine la Secretaría, con excepción de aquellos datos que en términos de la Ley, sean de carácter confidencial.	**Artículo 49.** El Registro Nacional de Turismo deberá operar bajo el principio de máxima publicidad, por lo que la información contenida o que se desprenda del mismo deberá estar disponible al público en general, en la forma y términos que determine la Secretaría, con excepción de aquellos datos que en términos de la Ley, sean de carácter confidencial. **Como medida para prevenir la suplantación digital de identidad corporativa, la información relativa a la identidad del prestador, vigencia de su inscripción y medios digitales oficiales de contacto, comercialización y atención, en su caso, deberá estar disponible al público en general en la forma y términos que determine la Secretaría.**
Artículo 51. La base de datos del Registro Nacional de Turismo quedará bajo la guarda de la Secretaría, siendo responsabilidad de las autoridades de los Estados, Municipios y la Ciudad de México, constatar la veracidad de la información que proporcionen los prestadores de servicios turísticos.	**Artículo 51.** La base de datos del Registro Nacional de Turismo quedará bajo la guarda de la Secretaría, siendo responsabilidad de las autoridades de los Estados, Municipios y la Ciudad de México, constatar la veracidad de la información que proporcionen los prestadores de servicios turísticos, **incluida la relativa a sus medios digitales oficiales, en**

	los términos que determine el Reglamento.
Artículo 58. Son obligaciones de los prestadores de servicios turísticos: .... Sin correlativo	**Artículo 58.** Son obligaciones de los prestadores de servicios turísticos: .... **XII. Identificar de manera clara y verificable sus medios oficiales de contacto, comercialización, reservación, pago y atención al turista, en los términos que determine el Reglamento;** **XIII. Mantener actualizada en el Registro Nacional de Turismo la información relativa a dichos medios oficiales;** **XIV. Dar aviso oportuno a la Secretaría y a las autoridades competentes cuando tengan conocimiento del uso indebido, falsificación o suplantación digital de su identidad comercial que pueda afectar a turistas o usuarios.** **XV. Las demás previstas en éste y otros ordenamientos.**
Artículo 61. Los turistas, con independencia de los derechos que les asisten como consumidores, tendrán en los términos previstos en esta Ley, los siguientes derechos: .... Sin correlativo	**Artículo 61.** Los turistas, con independencia de los derechos que les asisten como consumidores, tendrán en los términos previstos en esta Ley, los siguientes derechos: .... **VIII. Recibir orientación y canalización inmediata ante la autoridad competente cuando sean víctimas o probables víctimas de fraude por suplantación digital vinculada con servicios turísticos.**
Artículo 68. Las infracciones a lo dispuesto en esta Ley, su Reglamento y las Normas Oficiales Mexicanas, así como las derivadas de las quejas de los turistas, serán sancionadas por la Secretaría, para lo cual deberá iniciar y resolver el procedimiento	**Artículo 68.** Las infracciones a lo dispuesto en esta Ley, su Reglamento y las Normas Oficiales Mexicanas, así como las derivadas de las quejas de los turistas, serán sancionadas por la Secretaría, para lo cual deberá iniciar y resolver el procedimiento

