PROPOSICIÓN CON PUNTO DE ACUERDO POR EL SE EXHORTA AL EJECUTIVO FEDERAL INFORME SOBRE LOS ACUERDOS Y EL PROCESO INTERSECRETARIAL QUE MEXICO HA MANTENIDO PARA INTEGRASE A LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA DE LAS NACIONES UNIDAS DEL AÑO 2024.

Los que suscriben, Héctor Saúl Téllez Hernández, las diputadas y los diputados del Grupo Parlamentario del Partido Acción Nacional de la LXVI Legislatura de la Cámara de Diputados del honorable Congreso de la Unión, con fundamento en lo señalado en los artículos 58, 59 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, sometemos a consideración de la Comisión Permanente la presente proposición con punto de acuerdo, al tenor de las siguientes

Consideraciones

La rápida evolución de Internet y de las tecnologías de la información han favorecido el crecimiento económico y social en todo el mundo. Ante la nueva digitalización de los sistemas de información y comunicación surgen los ataques cibernéticos, que toman relevancia por sus diversas formas sofisticadas de intervención, que generan efectos indeseados y causan daños a las instituciones públicas, privadas y la vida de las personas.

Las principales amenazas cibernéticas en México fueron los ataques de *ransomware*, que consiste en cifrar datos por el que exige un rescate para restaurar el acceso; y los ataques de *phishing,* táctica de engaño para robar información confidencial simulando ser una entidad legítima.

Durante el primer semestre de 2024, los ataques de *ransomware* en México crecieron más del 4% en comparación con el mismo período del año anterior, siendo el sector financiero, la salud, manofactura y construcción los más afectados. Por otro lado, desde agosto de 2023 a julio de 2024 hubo un crecimiento de 220% en ataques de *phishing*, promediando unos 325 mil ataques por día.[1]

En México, como parte de una transgresión a los sistemas de información, en 2022 se dio a conocer el caso de Guacamaya Likns, donde información de alta seguridad generada por la Secretaría de la Defensa Nacional (Sedena), quedo expuesta por piratas cibernéticos. Millones de correos electrónicos y documentos militares de México quedaron expuestos después de que un grupo de hackers se infiltrara en un servidor de la corporación militar, y extrajera 6 terabytes de información interna y confidencial generada durante los últimos 10 años.[2]

[1] Consultado en https://www.deltaprotect.com/blog/ciberseguridad-en-mexico, en fecha 15 de marzo de 2025.
[2] Consultado en: Guacamaya Leaks evidencian brecha de profesionales de ciberseguridad, en fecha 15 de marzo de 2025.

Por otro lado, el Instituto Nacional de Estadística y Geografía (INEGI) en 2023, dio a conocer los resultados del Módulo sobre Ciberacoso (MOCIBA) 2023, señalando las cifras que a continuación se describen:

- El 20.9 % de la población usuaria de internet1 (18.4 millones de personas de 12 años y más) vivió alguna situación de ciberacoso.

- El mismo año, 22.0 % de las mujeres y 19.6 % de los hombres que usaron internet fueron víctimas de ciberacoso.

- El ciberacoso más frecuente que experimentaron ambos sexos fue el contacto mediante identidades falsas.

- Las 3 entidades federativas con mayor porcentaje de población de 12 años y más que experimentaron alguna situación de ciberacoso fueron: Durango (28.8 %), Oaxaca (25.5 %) y Puebla (25.0 %) y las entidades con menor prevalencia fueron Guerrero, con 17.4 % y Sinaloa y Ciudad de México, ambas con 17.6 %.[3]

Un caso más reciente de ataque de ciberdelincuencia en México, fue en el año 2024, donde el sector financiero reportó formalmente al Banco de México cuatro incidentes cibernéticos, uno realizado a una Sociedad Popular (Sofipo) por más de 124 millones de pesos, y a tres bancos, uno de ellos por más de 24 millones de pesos, generando fraude y que los datos de los usuarios de estos servicios quedaran expuestos.

