

CONTENIDO

Iniciativas

- 2** Que reforma el párrafo décimo del artículo 4o., el párrafo tercero del artículo 6o. y el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en materia de reconocimiento y protección de la identidad digital, a cargo de la diputada Karina Margarita del Río Zenteno, del Grupo Parlamentario de Morena
- 45** Que reforma el artículo 20 de la Constitución Política de los Estados Unidos Mexicanos, en materia de delitos de índole sexual en niñas, niños o adolescentes para que en la recepción del testimonio de la víctima pueda usarse herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales, a cargo de la diputada Olga Leticia Chávez Rojas, del Grupo Parlamentario de Morena
- 57** Que adiciona un Capítulo VIII Bis, denominado “Del uso Responsable de Sistemas de Inteligencia Artificial en los Servicios Consulares”, integrado por los artículos 46 Bis, 46 Ter, 46 Quáter, 46 Quinquies, 46 Sexies, 46 Septies, 46 Octies, 46 Nonies y 46 Decies, a la Ley del Servicio Exterior Mexicano, a cargo de la diputada Giselle Yunueen Arellano Ávila, del Grupo Parlamentario de Morena
- 121** Que reforma la denominación del Capítulo II del Título Noveno y adiciona una fracción XVII al apartado a del artículo 11 Bis y los artículos 211 Bis 8 a 211 Bis 14 al Código Penal Federal, en materia de tipificación de ciberataques y delitos informáticos, en armonización con los estándares internacionales en la materia, a cargo de la diputada Giselle Yunueen Arellano Ávila, del Grupo Parlamentario de Morena
- 149** Que adiciona una fracción V Ter al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente, en materia de definición de la ciencia ciudadana, en armonización con los estándares internacionales de ciencia abierta, a cargo de la diputada Giselle Yunueen Arellano Ávila, del Grupo Parlamentario de Morena
- 171** Que reforma y adiciona diversas disposiciones de la Ley Federal de Protección al Consumidor, en materia de disponibilidad obligatoria de refacciones, a cargo de la diputada Rocío Adriana Abreu Artiñano, del Grupo Parlamentario de Morena

Anexo II-1-5

Iniciativa con Proyecto de Decreto que reforma el párrafo décimo del artículo 4º, el párrafo tercero del artículo 6º y el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en materia de reconocimiento y protección de la identidad digital.

Karina Margarita Del Río Zenteno, Diputada Federal integrante del Grupo Parlamentario de Morena, en la LXVI Legislatura, con fundamento en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 6, numeral 1, fracción I, 77, 78 y 82 numeral 2 fracción I del Reglamento de la Cámara de Diputados, someto a consideración del pleno de esta asamblea la presente iniciativa de decreto al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

I) CONTEXTO

El derecho a la identidad es un derecho humano reconocido en diversos instrumentos internacionales. En México el concepto de identidad fue reconocido como derecho humano mediante una reforma al artículo 4º Constitución Política de los Estado Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 17 de junio de 2014.¹

Quedando establecido que toda persona tiene derecho a la identidad y a ser registrado gratuitamente de manera inmediata a su nacimiento y señala la obligación del estado mexicano de garantizar el cumplimiento de estos derechos:

“Artículo 4o. ...

Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos

¹ Diario Oficial de la Federación. Martes 17 de junio de 2014. Decreto por el que se adiciona el artículo 4o. de la Constitución Política de los Estados Unidos Mexicanos.
https://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_217_17jun14.pdf

derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento.”

El derecho al nombre propio, a la personalidad jurídica, a la nacionalidad y por ende **a la identidad**, constituye el derecho primigenio que se convierte de manera automática en la llave de acceso a otros derechos esenciales como el derecho a la salud, a la educación, a la protección y a la inclusión en la vida económica, cultural y política del país para cualquier persona.

El derecho a la identidad como todo derecho humano, es universal, no puede tener caducidad, es único, irrenunciable, intransferible e indivisible.

En este contexto, la reivindicación de la dignidad de las personas y el pleno respeto a sus derechos humanos y, dentro de este marco, el **derecho a la identidad** a fin de que este derecho se convierta verdaderamente en la puerta de acceso a todos los demás derechos.

El Derecho a la Identidad tiene dos pilares fundamentales para su ejercicio: la identidad jurídica y la identidad biométrica, ligadas a través del identificador único que es la CURP, y así garantizar su unicidad, sin la cual no hay identidad.²

La identidad jurídica de las personas la garantizan tanto el gobierno federal como los gobiernos de las 32 entidades federativas, quienes a través de sus Registros Civiles. El reconocimiento a través del registro de nacimiento permite, además de adquirir una identidad, un nombre y una nacionalidad, acceder a un conjunto de derechos humanos reconocidos en la legislación de un país.

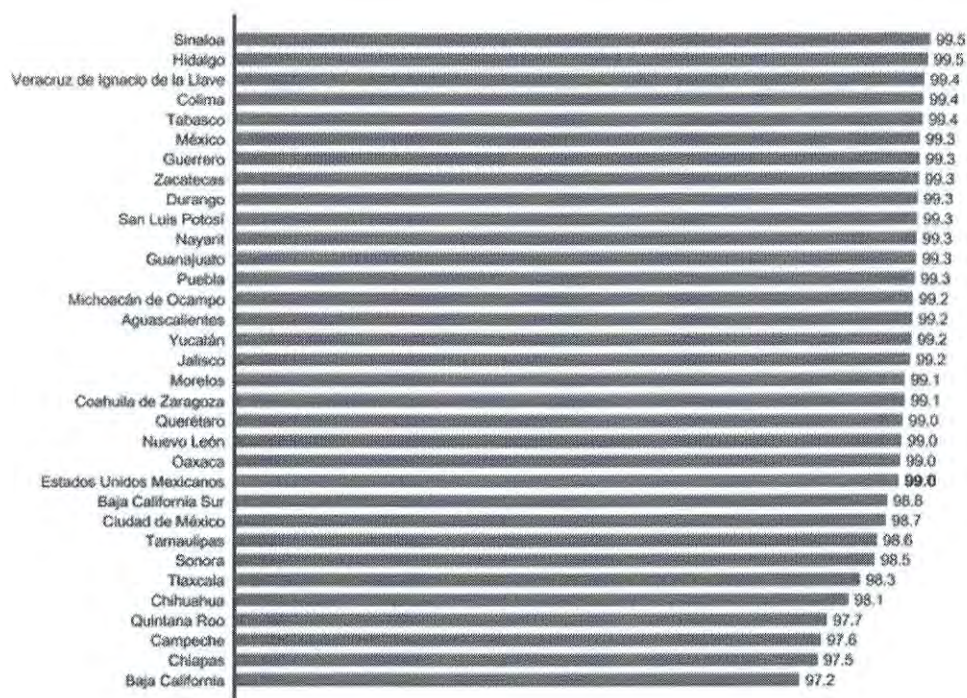
² Gobierno de México. Derecho a la identidad, la puerta de acceso a tus derechos.
<https://www.gob.mx/segob/%7Crenapo/acciones-y-programas/derecho-a-la-identidad-la-puerta-de-acceso-a-tus-derechos>

Con la información del Cuestionario Ampliado del Censo 2020, se estima que en México 99.0% del total de la población ha sido registrada.³ Por otra parte, se estima que los estados donde la población presenta el mayor porcentaje de registro de nacimiento son: Sinaloa e Hidalgo con 99.5%, seguidas por Veracruz de Ignacio de Llave, Colima y Tabasco con 99.4% cada uno. En contraste, las entidades federativas con el menor porcentaje de población registrada son: Campeche, Chiapas y Baja California con 97.6, 97.5 y 97.2% respectivamente.⁴ Tal y como se muestra en la siguiente tabla:



Censo de Población y Vivienda
2020

PORCENTAJE DE POBLACIÓN CON REGISTRO DE NACIMIENTO EN EL PAÍS POR ENTIDAD FEDERATIVA



Fuente: INEGI, Censo de Población y Vivienda 2020, Cuestionario Ampliado.

³ INEGI. Principales resultados del Censo de Población y Vivienda 2020 Estados Unidos Mexicanos.
https://www.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estru_c/702825198060.pdf

⁴ Ibid.

Actualmente, México no cuenta con una base de datos que vincule la identidad jurídica y la biométrica de toda la población, lo que impide vincular y proteger la identidad legal y la identidad digital, lo cual facilita el robo de identidad, el fraude y la inseguridad.

Sin embargo, el desarrollo de la tecnología nos ha llevado a una realidad inesperada: el **mundo digital**. En el siglo XXI, la vida humana se desarrolla de manera indisoluble entre el entorno físico y el entorno digital. Las interacciones sociales, las transacciones económicas, el acceso a servicios públicos y el ejercicio de derechos fundamentales ocurren cada vez más en el ciberespacio. En este contexto, ha surgido una nueva dimensión de la personalidad jurídica: la **identidad digital**.

La Identidad Digital se ha convertido en una forma de extensión de la persona que no se limita a las credenciales de acceso o contraseñas; abarca la huella digital, los datos biométricos, el historial de navegación, el comportamiento en línea y el perfilamiento algorítmico que terceros realizan sobre los individuos.

Actualmente, nuestra Constitución reconoce el derecho a la protección de datos personales y los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), pero el marco resulta insuficiente frente a la minería de datos masiva (Big Data), la inteligencia artificial y el robo de identidad en plataformas tecnológicas.

Es decir, tenemos la identidad legal como un derecho humano básico que garantiza el reconocimiento oficial de una persona mediante atributos como el nombre, la filiación y la nacionalidad. Por su parte, la identidad digital es la proyección y el conjunto de datos de esa misma persona en el entorno virtual.

- Ambos conceptos buscan salvaguardar el valor de la persona, garantizando que sea reconocida de forma justa y sin sufrir engaños o ataques a su imagen.

- Los dos se apoyan en normativas de derechos humanos y leyes de protección de datos para evitar abusos por parte de terceros o de empresas tecnológicas.

Sin embargo, existen amplias diferencias:

1. El derecho a la identidad opera principalmente en el mundo físico y legal tradicional, mientras que la identidad digital vive en redes, bases de datos y plataformas de internet.
2. Los atributos esenciales de la identidad tradicional son otorgados e inscritos por el Estado, como el acta de nacimiento, en cambio, la identidad digital suele construirse mediante acciones del usuario, publicaciones y rastros informáticos que a veces escapan a su control total.
3. La identidad legal se compone de datos fijos y formales, mientras que la identidad digital incluye datos de comportamiento, historiales de navegación, perfiles y reputación en línea.

Diversos análisis jurídicos y académicos, como los trabajos sobre el Derecho a la identidad digital publicados en normativas europeas y iberoamericanas, discuten cómo extender los principios tradicionales de la personalidad hacia el ecosistema de algoritmos y redes. Asimismo, autores como Stefano Rodotà han estudiado la identidad como un reflejo dinámico frente a los nuevos retos tecnológicos.

En México, el marco legal que divide y entrelaza el derecho a la identidad y la identidad digital se encuentra en una etapa de profunda transformación. Mientras que el primero está consolidado constitucionalmente, el segundo se construye a través de reformas recientes y nuevas agencias gubernamentales.

Cabe señalar que la Presidenta de la República, la Doctora Claudia Sheiubbaum Pardo, en su primer informe de gobierno, se refirió específicamente a **identidad digital** y señaló:

“Crear la Identidad Digital Nacional”⁵

Con el objetivo de garantizar plenamente el derecho a la identidad, se impulsó la iniciativa de integrar datos biométricos a la Clave Única de Registro de Población (CURP),⁶ transformándola en un documento de identidad digital nacional capaz de reconocer de forma única e inequívoca a cada persona. Este documento contará con dos modalidades: física y digital. Entre enero⁷ y junio de 2025 se realizaron diversas acciones, de las cuales se destacan las siguientes:

- Hasta el 30 de junio de 2025, las distintas instituciones del Gobierno Federal responsables de recabar datos biométricos, reportaron aproximadamente 29 millones de registros con fotografía y huellas dactilares. Adicionalmente, 25 millones de registros incluyen fotografías, mientras que 76 millones de personas no tienen registro con biométricos.
- Para agilizar la incorporación de datos biométricos a la CURP, se implementará un programa de enrolamiento en todos los estados del país, coordinado por el Registro Nacional de Población (RENAPO). En una primera etapa, está prevista la adquisición de al menos 4 mil kits de enrolamiento, con la proyección de incrementar la capacidad hasta 8 mil kits en fases posteriores. Además, se sumarán a la estrategia de enrolamiento la Secretaría del Bienestar.
- Hasta el momento se ha alcanzado un registro de más de 8.8 millones de usuarios en la Llave MX, que facilita el acceso a los servicios de inscripción

⁵ 1er. Informe de Gobierno. 2024- 2025. Página 234 – 235.

https://www.informegobierno.gob.mx/usercontent/68b4162a4d926-11G-INFORME-INTEGRADO-FINAL_26_08_2025

⁶ Este documento contará con dos modalidades: física y digital. En su versión digital, podrá obtenerse a través de la aplicación APP MX (la cual está siendo desarrollada por la misma Agencia). El proceso consistirá en ingresar la CURP para realizar una búsqueda en los registros oficiales que contengan datos biométricos. En caso de localizar un registro, se solicitará una prueba de vida para verificar la identidad de la persona y asociar su CURP Identidad. La aplicación opera con altos estándares de seguridad y validación, garantizando la protección de los datos personales de la ciudadanía. Esta aplicación servirá como un mecanismo de autenticación que unificará el acceso a diversos servicios gubernamentales en una primera etapa y privados una vez que su adopción y maduración lo permita. Todo el procedimiento se realizará con el consentimiento expreso del titular, incluyendo la autorización para transferir los datos biométricos al RENAPO, cuando estos se encuentren en una base distinta a la de dicha Institución.

⁷ La Reforma a la Ley Orgánica de la APF, publicada el 28 de noviembre de 2024 en el DOF, creó la Agencia de Transformación Digital y Telecomunicaciones, que inició actividades el 1 de enero de 2025.

a Programas del Bienestar; emisión de documentos oficiales; realización de trámites de manera digital como son la apertura de negocios.

- Gracias a este mecanismo digital que interopera en 67 sistemas o plataformas web del Gobierno de México, virtualmente se pudieron gestionar los siguientes apoyos y servicios públicos:

1. Registro de candidaturas para elección del Poder Judicial, proyecto en el que 25,689 aspirantes se inscribieron, de los cuales 18,447 fueron considerados elegibles;

2. Registro de poco más de 5 millones de madres, padres y tutores de estudiantes de nivel básico para solicitar la Beca Universal de Educación Básica “Rita Cetina”; 3. Cerca de 1.5 millones de estudiantes de educación media superior utilizaron Llave MX para solicitar la “Nueva Beca Universal Benito Juárez” y;

4. Alrededor de medio millón de madres, padres y tutores del estado de Oaxaca pudieron generar el “Registro para la entrega de apoyos para uniformes” a estudiantes de nivel básico.

Modelo Nacional de Simplificación y Digitalización de Trámites Administrativos

A fin de habilitar el Modelo de Nacional de Simplificación y Digitalización, se presentó ante la Cámara de Senadores el proyecto de Decreto por el que expide la Ley Nacional para Eliminar Trámites Burocráticos, con el objetivo de establecer herramientas, instrumentos y acciones de observancia obligatoria para las autoridades de los tres órdenes de gobierno a fin de facilitar el acceso y obtención de trámites y servicios.

- En este sentido, y derivado de los trabajos realizados en materia de simplificación, con el propósito de disminuir trámites, requisitos y tiempo de resolución, al 30 de junio de 2025 se presentaron propuestas de simplificación de 965 trámites de 42 autoridades de la Administración Pública Federal, de los cuales 579 ya fueron simplificados mediante instrumentos

jurídicos publicados en el Diario Oficial de la Federación. Dando como resultado los siguientes logros:

A. Se eliminó un 57% de los trámites.

B. Se redujo un 57% de requisitos solicitados.

C. Se redujo un 40% el tiempo máximo de resolución de los trámites.

- Asimismo, se desarrolló la primera etapa de la Ventanilla Digital Nacional de Inversiones, a través de la cual las personas empresarias pueden realizar un cuestionario para conocer los trámites, requisitos, tiempo de resolución y autoridad responsable de los tres órdenes de gobierno, necesarios para constituir, construir y operar una empresa en México. Desde su publicación, el 21 de abril de 2025, y hasta el 10 de junio, la ventanilla ha contado con más de 10 mil usuarios activos, de 45 países distintos.*

- Fue desarrollado un nuevo Portal de Turismo con un modelo de inteligencia artificial para fomentar el turismo mexicano, brindando, conforme a las necesidades de cada persona, destinos turísticos, actividades y eventos por cada Entidad Federativa. Desde el 26 de abril de 2025, fecha de su lanzamiento, y hasta el 10 de junio, la página ha sido visitada por más de 72 mil usuarios activos.*

- Se realizó una colaboración con diferentes Secretarías de Estado con el objetivo de mapear y simplificar procesos, así como diseñar interfaces gráficas y generar pruebas digitales para el desarrollo y modernización de ventanillas de trámites. Entre los proyectos destacados se encuentran la Ventanilla Digital CONAGUA y la Renovación del Portal Mi Consulado.*

- Con el fin de eliminar la corrupción y reducir la evasión fiscal, se puso en marcha un nuevo semáforo de inteligencia aduanera en coordinación con la Secretaría de Hacienda y Crédito Público y la Agencia Nacional de Aduanas de México, el cual aumenta la precisión del semáforo mejorando la detección de patrones de riesgo de contrabando y evasión, lo cual permite reducir el contrabando técnico y la subvaluación de mercancías aumentando así la recaudación fiscal.”*

Cabe señalar que a pesar de los enormes esfuerzos gubernamentales que se han

realizado para “*Crear la Identidad Digital Nacional*”, hasta el momento, en legislación vigente aún no se ha reconocido ni protegido el derecho a la identidad digital. De ahí la importancia de la iniciativa que se presenta para establecer a nivel Constitucional, el derecho a la identidad digital, así como la consecuente tutela y salvaguarda.

Para ilustrar la necesidad de legislar en la materia de identidad digital, el estudio denominado “*Desarrollo e implementación de procesos de identificación digital en los países de América Latina*”⁸, elaborado por el Banco Interamericano de Desarrollo, de febrero de 2026, entre otros puntos, señala que:

“A nivel internacional, la identificación digital ha experimentado un desarrollo significativo, ofreciendo experiencias y aprendizajes valiosos para la región. La implementación exitosa de estos sistemas se ha basado en la existencia de condiciones previas robustas, como marcos legales sólidos, una infraestructura de tecnología de la información bien desarrollada y una alta penetración de internet. Por otro lado, el desarrollo de medidas de seguridad y un diseño pensado en el usuario promueve la confianza de estos. Asimismo, la interoperabilidad surge como un patrón claro en estos casos de éxito. Otro aspecto destacado es el modelo federado adoptado por algunos de estos países, donde diferentes entidades gubernamentales y privadas pueden conectarse e intercambiar información a través de un marco de identificación digital común.

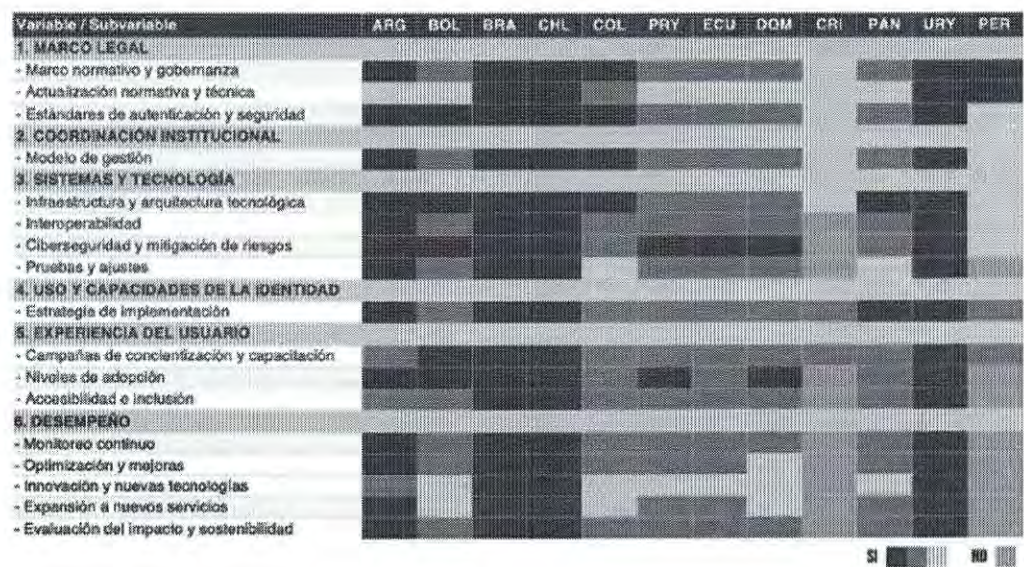
Experiencia de otros países en desarrollo resultan particularmente útiles para América Latina por contar con desafíos estructurales similares. El panorama africano es heterogéneo. Mientras algunos países arrastran sistemas legados coloniales, otros están adoptando arquitecturas de “tercera generación” (identidad digital nativa) financiadas por organismos internacionales como el Banco Mundial (programa ID4D). Países como

⁸ BID.

Nigeria, Kenia, Etiopía y Marruecos han desplegado sistemas nacionales de identificación digital basados en identificadores únicos y verificación biométrica, concebidos como infraestructuras habilitantes para la provisión de servicios públicos.

El desarrollo de la identificación digital en América Latina se encuentra en distintas etapas y presenta diversidad en sus enfoques.

Análisis comparativo de los sistemas de identificación digital



Fuente: análisis SmC+.

Nota: la escala de colores se basa en una calificación cualitativa de 0 a 3, donde el color más oscuro representa un nivel de desarrollo avanzado (3), asociado a marcos normativos consolidados, altos estándares de interoperabilidad y adopción ciudadana sostenida; el tono intermedio identifica un nivel medio (2), caracterizado por avances parciales en la implementación; el tono claro señala un desarrollo inicial (1), con presencia normativa o institucional incipiente; y el gris corresponde a ausencia o falta de evidencia pública (0). La clasificación fue validada con los organismos nacionales responsables de cada sistema a partir de información oficial disponible hasta agosto de 2025.

La identificación digital tiene el potencial de contribuir en más de 1.600 mil millones USD al PIB de América Latina y Caribe. Se plantearon dos escenarios de adopción de la identificación digital (uno moderado y uno acelerado), en los cuales su impacto económico regional podría llegar a alcanzar el 1,8% y al 2,1%, respectivamente, del Producto Interno Bruto (PIB). En el escenario de “adopción moderada”, se espera que entre el 41% y el 90% de la población adopte la identificación digital de manera gradual, considerando factores como la infraestructura existente y la resistencia al

cambio. A modo de referencia, países como Estonia y Singapur han logrado tasas de adopción digital significativamente más altas (cercasas al 100%) en sistemas que ya llevan más de una década desde su implementación. En contraste, el escenario de ‘adopción acelerada’ considera una adopción entre el 54% y el 99% de la población. Este escenario se utiliza como ejercicio teórico para explorar el máximo potencial de impacto.

Las principales variables del estudio de impacto, considerando su relevancia económica son la reducción del fraude a gobiernos, el incremento de la recaudación impositiva y ahorros producto de un mayor nivel de digitalización.

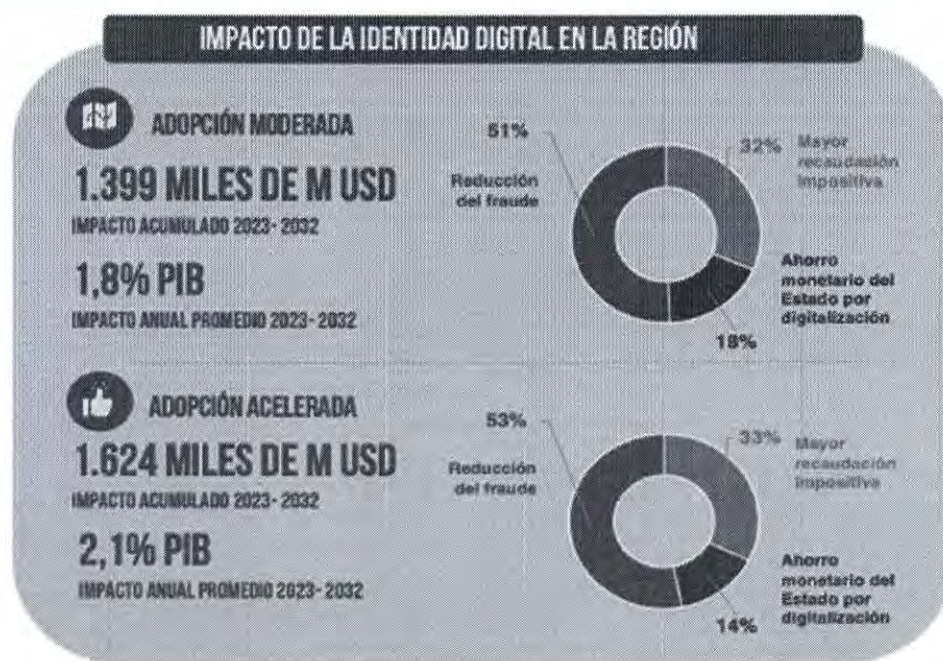
	VARIABLE DE IMPACTO ECONÓMICO	RELEVANCIA EN EL IMPACTO*
	Reducción del fraude a gobiernos	51%
	Incremento de la recaudación impositiva	32%
	Generación de ahorros para gobiernos producto de un mayor nivel de digitalización	18%

Notas: (*) valores de referencia para el escenario de adopción moderada.

Fuente: análisis SmC+

Los resultados del impacto de la identificación digital en el PIB muestran variaciones entre los países analizados, dependiendo del nivel de adopción y las variables consideradas en el modelo. En un escenario de adopción acelerado, donde se alcanza entre el 54% y el 99% de adopción, en algunos países se observa un impacto económico en el PIB de hasta un 3,5% para el año 2032. Para la extrapolación a nivel regional (América Latina y Caribe), se ha proyectado el impacto de la identificación digital en estos países tomando como referencia su PIB.

Resultados del estudio de impacto económico para América Latina y Caribe



Fuente: análisis SmC+

La adopción de la identificación digital en la región de América Latina y el Caribe debe sortear una serie de barreras para alcanzar niveles de uso relevantes. Las barreras identificadas para la implementación y adopción de la identificación digital incluyen aspectos tecnológicos, la brecha digital, la disponibilidad de recursos económicos y factores relacionados con la cultura organizacional y la gobernanza, como ser la necesidad de un liderazgo y la cultura organizacional para la digitalización de procesos de gobierno.

Principales barreras para la implementación de la identificación digital en América Latina



Fuentes: análisis SmC+ a partir de Programa de Naciones Unidas para el Desarrollo y Grupo Banco Mundial. (2022). Acceso y Uso de Internet en América Latina y el Caribe. Resultados de las encuestas telefónicas de alta frecuencia de ALC 2021; OCDE. (2020). *Latin American Economic Outlook 2020: Digital Transformation for Building Back Better*; Edelman. (2022). *Edelman Trust Barometer*.

Se proponen estrategias para guiar a los países según su nivel de desarrollo en sistemas de identificación digital. Para los países en etapas iniciales, como Perú y Costa Rica, se recomienda enfocar esfuerzos en establecer una arquitectura institucional y normativa básica. Esto incluye definir una autoridad rectora, establecer estándares de seguridad e interoperabilidad, y crear una hoja de ruta nacional. Paralelamente, deben priorizar la digitalización de servicios públicos esenciales (como salud, educación y registro civil) y lanzar campañas de alfabetización digital para fomentar el uso inclusivo de estos sistemas. Es importante destacar que, en el caso específico de Costa Rica, estos cuatro elementos se encuentran delineados, aunque aún requieren procesos de consolidación y formalización. Más que crear una arquitectura básica, el desafío radica en fortalecer la existente.

Para los países de la primera ola de adopción masiva, como Paraguay, Panamá, República Dominicana y Bolivia, resulta prioritario consolidar la gobernanza de sus sistemas de identidad digital, formalizando marcos

legales sobre autenticación, protección de datos y firma digital. Es fundamental integrar gradualmente servicios prioritarios bajo plataformas únicas de autenticación, asegurando la interoperabilidad entre instituciones. El fortalecimiento de la coordinación interinstitucional y la inversión en infraestructura digital también son claves en esta fase.

En la segunda ola de adopción, que incluye a Colombia y Ecuador, una posible línea de acción es avanzar hacia modelos federados de identidad digital, que permitan autenticar a los usuarios mediante múltiples mecanismos (como certificados digitales, biometría o banca digital), a través de brokers de identidad. Es prioritario fortalecer la experiencia de usuario (con autenticación multifactor, accesibilidad y diseño centrado en el ciudadano) y mejorar la interoperabilidad entre bases de datos estatales.

En países con mayor desarrollo en la materia, como Brasil, Uruguay, Chile y Argentina, una prioridad es consolidar la interoperabilidad tanto interna como regional. Esto implica ampliar el alcance de la identificación digital hacia nuevos casos de uso, como trámites diferenciados por segmento poblacional (jubilaciones, servicios para menores, etc.) o por contexto (emergencias sanitarias o climáticas). Además, deben adoptar tecnologías avanzadas de autenticación como biometría y 2FA16, y fortalecer sus mecanismos de ciberseguridad. Para sostener la mejora continua, es fundamental establecer métricas claras sobre satisfacción ciudadana, facilidad de uso y confianza en el sistema, que guíen la toma de decisiones estratégicas basadas en evidencia.”

II) MARCO LEGAL

El derecho a la identidad se encuentra establecido en primer término en la Constitución Política de los Estados Unidos Mexicanos y en las leyes, federales y locales, así como en diversos instrumentos internacionales.

1. Constitucional

La adición constitucional, publicada en el *Diario Oficial de la Federación* del 17 de junio de 2014, del artículo 4, párrafo octavo, fue el parteaguas para reconocerse en México el derecho a la identidad como derecho fundamental para que las personas tengan la certeza de que el Estado tiene que reconocer y buscar los mecanismos legales para hacerla efectiva.

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 4, párrafo décimo, menciona: *“toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento”*.⁹

2. Legales

A) Código Civil Federal

En el ámbito civil federal, este derecho e institución se rige a través del **Libro Primero del Código Civil Federal (CCF)**, específicamente en el **Título Cuarto (Del Registro Civil)**:

“Artículo 35.- En el Distrito Federal, estará a cargo de los Jueces del Registro Civil autorizar los actos del estado civil y extender las actas relativas a nacimiento, reconocimiento de hijos, adopción, matrimonio, divorcio administrativo y muerte de los mexicanos y extranjeros residentes en los perímetros de las Delegaciones del Distrito Federal, así como inscribir las ejecutorias que declaren la ausencia, la presunción de muerte, el divorcio judicial, la tutela o que se ha perdido o limitado la capacidad legal para administrar bienes.

⁹ Cámara de Diputados. Constitución Política de los Estados Unidos Mexicanos.
<https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>

Artículo 54.- Las declaraciones de nacimiento se harán presentando al niño ante el Juez del Registro Civil en su oficina o en el lugar donde aquél hubiere nacido.”

B) **La Ley General de los Derechos de Niñas, Niños y Adolescentes** en México, en su artículo 19, señala los elementos del derecho a la identidad, el cual a la letra dice:

“Artículo 19. Niñas, niños y adolescentes, en términos de la legislación civil aplicable, desde su nacimiento, tienen derecho a:

- I. Contar con nombre y los apellidos que les correspondan, así como a ser inscritos en el Registro Civil respectivo de forma inmediata y gratuita, y a que se les expida en forma ágil y sin costo la primer copia certificada del acta correspondiente, en los términos de las disposiciones aplicables;
 - II. Contar con nacionalidad, de conformidad con lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales;
 - III. Conocer su filiación y su origen, en la medida de lo posible y siempre que ello sea acorde con el interés superior de la niñez, y
 - IV. Preservar su identidad, incluidos el nombre, la nacionalidad y su pertenencia cultural, así como sus relaciones familiares.³
- ...”

2. Fundamentación Convencional e Internacional

Diversos organismos internacionales reconocen que la identidad digital es un catalizador clave para los Objetivos de Desarrollo Sostenible (ODS 16.9 de la Agenda 2030 de la ONU: “Proporcionar acceso a una identidad jurídica para todos”).

Asimismo, en el ámbito comparado (como el Reglamento eIDAS de la Unión Europea y las directrices de la Organización de los Estados Americanos), se ha

demostrado que el reconocimiento constitucional de la identidad digital salvaguarda principios clave:

- **Autodeterminación informativa:** El control exclusivo del ciudadano sobre sus atributos identitarios.
- **Privacidad desde el diseño:** Garantía de que los sistemas de identidad no se conviertan en instrumentos de vigilancia o control estatal masivo.

III) OBJETO DE LA INICIATIVA

La Iniciativa que se presenta tiene como objeto elevar a rango constitucional el reconocimiento a la identidad digital y su protección, al efecto se propone:

Reformar el párrafo décimo del artículo 4º y se mandata al Estado Mexicano a garantizar el reconocimiento, la protección, el uso seguro y la inclusión de las personas en el entorno digital, sentando las bases para una futura Ley General en la materia.

Así mismo se propone reformar el párrafo tercero del artículo 6º para establecer que: *“El Estado garantizará la protección de la infraestructura crítica, la ciberseguridad y la salvaguarda integral de la identidad digital y los datos personales y biométricos de las personas. La ley regulará los mecanismos de autodeterminación informativa y asegurará que la adopción de medios digitales no discrimine ni excluya el acceso a trámites o servicios en formato presencial.”*

Y por último, se propone reformar el párrafo segundo del artículo 16 de la Constitución Federal, para que el Estado mexicano garantice que el desarrollo tecnológico no ocurra a expensas de la dignidad humana y la privacidad, se **Proteja a los ciudadanos frente al perfilamiento automatizado, el uso no autorizado de su** identidad digital e **información biométrica** y se incorpore el derecho a la **portabilidad** de los datos personales, un estándar internacional indispensable para la libre competencia y el control del usuario sobre su propia información.

Para mejor comprensión de lo anterior se presenta el siguiente cuadro comparativo:

Constitución Política de los Estados Unidos Mexicanos.

Texto vigente	Propuesta de la Iniciativa
Artículo 4o.- La mujer y el hombre son iguales ante la ley. Ésta protegerá la organización y el desarrollo de las familias. El Estado garantizará el goce y ejercicio del derecho a la igualdad sustantiva de las mujeres.	Artículo 4o.- ...
Toda persona tiene derecho a decidir de manera libre, responsable e informada sobre el número y el espaciamiento de sus hijos.	...
Toda persona tiene derecho a la alimentación nutritiva, suficiente y de calidad. El Estado lo garantizará. México es centro de origen y diversidad del maíz, que es un elemento de identidad nacional, alimento básico del pueblo de México y base de la existencia de los pueblos indígenas y afromexicanos. Su cultivo en el territorio nacional debe ser libre de modificaciones genéticas producidas con técnicas que superen las barreras naturales de la reproducción o la recombinación, como las transgénicas. Todo otro uso del maíz genéticamente modificado debe ser evaluado en los términos de las disposiciones legales para quedar libre de amenazas para la	...

bioseguridad, la salud y el patrimonio biocultural de México y su población. Debe priorizarse la protección de la biodiversidad, la soberanía alimentaria, su manejo agroecológico, promoviendo la investigación científica-humanística, la innovación y los conocimientos tradicionales.	
Toda Persona tiene derecho a la protección de la salud. La Ley definirá las bases y modalidades para el acceso a los servicios de salud y establecerá la concurrencia de la Federación y las entidades federativas en materia de salubridad general, conforme a lo que dispone la fracción XVI del artículo 73 de esta Constitución. La Ley definirá un sistema de salud para el bienestar, con el fin de garantizar la extensión progresiva, cuantitativa y cualitativa de los servicios de salud para la atención integral y gratuita de las personas que no cuenten con seguridad social.	...
Para garantizar el derecho de protección a la salud de las personas, la ley sancionará toda actividad relacionada con cigarrillos electrónicos, vapeadores y demás sistemas o dispositivos análogos que señale la ley; así como la producción, distribución y enajenación de sustancias tóxicas, precursores químicos, el uso ilícito del fentanilo y demás drogas sintéticas no autorizadas.	...

