INICIATIVA QUE ADICIONA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, A FIN DE FACULTAR AL CONGRESO DE LA UNIÓN PARA LEGISLAR EN MATERIA DE CIBERSEGURIDAD, A CARGO DE LA DIPUTADA IVONNE ARACELLY ORTEGA PACHECO, DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO

Quien suscribe, diputada Ivonne Aracelly Ortega Pacheco, Coordinadora del Grupo Parlamentario de Movimiento Ciudadano en la LXVI Legislatura, con fundamento en lo dispuesto en el artículo 71, fracción II, y 78, párrafo segundo, fracción III, de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 116 y 122, numeral 1, de la Ley Orgánica del Congreso General, y 55, fracción II y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, somete a consideración la siguiente iniciativa con proyecto de decreto por el que se adiciona el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para facultar al Congreso de la Unión a legislar en materia de ciberseguridad, al tenor de la siguiente:

Exposición de Motivos

El desarrollo acelerado de las tecnologías de la información y la comunicación ha generado un nuevo entorno de interacción social, económica e institucional conocido como ciberespacio. En dicho entorno se realizan actividades esenciales para el funcionamiento del Estado, la prestación de servicios públicos, la operación del sistema financiero, la protección de datos personales y el ejercicio de derechos fundamentales. A diferencia de los espacios físicos, el ciberespacio no está limitado por la geografía; existe como un dominio compartido donde los individuos, las organizaciones y los gobiernos interactúan, se comunican y realizan transacciones en tiempo real.[1]

No obstante, el marco constitucional mexicano no reconoce de manera expresa la facultad del Congreso de la Unión para legislar en materia de ciberseguridad, lo que ha provocado una regulación fragmentada, dispersa y, en algunos casos, insuficiente para atender los riesgos derivados de amenazas cibernéticas, ataques informáticos y vulneraciones a sistemas críticos.

La ausencia de una atribución constitucional clara genera incertidumbre jurídica sobre la competencia de los distintos órdenes de gobierno, dificulta la coordinación institucional y limita la capacidad del Estado mexicano para diseñar políticas públicas integrales en materia de prevención, gestión y respuesta ante incidentes cibernéticos.

En México, el uso intensivo de tecnologías de la información, servicios digitales, plataformas financieras, bases de datos y sistemas críticos ha incrementado la eficiencia institucional, pero también ha generado nuevas vulnerabilidades en el ciberespacio.

Actualmente, México carece de un marco jurídico integral en materia de ciberseguridad. La regulación vigente se encuentra dispersa en distintos ordenamientos, como el Código Penal Federal, la Ley Federal de Protección de Datos Personales y la Ley de Seguridad Nacional, lo que genera vacíos normativos, duplicidades y falta de coordinación institucional.

Los ciberataques, el robo de información, la suplantación de identidad, el *ransomware,* [2] la afectación a infraestructuras críticas y la vulneración de datos personales representan riesgos reales para la seguridad nacional, la economía, la confianza ciudadana y los derechos fundamentales, particularmente el derecho a la privacidad y a la protección de datos.

Diversos organismos internacionales recomiendan a los Estados adoptar estrategias nacionales de ciberseguridad, con enfoque preventivo, coordinación interinstitucional y respeto a los derechos humanos. Un ejemplo de lo anterior es la Convención de las Naciones Unidas contra la Ciberdelincuencia,[3] aprobado por la Asamblea General en diciembre de 2024, la cual marca una pauta de fortalecimiento de la capacidad de los países firmantes y de cooperación internacional que se suma a la Convención de Palermo sobre Delincuencia Organizada adoptada en el año 2000.

En este sentido, resulta indispensable que el Congreso de la Unión establezca una Ley General de Ciberseguridad que fije principios, competencias mínimas y mecanismos de coordinación entre la Federación, las entidades federativas y los municipios, y con ello sume esfuerzos para combatir los delitos en la web.

De igual manera es bien sabido que la revolución digital ha transformado profundamente la manera en que el Estado, la economía y la sociedad interactúan. Sin embargo, y como ya se ha mencionado con anterioridad, este avance tecnológico también ha generado graves vulnerabilidades en el ciberespacio que requieren atención inmediata por parte del marco jurídico mexicano.