Así como, ataques a una cadena de conveniencia, que quedó sin servicio varias semanas, situación que no se hizo de conocimiento a la Comisión Nacional Bancaria y de Valores de este incidente de ciberseguridad, al no estar obligados a reportar por ley.[4]

Como parte de las estrategias en materia de ciberseguridad o ciberdelitos, México anunció el desarrollo de la Estrategia Nacional de Ciberseguridad (ENCS), en el año 2017, si bien representó un paso adelante, sin embargo, no se ha dado a conocer a la opinión pública sobre sus mecanismos técnicos de aplicación durante los años de 2018 a 2024 sobre su cumplimiento y ejecución.

Así mismo, en el Senado se presentó la Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024-2030, propuesta que contiene consideraciones en temas de ciberseguridad, que a la fecha no se ha dado a conocer a la opinión pública sobre las conclusiones ni el seguimiento de este último tema.

México a la fecha no cuenta con una legislación que sancione los delitos cibernéticos, ni una Ley sobre ciberseguridad, en virtud de que no ha existido la

[3] Consultado en: Módulo sobre Ciberacoso (MOCIBA) 2023, el 23 de marzo de 2025.
[4] Consultado en: Los focos en los hackeos – El Financiero, en fecha 25 de marzo de 2025.

voluntad política para regular sobre estos temas que son de interés para la ciudadanía y de seguridad nacional.

Cabe destacar que, México a la fecha ha manifestado no ser parte y no se ha adherido el Convenio No. 185 del Consejo de Europa contra la Delincuencia, aprobado en Budapets, Hungría en 2001, a pesar de que fue invitado a formar parte no ha seguido el procedimiento que señala la Constitución Política de los Estados Unidos para la aprobación de cualquier acuerdo o convenio internacional.

Ante las diversas excitativas que se han hecho por parte del poder legislativo al gobierno federal para que México deje de ocupar el papel de observador ante dicho Convenio, en respuesta de fecha del 25 de noviembre de 2024, por parte del Director General de Coordinación Política de la Secretaría de Relaciones Exteriores al Titular de la Unidad de Enlace de la Secretaría de Gobernación, manifestó que:

… el Convenio de Budapets no permite a los Estados hacer reservas al momento de su adhesión, lo cual requiere estar en cumplimiento pleno de sus disposiciones, previo a su adhesión.

Por lo que, ser realizaron las modificaciones al Código Penal Federal, al Código Federal de Procedimientos Penales, Ley Federal de Telecomunicaciones y quizás a la Ley General del Transparencia y Acceso a la Información Pública.

Asimismo, dicho documento refiere que …*para avanzar en la adhesión, se observa que algunas disposiciones originales del convenio han quedado superadas en los últimos 20 años respecto de las tecnologías de la información, haciendo hincapié al considerar que, las disposiciones del Convenio deben ser compatibles con los recientes avances sobre la privacidad en la red y la protección de los derechos humanos en línea.*

Aunque afirma que México, no es parte de este Acuerdo, sigue como observador y trabaja con los organismos de este Convenio a través de las funciones que realiza la policía cibernética de la Guardia Nacional y de la Unidad de Investigación de Delitos cibernéticos de la Fiscalía General de la República.

En el mismo contexto, establece que México participó en el Convenio Internacional contra el uso de las tecnologías de la información con fines delictivos, por lo que ante el mandato de la Asamblea General de la Organización de las Naciones Unidas (AGONU), fue parte en los trabajos para la Convención Internacional contra el uso de las tecnologías de la información con fines delictivos, del 8 de agosto de 2024.

Ante la intervención que México ha tenido con las instancias internacionales para la toma de decisiones sobre el Convenio Internacional contra el uso de las tecnologías de la información con fines delictivos, el documento no refiere alguna propuesta que México plantee para que la misma sea tomada en cuenta en esta resolución, por lo que es necesario dar a conocer a la opinión pública lo que dispone esta resolución a los Estados invitados a ser parte del Convenio.

