INICIATIVA QUE ADICIONA LOS ARTÍCULOS 5°., 6°. Y 13 DE LA LEY DE SEGURIDAD NACIONAL, A CARGO DE LA DIPUTADA MARÍA EUGENIA HERNÁNDEZ PÉREZ, DEL GRUPO PARLAMENTARIO DE MORENA

La suscrita, María Eugenia Hernández Pérez, diputada integrante del Grupo Parlamentario de Morena en la LXV Legislatura, con fundamento en los artículos 71, fracción II, y 73, fracción XXIII, de la Constitución Política de los Estados Unidos Mexicanos; 6, numeral 1, fracción I, 77, numeral 1, 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 adiciona la fracción XIV al artículo 5, una fracción VII al artículo 6 y se reforma el artículo 13 de la Ley de Seguridad Nacional, al tenor del siguiente:

Planteamiento del problema

A través de los últimos años, las tecnologías digitales se han vuelto pilar importante de la economía mundial, al punto de volverse recursos críticos para distintos sectores clave en la economía nacional, se han creado nuevas tecnologías complejas que, por ejemplo, gestionan y mantienen a flote nuestras finanzas, se encargan de tareas críticas y de alta precisión en distintos 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 criminales, competencia entre empresas, ataques financiados, desastres naturales, o simplemente por errores humanos[1] .

Según Willis Towers Watson, compañía mundial lider en gestión de riesgos, en 2018, 83 por ciento de las empresas mexicanas fueron víctimas de ciberataques al menos una vez al año y solo el 30% de estas 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[2] .

En este sentido, múltiples mercados y en particular los sectores aseguradores, los de tecnologías de la información, los financieros y hasta la **seguridad nacional**, evolucionan a la par de la tecnología con nuevas herramientas para su operación, así como con productos y servicios novedosos, quedando potencialmente expuestos a ciber riesgos que pueden impactar directamente en la solvencia y estabilidad de las instituciones y en consecuencia en menoscabo de los intereses de los consumidores.

Con todas estas nuevas tecnologías que tienen como principal base la disponibilidad del **Internet,** nace el concepto de otro nuevo tipo de espacio de interacción humana, el Ciberespacio, un nuevo espacio Global común, como los tradicionales terrestres, marítimo, aéreo y espacial[3] , que tiene una singularidad natural, es virtual. A través de este espacio podemos interactuar con personas de todo el mundo en tiempo real, trascendiendo barreras físicas y temporales, así como las fronteras entre países gracias a la interacción de personas, software y servicios en Internet mediante dispositivos tecnológicos. El término ciberespacio fue utilizado por primera vez en la obra *Neuromante* del escritor norteamericano William Gibson y publicada en el emblemático 1984 que presagió el escritor británico George Orwell.

En este orden de ideas, es pertinente la pregunta: ¿Qué es la Ciberseguridad y Cuáles son los riegos cibernéticos en torno a ella?

Según el NIST, Instituto Nacional de Estándares y Tecnología de Estados Unidos, se define el riesgo cibernético[4] como el riesgo de pérdida financiera, interrupción operativa o daño, debido a la falla de las

tecnologías digitales empleadas para funciones informativas y/o operativas introducidas a un sistema por medios electrónicos sin acceso autorizado, para el uso, divulgación, interrupción, modificación o destrucción de los sistemas. El termino ciber riesgo, se encuentra íntimamente vinculado a los conceptos de ciber amenaza y ciber ataque. **La ciber seguridad,** según la Organización Internacional de Estandarización (ISO), en la norma ISO/IEC 27032[4] es definida como la preservación de la **confidencialidad**, **integridad** y **disponibilidad** de la información en el ciber espacio. Con este panorama podemos concluir que los ciber ataques son incidentes que pueden ocasionar una multiplicidad de daños, que podrían generar a su vez repercusiones en cadena sobre los distintos eslabones de la cadena productiva y que la ciber seguridad se refiere al proceso de proteger la información o sistemas de información, mediante la prevención, detección y respuesta a uno o varios ciber ataques.

