INICIATIVA CON PROYECTO DE DECRETO QUE DECLARA EL 23 DE NOVIEMBRE DE CADA AÑO COMO "DÍA NACIONAL DE LA CIBERSEGURIDAD", 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 los artículos 70, 71, fracción II, y 78, párrafo segundo, fracción III, de la Constitución Política de los Estados Unidos Mexicanos; 116 y 122, numeral 1, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; y 55, fracción II, del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, somete a la consideración de esta Soberanía, la siguiente Iniciativa con Proyecto de Decreto que declara el 23 de noviembre de cada año como "Día Nacional de la Ciberseguridad", al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

El uso de las tecnologías es cada vez más extendido, su aplicación abarca prácticamente todos los ámbitos de la vida pública, privada, empresarial y social. Las tecnologías han generado una revolución permanente en la organización, la comunicación y la sistematización de las actividades económicas, académicas, educativas, de salud, financieras, militares, y un largo etcétera. Cada vez es más evidente que la innovación y aplicación especializada, masiva y sofisticada de tecnologías tiene pocos límites, que no se detiene ante fronteras ni regulaciones constrictivas.

La vida contemporánea se vuelve cada vez más fluida y dinámica gracias a la tecnología, si bien es importante advertir una creciente dependencia de la humanidad de los instrumentos, las redes, los sistemas, los aparatos que condensan las tecnologías, de tal forma que cuando se presentan fallas, son muchos los ámbitos y muchas las personas que resultan afectadas seriamente. Sin embargo, lo más preocupante es la cuestión de las diversas formas en que la delincuencia está utilizando los propios recursos de las tecnologías para vulnerar y sustraer la

seguridad, el patrimonio y la integridad de las personas, de las empresas, de las organizaciones, de las instituciones públicas y del Estado en su conjunto.

En efecto, las tecnologías digitales se han vuelto pilar importante 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. 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 orden de ideas, cobra gran relevancia la cuestión de la ciberseguridad, para evitar riesgos que pueden afectar la disponibilidad de estos sistemas, lo cual tendría repercusiones en 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.[i]

Es importante, en este orden de ideas, aproximarnos a la idea de lo que es la ciberseguridad y cuáles son los riegos cibernéticos en torno a ella. La ciberseguridad, según la Organización Internacional de Estandarización (ISO), en la norma ISO/IEC 270325, es definida como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Los ciberataques 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; por lo tanto, la ciberseguridad se refiere al proceso de proteger la información o sistemas de información, mediante la prevención, detección y respuesta a uno o varios ciberataques.[ii]

La ciberseguridad está íntimamente ligada al crecimiento de internet a nivel global y la creación de nuevos avances tecnológicos; esto 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 ciberataques que atenten contra la privacidad de la información privilegiada de la nación. [iii]

Cabe señalar que hasta hace un par de años los ataques cibernéticos no parecían tener relevancia en nuestro país. Los crímenes cibernéticos se centraban 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 ciberataques que le han costado grandes cantidades de dinero a nuestro país, como el registrado el 17 de abril del año 2018 al Sistema de Pagos Electrónicos Interbancarios (SPEI), del Banco de México, que hace envíos y transferencias de fondos en moneda nacional; el monto sustraído a través del ciberataque 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 periódico El Financiero.[iv]

Otro tipo de ataque cibernético reportado recientemente en América Latina ha sido el ataque por ransomware (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% entre 2014 y 2016, con los indicadores apuntando a que la tendencia se mantendrá.[v] Cabe destacar el ciberataque más reciente, dirigido contra Petróleos Mexicanos (Pemex), 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.

Como puede observarse, la vulneración de la ciberseguridad es un fenómeno que cada vez abarca a más países y más ámbitos en el mundo. 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. De hecho, los daños que la ciberdelincuencia pueden ser muy graves, toda vez que pueden desquiciar los sistemas financieros, de salud, educativos, militares; de tal forma que garantizar la ciberseguridad se convierte en una cuestión de seguridad nacional.