administrativo de infracción, de conformidad con lo dispuesto en la Ley, su reglamento y la Ley Federal del Procedimiento Administrativo. ...	administrativo de infracción, de conformidad con lo dispuesto en la Ley, su reglamento y la Ley Federal del Procedimiento Administrativo. ... **Cuando la queja o denuncia presentada verse sobre probable suplantación digital de identidad de un prestador de servicios turísticos, o sobre medios digitales que aparenten corresponderle, la Secretaría podrá requerir información al prestador, emitir alertas preventivas al público y dar vista inmediata a las autoridades competentes, en términos de las disposiciones aplicables.**
Artículo 69. Los prestadores que no se inscriban en el Registro Nacional de Turismo en los plazos señalados por esta Ley, serán sancionados con multa que podrá ir de quinientas hasta mil quinientas veces de la Unidad de Medida y Actualización, vigente al momento en que se cometa la violación.	**Artículo 69.** Los prestadores que no se inscriban en el Registro Nacional de Turismo en los plazos señalados por esta Ley, serán sancionados con multa que podrá ir de quinientas hasta mil quinientas veces de la Unidad de Medida y Actualización, vigente al momento en que se cometa la violación. ... **Los prestadores de servicios turísticos que omitan registrar, actualizar o corregir la información relativa a sus medios digitales oficiales en el Registro Nacional de Turismo, o proporcionen información inexacta sobre éstos, serán requeridos para que en un término de cinco días hábiles subsanen la omisión o corrijan la información. En caso de incumplimiento, se harán acreedores a una multa de doscientas a quinientas veces el valor diario de la Unidad de Medida y Actualización.**
Ley Federal de Protección al Consumidor	
ARTÍCULO 76 BIS.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de	**ARTÍCULO 76 BIS.**- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de

medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente: I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; ...	medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente: I. El proveedor utilizará la información proporciona da por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; ... **VIII. El proveedor deberá identificar de manera clara sus canales oficiales de contratación y pago, y abstenerse de inducir a error respecto de su identidad o la autenticidad de los medios electrónicos utilizados.**
Sin correlativo	**ARTÍCULO 76 BIS 2.-** Intermediación digital. Cuando, para la realización de transacciones con consumidores, intervenga un tercero que, de manera directa o indirecta, facilite la promoción, contratación, cobro, o canalización hacia un proveedor mediante medios electrónicos, ópticos o cualquier otra tecnología, dicho tercero será considerado intermediario digital para efectos de este Capítulo y estará obligado a: I. Implementar medidas razonables y proporcionales para verificar la identidad y medios de contacto del proveedor que utilice sus servicios para ofertar o contratar con consumidores, y mantenerlos actualizados; II. Establecer mecanismos accesibles para la recepción de reportes de posibles suplantaciones, sitios apócrifos o prácticas

	engañosas, así como un procedimiento de atención expedita; III. Adoptar medidas de conservación inmediata de registros y datos vinculados con la oferta, contratación, pagos y comunicaciones relativas a la transacción, cuando medie solicitud de autoridad competente en términos de la legislación aplicable; IV. Colaborar con las autoridades competentes en la identificación y mitigación de prácticas que puedan inducir a error o engaño al consumidor, en los términos de esta Ley y demás disposiciones aplicables. La Procuraduría podrá emitir criterios de carácter general para la aplicación del presente artículo, atendiendo a un enfoque basado en riesgos y a la protección de la población vulnerable.
Código Penal Federal	
Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán: I.- Al que obtenga dinero, valores o cualquiera otra cosa ofreciendo encargarse de la defensa de un procesado o de un reo, o de la dirección o patrocinio en un asunto civil o administrativo, si no efectúa aquélla o no realiza ésta, sea porque no se haga cargo legalmente de la misma, o porque renuncie o abandone el negocio o la causa sin motivo justificado; ...	**Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán: I.- Al que obtenga dinero, valores o cualquiera otra cosa ofreciendo encargarse de la defensa de un procesado o de un reo, o de la dirección o patrocinio en un asunto civil o administrativo, si no efectúa aquélla o no realiza ésta, sea porque no se haga cargo legalmente de la misma, o porque renuncie o abandone el negocio o la causa sin motivo justificado; ... **XXII.- A quien, para procurarse ilícitamente un bien u obtener un lucro indebido, mediante el uso de sitios web,**