El crecimiento de Internet de manera global y la creación de nuevos avances tecnológicos nos obliga a tomar acciones que salvaguarden la **integridad**, **disponibilidad** y **confidencialidad** de la información que compartimos en Internet, por otro lado, la seguridad de la información se vuelve forzosamente del interés del gobierno, ya que la digitalización de documentos y servicios del Estado son también propensos a ciber ataques que atenten contra la privacidad de la información privilegiada de la nación.

Hasta hace un par de años los ataques cibernéticos no parecían tener relevancia en nuestro país, la atención de los criminales cibernéticos se centraba en países como Israel, China, EU, o Corea del Sur, países líderes en tecnología que cuentan con información privilegiada, sin embargo, en los últimos años la situación ha ido cambiando en América Latina. En México se han presenciado incidentes de ciber ataques que le han costado grandes cantidades de dinero a nuestro país, prueba de ello es el incidente registrado el 17 de abril de 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) que le permite a las distintas instituciones que colaboran en el sistema, interactuar entre ellas haciendo envíos y transferencias de fondos en moneda nacional; el monto sustraído a través del ciber ataque al sistema no fue 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 Financiero* .[6]

Otro tipo de ataque cibernético reportado recientemente en América Latina, ha sido el ataque por **ransonware** (virus informático que cifra la información valiosa del afectado, y los ejecutores piden un depósito monetario a cambio de la contraseña para descifrar la información) que ha tenido un aumento anual del 30 por ciento entre 2014 y 2016, con los indicadores a que la tendencia se mantendrá. De acuerdo con datos revelados por Kaspersky Lab[7] , Brasil encabeza la lista de los países latinoamericanos con 54.91 por ciento de los ataques, seguido por México con 23.40 por ciento.

Cabe destacar el ciber ataque más reciente, dirigido contra Petróleos Mexicanos (**Pemex)** , importante conglomerado de petróleo en México, también este ataque fue del tipo **ransomware** , donde los ejecutores esperaban recibir 4.9 millones de dólares a cambio de restaurar los archivos de la petrolera. Respecto a este hecho, el Presidente Andrés Manuel López Obrador, a través de la Titular de la Secretaría de Energía, Rocío Nahle, sostuvo que el gobierno no cederá a esta extorsión ya que el departamento de informática ya estaba tomando acciones al respecto[8] .

Entre las consecuencias de los ataques mencionados, no solo están las perdidas monetarias, si no el robo de información privilegiada o la pérdida de datos de alta importancia en las instituciones bancarias, empresas productivas del Estado como Pemex, empresas de tecnología y a los ciudadanos en general. Laura Jiménez, directora regional de la empresa de ciberseguridad Darktrace, indicó que, aunque el daño generado por el reciente ataque contra PEMEX parezca ser mínimo, debería tomarse como una llamada de alerta, y que las amenazas cibernéticas a la infraestructura son una de las **mayores amenazas a la seguridad nacional** de México".[9]

En 2017 se llevó a cabo el proceso de desarrollo de la Estrategia Nacional de Ciberseguridad (ENCS)[10] , con apoyo y participación de diferentes actores en México: sociedad civil, sector privado, comunidad técnica y académica, e instituciones públicas de los tres poderes.

La presente iniciativa plantea reformas legislativas para enfrentar este complejo problema, en la perspectiva de salvaguardar la seguridad nacional, en concordancia con los postulados de la ENCS.