Toda persona tiene derecho a un medio ambiente sano para su desarrollo y bienestar. El Estado garantizará el respeto a este derecho. El daño y deterioro ambiental generará responsabilidad para quien lo provoque en términos de lo dispuesto por la ley.	...
Queda prohibido el maltrato a los animales. El Estado mexicano debe garantizar la protección, el trato adecuado, la conservación y el cuidado de los animales, en los términos que señalen las leyes respectivas.	...
Toda persona tiene derecho al acceso, disposición y saneamiento de agua para consumo personal y doméstico en forma suficiente, salubre, aceptable y asequible. El Estado garantizará este derecho y la ley definirá las bases, apoyos y modalidades para el acceso y uso equitativo y sustentable de los recursos hídricos, estableciendo la participación de la Federación, las entidades federativas y los municipios, así como la participación de la ciudadanía para la consecución de dichos fines.	...
Toda persona tiene derecho a disfrutar de vivienda adecuada. La Ley establecerá los instrumentos y apoyos necesarios a fin de alcanzar tal objetivo.	...

Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento.	Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. Este derecho comprende la identidad digital segura, interoperable y gratuita. El Estado garantizará la protección y cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de nacimiento y la clave de identidad digital vinculada a su registro. El Estado garantizará el ejercicio de este derecho, estableciendo los mecanismos tecnológicos y normativos que aseguren la inclusión, privacidad, ciberseguridad e interoperabilidad en el entorno digital, en los términos que establezca la ley.
En todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos. Los niños y las niñas tienen derecho a la satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo integral. Este principio deberá guiar el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez. Los ascendientes, tutores y custodios	
tienen la obligación de preservar y exigir el cumplimiento de estos derechos y	

principios.	
El Estado otorgará facilidades a los particulares para que coadyuven al cumplimiento de los derechos de la niñez.	...
Toda persona tiene derecho al acceso a la cultura y al disfrute de los bienes y servicios que presta el Estado en la materia, así como el ejercicio de sus derechos culturales. El Estado promoverá los medios para la difusión y desarrollo de la cultura, atendiendo a la diversidad cultural en todas sus manifestaciones y expresiones con pleno respeto a la libertad creativa. La ley establecerá los mecanismos para el acceso y participación a cualquier manifestación cultural.	...
Toda persona tiene derecho a la cultura física y a la práctica del deporte. Corresponde al Estado su promoción, fomento y estímulo conforme a las leyes en la materia.	...
La Federación y las entidades federativas garantizarán la entrega de una pensión no contributiva a las personas con discapacidad permanente menores de sesenta y cinco años, en los términos que fije la ley.	...
El Estado garantizará la rehabilitación y habilitación de las personas que viven con	...

discapacidad permanente, dando prioridad a las personas menores de dieciocho años de edad, en términos que fije la ley.	
Las personas adultas mayores de sesenta y cinco años tienen derecho a recibir por parte del Estado una pensión no contributiva en los términos que fije la ley.	...
A las personas con discapacidad permanente menores de sesenta y cinco años les corresponde la pensión no contributiva por discapacidad, y a todas las personas mayores de esa edad les corresponde la pensión no contributiva de adultos mayores.	...
El Estado establecerá un sistema de becas para las y los estudiantes de todos los niveles escolares del sistema de educación pública, con prioridad a las y los pertenecientes a las familias que se encuentren en condición de pobreza, para garantizar con equidad el derecho a la educación.	...
Toda persona tiene derecho a la movilidad en condiciones de seguridad vial, accesibilidad, eficiencia, sostenibilidad, calidad, inclusión e igualdad.	...
El Estado promoverá el desarrollo integral de las personas jóvenes, a través de políticas públicas con enfoque	...

multidisciplinario, que propicien su inclusión en el ámbito político, social, económico y cultural del país. La Ley establecerá la concurrencia de la Federación, entidades federativas, Municipios y demarcaciones territoriales de la Ciudad de México, para esos efectos.	
Toda persona tiene derecho a vivir una vida libre de violencias, el Estado tiene deberes reforzados de protección con las mujeres, adolescentes, niñas y niños. La ley definirá las bases y modalidades para garantizar su realización de conformidad con lo previsto en los artículos 21, párrafo noveno y 73, fracción XXI, penúltimo párrafo de esta Constitución.	...
El Estado destinará anualmente los recursos presupuestarios suficientes y oportunos, conforme al principio de progresividad, para garantizar los derechos establecidos en este artículo que impliquen la transferencia de recursos directos hacia la población destinataria. El monto de los recursos asignados no podrá ser disminuido, en términos reales, respecto del que se haya asignado en el ejercicio fiscal inmediato anterior.	...
Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún	Artículo 6o. ...

delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado. Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión. El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Ejecutivo Federal a través de la dependencia encargada de elaborar y conducir las políticas de telecomunicaciones y radiodifusión, establecerá condiciones de competencia efectiva en la prestación de dichos servicios.	... El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Ejecutivo Federal a través de la dependencia encargada de elaborar y conducir las políticas de telecomunicaciones y radiodifusión, establecerá condiciones de competencia efectiva en la prestación de dichos servicios. El Estado garantizará la protección de la infraestructura crítica, la ciberseguridad y la salvaguarda integral de la identidad digital y los datos personales y biométricos de las personas. La ley regulará los mecanismos de autodeterminación informativa y asegurará que la adopción de medios digitales no discrimine ni excluya el acceso a trámites o servicios en formato presencial.
---	--

Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:	...
A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:	...
I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.	...
II. La información que se refiere a la vida privada y los datos personales será	

protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados contarán con las facultades suficientes para su atención.	
Por lo que hace a la información relacionada con los datos personales en posesión de particulares, la ley a la que se refiere el artículo 90 de esta Constitución determinará la competencia para conocer de los procedimientos relativos a su protección, verificación e imposición de sanciones.	...
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.	...
IV. Se establecerán mecanismos de acceso a la información pública y procedimientos de revisión expeditos que se sustanciarán ante las instancias competentes en los términos que fija esta Constitución y las leyes.	...
V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán, a través de los medios electrónicos disponibles, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que	...

permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.	
VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.	...
VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.	...
VIII. Los sujetos obligados deberán promover, respetar, proteger y garantizar los derechos de acceso a la información pública y a la protección de datos personales. Las leyes en la materia determinarán las bases, principios generales y procedimientos del ejercicio de estos derechos, así como la competencia de las autoridades de control interno y vigilancia u homólogos en el ámbito federal y local para conocer de los procedimientos de revisión contra los actos que emitan los sujetos obligados.	...
Los sujetos obligados se registrarán por la ley general en materia de transparencia y acceso a la información pública y protección de datos personales, en los términos que ésta se emita por el Congreso de la Unión para establecer las bases,	...

principios generales y procedimientos del ejercicio de este derecho.	
El ejercicio de este derecho se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.	...
La ley establecerá aquella información que se considere reservada o confidencial.	...
B. En materia de radiodifusión y telecomunicaciones:	...
I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.	...
II. Las telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias.	...
III. La radiodifusión es un servicio público de interés general, por lo que el Estado garantizará que sea prestado en condiciones de competencia y calidad y brinde los beneficios de la cultura a toda la población, preservando la pluralidad y la	...

veracidad de la información, así como el fomento de los valores de la identidad nacional, contribuyendo a los fines establecidos en el artículo 3o. de esta Constitución.	
IV. Se prohíbe la transmisión de publicidad o propaganda presentada como información periodística o noticiosa; se establecerán las condiciones que deben regir los contenidos y la contratación de los servicios para su transmisión al público, incluidas aquellas relativas a la responsabilidad de los concesionarios respecto de la información transmitida por cuenta de terceros, sin afectar la libertad de expresión y de difusión.	...
V. La ley establecerá un organismo público descentralizado con autonomía técnica, operativa, de decisión y de gestión, que tendrá por objeto proveer el servicio de radiodifusión sin fines de lucro, a efecto de asegurar el acceso al mayor número de personas en cada una de las entidades de la Federación, a contenidos que promuevan la integración nacional, la formación educativa, cultural y cívica, la igualdad entre mujeres y hombres, la difusión de información imparcial, objetiva, oportuna y veraz del acontecer nacional e internacional, y dar espacio a las obras de producción independiente, así como a la expresión de la diversidad y pluralidad de	...

ideas y opiniones que fortalezcan la vida democrática de la sociedad.	
El organismo público contará con un Consejo Ciudadano con el objeto de asegurar su independencia y una política editorial imparcial y objetiva. Será integrado por nueve consejeros honorarios que serán elegidos mediante una amplia consulta pública por el voto de dos terceras partes de los miembros presentes de la Cámara de Senadores o, en sus recesos, de la Comisión Permanente. Los consejeros desempeñarán su encargo en forma escalonada, por lo que anualmente serán sustituidos los dos de mayor antigüedad en el cargo, salvo que fuesen ratificados por el Senado para un segundo periodo.	...
El Presidente del organismo público será designado, a propuesta del Ejecutivo Federal, con el voto de dos terceras partes de los miembros presentes de la Cámara de Senadores o, en sus recesos, de la Comisión Permanente; durará en su encargo cinco años, podrá ser designado para un nuevo periodo por una sola vez, y sólo podrá ser removido por el Senado mediante la misma mayoría.	...
El Presidente del organismo presentará anualmente a los Poderes Ejecutivo y Legislativo de la Unión un informe de actividades; al efecto comparecerá ante las	...

Cámaras del Congreso en los términos que dispongan las leyes. VI. La ley establecerá los derechos de los usuarios de telecomunicaciones, de las audiencias, así como los mecanismos para su protección.	...
Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.	Artículo 16. ... Toda persona tiene derecho a la protección de sus datos personales y de su identidad digital, al acceso, rectificación, cancelación y portabilidad de los mismos, así como a manifestar su oposición y a no ser objeto de decisiones automatizadas que afecten sus derechos, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. El Estado

	garantizará la protección del individuo frente al perfilamiento, el rastreo y el uso no autorizado de su información biométrica y comportamiento en entornos digitales, reconociendo la identidad digital como una extensión de la dignidad humana.
No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querrela de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.	...
La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculcado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.	...
Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a disposición de la autoridad civil más cercana y ésta con la misma prontitud, a la del Ministerio Público. Existirá un registro inmediato de la detención.	...

Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder.	...
En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley.	...
La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días.	...

Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.	...
Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.	...
En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia.	...
Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por	...

alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.	
Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.	...
Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u	...

ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.	
Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.	...
La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.	...
La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley.	...
En tiempo de paz ningún miembro de la Fuerza Armada permanente -el Ejército, la Fuerza Aérea, la Armada y la Guardia Nacional- podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento,	...

bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.	
---	--

IV) DECRETO

Sirvan los razonamientos y argumentos arriba expresados para someter a consideración de esta soberanía la siguiente Iniciativa con Proyecto de Decreto, que reforma el párrafo decimo del artículo 4º, el párrafo tercero del artículo 6º y el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, **en materia del reconocimiento y protección de la identidad digital**, para quedar como sigue:

Artículo Único. Se reforman el párrafo decimo del artículo 4º; el párrafo tercero del artículo 6º y el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, **en materia del reconocimiento y protección de la identidad digital**, para quedar como sigue:

Artículo 4o.- ...

...

...

...

...

...

...

...

...

Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. **Este derecho comprende la identidad digital segura, interoperable y gratuita.** El Estado garantizará la **protección** y cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia

certificada del acta de nacimiento y la clave de identidad digital vinculada a su registro. El Estado garantizará el ejercicio de este derecho, estableciendo los mecanismos tecnológicos y normativos que aseguren la inclusión, privacidad, ciberseguridad e interoperabilidad en el entorno digital, en los términos que establezca la ley.

...
...
...
...
...
...
...
...
...
...
...
...
...
...
...

Artículo 6o. ...

...

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Ejecutivo Federal a través de la dependencia encargada de elaborar y conducir las políticas de telecomunicaciones y radiodifusión, establecerá condiciones de competencia efectiva en la prestación de dichos servicios. **El Estado garantizará la protección de la infraestructura crítica, la ciberseguridad y la salvaguarda integral de la identidad digital y los datos personales y biométricos de las personas.** La ley regulará los mecanismos de autodeterminación informativa y asegurará que

la adopción de medios digitales no discrimine ni excluya el acceso a trámites o servicios en formato presencial.

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

Artículo 16. ...

Toda persona tiene derecho a la protección de sus datos personales **y de su identidad digital**, al acceso, rectificación, cancelación **y portabilidad** de los mismos, así como a manifestar su oposición **y a no ser objeto de decisiones automatizadas que afecten sus**

derechos, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. **El Estado garantizará la protección del individuo frente al perfilamiento, el rastreo y el uso no autorizado de su información biométrica y comportamiento en entornos digitales, reconociendo la identidad digital como una extensión de la dignidad humana.**

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

Transitorios

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

SEGUNDO. El Congreso de la Unión dispondrá de un plazo no mayor a **360 días naturales** contados a partir de la entrada en vigor del presente Decreto para expedir la **Ley General de Identidad y Ciudadanía Digital**, así como para armonizar el marco legal en materia de protección de datos personales en posesión de sujetos obligados, ciberseguridad y firma electrónica.

TERCERO. El Ejecutivo Federal, en coordinación con las entidades federativas, implementará el Sistema Nacional de Identidad Digital dentro de un plazo máximo de **dos años** posteriores a la entrada en vigor del Decreto correspondiente a la Ley General señalada en el artículo Transitorio Segundo, garantizando en todo momento la gratuidad, la accesibilidad universal y la adopción de tecnologías de cifrado y ciberseguridad avanzada.

ATENTAMENTE



KARINA MARGARITA DEL RÍO ZENTENO

Palacio Legislativo de San Lázaro a 1 de septiembre de 2026.

Iniciativa con Proyecto de Decreto por el que se Reforma la Constitución Política de los Estados Unidos Mexicanos, en materia de delitos de índole sexual en niñas, niños o adolescentes para que la recepción del testimonio de la víctima pueda usarse herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales.

Diputada Olga Leticia Chávez Rojas, integrante del Grupo Parlamentario de Morena en la Cámara de Diputados en la LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos; 6, numeral 1, fracción I, 77, 78 y demás relativos y aplicables del Reglamento de la Cámara de Diputados, someto a consideración de esta asamblea la siguiente iniciativa con proyecto de decreto, por el que se reforma el artículo 20, Apartado C, fracción V de la Constitución Política de los Estados Unidos Mexicanos, en materia de delitos de índole sexual en niñas, niños o adolescentes para que la recepción del testimonio de la víctima puedan usarse herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales, conforme a la siguiente:

Exposición de Motivos

El Estado mexicano ha implementado políticas públicas para erradicar la violencia contra las Niñas, Niños y Adolescentes, cuya finalidad es proteger y salvaguardar los derechos humanos de este sector de la población, muestra de ello, es la Ley General de los Derechos de Niñas, Niños y Adolescentes del 4 de diciembre de 2014, siendo unos de sus objetivos garantizar el pleno ejercicio, respeto, protección y promoción de los derechos humanos de niñas, niños y adolescentes conforme a lo establecido en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de los que el Estado mexicano forma parte.

El artículo 1º de la Constitución Política establece que en México todas las personas gozan de los derechos humanos, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que la propia Constitución establece.

Igualmente impone la obligación a todas las autoridades, en el ámbito de sus competencias, de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

El Convenio sobre los Derechos del Niño, aprobado el 20 de noviembre de 1989, en el que México es parte, determina en su numeral 19 que “Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo”.¹

No obstante, cifras del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública Centro Nacional de Información Incidencia delictiva del fuero común, indican que, de enero a junio de 2026, se han cometido 41,399 delitos contra libertad y la seguridad sexual; Abuso Sexual 16,744, Acoso Sexual 5,406, Hostigamiento Sexual 1,145, Violación Simple 6,875, Violación Equiparada 3,202.²

¹ Artículo 19 del Convenio sobre los Derechos del Niño.

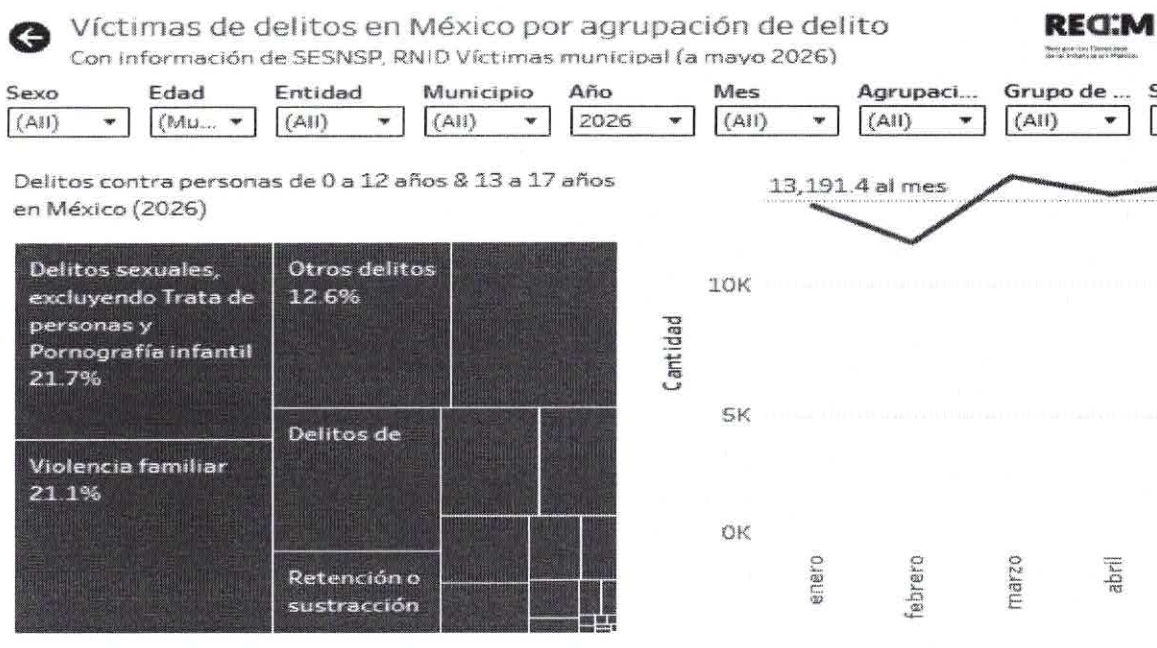
² Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública Centro Nacional de información Incidencia delictiva del fuero común.

**Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública Centro
Nacional de Información Incidencia delictiva del fuero común¹/ Nacional, 2026**

I. Clasificación de delitos													
Bien jurídico afectado	Tipo de delito, subtipo y modalidad	Enero	Febrero	Marzo	Abril	Mayo	Junio						
La libertad y la seguridad sexual	Total de delitos contra la libertad y la seguridad sexual	5,959	6,190	7,652	7,120	7,222	7,256						41,399
	Abuso sexual	2,331	2,493	3,121	2,844	2,968	2,987						16,744
	Acoso sexual	728	791	1,004	938	1,011	934						5,406
	Hostigamiento sexual	230	253	183	150	159	170						1,145
	Violación simple	942	984	1,307	1,160	1,198	1,284						6,875
	Violación equiparada	466	471	600	580	543	542						3,202
	Incesto	0	0	1	0	2	1						4
	Violación a la intimidad sexual	575	536	731	743	670	671						3,926
	Otros delitos que atentan contra la libertad y la seguridad sexual	687	662	705	705	671	667						4,097

Otro dato para destacar es que en nuestro país los delitos cometidos contra menores de edad van en ascenso, tan solo de enero a mayo del 2026, se cometieron 65,957 delitos a personas de 0 a 17 años, correspondiendo 21.7% a delitos sexuales³, es decir se violentaron en ese periodo a 14,312 menores de edad, cifra alarmante.

³ Blog de datos e incidencia Política de REDIM-Derechos de infancia y adolescencia en Mexico.



El constituyente mexicano estableció, al inicio del artículo 20 de la Constitución Política de los Estados Unidos Mexicanos, que el proceso penal oral y acusatorio se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación. Esos principios tienen como finalidad garantizar los derechos de las partes, son medios para la realización del debido proceso y principios de operación.⁴

El principio de inmediación es característico del sistema penal acusatorio mexicano que apunta a que se pueda realizar el derecho de defensa de las partes a través de la contradicción. Este principio surgió como consecuencia del proceso liberal que se contraponía al sistema de justicia secreta. Por tanto, ahora el juicio debe ser oral y público para que cualquiera pueda verlo y oírlo. Así, la introducción del principio de inmediación se traduce en un punto de la legitimidad del juicio, pues que todas las

⁴ Exposición de motivos de la reforma constitucional 2008

partes estén en una audiencia con la persona juzgadora y que en ese momento ejerzan su derecho de contradicción frente a todos genera confiabilidad en la impartición de justicia.⁵

En se sentido, el principio de inmediación implica que el juzgador que dicta la resolución debe presidir las audiencias, observar por sí mismo la recepción de la prueba (o datos de prueba, según la etapa procesal) y el debate generado para extraer directamente la información necesaria que servirá como motivación de su decisión. En consecuencia, respetar el principio de inmediación en las audiencias del proceso penal también permite dar confiabilidad a los argumentos que el juzgador expone en sus resoluciones respecto a la información que las partes introducen al proceso penal.⁶

Precisamente nos centraremos en el principio de inmediación ya que presupone que todos los elementos de prueba vertidos en un proceso y que servirán para decidir sobre la responsabilidad penal de una persona, deben ser presenciados sin mediaciones o intermediarios por el juez en una audiencia. Los alcances de dicho propósito implican reconocer que es en la etapa de juicio donde la inmediación cobra plena aplicación, porque en esta vertiente configura una herramienta metodológica para la formación de la prueba, la cual exige el contacto directo y personal que el juez debe tener con los sujetos y el objeto del proceso durante la realización de la audiencia de juicio, porque de esa manera se coloca al juez en las mejores condiciones posibles para percibir –sin intermediarios– toda la información que surja de las pruebas personales, es decir, no sólo la de contenido verbal, sino que la inmediación también lo ubica en óptimas

⁵ Cuadernos de jurisprudencia, Pg. 2, Suprema Corte de Justicia de la Nación, Centro de Estudios Constitucionales.

⁶ Idem.

condiciones para constatar una serie de elementos que acompañan a las palabras del declarante, habilitados para transmitir y recepcionar de mejor manera el mensaje que se quiere entregar, como el manejo del tono, volumen o cadencia de la voz, pausas, titubeos, disposición del cuerpo, dirección de la mirada, muecas o sonrojo, que la doctrina denomina componentes paralingüísticos⁷.

Ahora bien, en un procedimiento penal que involucre a un menor que fue violentado (víctima del delito), tiene que comparecer a juicio frente a su victimario y por ende se le revictimiza, esta problemática y la ausencia clara y precisa en la ley de que se pueda utilizar la tecnología en la presentación del testimonio del menor a generado recursos jurisdiccionales para evadir la acción de la justicia o para retrasarla, utilizando el principio inmediación que rige el proceso penal acusatorio y oral (Art. 20, apartado A, fracción II de la Constitución).

La Ley General de los Derechos de Niñas, Niños y Adolescentes, indica los principios rectores, dentro de los que se encuentra el interés superior de la niñez y el principio de no revictimización del menor en juicios cuando intervienen en procedimientos judiciales como víctimas o testigos.

En ese sentido el objetivo de la presente iniciativa es que, tratándose de delitos de índole sexual, la recepción del testimonio de la víctima niña, niño o adolescente podrá presentarse mediante herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales. Esto es, al momento de que un menor rinda su testimonio

⁷ Registro digital: 2020268, Décima Época, tesis 1a./J. 54/2019 (10a.), Gaceta del Semanario Judicial de la Federación. Libro 68, Julio de 2019, Tomo I, página 184, de rubro PRINCIPIO DE INMEDIACIÓN COMO HERRAMIENTA METODOLÓGICA PARA LA FORMACIÓN DE LA PRUEBA. EXIGE EL CONTACTO DIRECTO Y PERSONAL DEL JUEZ CON LOS SUJETOS Y EL OBJETO DEL PROCESO DURANTE LA AUDIENCIA DE JUICIO.

Olga Leticia Chávez Rojas
DIPUTADA FEDERAL

como víctima de un delito sexual lo podrá hacer a través de los medios tecnológicos (vía electrónica, por “**Zoom**” dentro de la audiencia).

Para mayor claridad de lo planteado se presenta la siguiente tabla:

Constitución Política de los Estados Unidos Mexicanos Texto Actual	Constitución Política de los Estados Unidos Mexicanos Texto propuesto
Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación. A. De los principios generales: I a XI... B. De los derechos de toda persona imputada: I a IX... C. De los derechos de la víctima o del ofendido: I a IV... V. Al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa. Sin correlativo	Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación. A. De los principios generales: I a XI... B. De los derechos de toda persona imputada: I a IX... C. De los derechos de la víctima o del ofendido: I a IV... V. Al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa. Tratándose de delitos de índole sexual, la recepción del testimonio de la víctima niña, niño o adolescente podrá presentarse mediante herramientas

Olga Leticia Chávez Rojas

DIPUTADA FEDERAL

El Ministerio Público deberá garantizar la protección de víctimas, ofendidos, testigos y en general todos los sujetos que intervengan en el proceso. Los jueces deberán vigilar el buen cumplimiento de esta obligación; VI... VII...	tecnológicas, con la finalidad de proteger sus derechos fundamentales. El Ministerio Público deberá garantizar la protección de víctimas, ofendidos, testigos y en general todos los sujetos que intervengan en el proceso. Los jueces deberán vigilar el buen cumplimiento de esta obligación; VI... VII...
--	---

Cabe indicar que la Suprema Corte de Justicia de la Nación ha resuelto el Amparo Directo 38/2025 en sentido positivo en donde la postura es que se puede utilizar la tecnología para que el menor (víctima) pueda rendir su testimonio, en virtud que se argumentaba que se violaba el principio de inmediación, porque el menor compareció a juicio vía **“Zoom”** (utilizando la tecnología). En dicha resolución el órgano jurisdiccional determinó:

“Por lo tanto, si se realiza una interpretación sistemática del principio de inmediación a fin de salvaguardar ese interés superior, debe concluirse que el desahogo de la entrevista de la víctima niña, niño o adolescente mediante videoconferencia, con la imagen difuminada o en negro, no vulnera dicho principio, pues basta con que se tenga certeza de su identidad y de que es la persona que participa en la diligencia, lo cual permite considerar que la prueba se desahoga ante el juzgador y las partes, aun y cuando ello ocurra de manera remota y no en presencia física”.⁸

⁸ Amparo Directo 38/2025

“La CPEUM protege el interés superior de la infancia, que es un derecho multidimensional que funciona como un derecho sustantivo, como un principio jurídico de interpretación fundamental y como una norma de procedimiento. Así, aun cuando el principio de inmediación implica que la prueba se desahogue ante el tribunal y en presencia de las partes, el interés superior de las infancias, a su vez, conlleva que no se revictimice a una niña, niño o adolescente al enfrentarlo contra su agresor”.⁹

En ese sentido la presente iniciativa tiene como eje principal salvaguardar el interés superior del niño, por ello se pretende especificar constitucionalmente que, tratándose de delitos de índole sexual, la recepción del testimonio de la víctima niña, niño o adolescente podrá presentarse mediante herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales.

Por último, cabe indicar y en cumplimiento con el artículo 77, numeral 5 del Reglamento de la Cámara de Diputados, la presente iniciativa está correlacionada con la iniciativa que adiciona un segundo párrafo al artículo 59 de Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes; Se adiciona la fracción VII al artículo 86 de la Ley General de los Derechos de Niñas, Niños y Adolescentes; Se reforma la fracción XI del artículo 12 de la Ley General de Víctimas, en materia de delitos de índole sexual en niñas, niños o adolescentes para que la recepción del testimonio de la víctima pueda usarse herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales.

⁹ Idem.

Por lo expuesto, someto a consideración de esta Honorable Soberanía el siguiente:

Decreto por el que se reforma el artículo 20 apartado C fracción V de la Constitución Política de los Estados Unidos Mexicanos, en materia de delitos de índole sexual en niñas, niños o adolescentes para que la recepción del testimonio de la víctima pueda usarse herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales.

Artículo Único. Se reforma el artículo 20, Apartado C, fracción V de la Constitución Política de los Estados Unidos Mexicanos para quedar como sigue:

Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación.

A. De los principios generales:

I a XI...

B. De los derechos de toda persona imputada:

I a IX...

C. De los derechos de la víctima o del ofendido:

I a IV...

V. Al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa.

Tratándose de delitos de índole sexual, la recepción del testimonio de la víctima niña, niño o adolescente podrá presentarse mediante herramientas tecnológicas, con la finalidad de proteger sus derechos fundamentales.

El Ministerio Público deberá garantizar la protección de víctimas, ofendidos, testigos y en general todos los sujetos que intervengan en el proceso. Los jueces deberán vigilar el buen cumplimiento de esta obligación;

VI...

VII...

TRANSITORIOS

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

Palacio Legislativo de San Lázaro, a 2 de septiembre de 2026.



Diputada Olga Leticia Chávez Rojas

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN CAPÍTULO VIII BIS, DENOMINADO “DEL USO RESPONSABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL EN LOS SERVICIOS CONSULARES”, INTEGRADO POR LOS ARTÍCULOS 46 BIS, 46 TER, 46 QUÁTER, 46 QUINQUIES, 46 SEXIES, 46 SEPTIES, 46 OCTIES, 46 NONIES Y 46 DECIES, A LA LEY DEL SERVICIO EXTERIOR MEXICANO.

La proponente, Giselle Yunueen Arellano Ávila, Diputada Federal del grupo parlamentario MORENA de la LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en el artículo 71, fracción II y 135 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 6, numeral 1, fracción I, 77 y 78 y 82 fracción I del Reglamento de la Cámara de Diputados, someto a consideración del Pleno de la H. Cámara de Diputados la presente **iniciativa con proyecto de decreto por el que se adiciona un Capítulo VIII Bis, denominado Del Uso Responsable de Sistemas de Inteligencia Artificial en los Servicios Consulares, integrado por los artículos 46 Bis, 46 Ter, 46 Quáter, 46 Quinquies, 46 Sexies, 46 Septies, 46 Octies, 46 Nonies y 46 Decies, a la Ley del Servicio Exterior Mexicano**, al tenor de la siguiente:

Exposición de Motivos.

I. Antecedentes

La transformación tecnológica de las administraciones públicas ha modificado de manera sustancial la forma en que el Estado atiende las necesidades de la población. La incorporación de herramientas digitales permite reducir tiempos de gestión, facilitar el acceso a los servicios públicos y mejorar los mecanismos de atención; sin embargo, cuando estas herramientas incorporan sistemas capaces de procesar grandes volúmenes de información, generar recomendaciones o identificar patrones, su utilización también plantea nuevos retos jurídicos, particularmente cuando intervienen en procedimientos que pueden incidir en los derechos de las personas.

En este contexto, la inteligencia artificial ha dejado de constituir una herramienta circunscrita al ámbito estrictamente tecnológico para convertirse en un elemento con

presencia creciente en actividades económicas, sociales y gubernamentales. Su incorporación a la gestión pública puede representar una oportunidad para fortalecer la capacidad institucional, siempre que su utilización se encuentre sujeta a reglas claras que preserven la intervención de la autoridad, la protección de los datos personales, la igualdad y la no discriminación, así como la posibilidad de que las personas conozcan, cuestionen y, en su caso, impugnen las determinaciones que les afecten.

En México, el Congreso de la Unión ha comenzado a desarrollar una discusión legislativa cada vez más amplia en torno a la inteligencia artificial. Durante los últimos años se han presentado diversas iniciativas encaminadas a establecer principios, obligaciones y mecanismos de supervisión aplicables a esta tecnología desde distintas materias y perspectivas. Asimismo, se han planteado propuestas relacionadas con sus implicaciones en ámbitos específicos, entre ellos la protección de datos personales, los derechos de autor, las relaciones laborales, la seguridad, la administración pública y la protección frente a contenidos generados artificialmente.

Esta evolución legislativa resulta relevante para el ámbito del Servicio Exterior Mexicano. Las representaciones diplomáticas y consulares constituyen uno de los principales puntos de contacto entre el Estado y las personas mexicanas que se encuentran fuera del territorio nacional. En ellas se realizan trámites, se proporciona asistencia y protección consular, se expiden documentos y se atienden situaciones que, en determinados casos, pueden revestir un carácter urgente y tener consecuencias directas sobre la vida, la integridad, la identidad o la situación jurídica de las personas.

La prestación de estos servicios enfrenta, además, condiciones particulares. La dispersión geográfica de la población mexicana en el exterior, el volumen de solicitudes, las diferencias lingüísticas, los horarios y las circunstancias extraordinarias en las que frecuentemente se requiere asistencia consular demandan mecanismos de atención que permitan aprovechar de mejor manera la capacidad institucional disponible.

La Secretaría de Relaciones Exteriores ha avanzado en la incorporación de herramientas digitales para facilitar la atención de las personas usuarias. Entre estas acciones se encuentran mecanismos de orientación y gestión remota que permiten ampliar los canales de contacto con las representaciones mexicanas. Este proceso de modernización administrativa constituye una base sobre la cual, en su caso, pueden desarrollarse herramientas de inteligencia artificial destinadas a apoyar determinadas tareas consulares. No obstante, la incorporación de estas tecnologías no debe entenderse como una sustitución de la función pública ni de la responsabilidad que corresponde a las personas servidoras públicas encargadas de la prestación de los servicios consulares. Por el contrario, su utilización debe concebirse como un instrumento auxiliar para mejorar la capacidad de respuesta institucional, particularmente en aquellas actividades susceptibles de ser apoyadas mediante procesos automatizados, sin trasladar a un sistema tecnológico la responsabilidad de adoptar determinaciones que correspondan a la autoridad.

De ahí que resulte pertinente establecer en la Ley del Servicio Exterior Mexicano un marco jurídico específico que determine los principios y límites bajo los cuales podrán utilizarse sistemas de inteligencia artificial en los servicios consulares. La ausencia de reglas sectoriales no debe ser entendida como una prohibición para la innovación tecnológica, sino como una oportunidad para que ésta se incorpore de manera ordenada, gradual y compatible con las obligaciones constitucionales y legales que rigen la actuación del Estado mexicano.

La presente iniciativa parte, por tanto, de una premisa fundamental: la modernización de los servicios consulares debe tener como finalidad fortalecer la protección y atención de las personas mexicanas en el exterior, y no sustituir la responsabilidad de la autoridad ni limitar el ejercicio de sus derechos.

Bajo esta consideración, se propone incorporar en la Ley del Servicio Exterior Mexicano disposiciones específicas que permitan a la Secretaría de Relaciones Exteriores utilizar sistemas de inteligencia artificial como herramientas de apoyo en

aquellas actividades en las que puedan generar beneficios para la prestación del servicio, al tiempo que se establecen salvaguardas frente a los riesgos derivados de su utilización.

La regulación propuesta busca generar certeza tanto para las personas usuarias como para las propias instituciones y quienes integran el Servicio Exterior Mexicano. Se pretende, así, que la incorporación de nuevas tecnologías no dependa exclusivamente de decisiones administrativas o de desarrollos tecnológicos particulares, sino que se encuentre vinculada a principios jurídicos que permitan delimitar responsabilidades, establecer mecanismos de supervisión y garantizar que cualquier actuación apoyada en inteligencia artificial permanezca sujeta al marco constitucional y legal aplicable.

II. Evolución del debate legislativo y necesidad de una regulación sectorial

La discusión legislativa en torno a la inteligencia artificial ha adquirido una dimensión creciente en el Congreso de la Unión. El interés por establecer reglas que permitan aprovechar sus beneficios y, al mismo tiempo, prevenir afectaciones a los derechos de las personas, ha dado lugar a diversas propuestas de carácter general y sectorial.

Entre ellas se encuentra la iniciativa presentada el 27 de febrero de 2024 por el entonces senador Ricardo Monreal Ávila, mediante la cual se planteó expedir una Ley Federal que Regula la Inteligencia Artificial¹; asimismo, en el Senado de la República se han desarrollado trabajos encaminados a la construcción de un ordenamiento de carácter general que establezca principios y reglas para el desarrollo y utilización de estas tecnologías en el país.

La Cámara de Diputados tampoco ha permanecido ajena a este proceso. Durante la presente Legislatura se han presentado propuestas orientadas a establecer un marco jurídico para el desarrollo ético y tecnológico de la inteligencia artificial, así como

¹ https://infosen.senado.gob.mx/sgsp/gaceta/65/3/2024-04-02-1/assets/documentos/Inic_Morena_Sen_Monreal_Ley_Fed_Inteligencia_Artificial_02042024.pdf

iniciativas que buscan atender sus efectos en materias específicas, entre ellas los derechos de autor, las relaciones laborales, la protección de las personas frente a contenidos generados artificialmente y la seguridad en el entorno digital². A ello se suman propuestas dirigidas a fortalecer las facultades del Congreso de la Unión en materia de tecnologías de la información y comunicación, así como diversos planteamientos relacionados con la ciberseguridad y la utilización responsable de nuevas tecnologías.