– Amenazas de ciberseguridad en México y su impacto

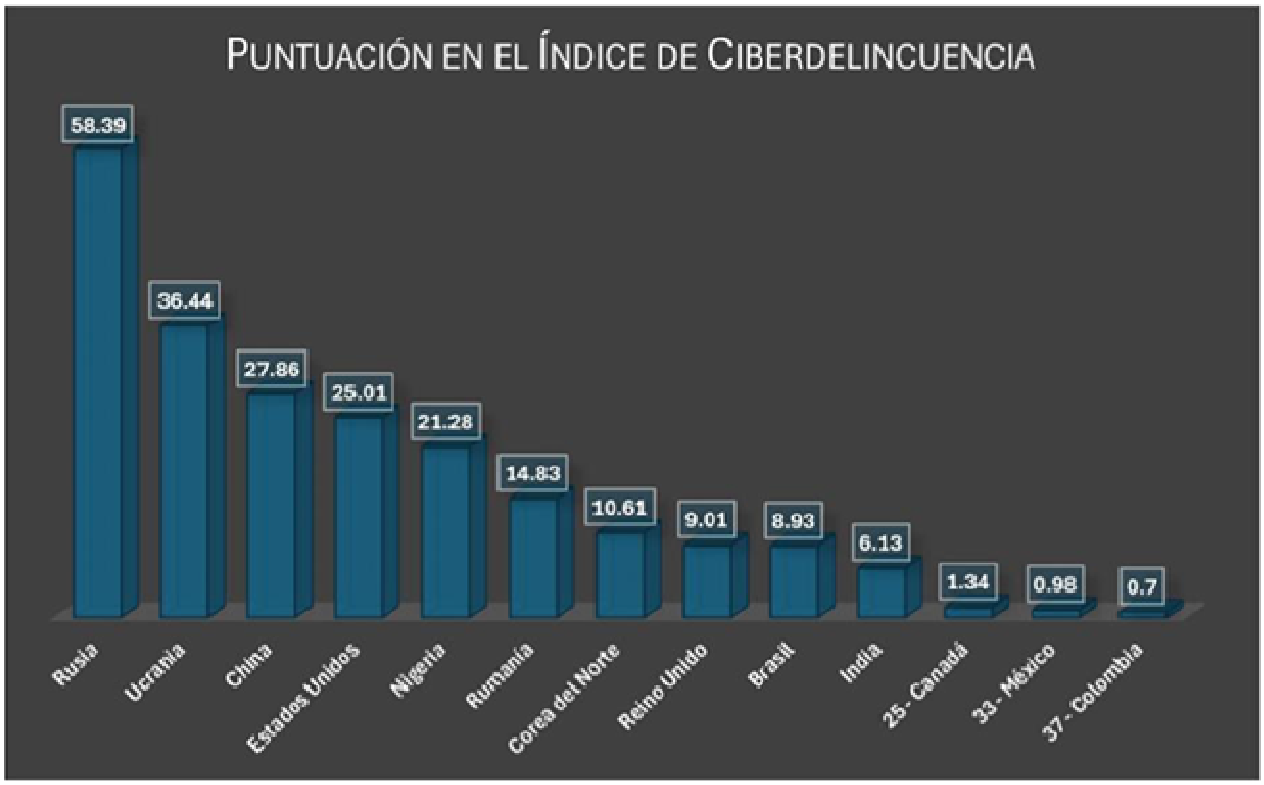
Durante la primera mitad de 2024, México enfrentó más de 31 mil millones de intentos de ciberataques,[4] lo que representó aproximadamente 55 por ciento de todos los incidentes registrados en América Latina, posicionándolo como uno de los países más atacados de la región. Este dato es preocupante por esta tendencia, no solo por el volumen de ataques, sino también por el impacto que seguirá teniendo en los siguientes años, especialmente en los sectores empresarial y gubernamental mexicano.

En el entorno cotidiano, más de 13 millones de personas han sido víctimas de fraudes cibernéticos, como phishing,[5] en los últimos siete años, con pérdidas estimadas en más de 20 mil millones de pesos solo en 2024. Un dato relevante derivado de esta práctica es que el 34 por ciento de los internautas ha recibido mensajes sospechosos solicitando datos personales y uno de cada tres conoce a alguien que ha caído en la trampa. Del total de los afectados, el 61,5 por ciento perdió contraseñas; el 38,5 por ciento, información privada (como direcciones o números telefónicos), y el 15,4 por ciento, acceso a sus cuentas bancarias.[6]

Aunado a los datos señalados anteriormente y de acuerdo con el nuevo Índice Mundial de Ciberdelincuencia, la mayoría de las amenazas de los ciberdelincuentes se concentran en nueve países. Por un amplio margen, los cinco países donde hay más cibercriminales son: Rusia, Ucrania, China, Estados Unidos y Nigeria; el único latinoamericano es Brasil, en la

novena posición, y México está en la posición 33 del total de 97 países.[7] Factores como su proximidad económica y tecnológica a Estados Unidos, la creciente digitalización de procesos y la adopción acelerada de tecnologías (a menudo sin protección suficiente) han convertido a México en terreno fértil para grupos cibercriminales.