	aplicaciones, nombres de dominio, perfiles digitales o cualquier medio tecnológico, suplante o haga aparecer como propia la identidad comercial o institucional de un tercero, induciendo a error al consumidor o usuario para la realización de pagos, transferencias o entrega de datos.
Código Nacional de Procedimientos Penales	
Sin correlativo	**Artículo 303 Bis.** Conservación y entrega de datos por intermediarios digitales y prestadores de servicios tecnológicos. Cuando el Ministerio Público considere necesaria la conservación inmediata o la entrega de datos vinculados con hechos que se investigan y que obren en poder de prestadores de servicios de alojamiento digital, nombres de dominio, servicios de aplicaciones y contenidos, plataformas de intermediación o publicidad digital, o proveedores de servicios tecnológicos análogos, el Procurador o el servidor público en quien se delegue la facultad podrá solicitar al Juez de control que requiera la conservación y, en su caso, la entrega de dichos datos con la oportunidad y suficiencia necesaria. El Juez de control, cuando sea estrictamente necesario para impedir la continuación de la conducta delictiva o evitar un daño inminente a víctimas, podrá autorizar de manera temporal y proporcional la suspensión provisional del acceso o disponibilidad del recurso digital identificado, garantizando mecanismos de revisión y contradicción.

	Excepcionalmente, cuando exista riesgo de pérdida inminente de evidencia o continuación del daño, el Procurador, bajo su más estricta responsabilidad, podrá requerir la conservación inmediata por un plazo breve, debiendo informar al Juez de control dentro de cuarenta y ocho horas para su ratificación; de no ratificarse, la información no podrá incorporarse al procedimiento.
Ley de Sistemas de Pagos	
Artículo 6o. Las Normas Internas de cualquier Sistema de Pagos deberán propiciar su eficiencia y seguridad, así como el desarrollo competitivo de los servicios que se presten utilizando el citado Sistema de Pagos. Asimismo, las Normas Internas deberán sujetarse a la autorización del Banco de México y a las disposiciones de carácter general que, en su caso, este último emita. En todo caso, las Normas Internas, por lo que se refiere a las de adhesión y funcionamiento o a los manuales, según corresponda, deberán prever cuando menos: I. El momento en que las Órdenes de Transferencia enviadas al Sistema de Pagos de que se trate se consideren Órdenes de Transferencia Aceptadas; ...	**Artículo 6o.** Las Normas Internas de cualquier Sistema de Pagos deberán propiciar su eficiencia y seguridad, así como el desarrollo competitivo de los servicios que se presten utilizando el citado Sistema de Pagos. Asimismo, las Normas Internas deberán sujetarse a la autorización del Banco de México y a las disposiciones de carácter general que, en su caso, este último emita. En todo caso, las Normas Internas, por lo que se refiere a las de adhesión y funcionamiento o a los manuales, según corresponda, deberán prever cuando menos: I. El momento en que las Órdenes de Transferencia enviadas al Sistema de Pagos de que se trate se consideren Órdenes de Transferencia Aceptadas; ... **VIII. Mecanismos de prevención, detección, contención y atención de fraudes inducidos por engaño o suplantación digital en las órdenes de transferencia, incluyendo medidas de verificación y acciones correctivas para reducir riesgos, en términos de las disposiciones de**

	carácter general y de las autorizaciones que, en su caso, emita el Banco de México.

DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DE LA LEY GENERAL DE TURISMO, LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, CÓDIGO PENAL FEDERAL, CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES Y LEY DE SISTEMA DE PAGOS EN MATERIA DE PREVENCIÓN Y RESPUESTA RÁPIDA FRENTE A PÁGINAS FALSAS Y FRAUDES EN RESERVAS DE HOSPEDAJE Y PAQUETES VACACIONALES A CARGO DEL SENADOR EUGENIO SEGURA VÁZQUEZ, DEL GRUPO PARLAMENTARIO DE MORENA

ARTÍCULO PRIMERO. Se adicionan la fracción XIV Bis y XIV Ter del artículo 7; un párrafo al artículo 46; un párrafo al artículo 49; una oración al artículo 51; las fracciones XII, XIII, XIV y XV del artículo 58; la fracción VIII del artículo 61 y un párrafo al artículo 69.

Ley General de Turismo

Artículo 7. Para el cumplimiento de la presente Ley, corresponde a la Secretaría:

...