Este conjunto de trabajos revela que el Poder Legislativo se encuentra frente a una materia en proceso de construcción normativa. No obstante, la amplitud de la discusión general no elimina la necesidad de atender aquellos ámbitos de la función pública que, por la naturaleza de sus atribuciones y de las personas a quienes sirven, requieren previsiones específicas. La función consular constituye uno de ellos.

En efecto, los servicios consulares no se agotan en la realización de trámites administrativos. Comprenden actividades vinculadas con la protección y asistencia de personas mexicanas en el extranjero, la expedición de documentación, el registro de determinados actos del estado civil, la atención de situaciones de vulnerabilidad y, en general, el ejercicio de funciones mediante las cuales el Estado mantiene una presencia institucional frente a sus nacionales fuera del territorio.

Por esa razón, la eventual utilización de inteligencia artificial en este ámbito no puede sujetarse únicamente a criterios de eficiencia tecnológica. Cualquier herramienta que intervenga en la recepción de información, prevalidación documental, orientación, identificación de posibles irregularidades o gestión de solicitudes debe operar dentro de un marco que preserve la responsabilidad de la autoridad y garantice los derechos de las personas usuarias.

La necesidad de una regulación sectorial adquiere mayor relevancia si se considera que una legislación general sobre inteligencia artificial, aun cuando establezca

² <https://www.observatorio-ia-mexico.com/proceso-legislativo>

principios aplicables a todas las autoridades y sectores, no necesariamente podrá atender las particularidades de la función consular. La distancia geográfica respecto del territorio nacional, la diversidad de contextos jurídicos en los países de acreditación, la atención de personas en situación de emergencia y la obligación permanente de brindar protección a los nacionales mexicanos exigen reglas que respondan a esas circunstancias.

Por otra parte, la ausencia de una regulación específica tampoco debe conducir a que el desarrollo tecnológico del servicio consular quede sujeto exclusivamente a disposiciones administrativas, contratos tecnológicos o criterios internos cuya naturaleza puede modificarse con el tiempo. La incorporación de herramientas con capacidad para procesar información personal, generar recomendaciones o intervenir en la atención de las personas requiere un fundamento jurídico que establezca, desde la ley, los límites de su utilización y las responsabilidades que corresponden a la autoridad.

La presente propuesta no pretende anticiparse ni sustituir los trabajos que el Congreso de la Unión desarrolla para establecer un marco general en materia de inteligencia artificial. Su propósito es distinto y complementario: incorporar en la Ley del Servicio Exterior Mexicano las reglas mínimas que permitan orientar su utilización dentro de la función consular, atendiendo a la naturaleza especializada de ésta y a las obligaciones que el Estado mexicano tiene respecto de sus nacionales en el exterior.

De esta manera, la regulación sectorial que se propone podrá coexistir con un eventual ordenamiento general en la materia, sujetándose a sus principios y disposiciones y atendiendo, cuando corresponda, las particularidades propias de los servicios consulares. Con ello se evita generar un régimen aislado y, al mismo tiempo, se previene que la incorporación de estas tecnologías avance en un ámbito particularmente sensible sin contar con salvaguardas jurídicas expresas.

La oportunidad de legislar en esta materia no deriva únicamente del desarrollo acelerado de la inteligencia artificial. Surge, sobre todo, de la necesidad de asegurar

que la transformación tecnológica de los servicios consulares se produzca bajo parámetros de legalidad, responsabilidad pública y respeto irrestricto a los derechos humanos. El Estado mexicano no debe esperar a que la utilización de estas herramientas genere controversias o afectaciones para establecer las reglas que deberán observarse; corresponde al legislador anticipar los riesgos razonablemente previsibles y construir, desde ahora, las condiciones jurídicas para una innovación responsable.

III. Fundamento constitucional

La presente iniciativa encuentra sustento, en primer término, en el artículo 1º de la Constitución Política de los Estados Unidos Mexicanos, conforme al cual todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos. Esta obligación adquiere particular relevancia cuando el Estado incorpora herramientas tecnológicas a la prestación de servicios públicos, pues la innovación administrativa no modifica la naturaleza de las obligaciones constitucionales de la autoridad ni puede constituirse en una vía para disminuir el nivel de protección reconocido a las personas.

En materia consular, dicho mandato se proyecta sobre una población que se encuentra fuera del territorio nacional y que, precisamente por esa circunstancia, puede enfrentar condiciones de vulnerabilidad distintas a las que se presentan dentro de México. La utilización de sistemas de inteligencia artificial en la atención de personas mexicanas en el exterior debe, por ello, observar los principios de universalidad, interdependencia, indivisibilidad y progresividad de los derechos humanos, así como la prohibición de toda forma de discriminación. No se trata únicamente de que una herramienta tecnológica sea eficiente; su empleo por una autoridad mexicana debe ser compatible con el deber de garantizar un servicio público accesible, digno y jurídicamente controlable.

El artículo 16 constitucional constituye, a su vez, uno de los principales referentes para la regulación que se propone. La protección de los datos personales y el derecho a la privacidad adquieren especial importancia frente a sistemas capaces de procesar información de identificación, documentación oficial, datos biométricos y demás

elementos que pueden encontrarse en los expedientes y trámites consulares. El hecho de que determinada información sea procesada mediante una herramienta tecnológica no releva a la autoridad de observar los principios y obligaciones que derivan de la Constitución y de la legislación aplicable en materia de protección de datos personales³.

De igual manera, el principio de legalidad exige que las actuaciones de la administración pública encuentren fundamento en normas previamente establecidas y que las personas puedan conocer las reglas bajo las cuales se desarrolla la actuación de la autoridad. Esta exigencia resulta particularmente significativa cuando intervienen sistemas automatizados, puesto que la incorporación de una herramienta tecnológica no puede generar una zona exenta de responsabilidad administrativa ni permitir que una determinación de la autoridad resulte inexplicable únicamente porque en su elaboración intervino un sistema informático.

La propuesta también guarda relación con el artículo 6º constitucional, particularmente en lo concerniente al derecho de acceso a la información y a la protección de los datos personales. La transparencia en el uso institucional de sistemas de inteligencia artificial debe entenderse de manera compatible con las restricciones legítimas derivadas de la seguridad, la protección de datos personales y aquella información cuya divulgación pueda afectar las funciones del Estado. En consecuencia, el deber de transparencia que se propone no supone hacer públicos códigos fuente, información de seguridad o datos cuya difusión se encuentre legalmente restringida, sino establecer condiciones que permitan conocer qué herramientas utiliza la autoridad, con qué finalidad y bajo qué reglas generales se encuentran sujetas a supervisión.

Por su parte, el artículo 8º constitucional reconoce el derecho de petición y establece la obligación de la autoridad de recaer un acuerdo escrito a las solicitudes formuladas en los términos previstos por la propia norma. La utilización de herramientas

³ <https://www.scjn.gob.mx/sites/default/files/cpeum/documento/cpeum.pdf>

tecnológicas para facilitar la recepción, clasificación u orientación de las solicitudes no puede alterar esta garantía ni convertir la interacción con un sistema automatizado en un sustituto de la respuesta que corresponde a la autoridad. La tecnología podrá auxiliar en la gestión, pero la responsabilidad institucional permanece en quien legalmente debe ejercerla.

El artículo 17 constitucional aporta otro elemento relevante al establecer el derecho a una justicia pronta, completa e imparcial. Si bien la prestación de servicios consulares no constituye, en sentido estricto, una función jurisdiccional, el mandato constitucional de garantizar mecanismos institucionales eficaces y accesibles guarda correspondencia con la finalidad de reducir obstáculos innecesarios para que las personas puedan ejercer sus derechos. Bajo esta perspectiva, la utilización responsable de herramientas tecnológicas puede contribuir a disminuir tiempos de espera, orientar a las personas usuarias y facilitar el acceso a los servicios, siempre que su empleo no introduzca nuevas barreras ni sustituya las garantías que corresponden a la actuación humana.

En el ámbito específico de las relaciones exteriores, el artículo 89, fracción X, de la Constitución establece los principios normativos que deben orientar la conducción de la política exterior y reconoce expresamente la protección de los mexicanos en el extranjero como uno de ellos. Esta previsión constitucional otorga una dimensión particular a la función consular: la atención de las personas mexicanas fuera del país no constituye exclusivamente una actividad administrativa, sino una manifestación concreta de la responsabilidad del Estado mexicano de proteger a sus nacionales en el exterior.

A su vez, el artículo 90 constitucional dispone las bases de organización de la Administración Pública Federal, dentro de la cual corresponde a las dependencias del Ejecutivo ejercer las atribuciones que les confieren la Constitución y las leyes. En este marco se inscribe la actuación de la Secretaría de Relaciones Exteriores y, particularmente, la del Servicio Exterior Mexicano como cuerpo permanente del

Estado encargado de representar al país y cumplir las funciones que el orden jurídico le encomienda en el exterior.

La facultad legislativa del Congreso de la Unión deriva de sus atribuciones constitucionales en materia de organización y funcionamiento de la Administración Pública Federal, así como de las competencias que corresponden al Estado mexicano en materia de política exterior y servicio exterior. El establecimiento de reglas para el uso de herramientas tecnológicas dentro de la prestación de servicios consulares forma parte de esa potestad de configuración legislativa, en tanto determina las condiciones jurídicas bajo las cuales una dependencia de la Administración Pública Federal podrá desarrollar y utilizar instrumentos destinados a mejorar el cumplimiento de funciones que le han sido legalmente conferidas.

Finalmente, el artículo 133 constitucional obliga a que toda actuación de las autoridades se ajuste a la Constitución, a las leyes que de ella emanen y a los tratados internacionales celebrados por el Estado mexicano que se encuentren de acuerdo con la misma. Esta disposición adquiere particular importancia tratándose de servicios consulares, cuya prestación se desarrolla necesariamente en un contexto internacional y se encuentra vinculada con las obligaciones que México ha asumido en materia de derechos humanos, protección consular, igualdad y no discriminación.

De esta manera, el fundamento constitucional de la reforma no descansa en la incorporación de la tecnología como un fin en sí mismo. Su razón jurídica se encuentra en la posibilidad de emplear nuevas herramientas para fortalecer una función estatal ya existente, bajo condiciones que aseguren que la innovación administrativa permanezca subordinada a la Constitución, a los derechos humanos y a la responsabilidad que corresponde a las autoridades mexicanas. La inteligencia artificial puede contribuir a hacer más eficiente la prestación de los servicios consulares; lo que no puede hacer es desplazar las obligaciones constitucionales de quienes tienen a su cargo cumplirlos.

IV. Fundamento convencional e instrumentos internacionales

La actuación del Estado mexicano en el exterior se encuentra sujeta no sólo al orden constitucional interno, sino también a las obligaciones internacionales que México ha asumido. Esta consideración resulta especialmente relevante en materia consular, pues las personas destinatarias de estos servicios se encuentran bajo la protección de instituciones mexicanas que desarrollan sus funciones fuera del territorio nacional, en un contexto en el que convergen el derecho interno, las obligaciones internacionales del Estado y las disposiciones del país receptor.

En este ámbito, la Convención de Viena sobre Relaciones Consulares de 1963 constituye el referente convencional fundamental. Su artículo 5 establece entre las funciones consulares la protección de los intereses del Estado que envía y de sus nacionales, así como la prestación de ayuda y asistencia a éstos⁴. Si bien dicho instrumento fue adoptado en una época anterior al desarrollo de las tecnologías que hoy nos ocupan, sus disposiciones no impiden que los Estados modernicen los medios mediante los cuales cumplen sus funciones. Por el contrario, la utilización de nuevas herramientas debe permanecer subordinada a la finalidad esencial de la función consular: brindar protección y asistencia efectiva a las personas nacionales.

Esta consideración adquiere especial importancia cuando la tecnología interviene en procesos relacionados con la identidad, la documentación, la comunicación con las autoridades o la atención de una persona que requiere asistencia. La incorporación de herramientas tecnológicas puede modificar los medios empleados por la autoridad, pero no modifica las obligaciones que ésta tiene frente a las personas. La innovación, por tanto, no constituye una fuente autónoma de facultades ni puede utilizarse para restringir derechos reconocidos por el orden jurídico⁵.

En materia de derechos humanos, la Declaración Universal de Derechos Humanos proporciona un marco de referencia indispensable. Los principios de igualdad y no

⁴ <https://www.oas.org/legal/spanish/documentos/convvienaconsulares.htm>

⁵ <https://www.sitios.scjn.gob.mx/cec/sites/default/files/publication/documents/2025-08/JusticiayTecnologia.pdf>

discriminación, así como el reconocimiento de los derechos que corresponden a toda persona sin distinción, adquieren particular relevancia ante la posibilidad de que determinados procedimientos tecnológicos reproduzcan sesgos o generen resultados diferenciados que no encuentren una justificación objetiva y razonable⁶.

El Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos refuerzan esta obligación. El Estado mexicano debe garantizar los derechos reconocidos en dichos instrumentos sin distinción alguna y asegurar la existencia de recursos efectivos frente a actos que puedan vulnerarlos. En consecuencia, cuando una herramienta tecnológica sea empleada como apoyo en la prestación de un servicio consular, las personas usuarias deberán conservar la posibilidad real de acudir ante una autoridad competente, solicitar la revisión de una determinación y hacer valer los medios de defensa que correspondan.

La Convención Americana adquiere una dimensión adicional en el contexto de esta iniciativa, debido a que sus disposiciones sobre igualdad ante la ley y protección judicial obligan a que las diferencias en el acceso o tratamiento de las personas por parte de las autoridades tengan una justificación legítima y sean compatibles con los derechos reconocidos por el propio instrumento. De ello se desprende que la utilización de herramientas tecnológicas en los servicios consulares no puede traducirse en una forma indirecta de discriminación por nacionalidad, origen étnico, género, edad, discapacidad, condición migratoria, idioma o cualquier otra condición protegida⁷.

A estas obligaciones se suma la protección internacional de la vida privada y de los datos personales. El tratamiento de información vinculada con la identidad, documentación, situación familiar, datos biométricos o circunstancias particulares de las personas mexicanas que acuden ante una representación consular exige que las herramientas empleadas por el Estado observen criterios de necesidad,

⁶ <https://www.un.org/es/about-us/universal-declaration-of-human-rights>

⁷ <https://www.corteidh.or.cr/tablas/17229a.pdf>

proporcionalidad, seguridad y finalidad legítima. El carácter sensible de buena parte de la información que se genera en los procedimientos consulares impone una especial diligencia a la autoridad responsable de su tratamiento.

Junto con los instrumentos jurídicamente vinculantes, la comunidad internacional ha desarrollado principios y directrices específicamente orientados al uso responsable de la inteligencia artificial. Entre ellos destaca la Recomendación sobre la Ética de la Inteligencia Artificial, adoptada por la UNESCO en 2021, que propone un marco centrado en los derechos humanos, la dignidad de las personas, la transparencia, la supervisión humana, la responsabilidad y la prevención de daños⁸. Por su naturaleza, este instrumento no sustituye las obligaciones derivadas de la Constitución ni de los tratados internacionales; constituye, sin embargo, un referente internacional relevante para orientar el diseño de políticas públicas y marcos regulatorios nacionales.

En términos semejantes, los Principios de la Organización para la Cooperación y el Desarrollo Económicos sobre Inteligencia Artificial han destacado la necesidad de que estos sistemas sean utilizados de manera compatible con los valores democráticos, los derechos humanos y el Estado de derecho, además de sujetarse a criterios de transparencia, seguridad y responsabilidad⁹. Tales principios resultan particularmente pertinentes para el sector público, en el que el uso de herramientas tecnológicas debe encontrarse vinculado al cumplimiento de una función estatal y no exclusivamente a objetivos de eficiencia.

El desarrollo de estos estándares internacionales permite advertir una tendencia común: la utilización de inteligencia artificial por parte de los poderes públicos debe conservar un vínculo verificable con la responsabilidad humana. No basta, por ello, con que un sistema produzca resultados técnicamente eficientes; cuando éstos puedan incidir en los derechos de una persona, debe existir una autoridad

⁸ https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

⁹ <https://oecd.ai/en/ai-principles>

responsable de supervisar su utilización, valorar sus resultados y, cuando corresponda, apartarse de ellos.

Esta perspectiva encuentra además respaldo en los desarrollos regulatorios internacionales más recientes. El Reglamento (UE) 2024/1689, conocido como Reglamento de Inteligencia Artificial de la Unión Europea, establece un sistema diferenciado de obligaciones en función del nivel de riesgo que presentan los distintos usos de esta tecnología¹⁰. Aunque sus disposiciones no resultan aplicables al Estado mexicano, constituyen un referente de derecho comparado de especial interés por haber trasladado al ámbito normativo principios como la supervisión humana, la gestión de riesgos, la transparencia y la protección de los derechos fundamentales.

De igual manera, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho¹¹ representa un desarrollo relevante del derecho internacional contemporáneo al vincular expresamente la gobernanza de estas tecnologías con la protección de los derechos humanos y el funcionamiento de las instituciones democráticas. Su valor para la presente propuesta no deriva de su aplicación directa al orden jurídico mexicano, sino de la consolidación de una tendencia internacional que reconoce que la innovación tecnológica y la protección de los derechos no son objetivos incompatibles, siempre que el desarrollo y utilización de estas herramientas se sometan a controles jurídicos adecuados.

La revisión de estos instrumentos permite sostener que México no parte de cero. Existe ya un conjunto de obligaciones convencionales y estándares internacionales que proporcionan elementos suficientes para orientar una regulación nacional responsable. Lo que corresponde al legislador es trasladar esos principios al ámbito concreto en el que habrán de operar, atendiendo a las características propias del

¹⁰ https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

¹¹ <https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-80706>

Servicio Exterior Mexicano y, particularmente, a la naturaleza de los servicios que las representaciones consulares prestan a las personas mexicanas en el extranjero.

Desde esta perspectiva, la reforma propuesta no pretende incorporar al orden jurídico nacional una regulación extranjera ni conferir carácter obligatorio a instrumentos que no lo tienen. Busca, en cambio, armonizar el desarrollo tecnológico de los servicios consulares con las obligaciones internacionales que ya vinculan al Estado mexicano y aprovechar, como elementos de referencia, los avances que en materia de inteligencia artificial han sido desarrollados en el ámbito internacional.

La regla que debe prevalecer es clara: ninguna innovación tecnológica puede disminuir el nivel de protección que corresponde a las personas en virtud de la Constitución y de los tratados internacionales de los que México es parte. La inteligencia artificial podrá modificar la manera en que se presta un servicio; no puede modificar los derechos de quien lo recibe ni relevar al Estado de la responsabilidad que constitucional y convencionalmente le corresponde.

V. Criterios jurisdiccionales y protección de los derechos frente al uso de nuevas tecnologías

La incorporación de herramientas tecnológicas a las funciones del Estado plantea cuestiones que, aunque son relativamente recientes en su formulación, se encuentran vinculadas con principios jurídicos que cuentan con un amplio desarrollo en el orden constitucional mexicano. La legalidad de la actuación administrativa, la protección de los datos personales, la igualdad, la no discriminación, el debido proceso y la posibilidad de controvertir los actos de autoridad no desaparecen frente a la utilización de nuevas tecnologías. Por el contrario, adquieren una dimensión particular cuando una herramienta informática participa en la formación de una determinación que puede afectar a una persona.

En este sentido, resulta relevante considerar que el Poder Judicial de la Federación ha comenzado a pronunciarse sobre el empleo de inteligencia artificial,

particularmente respecto de las condiciones que deben observarse cuando estas herramientas son utilizadas en actividades relacionadas con la impartición de justicia.

Si bien tales criterios no fueron emitidos específicamente para la función consular, permiten identificar principios jurídicos que resultan útiles para orientar la actuación de las autoridades administrativas ante la incorporación de tecnologías de esta naturaleza.

Entre estos precedentes destaca la tesis publicada en el Semanario Judicial de la Federación el 22 de agosto de 2025, emitida por un Tribunal Colegiado en Materia Civil del Segundo Circuito, cuyo rubro es **“INTELIGENCIA ARTIFICIAL APLICADA EN PROCESOS JURISDICCIONALES. ELEMENTOS MÍNIMOS QUE DEBEN OBSERVARSE PARA SU USO ÉTICO Y RESPONSABLE CON PERSPECTIVA DE DERECHOS HUMANOS”**¹². El criterio parte de la necesidad de que, ante la utilización de estas herramientas, prevalezca una perspectiva de derechos humanos y se mantenga la responsabilidad de la persona juzgadora respecto de las determinaciones adoptadas.

Aunque el criterio referido se encuentra circunscrito al ámbito jurisdiccional y, por tanto, no puede trasladarse mecánicamente a la actividad administrativa, su relevancia para la presente iniciativa radica en un principio que trasciende la materia en la que fue emitido: la utilización de una herramienta tecnológica no desplaza la responsabilidad jurídica de la autoridad que tiene a su cargo la decisión. Esta premisa resulta plenamente pertinente para los servicios consulares, en los que determinadas actuaciones pueden incidir directamente en la situación jurídica o en el ejercicio de derechos de las personas usuarias.

La distinción es particularmente importante. Una herramienta tecnológica puede auxiliar en la clasificación de información, identificar inconsistencias documentales, facilitar la orientación de una persona o contribuir a organizar la demanda de atención;

¹² <https://sjf2.scjn.gob.mx/detalle/tesis/2031640>

pero corresponde a la autoridad determinar el alcance jurídico de la información obtenida y asumir la responsabilidad por la decisión que, en su caso, se adopte.

En la misma línea, el desarrollo jurisprudencial relacionado con la protección de datos personales permite advertir que el tratamiento de información por parte de las autoridades se encuentra sujeto a principios de finalidad, proporcionalidad, seguridad y responsabilidad¹³. Estos principios adquieren una especial dimensión en el ámbito consular, donde pueden recabarse datos de identificación, información familiar, documentación migratoria, elementos biométricos y otros datos cuya utilización indebida podría generar consecuencias particularmente graves para las personas mexicanas en el exterior.

Por ello, la presente propuesta no se limita a reconocer la posibilidad de que la Secretaría de Relaciones Exteriores emplee herramientas tecnológicas. Busca establecer condiciones jurídicas para que dicha utilización pueda ser revisada y, en su caso, cuestionada. La persona usuaria debe conservar la posibilidad de conocer que una herramienta tecnológica intervino en la gestión de su solicitud, solicitar la intervención de una persona servidora pública y obtener una explicación suficiente sobre la determinación que le afecte, en los términos que permita la legislación aplicable.

Este último aspecto guarda relación con el principio de tutela efectiva de los derechos.

La existencia de mecanismos de revisión no constituye un obstáculo para la modernización administrativa; por el contrario, es una condición para que la confianza en las instituciones pueda mantenerse cuando sus procedimientos incorporan tecnologías cuyo funcionamiento puede resultar complejo para las personas usuarias.

La experiencia jurisdiccional permite advertir, asimismo, que la utilización de sistemas tecnológicos exige cautela cuando existe la posibilidad de que reproduzcan sesgos o

¹³ <https://sjf2.scjn.gob.mx/detalle/ejecutoria/32987>

generen resultados diferenciados. En el ámbito consular, esta consideración no es menor. Una herramienta que intervenga en la atención de personas mexicanas en el exterior deberá ser diseñada y supervisada de manera que no produzca consecuencias adversas por razón de origen étnico o nacional, género, edad, discapacidad, idioma, condición migratoria u otra circunstancia protegida por el orden jurídico.

No se propone, por tanto, impedir el empleo de herramientas tecnológicas por el solo hecho de que puedan presentar riesgos. El objetivo es establecer controles adecuados a la naturaleza de las funciones en las que habrán de utilizarse. La respuesta jurídica frente al desarrollo tecnológico no debe ser la prohibición general, sino la definición de responsabilidades, límites y mecanismos de supervisión que permitan distinguir entre los usos que contribuyen a mejorar el servicio y aquellos que pueden comprometer derechos.

Desde esta perspectiva, los criterios judiciales existentes aportan un elemento de especial relevancia para la reforma: la incorporación de inteligencia artificial a una función pública no genera una nueva categoría de autoridad ni transfiere a un sistema tecnológico las atribuciones conferidas legalmente a las personas servidoras públicas. La responsabilidad continúa siendo institucional y humana.

Esta premisa permite establecer una diferencia sustancial entre utilizar la tecnología para facilitar el cumplimiento de una función y permitir que ésta determine, por sí misma, el ejercicio de un derecho. La primera posibilidad puede contribuir a una administración pública más eficiente; la segunda requiere controles reforzados y, en determinados supuestos, debe encontrarse expresamente excluida.

En consecuencia, la iniciativa propone que cualquier sistema de inteligencia artificial utilizado en los servicios consulares tenga una naturaleza instrumental y se encuentre sometido a supervisión humana efectiva. Cuando su intervención pueda producir consecuencias jurídicas o afectar de manera significativa a una persona, la determinación final deberá corresponder a una persona servidora pública

competente, quien deberá contar con elementos suficientes para revisar el resultado obtenido y apartarse de éste cuando existan razones jurídicas o fácticas que así lo justifiquen.

La regulación propuesta recoge, de esta manera, una preocupación que ya comienza a reflejarse en el ámbito jurisdiccional mexicano: la innovación tecnológica puede incorporarse al ejercicio de las funciones del Estado, pero no puede convertirse en un mecanismo para diluir la responsabilidad de las autoridades ni para reducir las garantías que corresponden a las personas. En materia consular, esta exigencia adquiere un significado especial porque detrás de cada trámite, solicitud de asistencia o documento se encuentra una persona respecto de la cual el Estado mexicano mantiene obligaciones concretas de protección y atención.

VI. Derecho comparado y experiencias internacionales

La incorporación de herramientas tecnológicas a las funciones de atención y gestión migratoria no constituye un fenómeno exclusivo de México. Diversos Estados han recurrido, con distintos alcances y bajo esquemas regulatorios diversos, a sistemas automatizados para facilitar trámites, proporcionar información, analizar documentación y ordenar la atención de solicitudes. La experiencia internacional permite advertir que el debate ya no se centra únicamente en la conveniencia de incorporar tecnología a los servicios públicos, sino en las condiciones bajo las cuales debe hacerlo una autoridad cuando sus actuaciones pueden incidir en los derechos de las personas.

En los Estados Unidos de América se han desarrollado mecanismos tecnológicos para apoyar la gestión de solicitudes de viaje y determinados procedimientos relacionados con la movilidad internacional. El Sistema Electrónico para la Autorización de Viaje constituye un ejemplo de la utilización de herramientas automatizadas para efectuar una evaluación previa de información proporcionada por las personas solicitantes. Su existencia demuestra la posibilidad de emplear soluciones tecnológicas para atender volúmenes considerables de solicitudes; al mismo tiempo, pone de manifiesto la importancia de establecer mecanismos

institucionales que permitan distinguir entre una herramienta de apoyo y la decisión que corresponde adoptar a la autoridad competente¹⁴.

En el ámbito europeo, el Sistema Europeo de Información y Autorización de Viajes constituye otro referente de interés. Su diseño responde a la necesidad de procesar información de manera anticipada para determinados viajeros y se encuentra vinculado con un entramado normativo que incorpora obligaciones en materia de protección de datos, derechos fundamentales y tratamiento de información. La experiencia europea resulta relevante no porque deba reproducirse en México, sino porque muestra la importancia de acompañar la innovación tecnológica con reglas destinadas a controlar sus efectos y delimitar las responsabilidades institucionales. Australia y Canadá también han incorporado herramientas de procesamiento automatizado en procedimientos relacionados con solicitudes de visado y movilidad internacional¹⁵. En ambos casos, la tecnología ha sido empleada como un mecanismo para administrar grandes cantidades de información y contribuir a la gestión de expedientes. Estas experiencias permiten identificar una utilidad concreta de los sistemas tecnológicos en actividades de naturaleza auxiliar: ordenar información, detectar determinados patrones y apoyar la gestión administrativa, sin que ello implique que la tecnología adquiera por sí misma la titularidad de las atribuciones que corresponden a la autoridad.

España ofrece, por otra parte, una experiencia particularmente cercana a la finalidad que persigue esta iniciativa, en la medida en que se han desarrollado herramientas de asistencia y orientación en materias relacionadas con extranjería y nacionalidad¹⁶. Este tipo de soluciones permite atender consultas frecuentes y facilitar el acceso inicial a información especializada, reduciendo cargas administrativas que pueden

¹⁴ https://www-cbp-gov.translate.google/travel/international-visitors/esta?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

¹⁵ https://www-canada-ca.translate.google/en/immigration-refugees-citizenship/corporate/reports-statistics/evaluations/biometrics-canada-united-states-immigration-information-sharing-initiatives.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

¹⁶ <https://www.inclusion.gob.es/w/migraciones-presenta-los-resultados-de-trayectorias-un-estudio-sobre-la-juventud-espanola-residente-en-el-exterior-y-sus-expectativas-de-retorno>

resolverse mediante orientación básica. Su utilidad radica precisamente en complementar la atención profesional y no en sustituirla.

Las experiencias referidas permiten extraer una conclusión común: el mayor aprovechamiento de las nuevas tecnologías en los servicios vinculados con movilidad internacional se produce cuando éstas se destinan a tareas claramente delimitadas, cuentan con objetivos verificables y permanecen sujetas a mecanismos de control.

La eficiencia administrativa, por sí sola, no constituye una justificación suficiente para utilizar cualquier herramienta o para extender su intervención a decisiones que puedan afectar derechos.

También resulta necesario considerar el reverso de esta transformación. La expansión de herramientas de inteligencia artificial ha generado nuevas modalidades de fraude y suplantación de identidad que pueden afectar precisamente a las personas que buscan asistencia o información de las autoridades. La utilización de sistemas capaces de reproducir imágenes, voces o formas de comunicación institucional ha incrementado la dificultad para distinguir entre una comunicación oficial y aquella generada por terceros con fines ilícitos.

Esta circunstancia adquiere especial importancia para México debido al tamaño de su comunidad residente en el exterior y a la amplitud de su red de representaciones.

La protección de las personas mexicanas no puede limitarse a responder una vez que se ha producido un fraude; también debe comprender medidas preventivas que permitan identificar los canales oficiales, verificar la autenticidad de las comunicaciones y reducir los espacios que puedan ser aprovechados por quienes pretendan hacerse pasar por servidores públicos.

De ahí que el derecho comparado resulte útil no sólo para identificar herramientas que podrían mejorar la prestación de los servicios consulares, sino también para reconocer los riesgos que acompañan su utilización. Una política pública responsable en esta materia debe considerar ambos aspectos. El Estado que incorpora tecnología

para agilizar un trámite también debe contar con mecanismos suficientes para preservar la seguridad de la información, proteger la identidad institucional y evitar que las personas usuarias queden expuestas a nuevas formas de engaño.

Ahora bien, ninguna de las experiencias señaladas puede trasladarse de manera automática al orden jurídico mexicano. Las facultades de las autoridades, la estructura administrativa, el régimen de protección de datos personales, los medios de defensa y las obligaciones constitucionales de nuestro país responden a un sistema propio. El derecho comparado proporciona elementos de referencia, pero corresponde al legislador determinar cuáles de ellos resultan compatibles con las instituciones nacionales y cuáles requieren una adaptación sustantiva.

En ese sentido, la presente iniciativa adopta una posición deliberadamente prudente.

No pretende establecer un modelo basado en la automatización de las decisiones consulares ni reproducir esquemas extranjeros de evaluación o control migratorio. La propuesta se concentra en aquellas funciones en las que el uso de herramientas tecnológicas puede fortalecer la capacidad de atención de las representaciones mexicanas: orientación, gestión de citas, prevalidación documental, apoyo en la detección de posibles irregularidades, traducción y generación de información para la planeación del servicio.

La diferencia es sustancial. Mientras algunos modelos internacionales emplean sistemas automatizados como parte de procesos de autorización o control migratorio, la propuesta que se somete a consideración de esta soberanía coloca en el centro la función de protección y asistencia consular. La tecnología se concibe como un medio para facilitar el cumplimiento de esa función, no como una instancia adicional de decisión frente a las personas mexicanas.

Por ello, el referente internacional que debe guiar esta reforma no es la automatización por sí misma, sino la construcción de mecanismos que permitan aprovechar sus beneficios sin desdibujar la responsabilidad de la autoridad. La

experiencia de otros países demuestra que es posible utilizar herramientas tecnológicas en servicios vinculados con la movilidad y la atención consular; el orden constitucional mexicano exige, además, que su incorporación se realice con pleno respeto a los derechos humanos, a la protección de los datos personales y a las garantías de legalidad.

El derecho comparado, en consecuencia, aporta una lección que resulta pertinente para esta reforma: la modernización de los servicios públicos adquiere legitimidad cuando la tecnología se encuentra al servicio de las personas y permanece sometida al derecho. Sobre esa base debe construirse cualquier incorporación de inteligencia artificial al Servicio Exterior Mexicano.

VII. Dimensión de la población mexicana en el exterior y retos de la atención consular

La dimensión de la población mexicana que reside fuera del territorio nacional obliga a considerar la función consular desde una perspectiva que trasciende la prestación ordinaria de trámites administrativos. México es, por su propia realidad demográfica y migratoria, un país cuya comunidad nacional se encuentra distribuida más allá de sus fronteras. De acuerdo con información presentada por el Instituto de Mexicanas y Mexicanos en el Exterior, aproximadamente 11.7 millones de personas nacidas en México residían en el extranjero, principalmente en los Estados Unidos de América; a esta población se suman alrededor de 13.5 millones de personas nacidas en el extranjero que corresponden a la primera generación y aproximadamente 12 millones de segunda y posteriores generaciones¹⁷.

Estas cifras adquieren una dimensión particular a partir de la evolución constitucional del concepto de nacionalidad. Las reformas de 1997 y, posteriormente, de 2021 ampliaron los supuestos para el reconocimiento de la nacionalidad mexicana de personas nacidas fuera del territorio nacional. En consecuencia, la relación entre el Estado mexicano y su población en el exterior ya no puede analizarse exclusivamente

¹⁷ https://www.datos.gob.mx/dataset/poblacion_mexicana_exterior

a partir de quienes emigraron desde México. La comunidad mexicana fuera del territorio comprende también a generaciones nacidas en otros países que mantienen un vínculo jurídico con México y que, en determinados momentos de su vida, pueden requerir documentación, registro, asistencia o protección consular.

La magnitud de esta población tiene una expresión concreta en la demanda de servicios. Tan sólo en los Estados Unidos de América, donde México mantiene su red consular más amplia, durante 2025 se expidieron 1,295,181 pasaportes mexicanos, además de otros documentos y servicios relacionados con poderes notariales, registro civil, salud, educación financiera y atención a grupos en situación de vulnerabilidad¹⁸.

El dato anterior no representa una actividad aislada. Revela la escala cotidiana de una red institucional que debe atender simultáneamente trámites documentales, solicitudes de asistencia, casos de protección y situaciones que pueden requerir una intervención inmediata. La propia Cámara de Diputados reconoció, al analizar el Presupuesto de Egresos de la Federación para 2025, la necesidad de fortalecer los recursos destinados al programa de Atención, Protección, Servicios y Asistencia Consular de los Mexicanos en el Exterior, al plantear un incremento de 300 millones de pesos y señalar particularmente la dimensión de la red consular mexicana en Estados Unidos, integrada por 50 consulados.

La discusión presupuestaria constituye, en sí misma, un indicador institucional que no debe soslayarse. Para el ejercicio fiscal 2025 se contemplaron inicialmente 524.2 millones de pesos para el Programa Presupuestario E002, correspondiente a la atención, protección, servicios y asistencia consulares, monto que representaba una disminución de 9.8 por ciento respecto del ejercicio anterior, de acuerdo con la

¹⁸ <https://embamex.sre.gob.mx/eua/index.php/es/comunicados/105-comunicados-2026/2041-los-consulados-de-mexico-en-estados-unidos-servicio-proteccion-y-cooperacion-que-fortalece-la-relacion-bilateral>

documentación presentada ante la Comisión de Relaciones Exteriores de la Cámara de Diputados¹⁹.

En estas condiciones, la modernización tecnológica adquiere una dimensión adicional. No se trata de incorporar herramientas digitales por una consideración meramente instrumental, sino de explorar mecanismos que permitan ampliar la capacidad de atención de las representaciones sin trasladar a la tecnología aquellas funciones que, por su naturaleza, exigen valoración y responsabilidad de una persona servidora pública.

La necesidad de aprovechar mejor los recursos institucionales se hace todavía más evidente cuando se observa que la demanda consular no es homogénea. Existen trámites que pueden ser orientados mediante información estandarizada, solicitudes que requieren únicamente una revisión preliminar y procesos que admiten mecanismos de gestión remota; pero también existen casos de protección que involucran personas detenidas, situaciones de violencia, pérdida de documentos, emergencias, niñas, niños y adolescentes, personas en situación de vulnerabilidad o circunstancias que requieren comunicación inmediata con autoridades del país de residencia. La tecnología puede contribuir a separar y ordenar estas necesidades, pero no puede determinar por sí misma el tratamiento jurídico que corresponda a cada caso²⁰.