Además, de la falta de legislación, una carente cultura de prevención cibernética y la baja inversión en equipos especializados agravan la situación.



Fuente: Índice Mundial de Ciberdelincuencia

La ausencia de políticas coherentes y obligatorias de ciberseguridad se traduce en una elevada exposición de infraestructuras críticas, empresas del sector productivo y organismos públicos a vulnerabilidades que pueden tener consecuencias económicas, sociales y de seguridad nacional.

Además, aunque México ha adoptado instrumentos dispersos, como el Código Penal Federal para delitos informáticos y la Estrategia Nacional de Ciberseguridad de 2017, carece de una base constitucional que habilite al Congreso a legislar de manera integral y coordinada sobre esta materia.

De cara al mundial de fútbol, la ciberseguridad se perfila como uno de los principales desafíos para empresas y usuarios, en un contexto marcado por el uso intensivo de tecnologías digitales, el avance de la inteligencia artificial y la celebración del Mundial de Futbol 2026, se advierte que dicho evento incrementará de forma significativa los intentos de fraude y ataques informáticos.

– Marco internacional, legislación en ciberseguridad

Diversos países han desarrollado marcos legales robustos para enfrentar amenazas cibernéticas y proteger tanto infraestructuras críticas como a la sociedad, algunos ejemplos son los siguientes:

Unión Europea (UE)

Directiva NIS2: La UE adoptó la Directiva 2022/2555 (NIS2)[8] para establecer un marco legal común y obligatorio en ciberseguridad, que obliga a estados miembros a definir estrategias nacionales, identificar sectores críticos, gestionar riesgos y reportar incidentes con plazos y obligaciones claras.

La implementación de esta implica proteger los sistemas de red e información (NIS), sus usuarios y otras personas afectadas frente a incidentes y amenazas cibernéticas. Para responder a la creciente exposición de Europa a las amenazas cibernéticas. A través de esta se les exige a los Estados miembros que mejoren sus capacidades de ciberseguridad, al tiempo que introducen medidas de gestión de riesgos y requisitos de reporte a entidades de más sectores y establezcan normas para la cooperación, el intercambio de información, la supervisión y la aplicación de las medidas de ciberseguridad.

Irlanda y otros países europeos, están adaptando marcos como NIS2 a su legislación local para fortalecer la responsabilidad de entidades esenciales, establecer autoridades nacionales y registrar sistemas críticos con obligaciones de notificación y gestión de riesgos.

Japón

En 2025, el Parlamento japonés promulgó la Active Cyber Defence Law (Ley de Defensa Cibernética Activa) que habilita al Estado a implementar medidas más proactivas de defensa cibernética y exige a operadores de infraestructuras críticas reportar incidentes, buscando incrementar la resiliencia ante ataques sofisticados.

La interceptación de tráfico extranjero y la notificación obligatoria de incidentes servirán como fuentes de inteligencia fundamentales para detectar ciberataques en curso o potenciales. A su vez, las respuestas serán ejecutadas por la Agencia Nacional de Policía o por las Fuerzas de Autodefensa.

La Agencia de Seguridad Nacional y la Red de Comunicaciones del Gobierno hicieron una transición fluida a los ámbitos cibernéticos, la postura de inteligencia y militar de Japón se enfocó en roles defensivos y no intervencionistas. Esto ha creado un conjunto único ya que Japón busca construir capacidades cibernéticas proactivas, asegurando que nuevas iniciativas como la ley sigan cumpliendo con las restricciones constitucionales mientras abordan las amenazas cibernéticas en rápida evolución.

La ley se basa en tres pilares principales, que se implementarán y entrarán en vigor en fases:

Pilar 1 – Fortalecimiento de la Colaboración Público-Privada: La ley establece un nuevo Consejo Cibernético, que tiene como objetivo mejorar el intercambio de información y la respuesta a incidentes entre agencias gubernamentales y socios clave del sector privado. Este Consejo será una plataforma central para el intercambio de inteligencia de amenazas, la coordinación de respuestas y la planificación estratégica.

Pilar 2 – Aprovechar la información y los datos bajo las comunicaciones para la detección de amenazas: La ley otorga una autoridad legal clara para el uso de datos relacionados con las comunicaciones para identificar y analizar amenazas cibernéticas.