XIV Bis. Coordinarse con la Procuraduría Federal del Consumidor y las demás autoridades competentes para la orientación, prevención, atención y canalización de reportes relacionados con la suplantación digital de identidad de prestadores de servicios turísticos;

XIV Ter. Emitir alertas y recomendaciones al público, en los términos que establezca el Reglamento, cuando existan elementos suficientes sobre medios digitales que aparenten corresponder a prestadores de servicios turísticos y puedan inducir a error o engaño a los turistas;

....

Artículo 46. El Registro Nacional de Turismo, es el catálogo público de prestadores de servicios turísticos en el país, el cual constituye el mecanismo por el que el Ejecutivo Federal, los Estados, Municipios y la Ciudad de México, podrán contar con información sobre los prestadores de servicios turísticos a nivel nacional, con objeto de conocer mejor el mercado turístico y establecer comunicación con las empresas cuando se requiera.

Asimismo, constituirá un mecanismo de verificación pública de la identidad y, en su caso, de los medios digitales oficiales de contacto, comercialización y atención de los prestadores de servicios turísticos, en los términos que determinen las disposiciones reglamentarias.

En las disposiciones reglamentarias se establecerán todas aquellas personas físicas y morales obligadas a inscribirse en el Registro Nacional de Turismo.

Artículo 49. El Registro Nacional de Turismo deberá operar bajo el principio de máxima publicidad, por lo que la información contenida o que se desprenda del mismo deberá estar disponible al público en general, en la forma y términos que determine la Secretaría, con excepción de aquellos datos que en términos de la Ley, sean de carácter confidencial.

Como medida para prevenir la suplantación digital de identidad corporativa, la información relativa a la identidad del prestador, vigencia de su inscripción y medios digitales oficiales de contacto, comercialización y atención, en su caso, deberá estar disponible al público en general en la forma y términos que determine la Secretaría.

Artículo 51. La base de datos del Registro Nacional de Turismo quedará bajo la guarda de la Secretaría, siendo responsabilidad de las autoridades de los Estados, Municipios y la Ciudad de México, constatar la veracidad de la información que proporcionen los prestadores de servicios turísticos, **incluida la relativa a sus medios digitales oficiales, en los términos que determine el Reglamento.**

Artículo 58. Son obligaciones de los prestadores de servicios turísticos:

....

XII. Identificar de manera clara y verificable sus medios oficiales de contacto, comercialización, reservación, pago y atención al turista, en los términos que determine el Reglamento;

XIII. Mantener actualizada en el Registro Nacional de Turismo la información relativa a dichos medios oficiales;

XIV. Dar aviso oportuno a la Secretaría y a las autoridades competentes cuando tengan conocimiento del uso indebido, falsificación o suplantación digital de su identidad comercial que pueda afectar a turistas o usuarios.

XV. Las demás previstas en éste y otros ordenamientos.

Artículo 61. Los turistas, con independencia de los derechos que les asisten como consumidores, tendrán en los términos previstos en esta Ley, los siguientes derechos:

....

VIII. Recibir orientación y canalización inmediata ante la autoridad competente cuando sean víctimas o probables víctimas de fraude por suplantación digital vinculada con servicios turísticos.

Artículo 68. Las infracciones a lo dispuesto en esta Ley, su Reglamento y las Normas Oficiales Mexicanas, así como las derivadas de las quejas de los turistas, serán sancionadas por la Secretaría, para lo cual deberá iniciar y resolver el procedimiento administrativo de infracción, de conformidad con lo dispuesto en la Ley, su reglamento y la Ley Federal del Procedimiento Administrativo.

...

Cuando la queja o denuncia presentada verse sobre probable suplantación digital de identidad de un prestador de servicios turísticos, o sobre medios digitales que aparenten corresponderle, la Secretaría podrá requerir información al prestador, emitir alertas preventivas al público y dar vista inmediata a las autoridades competentes, en términos de las disposiciones aplicables.

Artículo 69. Los prestadores que no se inscriban en el Registro Nacional de Turismo en los plazos señalados por esta Ley, serán sancionados con multa que podrá ir de quinientas hasta mil quinientas veces de la Unidad de Medida y Actualización, vigente al momento en que se cometa la violación.