El propio Gobierno de México dispone actualmente de herramientas digitales destinadas a facilitar la relación de las personas mexicanas con las autoridades consulares. La plataforma Mi Consulado concentra servicios relacionados con pasaportes, menaje de casa, registro civil, visas, agenda de citas, ubicación de consulados y protección a personas mexicanas en el exterior; asimismo, ofrece mecanismos de contacto para casos de emergencia y orientación²¹.

¹⁹

https://www.pef.hacienda.gob.mx/work/models/GOp25P/PEF2025/Loungbqw/docs/05/r05_epr.pdf

²⁰ <https://www.gob.mx/sre/prensa/servicios-con-calidad-y-eficiencia-prioridad-de-la-secretaria-de-relaciones-exteriores-canciller-de-la-fuente>

²¹ <https://www.miconsulado.sre.gob.mx>

A ello se suma el Sistema de Registro para Mexicanos en el Exterior, concebido como un mecanismo para facilitar la comunicación entre el Gobierno de México y sus nacionales durante estancias o residencias fuera del país.²² La existencia de estas herramientas demuestra que la transformación digital de los servicios consulares no constituye una hipótesis futura: se trata de un proceso que ya forma parte de la relación cotidiana entre las instituciones mexicanas y la población que atienden.

El siguiente paso, por tanto, no debe consistir en incorporar indiscriminadamente nuevas tecnologías, sino en establecer las condiciones jurídicas que permitan determinar cuándo, para qué y bajo qué controles pueden emplearse sistemas con capacidades más avanzadas de procesamiento de información. La diferencia es sustancial. Una plataforma para solicitar una cita o consultar los requisitos de un trámite cumple una función distinta de un sistema capaz de analizar información, formular recomendaciones o identificar patrones que puedan influir en la actuación de una autoridad.

Existe, además, un elemento demográfico que exige considerar la accesibilidad como parte de la política consular. La población mexicana en el exterior no constituye un grupo uniforme: comprende personas de distintas edades, niveles educativos, capacidades, condiciones socioeconómicas y contextos culturales. A ello se agregan diferencias lingüísticas y diversos grados de acceso y familiaridad con las herramientas digitales. Una estrategia de modernización que únicamente trasladara los servicios a medios tecnológicos podría generar nuevas barreras en lugar de reducirlas.

Los datos disponibles sobre migración internacional muestran también la complejidad de los procesos que conducen a la residencia de mexicanos fuera del país. La ENADID 2023 estimó que, entre la población de cinco años y más que residía en

²² <https://embamex.sre.gob.mx/suecia/index.php/es/avisos/600-sistema-de-registro-para-mexicanos-en-el-exterior>

México, 419,443 personas habían vivido en otro país en agosto de 2018; de ellas, 72.5 por ciento había residido en los Estados Unidos de América. La misma encuesta registró que, entre las personas que migraron a Estados Unidos, 40.6 por ciento declaró haber ingresado sin documento en 2023, frente a 27.0 por ciento en 2018²³.

Estos indicadores no significan que todas esas personas requieran asistencia consular, ni permiten por sí mismos cuantificar la demanda de los consulados. Su relevancia para esta iniciativa es distinta: muestran que la movilidad internacional de la población mexicana ocurre bajo circunstancias diversas y que la interacción con las instituciones consulares puede producirse en contextos jurídicos y personales muy diferentes. Por ello, cualquier herramienta tecnológica que intervenga en la prestación del servicio deberá diseñarse bajo criterios de accesibilidad, seguridad y proporcionalidad, evitando que una clasificación automatizada o un procedimiento uniforme desconozca las particularidades del caso concreto.

La dimensión de la tarea consular debe analizarse, además, a la luz de la distribución territorial de la población mexicana. La red de representaciones constituye un mecanismo permanente de presencia institucional y de vinculación con comunidades que se encuentran a miles de kilómetros del territorio nacional. En esas circunstancias, reducir tiempos de atención, mejorar la gestión de información y anticipar necesidades operativas puede tener un valor significativo, particularmente cuando se trata de situaciones de emergencia o de alta demanda.

Por ello, la incorporación regulada de herramientas de inteligencia artificial puede contribuir a que el personal consular concentre una mayor proporción de su tiempo y capacidad profesional en aquellas actuaciones que requieren criterio, sensibilidad y responsabilidad jurídica. La finalidad no sería disminuir la importancia del servidor público, sino precisamente reservar su intervención para aquellas decisiones en las que la valoración humana resulta indispensable, mientras que las tareas susceptibles de apoyo tecnológico puedan realizarse con mayor oportunidad y consistencia.

²³ <https://www.inegi.org.mx/programas/enadid/2023/>

La evidencia disponible conduce, así, a una conclusión de política pública: México cuenta con una población nacional de dimensión transterritorial, una red consular de considerable amplitud y una demanda de servicios que involucra tanto trámites ordinarios como situaciones de protección. Al mismo tiempo, las instituciones ya han iniciado un proceso de digitalización de la atención. El reto legislativo consiste en acompañar esa transformación con reglas que permitan aprovechar sus beneficios sin comprometer los derechos de las personas ni diluir la responsabilidad de la autoridad.

La presente iniciativa responde a esa necesidad. No parte de la premisa de que la tecnología pueda resolver por sí misma las dificultades de la atención consular. Parte de una realidad más concreta: cuando la demanda de servicios públicos crece, los recursos institucionales son necesariamente limitados y las herramientas digitales ya forman parte de la prestación del servicio, corresponde al legislador establecer las condiciones para que su utilización sea jurídicamente segura, socialmente útil y compatible con la obligación constitucional de proteger a las personas mexicanas en el exterior.

VIII. Riesgos y desafíos asociados al uso de inteligencia artificial en los servicios consulares

La incorporación de sistemas de inteligencia artificial a los servicios consulares ofrece posibilidades relevantes para mejorar la gestión de información, ordenar la demanda, agilizar determinadas tareas y ampliar los canales de atención. Sin embargo, su utilización introduce riesgos que no pueden ser tratados como cuestiones exclusivamente técnicas. Cuando los datos procesados por un sistema se encuentran vinculados con la identidad, nacionalidad, situación familiar, condición migratoria o circunstancias personales de quien solicita un servicio consular, un error de diseño, de información o de interpretación puede trascender el ámbito informático y producir consecuencias jurídicas para una persona.

Uno de los principales desafíos se encuentra en la calidad de los datos. Un sistema no genera información confiable por el solo hecho de emplear técnicas sofisticadas de procesamiento. Sus resultados dependen, entre otros factores, de la integridad, actualidad, representatividad, consistencia y pertinencia de los datos utilizados. Si la información de entrada contiene errores, registros incompletos, duplicidades o patrones históricos que reflejan desigualdades, el resultado obtenido puede reproducirlos e incluso amplificarlos²⁴.

Esta cuestión adquiere especial importancia en materia consular. Los registros utilizados para apoyar una determinada gestión pueden provenir de momentos distintos, contener diferencias en la forma de capturar nombres o documentos, responder a sistemas informáticos diversos o presentar información que requiere actualización. En consecuencia, antes de utilizar cualquier sistema que procese estos datos deberá existir certeza razonable sobre su calidad y sobre la finalidad específica para la cual fueron recabados.

La trazabilidad constituye otro elemento indispensable. Una decisión administrativa apoyada en una herramienta tecnológica debe poder reconstruirse en términos suficientes para conocer qué información fue utilizada, qué sistema intervino, cuál fue su función dentro del procedimiento y qué persona servidora pública tuvo a su cargo la valoración final. Sin esta posibilidad, la autoridad enfrentaría dificultades para explicar su actuación y las personas afectadas encontrarían mayores obstáculos para cuestionarla²⁵.

No se trata de exigir que cada persona usuaria conozca el funcionamiento matemático de un algoritmo. La exigencia jurídica es distinta: debe existir una cadena de responsabilidad identificable. Desde la perspectiva de la administración pública, un sistema que participa en un procedimiento no puede convertirse en un punto ciego

²⁴ <https://sre.gob.mx/images/stories/marconormativodoc/dof130710.pdf>

²⁵ <https://openknowledge.fao.org/items/ce5d9fab-376c-46ad-89a5-9149d3cf3133>

en el que desaparezcan los datos de entrada, los criterios de operación y la responsabilidad institucional.

Los sesgos en los datos y en los modelos de procesamiento constituyen, asimismo, un riesgo que merece atención legislativa. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO advierte que estas tecnologías pueden reproducir o exacerbar sesgos existentes y generar efectos discriminatorios, desigualdad, brechas digitales y exclusión. El mismo instrumento plantea la necesidad de que los sistemas sean sometidos a mecanismos de evaluación, supervisión y rendición de cuentas²⁶.

En el ámbito consular, un sesgo puede manifestarse de formas menos evidentes que una decisión abiertamente discriminatoria. Puede encontrarse, por ejemplo, en la selección de los datos utilizados para entrenar o validar un sistema, en la manera en que se clasifican determinadas solicitudes, en la ponderación de variables o en la existencia de grupos que se encuentran insuficientemente representados en los datos disponibles. Por ello, la ausencia de una intención discriminatoria no resulta suficiente para descartar el riesgo.

De ahí la importancia de que los sistemas destinados a apoyar la función consular sean sometidos a pruebas de validación y desempeño antes de su puesta en operación y durante su funcionamiento. La evaluación no debe limitarse a determinar si el sistema produce resultados técnicamente correctos; también debe examinar su comportamiento frente a distintos grupos de usuarios, la frecuencia de errores, la consistencia de sus resultados y la existencia de efectos adversos que no hubieran sido previstos inicialmente.

La supervisión tampoco puede agotarse en el momento de adquisición o implementación de una herramienta. Los sistemas pueden modificar su comportamiento cuando cambian los datos, los procedimientos administrativos, los

²⁶ <https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence>

criterios jurídicos o las condiciones en las que son utilizados. Por ello, la evaluación debe entenderse como un proceso continuo y no como un requisito único que se satisface antes de poner en funcionamiento una aplicación.

Este enfoque coincide con los principios internacionales de gestión de riesgos. La UNESCO ha señalado la necesidad de evaluar los sistemas durante su ciclo de vida, garantizar su trazabilidad y establecer mecanismos de supervisión, auditoría y evaluación de impacto; por su parte, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos ha desarrollado un marco de gestión de riesgos de inteligencia artificial orientado a identificar, evaluar y administrar los riesgos que estas tecnologías pueden generar para las personas, las organizaciones y la sociedad²⁷.

Otro aspecto que merece especial atención es la seguridad de la información. Los sistemas empleados en los servicios consulares podrían concentrar o procesar grandes cantidades de información personal y documental. Una vulneración de sus mecanismos de seguridad no tendría únicamente consecuencias patrimoniales o administrativas; podría comprometer identidades, documentos, datos de contacto, información familiar o circunstancias personales de quienes recurren a una representación mexicana²⁸.

La dimensión transfronteriza de la función consular añade complejidad al problema. La información puede ser capturada en una representación ubicada en un país extranjero, procesada mediante infraestructura tecnológica localizada en otro territorio o administrada por proveedores tecnológicos sujetos a distintas jurisdicciones. Esta circunstancia obliga a establecer controles claros respecto del acceso, almacenamiento, transferencia, conservación y eliminación de la información, de conformidad con la legislación mexicana aplicable y con las obligaciones internacionales correspondientes.

²⁷ https://unesdoc.unesco.org/ark:/48223/pf0000127207_spa

²⁸ <https://www.sitios.scjn.gob.mx/cec/editorial/derecho-la-notificacion-contacto-y-asistencia-consular>

También debe considerarse el riesgo de automatización indebida. La eficiencia que puede ofrecer un sistema constituye precisamente una de las razones por las cuales una autoridad podría sentirse inclinada a confiar en sus resultados. Sin embargo, una tasa elevada de aciertos no convierte automáticamente al sistema en titular de una facultad jurídica. En asuntos donde una persona pueda sufrir una afectación relevante, la validación humana no debe reducirse a una aprobación mecánica de lo que la herramienta propone.

La diferencia entre asistencia y decisión debe quedar claramente delimitada. Un sistema puede señalar que determinados datos presentan inconsistencias; puede ordenar solicitudes de acuerdo con parámetros previamente establecidos; puede sugerir información que facilite la orientación de una persona usuaria. Lo que no debe hacer, por sí mismo, es convertir una correlación estadística en una determinación jurídica.

Esta distinción resulta particularmente importante frente al denominado sesgo de automatización, entendido como la tendencia de las personas a confiar en exceso en resultados producidos por sistemas tecnológicos, incluso cuando existen elementos que aconsejan revisarlos. En una oficina consular, una recomendación generada por un sistema podría adquirir una apariencia de objetividad que no necesariamente corresponde con la calidad de los datos o con las particularidades del caso concreto.

La supervisión humana debe ser, por ello, sustantiva y no meramente formal.

La explicabilidad plantea un desafío adicional. No todos los sistemas requieren revelar el mismo nivel de información ni resulta jurídicamente procedente exigir la divulgación irrestricta de componentes tecnológicos cuya publicidad pueda comprometer la seguridad de una infraestructura. Pero sí debe garantizarse que la persona pueda conocer, en términos comprensibles, cuándo una herramienta tecnológica intervino en la gestión de su asunto, cuál fue su función y qué autoridad asumió la responsabilidad por la determinación correspondiente.

Esta exigencia debe armonizarse con otros bienes jurídicamente protegidos. La transparencia no puede significar la exposición de datos personales, secretos comerciales, vulnerabilidades de seguridad o información cuya divulgación se encuentre legalmente restringida. De ahí que la regulación deba establecer un equilibrio entre transparencia, protección de datos, seguridad de la información y rendición de cuentas²⁹.

Existe, finalmente, un riesgo que suele quedar fuera de las discusiones estrictamente tecnológicas: la brecha digital. La modernización de los servicios consulares no puede presumir que todas las personas cuentan con las mismas capacidades para utilizar plataformas digitales, acceso estable a internet o conocimientos suficientes para interactuar con sistemas automatizados. Una política que sustituyera indiscriminadamente la atención humana por canales tecnológicos podría terminar excluyendo precisamente a quienes enfrentan mayores dificultades para acceder a los servicios públicos.

La situación adquiere particular relevancia cuando la persona se encuentra en una condición de vulnerabilidad o enfrenta una emergencia. En estos casos, la posibilidad de comunicarse con una persona servidora pública no debe quedar supeditada a la capacidad del usuario para comprender una interfaz digital o seguir correctamente un procedimiento automatizado.

Por otra parte, los sistemas de inteligencia artificial pueden convertirse en objetivos de ataques destinados a alterar datos, manipular resultados, extraer información o inducir al sistema a generar respuestas incorrectas. En consecuencia, la seguridad debe ser considerada desde el diseño y durante todo el periodo en que la herramienta permanezca en operación. No resulta suficiente proteger la base de datos si el sistema que la consulta puede ser manipulado, ni basta con proteger la aplicación si las credenciales y mecanismos de acceso carecen de controles adecuados.

²⁹ <https://www.plataformadetransparencia.org.mx/preguntas-frecuentes>

La gestión de estos riesgos exige, por tanto, una aproximación basada en gobernanza de datos y gestión del ciclo de vida del sistema. La autoridad debe conocer qué información utiliza, con qué propósito, durante cuánto tiempo la conserva, quién puede acceder a ella, cómo se documentan los cambios realizados al sistema, qué mecanismos existen para detectar errores y qué procedimiento debe seguirse cuando se identifica un comportamiento anómalo³⁰.

El objetivo de la regulación no debe ser construir un esquema burocrático que haga inviable la innovación. Se trata de establecer controles proporcionales al riesgo. No tendría sentido imponer las mismas exigencias a una herramienta destinada exclusivamente a responder preguntas frecuentes que a un sistema utilizado para analizar información cuya valoración pueda incidir de manera significativa en la situación de una persona.

Esta diferenciación permitirá que la Secretaría de Relaciones Exteriores pueda aprovechar las ventajas de la tecnología sin convertir la innovación en un fin en sí mismo. La intensidad de la supervisión, las pruebas de validación, los controles de seguridad y las obligaciones de documentación deberán guardar correspondencia con la naturaleza de la función desarrollada, la sensibilidad de los datos tratados y el posible impacto de los resultados.

La evidencia internacional converge en una premisa que resulta particularmente pertinente para esta reforma: los riesgos de la inteligencia artificial no pueden gestionarse exclusivamente después de que se produce un daño. La prevención requiere identificar desde el diseño los posibles puntos de falla, establecer indicadores de desempeño, documentar decisiones, monitorear resultados y conservar mecanismos efectivos para corregir el funcionamiento del sistema. La propia UNESCO vincula la protección de datos, la evaluación de impacto, la

³⁰ https://unesdoc.unesco.org/ark:/48223/pf0000394518_spa

trazabilidad, la supervisión humana y la rendición de cuentas como elementos de una gestión responsable de estas tecnologías³¹.

En consecuencia, la regulación propuesta debe partir de una lógica de prevención, proporcionalidad y responsabilidad. La inteligencia artificial puede ser un instrumento útil para ampliar la capacidad de respuesta de las representaciones mexicanas; pero cuanto mayor sea su capacidad para procesar información o incidir en un procedimiento, mayores deberán ser las exigencias de validación, supervisión y control.

El desafío legislativo consiste, precisamente, en establecer ese punto de equilibrio. México no necesita una regulación que cierre la puerta al desarrollo tecnológico, pero tampoco una que permita incorporar sistemas de alta complejidad sin conocer sus fuentes de información, sus márgenes de error, sus condiciones de operación y las consecuencias que pueden derivarse de sus resultados. En los servicios consulares, donde una decisión puede afectar directamente a una persona mexicana que busca protección o asistencia del Estado, **la eficiencia tecnológica debe estar subordinada a la certeza jurídica, la protección de los derechos y la responsabilidad de la autoridad.**

IX. Propuesta legislativa y principios que deben regir la utilización de inteligencia artificial en los servicios consulares

La realidad expuesta permite advertir que la incorporación de herramientas de inteligencia artificial al Servicio Exterior Mexicano no debe quedar circunscrita a decisiones administrativas aisladas ni depender exclusivamente de la evolución de las capacidades tecnológicas disponibles. Cuando una herramienta puede intervenir en la atención de las personas, procesar información personal o auxiliar en actividades propias de una representación consular, su utilización debe encontrarse sujeta a reglas que otorguen certeza a la autoridad y, al mismo tiempo, salvaguarden los derechos de quienes recurren a ella.

³¹ <https://www.unesco.org/es/artificial-intelligence/recommendation-ethics>

La presente iniciativa propone, por ello, reconocer expresamente en la Ley del Servicio Exterior Mexicano la posibilidad de que la Secretaría de Relaciones Exteriores utilice sistemas de inteligencia artificial como instrumentos auxiliares para el cumplimiento de sus funciones consulares. El reconocimiento legal de esta facultad no pretende conferir a dichos sistemas atribuciones propias de la autoridad. Su finalidad es establecer un marco jurídico que permita aprovechar las posibilidades que ofrece la tecnología sin alterar la distribución de competencias prevista en el ordenamiento.

La diferencia no es menor. La autoridad podrá servirse de una herramienta tecnológica para realizar determinadas tareas con mayor rapidez o precisión; pero el ejercicio de una atribución pública continuará correspondiendo a quien tenga competencia legal para ejercerla. En ningún caso la existencia de un sistema automatizado podrá interpretarse como una delegación de facultades que la ley no autorice.

El primer principio que debe orientar este régimen es el de supervisión humana efectiva. La intervención de una persona servidora pública no debe reducirse a validar mecánicamente el resultado producido por un sistema. Cuando la utilización de la inteligencia artificial pueda incidir de manera relevante en los derechos o intereses de una persona, deberá existir una revisión que permita valorar las circunstancias concretas del caso, identificar posibles errores y, cuando proceda, apartarse del resultado obtenido mediante la herramienta tecnológica.

La responsabilidad administrativa y jurídica deberá permanecer, en consecuencia, plenamente identificada. Ninguna determinación podrá justificarse exclusivamente bajo el argumento de que fue generada o recomendada por un sistema. La autoridad que adopte una decisión será responsable de verificar que ésta encuentre fundamento en la Constitución, en las leyes aplicables y en las circunstancias acreditadas en el expediente correspondiente.

Otro elemento esencial será el principio de finalidad. Los sistemas de inteligencia artificial no podrán utilizarse de manera genérica o indeterminada respecto de la información que obre en poder de las representaciones consulares. Toda herramienta deberá responder a una finalidad concreta, legítima y previamente definida, de manera que exista correspondencia entre los datos que se procesan y la función pública para la cual fueron recabados.

Este principio adquiere particular relevancia cuando se trate de información personal.

El hecho de que una autoridad tenga legítimamente acceso a determinados datos no significa que pueda utilizarlos para cualquier propósito tecnológico. El tratamiento deberá sujetarse a las disposiciones constitucionales y legales en materia de protección de datos personales, así como a los principios que rigen su obtención, utilización, conservación y, en su caso, supresión.

La iniciativa incorpora también el principio de proporcionalidad. No toda actividad consular requiere el mismo nivel de intervención tecnológica y no todo sistema presenta los mismos riesgos. Por ello, la regulación debe permitir que las medidas de control correspondan a la naturaleza de la herramienta, al tipo de información procesada y a las consecuencias que pudieran derivarse de sus resultados.

Así, una herramienta destinada exclusivamente a proporcionar información general sobre los requisitos de un trámite no puede recibir el mismo tratamiento jurídico que aquella que procese información personal para formular una recomendación susceptible de influir en una actuación de la autoridad. La regulación debe distinguir estas situaciones y evitar tanto la ausencia de controles como la imposición de cargas innecesarias a aplicaciones de bajo riesgo.

La igualdad y la no discriminación constituyen igualmente límites infranqueables. Ningún sistema podrá ser diseñado, implementado o utilizado de manera que produzca un trato diferenciado injustificado entre las personas usuarias de los servicios consulares. Para ello, no bastará con revisar las reglas formales del sistema;

deberán considerarse también los datos utilizados, los criterios de procesamiento y los resultados que genere en la práctica.

La prevención de la discriminación deberá acompañarse de mecanismos de revisión.

Cuando se detecte que una herramienta produce resultados sistemáticamente desfavorables para determinado grupo de personas, la autoridad deberá contar con facultades y procedimientos para suspender su utilización, corregir sus parámetros o sustituirla, según corresponda. Una vez identificado un comportamiento contrario al marco jurídico, la permanencia del sistema no puede justificarse por el solo hecho de que su implementación haya requerido recursos públicos.

La transparencia deberá entenderse de manera compatible con la protección de la información. Las personas usuarias tienen derecho a conocer, en términos accesibles, cuándo una herramienta de inteligencia artificial participa en la gestión de un servicio, cuál es su finalidad y qué autoridad conserva la responsabilidad sobre el procedimiento. Esta obligación no implica revelar información técnica cuya divulgación pueda comprometer la seguridad del sistema, ni hacer públicos datos personales o información protegida por la legislación.

La propuesta contempla asimismo la trazabilidad de las actuaciones apoyadas por inteligencia artificial. La Secretaría de Relaciones Exteriores deberá contar con mecanismos que permitan identificar los sistemas utilizados, las finalidades para las que fueron autorizados, las modificaciones relevantes que hayan experimentado y las personas servidoras públicas responsables de su operación y supervisión. En aquellos casos en que la herramienta intervenga de manera significativa en un procedimiento, deberá existir constancia suficiente de su participación.

La trazabilidad cumple una función jurídica concreta: permite reconstruir la actuación administrativa. Sin ella, la revisión posterior de un procedimiento puede resultar insuficiente y la determinación de responsabilidades puede verse obstaculizada. La

autoridad debe encontrarse en condiciones de explicar qué hizo, con qué información lo hizo y quién asumió la decisión correspondiente.

La seguridad de la información constituye otro componente indispensable del régimen propuesto. Los sistemas que procesen información relacionada con personas mexicanas en el exterior deberán contar con medidas de protección acordes con la naturaleza de los datos y con los riesgos asociados a su tratamiento. La seguridad deberá abarcar tanto la infraestructura tecnológica como los mecanismos de acceso, administración, conservación y eliminación de la información.

No menos importante será establecer una obligación de evaluación previa y periódica. Antes de poner en operación un sistema cuyo funcionamiento pueda generar efectos relevantes sobre las personas, la autoridad deberá determinar sus posibles riesgos y establecer las medidas necesarias para prevenirlos. Esa valoración no puede considerarse definitiva: deberá revisarse cuando se modifique el sistema, cambie la finalidad para la que fue implementado o se adviertan resultados que hagan necesaria una nueva evaluación.

La experiencia demuestra que ningún sistema tecnológico permanece inalterable.

Cambian los datos, las necesidades institucionales, los procedimientos administrativos y las condiciones en las que se utiliza. Por ello, la evaluación debe acompañar al sistema durante su ciclo de operación y no limitarse a la etapa previa a su adquisición.

La iniciativa reconoce, además, el derecho de revisión humana como una garantía indispensable. Cuando una persona considere que la utilización de una herramienta tecnológica ha incidido de manera adversa en la atención de su solicitud, deberá contar con la posibilidad de solicitar la intervención de una persona servidora pública competente, en los términos que establezca la legislación aplicable. La existencia de

esta vía no supone desconocer los procedimientos administrativos vigentes; busca asegurar que la automatización no cierre las puertas de la atención institucional.

Debe quedar igualmente excluida cualquier interpretación conforme a la cual los sistemas de inteligencia artificial puedan adoptar por sí mismos decisiones que impliquen el ejercicio de facultades reservadas a las autoridades. La tecnología puede auxiliar; la atribución legal sólo puede ejercerse por quien se encuentre facultado para ello.

Este límite resulta particularmente necesario en materia consular. Las circunstancias que rodean a una persona que solicita asistencia no siempre pueden ser reducidas a variables susceptibles de procesamiento automatizado. Existen casos en los que la valoración de elementos humanos, familiares, culturales o de vulnerabilidad resulta indispensable para determinar la forma adecuada de intervención institucional. Una herramienta tecnológica puede aportar información; difícilmente puede sustituir el juicio profesional que exige una situación de esta naturaleza.

La regulación propuesta pretende, asimismo, preservar la continuidad del servicio público. La eventual falla de un sistema, la imposibilidad de acceder a una plataforma o la detección de una anomalía en sus resultados no deberá traducirse en la suspensión de la atención consular. Las representaciones deberán mantener mecanismos alternativos que permitan atender a las personas cuando la vía tecnológica no sea adecuada o no se encuentre disponible.

Con ello se evita que la digitalización se convierta en una nueva barrera de acceso.

La modernización debe ampliar las posibilidades de atención, no condicionarlas exclusivamente a la disponibilidad de un dispositivo, una conexión a internet o la capacidad de una persona para utilizar una plataforma determinada.

Finalmente, el modelo propuesto se sustenta en un criterio de responsabilidad pública. La Secretaría de Relaciones Exteriores deberá establecer las reglas internas

necesarias para determinar qué sistemas pueden utilizarse, para qué funciones, bajo qué condiciones y con qué mecanismos de supervisión. La regulación legal deberá proporcionar el marco general, pero su aplicación tendrá que desarrollarse mediante procedimientos administrativos, protocolos técnicos y mecanismos de evaluación que puedan actualizarse conforme evolucione la tecnología.

La iniciativa busca, en suma, establecer una relación equilibrada entre innovación y derecho. No pretende frenar la incorporación de herramientas que pueden mejorar la capacidad de atención del Estado mexicano, pero tampoco acepta que la velocidad del desarrollo tecnológico determine por sí misma los límites de la actuación pública.

El principio rector debe ser sencillo: la inteligencia artificial podrá fortalecer los servicios consulares en la medida en que permanezca subordinada a la ley, a los derechos humanos y a la responsabilidad de las autoridades mexicanas. Bajo esta premisa, la tecnología deja de ser un riesgo que deba enfrentarse únicamente mediante restricciones y se convierte en una herramienta cuyo valor dependerá de la forma en que el Estado decida gobernarla.

X. Impacto legislativo y viabilidad de la propuesta

La reforma que se plantea parte de una premisa sencilla: la inteligencia artificial ya forma parte de la transformación tecnológica de las instituciones públicas y su incorporación a los servicios consulares no puede quedar al margen de la ley. Lo que corresponde al legislador es establecer las condiciones para que esa incorporación ocurra de manera ordenada, responsable y compatible con el régimen de derechos que protege a las personas mexicanas en el exterior.

La propuesta no modifica las atribuciones sustantivas de la Secretaría de Relaciones Exteriores ni altera la estructura del Servicio Exterior Mexicano. Tampoco crea una nueva autoridad para la gestión de los servicios consulares. Lo que hace es reconocer un instrumento que puede ser utilizado para apoyar funciones que ya se encuentran conferidas a las autoridades competentes y, a partir de ese reconocimiento, fijar límites que otorguen certeza tanto a la administración como a las personas usuarias.

Esta precisión resulta necesaria porque la utilización de una herramienta tecnológica no equivale al ejercicio de una atribución pública. Un sistema puede procesar información, identificar coincidencias, ordenar solicitudes o proporcionar una recomendación; la facultad para decidir continúa perteneciendo a la autoridad que la ley determine. No existe, por tanto, transferencia de competencia hacia el sistema ni posibilidad de que una decisión administrativa encuentre su única justificación en el resultado producido por una máquina.

La responsabilidad debe permanecer identificada.

Cuando una actuación pueda producir consecuencias relevantes para una persona, deberá existir una persona servidora pública que conozca el asunto, valore la información disponible y responda jurídicamente por la determinación adoptada. La inteligencia artificial podrá proporcionar elementos para esa valoración, pero no sustituirla. Éste es uno de los límites que la reforma considera indispensables.

La propuesta también resulta compatible con el régimen constitucional y legal de protección de datos personales. El reconocimiento del uso de inteligencia artificial no constituye una autorización abierta para recopilar información ni para utilizarla con finalidades distintas de aquellas que justificaron su obtención. Cada tratamiento deberá encontrar sustento en una finalidad determinada y sujetarse a los principios y obligaciones previstos en la legislación aplicable.

Esta consideración adquiere particular importancia en materia consular. La información que obra en una representación mexicana puede referirse a identidad, nacionalidad, vínculos familiares, documentación, domicilio, situación migratoria, circunstancias de vulnerabilidad y otros aspectos de la vida privada. Que esos datos se encuentren legítimamente en poder de la autoridad no significa que puedan ser empleados sin límites para alimentar cualquier sistema tecnológico.

La iniciativa adopta, por ello, un criterio de proporcionalidad. No sería razonable someter una herramienta destinada exclusivamente a proporcionar información general sobre los requisitos de un trámite a las mismas exigencias que deberían aplicarse a un sistema capaz de analizar información personal y formular recomendaciones que puedan influir en una actuación administrativa.

La regulación debe atender al riesgo real.

Una herramienta de bajo impacto podrá sujetarse a controles acordes con su función; aquellas que procesen información sensible o intervengan en procedimientos con posibles consecuencias para las personas deberán enfrentar mayores exigencias de evaluación, seguridad, supervisión y documentación. Esta diferenciación permite proteger derechos sin convertir la regulación en un obstáculo innecesario para la innovación.

La igualdad y la no discriminación constituyen límites que tampoco pueden quedar sujetos a la conveniencia tecnológica. Los sistemas utilizados por las representaciones consulares deberán ser revisados para evitar que sus datos, parámetros o formas de operación produzcan resultados que coloquen injustificadamente a determinadas personas o grupos en una situación de desventaja.

No basta, para estos efectos, con verificar que el código de un sistema no contenga una regla expresamente discriminatoria. Los resultados también deben ser observados. Si una herramienta comienza a producir patrones de error o de trato diferenciado que no encuentran una justificación objetiva, la autoridad deberá contar con mecanismos para corregirla, limitar su uso o suspenderla.

La transparencia debe seguir una lógica semejante. La persona que utiliza un servicio consular debe poder saber, en términos comprensibles, si una herramienta de inteligencia artificial intervino en la atención de su asunto y cuál fue la función que desempeñó. No se propone revelar información técnica cuya divulgación pudiera comprometer la seguridad de los sistemas, pero tampoco resulta admisible que la

utilización de una herramienta tecnológica permanezca completamente oculta cuando ésta haya tenido una intervención relevante.

Junto con la transparencia debe existir trazabilidad.

La autoridad debe encontrarse en posibilidad de reconstruir la actuación: identificar qué sistema intervino, para qué finalidad fue utilizado, qué información procesó en los términos jurídicamente permitidos y qué persona servidora pública asumió la decisión. No se trata de generar cargas documentales innecesarias, sino de conservar los elementos indispensables para revisar posteriormente una actuación administrativa y, en su caso, determinar responsabilidades.

La seguridad de la información constituye otra condición de viabilidad. Los sistemas destinados a apoyar los servicios consulares no podrán operar al margen de las políticas institucionales de seguridad ni generar nuevos puntos de exposición que comprometan la información de las personas mexicanas. Los controles deberán comprender los accesos, la infraestructura, la transmisión, el almacenamiento y la eliminación de los datos, de acuerdo con la naturaleza de la información y el riesgo asociado.

La implementación, además, deberá ser gradual.

No todas las representaciones consulares enfrentan las mismas condiciones operativas ni tienen idénticas necesidades. Tampoco todas las herramientas tecnológicas ofrecen el mismo beneficio ni presentan los mismos riesgos. Pretender una incorporación simultánea y uniforme no sólo sería innecesario; podría dificultar la evaluación de resultados y elevar los costos de una eventual corrección.

La Secretaría de Relaciones Exteriores podrá comenzar por aquellas aplicaciones cuya utilidad institucional sea susceptible de medirse y cuyos riesgos puedan mantenerse bajo control. Los resultados obtenidos deberán servir para determinar si una herramienta debe ampliarse, modificarse o descartarse. La innovación pública

requiere también capacidad para reconocer cuándo una solución tecnológica no está funcionando como se esperaba.

Este modelo supone necesariamente capacitación. La incorporación de inteligencia artificial no termina con la adquisición de una plataforma. Quienes deban utilizarla necesitan conocer sus alcances, identificar sus limitaciones y advertir cuándo un resultado requiere revisión. De poco serviría establecer una obligación de supervisión humana si, en la práctica, el personal careciera de elementos para cuestionar aquello que el sistema presenta como resultado.

La transformación tecnológica debe acompañarse, entonces, de fortalecimiento institucional. La persona servidora pública no pierde relevancia frente a la tecnología; cambia la naturaleza de algunas de las herramientas con las que desempeña su función. La responsabilidad de interpretar, valorar y decidir permanece en ella.

Desde el punto de vista presupuestario, la reforma no crea por sí misma órganos administrativos, unidades nuevas ni plazas adicionales. Tampoco obliga a la Secretaría a adquirir una plataforma específica o a incorporar inmediatamente sistemas de inteligencia artificial en toda su red consular.

Ello no significa desconocer que la implementación tendrá costos. La capacitación, las adecuaciones tecnológicas, las evaluaciones, las medidas de seguridad y, en su caso, contratación de servicios especializados deberán atenderse con cargo a los recursos que correspondan, conforme a las disponibilidades presupuestarias y a las disposiciones aplicables. La diferencia consiste en que la ley no impone una erogación inmediata ni predetermina una solución tecnológica cuyo costo hoy no puede conocerse con precisión.

La reforma tampoco genera una duplicidad de competencias. La Secretaría de Relaciones Exteriores conservará las atribuciones que actualmente tiene y deberá coordinar, cuando corresponda, las acciones relacionadas con protección de datos personales, seguridad de la información y demás materias vinculadas con el uso de

estas herramientas. El propósito es articular capacidades, no crear estructuras paralelas.

Existe, además, un beneficio legislativo que conviene destacar. Establecer estas reglas desde ahora permite evitar que la evolución tecnológica avance sin un referente jurídico específico dentro de los servicios consulares. La ley no puede anticipar qué herramienta será utilizada dentro de cinco o diez años, pero sí puede determinar qué principios deberán respetarse cualquiera que sea la tecnología disponible.

Esa es precisamente la ventaja de una regulación basada en principios y responsabilidades. Permite que la norma conserve vigencia frente a cambios tecnológicos sin renunciar a límites jurídicos claros.

La propuesta es, por tanto, susceptible de implementarse de manera progresiva, dentro de las atribuciones existentes y mediante los instrumentos administrativos que correspondan. Su aplicación deberá considerar las capacidades reales de la institución, las condiciones presupuestarias y la evaluación permanente de los resultados.