Argumentación

Seguridad Nacional y Ciberseguridad

La Ley General del Sistema Nacional de Seguridad Pública, reglamentaria del artículo 21 constitucional, establece que la seguridad pública tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el **orden** y la **paz** públicos. En ese sentido el actual gobierno del presidente Andrés Manuel López Obrador en su "Estrategia Nacional de Seguridad Pública" establece que se promoverán acciones legislativas, operativas, orgánicas y presupuestales para consolidar una unidad policial especializada, así como la orientación de la Policía Cibernética para una plena operatividad[11] , esfuerzos apropiados para el tratamiento de crímenes sofisticados que involucran el uso de las nuevas tecnologías. Aun así, es importante considerar la importancia de asegurar y mantener la integridad de la **infraestructura tecnológica critica** del país, considerando que está, es parte del ciberespacio y goza de los beneficios y riesgos que esto lleva consigo, como **la exposición de las infraestructuras críticas** a las amenazas internacionales, **guerra cibernética**, **ciberespionaje**, y la continua **militarización** del ciberespacio. Estos riesgos pueden comprometer la **Seguridad Nacional** de distintas maneras, tales como la filtración de datos confidenciales de la nación, la intervención de las comunicaciones privadas del Estado, así como la vulneración de activos informáticos críticos para la provisión de servicios vitales como el agua, la luz y el mismo Internet. Es por esto, que es de singular importancia considerar el valor de los espacios comunes globales (dominios no susceptibles de apropiación, presididos por el **principio de libertad)** como lo es el **ciberespacio,** ya que su buen uso resulta indispensable para la seguridad nacional del país.

En los próximos años, es altamente probable que crezca el uso de tecnologías de información en el sector público, sector privado y la sociedad, incrementando la amenaza de los ciberriesgos. Por lo tanto, el fomento de una verdadera inclusión de la ciberseguridad como eje trascendente y transversal en la política nacional de seguridad por parte del gobierno se convierte en una prioridad para el desarrollo de México.

La propia naturaleza del ciberespacio y el Internet de trascender fronteras territoriales y espaciales nos propone considerar **la cooperación internacional** como una herramienta completamente necesaria para abordar el tema de la ciberseguridad, ya que los atacantes y criminales cibernéticos podrían estar en nuestro territorio nacional o a miles de kilómetros en cualquier otro país. La necesidad de articular convenios de cooperación internacional que faciliten el rastreo de ataques cibernéticos, que propongan la protección de la infraestructura critica de los países y creen una dinámica continua distribución de documentos técnicos y reportes especializados en torno a el combate a ataques cibernéticos especializados, es primordial en el tema de la ciberseguridad.

El instrumento más importante en torno a la ciberseguridad y cooperación internacional fue creado en noviembre del 2001, denominado **Convenio sobre la Ciberdelincuencia** [12] o mejor conocido como el **Convenio de Budapest** debido a la ciudad donde fue desarrollado, este Convenio tiene por objetivo combatir la ejecución de delitos cometidos a través de Internet y otras redes informáticas, el convenio entró en vigor en el año 2004 y constituye hasta ahora el único instrumento internacional que aborda de manera directa el tema del cibercrimen. En sus 48 artículos describe los tipos de actividades en el ciberespacio que serán acreedoras a una sanción penal, si se toma como referencia este tratado, y al mismo tiempo emite una seria de medidas y

recomendaciones para acompañar las sanciones jurídicas como: asistencia 24/7 los 365 días del año, asistencia mutua para la obtención de datos en tiempo real, consultas entre miembros del convenio, etcétera.

Si bien en su mayoría el Convenio de Budapest es un marco de referencia para tipificar los delitos cibernéticos y proponer sanciones a los mismos, podemos notar que el tratado también busca acciones internacionales que sumen esfuerzos para combatir la amenaza de los ciber delitos que por la misma naturaleza de estos trasciende a un asunto de interés internacional. La ciberseguridad desempeña cada vez un papel más importante en muy diversos ámbitos de las relaciones internacionales, como los derechos humanos, el desarrollo económico, las transacciones, el comercio, el control de armamentos, la seguridad, la estabilidad, la paz y la resolución de conflictos.

Por lo tanto, la política de seguridad nacional debe reconocer la naturaleza sin fronteras de la ciberseguridad y destacar la necesidad de cooperar no sólo con los agentes nacionales, sino también con los internacionales. Los compromisos internacionales con los agentes públicos y privados son fundamentales para facilitar un diálogo constructivo, instaurar mecanismos de confianza y cooperación, encontrar soluciones mutuamente aceptables a problemas comunes y crear una cultura mundial de ciberseguridad.

