PROPOSICIÓN CON PUNTO DE ACUERDO QUE EXHORTA AL TITULAR DEL EJECUTIVO FEDERAL, A QUE, CON EL AUXILIO DE LA SECRETARÍA DE GOBERNACIÓN, LA SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA Y LA SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, Y CON BASE EN SUS RESPECTIVAS ATRIBUCIONES, REALICEN UN DIAGNÓSTICO INTEGRAL DE LA INFRAESTRUCTURA CRITICA DEL ESTADO MEXICANO EN MATERIA DE CIBERSEGURIDAD; Y ELABORE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE MÉXICO, A CARGO DE LA DIPUTADA MARÍA EUGENIA HERNÁNDEZ PÉREZ.

La que suscribe, María Eugenia Hernández Pérez, Diputada Federal de la LXIV Legislatura del Honorable Congreso de la Unión, e integrante del Grupo Parlamentario de MORENA, con fundamento en lo señalado en el artículo 78, párrafo segundo, fracción III de la Constitución Política de los Estados Unidos Mexicanos y los artículos 116 y 122, numeral 1 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, así como los artículos 58 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicano, somete a la consideración de esta Asamblea la siguiente Proposición con Punto de Acuerdo que exhorta al titular del Ejecutivo Federal, a que, con el auxilio de la Secretaría de Gobernación, la Secretaría de Seguridad y Protección Ciudadana y la Secretaría de Comunicaciones y Transportes, y con base en sus respectivas atribuciones, realicen un diagnóstico integral de la infraestructura critica del Estado mexicano en materia de ciberseguridad; y elabore la Estrategia Nacional de Ciberseguridad de México, en términos de las siguientes.

CONSIDERACIONES

Primera.- A través de los últimos años, las tecnologías digitales se han vuelto pilar importante de la economía mundial, en los años 60´s del siglo pasado, Paul Baran propuso la sustitución de las instalaciones y de los sistemas de comunicaciones centralizados por un sistema reticular de comunicación y un método de división y conmutación de la información en bloques, lo que se considera el origen de ARPANET en 1969, rebautizado como INTERNET en los noventa. Desde entonces, las tecnologías de la información y de la comunicación (TIC) han avanzado a una velocidad imparable, al punto de volverse recursos críticos para distintos sectores clave en la economía nacional, por ejemplo, combinaciones de tecnologías complejas que, gestionan y mantienen a flote nuestras finanzas, se encargan de tareas críticas y de alta precisión

en distintos en sectores relevantes como el energético, las comunicaciones, salud y transporte.

Incluso los nuevos modelos de negocio están construidos con base en una continua y estable **disponibilidad** del internet y el funcionamiento de los sistemas informáticos. En este contexto, los incidentes de ciberseguridad pueden irrumpir en la disponibilidad de estos sistemas con repercusiones a sistemas vitales para nuestra existencia, como el abastecimiento de recursos vitales como la electricidad y el agua. Este tipo de incidentes puede tener distintos orígenes e intereses, como son los criminales, de competencia entre empresas, ataques financiados, desastres naturales, diferencias entre países, o simplemente por errores humanos[1].

Segunda.- De esta manera, la articulación de un modelo jurídico del ciberespacio no es una opción, sino una necesidad, incluso un imperativo. Operar mediante una mera traslación de las normas existentes desde el espacio físico al mundo virtual es insuficiente y erróneo. La eficacia del derecho como instrumento de ordenación de la vida en sociedad depende de su capacidad para responder a las coordenadas y singularidades propias de la realidad que está llamado a regular[2]. El ciberespacio no solo es una realidad diferente, sino que también es una realidad capacitada para alterar la naturaleza y el funcionamiento de la realidad no virtual.

Según *Willis Towers Watson*, compañía mundial líder en gestión de riesgos, en el año 2018 el 83% de las empresas mexicanas fueron víctimas de ciberataques al menos una vez al año y solo el 30% de éstas tenían algún plan de protección contra incidentes informáticos. De igual forma para 2019 las pérdidas a causa de ciberataques se encontraban cerca de 1.5 millones de dólares, y se estimó que el costo total anual por delito cibernético en la economía mundial podría sobrepasar los 2 billones de dólares[3].

Tercera.- En México, durante los últimos años los ciberataques a la infraestructura critica de las instituciones públicas, estatales y de gobierno federal, han aumentado de manera drástica. Basta enlistar un par de casos recientes para justificar la urgencia de

---

1 Diciembre 2019 Consultado: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

2 Margarita Robles Carrillo. (2015). EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO. Boletín Electrónico: ieee.es.