No se propone una modernización tecnológica a cualquier costo. Tampoco se pretende que la inteligencia artificial resuelva problemas que son, en esencia, institucionales. Se propone algo más concreto: que cuando el Estado mexicano decida utilizar estas herramientas para atender a sus nacionales en el exterior, exista una norma que establezca de antemano las reglas que deberá observar.

La viabilidad de la reforma deriva precisamente de esa naturaleza. No exige sustituir el modelo consular ni modificar las competencias fundamentales del Servicio Exterior Mexicano. Permite incorporar nuevas herramientas dentro de la estructura existente, sujetándolas a controles jurídicos y administrativos que hagan posible evaluar sus resultados y corregir sus deficiencias.

El legislador tiene aquí una responsabilidad que no puede posponerse indefinidamente. La tecnología seguirá avanzando con independencia de que exista o no una regulación sectorial. Lo que sí puede decidir el Estado es bajo qué condiciones permitirá que esa tecnología intervenga en una función tan estrechamente vinculada con la protección de sus nacionales.

La presente iniciativa busca establecer esas condiciones.

Su propósito final no es automatizar la función consular, sino fortalecerla; no sustituir al servidor público, sino dotarlo de mejores herramientas; no facilitar el tratamiento indiscriminado de información, sino ordenar su utilización; y no colocar a la tecnología por encima de la persona, sino asegurar que permanezca subordinada a la ley y al interés público.

Desde esta perspectiva, la incorporación de inteligencia artificial a los servicios consulares puede representar una oportunidad de modernización institucional. Pero sólo será una verdadera mejora si se traduce en servicios más accesibles, decisiones mejor sustentadas, mayor capacidad de respuesta y una protección más eficaz para las personas mexicanas en el exterior.

Ese es, en última instancia, el sentido de la reforma que se somete a consideración de esta Soberanía.

XI. Conclusión legislativa

La función consular constituye una de las expresiones más directas de la presencia del Estado mexicano frente a sus nacionales que se encuentran fuera del territorio. Su eficacia no se mide únicamente por el número de trámites que puede desahogar una representación, sino por su capacidad para responder, con oportunidad y sentido humano, a las necesidades de quienes acuden a ella. En determinados momentos, esa intervención puede significar la diferencia entre recibir orientación adecuada o permanecer en la incertidumbre; entre acceder oportunamente a un servicio o enfrentar mayores obstáculos para ejercer un derecho.

México se encuentra ante una transformación tecnológica que no puede ser ignorada por el legislador. La inteligencia artificial ofrece herramientas capaces de procesar grandes volúmenes de información, identificar patrones, facilitar tareas administrativas y ampliar los canales mediante los cuales las personas pueden relacionarse con las instituciones públicas. Sus posibilidades son relevantes, pero también lo son los riesgos que acompañan su utilización cuando se trata de información personal y de actuaciones que pueden tener consecuencias jurídicas.

Por esa razón, esta iniciativa no propone adoptar la inteligencia artificial de manera irreflexiva ni convertirla en sustituto de la función consular. Propone establecer reglas.

Que la tecnología pueda utilizarse cuando resulte útil; que su empleo tenga una finalidad definida; que los datos se encuentren protegidos; que sus resultados puedan ser revisados; que existan mecanismos para identificar y corregir errores y, sobre todo, que la responsabilidad de la actuación pública permanezca en manos de las autoridades competentes.

La modernización de los servicios consulares no debe medirse por el grado de automatización que alcancen, sino por la capacidad que tengan para atender mejor a las personas. Una plataforma más sofisticada carecería de sentido si dificulta el acceso de quien necesita asistencia; un sistema capaz de procesar millones de datos perdería toda utilidad si no puede garantizar su integridad y seguridad; y una herramienta que ofrece resultados con rapidez no representa un avance si la autoridad deja de valorar las circunstancias particulares de un caso.

De ahí que la propuesta coloque a la persona en el centro de la transformación tecnológica. La inteligencia artificial debe ser un medio para fortalecer la capacidad institucional, no un mecanismo para diluir responsabilidades. Debe permitir que el personal consular disponga de mejores instrumentos para orientar, atender y proteger, particularmente en aquellos casos en los que la oportunidad de la respuesta puede resultar determinante.

La reforma que se propone también responde a una responsabilidad legislativa de carácter preventivo. Esperar a que la utilización de estas tecnologías se generalice para comenzar a discutir sus límites significaría permitir que las prácticas administrativas se desarrollen antes de contar con un marco jurídico suficientemente claro. El momento adecuado para establecer principios, responsabilidades y salvaguardas es precisamente cuando su incorporación puede todavía realizarse de manera ordenada.

No se trata de legislar sobre una tecnología pasajera. Se trata de establecer las condiciones jurídicas bajo las cuales el Estado mexicano podrá incorporar herramientas tecnológicas cada vez más sofisticadas a una función pública permanente. La regulación debe ser suficientemente firme para proteger derechos y, al mismo tiempo, suficientemente flexible para permitir que las instituciones evolucionen.

Esta Soberanía tiene la oportunidad de acompañar la transformación digital del Servicio Exterior Mexicano con una visión de largo plazo. Una visión que reconozca que la innovación y el derecho no son conceptos contrapuestos y que, cuando se encuentran adecuadamente articulados, pueden contribuir a construir instituciones más eficientes sin sacrificar las garantías que justifican su existencia.

Por las consideraciones anteriormente expuestas, la presente iniciativa busca que la utilización de sistemas de inteligencia artificial en los servicios consulares se desarrolle bajo parámetros de legalidad, responsabilidad, supervisión humana, protección de datos personales, seguridad de la información, transparencia, igualdad y respeto irrestricto de los derechos humanos.

El objetivo es claro: que México avance hacia servicios consulares más modernos, accesibles y capaces de responder a las necesidades de sus nacionales en el exterior, sin permitir que la innovación tecnológica desplace la responsabilidad que corresponde al Estado ni la dignidad que debe reconocerse a cada persona.

Es en esa convicción que se somete a consideración de esta Soberanía el proyecto de decreto que se acompaña, con la certeza de que fortalecer la capacidad tecnológica del Estado mexicano no significa hacer más distante a la autoridad, sino proporcionarle mejores instrumentos para cumplir una de sus responsabilidades esenciales: proteger y atender a las personas mexicanas, dondequiera que se encuentren.

A efecto de tener mayor claridad de la reforma propuesta, se expone el siguiente cuadro comparativo:

LEY DEL SERVICIO EXTERIOR MEXICANO

Texto Vigente	Propuesta de Modificación
Sin correlativo	CAPÍTULO VIII BIS DEL USO RESPONSABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL EN LOS SERVICIOS CONSULARES
Sin correlativo	ARTÍCULO 46 BIS. La Secretaría podrá utilizar sistemas de inteligencia artificial como herramientas auxiliares para la prestación de servicios consulares, la gestión administrativa, la atención y orientación de las personas usuarias y el desarrollo de las demás funciones que correspondan a las oficinas consulares, siempre que su utilización se encuentre vinculada con una finalidad determinada, legítima y compatible con las atribuciones conferidas por esta Ley y demás disposiciones aplicables. La utilización de dichos sistemas se sujetará, en todo momento, a los principios de legalidad, certeza jurídica, proporcionalidad, seguridad, transparencia, responsabilidad, igualdad y no discriminación, protección de datos personales, accesibilidad y respeto a los derechos humanos.

	Los sistemas de inteligencia artificial no conferirán a las oficinas consulares atribuciones distintas de aquellas que les correspondan conforme al marco jurídico aplicable.
Sin correlativo	ARTÍCULO 46 TER. La utilización de sistemas de inteligencia artificial en los servicios consulares tendrá carácter auxiliar. Las decisiones, actos o determinaciones que correspondan a las autoridades consulares continuarán siendo responsabilidad de las personas servidoras públicas competentes. En ningún caso un sistema de inteligencia artificial podrá sustituir el ejercicio de las atribuciones que la Constitución, los tratados internacionales, esta Ley u otras disposiciones jurídicas confieran de manera exclusiva a una autoridad. Cuando el resultado generado por un sistema pueda incidir de manera relevante en los derechos, intereses o situación jurídica de una persona, deberá existir supervisión humana efectiva y suficiente para valorar las circunstancias particulares del caso. La intervención humana deberá ser sustantiva y no podrá reducirse a una validación automática o meramente formal del resultado generado por el sistema.
Sin correlativo	ARTÍCULO 46 QUÁTER. Queda prohibido utilizar sistemas de inteligencia artificial para emitir, por sí mismos, decisiones, resoluciones o determinaciones administrativas individualizadas que tengan por objeto negar, restringir, suspender, cancelar o afectar de manera directa derechos o



	intereses jurídicamente protegidos de las personas usuarias de los servicios consulares. Cuando un sistema de inteligencia artificial genere una recomendación, clasificación, predicción o resultado que pueda servir de apoyo para una determinación de esa naturaleza, la autoridad competente deberá realizar una valoración independiente y fundada del asunto. La persona interesada tendrá derecho a solicitar, en los términos de las disposiciones aplicables, la intervención de una persona servidora pública competente cuando considere que la utilización de un sistema de inteligencia artificial incidió de manera desfavorable en la atención o resolución de su asunto. Lo dispuesto en este artículo se aplicará sin perjuicio de los medios de defensa establecidos en las disposiciones jurídicas correspondientes.
Sin correlativo	ARTÍCULO 46 QUINQUES. Los sistemas de inteligencia artificial utilizados en los servicios consulares deberán diseñarse, seleccionarse, implementarse y operarse de manera que se prevengan resultados discriminatorios o diferenciados injustificadamente por razón de origen étnico o nacional, género, edad, discapacidad, condición social, condición migratoria, lengua, religión, opinión, situación económica, estado civil o cualquier otra condición protegida por el orden jurídico. La Secretaría establecerá mecanismos para identificar, documentar y corregir sesgos o resultados que puedan producir efectos discriminatorios.



	Cuando se advierta que un sistema genera resultados que puedan vulnerar el principio de igualdad y no discriminación, la Secretaría deberá adoptar las medidas necesarias para corregir, limitar o suspender su utilización, según la gravedad y naturaleza del riesgo identificado.
Sin correlativo	ARTÍCULO 46 SEXIES. El tratamiento de datos personales mediante sistemas de inteligencia artificial deberá sujetarse estrictamente a los principios, deberes y obligaciones establecidos en la legislación aplicable en materia de protección de datos personales. La Secretaría deberá garantizar que los datos personales utilizados por estos sistemas sean adecuados, relevantes y proporcionales respecto de las finalidades para las cuales sean tratados. Cuando la utilización o modificación de un sistema implique un tratamiento intensivo o relevante de datos personales, se observarán las obligaciones relativas a la evaluación de impacto en la protección de datos personales previstas en la legislación aplicable. En ningún caso la incorporación de sistemas de inteligencia artificial podrá entenderse como autorización para recopilar, utilizar, conservar o transferir datos personales para finalidades distintas de aquellas que jurídicamente correspondan.
Sin correlativo	ARTÍCULO 46 SEPTIES. La Secretaría establecerá mecanismos de trazabilidad respecto de los sistemas

	de inteligencia artificial que utilice en los servicios consulares. Para tal efecto, deberá contar, cuando resulte técnicamente posible y jurídicamente procedente, con información que permita identificar: I. El sistema utilizado y su finalidad; II. La unidad administrativa o representación consular responsable de su operación; III. La naturaleza de las funciones en las que intervenga; IV. Los mecanismos de supervisión humana aplicables; V. Las modificaciones sustantivas realizadas al sistema, y VI. Los resultados de las evaluaciones o revisiones que correspondan conforme a esta Ley y demás disposiciones aplicables. La información a que se refiere este artículo deberá conservarse durante el plazo que establezcan las disposiciones aplicables y mantenerse disponible para las autoridades competentes cuando resulte necesaria para fines de supervisión, auditoría o determinación de responsabilidades.
Sin correlativo	ARTÍCULO 46 OCTIES. La Secretaría integrará y mantendrá actualizado un registro público de los sistemas de inteligencia artificial utilizados en los servicios consulares. El registro contendrá, al menos: I. La denominación o identificación del sistema; II. La finalidad para la cual se utiliza;

	III. El tipo de función o servicio consular en el que interviene; IV. La unidad administrativa o representación consular responsable; V. La fecha de inicio de operación y, en su caso, de suspensión o conclusión; VI. Las medidas generales de supervisión humana aplicables, y VII. La información que determine la Secretaría en los lineamientos correspondientes. La publicidad de la información se realizará de conformidad con las disposiciones aplicables en materia de transparencia, protección de datos personales, seguridad de la información y protección de la información que legalmente deba reservarse.
Sin correlativo	ARTÍCULO 46 NONIES. La Secretaría establecerá mecanismos de evaluación y revisión periódica de los sistemas de inteligencia artificial utilizados en los servicios consulares, atendiendo a la naturaleza de la función que desempeñen, al tipo de información que procesen y a los riesgos que puedan generar para las personas. Las evaluaciones podrán comprender, entre otros aspectos: I. La precisión, consistencia y confiabilidad de los resultados; II. La existencia de sesgos o resultados discriminatorios; III. El cumplimiento de las finalidades para las cuales fue implementado el sistema; IV. La observancia de las disposiciones en materia de protección de datos personales;

	V. Las medidas de seguridad de la información; VI. La eficacia de los mecanismos de supervisión humana, y VII. La existencia de riesgos que hagan necesaria su modificación, limitación o suspensión. Cuando de las evaluaciones se desprenda la existencia de riesgos que puedan afectar derechos o intereses de las personas, la Secretaría deberá adoptar las medidas correctivas que resulten procedentes.
Sin correlativo	ARTÍCULO 46 DECIES. La Secretaría promoverá la capacitación y actualización del personal que intervenga en la selección, implementación, operación, supervisión o evaluación de sistemas de inteligencia artificial utilizados en los servicios consulares. La capacitación deberá comprender, al menos, aspectos relacionados con el funcionamiento y limitaciones de los sistemas, protección de datos personales, seguridad de la información, identificación de errores o resultados anómalos, prevención de la discriminación y responsabilidades derivadas de su utilización. La Secretaría procurará que la incorporación de estas herramientas se realice de manera gradual y conforme a las capacidades institucionales, necesidades del servicio, disponibilidad presupuestaria y evaluación de los resultados obtenidos.

Por lo anteriormente expuesto y fundado, someto a consideración de esta Soberanía el siguiente:

**DECRETO POR EL QUE SE ADICIONA UN CAPÍTULO VIII BIS, DENOMINADO
DEL USO RESPONSABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL EN
LOS SERVICIOS CONSULARES, INTEGRADO POR LOS ARTÍCULOS 46 BIS,
46 TER, 46 QUÁTER, 46 QUINQUIES, 46 SEXIES, 46 SEPTIES, 46 OCTIES, 46
NONIES Y 46 DECIES, A LA LEY DEL SERVICIO EXTERIOR MEXICANO**

Artículo Único. Se adiciona un Capítulo VIII Bis, denominado “Del uso responsable de sistemas de inteligencia artificial en los servicios consulares”, integrado por los artículos 46 Bis, 46 Ter, 46 Quáter, 46 Quinquies, 46 Sexies, 46 Septies, 46 Octies, 46 Nonies y 46 Decies, a la Ley del Servicio Exterior Mexicano, para quedar como sigue:

CAPÍTULO VIII BIS

**DEL USO RESPONSABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL EN
LOS SERVICIOS CONSULARES**

ARTÍCULO 46 BIS.

La Secretaría podrá utilizar sistemas de inteligencia artificial como herramientas auxiliares para la prestación de servicios consulares, la gestión administrativa, la atención y orientación de las personas usuarias y el desarrollo de las demás funciones que correspondan a las oficinas consulares, siempre que su utilización se encuentre vinculada con una finalidad determinada, legítima y compatible con las atribuciones conferidas por esta Ley y demás disposiciones aplicables.

La utilización de dichos sistemas se sujetará, en todo momento, a los principios de legalidad, certeza jurídica, proporcionalidad, seguridad, transparencia, responsabilidad, igualdad y no discriminación, protección de datos personales, accesibilidad y respeto a los derechos humanos.

Los sistemas de inteligencia artificial no conferirán a las oficinas consulares atribuciones distintas de aquellas que les correspondan conforme al marco jurídico aplicable.

ARTÍCULO 46 TER.

La utilización de sistemas de inteligencia artificial en los servicios consulares tendrá carácter auxiliar. Las decisiones, actos o determinaciones que correspondan a las autoridades consulares continuarán siendo responsabilidad de las personas servidoras públicas competentes.

En ningún caso un sistema de inteligencia artificial podrá sustituir el ejercicio de las atribuciones que la Constitución, los tratados internacionales, esta Ley u otras disposiciones jurídicas confieran de manera exclusiva a una autoridad.

Cuando el resultado generado por un sistema pueda incidir de manera relevante en los derechos, intereses o situación jurídica de una persona, deberá existir supervisión humana efectiva y suficiente para valorar las circunstancias particulares del caso.

La intervención humana deberá ser sustantiva y no podrá reducirse a una validación automática o meramente formal del resultado generado por el sistema.

ARTÍCULO 46 QUÁTER.

Queda prohibido utilizar sistemas de inteligencia artificial para emitir, por sí mismos, decisiones, resoluciones o determinaciones administrativas individualizadas que tengan por objeto negar, restringir, suspender, cancelar o afectar de manera directa derechos o intereses jurídicamente protegidos de las personas usuarias de los servicios consulares.

Cuando un sistema de inteligencia artificial genere una recomendación, clasificación, predicción o resultado que pueda servir de apoyo para una determinación de esa naturaleza, la autoridad competente deberá realizar una valoración independiente y fundada del asunto.

La persona interesada tendrá derecho a solicitar, en los términos de las disposiciones aplicables, la intervención de una persona servidora pública competente cuando considere que la utilización de un sistema de inteligencia artificial incidió de manera desfavorable en la atención o resolución de su asunto.

Lo dispuesto en este artículo se aplicará sin perjuicio de los medios de defensa establecidos en las disposiciones jurídicas correspondientes.

ARTÍCULO 46 QUINQUES.

Los sistemas de inteligencia artificial utilizados en los servicios consulares deberán diseñarse, seleccionarse, implementarse y operarse de manera que se prevengan resultados discriminatorios o diferenciados injustificadamente por razón de origen étnico o nacional, género, edad, discapacidad, condición social, condición migratoria, lengua, religión, opinión, situación económica, estado civil o cualquier otra condición protegida por el orden jurídico.

La Secretaría establecerá mecanismos para identificar, documentar y corregir sesgos o resultados que puedan producir efectos discriminatorios.

Cuando se advierta que un sistema genera resultados que puedan vulnerar el principio de igualdad y no discriminación, la Secretaría deberá adoptar las medidas necesarias para corregir, limitar o suspender su utilización, según la gravedad y naturaleza del riesgo identificado.

ARTÍCULO 46 SEXIES.

El tratamiento de datos personales mediante sistemas de inteligencia artificial deberá sujetarse estrictamente a los principios, deberes y obligaciones establecidos en la legislación aplicable en materia de protección de datos personales.

La Secretaría deberá garantizar que los datos personales utilizados por estos sistemas sean adecuados, relevantes y proporcionales respecto de las finalidades para las cuales sean tratados.

Cuando la utilización o modificación de un sistema implique un tratamiento intensivo o relevante de datos personales, se observarán las obligaciones relativas a la evaluación de impacto en la protección de datos personales previstas en la legislación aplicable.

En ningún caso la incorporación de sistemas de inteligencia artificial podrá entenderse como autorización para recopilar, utilizar, conservar o transferir datos personales para finalidades distintas de aquellas que jurídicamente correspondan.

ARTÍCULO 46 SEPTIES.

La Secretaría establecerá mecanismos de trazabilidad respecto de los sistemas de inteligencia artificial que utilice en los servicios consulares.

Para tal efecto, deberá contar, cuando resulte técnicamente posible y jurídicamente procedente, con información que permita identificar:

- I. El sistema utilizado y su finalidad;
- II. La unidad administrativa o representación consular responsable de su operación;
- III. La naturaleza de las funciones en las que intervenga;
- IV. Los mecanismos de supervisión humana aplicables;
- V. Las modificaciones sustantivas realizadas al sistema, y
- VI. Los resultados de las evaluaciones o revisiones que correspondan conforme a esta Ley y demás disposiciones aplicables.

La información a que se refiere este artículo deberá conservarse durante el plazo que establezcan las disposiciones aplicables y mantenerse disponible para las autoridades competentes cuando resulte necesaria para fines de supervisión, auditoría o determinación de responsabilidades.

ARTÍCULO 46 OCTIES.

La Secretaría integrará y mantendrá actualizado un registro público de los sistemas de inteligencia artificial utilizados en los servicios consulares.

El registro contendrá, al menos:

- I. La denominación o identificación del sistema;
- II. La finalidad para la cual se utiliza;

- III. El tipo de función o servicio consular en el que interviene;
- IV. La unidad administrativa o representación consular responsable;
- V. La fecha de inicio de operación y, en su caso, de suspensión o conclusión;
- VI. Las medidas generales de supervisión humana aplicables, y
- VII. La información que determine la Secretaría en los lineamientos correspondientes.

La publicidad de la información se realizará de conformidad con las disposiciones aplicables en materia de transparencia, protección de datos personales, seguridad de la información y protección de la información que legalmente deba reservarse.

ARTÍCULO 46 NONIES.

La Secretaría establecerá mecanismos de evaluación y revisión periódica de los sistemas de inteligencia artificial utilizados en los servicios consulares, atendiendo a la naturaleza de la función que desempeñen, al tipo de información que procesen y a los riesgos que puedan generar para las personas.

Las evaluaciones podrán comprender, entre otros aspectos:

- I. La precisión, consistencia y confiabilidad de los resultados;
- II. La existencia de sesgos o resultados discriminatorios;
- III. El cumplimiento de las finalidades para las cuales fue implementado el sistema;
- IV. La observancia de las disposiciones en materia de protección de datos personales;
- V. Las medidas de seguridad de la información;
- VI. La eficacia de los mecanismos de supervisión humana, y
- VII. La existencia de riesgos que hagan necesaria su modificación, limitación o suspensión.

Cuando de las evaluaciones se desprenda la existencia de riesgos que puedan afectar derechos o intereses de las personas, la Secretaría deberá adoptar las medidas correctivas que resulten procedentes.

ARTÍCULO 46 DECIES.

La Secretaría promoverá la capacitación y actualización del personal que intervenga en la selección, implementación, operación, supervisión o evaluación de sistemas de inteligencia artificial utilizados en los servicios consulares.

La capacitación deberá comprender, al menos, aspectos relacionados con el funcionamiento y limitaciones de los sistemas, protección de datos personales, seguridad de la información, identificación de errores o resultados anómalos, prevención de la discriminación y responsabilidades derivadas de su utilización.

La Secretaría procurará que la incorporación de estas herramientas se realice de manera gradual y conforme a las capacidades institucionales, necesidades del servicio, disponibilidad presupuestaria y evaluación de los resultados obtenidos.

TRANSITORIOS

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

SEGUNDO. La Secretaría de Relaciones Exteriores deberá emitir, dentro de los ciento ochenta días naturales siguientes a la entrada en vigor del presente Decreto, los lineamientos generales necesarios para su aplicación.

Los lineamientos deberán establecer, al menos, los criterios para la selección, implementación, supervisión, evaluación, registro y, en su caso, suspensión de los sistemas de inteligencia artificial utilizados en los servicios consulares.

TERCERO. La Secretaría de Relaciones Exteriores contará con un plazo de ciento ochenta días naturales, contados a partir de la entrada en vigor del presente Decreto, para integrar el registro público previsto en el artículo 46 Octies de la Ley del Servicio Exterior Mexicano.

CUARTO. Los sistemas de inteligencia artificial que se encuentren en operación en los servicios consulares a la entrada en vigor del presente Decreto deberán ser identificados y sujetos a un proceso de revisión conforme a las disposiciones del mismo.

La Secretaría determinará, atendiendo al nivel de riesgo y a la naturaleza de las funciones en las que intervengan, el plazo y las medidas necesarias para su adecuación al presente Decreto.

QUINTO. Las disposiciones administrativas que se opongan al presente Decreto quedarán sin efectos en lo que corresponda, y aquellas que resulten necesarias para su aplicación deberán adecuarse dentro del plazo previsto en el artículo Segundo Transitorio.

SEXTO. La implementación de las disposiciones previstas en el presente Decreto se realizará con cargo al presupuesto aprobado a la Secretaría de Relaciones Exteriores para el ejercicio fiscal correspondiente, por lo que no implicará, por sí misma, ampliaciones presupuestarias adicionales.

SÉPTIMO. La Secretaría de Relaciones Exteriores deberá presentar anualmente a las comisiones del Congreso de la Unión competentes en materia de relaciones exteriores un informe sobre la implementación y funcionamiento de los sistemas de inteligencia artificial utilizados en los servicios consulares.

El informe deberá contener, al menos, información sobre los sistemas registrados, sus principales finalidades, las evaluaciones realizadas, las medidas correctivas adoptadas y, en su caso, los sistemas cuya utilización haya sido suspendida o modificada.

OCTAVO. La aplicación del presente Decreto deberá realizarse en armonía con las disposiciones constitucionales, los tratados internacionales de los que el Estado mexicano sea parte y la legislación aplicable en materia de protección de datos personales, transparencia, acceso a la información pública, seguridad de la información, responsabilidades administrativas y derechos humanos.

NOVENO. La Secretaría de Relaciones Exteriores deberá considerar, en la implementación de los sistemas de inteligencia artificial, mecanismos que permitan mantener alternativas de atención no automatizada cuando las circunstancias particulares del caso, las condiciones de accesibilidad, la naturaleza del trámite o la indisponibilidad del sistema así lo requieran.

DÉCIMO. La Secretaría de Relaciones Exteriores realizará las acciones necesarias para que los sistemas de inteligencia artificial que se incorporen con posterioridad a la entrada en vigor del presente Decreto sean sometidos, antes de su puesta en operación, a los mecanismos de evaluación y control previstos en la Ley y en las disposiciones administrativas que de ella deriven.

DÉCIMO PRIMERO. El Ejecutivo Federal realizará las adecuaciones reglamentarias necesarias para armonizar el Reglamento de la Ley del Servicio Exterior Mexicano con las disposiciones del presente Decreto dentro de los ciento ochenta días naturales siguientes a su entrada en vigor.

DÉCIMO SEGUNDO. Se derogan todas las disposiciones que se opongan al presente Decreto

ATENTAMENTE



DIP. GISELLE YUNUEEN ARELLANO AVILA

**DADO EN PALACIO LEGISLATIVO DE SAN LÁZARO A 1° DE SEPTIEMBRE DE
2026.**

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA DENOMINACIÓN DEL CAPÍTULO II DEL TÍTULO NOVENO Y SE ADICIONAN UNA FRACCIÓN XVII AL APARTADO A DEL ARTÍCULO 11 BIS Y LOS ARTÍCULOS 211 BIS 8 A 211 BIS 14 AL CÓDIGO PENAL FEDERAL, EN MATERIA DE TIPIFICACIÓN DE CIBERATAQUES Y DELITOS INFORMÁTICOS, EN ARMONIZACIÓN CON LOS ESTÁNDARES INTERNACIONALES EN LA MATERIA

La proponente, **Giselle Yunueen Arellano Ávila**, Diputada Federal del grupo parlamentario MORENA de la LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en el artículo 71, fracción II y 135 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 6, numeral 1, fracción I, 77 y 78 y 82 fracción I del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de decreto por el que se reforma la denominación del Capítulo II del Título Noveno y se adicionan una fracción XVII al apartado A del artículo 11 Bis y los artículos 211 Bis 8 a 211 Bis 14 al Código Penal Federal, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

I. ANTECEDENTES

La protección penal de los sistemas informáticos en el orden jurídico mexicano se remonta al 17 de mayo de 1999, fecha en que se incorporó al Código Penal Federal el Capítulo II del Título Noveno, integrado por los artículos 211 Bis 1 a 211 Bis 7. Dicho ordenamiento tipificó por primera vez el acceso no autorizado a sistemas informáticos y distinguió cuatro categorías de sistema afectado —particular, del Estado, de instituciones financieras y de seguridad pública—, con penas escalonadas de tres meses a diez años de prisión según la categoría y la conducta. En su momento, la reforma constituyó un paso adelante que colocó a México entre los primeros países de la región con un régimen penal específico en materia informática.

El paradigma bajo el cual se construyó ese régimen respondía a la realidad tecnológica propia de finales del siglo XX. Las conductas típicas se articularon en torno a los verbos rectores característicos de aquella etapa —conocer, copiar, modificar, destruir o provocar pérdida de información—, con la premisa de que el bien

jurídico a tutelar era la confidencialidad del contenido almacenado en un equipo determinado. Desde entonces, la operación masiva en la nube, las plataformas digitales de escala global, la delincuencia organizada especializada en ciberataques y la inteligencia artificial aplicada a la generación de código malicioso han transformado el panorama, abriendo un espacio de oportunidad para que el legislador federal incorpore al ordenamiento las modalidades contemporáneas de ciberdelincuencia.

Las reformas posteriores al Capítulo II —entre ellas la adición de un agravante para servidores públicos de instituciones de seguridad pública, publicada el 24 de junio de 2009, y la última modificación relevante, publicada el 7 de junio de 2024— han abordado aspectos puntuales del capítulo. La presente iniciativa complementa ese trabajo legislativo previo mediante la incorporación de modalidades hoy dominantes de ciberdelincuencia que ganan con la tipificación autónoma que aquí se propone: el secuestro de datos mediante cifrado (**ransomware**), la suplantación de identidad por medios electrónicos (**phishing**), la denegación distribuida de servicio (**DDoS**), las intrusiones sostenidas con fines de espionaje (**amenazas persistentes avanzadas o APT**), la distribución deliberada de código malicioso (**malware**) y el compromiso de proveedores tecnológicos (**ataques a la cadena de suministro**), todas ellas con descripción típica propia que facilita su persecución y sanción.

La actualización del marco no es un planteamiento inédito. Entre 2015 y 2024, el Congreso de la Unión recibió al menos media docena de iniciativas dirigidas al tema. El entonces diputado Javier Joaquín López Casarín presentó, en dos ocasiones, sendos proyectos para expedir una Ley Federal de Ciberseguridad. El diputado Salvador Caro Cabrera presentó, el 6 de diciembre de 2023, una iniciativa para expedir la Ley General del Sistema Nacional de Seguridad Digital. En el Senado se registraron propuestas orientadas a la armonización de la legislación existente. Ninguna de esas iniciativas concluyó su proceso legislativo. La reiteración del diagnóstico entre bancadas distintas, a lo largo de casi una década, evidencia que la modernización del marco es una lectura transversal. La presente propuesta aprende de esa experiencia y opta por una reforma acotada al Código Penal Federal, sin

creación de organismos, agencias ni estructuras administrativas nuevas y sin modificar las reglas vigentes de competencia federal.

Cabe precisar, para efectos del alcance de la presente iniciativa, que los artículos 211 Bis 1 a 211 Bis 7 vigentes se conservan sin modificación. La eventual revisión del régimen punitivo de dichos tipos corresponde a un ejercicio legislativo posterior, cuya oportunidad y contenido serán objeto de análisis específico. El objeto del presente decreto se concentra en incorporar al mismo Capítulo las modalidades contemporáneas de ciberdelincuencia con descripción típica propia, sin alterar el catálogo básico de acceso ilícito, a fin de preservar la continuidad interpretativa y evitar afectaciones a los procesos en trámite.

II. MARCO CONSTITUCIONAL

La reforma que se propone encuentra sustento directo en la Constitución Política de los Estados Unidos Mexicanos, cuyo articulado ofrece tanto el fundamento competencial para legislar en la materia como los principios sustantivos que orientan su contenido.

En primer término, el **artículo 73, fracción XXI, inciso b)**, confiere al Congreso de la Unión la facultad de expedir la legislación que establezca los delitos y las faltas contra la Federación, así como las penas y sanciones correspondientes. Esta atribución permite al legislador federal tipificar conductas que lesionen bienes, instituciones, servicios o funciones pertenecientes al ámbito federal, sin que ello suponga una habilitación general para federalizar cualquier conducta por su sola dimensión tecnológica o por producir efectos en más de una entidad federativa. El Pleno de la Suprema Corte de Justicia de la Nación, al resolver la **Acción de Inconstitucionalidad 110/2019**, reconoció expresamente que corresponde al Congreso de la Unión establecer los delitos dirigidos contra instituciones federales y nacionales, mientras que las entidades federativas conservan su potestad penal respecto de conductas vinculadas con su propio ámbito competencial.¹

¹ Suprema Corte de Justicia de la Nación, Pleno, Acción de Inconstitucionalidad 110/2019, resuelta el 19 de mayo de 2022, apartado relativo a la competencia del legislador local frente al artículo 73, fracción XXI, inciso b), constitucional.
https://www2.scjn.gob.mx/juridica/engroses/3/2019/19/3_264269_6162_firmado.pdf

En congruencia con ese parámetro, el **artículo 48, fracción I, de la Ley Orgánica del Poder Judicial de la Federación** enumera los supuestos que determinan el carácter federal de los delitos. Entre ellos se encuentran los señalados en los artículos 2o. a 5o. del Código Penal Federal; aquellos en que la Federación sea sujeto pasivo; los perpetrados con motivo del funcionamiento de un servicio público federal, incluso descentralizado o concesionado; los cometidos contra dicho funcionamiento o contra los bienes afectados a su prestación; y aquellos que ataquen, dificulten o imposibiliten el ejercicio de una atribución o facultad reservada a la Federación. A su vez, el artículo 1o. del Código Penal Federal dispone que dicho ordenamiento se aplicará en toda la República para los delitos del orden federal. La presente iniciativa no modifica esas reglas ni introduce criterios autónomos de federalización: los nuevos tipos se aplicarán en el orden federal cuando se actualice alguno de los supuestos legales vigentes. En consecuencia, la sola utilización de tecnologías de la información, redes de telecomunicaciones o internet, o el hecho de que una conducta produzca efectos en más de una entidad federativa, no bastarán por sí mismos para atribuir competencia federal.²

El **artículo 21**, en sus párrafos noveno y décimo, dispone que la seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los municipios, cuyo objeto comprende la prevención, investigación y persecución de los delitos. La creciente incidencia de ataques informáticos dirigidos contra instituciones públicas, infraestructura crítica y servicios esenciales pone de manifiesto que la ciberseguridad se ha convertido en una dimensión indispensable de la seguridad pública en el sentido constitucional, y que dotar a las autoridades de tipos penales adecuados forma parte del cumplimiento de ese mandato.

El **artículo 16, párrafo segundo**, reconoce el derecho fundamental a la protección de los datos personales. Modalidades como el **phishing**, el robo de credenciales o el **ransomware** afectan de manera directa este derecho, al comprometer información personal, financiera o confidencial de las personas y de las instituciones. La

² Ley Orgánica del Poder Judicial de la Federación, artículo 48, fracción I, texto vigente.
<https://www.diputados.gob.mx/LeyesBiblio/pdf/LOPJF.pdf>

actualización del régimen penal constituye, por tanto, uno de los mecanismos mediante los cuales el Estado hace efectiva esa tutela constitucional.

El **artículo 25** reconoce la rectoría del Estado en el desarrollo nacional y le impone garantizar que éste sea integral y sustentable, fortaleciendo la soberanía y la competitividad del país. En una economía crecientemente digitalizada, la continuidad de la infraestructura tecnológica —gubernamental, financiera, energética, sanitaria y de telecomunicaciones— es presupuesto indispensable del desarrollo. Su protección jurídica forma parte, en consecuencia, de las obligaciones del Estado bajo este precepto.

Por último, el **artículo 6º, apartado B**, al reconocer el derecho de acceso a las tecnologías de la información y las comunicaciones y a los servicios de banda ancha e internet, impone al Estado la obligación de garantizar condiciones de disponibilidad, continuidad y seguridad. La tipificación de conductas que atentan contra esa disponibilidad —como el **ataque de denegación distribuida de servicio**— es una expresión legítima de esa obligación.

III. MARCO INTERNACIONAL

La respuesta jurídica a la ciberdelincuencia se ha construido en las últimas dos décadas como un esfuerzo esencialmente cooperativo, en el entendido de que la naturaleza transfronteriza de las conductas exige respuestas armonizadas entre los Estados. La presente iniciativa se inscribe en ese esfuerzo, y encuentra referentes específicos en tres instrumentos internacionales de particular relevancia para el Estado mexicano.