Pilar 3 – Acceso remoto y medidas de neutralización: El tercer pilar faculta a las autoridades gubernamentales para acceder y neutralizar remotamente infraestructuras atacantes, como servidores maliciosos o nodos de comandos de malware. Estas acciones se llevarán a cabo bajo estricta supervisión legal y procesal, y solo cuando sea necesario para prevenir o mitigar incidentes cibernéticos graves.

China

Desde 2017 China cuenta con la Ley de Ciberseguridad[9] la cual regula la protección del ciberespacio, la seguridad de las redes y datos, y refiere obligaciones específicas para operadores de redes y sistemas. En octubre del 2025, el Comité de Constitución y Derecho del Congreso Nacional del Pueblo de la República de China comunicó que enmendó su Ley de Ciberseguridad, para incorporar conceptos como el de seguridad nacional, promoción de la investigación en IA (con creación de la infraestructura necesaria y la mejora de los estándares éticos); además de incorporarla como herramienta de resguardo.

La actualización normativa incrementa las penalizaciones por la responsabilidad cibernético-informática, a la vez que clasifica y penaliza la violación de una red. Por ejemplo, se multiplican las cargas y multas por una vulnerabilidad, donde las personas responsables y las empresas pueden enfrentar el pago de tasas que varían según sea la gravedad y el impacto, mientras que los operadores de infraestructura crítica pueden sufrir hasta la revocación de sus licencias, entre otros castigos administrativos severos.

Lo anterior nos muestra como China tiene ya años de avances en el tema y constantemente se actualiza, dado que día con día la sociedad hace uso de las herramientas digitales y son susceptibles a lidiar con los desafíos que esto implica.

Estados Unidos

Aunque el enfoque se da mediante leyes sectoriales y múltiples normas, por ejemplo, la Ley de Intercambio de Información sobre Ciberseguridad[10] (CISA), representa uno de los marcos más desarrollados por volumen de normas y mecanismos de colaboración público-privada.

Dicha Ley anima a las empresas y al gobierno federal a compartir información sobre las amenazas cibernéticas. Este intercambio ayuda a todos los implicados a mejorar sus defensas frente a los ciberataques.

En general, una amplia variedad de leyes penales en Estados Unidos hace referencia a la ciberseguridad de una forma u otra. Por ejemplo, los estatutos penales federales abordan las siguientes actividades, entre otras:

- Hackeo de ordenadores;
- Robo de identidad;
- Espionaje económico;
- Robo de secretos comerciales;
- Irrumpir en sistemas informáticos y acceder, modificar o eliminar datos;
- Robar información confidencial;
- Desfigurar sitios web de Internet; y
- Inundar sitios web con grandes volúmenes de tráfico de Internet irrelevante para hacer que los sitios web no estén disponibles para clientes reales.

La seguridad cibernética ha sido una preocupación tanto para el gobierno como para el sector privado en Estados Unidos. Sin embargo, el crecimiento del sector de tecnología de la información y comercio electrónico ha dado lugar a delitos cibernéticos. Y eso ha causado una gran pérdida para el gobierno de los Estados Unidos y sus ciudadanos.[11]

Estos ejemplos muestran una tendencia global, los países están fortaleciendo sus marcos jurídicos para garantizar una ciberseguridad integral, coordinada y con mecanismos claros de prevención y respuesta, incluso incorporando obligaciones de reportar incidentes en plazos definidos y sanciones a incumplimientos, lo que permite elevar la respuesta frente a amenazas digitales.

– Necesidad de una base constitucional en México

La inexistencia de una facultad constitucional expresa del Congreso de la Unión para legislar en materia de ciberseguridad impide crear un marco nacional uniforme y obliga a depender de normas fragmentadas, estrategias obsoletas y decisiones sectoriales aisladas. Ante un entorno en que ataques cibernéticos alcanzan cifras extraordinarias y tienen impacto real en la economía, la administración pública y la vida de las personas, es indispensable que el orden constitucional habilite al Congreso para expedir leyes que protejan el ciberespacio, coordinen esfuerzos y establezcan obligaciones mínimas de seguridad para sectores públicos y privados, respetando los derechos fundamentales de la población.

Otorgar al Congreso de la Unión la facultad expresa para legislar en materia de ciberseguridad permitirá establecer un marco normativo homogéneo, respetuoso del federalismo y de los derechos humanos, que dote al país de instrumentos legales

adecuados para proteger el ciberespacio, sin invadir competencias locales ni ampliar de manera indebida las facultades del Estado en perjuicio de las libertades fundamentales.

El legislar en materia de Ciberseguridad, por tanto, se configura como una herramienta indispensable para articular una política pública moderna y eficaz que asegure un entorno digital libre, seguro y respetuoso de los derechos humanos, a la altura de los compromisos constitucionales y de los estándares internacionales más avanzados.

