PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE LA COMISIÓN PERMANENTE EXHORTA RESPETUOSAMENTE A LA SECRETARIA DE GOBERNACIÓN PARA EL ANÁLISIS, CREACIÓN E IMPLEMENTACIÓN DE UN PLAN NACIONAL EN MATERIA DE CIBERSEGURIDAD, A CARGO DEL DIPUTADO ALEJANDRO VIEDMA VELÁZQUEZ, DEL GRUPO PARLAMENTARIO DE MORENA

El que suscribe, **Alejandro Viedma Velázquez**, Diputado Federal de la LXIV Legislatura, integrante del Grupo Parlamentario de MORENA, con fundamento en los artículos 58, 59 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, así como las demás disposiciones aplicables, someto a consideración de esta soberanía la siguiente proposición con punto de acuerdo por el que se exhorta respetuosamente a **la Secretaría de Gobernación para el análisis, creación e implementación de un Plan Nacional en materia de Ciberseguridad en cuanto a la comisión de delitos cibernéticos para proteger a la ciudadanía, conforme a la siguiente:**

EXPOSICIÓN DE MOTIVOS

El uso de tecnologias es cada vez más relevante en el uso cotidiano, la forma de vida ha cambiado y la implementación de herramientas cibernéticas creció con la llegada de la pandemia provocada por el COVID-19.

El trabajo a distancia, reuniones virtuales, compras en línea, etc., y el mayor flujo de información ha incrementado la violencia y crimen; convirtiéndose en ciberataques que pueden crear grandes problemas a empresas, organismos públicos y particulares.

Según el estudio sobre los Hábitos de Internet en México elaborado por la Asociación de Internet.mx y la consultoría The Competitive Intelligence Unit (The CIU, 2019), en México 86.8 millones de personas están conectadas a internet, es decir que ese mismo número de personas puede ser víctima de un crimen cibernético.

Como parte del contexto, es importante recordar que, en noviembre de 2001, los Estados miembros del Consejo de Europa firmaron el "*Convenio sobre la Ciberdelincuencia",* en Budapest. Dicho Convenio reconoce la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como proteger los intereses legítimos en la utilización y el desarrollo de tecnologías de la información.

El Convenio previene los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de estos, garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y sanción.

En México, diversas voces se han manifestado sobre la urgencia de discutir una Ley General de Ciberseguridad, entre esas voces se encuentran legisladores, legisladoras, y la del titular de la Secretaría de Seguridad y Protección Ciudadana al manifestar que esto es así en virtud de que "parte de los delitos que se cometen en el país se dan en el ciberespacio".

Ahora bien, resulta fundamental tener claro que un ciberataque es un conjunto de acciones ofensivas contra sistemas de información como bases de datos, redes computacionales, etc., hechas para dañar, alterar o destruir instituciones, personas o empresas.

Estos ciberataques se han incrementado debido a vacíos legales dentro del marco jurídico, es decir que hay una brecha entre la tecnología y la legislación, como consecuencia miles de personas usuarias quedan indefensas.

Asimismo, hay que señalar que cada vez las actividades sociales, económicas y hasta militares de un Estado se hacen más dependientes del uso de las Tecnologías de la Información y de la Comunicación, lo que implica una mayor vulnerabilidad y exposición a los ciberataques.

Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo, conlleva serios riesgos y

amenazas que pueden afectar a la Seguridad Nacional. Esto nos llama a fortalecer la seguridad de la ciudadanía, los privados y del Estado en el entorno digital, a nivel nacional y transnacional. Por tanto, es necesario fortalecer la defensa y la soberanía nacional en el entorno digital.

Como ejemplo, la estrategia de seguridad cibernética que ha implementado en Gobierno de Panamá, señalo algunos puntos fundamentales:

1. Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio.
2. Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos.
3. Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales.
4. Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares.