Conviene precisar, desde el inicio, que los dos tratados principales en la materia —el Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Convención de las Naciones Unidas contra la Ciberdelincuencia— son instrumentos **distintos y complementarios**, no alternativos ni sustitutivos entre sí. El primero es el estándar técnico consolidado a nivel mundial, con más de dos décadas de aplicación y 82 Estados Parte. La segunda es el estándar emergente de vocación universal, adoptada por consenso apenas en diciembre de 2024, cuya arquitectura de



cooperación internacional es más amplia. Un Estado puede ser parte de ambos, de uno solo o de ninguno; los diez Estados de América Latina y el Caribe ya adheridos al Convenio de Budapest pueden, y previsiblemente lo harán, firmar además la Convención de las Naciones Unidas. Los tipos penales mínimos que uno y otro exigen son en lo esencial coincidentes, de modo que la armonización del ordenamiento interno con esos tipos —objeto de la presente iniciativa— avanza en ambos frentes al mismo tiempo, sin prejuzgar la decisión soberana que corresponde al Ejecutivo Federal, en términos del artículo 89 constitucional, respecto de la firma, adhesión o ratificación de cada instrumento.

1. Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest, 2001)

El Convenio de Budapest, adoptado el 23 de noviembre de 2001, es el primer y hasta hoy el más completo tratado internacional en materia de ciberdelincuencia. Su arquitectura sirvió de modelo para la legislación penal de más de setenta jurisdicciones y estableció el catálogo mínimo de conductas que un ordenamiento contemporáneo debe tipificar: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de dispositivos y falsificación y fraude informáticos.³ A julio de 2026, de acuerdo con la Oficina del Programa de Ciberdelincuencia del Consejo de Europa, 82 Estados son Parte del Convenio, incluyendo a la totalidad de los miembros de la Unión Europea, los Estados Unidos de América, el Canadá, el Japón, Australia, Israel y diez Estados de América Latina y el Caribe: la República Argentina, la República Federativa del Brasil, la República de Chile, la República de Colombia, la República de Costa Rica, la República del Ecuador, la República de Panamá, la República del Paraguay, la República del Perú y la República Dominicana.⁴

El Estado mexicano fue invitado a adherirse al Convenio y participa desde entonces

³Consejo de Europa, Convenio sobre la Ciberdelincuencia (ETS No. 185), Budapest, 23 de noviembre de 2001, artículos 2 a 10.

⁴Consejo de Europa, Oficina del Programa de Ciberdelincuencia, "Joining the Convention on Cybercrime: Benefits", versión de 1 de julio de 2026, que reporta 82 Estados Parte. <https://rm.coe.int/cyber-buda-benefits-1-july-2026-en/48802c5c24>

como observador, sin haber completado el proceso formal de adhesión. La presente reforma armoniza el Código Penal Federal con las conductas típicas descritas en el artículo 2 y siguientes del Convenio —acceso ilícito, ataques a la integridad de los datos y del sistema, abuso de dispositivos—, contribuyendo así a preparar el terreno normativo para una eventual adhesión y a homologar los estándares mexicanos con los de sus principales socios comerciales y de cooperación.

2. Convención de las Naciones Unidas contra la Ciberdelincuencia (Convención de Hanói, 2024)

El 24 de diciembre de 2024, la Asamblea General de las Naciones Unidas adoptó por consenso la primera Convención de las Naciones Unidas contra la Ciberdelincuencia, negociada en el marco de un Comité Especial establecido por la propia Asamblea en 2019. La Convención fue abierta a la firma de los Estados en una ceremonia celebrada en Hanói, República Socialista de Viet Nam, en octubre de 2025, y permanecerá abierta a la firma en la sede de las Naciones Unidas en Nueva York hasta el **31 de diciembre de 2026**.⁵

La delegación del Estado mexicano participó en la ceremonia de alto nivel de Hanói y emitió una declaración oficial de respaldo político al instrumento, en la que precisó que México se encuentra **avanzando en sus procesos internos de armonización legislativa y revisión jurídica, con miras a concretar su adhesión a este tratado en el corto plazo**.⁶ En congruencia con esa declaración pública, y anticipándose a los pasos formales de firma y ratificación que corresponden al Ejecutivo Federal, la presente iniciativa aporta al ordenamiento interno los tipos penales que armonizan la legislación mexicana con los estándares que la propia Convención establece.

3. Referentes contemporáneos: la Directiva SRI 2 de la Unión Europea

En el ámbito regional europeo, la Directiva (UE) 2022/2555, conocida como Directiva SRI 2 o NIS 2, adoptada el 14 de diciembre de 2022 y de aplicación obligatoria a partir

⁵ Organización de las Naciones Unidas, Convención de las Naciones Unidas contra la Ciberdelincuencia, adoptada por consenso por la Asamblea General el 24 de diciembre de 2024. Ceremonia de apertura a la firma, Hanói, octubre de 2025. Ventana de firma abierta hasta el 31 de diciembre de 2026 en la Sede de las Naciones Unidas en Nueva York.

⁶ Declaración oficial de la delegación mexicana en la ceremonia de alto nivel de Hanói, octubre de 2025.

del 18 de octubre de 2024, actualizó el régimen de la Unión Europea en materia de seguridad de las redes y los sistemas de información. Amplió su alcance a dieciocho sectores críticos —entre ellos energía, transporte, banca, sanidad, infraestructura digital, aguas, administración pública y manufactura— y estableció un régimen sancionador armonizado para las entidades esenciales e importantes.⁷ La presente iniciativa no busca replicar ese modelo administrativo —que corresponde a un ámbito regulatorio distinto—, pero toma de él la lectura contemporánea sobre qué constituye infraestructura crítica y cuáles son las conductas cuya persecución debe reforzarse.

4. Contraste regional

A efecto de dimensionar la posición del Estado mexicano frente a sus pares latinoamericanos, se presenta a continuación un cuadro comparativo sobre la situación normativa e internacional de los principales países de la región:

País	Año de adhesión al Convenio de Budapest	Marco penal contemporáneo de ciberdelitos
República Dominicana	2013	Ley 53-07 (2007) contra crímenes y delitos de alta tecnología.
República de Panamá	2014	Ley 51 (2008) sobre delitos financieros informáticos, con reformas al Código Penal en delitos informáticos.
República de Costa Rica	2017	Ley 9048 (2012), reforma al Código Penal en delitos informáticos y conexos.
República de Chile	2017	Ley 21.459 (2022) sobre delitos informáticos, en armonización directa con el Convenio de Budapest.
República Argentina	2018	Ley 26.388 (2008), reforma integral al Código Penal en materia de delitos informáticos.
República del Paraguay	2018	Ley 4439 (2011), incorporación de delitos informáticos al Código Penal.
República de Colombia	2020	Ley 1273 (2009) sobre protección de la información y los datos.
República del Perú	2020	Ley 30096 (2013), Ley de Delitos Informáticos.
República Federativa del Brasil	2022	Ley 12.737 (Ley Carolina Dieckmann, 2012) y Ley 14.155 (2021) sobre fraudes electrónicos y delitos informáticos.
República del Ecuador	2024	Reformas al Código Orgánico Integral Penal (2020-2021) para armonización con el Convenio, previas a la adhesión.
Estados Unidos Mexicanos	No (invitado, observador)	Código Penal Federal, Capítulo II del Título Noveno (1999), sin actualización integral.

⁷ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2). Fecha de aplicación: 18 de octubre de 2024.

El cuadro muestra que México se encuentra entre las jurisdicciones que aún no han adherido al Convenio de Budapest, en un contexto regional donde diez Estados de América Latina y el Caribe ya son Parte. La presente reforma se propone cerrar esa brecha por la vía más eficiente disponible al legislador federal: la actualización del catálogo de tipos penales existente, en armonización con los estándares que los referentes internacionales han consolidado.

IV. CRITERIOS JURISPRUDENCIALES

La presente iniciativa se sustenta en criterios del Poder Judicial de la Federación en cuatro materias directamente aplicables al diseño normativo que se propone: la distribución constitucional de competencias en materia penal, el principio de taxatividad, la protección constitucional de los datos personales como derecho fundamental y la exigencia de proporcionalidad en la individualización de las penas.

En materia de competencia legislativa, el Pleno de la Suprema Corte de Justicia de la Nación, al resolver la Acción de Inconstitucionalidad 110/2019, declaró inválida la porción de una norma penal local que pretendía tutelar funciones de instituciones federales, nacionales y de las Fuerzas Armadas, al considerar que invadía la competencia exclusiva del Congreso de la Unión prevista en el artículo 73, fracción XXI, inciso b), constitucional. Este criterio confirma que la intervención del legislador federal debe mantenerse vinculada al ámbito constitucional de la Federación y que la aplicación de los nuevos tipos penales debe sujetarse a los supuestos de federalidad ya establecidos en el artículo 48, fracción I, de la Ley Orgánica del Poder Judicial de la Federación, sin derivar la competencia de la mera utilización de tecnología o de la extensión territorial de los efectos.

En materia de **taxatividad**, la Primera Sala de la Suprema Corte de Justicia de la Nación, en la tesis de jurisprudencia 1a./J. 54/2014 (10a.) de rubro "PRINCIPIO DE LEGALIDAD PENAL EN SU VERTIENTE DE TAXATIVIDAD. ANÁLISIS DEL CONTEXTO EN EL CUAL SE DESENVUELVEN LAS NORMAS PENALES, ASÍ

COMO DE SUS POSIBLES DESTINATARIOS",⁸ ha sostenido que el derecho fundamental de exacta aplicación de la ley en materia penal, previsto en el artículo 14 constitucional, exige del legislador la emisión de normas claras, precisas y exactas respecto de la conducta reprochable y de la consecuencia jurídica por su comisión. El propio criterio precisa que el grado de determinación de la conducta típica debe ser tal que lo que es objeto de prohibición pueda ser conocido por el destinatario de la norma, sin que ello implique exigir la mayor precisión imaginable ni la definición exhaustiva de cada vocablo, criterio que la propia Sala ha reiterado en pronunciamientos posteriores.⁹ En congruencia con este parámetro, cada uno de los tipos penales que la presente iniciativa propone se formula de manera autosuficiente, mediante verbos rectores acotados y elementos objetivos claramente delimitados, de modo que la conducta prohibida pueda identificarse directamente en el propio precepto sin depender de definiciones tecnológicas externas. La sofisticación técnica de las conductas no exime de esa exigencia, sino que la refuerza, garantizando así la seguridad jurídica de los gobernados frente a la potestad punitiva del Estado.

En materia de **protección de datos personales**, la Primera Sala ha reconocido que el artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos consagra el derecho a la protección de datos personales, entendido como el control de cada individuo sobre el acceso y uso de la información personal en aras de preservar la vida privada de las personas.¹⁰ Este derecho fundamental exige del Estado no solo la abstención de intervenciones injustificadas, sino la adopción de medidas positivas que aseguren su tutela frente a terceros, lo que comprende, por definición, el establecimiento de mecanismos jurídicos eficaces para prevenir, investigar y sancionar las conductas que lo vulneren. Las modalidades de ciberdelincuencia que tienen por objeto obtener credenciales, datos financieros o

⁸Suprema Corte de Justicia de la Nación, Primera Sala, tesis de jurisprudencia 1a./J. 54/2014 (10a.), de rubro "PRINCIPIO DE LEGALIDAD PENAL EN SU VERTIENTE DE TAXATIVIDAD. ANÁLISIS DEL CONTEXTO EN EL CUAL SE DESENVUELVEN LAS NORMAS PENALES, ASÍ COMO DE SUS POSIBLES DESTINATARIOS", Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 8, julio de 2014, Tomo I, página 131, registro digital 2006867.

⁹Cfr. Suprema Corte de Justicia de la Nación, Primera Sala, tesis en materia de taxatividad publicada en la Gaceta del Semanario Judicial de la Federación, Libro 37, mayo de 2024, Tomo II, página 1632, registro digital 2028874, que reitera el estándar interpretativo de la tesis 1a./J. 54/2014 (10a.).

¹⁰Suprema Corte de Justicia de la Nación, Primera Sala, tesis 1a. CCLXXXI/2016 (10a.), en materia de protección de datos personales derivada del artículo 16, párrafo segundo, constitucional, Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 37, diciembre de 2016, Tomo I, página 362, registro digital 2013198.

información confidencial —singularmente el **phishing** y el **ransomware**— afectan de manera directa este derecho, por lo que su tipificación específica constituye un desarrollo legislativo congruente con la doctrina constitucional sobre la materia.

En materia de **proporcionalidad de las penas**, el Poder Judicial de la Federación ha sostenido que la individualización de la sanción exige parámetros objetivos que orienten al juzgador cuando el tipo prevé rangos punitivos amplios, a fin de que la aplicación concreta de la norma no vulnere el principio de proporcionalidad ni conduzca a resultados arbitrarios. Este estándar se refleja en el diseño de los tipos propuestos, que distinguen expresamente entre modalidades de baja y de alta lesividad dentro de cada conducta —por ejemplo, el **phishing** con y sin daño patrimonial consumado— y que, en el caso del delito de amenaza persistente avanzada, incorporan criterios explícitos para la individualización de la pena dentro del rango previsto: la duración de la intrusión, la sensibilidad de la información comprometida y el grado de sofisticación técnica empleado.

Los criterios anteriores integran, en conjunto, el parámetro constitucional al que se ajusta el diseño de la reforma, y permiten sostener que la iniciativa tutela un bien jurídico específico —la **integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos**— como presupuesto de otros bienes jurídicos constitucionalmente reconocidos, sin invadir el ámbito de tipos ya existentes en el ordenamiento federal.

V. DERECHO COMPARADO

El estudio del derecho comparado evidencia una tendencia convergente en las jurisdicciones que han actualizado su régimen penal en materia informática durante los últimos veinte años. Las legislaciones contemporáneas han abandonado el modelo original —centrado en el acceso ilícito como conducta genérica— y han incorporado tipos penales específicos que atienden las modalidades de ataque surgidas con la evolución tecnológica.

En el ámbito europeo, la **República Federal de Alemania** tipifica en el §303a del Código Penal el sabotaje informático mediante alteración de datos, y en el §303b un

tipo agravado cuando la conducta afecta empresas, autoridades o infraestructuras esenciales para la colectividad. El **Reino de España** incorporó en 2010, mediante la Ley Orgánica 5/2010, los artículos 197 bis y 197 ter del Código Penal, que sancionan el acceso ilícito a datos o programas informáticos, y en 2015 los artículos 264 a 264 quater, referidos al daño informático y a la producción y facilitación de programas destinados a cometerlos. La **República Francesa** regula la materia en el Capítulo III del Título II del Libro III de su Código Penal, con tipos específicos para el acceso y mantenimiento fraudulentos en sistemas de tratamiento automatizado, la obstaculización de su funcionamiento y la alteración de datos.

En el ámbito latinoamericano, la **República Argentina** modificó su Código Penal mediante la Ley 26.388, publicada en 2008, que incorporó tipos específicos para el daño informático, la interrupción de comunicaciones, el fraude informático y la alteración de pruebas electrónicas. La **República de Chile**, en línea con su adhesión al Convenio de Budapest, expidió en 2022 la Ley 21.459, que estableció un catálogo completo de delitos informáticos en armonización directa con el instrumento europeo. La **República Federativa del Brasil** avanzó con la Ley 12.737 —conocida como Ley Carolina Dieckmann— y con la Ley 14.155 de 2021, que fortaleció las sanciones para los fraudes electrónicos y la invasión de dispositivos informáticos.

La lectura comparada arroja una conclusión clara. Los ordenamientos que han modernizado su régimen penal han seguido, en lo esencial, tres criterios comunes: tipificar de manera autónoma las conductas hoy dominantes —ransomware, ataques a la integridad de los datos y del sistema, abuso de dispositivos—, agravar las penas cuando el ataque compromete infraestructura crítica o servicios esenciales, y armonizar la terminología con los instrumentos internacionales de referencia. La presente iniciativa recoge estos tres criterios y los adapta a la técnica legislativa mexicana, sin trasplantar de manera acrítica figuras propias de otros sistemas jurídicos.

VI. Diagnóstico del marco jurídico nacional y justificación de la reforma

El diagnóstico que motiva la presente iniciativa se sustenta en cuatro elementos convergentes: la oportunidad de incorporar al catálogo típico las modalidades



contemporáneas de ciberdelincuencia, la conveniencia de ajustar el régimen punitivo a la escala actual del daño potencial, la magnitud objetiva del fenómeno documentada por fuentes primarias, y la incidencia comprobada de ataques contra instituciones estratégicas del Estado mexicano.

1. Incorporación de las modalidades contemporáneas al catálogo típico

El Código Penal Federal vigente articula la protección penal de los sistemas informáticos alrededor de conductas genéricas —acceso ilícito, conocimiento, copia, modificación o destrucción de información—, propias del paradigma de finales del siglo XX. La presente iniciativa suma a ese catálogo las modalidades hoy dominantes: el **ransomware**, el **phishing**, los ataques de denegación distribuida de servicio, las amenazas persistentes avanzadas, la distribución de **malware** y los ataques a la cadena de suministro, cada una con descripción típica autónoma. Con ello, los operadores del sistema de justicia contarán con tipos penales específicos para conductas técnicamente distintas, lo que fortalecerá la seguridad jurídica, la eficacia probatoria y la cooperación internacional en materia de ciberdelincuencia.

2. Adecuación del régimen punitivo a la escala contemporánea del daño

Las escalas de sanciones vigentes fueron diseñadas para una realidad tecnológica en la que los ataques informáticos afectaban equipos aislados o bases de datos de alcance limitado. En el paradigma contemporáneo, un solo ataque de **ransomware** puede paralizar hospitales, sistemas financieros, dependencias gubernamentales o redes nacionales de comunicaciones, con pérdidas económicas millonarias e interrupciones prolongadas de servicios esenciales. Ajustar la escala punitiva a la magnitud potencial del daño fortalece el efecto disuasivo del derecho penal y coloca las sanciones en proporción con la gravedad real de las conductas.

3. Magnitud objetiva de la amenaza

De acuerdo con el Reporte Global de Amenazas de FortiGuard Labs, división de investigación de Fortinet, durante el primer trimestre de 2025 el territorio mexicano registró aproximadamente **35,200 millones de intentos de ciberataque**; y durante el primer semestre del mismo año, **40,600 millones**, de los cuales cerca de 17,000

millones correspondieron a escaneos activos automatizados.¹¹ En volumen bruto de intentos, México se ubica en el segundo lugar de América Latina, únicamente por detrás de la República Federativa del Brasil. En rubros específicos —particularmente en la distribución de ciertas familias de **ransomware** y en los ataques dirigidos a los sectores industrial y manufacturero— México figura recurrentemente en el primer lugar regional.

La Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) del Instituto Nacional de Estadística y Geografía documenta un incremento sostenido de los fraudes cibernéticos como delito de mayor incidencia entre las personas usuarias de servicios digitales, lo que subraya la oportunidad de fortalecer la capacidad institucional de respuesta.

4. Incidentes contra instituciones estratégicas del Estado

La pertinencia de la reforma se ilustra con incidentes documentados que, bajo el marco vigente, encuadran de forma imprecisa en tipos concebidos para realidades tecnológicas distintas. En noviembre de 2019, **Petróleos Mexicanos** fue víctima de un ataque con el **ransomware** DoppelPaymer, que afectó aproximadamente el cinco por ciento de sus equipos de cómputo; los atacantes exigieron un rescate de 565 bitcoins, equivalente entonces a 4.9 millones de dólares, y ante la negativa de pago publicaron parte de la información sustraída. En junio de 2021, la **Lotería Nacional** fue objeto de un ataque atribuido al grupo Avaddon, que comprometió sus sistemas. Entre febrero y marzo de 2022, la unidad de investigación de la firma SILIKN documentó la presencia del **ransomware** BlackCat, también conocido como ALPHV, en al menos doce empresas de los sectores industrial y manufacturero en Guanajuato, Ciudad de México, Chihuahua, Nuevo León, Jalisco y el Estado de México. En 2023, la **Caja Popular Mexicana** enfrentó un ataque con esa misma familia de **ransomware**, con afectación a sus más de tres millones de socios. A la par, diversas dependencias federales redujeron su presupuesto en informática y seguridad digital entre 2022 y 2025; el caso de la Secretaría de Infraestructura,

¹¹ Fortinet, FortiGuard Labs, Reporte Global de Amenazas, mediciones correspondientes al primer trimestre y primer semestre de 2025 para México.



Comunicaciones y Transportes es ilustrativo, con una reducción superior al ochenta y cinco por ciento en ese rubro durante el periodo.¹²

El volumen y la sofisticación crecientes de la ciberdelincuencia, la naturaleza estratégica de la infraestructura hoy expuesta y la incidencia comprobada de ataques contra instituciones del Estado imponen al legislador federal la responsabilidad de dotar al sistema penal de instrumentos técnicos a la altura del fenómeno. La presente iniciativa asume esa responsabilidad, con la vía más eficiente disponible al legislador: la actualización del catálogo de tipos penales existente.

VII. Justificación de la reforma al Capítulo II del Título Noveno y adecuaciones correlativas

La iniciativa propone una actualización integral del Capítulo II del Título Noveno del Código Penal Federal, mediante la reforma de su denominación, seis tipos penales autónomos correspondientes a las modalidades contemporáneas de ciberdelincuencia y un agravante escalonado para la afectación a infraestructura pública federal y a infraestructura crítica o estratégica de competencia federal, además de reglas sobre responsabilidad de personas jurídicas y reparación integral. Los tipos se redactan de manera autosuficiente y tecnológicamente neutral: cada precepto describe directamente la conducta, sus elementos y la consecuencia jurídica, mientras que las denominaciones técnicas de uso internacional se conservan en la exposición de motivos como referentes explicativos. De manera correlativa, se adiciona una fracción XVII al apartado A del artículo 11 Bis del propio Código, a fin de incorporar estos delitos al catálogo aplicable a la responsabilidad penal de personas jurídicas. El diseño se sujeta a los principios de taxatividad, mínima intervención penal, proporcionalidad y respeto al federalismo.

La reforma a la **denominación del Capítulo** —que pasa a comprender expresamente los ciberataques junto con el acceso ilícito— responde a una exigencia de técnica legislativa: el nombre vigente describe únicamente el paradigma de 1999 y podría

¹²Fuentes periodísticas especializadas (Excélsior, El Universal, Expansión, El Financiero, Sin Embargo, La Jornada) para los casos Pemex/DoppelPaymer (2019), Lotería Nacional/Avaddon (2021), sector industrial/BlackCat (2022), Caja Popular Mexicana (2023) y recorte presupuestal en SICT.

estrechar interpretativamente el ámbito de las modalidades que ahora se incorporan. El nuevo enunciado dota al Capítulo de una sombra normativa amplia y coherente con su contenido actualizado.

Precisamente para preservar el federalismo penal y evitar duplicidades normativas, la iniciativa no incorpora una cláusula especial de competencia en el Código Penal Federal ni propone modificar la Ley Orgánica del Poder Judicial de la Federación. Los nuevos tipos quedan sujetos a las reglas generales ya vigentes: el artículo 1o. del Código Penal Federal limita su aplicación a los delitos del orden federal, y el artículo 48, fracción I, de la Ley Orgánica del Poder Judicial de la Federación determina los supuestos en que corresponde conocer a las y los jueces federales penales. De este modo, la reforma no federaliza una conducta por el solo uso de redes de telecomunicaciones, por la producción de efectos en más de una entidad federativa ni por la relevancia de un servicio de carácter estrictamente local; la competencia federal deberá desprenderse, en cada caso, de alguno de los supuestos legales vigentes, sin perjuicio de la legislación y competencia locales que resulten aplicables.

La previsión sobre responsabilidad penal de personas jurídicas requiere una adecuación correlativa al catálogo del artículo 11 Bis del Código Penal Federal, pues el artículo 421 del Código Nacional de Procedimientos Penales condiciona dicha responsabilidad a los delitos expresamente previstos en la legislación penal correspondiente. Por ello se adiciona una fracción XVII al apartado A del artículo 11 Bis para incorporar los delitos previstos en los artículos 211 Bis 8 a 211 Bis 13. La modificación no crea un régimen distinto de responsabilidad, sino que habilita, para estos nuevos tipos, la aplicación de las consecuencias jurídicas ya previstas en el ordenamiento vigente.

La reforma **no crea bienes jurídicos nuevos**. Fortalece la tutela penal de bienes ya reconocidos constitucionalmente —seguridad pública, protección de datos personales, patrimonio, continuidad de los servicios públicos, seguridad nacional e integridad de la infraestructura tecnológica del Estado— mediante tipos penales más precisos y ajustados a la realidad que hoy los amenaza. Tampoco crea estructuras administrativas, organismos ni plazas: se limita a modificar el catálogo delictivo del

Código Penal Federal, dejando la operación de las nuevas figuras a cargo de las autoridades ministeriales y judiciales ya existentes.

La opción por reformar exclusivamente el Código Penal Federal, en lugar de expedir un ordenamiento nuevo o alterar las reglas orgánicas de competencia, responde a la naturaleza y alcance de la propuesta. El Código Penal Federal concentra la descripción de las conductas punibles que corresponden al orden federal, mientras que la Ley Orgánica del Poder Judicial de la Federación ya determina los supuestos de competencia de las y los jueces federales penales. Mantener intacta esa distribución preserva la arquitectura vigente del sistema federal de justicia, evita duplicidades y reduce al mínimo indispensable el impacto normativo de la iniciativa.

El objeto de la presente reforma se concentra en las conductas que afectan la **integridad, confidencialidad y disponibilidad** de los sistemas informáticos y de los datos —el núcleo duro de la ciberdelincuencia contemporánea—, en tanto que las demás conductas que los instrumentos internacionales exigen tipificar ya se encuentran previstas en el ordenamiento federal mexicano por vías distintas: el fraude en los artículos 386 y siguientes del propio Código Penal Federal, la falsificación en los artículos 243 y siguientes, los delitos contra menores en los artículos 200 a 204, la protección penal de los derechos de autor en la Ley Federal del Derecho de Autor, y la prevención del uso de recursos de procedencia ilícita en la ley especial de la materia. La técnica legislativa mexicana ha optado, así, por distribuir la protección penal según el bien jurídico afectado, y la presente iniciativa respeta esa arquitectura sin duplicarla.

VIII. IMPACTO REGULATORIO

La presente iniciativa no genera cargas administrativas o regulatorias adicionales para los particulares. Si bien incorpora nuevas prohibiciones y consecuencias jurídicas de naturaleza penal, no instituye permisos, licencias, autorizaciones, registros ni trámites; no crea obligaciones de reporte para sujetos regulados; ni modifica requisitos administrativos para el ejercicio de actividades económicas o funciones públicas. La adición al artículo 11 Bis del Código Penal Federal se limita a incorporar los nuevos tipos al catálogo ya existente de responsabilidad penal de

personas jurídicas. La iniciativa no modifica las reglas vigentes de competencia federal ni crea estructuras administrativas adicionales.

Su efecto es sustantivo y consiste en crear el marco típico necesario para que las autoridades ministeriales y judiciales puedan describir, perseguir y sancionar las modalidades contemporáneas de ciberdelincuencia con base en tipos penales específicos, en lugar de subsumirlas forzosamente en descripciones concebidas para un paradigma tecnológico distinto. En esa medida, la iniciativa no incrementa la carga regulatoria del Estado ni la de los sujetos obligados; la fortalece cualitativamente sin agregar volumen normativo innecesario.

IX. IMPACTO PRESUPUESTARIO

La iniciativa no requiere ampliaciones presupuestarias ni la creación de estructuras administrativas, plazas, unidades, organismos, agencias, fondos o programas de nueva creación. La aplicación de los tipos penales propuestos corresponderá a las autoridades ministeriales y judiciales competentes conforme al marco vigente, con cargo a sus presupuestos autorizados y con apego a los principios de racionalidad, austeridad y disciplina presupuestaria previstos en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos. Las actividades de capacitación que resulten necesarias deberán atenderse con los recursos aprobados para las instituciones competentes.

X. IMPACTO SOCIAL

El beneficio social de la reforma es directo y de amplio alcance. Fortalecer la capacidad del Estado para perseguir y sancionar las modalidades contemporáneas de ciberdelincuencia protege a las personas usuarias de servicios digitales frente al fraude electrónico, el robo de identidad y el uso indebido de sus datos; blinda la continuidad de los servicios públicos esenciales que hoy dependen de infraestructura tecnológica; y resguarda la confianza de la ciudadanía en los sistemas digitales que sostienen la actividad económica y gubernamental del país. Al alinear el ordenamiento interno con los estándares internacionales, la reforma también facilita la cooperación con las autoridades de otros Estados en la investigación y persecución



de delitos que, por su naturaleza, rara vez ocurren dentro de una sola frontera. El instrumento penal, en suma, se pone al día con la realidad que le corresponde regir.

CUADRO COMPARATIVO

Para facilitar la identificación y comprensión de las modificaciones propuestas, se presenta a continuación un cuadro comparativo entre el texto vigente y el texto propuesto. Tratándose de disposiciones de nueva creación, en la columna correspondiente al texto vigente se indica expresamente **“Sin correlativo”**, seguida de una breve referencia al tratamiento que actualmente recibe la conducta en el ordenamiento. Los artículos 211 Bis 1 a 211 Bis 7 del Código Penal Federal se conservan sin modificación y, por economía expositiva, no se reproducen. Asimismo, se incluye la adecuación correlativa del artículo 11 Bis en materia de responsabilidad penal de las personas jurídicas. Las reglas vigentes para determinar el carácter federal de los delitos y la competencia de los órganos jurisdiccionales permanecen sin modificación.

Texto vigente	Propuesta de modificación
1. Denominación del Capítulo II del Título Noveno CAPÍTULO II Acceso ilícito a Sistemas y Equipos de Informática	1. Denominación del Capítulo II del Título Noveno CAPÍTULO II <u>De los Ciberataques y del Acceso Ilícito a Sistemas y Equipos de Informática</u>
Sin correlativo. Bajo el paradigma vigente, la distribución de código malicioso se procesa por la vía de los tipos genéricos del artículo 211 Bis 1, relativos a modificar, destruir o provocar pérdida de información. La tipificación autónoma que se propone permite distinguir las fases de diseño, desarrollo, distribución, introducción y ejecución de software o código destinado a comprometer sistemas informáticos.	2. Artículo 211 Bis 8 · Desarrollo, distribución o ejecución de software o código malicioso <u>Artículo 211 Bis 8. Comete el delito de desarrollo, distribución o ejecución de software o código malicioso quien, sin autorización o excediendo la autorización que se le hubiere concedido, diseñe, desarrolle, distribuya, introduzca o ejecute software o código destinado a infiltrarse, dañar, alterar el funcionamiento o tomar el control, total o parcial, de un sistema informático ajeno.</u>



Texto vigente	Propuesta de modificación
	<u>A quien cometa este delito se le impondrá pena de cuatro a ocho años de prisión y multa de quinientas a mil quinientas Unidades de Medida y Actualización.</u> <u>No será constitutiva de este delito la conducta realizada en el marco de actividades de investigación en seguridad informática, pruebas de penetración autorizadas o programas de reporte responsable de vulnerabilidades, siempre que exista consentimiento del titular del sistema afectado y la conducta se mantenga dentro de los términos de la autorización otorgada.</u>
Sin correlativo. Bajo el paradigma vigente, el secuestro de datos mediante cifrado se procesa por la vía del tipo genérico de modificación o pérdida de información. Los casos documentados de afectaciones mediante esta modalidad muestran la oportunidad de contar con una descripción típica autónoma que refleje su naturaleza específica y su lesividad contemporánea.	3. Artículo 211 Bis 9 · Secuestro de datos <u>Artículo 211 Bis 9. Comete el delito de secuestro de datos quien, mediante software o código, cifre, bloquee o restrinja de cualquier forma el acceso legítimo a sistemas informáticos, redes o datos ajenos, condicionando su restitución, liberación o desbloqueo a la entrega de un rescate económico o de cualquier otra naturaleza.</u> <u>A quien cometa este delito se le impondrá pena de seis a doce años de prisión y multa de mil a tres mil Unidades de Medida y Actualización.</u> <u>La pena se aumentará en una mitad cuando, además, el sujeto activo amenace con divulgar, vender o hacer pública la información sustraída como medio de presión para obtener el rescate.</u>
Sin correlativo. La suplantación de identidad por medios electrónicos para obtener credenciales o datos financieros se procesa actualmente mediante figuras generales, entre ellas el fraude previsto en el artículo 386. La	4. Artículo 211 Bis 10 · Suplantación por medios electrónicos con fines de apropiación de información <u>Artículo 211 Bis 10. Comete el delito de suplantación por medios electrónicos con fines de apropiación de información quien</u>



Texto vigente	Propuesta de modificación
tipificación específica que se propone permite describir de manera autónoma la conducta y preservar, en su caso, la aplicación de las reglas de concurso correspondientes.	<u>simule la identidad de una persona física, persona jurídica o institución legítima, con el fin de engañar a otra persona y obtener, sin su consentimiento, credenciales de acceso, datos personales, financieros o cualquier información confidencial.</u> <u>A quien cometa este delito se le impondrá pena de uno a tres años de prisión y multa de cien a trescientas Unidades de Medida y Actualización.</u> <u>Cuando de la conducta se derive un daño patrimonial efectivo, robo de identidad o acceso no autorizado consumado a cuentas o sistemas de la víctima, la pena será de cuatro a ocho años de prisión y multa de quinientas a mil Unidades de Medida y Actualización, sin perjuicio de las reglas de concurso que resulten aplicables con el delito de fraude.</u>
Sin correlativo. El Capítulo II vigente se articula principalmente en torno al acceso, conocimiento, modificación, destrucción y copia de información. La incorporación de un tipo específico de saturación deliberada de sistemas complementa el marco existente al proteger expresamente la disponibilidad, además de la confidencialidad e integridad, de los sistemas informáticos.	5. Artículo 211 Bis 11 · Interrupción deliberada de servicios informáticos <u>Artículo 211 Bis 11.</u> <u>Comete el delito de interrupción deliberada de servicios informáticos quien, mediante el envío masivo y coordinado de tráfico, solicitudes o instrucciones, valiéndose o no de una red de dispositivos comprometidos, sature, inhabilite o interrumpa deliberadamente la disponibilidad de un sistema, red o servicio informático ajeno.</u> <u>A quien cometa este delito se le impondrá pena de cuatro a nueve años de prisión y multa de quinientas a mil quinientas Unidades de Medida y Actualización.</u>
Sin correlativo. Las intrusiones prolongadas con fines de espionaje o sabotaje sostenido se procesan actualmente mediante tipos concebidos principalmente para accesos puntuales. La	6. Artículo 211 Bis 12 · Intrusión sostenida con fines de espionaje o sabotaje <u>Artículo 211 Bis 12.</u> <u>Comete el delito de intrusión sostenida con fines de espionaje o</u>



Texto vigente	Propuesta de modificación
tipificación autónoma que se propone permite valorar de manera específica la permanencia no autorizada, la continuidad de la intrusión y la finalidad perseguida.	sabotaje quien, mediante técnicas de intrusión encubierta y sostenida en el tiempo, acceda o permanezca sin autorización dentro de un sistema o red informática ajena, con el propósito de realizar espionaje, sabotaje o extracción continuada de información. <u>A quien cometa este delito se le impondrá pena de seis a quince años de prisión y multa de dos mil a cinco mil Unidades de Medida y Actualización.</u> <u>Para la individualización de la pena dentro del rango previsto, el juzgador atenderá a la duración de la intrusión, la sensibilidad de la información comprometida y el grado de sofisticación técnica empleado.</u>
Sin correlativo. El compromiso de proveedores tecnológicos como vector de ataque a los sistemas del usuario final carece actualmente de una descripción típica específica. La propuesta reconoce esta modalidad mediante la descripción de conductas dirigidas a alterar o manipular componentes, actualizaciones o servicios provistos por terceros.	7. Artículo 211 Bis 13 · Compromiso de la cadena de suministro tecnológico <u>Artículo 211 Bis 13.</u> Comete el delito de compromiso de la cadena de suministro tecnológico quien, mediante la alteración, sustitución o manipulación no autorizada de software, hardware, componentes, actualizaciones o servicios provistos por un tercero, comprometa la integridad, confidencialidad o disponibilidad de los sistemas o redes del usuario o cliente final que dependa de dicho proveedor. <u>A quien cometa este delito se le impondrá pena de seis a doce años de prisión y multa de mil quinientas a cuatro mil Unidades de Medida y Actualización.</u>
Sin correlativo. El Capítulo II vigente contempla agravantes para determinados supuestos de afectación a sistemas públicos. La iniciativa complementa ese esquema con un régimen aplicable a las nuevas modalidades de ciberataque, circunscrito a infraestructura pública federal o infraestructura crítica o	8. Artículo 211 Bis 14 · Agravantes por afectación a infraestructura pública o crítica, responsabilidad de personas jurídicas y reparación integral <u>Artículo 211 Bis 14. Agravantes por afectación a infraestructura pública o crítica.</u> Las penas previstas en los artículos 211 Bis 8 a 211 Bis 13 se aumentarán:



Texto vigente	Propuesta de modificación
estratégica de competencia federal, e incorpora reglas específicas sobre responsabilidad penal de personas jurídicas y reparación integral del daño.	<u>I. En una mitad, cuando la conducta se dirija, afecte o comprometa sistemas, redes, infraestructura tecnológica, plataformas o bases de datos pertenecientes o utilizadas por los Poderes de la Unión, dependencias o entidades de la Administración Pública Federal, órganos constitucionales autónomos o empresas públicas del Estado, fuera del supuesto de la fracción II;</u> Y <u>II. Hasta el doble, cuando la conducta afecte infraestructura crítica o estratégica de competencia federal cuya interrupción comprometa la seguridad nacional, la defensa, la salud pública en el ámbito federal, la continuidad de un servicio público federal, el suministro de energía, las telecomunicaciones y radiodifusión, el sistema financiero o los procesos electorales federales.</u> <u>Cuando el delito sea cometido por o a través de una persona jurídica, se estará a lo dispuesto en el artículo 11 Bis de este Código y en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, con independencia de la responsabilidad penal individual de sus directivos o representantes.</u> <u>En todos los casos procederá la reparación integral del daño, que comprenderá los costos de restitución de los sistemas afectados, la pérdida de información, la interrupción operativa y, en su caso, el rescate pagado.</u>
9. Artículo 11 Bis del Código Penal Federal · Responsabilidad penal de personas jurídicas Artículo 11 Bis. Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán	9. Artículo 11 Bis del Código Penal Federal · Responsabilidad penal de personas jurídicas Artículo 11 Bis. Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán



Texto vigente	Propuesta de modificación
imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos: A. De los previstos en el presente Código: I. a XVI. ... (Sin correlativo) B. ...	imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos: A. De los previstos en el presente Código: I. a XVI. ... <u>XVII. Ciberataques y delitos informáticos, previstos en los artículos 211 Bis 8 a 211 Bis 13;</u> B. ...