La Ley de Seguridad Nacional no reconoce a las amenazas cibernéticas como amenazas a la Seguridad Nacional, dicha ley en su **artículo 5** enlista todos los incidentes que considera "**amenazas a la seguridad nacional"** , sin embargo, a lo largo de sus **XIII** fracciones no incluye los ataques cibernéticos, ni las acciones criminales en el ciberespacio. Otros países en una etapa de maduración más favorable en torno a la ciberseguridad como es el caso de España adhieren y consideran en sus estrategias de desarrollo nacional a las ciber amenazas y el uso ilegitimo del ciberespacio como amenazas y riesgos a la Seguridad Nacional[13] ; esa política es pertinente para evitar situaciones de inestabilidad y mantener en paz y legitima soberanía a una Nación en esta era de cambio tecnológico exponencial.

Por último, es necesario reconocer dentro de la sensibilidad de los ciberataques el recientemente anunciado ataque a las Fuerzas Armadas, en el cual se concluye que una tardía reacción por parte del gobierno federal que permitió que información sensible se usara con fines políticos y mediáticos. Juan Manuel Aguilar, investigador en ciberseguridad del Colectivo de Análisis de la Seguridad con Democracia, AC (Casede), en entrevista con el independiente[14] comenta que nunca se había tenido este precedente de un tema de ciberseguridad en México que dañará el caso concreto de la esfera de la seguridad nacional. Habíamos tenido el caso de Lotería Nacional, del Banco de México, pero no con ese manejo de una explotación y extracción de información que pudiera comprometer la imagen del presidente y de las Fuerzas Armadas. En la misma entrevista comenta, que se hablan de 6 terabytes de información extraída de los sistemas estratégicos, que es una cantidad tremenda de datos y lo que tendríamos que se tendría que ponderar es un análisis de riesgos reputacional, riesgo político y riesgo institucional en el ámbito concreto que podría afectar la imagen de las instituciones y puede estar disponible para medios de comunicación y diferentes actores políticos en el marco de los próximos meses, incluso años. Es por ende de que independientemente de que algunas asociaciones de la sociedad civil opinan que no es necesaria la visión militar en la atención a los denominados ciberataques la realidad de nuevo nos alcanza y nos obliga a no caer en vacíos legales que vulneren no solo al gobierno federal y fuerzas armadas, si no que evitemos futuros estragos a la ciudadanía, iniciativa privada y el sector académico.

Es importante señalar que en México existen algunos esfuerzos importantes de ciberseguridad, pero todos ellos están enfocados principalmente a la seguridad de cada institución de gobierno y no a coordinar la ciberseguridad nacional, por lo que el Programa Sectorial de Defensa Nacional 2013-2018 señala que:

> "La seguridad en el ciberespacio en México no se ha abordado desde el punto de vista de la defensa nacional, ya que sólo se ha atendido desde el ámbito de la seguridad institucional y persecución del delito, no obstante

que en la agenda nacional de riesgos 2012 se planteó que la vulnerabilidad cibernética puede impactar en la defensa del Estado mexicano" (2013:21).

Es entonces evidente que el ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra.

En base a los argumentos antes expuestos, la presente Iniciativa plantea la propuesta de reformar el artículo 5, de la Ley de Seguridad Nacional, con el objeto de establecer lo siguiente:

- Reconocer a los ataques cibernéticos como amenazas a la Seguridad Nacional.

- Que se cree una estrategia de defensa a los ataques cibernéticos.

- Que se fomente la cooperación internacional en torno a la ciberseguridad como política exterior.

Con la presente Iniciativa, se busca reconocer los ataques cibernéticos como amenazas a la Seguridad Nacional, teniendo en mente que la mayoría de las instituciones de gobierno, incluyendo a la Secretaría de Seguridad y Protección Ciudadana, la Marina y la Sedena, tienen una tendencia a la digitalización de sus servicios y operaciones diarias y se han vuelto altamente dependientes de la disponibilidad de sus infraestructuras críticas.