Por lo expuesto anteriormente, la presente iniciativa que adiciona la Constitución Política tiene un carácter habilitante, en tanto sienta las bases constitucionales necesarias para que el Congreso de la Unión expida la Ley de Ciberseguridad, con un enfoque integral, preventivo y respetuoso de los derechos humanos.

Desde la Bancada Naranja, se parte de la convicción de que la legislación debe poner las causas al frente y a las personas al centro, atendiendo los riesgos reales que enfrenta la ciudadanía en el entorno digital, sin recurrir a soluciones autoritarias, desproporcionadas o que vulneren libertades fundamentales. La ciberseguridad no debe concebirse únicamente como un asunto técnico o de control, sino como una política pública orientada a proteger a las personas, sus datos, su patrimonio y su confianza en las instituciones, al tiempo que se fortalece la seguridad nacional y la competitividad del país.

Con esta reforma constitucional, se busca dotar al Estado mexicano de las herramientas jurídicas necesarias para construir, de manera democrática y plural, un marco legal moderno en materia de ciberseguridad, que responda a los desafíos del siglo XXI y coloque a México a la altura de los estándares internacionales, siempre con una visión centrada en las personas y en la defensa de sus derechos.

A continuación, se agrega un cuadro comparativo de la propuesta de reforma:

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

TEXTO VIGENTE	PROPUESTA DE MODIFICACIÓN
Sección III De las Facultades del Congreso	Sección III De las Facultades del Congreso
Artículo 73. El Congreso tiene facultad:	**Artículo 73.** El Congreso tiene facultad:
I a XXIII Bis. ...	I a XXIII Bis. ...
XXIII Ter. SIN CORRELATIVO	XXIII Ter. Para expedir la Ley de Ciberseguridad, estableciendo las bases de coordinación entre la Federación, las entidades federativas y los municipios, así como los principios para la prevención, atención y mitigación de riesgos en el ciberespacio, con pleno respeto a los derechos humanos.
XXIV a XXXII. ...	XXIV a XXXII. ...

En tal virtud, someto a la consideración de esta la siguiente iniciativa con proyecto de:

Decreto por el que se adiciona una fracción XXIII Ter al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para facultar al congreso de la unión a legislar en materia de ciberseguridad

Único. Se adiciona la fracción XXIII Ter al artículo 73 de la Constitución Política De Los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I a XXIII Bis. ...

XXIII Ter. Para expedir la Ley de Ciberseguridad, estableciendo las bases de coordinación entre la Federación, las entidades federativas y los municipios, así como los principios para la prevención, atención y mitigación de riesgos en el ciberespacio, con pleno respeto a los derechos humanos.

XXIV a XXXII. ...

Transitorios

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

Segundo. El Congreso de la Unión deberá expedir la Ley de Ciberseguridad dentro de un plazo de ciento ochenta días naturales contados a partir de la entrada en vigor del presente decreto.

Notas

1 ¿Qué es el ciberespacio?, disponible https://phoenixnap.es/glosario/que-es-el-ciberespacio

2 El *ransomware* es un tipo de?malware?que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante.

3 Sesenta y cinco países firman el primer tratado contra la ciberdelincuencia, un hito para la cooperación digital, disponible en https://news.un.org/es/story/2025/10/1540631

4 México sufre 31.000 millones de ciberataques en 6 meses, disponible en https://www.cyberpeace.tech/en/post/mexico-suffers-31-billion-cyberattacks-in-6-months

5 El phishing es un tipo de ciberataque que utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para engañar a la gente y hacer que comparta datos confidenciales, descargue malware o se exponga a la ciberdelincuencia.

6 https://elpais.com/mexico/2025-07-23/mas-de-13-millones-de-victimas-por -fraudes-ciberneticos-en-mexico.html

7 México, lugar 33 en ciberdelincuencia mundial, disponible en https://tribunaeconomica.com.mx/publicaciones/seccion/internacional/mex ico-lugar-33-en-ciberdelincuencia-mundial/

8 Directiva NIS2: protección de redes y sistemas de información, disponible en https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm

9 Ciberseguridad en China, disponible en https://ciberseguridad.com/normativa/china

10 Ciberseguridad EU
https://ciberseguridad.com/normativa/eeuu/#Legislacion_de_ciberseguridad_en_EEUU

11 Ibídem

Palacio Legislativo de San Lázaro, a 7 de enero de 2026.

Diputada Ivonne Aracelly Ortega Pacheco (rúbrica)