...

Los prestadores de servicios turísticos que omitan registrar, actualizar o corregir la información relativa a sus medios digitales oficiales en el Registro Nacional de Turismo, o proporcionen información inexacta sobre éstos, serán requeridos para que en un término de cinco días hábiles subsanen la omisión o corrijan la información. En caso de incumplimiento, se harán acreedores a una multa de doscientas a quinientas veces el valor diario de la Unidad de Medida y Actualización.

ARTÍCULO SEGUNDO. Se adiciona la fracción VIII del artículo 76 Bis y se adiciona el artículo 76 Bis 2, ambos de la Ley Federal de Protección al Consumidor para quedar como siguen:

Ley Federal de Protección al Consumidor

...

ARTÍCULO 76 BIS.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

...

VIII. El proveedor deberá identificar de manera clara sus canales oficiales de contratación y pago, y abstenerse de inducir a error respecto de su identidad o la autenticidad de los medios electrónicos utilizados.

ARTÍCULO 76 BIS 2.- Intermediación digital. Cuando, para la realización de transacciones con consumidores, intervenga un tercero que, de manera directa o indirecta, facilite la promoción, contratación, cobro, o canalización hacia un proveedor mediante medios electrónicos, ópticos o cualquier otra tecnología, dicho tercero será considerado intermediario digital para efectos de este Capítulo y estará obligado a:

I. Implementar medidas razonables y proporcionales para verificar la identidad y medios de contacto del proveedor que utilice sus servicios para ofertar o contratar con consumidores, y mantenerlos actualizados;

II. Establecer mecanismos accesibles para la recepción de reportes de posibles suplantaciones, sitios apócrifos o prácticas engañosas, así como un procedimiento de atención expedita;

III. Adoptar medidas de conservación inmediata de registros y datos vinculados con la oferta, contratación, pagos y comunicaciones relativas a la transacción, cuando medie solicitud de autoridad competente en términos de la legislación aplicable;

IV. Colaborar con las autoridades competentes en la identificación y mitigación de prácticas que puedan inducir a error o engaño al consumidor, en los términos de esta Ley y demás disposiciones aplicables.

La Procuraduría podrá emitir criterios de carácter general para la aplicación del presente artículo, atendiendo a un enfoque basado en riesgos y a la protección de la población vulnerable.

ARTÍCULO TERCERO. Se adiciona la fracción XXII al artículo 387 del Código Penal Federal para quedar como sigue:

Código Penal Federal

...

Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

I.- Al que obtenga dinero, valores o cualquiera otra cosa ofreciendo encargarse de la defensa de un procesado o de un reo, o de la dirección o patrocinio en un asunto civil o administrativo, si no efectúa aquélla o no realiza ésta, sea porque no se haga cargo legalmente de la misma, o porque renuncie o abandone el negocio o la causa sin motivo justificado;

...

XXII.- A quien, para procurarse ilícitamente un bien u obtener un lucro indebido, mediante el uso de sitios web, aplicaciones, nombres de dominio, perfiles digitales o cualquier medio tecnológico, suplante o haga aparecer como propia la identidad comercial o institucional de un tercero, induciendo a error al consumidor o usuario para la realización de pagos, transferencias o entrega de datos.

ARTÍCULO CUARTO. Se adiciona el artículo 303 Bis del Código Nacional de Procedimientos Penales para quedar como sigue:

Código Nacional de Procedimientos Penales

...

Artículo 303 Bis. Conservación y entrega de datos por intermediarios digitales y prestadores de servicios tecnológicos.

Cuando el Ministerio Público considere necesaria la conservación inmediata o la entrega de datos vinculados con hechos que se investigan y que obren en poder de prestadores de servicios de alojamiento digital, nombres de dominio, servicios de aplicaciones y contenidos, plataformas de intermediación o publicidad digital, o proveedores de servicios tecnológicos análogos, el Procurador o el servidor público en quien se delegue la facultad podrá solicitar al Juez de control que requiera la conservación y, en su caso, la entrega de dichos datos con la oportunidad y suficiencia necesaria.