Por lo anteriormente expuesto y fundado, someto a consideración de esta Soberanía el siguiente:

DECRETO POR EL QUE SE REFORMA LA DENOMINACIÓN DEL CAPÍTULO II DEL TÍTULO NOVENO Y SE ADICIONAN UNA FRACCIÓN XVII AL APARTADO A DEL ARTÍCULO 11 BIS Y LOS ARTÍCULOS 211 BIS 8 A 211 BIS 14 AL CÓDIGO PENAL FEDERAL

ARTÍCULO ÚNICO. Se reforma la denominación del Capítulo II del Título Noveno y se adicionan una fracción XVII al apartado A del artículo 11 Bis y los artículos 211 Bis 8 a 211 Bis 14 al Código Penal Federal, para quedar como sigue:

Artículo 11 Bis. Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos:

A. De los previstos en el presente Código:

I. a XVI. ...

XVII. Ciberataques y delitos informáticos, previstos en los artículos 211 Bis 8 a 211 Bis 13;

B. ...

TÍTULO NOVENO

Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática

CAPÍTULO II

De los Ciberataques y del Acceso Ilícito a Sistemas y Equipos de Informática

Artículo 211 Bis 8. Comete el delito de desarrollo, distribución o ejecución de software o código malicioso quien, sin autorización o excediendo la autorización que se le hubiere concedido, diseñe, desarrolle, distribuya, introduzca o ejecute software o código destinado a infiltrarse, dañar, alterar el funcionamiento o tomar el control, total o parcial, de un sistema informático ajeno.

A quien cometa este delito se le impondrá pena de **cuatro a ocho años de prisión** y multa de quinientas a mil quinientas Unidades de Medida y Actualización.

No será constitutiva de este delito la conducta realizada en el marco de actividades de investigación en seguridad informática, pruebas de penetración autorizadas o programas de reporte responsable de vulnerabilidades, siempre que exista consentimiento del titular del sistema afectado y la conducta se mantenga dentro de los términos de la autorización otorgada.

Artículo 211 Bis 9. Comete el delito de secuestro de datos quien, mediante software o código, cifre, bloquee o restrinja de cualquier forma el acceso legítimo a sistemas informáticos, redes o datos ajenos, condicionando su restitución, liberación o desbloqueo a la entrega de un rescate económico o de cualquier otra naturaleza.

A quien cometa este delito se le impondrá pena de **seis a doce años de prisión** y multa de mil a tres mil Unidades de Medida y Actualización.

La pena se aumentará en una mitad cuando, además, el sujeto activo amenace con divulgar, vender o hacer pública la información sustraída como medio de presión para obtener el rescate.

Artículo 211 Bis 10. Comete el delito de suplantación por medios electrónicos con fines de apropiación de información quien simule la identidad de una persona física, persona jurídica o institución legítima, con el fin de engañar a otra persona y obtener, sin su consentimiento, credenciales de acceso, datos personales, financieros o cualquier información confidencial.

A quien cometa este delito se le impondrá pena de **uno a tres años de prisión** y multa de cien a trescientas Unidades de Medida y Actualización.

Cuando de la conducta se derive un daño patrimonial efectivo, robo de identidad o acceso no autorizado consumado a cuentas o sistemas de la víctima, la pena será de **cuatro a ocho años de prisión** y multa de quinientas a mil Unidades de Medida y Actualización, sin perjuicio de las reglas de concurso que resulten aplicables con el delito de fraude.

Artículo 211 Bis 11. Comete el delito de interrupción deliberada de servicios informáticos quien, mediante el envío masivo y coordinado de tráfico, solicitudes o instrucciones, valiéndose o no de una red de dispositivos comprometidos, sature, inhabilite o interrumpa deliberadamente la disponibilidad de un sistema, red o servicio informático ajeno.

A quien cometa este delito se le impondrá pena de **cuatro a nueve años de prisión** y multa de quinientas a mil quinientas Unidades de Medida y Actualización.

Artículo 211 Bis 12. Comete el delito de intrusión sostenida con fines de espionaje o sabotaje quien, mediante técnicas de intrusión encubierta y sostenida en el tiempo, acceda o permanezca sin autorización dentro de un sistema o red informática ajena, con el propósito de realizar espionaje, sabotaje o extracción continuada de información.

A quien cometa este delito se le impondrá pena de **seis a quince años de prisión** y multa de dos mil a cinco mil Unidades de Medida y Actualización.

Para la individualización de la pena dentro del rango previsto, el juzgador atenderá a la duración de la intrusión, la sensibilidad de la información comprometida y el grado de sofisticación técnica empleado.

Artículo 211 Bis 13. Comete el delito de compromiso de la cadena de suministro tecnológico quien, mediante la alteración, sustitución o manipulación no autorizada de software, hardware, componentes, actualizaciones o servicios provistos por un tercero, comprometa la integridad, confidencialidad o disponibilidad de los sistemas o redes del usuario o cliente final que dependa de dicho proveedor.

A quien cometa este delito se le impondrá pena de **seis a doce años de prisión** y multa de mil quinientas a cuatro mil Unidades de Medida y Actualización.

Artículo 211 Bis 14. Agravantes por afectación a infraestructura pública o crítica. Las penas previstas en los artículos 211 Bis 8 a 211 Bis 13 se aumentarán:

I. En una mitad, cuando la conducta se dirija, afecte o comprometa sistemas, redes, infraestructura tecnológica, plataformas o bases de datos pertenecientes o utilizadas por los Poderes de la Unión, dependencias o entidades de la Administración Pública Federal, órganos constitucionales autónomos o empresas públicas del Estado, fuera del supuesto de la fracción II; y

II. Hasta el doble, cuando la conducta afecte infraestructura crítica o estratégica de competencia federal cuya interrupción comprometa la seguridad nacional, la defensa, la salud pública en el ámbito federal, la continuidad de un servicio público federal, el suministro de energía, las telecomunicaciones y radiodifusión, el sistema financiero o los procesos electorales federales.

Cuando el delito sea cometido por o a través de una persona jurídica, se estará a lo dispuesto en el artículo 11 Bis de este Código y en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, con independencia de la responsabilidad penal individual de sus directivos o representantes. En todos los casos procederá la reparación integral del daño, que comprenderá los costos de restitución de los sistemas afectados, la pérdida de información, la interrupción operativa y, en su caso, el rescate pagado.

TRANSITORIOS

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

SEGUNDO. Las conductas cometidas con anterioridad a la entrada en vigor del presente Decreto se juzgarán conforme a las disposiciones vigentes al momento de su comisión, salvo que la nueva legislación resulte más favorable a la persona imputada, en cuyo caso se aplicará ésta de conformidad con el artículo 14, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos y el artículo 56 del Código Penal Federal.

TERCERO. La aplicación de los tipos penales que se adicionan se realizará con cargo a los presupuestos autorizados de las autoridades ministeriales y judiciales competentes, por lo que la entrada en vigor del presente Decreto no requerirá la asignación de recursos adicionales ni la creación de estructuras administrativas o plazas.

CUARTO. La Fiscalía General de la República y el Poder Judicial de la Federación, en el ámbito de sus respectivas competencias y con cargo a sus presupuestos autorizados, capacitarán a su personal ministerial y judicial en la investigación, persecución y juzgamiento de las conductas previstas en el presente Decreto, dentro de los ciento ochenta días naturales siguientes a su entrada en vigor.

ATENTAMENTE



DIP. GISELLE YUNUEEN ARELLANO ÁVILA

**DADO EN PALACIO LEGISLATIVO DE SAN LÁZARO, A 1 DE SEPTIEMBRE DE
2026.**

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN V TER AL ARTÍCULO 3o DE LA LEY GENERAL DEL EQUILIBRIO ECOLÓGICO Y LA PROTECCIÓN AL AMBIENTE, EN MATERIA DE DEFINICIÓN DE LA CIENCIA CIUDADANA, EN ARMONIZACIÓN CON LOS ESTÁNDARES INTERNACIONALES DE CIENCIA ABIERTA

La proponente, **Giselle Yunueen Arellano Ávila**, Diputada Federal del grupo parlamentario MORENA de la LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en el artículo 71, fracción II y 135 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 6, numeral 1, fracción I, 77 y 78 y 82 fracción I del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de decreto por el que se adiciona una fracción V Ter al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

I. ANTECEDENTES

La Ley General del Equilibrio Ecológico y la Protección al Ambiente, publicada en el Diario Oficial de la Federación el 28 de enero de 1988, constituye el ordenamiento marco de la política ambiental mexicana. Su artículo 3o. es el catálogo de definiciones sobre el cual se articulan las categorías conceptuales que dan sustento operativo al resto de la ley: ambiente, aprovechamiento sustentable, biodiversidad, biotecnología, cambio climático, contaminación, contingencia ambiental, criterios ecológicos, ecosistema, entre otras. La incorporación de nuevas definiciones al artículo 3o. ha sido, a lo largo de las últimas tres décadas, la vía técnicamente adecuada para actualizar el ordenamiento conforme evolucionan los paradigmas científicos y las prácticas de gestión ambiental.

Entre las categorías incorporadas por reformas sucesivas al artículo 3o. figuran, entre otras, el **cambio climático** —adicionado por decreto publicado el 28 de enero de 2011, como fracción V Bis—, la **contaminación por ruido** —adicionada como fracción VI Ter— y la **luz intrusa** —adicionada como fracción XX Bis en materia de contaminación lumínica—. La técnica legislativa empleada permite incorporar categorías adicionales mediante fracciones intercalares —Bis, Ter y las que correspondan—, preservando la numeración de las fracciones ordinarias subsiguientes.



La presente iniciativa se inscribe en esa línea de actualización conceptual. Su objeto es incorporar al artículo 3o. la definición de **ciencia ciudadana**, categoría hoy consolidada en el ordenamiento internacional de ciencia abierta y aplicada de forma creciente en la política ambiental mexicana, particularmente en materia de monitoreo de calidad del aire, biodiversidad, calidad del agua y observación de fenómenos climáticos. La adición de la fracción permite que la ley reconozca expresamente esta modalidad de generación de conocimiento y proporciona base terminológica clara a las autoridades federales, estatales y municipales para incorporarla en sus programas.

II. MARCO CONSTITUCIONAL

La reforma que se propone encuentra sustento directo en diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, tanto por los derechos que tutela como por la competencia legislativa del Congreso de la Unión.

En primer término, el **artículo 4o.** reconoce el derecho de toda persona a un medio ambiente sano para su desarrollo y bienestar, así como el deber del Estado de garantizarlo. La generación de información ambiental de calidad, oportuna y suficientemente distribuida en el territorio es una condición material relevante para la protección de ese derecho. La ciencia ciudadana puede ampliar la base de información disponible y contribuir a observar zonas o fenómenos que la infraestructura institucional convencional no siempre alcanza.

En segundo término, el **artículo 3o., fracciones V y VII**, mandata al Estado apoyar la investigación científica y tecnológica y garantizar la libertad de investigación en las instituciones de educación superior. La ciencia ciudadana es una modalidad reconocida internacionalmente de participación en la investigación científica, complementaria a la que realizan las instituciones formales, y encuentra en este precepto constitucional base habilitante clara.

En tercer término, el **artículo 6o., apartado A**, garantiza el derecho de acceso a la información. La ciencia ciudadana puede contribuir a ampliar la disponibilidad de datos e información ambiental para investigadores, autoridades y sociedad, con sujeción a la legislación aplicable y a los estándares de calidad, protección de datos

y demás salvaguardas que correspondan. Reconocer la categoría en la ley marco resulta congruente con los principios de transparencia y máxima publicidad.

Finalmente, el **artículo 73, fracción XXIX-G**, faculta al Congreso de la Unión para expedir leyes que establezcan la concurrencia del Gobierno Federal, de las entidades federativas, de los Municipios y, en su caso, de las demarcaciones territoriales de la Ciudad de México, en el ámbito de sus respectivas competencias, en materia de protección al ambiente, preservación y restauración del equilibrio ecológico. Esta habilitación constituye el fundamento competencial directo para actualizar la Ley General del Equilibrio Ecológico y la Protección al Ambiente mediante una definición de alcance conceptual.

III. MARCO INTERNACIONAL

La ciencia ciudadana es, desde 2021, categoría formalmente reconocida por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en el ordenamiento internacional de ciencia abierta. Diversas jurisdicciones de referencia han incorporado la categoría a sus ordenamientos nacionales, y otras la han desarrollado por la vía de políticas públicas oficiales de sus agencias de ciencia y tecnología. El panorama internacional que sustenta la presente iniciativa se despliega en cinco referentes principales.

1. Recomendación de la UNESCO sobre la Ciencia Abierta (2021)

La Recomendación sobre la Ciencia Abierta, adoptada por la Conferencia General de la UNESCO en su 41ª reunión, celebrada del 9 al 24 de noviembre de 2021, es el primer instrumento internacional de establecimiento de normas en materia de ciencia abierta.¹ Aprobada por los 193 Estados Miembros de la Organización, la Recomendación define la ciencia abierta como un constructo inclusivo que combina diversos movimientos y prácticas para hacer que el conocimiento científico esté abierta y libremente disponible, sea accesible y reutilizable, aumente las colaboraciones científicas y el intercambio de información en beneficio de la ciencia

¹ Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Recomendación sobre la Ciencia Abierta, adoptada por la Conferencia General en su 41ª reunión, París, 23 de noviembre de 2021. Instrumento aprobado por los 193 Estados Miembros de la Organización.



y la sociedad, y abra los procesos de creación, evaluación y comunicación del conocimiento científico a los actores sociales más allá de la comunidad científica tradicional.

La Recomendación identifica cuatro pilares interconectados de la ciencia abierta, uno de los cuales es precisamente el **compromiso abierto con los actores sociales**, dentro del cual la ciencia ciudadana ocupa un lugar central. El instrumento reconoce que la ciencia ciudadana y la participación de la ciudadanía se han desarrollado como modelos de investigación científica llevados a cabo por personas no profesionales de la ciencia, siguiendo metodologías científicamente válidas y frecuentemente en asociación con programas científicos formales o con personas profesionales de la ciencia. México, en su calidad de Estado Miembro de la UNESCO, se encuentra entre los destinatarios de la Recomendación y puede avanzar en su implementación conforme a su contexto constitucional, jurídico e institucional.

2. Reino de España · Ley 17/2022 de la Ciencia, la Tecnología y la Innovación

La **Ley 17/2022, de 5 de septiembre**, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, constituye un referente especialmente relevante en el ámbito iberoamericano. La reforma española, publicada en el Boletín Oficial del Estado el 6 de septiembre de 2022 y vigente desde el 7 de septiembre del mismo año, dedica el **artículo 37** al fomento de la ciencia abierta y el **artículo 38** a la participación de la sociedad civil en los procesos científicos. El preámbulo de la ley reconoce el valor de la ciencia como bien común y establece expresamente el fomento de la participación de la ciudadanía en el proceso científico-técnico en todas sus fases: definición de agendas de investigación, observación, recopilación y procesamiento de datos, y otros procesos de participación ciudadana. La regulación muestra la incorporación expresa de la participación ciudadana en el marco legal de ciencia abierta.

3. Comunidad Autónoma de Cataluña · Ley 9/2022 de la Ciencia

La **Ley 9/2022, de 21 de diciembre, de la ciencia**, aprobada por el Parlamento de Cataluña, es referente subnacional relevante porque desarrolla la ciencia ciudadana como eje coordinador y vertebrador del sistema catalán de ciencia abierta. La ley se

propone consolidar el sistema de conocimiento con la implicación de todos los agentes, de modo que la investigación y la transferencia del conocimiento se realicen de forma más cooperativa, transparente y accesible a la ciudadanía. Es prueba de que la categoría normativa admite desarrollos tanto en el orden nacional como en el subnacional, referencia útil para el modelo federal mexicano.

4. República Argentina · Política pública de ciencia ciudadana del Ministerio de Ciencia, Tecnología e Innovación

La República Argentina desarrolla la ciencia ciudadana como política pública oficial mediante el **Programa Nacional de Promoción de la Ciencia Ciudadana**, creado por la **Resolución 620/2022** del entonces Ministerio de Ciencia, Tecnología e Innovación. El programa reconoce la ciencia ciudadana como una modalidad de generación de conocimiento científico con participación activa de comunidades y personas no profesionales de la ciencia, y promueve el fortalecimiento, la visibilización y el financiamiento de proyectos en la materia. Argentina ilustra un modelo de desarrollo de la categoría por la vía de política pública sectorial, complementaria al reconocimiento normativo.

5. República de Colombia · Política Nacional de Ciencia Abierta

La República de Colombia incorpora la ciencia ciudadana como componente central de la **Política Nacional de Ciencia Abierta**, formulada por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias), y de la **Política Pública de Apropiación Social del Conocimiento en el marco de la Ciencia, Tecnología e Innovación (2021)**. Ambos instrumentos reconocen la ciencia ciudadana como estrategia para acercar la ciencia a la sociedad, generar condiciones para el uso, inclusión e intercambio de saberes y conocimientos en ciencia, tecnología e innovación, y avanzar en la democratización del conocimiento. Colombia representa el modelo latinoamericano más articulado de incorporación de la categoría en instrumentos oficiales de política.

El panorama internacional confirma la solidez conceptual de la categoría **ciencia ciudadana** como estándar contemporáneo de ciencia abierta. La presente iniciativa incorpora la definición al ordenamiento mexicano, en congruencia con la



Recomendación de la UNESCO de 2021 y con las mejores prácticas de referentes iberoamericanos.

IV. CRITERIOS JURISPRUDENCIALES

El Poder Judicial de la Federación ha desarrollado criterios que vinculan la tutela ambiental con la participación social. La Primera Sala de la Suprema Corte de Justicia de la Nación, en la tesis **1a. CCXC/2018 (10a.), registro digital 2018694**, de rubro **“INTERÉS LEGÍTIMO PARA PROMOVER UN JUICIO DE AMPARO EN MATERIA AMBIENTAL. OBLIGACIÓN DE LOS JUZGADORES EN SU ANÁLISIS”**, sostuvo que, a la luz del principio de participación ciudadana y del correlativo de iniciativa pública, el Estado debe fomentar la participación de la ciudadanía en la defensa del medio ambiente y crear entornos propicios para ese efecto.

Asimismo, la Segunda Sala, en la tesis **2a. LXXII/2010, registro digital 164105**, de rubro **“DERECHO A LA INFORMACIÓN MEDIOAMBIENTAL. SON INCONSTITUCIONALES LOS ACTOS DE AUTORIDAD QUE DENIEGAN, EN FORMA ABSOLUTA, LA OBTENCIÓN DE AQUÉLLA”**, reconoció la relevancia de contar con información ambiental oportuna, idónea y necesaria y vinculó su disponibilidad con los principios de máxima publicidad y transparencia. Más recientemente, la jurisprudencia **1a./J. 158/2025 (11a.), registro digital 2030816**, reiteró que el derecho a un medio ambiente sano posee una dimensión objetiva, que exige un sistema normativo e institucional de preservación y restauración de los ecosistemas. Estos criterios ofrecen sustento constitucional suficiente para una reforma de carácter definitorio que favorece la participación social y la disponibilidad de información ambiental, sin crear nuevas atribuciones sustantivas.

V. DERECHO COMPARADO

El apartado internacional de la presente iniciativa despliega los principales referentes internacionales aplicables. A efecto de ofrecer al lector una síntesis comparada, se presenta el siguiente cuadro con las jurisdicciones y sus respectivos instrumentos:

Jurisdicción	Instrumento	Naturaleza
UNESCO (193 Estados Miembros)	Recomendación sobre la Ciencia Abierta (2021)	Instrumento internacional de establecimiento de normas.



Jurisdicción	Instrumento	Naturaleza
Reino de España	Ley 17/2022 de la Ciencia, la Tecnología y la Innovación (artículos 37 y 38)	Ley nacional.
Cataluña (España)	Ley 9/2022 de la ciencia	Ley subnacional autonómica.
República Argentina	Programa Nacional de Promoción de la Ciencia Ciudadana, creado por Resolución 620/2022	Política pública sectorial.
República de Colombia	Política Nacional de Ciencia Abierta y Política Pública de Apropiación Social del Conocimiento (2021)	Instrumentos oficiales de política.
Estados Unidos Mexicanos	(Sin definición en la ley marco)	Aplicación operativa sin reconocimiento normativo expreso.

El cuadro evidencia que la incorporación de la definición al ordenamiento mexicano se inscribe en una tendencia consolidada de reconocimiento normativo internacional, y armoniza el ordenamiento interno con los estándares que la UNESCO y las jurisdicciones de referencia han desarrollado.

VI. DIAGNÓSTICO Y JUSTIFICACIÓN

La ciencia ciudadana se practica desde hace décadas en México, principalmente en materia ambiental, aunque sin reconocimiento normativo expreso en la ley marco del sector. Instituciones del sistema nacional de ciencia y tecnología, universidades públicas, instancias especializadas como la **Comisión Nacional para el Conocimiento y Uso de la Biodiversidad (CONABIO)** —comisión intersecretarial que opera, entre otros instrumentos, a través de la plataforma **Naturalista**—, y organizaciones de la sociedad civil implementan proyectos de ciencia ciudadana en materia de monitoreo de biodiversidad, calidad del aire, calidad del agua, observación climática y salud ambiental. La generación de datos por vía ciudadana puede complementar la infraestructura institucional convencional y contribuir a observar zonas y fenómenos que de otro modo quedarían fuera del alcance del monitoreo formal.

El reconocimiento normativo de la categoría en el artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente aporta cuatro beneficios concretos. Primero, proporciona a las autoridades federales, estatales y municipales una



referencia terminológica común para identificar la ciencia ciudadana dentro de sus programas ambientales, sin depender de definiciones dispersas. Segundo, ofrece una base conceptual susceptible de facilitar, conforme a las disposiciones y estándares que resulten aplicables, el aprovechamiento institucional de datos generados mediante proyectos de ciencia ciudadana. Tercero, fortalece la posición de las instituciones mexicanas que participan en redes internacionales de ciencia ciudadana, al contar con una categoría nacional armonizada con la Recomendación de la UNESCO de 2021. Cuarto, reconoce una modalidad de participación social compatible con el derecho de acceso a la información y con el derecho a un medio ambiente sano reconocidos por la Constitución.

La incorporación de la definición permite armonizar el ordenamiento interno con estándares internacionales que la comunidad científica y diversas jurisdicciones han consolidado en la última década. La presente iniciativa opta por una intervención normativa acotada: la adición de una fracción intercalar al catálogo de definiciones vigente, sin alterar competencias, procedimientos ni estructuras administrativas.

VII. IMPACTO REGULATORIO

La presente iniciativa no genera impacto regulatorio adicional. La reforma no da lugar a disposiciones de observancia obligatoria distintas de las que ya rigen en materia ambiental; no instituye permisos, licencias, autorizaciones ni trámites de especie alguna; no altera los requisitos previstos para el ejercicio de funciones públicas; ni incide en las normas reglamentarias o disposiciones administrativas vigentes. Se limita a incorporar al catálogo de definiciones del artículo 3o. una categoría conceptual que aporta claridad interpretativa y base terminológica común para los operadores del sistema.

VIII. IMPACTO PRESUPUESTARIO

La presente iniciativa no requiere la asignación de recursos presupuestales adicionales. La adición de una fracción al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente no crea estructuras administrativas, organismos, plazas ni programas de gasto. Los proyectos de ciencia ciudadana que actualmente operan en México se realizan con cargo a los presupuestos autorizados



de las instituciones participantes y con recursos de la sociedad civil y de la cooperación internacional; la reforma no altera esa configuración financiera. El reconocimiento normativo, por su naturaleza definitoria, es plenamente compatible con la política de responsabilidad hacendaria.

IX. IMPACTO SOCIAL

El impacto social de la reforma es favorable, potencial e indirecto. El reconocimiento de la ciencia ciudadana puede ampliar la visibilidad de la participación social en la generación de conocimiento ambiental, con especial relevancia para comunidades rurales, indígenas y periurbanas que desarrollan actividades de observación y monitoreo de biodiversidad y calidad ambiental en sus territorios. La reforma no crea programas ni prestaciones nuevas; aporta una referencia jurídica común que puede facilitar la consideración de estas prácticas en la política ambiental vigente. Al alinear el ordenamiento interno con estándares internacionales, también favorece condiciones de cooperación técnica e intercambio de conocimiento sin generar obligaciones presupuestarias adicionales.

CUADRO COMPARATIVO

Para claridad de la propuesta, se presenta a continuación el cuadro comparativo entre el texto vigente del artículo 3º. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente y la propuesta de modificación. La adición se destaca en negritas y subrayado; el resto del articulado se conserva sin modificación, manteniéndose la numeración de las fracciones subsecuentes.

Texto Vigente	Propuesta de Modificación
Artículo 3º · Adición de fracción en materia de ciencia ciudadana	
Artículo 3o. Para los efectos de esta Ley se entiende por:	Artículo 3o. Para los efectos de esta Ley se entiende por:
I. Ambiente: [...]	I. Ambiente: [...]
II. Áreas naturales protegidas: [...]	II. Áreas naturales protegidas: [...]
III. Aprovechamiento sustentable: [...]	III. Aprovechamiento sustentable: [...]



Texto Vigente	Propuesta de Modificación
IV. Biodiversidad: [...]	IV. Biodiversidad: [...]
V. Biotecnología: [...]	V. Biotecnología: [...]
V Bis. Cambio climático: [...]	V Bis. Cambio climático: [...]
(Sin correlativo)	<u>V Ter. Ciencia ciudadana: modalidad de generación de conocimiento científico en la que personas no profesionales de la ciencia participan de manera activa y estructurada, de forma individual o colaborativa, mediante la recolección, análisis, interpretación o difusión de datos o información ambiental, conforme a metodologías científicamente válidas, con la finalidad de contribuir al conocimiento científico y a la toma de decisiones en materia ambiental.</u>
VI. Contaminación: [...]	VI. Contaminación: [...]
VI Bis. [...]	VI Bis. [...]
VI Ter. Contaminación por ruido: [...]	VI Ter. Contaminación por ruido: [...]
[El resto de fracciones se conserva sin modificación.]	[El resto de fracciones se conserva sin modificación.]

Por lo anteriormente expuesto y fundado, someto a la consideración esta Soberanía el siguiente:

**DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN V TER AL ARTÍCULO 3º.
DE LA LEY GENERAL DEL EQUILIBRIO ECOLÓGICO Y LA PROTECCIÓN AL
AMBIENTE**

ARTÍCULO ÚNICO. Se adiciona una fracción V Ter al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente, para quedar como sigue:

Artículo 3o. Para los efectos de esta Ley se entiende por:

I. a V Bis. ...

V Ter. Ciencia ciudadana: modalidad de generación de conocimiento científico en la que personas no profesionales de la ciencia participan de manera activa y estructurada, de forma individual o colaborativa, mediante la recolección, análisis, interpretación o difusión de datos o información ambiental, conforme a metodologías científicamente válidas, con la finalidad de contribuir al conocimiento científico y a la toma de decisiones en materia ambiental.

VI. a XXXIX. ...

TRANSITORIOS

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

SEGUNDO. La aplicación de la reforma que este Decreto contiene se realizará con cargo a los presupuestos autorizados de las autoridades competentes, por lo que su entrada en vigor no requerirá la asignación de recursos adicionales ni la creación de estructuras administrativas o plazas.

ATENTAMENTE

DIP. GISELLE YUNUEEN ARELLANO ÁVILA

**DADO EN PALACIO LEGISLATIVO DE SAN LÁZARO, A 1 DE SEPTIEMBRE DE
2026.**



INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN V TER AL ARTÍCULO 3o DE LA LEY GENERAL DEL EQUILIBRIO ECOLÓGICO Y LA PROTECCIÓN AL AMBIENTE, EN MATERIA DE DEFINICIÓN DE LA CIENCIA CIUDADANA, EN ARMONIZACIÓN CON LOS ESTÁNDARES INTERNACIONALES DE CIENCIA ABIERTA

La proponente, **Giselle Yunueen Arellano Ávila**, Diputada Federal del grupo parlamentario MORENA de la LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en el artículo 71, fracción II y 135 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 6, numeral 1, fracción I, 77 y 78 y 82 fracción I del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de decreto por el que se adiciona una fracción V Ter al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

I. ANTECEDENTES

La Ley General del Equilibrio Ecológico y la Protección al Ambiente, publicada en el Diario Oficial de la Federación el 28 de enero de 1988, constituye el ordenamiento marco de la política ambiental mexicana. Su artículo 3o. es el catálogo de definiciones sobre el cual se articulan las categorías conceptuales que dan sustento operativo al resto de la ley: ambiente, aprovechamiento sustentable, biodiversidad, biotecnología, cambio climático, contaminación, contingencia ambiental, criterios ecológicos, ecosistema, entre otras. La incorporación de nuevas definiciones al artículo 3o. ha sido, a lo largo de las últimas tres décadas, la vía técnicamente adecuada para actualizar el ordenamiento conforme evolucionan los paradigmas científicos y las prácticas de gestión ambiental.

Entre las categorías incorporadas por reformas sucesivas al artículo 3o. figuran, entre otras, el **cambio climático** —adicionado por decreto publicado el 28 de enero de 2011, como fracción V Bis—, la **contaminación por ruido** —adicionada como fracción VI Ter— y la **luz intrusa** —adicionada como fracción XX Bis en materia de contaminación lumínica—. La técnica legislativa empleada permite incorporar categorías adicionales mediante fracciones intercalares —Bis, Ter y las que correspondan—, preservando la numeración de las fracciones ordinarias subsecuentes.



La presente iniciativa se inscribe en esa línea de actualización conceptual. Su objeto es incorporar al artículo 3o. la definición de **ciencia ciudadana**, categoría hoy consolidada en el ordenamiento internacional de ciencia abierta y aplicada de forma creciente en la política ambiental mexicana, particularmente en materia de monitoreo de calidad del aire, biodiversidad, calidad del agua y observación de fenómenos climáticos. La adición de la fracción permite que la ley reconozca expresamente esta modalidad de generación de conocimiento y proporciona base terminológica clara a las autoridades federales, estatales y municipales para incorporarla en sus programas.

II. MARCO CONSTITUCIONAL

La reforma que se propone encuentra sustento directo en diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, tanto por los derechos que tutela como por la competencia legislativa del Congreso de la Unión.

En primer término, el **artículo 4o.** reconoce el derecho de toda persona a un medio ambiente sano para su desarrollo y bienestar, así como el deber del Estado de garantizarlo. La generación de información ambiental de calidad, oportuna y suficientemente distribuida en el territorio es una condición material relevante para la protección de ese derecho. La ciencia ciudadana puede ampliar la base de información disponible y contribuir a observar zonas o fenómenos que la infraestructura institucional convencional no siempre alcanza.

En segundo término, el **artículo 3o., fracciones V y VII**, mandata al Estado apoyar la investigación científica y tecnológica y garantizar la libertad de investigación en las instituciones de educación superior. La ciencia ciudadana es una modalidad reconocida internacionalmente de participación en la investigación científica, complementaria a la que realizan las instituciones formales, y encuentra en este precepto constitucional base habilitante clara.

En tercer término, el **artículo 6o., apartado A**, garantiza el derecho de acceso a la información. La ciencia ciudadana puede contribuir a ampliar la disponibilidad de datos e información ambiental para investigadores, autoridades y sociedad, con sujeción a la legislación aplicable y a los estándares de calidad, protección de datos



y demás salvaguardas que correspondan. Reconocer la categoría en la ley marco resulta congruente con los principios de transparencia y máxima publicidad.

Finalmente, el **artículo 73, fracción XXIX-G**, faculta al Congreso de la Unión para expedir leyes que establezcan la concurrencia del Gobierno Federal, de las entidades federativas, de los Municipios y, en su caso, de las demarcaciones territoriales de la Ciudad de México, en el ámbito de sus respectivas competencias, en materia de protección al ambiente, preservación y restauración del equilibrio ecológico. Esta habilitación constituye el fundamento competencial directo para actualizar la Ley General del Equilibrio Ecológico y la Protección al Ambiente mediante una definición de alcance conceptual.

III. MARCO INTERNACIONAL

La ciencia ciudadana es, desde 2021, categoría formalmente reconocida por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en el ordenamiento internacional de ciencia abierta. Diversas jurisdicciones de referencia han incorporado la categoría a sus ordenamientos nacionales, y otras la han desarrollado por la vía de políticas públicas oficiales de sus agencias de ciencia y tecnología. El panorama internacional que sustenta la presente iniciativa se despliega en cinco referentes principales.

1. Recomendación de la UNESCO sobre la Ciencia Abierta (2021)

La Recomendación sobre la Ciencia Abierta, adoptada por la Conferencia General de la UNESCO en su 41ª reunión, celebrada del 9 al 24 de noviembre de 2021, es el primer instrumento internacional de establecimiento de normas en materia de ciencia abierta.¹ Aprobada por los 193 Estados Miembros de la Organización, la Recomendación define la ciencia abierta como un constructo inclusivo que combina diversos movimientos y prácticas para hacer que el conocimiento científico esté abierta y libremente disponible, sea accesible y reutilizable, aumente las colaboraciones científicas y el intercambio de información en beneficio de la ciencia

¹ Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Recomendación sobre la Ciencia Abierta, adoptada por la Conferencia General en su 41ª reunión, París, 23 de noviembre de 2021. Instrumento aprobado por los 193 Estados Miembros de la Organización.

y la sociedad, y abra los procesos de creación, evaluación y comunicación del conocimiento científico a los actores sociales más allá de la comunidad científica tradicional.

La Recomendación identifica cuatro pilares interconectados de la ciencia abierta, uno de los cuales es precisamente el **compromiso abierto con los actores sociales**, dentro del cual la ciencia ciudadana ocupa un lugar central. El instrumento reconoce que la ciencia ciudadana y la participación de la ciudadanía se han desarrollado como modelos de investigación científica llevados a cabo por personas no profesionales de la ciencia, siguiendo metodologías científicamente válidas y frecuentemente en asociación con programas científicos formales o con personas profesionales de la ciencia. México, en su calidad de Estado Miembro de la UNESCO, se encuentra entre los destinatarios de la Recomendación y puede avanzar en su implementación conforme a su contexto constitucional, jurídico e institucional.

2. Reino de España · Ley 17/2022 de la Ciencia, la Tecnología y la Innovación

La **Ley 17/2022, de 5 de septiembre**, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, constituye un referente especialmente relevante en el ámbito iberoamericano. La reforma española, publicada en el Boletín Oficial del Estado el 6 de septiembre de 2022 y vigente desde el 7 de septiembre del mismo año, dedica el **artículo 37** al fomento de la ciencia abierta y el **artículo 38** a la participación de la sociedad civil en los procesos científicos. El preámbulo de la ley reconoce el valor de la ciencia como bien común y establece expresamente el fomento de la participación de la ciudadanía en el proceso científico-técnico en todas sus fases: definición de agendas de investigación, observación, recopilación y procesamiento de datos, y otros procesos de participación ciudadana. La regulación muestra la incorporación expresa de la participación ciudadana en el marco legal de ciencia abierta.