Al mismo tiempo esta Iniciativa busca detonar múltiples esfuerzos en las distintas instituciones públicas, en la iniciativa privada y el sector social, que ayuden a nuestro país a transitar hacia un estado de maduración en torno a la ciberseguridad congruente con el contexto tecnológico internacional. Así como plantear la cooperación, nacional e internacional como una necesidad indispensable para el tratamiento de los ciber ataques y sus consecuencias.

Por último, la presente iniciativa se enmarca en los objetivos generales de la Estrategia Digital Nacional que contempla a la ciberseguridad como uno de los nueve ejes de acción.

Por lo anteriormente expuesto, someto a consideración de esta honorable asamblea, la presente Iniciativa con proyecto de

Decreto por el que se adiciona la fracción XIV al artículo 5; una fracción VII al artículo 6 y se reforma la fracción IX del artículo 13; todos de la Ley de Seguridad Nacional

Único. Se adiciona la fracción XIV al artículo 5; una fracción VII al artículo 6 y se reforma la fracción IX del artículo 13; todos de la Ley de Seguridad Nacional, para quedar como sigue:

Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. a XIII. ...

XIV. Actos que tiendan a dañar, interrumpir u obtener acceso no autorizado a la Infraestructura Critica del Estado a través del ciberespacio, con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación, destruir la integridad de los datos o robar la información controlada.

Artículo 6. Para los efectos de la presente ley, se entiende por:

I. a VI. ...

VII. Ciberespacio: Dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores.

Artículo 13. El Consejo de Seguridad Nacional es una instancia deliberativa cuya finalidad es establecer y articular la política en la materia. Por tanto, conocerá los asuntos siguientes:

I. a VIII. ...

IX. Los procesos de clasificación**,** desclasificación **y resguardo** de información en materia de seguridad nacional, y

X. ...

Artículo Transitorio

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

Notas

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

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

3 El Ciberespacio nuevo escenario de confrontación, disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o /monografia_126.pdf

4 National Institute of Standards and Technology (NIST), glosario de términos, disponible en:

https://csrc.nist.gov/glossary/term/Cyber-Risk

5 International Organization for Standardization (ISO), norma ISO/IEC 27032, disponible en:

https://www.iso27001security.com/html/27032.html

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

7 Consultado en septiembre de 2019 a través de: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

8 Pemex no pagará por ciberataque; López Obrador: Hackeo no fue tan grave, disponible en:

https://www.excelsior.com.mx/nacional/pemex-no-pagara-por-ciberataque-l opez-obrador-hackeo-no-fue-tan-grave/1347669

9 Ciberataque a Pemex afectó al 5% de las computadoras, disponible en:

https://itmastersmag.com/seguridad/ciberataque-a-pemex-a fecto-al-5-de-las-computadoras/

10 Estrategia Nacional de Ciberseguridad, disponible en:

https://www.gob.mx/cms/uploads/attachment/file/271884/Es trategia_Nacional_Ciberseguridad.pdf

11 Plan Nacional de Desarrollo 2019-2024, disponible en:

https://dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019

12 Convenio sobre la Ciberdelincuencia, disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

13 Amenazas y desafíos para la seguridad nacional, disponible en: https://www.dsn.gob.es/sites/dsn/files/ESN2017_capitulo_4.pdf

14 Hackeo a Sedena desnuda descoordinación en los esfuerzos en materia de ciberseguridad. (2022, 3 octubre). El Independiente. Recuperado 4 de octubre de 2022, de

https://elindependiente.com.mx/2022/10/03/hackeo-a-sedena-desnuda-descoordinacion-en-los-esfuerzos-en-materia-de-ciberseguridad/

Palacio Legislativo de San Lázaro, a 11 octubre de 2022.

Diputada María Eugenia Hernández Pérez (rúbrica)