En 2024, la Asamblea General de las Naciones Unidas adoptó la *Convención de las Naciones Unidas contra la Ciberdelincuencia; Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves*[5], documento que sienta las bases para una cooperación internacional que proveerá de herramientas para el combate de la ciberdelincuencia de manera colectiva, expedita e inclusiva.

Además, que contribuirá a cerrar las brechas en la legislación en la materia y a establecer estándares que permitan una armonización normativa a nivel internacional, existe la especialización con los aspectos relacionados con el cibercrimen y la justicia penal. Algunos de los elementos más destacados incluyen:

- **Acceso Ilegal a Sistemas de Información**: Los Estados miembros deben promulgar leyes que penalicen y que al mismo tiempo protejan datos y sistemas que sean susceptibles a riesgos digitales.

- **Protección de la infancia en el entorno digital**. El aumento de casos de explotación sexual infantil, el *grooming* y el contenido sexual explícito, sugiere leyes más estrictas, además se abordan nuevas amenazas como el *deepfake* y la porno-venganza.

- **Recolección y Registro de Datos**: Hacer del cibercrimen autoridades que verifiquen y registren datos relacionados con actividades ilícitas en línea.

- **Cooperación Internacional**: Establece mecanismos claros para la preservación y recolección de pruebas digitales, y otorga a los Estados la capacidad de exigir a los proveedores de servicios de internet y telecomunicaciones que entreguen información para las investigaciones. Se enfatiza sobre el intercambio de información, la asistencia legal mutua y la extradición.

- **Derechos Humanos**: El tratado incluye disposiciones que aseguran que las medidas adoptadas para combatir el cibercrimen no comprometan los derechos fundamentales, como la libertad de expresión y el derecho a la privacidad

Cada Estado firmante adoptará las medidas legislativas para establecer las facultades y procedimientos necesarios para las investigaciones o procesos penales que tengan por objeto los diversos tipos de delitos.

En cuanto a lo que respecta a la ***Convención de las Naciones Unidas contra la Ciberdelincuencia; Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de***

[5] Consultado en Document Viewer, en fecha 25 de marzo de 2025.

Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves, del año 2024, que dio a conocer la Asamblea General de las Naciones Unidas. Se informó a los estados miembros de las Naciones Unidas, que podrán rubricarlo hasta el 31 de diciembre de 2026.

De la misma manera, invitó a sumarse las organizaciones regionales de integración económica, como la Unión Europea (UE), la Asociación de Naciones de Asia Sudoriental) o la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), donde México forma parte.

Sin un marco legal que este fortalecido, México no cuenta con la capacidad para enfrentar las amenazas cibernéticas de manera efectiva. Además, la falta de ratificación de este Convenio, puede limitar la cooperación internacional, elemento clave en la lucha contra la cibercriminalidad.

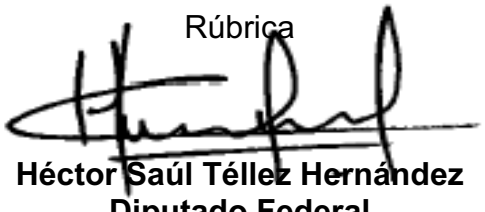
Por lo anteriormente expuesto, solicitamos su respaldo y sometemos a consideración de esta honorable Asamblea la presente proposición con

Punto de Acuerdo

Único. La Comisión Permanente del honorable Congreso de la Unión, exhorta al Ejecutivo Federal informe a la opinión pública sobre los acuerdos y el proceso intersecretarial que México ha mantenido para integrase a la Convención de las Naciones Unidas contra la ciberdelincuencia de las Naciones Unidas del año 2024.

Senado de la República, sede de la Comisión Permanente,
a los 5 días del mes de mayo de 2025

Rúbrica



Héctor Saúl Téllez Hernández
Diputado Federal