Con ello se busca proteger a las instituciones del Estado y a la sociedad frente a los ciberataques, lo anterior, a través de la instrumentación de acciones gubernamentales que permitan prevenir y sancionar los actos perpetrados por la ciberdelincuencia.

Por otro lado, la European Union Agency For Network and Information Security (en adelante ENISA) reconoció como las principales tendencias dentro del panorama de amenazas cibernéticas del 2020 las siguientes: Malware; Web Based Attacks; Web application Attacks; Phishing; DDos; Spam; Botnets; Data Breaches; Insider Threat; Physical manipulation/damage/theft/loss; Information Leakage; Identity Theft; Cryptohacking; Ramsomware; Cyber Espionage.

Esto indica que el uso malicioso de la tecnología amenaza la seguridad, la paz y estabilidad internacional. Es por lo que la ciberseguridad se ha vuelto una preocupación para la comunidad internacional.

La ciberseguridad en el ámbito personal, empresarial y gubernamental es uno de los desafíos clave de nuestro tiempo, por lo que es necesario en nuestro país un

Plan Nacional en materia de Ciberseguridad bajo el principio del respeto de los Derechos Humanos.

A fin de ser más puntual en este problema, el centro de respuestas a incidentes cibernéticos de la Dirección General Científica de la Guardia ha expuesto que los incidentes más registrados son: infección de código malicioso y el Phishing (método de engaño para obtener tu información mediante la suplantación de identidad).

Es decir, son conductas que afectan el patrimonio de los ciudadanos: Robo de identidad; fraude al comercio electrónico; fraude al usuario de la banca electrónica y extorsión.

En cuanto al ámbito político y público, nuestro país ha sufrido ataques cibernéticos, tanto en instituciones privadas (bancos) y públicas (gobiernos municipales, estatales y federales).

En contexto actual, varios servidores y servidoras públicas han reportado hackeos de sus cuentas celulares, y con ello, en algunos casos señalan robo de identidad para cometer extorsión y/o fraude. Entre dichos personajes destacan: el Presidente Nacional de Morena Mario Delgado; el Senador de Morena, Higinio Martínez Miranda; el Senador de Morena, Salomón Jara Cruz; el Gobernador electo de Sinaloa, Rubén Rocha Moya; el Senador del PRI, Manuel Añorve Baños; la Vicecoordinadora del PAN en el Senado, Kenia López Rabadán; la Diputada Federal con licencia, Dolores Padierna Luna; la Secretaria de Gobernación, Olga Sánchez Cordero; la Senadora Claudia Edith Anaya Mota; el Alcalde de Miguel Hidalgo, Víctor Hugo Romo; el Senador Ricardo Monreal Ávila; el Alcalde de Cuajimalpa, Adrián Rubalcava; el Diputado Casimiro Zamora Valdéz y la Diputada Yadira Santiago Marcos.

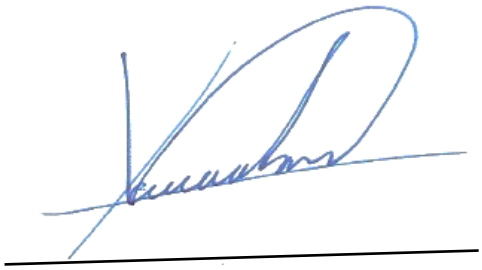
Bajo el contexto anterior, se plantea la necesidad de que exista un Plan Nacional en materia de Ciberseguridad para la investigación y persecución de las conductas que se han expuesto, y así salvaguardar a la ciudadanía y su información ante estos crímenes.

Por lo anteriormente expuesto, someto a consideración de esta Comisión Permanente del H. Congreso de la Unión la siguiente proposición con:

PUNTO DE ACUERDO

Único. Se exhorta respetuosamente a la Secretaría de Gobernación de México para el análisis, creación e implementación de un Plan Nacional en materia de Ciberseguridad.

Palacio Legislativo de San Lázaro a, 23 de agosto de 2021



Dip. Alejandro Viedma Velázquez