El Juez de control, cuando sea estrictamente necesario para impedir la continuación de la conducta delictiva o evitar un daño inminente a víctimas, podrá autorizar de manera temporal y proporcional la suspensión provisional del acceso o disponibilidad del recurso digital identificado, garantizando mecanismos de revisión y contradicción.

Excepcionalmente, cuando exista riesgo de pérdida inminente de evidencia o continuación del daño, el Procurador, bajo su más estricta responsabilidad, podrá requerir la conservación inmediata por un plazo breve, debiendo informar al Juez de control dentro de cuarenta y ocho horas para su ratificación; de no ratificarse, la información no podrá incorporarse al procedimiento.

ARTÍCULO QUINTO. Se adiciona la fracción VIII del artículo 6 de la Ley de Sistemas de Pagos para quedar como sigue:

Ley de Sistemas de Pagos

...

Artículo 6o. Las Normas Internas de cualquier Sistema de Pagos deberán propiciar su eficiencia y seguridad, así como el desarrollo competitivo de los servicios que se presten utilizando el citado Sistema de Pagos. Asimismo, las Normas Internas deberán sujetarse a la autorización del Banco de México y a las disposiciones de carácter general que, en su caso, este último emita.

En todo caso, las Normas Internas, por lo que se refiere a las de adhesión y funcionamiento o a los manuales, según corresponda, deberán prever cuando menos:

I. El momento en que las Órdenes de Transferencia enviadas al Sistema de Pagos de que se trate se consideren Órdenes de Transferencia Aceptadas;

...

VIII. Mecanismos de prevención, detección, contención y atención de fraudes inducidos por engaño o suplantación digital en las órdenes de transferencia, incluyendo medidas de verificación y acciones correctivas para reducir riesgos, en términos de las disposiciones de carácter general y de las autorizaciones que, en su caso, emita el Banco de México.

ARTÍCULOS TRANSITORIOS

Primero. El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo. Dentro de los 180 días naturales siguientes a la entrada en vigor, el Banco de México emitirá, en el ámbito de sus atribuciones y conforme a la Ley de Sistemas de Pagos, los ajustes regulatorios necesarios para incorporar en las

Normas Internas de los sistemas de pagos los mecanismos referidos en la fracción VIII del artículo 6o. incluyendo lineamientos basados en riesgos.

Tercero. Dentro de los 120 días naturales, la Procuraduría Federal del Consumidor, en coordinación con la Guardia Nacional y las instancias competentes, pondrá en operación un mecanismo de recepción de reportes y canalización expedita para mitigación de sitios apócrifos y preservación de evidencia, con lineamientos públicos de atención.

Cuarto. La autoridad financiera supervisora, en coordinación con las entidades financieras, continuará fortaleciendo medidas de control de riesgos para operaciones digitales en el marco de sus disposiciones aplicables.

Quinto. El Ejecutivo Federal dentro de los 180 días naturales siguientes a la entrada en vigor del presente Decreto, deberá adecuar el Reglamento de la Ley General de Turismo para materializar las disposiciones del presente decreto.

Sexto. La Secretaría de Turismo, dentro de los 180 días naturales siguientes a la entrada en vigor del presente Decreto, deberá adecuar la estructura operativa y tecnológica del Registro Nacional de Turismo a efecto de incorporar la información relativa a los medios digitales oficiales de contacto, comercialización, reservación, pago y atención al turista, así como los mecanismos de consulta pública que resulten procedentes.

Séptimo. Los prestadores de servicios turísticos inscritos en el Registro Nacional de Turismo contarán con un plazo de ciento ochenta días naturales, contados a partir de que entren en vigor las adecuaciones reglamentarias correspondientes, para registrar o actualizar la información relativa a sus medios digitales oficiales.

Suscribe.

Senador Eugenio Segura Vázquez
Integrante del Grupo Parlamentario de MORENA

A 08 de abril de 2026.