3. Comunidad Autónoma de Cataluña · Ley 9/2022 de la Ciencia

La **Ley 9/2022, de 21 de diciembre, de la ciencia**, aprobada por el Parlamento de Cataluña, es referente subnacional relevante porque desarrolla la ciencia ciudadana como eje coordinador y vertebrador del sistema catalán de ciencia abierta. La ley se

propone consolidar el sistema de conocimiento con la implicación de todos los agentes, de modo que la investigación y la transferencia del conocimiento se realicen de forma más cooperativa, transparente y accesible a la ciudadanía. Es prueba de que la categoría normativa admite desarrollos tanto en el orden nacional como en el subnacional, referencia útil para el modelo federal mexicano.

4. República Argentina · Política pública de ciencia ciudadana del Ministerio de Ciencia, Tecnología e Innovación

La República Argentina desarrolla la ciencia ciudadana como política pública oficial mediante el **Programa Nacional de Promoción de la Ciencia Ciudadana**, creado por la **Resolución 620/2022** del entonces Ministerio de Ciencia, Tecnología e Innovación. El programa reconoce la ciencia ciudadana como una modalidad de generación de conocimiento científico con participación activa de comunidades y personas no profesionales de la ciencia, y promueve el fortalecimiento, la visibilización y el financiamiento de proyectos en la materia. Argentina ilustra un modelo de desarrollo de la categoría por la vía de política pública sectorial, complementaria al reconocimiento normativo.

5. República de Colombia · Política Nacional de Ciencia Abierta

La República de Colombia incorpora la ciencia ciudadana como componente central de la **Política Nacional de Ciencia Abierta**, formulada por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias), y de la **Política Pública de Apropiación Social del Conocimiento en el marco de la Ciencia, Tecnología e Innovación (2021)**. Ambos instrumentos reconocen la ciencia ciudadana como estrategia para acercar la ciencia a la sociedad, generar condiciones para el uso, inclusión e intercambio de saberes y conocimientos en ciencia, tecnología e innovación, y avanzar en la democratización del conocimiento. Colombia representa el modelo latinoamericano más articulado de incorporación de la categoría en instrumentos oficiales de política.

El panorama internacional confirma la solidez conceptual de la categoría **ciencia ciudadana** como estándar contemporáneo de ciencia abierta. La presente iniciativa incorpora la definición al ordenamiento mexicano, en congruencia con la



Recomendación de la UNESCO de 2021 y con las mejores prácticas de referentes iberoamericanos.

IV. CRITERIOS JURISPRUDENCIALES

El Poder Judicial de la Federación ha desarrollado criterios que vinculan la tutela ambiental con la participación social. La Primera Sala de la Suprema Corte de Justicia de la Nación, en la tesis **1a. CCXC/2018 (10a.), registro digital 2018694**, de rubro **“INTERÉS LEGÍTIMO PARA PROMOVER UN JUICIO DE AMPARO EN MATERIA AMBIENTAL. OBLIGACIÓN DE LOS JUZGADORES EN SU ANÁLISIS”**, sostuvo que, a la luz del principio de participación ciudadana y del correlativo de iniciativa pública, el Estado debe fomentar la participación de la ciudadanía en la defensa del medio ambiente y crear entornos propicios para ese efecto.

Asimismo, la Segunda Sala, en la tesis **2a. LXXII/2010, registro digital 164105**, de rubro **“DERECHO A LA INFORMACIÓN MEDIOAMBIENTAL. SON INCONSTITUCIONALES LOS ACTOS DE AUTORIDAD QUE DENIEGAN, EN FORMA ABSOLUTA, LA OBTENCIÓN DE AQUÉLLA”**, reconoció la relevancia de contar con información ambiental oportuna, idónea y necesaria y vinculó su disponibilidad con los principios de máxima publicidad y transparencia. Más recientemente, la jurisprudencia **1a./J. 158/2025 (11a.), registro digital 2030816**, reiteró que el derecho a un medio ambiente sano posee una dimensión objetiva, que exige un sistema normativo e institucional de preservación y restauración de los ecosistemas. Estos criterios ofrecen sustento constitucional suficiente para una reforma de carácter definitorio que favorece la participación social y la disponibilidad de información ambiental, sin crear nuevas atribuciones sustantivas.

V. DERECHO COMPARADO

El apartado internacional de la presente iniciativa despliega los principales referentes internacionales aplicables. A efecto de ofrecer al lector una síntesis comparada, se presenta el siguiente cuadro con las jurisdicciones y sus respectivos instrumentos:

Jurisdicción	Instrumento	Naturaleza
UNESCO (193 Estados Miembros)	Recomendación sobre la Ciencia Abierta (2021)	Instrumento internacional de establecimiento de normas.



Jurisdicción	Instrumento	Naturaleza
Reino de España	Ley 17/2022 de la Ciencia, la Tecnología y la Innovación (artículos 37 y 38)	Ley nacional.
Cataluña (España)	Ley 9/2022 de la ciencia	Ley subnacional autonómica.
República Argentina	Programa Nacional de Promoción de la Ciencia Ciudadana, creado por Resolución 620/2022	Política pública sectorial.
República de Colombia	Política Nacional de Ciencia Abierta y Política Pública de Apropiación Social del Conocimiento (2021)	Instrumentos oficiales de política.
Estados Unidos Mexicanos	(Sin definición en la ley marco)	Aplicación operativa sin reconocimiento normativo expreso.

El cuadro evidencia que la incorporación de la definición al ordenamiento mexicano se inscribe en una tendencia consolidada de reconocimiento normativo internacional, y armoniza el ordenamiento interno con los estándares que la UNESCO y las jurisdicciones de referencia han desarrollado.

VI. DIAGNÓSTICO Y JUSTIFICACIÓN

La ciencia ciudadana se practica desde hace décadas en México, principalmente en materia ambiental, aunque sin reconocimiento normativo expreso en la ley marco del sector. Instituciones del sistema nacional de ciencia y tecnología, universidades públicas, instancias especializadas como la **Comisión Nacional para el Conocimiento y Uso de la Biodiversidad (CONABIO)** —comisión intersecretarial que opera, entre otros instrumentos, a través de la plataforma **Naturalista**—, y organizaciones de la sociedad civil implementan proyectos de ciencia ciudadana en materia de monitoreo de biodiversidad, calidad del aire, calidad del agua, observación climática y salud ambiental. La generación de datos por vía ciudadana puede complementar la infraestructura institucional convencional y contribuir a observar zonas y fenómenos que de otro modo quedarían fuera del alcance del monitoreo formal.

El reconocimiento normativo de la categoría en el artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente aporta cuatro beneficios concretos. Primero, proporciona a las autoridades federales, estatales y municipales una



referencia terminológica común para identificar la ciencia ciudadana dentro de sus programas ambientales, sin depender de definiciones dispersas. Segundo, ofrece una base conceptual susceptible de facilitar, conforme a las disposiciones y estándares que resulten aplicables, el aprovechamiento institucional de datos generados mediante proyectos de ciencia ciudadana. Tercero, fortalece la posición de las instituciones mexicanas que participan en redes internacionales de ciencia ciudadana, al contar con una categoría nacional armonizada con la Recomendación de la UNESCO de 2021. Cuarto, reconoce una modalidad de participación social compatible con el derecho de acceso a la información y con el derecho a un medio ambiente sano reconocidos por la Constitución.

La incorporación de la definición permite armonizar el ordenamiento interno con estándares internacionales que la comunidad científica y diversas jurisdicciones han consolidado en la última década. La presente iniciativa opta por una intervención normativa acotada: la adición de una fracción intercalar al catálogo de definiciones vigente, sin alterar competencias, procedimientos ni estructuras administrativas.

VII. IMPACTO REGULATORIO

La presente iniciativa no genera impacto regulatorio adicional. La reforma no da lugar a disposiciones de observancia obligatoria distintas de las que ya rigen en materia ambiental; no instituye permisos, licencias, autorizaciones ni trámites de especie alguna; no altera los requisitos previstos para el ejercicio de funciones públicas; ni incide en las normas reglamentarias o disposiciones administrativas vigentes. Se limita a incorporar al catálogo de definiciones del artículo 3o. una categoría conceptual que aporta claridad interpretativa y base terminológica común para los operadores del sistema.

VIII. IMPACTO PRESUPUESTARIO

La presente iniciativa no requiere la asignación de recursos presupuestales adicionales. La adición de una fracción al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente no crea estructuras administrativas, organismos, plazas ni programas de gasto. Los proyectos de ciencia ciudadana que actualmente operan en México se realizan con cargo a los presupuestos autorizados



de las instituciones participantes y con recursos de la sociedad civil y de la cooperación internacional; la reforma no altera esa configuración financiera. El reconocimiento normativo, por su naturaleza definitoria, es plenamente compatible con la política de responsabilidad hacendaria.

IX. IMPACTO SOCIAL

El impacto social de la reforma es favorable, potencial e indirecto. El reconocimiento de la ciencia ciudadana puede ampliar la visibilidad de la participación social en la generación de conocimiento ambiental, con especial relevancia para comunidades rurales, indígenas y periurbanas que desarrollan actividades de observación y monitoreo de biodiversidad y calidad ambiental en sus territorios. La reforma no crea programas ni prestaciones nuevas; aporta una referencia jurídica común que puede facilitar la consideración de estas prácticas en la política ambiental vigente. Al alinear el ordenamiento interno con estándares internacionales, también favorece condiciones de cooperación técnica e intercambio de conocimiento sin generar obligaciones presupuestarias adicionales.

CUADRO COMPARATIVO

Para claridad de la propuesta, se presenta a continuación el cuadro comparativo entre el texto vigente del artículo 3º. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente y la propuesta de modificación. La adición se destaca en negritas y subrayado; el resto del articulado se conserva sin modificación, manteniéndose la numeración de las fracciones subsecuentes.

Texto Vigente	Propuesta de Modificación
Artículo 3º · Adición de fracción en materia de ciencia ciudadana	
Artículo 3o. Para los efectos de esta Ley se entiende por:	Artículo 3o. Para los efectos de esta Ley se entiende por:
I. Ambiente: [...]	I. Ambiente: [...]
II. Áreas naturales protegidas: [...]	II. Áreas naturales protegidas: [...]
III. Aprovechamiento sustentable: [...]	III. Aprovechamiento sustentable: [...]



Texto Vigente	Propuesta de Modificación
IV. Biodiversidad: [...]	IV. Biodiversidad: [...]
V. Biotecnología: [...]	V. Biotecnología: [...]
V Bis. Cambio climático: [...]	V Bis. Cambio climático: [...]
(Sin correlativo)	<u>V Ter. Ciencia ciudadana: modalidad de generación de conocimiento científico en la que personas no profesionales de la ciencia participan de manera activa y estructurada, de forma individual o colaborativa, mediante la recolección, análisis, interpretación o difusión de datos o información ambiental, conforme a metodologías científicamente válidas, con la finalidad de contribuir al conocimiento científico y a la toma de decisiones en materia ambiental.</u>
VI. Contaminación: [...]	VI. Contaminación: [...]
VI Bis. [...]	VI Bis. [...]
VI Ter. Contaminación por ruido: [...]	VI Ter. Contaminación por ruido: [...]
[El resto de fracciones se conserva sin modificación.]	[El resto de fracciones se conserva sin modificación.]

Por lo anteriormente expuesto y fundado, someto a la consideración esta Soberanía el siguiente:

**DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN V TER AL ARTÍCULO 3º.
DE LA LEY GENERAL DEL EQUILIBRIO ECOLÓGICO Y LA PROTECCIÓN AL
AMBIENTE**

ARTÍCULO ÚNICO. Se adiciona una fracción V Ter al artículo 3o. de la Ley General del Equilibrio Ecológico y la Protección al Ambiente, para quedar como sigue:

Artículo 3o. Para los efectos de esta Ley se entiende por:

I. a V Bis. ...



V Ter. Ciencia ciudadana: modalidad de generación de conocimiento científico en la que personas no profesionales de la ciencia participan de manera activa y estructurada, de forma individual o colaborativa, mediante la recolección, análisis, interpretación o difusión de datos o información ambiental, conforme a metodologías científicamente válidas, con la finalidad de contribuir al conocimiento científico y a la toma de decisiones en materia ambiental.

VI. a XXXIX. ...

TRANSITORIOS

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

SEGUNDO. La aplicación de la reforma que este Decreto contiene se realizará con cargo a los presupuestos autorizados de las autoridades competentes, por lo que su entrada en vigor no requerirá la asignación de recursos adicionales ni la creación de estructuras administrativas o plazas.

ATENTAMENTE

DIP. GISELLE YUNUEEN ARELLANO ÁVILA

**DADO EN PALACIO LEGISLATIVO DE SAN LÁZARO, A 1 DE SEPTIEMBRE DE
2026.**

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DE LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, EN MATERIA DE DISPONIBILIDAD OBLIGATORIA DE REFACCIONES, SUSCRITA POR LA DIPUTADA ROCÍO ADRIANA ABREU ARTIÑANO, DEL GRUPO PARLAMENTARIO DE MORENA.

La que suscribe, **Diputada Federal Rocío Adriana Abreu Artiñano**, del Grupo Parlamentario de Morena en la LXVI Legislatura de la Cámara de Diputados del honorable Congreso de la Unión, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; artículos 6, numeral 1, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de Decreto por el que se reforman y adicionan diversas disposiciones de la **Ley Federal de Protección al Consumidor**, en materia de **disponibilidad obligatoria de refacciones**, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

México se encuentra en un momento decisivo y definitorio de su historia contemporánea en materia de movilidad, soberanía energética y protección sustantiva de los derechos del consumidor. Nos hallamos ante una encrucijada civilizatoria donde la imperiosa necesidad de mitigar los efectos devastadores del cambio climático ha precipitado una transformación radical en los modelos de producción y consumo de energía a nivel global, obligando a las naciones a reconfigurar sus industrias estratégicas y a replantear sus marcos normativos para dar

Diputado Federal
Rocío Adriana Abreu Artiñano

cabida a una nueva era tecnológica definida por la sustentabilidad y la eficiencia. Esta transformación profunda no es ajena a nuestra realidad nacional; por el contrario, la reconfiguración del modelo energético de nuestro país, impulsada por la necesidad urgente de reducir emisiones contaminantes, fortalecer la soberanía energética y modernizar la infraestructura productiva, ha colocado a la movilidad eléctrica como uno de los ejes estratégicos e ineludibles del desarrollo nacional y como una pieza clave en la construcción del segundo piso de la Cuarta Transformación.

En este contexto de redefinición geopolítica y geoeconómica, la transición hacia la electromovilidad no es simplemente una tendencia de mercado o una moda pasajera impuesta desde el exterior, sino un componente esencial de la estrategia de descarbonización planetaria y un pilar fundamental para el cumplimiento de los compromisos internacionales suscritos por el Estado Mexicano en materia ambiental, tales como el Acuerdo de París y la Agenda 2030 para el Desarrollo Sostenible.

México, gracias a su ubicación geográfica privilegiada, su vasta riqueza en recursos naturales estratégicos, como el litio, nuestro "oro blanco" y su sólida plataforma manufacturera, se ha posicionado como un actor protagónico en esta revolución industrial, atrayendo inversiones históricas bajo el fenómeno del *nearshoring* y convirtiéndose en un destino prioritario para la comercialización de nuevas tecnologías automotrices. Sin embargo, este vertiginoso crecimiento y la apertura de nuestro mercado a una multiplicidad de nuevos actores internacionales, particularmente provenientes del continente asiático, ha traído consigo una serie de desafíos regulatorios, vacíos legales y distorsiones de

**Diputado Federal
Rocío Adriana Abreu Artiñano**

mercado que, de no ser atendidos con prontitud, firmeza legislativa y visión de Estado, amenazan con vulnerar gravemente los derechos económicos de las familias mexicanas y comprometer la eficiencia, seguridad y estabilidad de nuestra infraestructura energética nacional.

En los últimos años, y con mayor énfasis en la presente administración, hemos promovido la adopción de tecnologías limpias en el transporte, particularmente a través del impulso a los vehículos eléctricos e híbridos. Esta política pública responde no solo a una obligación ambiental, sino también a una dolorosa realidad interna, el parque vehicular nacional, basado históricamente en la combustión interna, es uno de los principales generadores de emisiones contaminantes y gases de efecto invernadero, con impactos directos, cuantificables y severos en la salud pública, la calidad del aire de nuestras ciudades y la aceleración del calentamiento global. No obstante, la transición hacia la movilidad eléctrica no puede ni debe concebirse únicamente como un cambio tecnológico o una simple sustitución de motores de combustión por baterías; debe entenderse como un proceso integral, social, económico y jurídico que involucra derechos humanos fundamentales, protección efectiva al consumidor, planeación energética soberana, seguridad vial, acceso equitativo a la infraestructura y, sobre todo, la responsabilidad ética y legal de quienes introducen estas tecnologías al mercado nacional para lucrar con ellas.

Por lo que resulta innegable que la llegada de nuevas marcas automotrices y la diversificación de la oferta de vehículos eléctricos han democratizado el acceso a tecnologías más limpias y eficientes, permitiendo a más mexicanos acceder a vehículos de última generación.

**Diputado Federal
Rocío Adriana Abreu Artiñano**

Pero este proceso ha revelado una alarmante asimetría de poder entre las grandes corporaciones transnacionales y los consumidores mexicanos, quienes se han visto expuestos a prácticas comerciales que priorizan la colocación masiva de unidades en el mercado sobre la consolidación de una infraestructura de servicio postventa robusta y responsable.

Hemos sido testigos de un fenómeno donde la importación de vehículos ha superado con creces la capacidad logística instalada para garantizar su mantenimiento y reparación, creando una situación de indefensión para miles de usuarios que, tras realizar una inversión significativa para adquirir un automóvil, se enfrentan a la cruda realidad de no contar con el respaldo técnico necesario para mantenerlo en operación.

En este sentido la problemática que hoy nos ocupa y que motiva la presente iniciativa no es menor, ni aislada; **se trata de la inmovilización del patrimonio de los ciudadanos debido a la falta de disponibilidad de refacciones y autopartes esenciales**, una situación que ha escalado a **niveles críticos con tiempos de espera que en la actualidad oscilan vergonzosamente entre los ocho y los doce meses** para componentes que son vitales para el funcionamiento de las unidades.

Es imperativo reflexionar sobre el impacto social y económico de esta negligencia logística, pues para la inmensa mayoría de los hogares en México el automóvil particular no es un artículo de lujo ni un capricho, sino una herramienta de trabajo indispensable y el medio principal para garantizar el derecho a la movilidad, el acceso a la salud, a la educación y al desarrollo económico, por ello cuando un vehículo queda inoperante

**Diputado Federal
Rocío Adriana Abreu Artiñano**

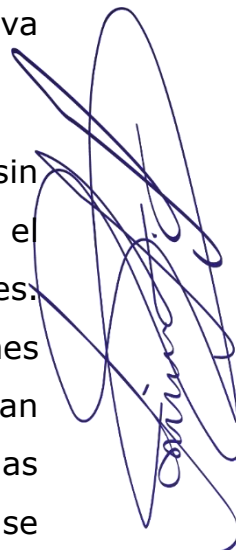
por periodos prolongados debido a la falta de una refacción, se está privando al ciudadano del uso y goce de su propiedad, generándole un daño patrimonial directo y una afectación a su calidad de vida que no tiene justificación alguna en un mercado que se dice abierto y competitivo.

En suma, a ello, si consideramos que muchos de estos vehículos son adquiridos mediante créditos automotrices onerosos, lo que obliga al consumidor a continuar pagando mensualidades, seguros e impuestos por un bien que no puede utilizar, atrapándolo en un ciclo de deuda y frustración que vulnera los principios más elementales de justicia contractual y protección al consumidor, conllevando a una situación de máxima vulnerabilidad al consumidor quedando atrapado entre contratos de compraventa que prometen garantías teóricas y un mercado que no asegura su cumplimiento real, dejándolo en un estado de indefensión jurídica total.

Es importante precisar que el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos establece de manera expresa que la ley protegerá a las personas consumidoras y propiciará su organización para el mejor cuidado de sus intereses. Este mandato constitucional impone al Estado la obligación activa de corregir asimetrías estructurales en el mercado cuando la dinámica comercial coloca a los consumidores en una posición de desventaja frente a los proveedores. En el caso de la comercialización de vehículos automotores, particularmente aquellos que incorporan nuevas tecnologías, la ausencia de reglas claras sobre servicio postventa y disponibilidad de refacciones genera una distorsión del mercado que afecta directamente el derecho del consumidor a la

reparación efectiva, a la información veraz y al uso pleno del bien adquirido, configurando una situación que exige intervención legislativa conforme al principio constitucional de protección al consumidor.

Asimismo, el propio artículo 28 constitucional prohíbe prácticas que, sin constituir monopolios en sentido estricto, restrinjan indebidamente el funcionamiento del mercado o lesionen los intereses de los consumidores. La falta de disponibilidad de refacciones y la opacidad en las condiciones de servicio postventa pueden traducirse en barreras indirectas que limitan la libertad real de elección del consumidor y generan dependencias forzadas frente a determinados proveedores. La presente iniciativa se inscribe, por tanto, dentro del marco constitucional que faculta y obliga al Estado a regular el mercado para garantizar condiciones de equidad, transparencia y competencia efectiva, asegurando que el desarrollo tecnológico y comercial se traduzca en beneficios reales para la población y no en nuevas formas de indefensión económica.



Ley Federal de Protección al Consumidor	
LEY VIGENTE	PROPUESTA DE LEY
ARTÍCULO 7.- Todo proveedor está obligado a informar y a respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, restricciones, plazos, fechas, modalidades,	ARTÍCULO 7.- Todo proveedor está obligado a informar y a respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, restricciones, plazos, fechas, modalidades,

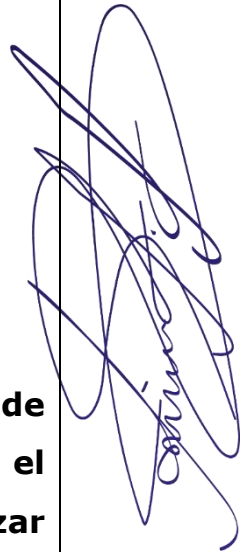
reservaciones y demás condiciones aplicables en la comercialización de bienes, productos o servicios, sobre todos aquellos que se hubiera ofrecido, obligado o convenido con el consumidor para la entrega del bien o prestación del servicio, ~~y bajo ninguna circunstancia serán negados estos bienes, productos o servicios a persona alguna, así como la información de los mismos.~~

SIN CORRELATIVO.

reservaciones y demás condiciones aplicables en la comercialización de bienes, productos o servicios, respecto de aquellos que se hubieran ofrecido, obligado o convenido con el consumidor para la entrega del bien o la prestación del servicio.

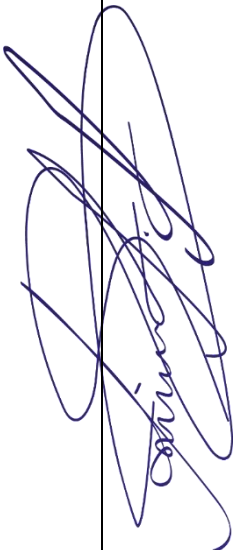
Tratándose de bienes de naturaleza duradera, el proveedor deberá garantizar que las condiciones ofrecidas permitan el uso, aprovechamiento, mantenimiento y reparación del bien en términos reales y efectivos, de conformidad con lo dispuesto en esta Ley.

Bajo ninguna circunstancia podrán negarse bienes, productos o servicios a persona



	alguna, ni limitarse u ocultarse la información necesaria para su adecuado uso, conservación o reparación.
SIN CORRELATIVO	Tratándose de vehículos automotores, nuevos o usados, incluidos los eléctricos e híbridos, el proveedor, fabricante, importador o distribuidor será responsable de garantizar la disponibilidad de refacciones, partes y componentes necesarios para su funcionamiento, mantenimiento y reparación, en los términos establecidos por esta Ley.
SIN CORRELATIVO	Artículo 77 Bis. Los proveedores, fabricantes e importadores de vehículos automotores, tienen la obligación ineludible de garantizar la disponibilidad efectiva de refacciones y componentes esenciales en territorio nacional.



	Tratándose de refacciones críticas que inmovilicen el funcionamiento del vehículo, el proveedor deberá asegurar un tiempo máximo de suministro al consumidor de sesenta días naturales. En caso de exceder dicho plazo, se considerará incumplimiento de contrato y el proveedor estará obligado a proporcionar un vehículo sustituto de características similares sin costo para el consumidor hasta la entrega de la refacción, o en su defecto, procederá la rescisión del contrato o la reposición del bien en los términos dispuestos por esta Ley.
SIN CORRELATIVO	Artículo 77 Ter. Para dar cumplimiento a la obligación de disponibilidad establecida en el artículo anterior, durante la comercialización de vehículos automotores los proveedores deberán:



I. Garantizar la disponibilidad de refacciones originales o compatibles, nuevas y certificadas, por un plazo mínimo de ocho años, contados a partir de la fecha en que se deje de comercializar el modelo en territorio nacional;

II. Mantener inventarios suficientes en territorio nacional o asegurar mecanismos logísticos eficientes que permitan la entrega de partes y componentes en un plazo no mayor a los sesenta días naturales establecidos en el artículo precedente; y

III. Abstenerse de condicionar la vigencia de la garantía a tiempos indefinidos por falta de refacciones, debiendo pausar el cómputo del plazo de garantía durante el tiempo que

	el vehículo permanezca inoperable por dicha causa.
SIN CORRELATIVO	Artículo 77 Quater. Previo a la celebración de la operación de compraventa, el proveedor deberá informar de manera clara, veraz y por escrito al consumidor sobre: I. La política de disponibilidad de refacciones y componentes; II. Los plazos máximos de entrega de refacciones; III. La ubicación de centros de servicio autorizados dentro del territorio nacional; IV. Las condiciones bajo las cuales opera la garantía cuando exista indisponibilidad temporal de refacciones. La omisión de esta información se considerará práctica comercial abusiva en términos de esta Ley.

**Diputado Federal
Rocío Adriana Abreu Artiñano**

Ahora bien, el marco jurídico vigente, establece principios de información y garantía para el consumidor, sin embargo, la ambigüedad de la norma al no establecer plazos perentorios ni consecuencias claras ante el incumplimiento ha permitido que algunas empresas importadoras y comercializadoras operen bajo esquemas predatorios de "inventario cero" en territorio nacional. Lo que Esta laguna legislativa ha permitido a ciertos actores trasladar el riesgo financiero y operativo de la cadena de suministro global a los hombros del consumidor mexicano, instaurando prácticas donde las refacciones son solicitadas al país de origen solo bajo pedido y una vez que el siniestro ha ocurrido, sometiendo al usuario a los vaivenes de la logística marítima internacional y aduanera, sin que exista un mecanismo legal efectivo que obligue a la empresa a asumir su responsabilidad por la demora. Esta omisión normativa genera una asimetría estructural inaceptable, ya que mientras el proveedor se beneficia del acceso irrestricto al mercado nacional y de las utilidades que este genera, la persona consumidora asume la totalidad del riesgo asociado a la falta de previsión logística.

Es por ello que resulta urgente reformar la ley para transitar de un concepto abstracto de "disponibilidad" a uno concreto de "disponibilidad efectiva y oportuna". La presente iniciativa propone establecer un plazo máximo y razonable para la entrega de refacciones críticas, entendiendo por estas aquellas cuya ausencia impide la movilización o el funcionamiento seguro del vehículo y una vez superado este plazo, el proveedor deberá asumir las consecuencias de su ineficiencia logística mediante la provisión de un vehículo sustituto o la reparación integral del daño. No se trata de una medida punitiva ni de imponer cargas imposibles al sector empresarial; se trata de establecer estándares mínimos de

calidad, servicio y dignidad que son comunes en otras jurisdicciones y que son necesarios para garantizar que el mercado mexicano no se convierta en un destino de segunda categoría donde se comercializan productos sin el respaldo postventa que la tecnología moderna exige. Esta reforma busca cerrar la brecha de impunidad comercial y enviar un mensaje claro, quien quiera vender en México, debe comprometerse con México y con sus consumidores.

En México, el crecimiento del parque vehicular eléctrico ha ocurrido de manera desordenada, caótica y sin una obligación jurídica correlativa para garantizar la protección efectiva de los intereses de los consumidores frente a prácticas que dañen su economía. En un régimen democrático y social de derecho, la libertad de comercio no puede interpretarse como una patente de corso para vulnerar los derechos de los ciudadanos ni para poner en riesgo la infraestructura estratégica de la nación. La soberanía energética, entendida en el siglo XXI, implica no solo la autosuficiencia en la generación de energía, sino también la capacidad soberana de definir los estándares tecnológicos que rigen su consumo y distribución en el territorio nacional, evitando dependencias tecnológicas nocivas y garantizando que la transición hacia energías limpias sea un motor de desarrollo equitativo y no una fuente de nuevas desigualdades.

Es crucial destacar que esta propuesta legislativa ha sido diseñada con un estricto apego a los compromisos internacionales asumidos por México. No pretende crear barreras al comercio internacional ni discriminar por el origen de los vehículos, sean estos asiáticos, europeos o norteamericanos. Por el contrario, establece reglas claras, generales, abstractas y no

discriminatorias, aplicables a todo vehículo eléctrico o no, que se comercialice en territorio nacional.

Y se respetan las normas de la Organización Mundial del Comercio, las cuales reconocen el derecho soberano de los Estados para adoptar las medidas técnicas necesarias para garantizar la seguridad nacional, la seguridad de los consumidores y la protección del medio ambiente. Exigir que un vehículo tenga refacciones disponibles no es proteccionismo; es regulación técnica básica para el funcionamiento ordenado de un mercado moderno, tal como lo han hecho ya la Unión Europea y el estado de California.

Con esta propuesta se busca que las personas consumidoras acceden a un mercado más justo, seguro y transparente, se trata de pasar de un modelo reactivo, donde el consumidor debía pelear para obtener una refacción, a un modelo preventivo, donde la ley asegura la disponibilidad.

Queremos que la inversión extranjera llegue, pero que lo haga con compromiso de permanencia, con infraestructura de soporte, con transferencia tecnológica y con respeto irrestricto a las leyes nacionales.

La grandeza de nuestra nación se mide también por su capacidad de proteger a sus ciudadanos ante las distorsiones de los mercados globales, nuestra tarea es legislar para proteger a nuestros ciudadanos, por lo que legislar en esta materia es cumplir con la obligación ética y política de poner la economía al servicio de las personas y no las personas al servicio de la economía, que se traduzcan en bienestar tangible para el pueblo de México y no en nuevas formas de dependencia o vulnerabilidad.

Por todo lo anterior, y con la convicción de que estamos construyendo el andamiaje jurídico para el México de las próximas décadas, someto a consideración de esta Honorable Asamblea la presente iniciativa de reformas a la Ley Federal de Protección al Consumidor, con el objetivo de dotar al país de un marco jurídico coherente, moderno, soberano y profundamente protector en materia de movilidad, someto a la consideración de esta Honorable Asamblea, la siguiente iniciativa con

PROYECTO DE DECRETO

ARTÍCULO ÚNICO. Se **adiciona** un segundo y tercer párrafo al artículo 7, se adiciona un artículo 77 **Bis, 77 Ter y 77 Quater** de la **Ley Federal de Protección al Consumidor**, para quedar como sigue:

ARTÍCULO 7.- Todo proveedor está obligado a informar y a respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, restricciones, plazos, fechas, modalidades, reservaciones y demás condiciones aplicables en la comercialización de bienes, productos o servicios, respecto de aquellos que se hubieran ofrecido, obligado o convenido con el consumidor para la entrega del bien o la prestación del servicio.

Tratándose de bienes de naturaleza duradera, el proveedor deberá garantizar que las condiciones ofrecidas permitan el uso, aprovechamiento, mantenimiento y reparación del bien en términos reales y efectivos, de conformidad con lo dispuesto en esta Ley.

Bajo ninguna circunstancia podrán negarse bienes, productos o servicios a persona alguna, ni limitarse u ocultarse la información necesaria para su adecuado uso, conservación o reparación.

Artículo 77 Bis. Los proveedores, fabricantes e importadores de vehículos automotores, tienen la obligación ineludible de garantizar la disponibilidad efectiva de refacciones y componentes esenciales en territorio nacional.

Tratándose de refacciones críticas que inmovilicen el funcionamiento del vehículo, el proveedor deberá asegurar un tiempo máximo de suministro al consumidor de sesenta días naturales. En caso de exceder dicho plazo, se considerará incumplimiento de contrato y el proveedor estará obligado a proporcionar un vehículo sustituto de características similares sin costo para el consumidor hasta la entrega de la refacción, o en su defecto, procederá la rescisión del contrato o la reposición del bien en los términos dispuestos por esta Ley.

Artículo 77 Ter. Para dar cumplimiento a la obligación de disponibilidad establecida en el artículo anterior, durante la comercialización de vehículos automotores los proveedores deberán:

I. Garantizar la disponibilidad de refacciones originales o compatibles, nuevas y certificadas, por un plazo mínimo de ocho años, contados a partir de la fecha en que se deje de comercializar el modelo en territorio nacional;

II. Mantener inventarios suficientes en territorio nacional o asegurar mecanismos logísticos eficientes que permitan la entrega de partes y componentes en un plazo no mayor a los sesenta días naturales establecidos en el artículo precedente; y

III. Abstenerse de condicionar la vigencia de la garantía a tiempos indefinidos por falta de refacciones, debiendo pausar el cómputo del plazo de garantía durante el tiempo que el vehículo permanezca inoperable por dicha causa.

Artículo 77 Quater. Previo a la celebración de la operación de compraventa, el proveedor deberá informar de manera clara, veraz y por escrito al consumidor sobre:

I. La política de disponibilidad de refacciones y componentes;

II. Los plazos máximos de entrega de refacciones;

III. La ubicación de centros de servicio autorizados dentro del territorio nacional;

IV. Las condiciones bajo las cuales opera la garantía cuando exista indisponibilidad temporal de refacciones.

La omisión de esta información se considerará práctica comercial abusiva en términos de esta Ley.

TRANSITORIOS

Primero. El presente Decreto entrará en vigor a los ciento ochenta días naturales siguientes a su publicación en el Diario Oficial de la Federación.

Segundo. La Procuraduría Federal del Consumidor emitirá, dentro de los noventa días siguientes a la entrada en vigor del presente Decreto, los lineamientos administrativos necesarios para su implementación.

Tercero. Se derogan todas las disposiciones que se opongan al presente Decreto.

Palacio Legislativo de San Lázaro de la
Cámara de Diputados del honorable Congreso de la Unión,
a 01 de septiembre de 2026

Suscribe,



Dip. Rocío Adriana Abreu Artiñano

Cámara de Diputados del Honorable Congreso de la Unión, LXVI Legislatura**Junta de Coordinación Política**

Diputados: Ricardo Monreal Ávila, presidente; José Elías Lixa Abimerhi, PAN; Carlos Alberto Puente Salas, PVEM; Reginaldo Sandoval Flores, PT; Rubén Ignacio Moreira Valdez, PRI; Ivonne Aracely Ortega Pacheco, MOVIMIENTO CIUDADANO.

Mesa Directiva

Diputados: Raúl Bolaños-Cacho Cué, presidente; vicepresidentes, Sergio Carlos Gutiérrez Luna, MORENA; Annia Sarahí Gómez Cárdenas, PAN; Nayeli Arlen Fernández Cruz, PVEM; secretarios, Julieta Villalpando Riquelme, MORENA; Diana Estefanía Gutiérrez Valtierra, PAN; Felipe Miguel Delgado Carrillo, PVEM; Francisco Amadeo Espinosa Ramos, PT; Fuensanta Guadalupe Guerrero Esquivel, PRI; Laura Irais Ballesteros Mancilla, MOVIMIENTO CIUDADANO.

Secretaría General**Secretaría de Servicios Parlamentarios****Gaceta Parlamentaria de la Cámara de Diputados**

Director: Juan Luis Concheiro Bórquez, **Edición:** Casimiro Femat Saldivar, Ricardo Águila Sánchez, Antonio Mariscal Pioquinto.

Apoyo Documental: Dirección General de Proceso Legislativo. **Domicilio:** Avenida Congreso de la Unión, número 66, edificio E, cuarto nivel, Palacio Legislativo de San Lázaro, colonia El Parque, CP 15969. Teléfono: 5036 0000, extensión 54046. **Dirección electrónica:** <http://gaceta.diputados.gob.mx/>