3 Riesgo Cibernético y Ciberseguridad 2019 disponible en: https://www.gob.mx/cms/uploads/attachment/file/478193/181.-_Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf

la creación de una **Estrategia Nacional de Ciberseguridad**. Por ejemplo, el ataque cibernético registrado el 17 de abril del año 2018 al Sistema de Pagos Electrónicos Interbancarios **(SPEI)**, el cual es un mecanismo de liquidación en tiempo real desarrollado por el Banco de México (Banxico); el monto sustraído a través de este ciberataque al sistema no es fácil de calcular, ya que no todas las instituciones afectadas publican cifras al respecto. Sin embargo, se estiman alrededor de **400 millones** de pesos de acuerdo cifras publicadas en el periódico El Financiero.[4]

Otro ejemplo importante a destacar es el ataque cibernético más reciente, dirigido contra Petróleos Mexicanos (PEMEX) en nviembre del 2019, este ataque fue del tipo ransomware (*ataque que cifra la información de la víctima, a cambio de un pago de rescate se devuelve el control sobre la información cifrada*), donde los ejecutores esperaban recibir 4.9 millones de dólares a cambio de restaurar los archivos de la petrolera. Por último, el ejemplo más reciente, donde la Suprema Corte de Justicia de la Nación (SCJN) informó que la página de internet del Alto Tribunal sufrió el martes 9 de Junio de 2020 una serie de ataques cibernéticos, donde La SCJN afirmó que se llevaron a cabo los protocolos de ciberseguridad y la funcionalidad de la página se restableció.

Cuarta.- Por otro lado, el Reporte de Estabilidad Financiera desarrollado por el Banco de México (Banxico)[5] señala que, de acuerdo con el Comité Especializado de Seguridad de la Información, órgano consultor del **Consejo de Seguridad Nacional**, durante los meses de contingencia sanitaria por la pandemia del Covid-19, el número de ciberataques a empresas, instituciones gubernamentales y personas a nivel mundial se ha incrementado hasta en 400 por ciento. Los atacantes están aprovechando que una gran cantidad de personas se encuentran trabajando desde sus hogares y que las empresas han otorgado mayor flexibilidad para que sus trabajadores puedan acceder a información laboral fuera de sus instalaciones.

Es entonces evidente que, las vulnerabilidades en sitios gubernamentales existen, son muchas y variadas. Esto debe alertar especialmente a aquellos profesionales que son los responsables de la seguridad de los sistemas del Estado Mexicano, pero sobre todo al mismo Estado en sí (en un sentido general, a todos sus niveles de poder).

---

4 Consultado en septiembre de 2019 a través de: https://www.elfinanciero.com.mx/economia/hackers-sustraen-400-mdp-de-bancos

5 ALEJANDRO DÍAZ DE LEÓN CARRILLO. (2020). Riesgos cibernéticos. En Reporte de Estabilidad Financiera(163). México: Banxico.

Quinta.- Para atender este fenómeno de seguridad es necesario que el gobierno federal construya una **Estrategia Nacional de Ciberseguridad,** que podemos definir como "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio". Esta estrategia le ayudara a transitar hacia un nuevo régimen de apropiación de la tecnología de manera segura y confiable, salvaguardando la integridad y privacidad de la información que enviamos y recibimos día a día.

El desarrollo de una estrategia integral puede plantear muchos desafíos, ya que es necesario lograr la cooperación y el acuerdo entre las partes interesadas, lograr un curso de acción común, y esta tarea no será fácil. Debe tenerse en cuenta que el proceso de desarrollo de la estrategia es probablemente tan importante como el documento resultante final. Como primer paso para transitar hacía la creación de esta estrategia nacional, es menester hacer un **diagnóstico integral** del estatus actual de la infraestructura critica del Estado, para marcar un punto de partida, analizar fortalezas y debilidades y detectar el nivel de vulnerabilidad de cada institución.

Es evidente que México necesita tomar acciones más contundentes y congruentes con la realidad actual, ya que la responsabilidad principal en esta tarea le corresponde al Estado, y requiere un planteamiento capaz de reconocer la presencia de dos condicionantes: uno, la superación real del **marco estatal** que impone la existencia del ciberespacio, en particular, en el ejercicio de la soberanía y de las competencias estatales vinculadas al territorio del Estado; y, dos, el imperativo de la **cooperación internacional** para la ordenación jurídica del ciberespacio[6].

Con base en las consideraciones expuestas, se somete a la consideración de esta Soberanía la siguiente proposición con:

PUNTO DE ACUERDO

6 Margarita Robles Carrillo. (2015). EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO. Boletín Electrónico: ieee.es.

PRIMERO. – La Comisión Permanente del Congreso de la Unión, exhorta respetuosamente, al titular del Ejecutivo Federal, a que, con el auxilio de la Secretaría de Gobernación, la Secretaría de Seguridad y Protección Ciudadana y la Secretaría de Comunicaciones y Transportes, y con base en sus respectivas atribuciones, realicen un diagnóstico integral de la infraestructura critica del Estado mexicano en materia de ciberseguridad, como punto de partida para fundamentar las decisiones legislativas e institucionales que procedan al respecto.

SEGUNDO. – La Comisión Permanente del Congreso de la Unión, exhorta respetuosamente, al titular del Ejecutivo Federal, a que, con el auxilio de la Secretaría de Gobernación, la Secretaría de Seguridad y Protección Ciudadana y la Secretaría de Comunicaciones y Transportes, y con base en sus respectivas atribuciones, elaboren la Estrategia Nacional de Ciberseguridad de México, en coordinación con las Comisiones de Ciencia, Tecnología e innovación y de Seguridad Pública de ambas Cámaras del Congreso de la Unión.

Dado en el salón de sesiones de la Comisión Permanente, a 1 de julio de 2020.

DIPUTADA MARÍA EUGENIA HERNÁNDEZ PÉREZ