Ahora bien, legislar sobre un tema como la ciberseguridad resulta sumamente complejo, dadas las características globales del fenómeno y la velocidad vertiginoso a la que cambian las tecnologías, los sistemas, los programas y las aplicaciones. Actualmente se está dando en el mundo un proceso de construcción de acuerdos a

nivel mundial para que los diversos Estados emitan legislaciones que permitan la cooperación internacional en la investigación, persecución y castigo de la ciberdelincuencia. Cabe mencionar al respecto el Convenio sobre la Ciberdelincuencia, mejor conocido como el Convenio de Budapest, creado en 2001 y en vigor desde 2004. El Convenio fue ratificado por los Estados miembros del Consejo de Europa, por los Estados no miembros que participaron en su elaboración, y quedó abierto para la adhesión de otros Estados no miembros.

El Convenio de Budapest describe las diversas modalidades de delitos que se pueden perpetrar en el ciberespacio y al mismo tiempo emite una seria de medidas y recomendaciones para acompañar las sanciones jurídicas. El Convenio de Budapest es un marco de referencia para tipificar los delitos cibernéticos y proponer sanciones a los mismos, promueve acciones internacionales que sumen esfuerzos para combatir la amenaza de los ciberdelitos, que por su misma naturaleza es un fenómeno de interés internacional. Es decir, el Convenio reconoce la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información, estimando que una lucha bien organizada contra la cibercriminalidad requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz. [vi]

México no ha firmado y ratificado el Convenio de Budapest, al igual que muchos otros países, a pesar de que el Consejo de Europa abrió a toda la comunidad internacional la posibilidad de que suscriban y asuman las medidas que proclama dicho Convenio. Sin embargo, México está cada vez más inmerso en la necesidad de legislar y generar políticas públicas encaminadas a garantizar la ciberseguridad, por la potencial capacidad de desestabilización nacional que implica su vulneración.

Los anteriores argumentos constituyen dan contexto a la presenta Iniciativa, cuya propuesta central es hacer visible en México la necesidad de garantizar la ciberseguridad, con el fin de que tanto el Estado como la sociedad, las empresas, las instituciones, la academia y los científicos enfoquen la mirada en la urgencia de construir el marco jurídico, las estrategias y las acciones necesarias para lograr ese objetivo. La propuesta de la presente Iniciativa, de declarar un Día Nacional de la Ciberseguridad, contribuirá significativamente a concentrar la atención y generar conciencia sobre las serias amenazas que la ciberdelincuencia representa para la

seguridad, la integridad y el bienestar de las personas, de las empresas, de las instituciones y del Estado mismo.

A manera de recapitulación y actualización del panorama de la ciberdelincuencia en México, cabe indicar que, en 2019, el 73% de las organizaciones en México han experimentado por lo menos un incidente de ciberseguridad, un porcentaje similar al 70% registrado a nivel mundial, de acuerdo con la encuesta *El Estado de la Seguridad en la Nube* realizada por *Sophos*. Según dicho estudio, los incidentes más comunes en México son malware (34%), ransomware (25%), exposición de datos internos (28%), robo de credenciales (19%) y crypto jacking (10%).

De esa forma, nuestro país figura en el décimo primer lugar a nivel mundial con más casos de este tipo, siendo la India el primer lugar con el 93% de las organizaciones afectadas en el último año. En cuanto a América Latina, nuestro país reportó menor porcentaje de incidentes que Brasil (79%) y Colombia (76%). De acuerdo con el informe, las firmas europeas sufrieron el menor porcentaje de incidentes de seguridad en la nube, un indicador alentador de que el cumplimiento del Reglamento General de Protección de Datos (GDPR) está ayudando a proteger a las organizaciones de ser comprometidas.[vii]

En conclusión, es de gran importancia que el Congreso de la Unión decrete la celebración del “Día Nacional de la Ciberseguridad”. En función de lo anteriormente señalado respecto a la relevancia del Convenio de Budapest, se considera que la fecha adecuada para establecer la celebración en comento, sería la el 23 de noviembre de cada año, toda vez que, en esa fecha, en 2001, fue elaborado y puesto a la firma de los Estados.

Por todo lo anteriormente expuesto, se somete a la consideración de esta Soberanía, el siguiente Proyecto de

DECRETO

Que declara el 23 de noviembre de cada año como “Día Nacional de la Ciberseguridad”.

ÚNICO. El honorable Congreso de la Unión, declara el 23 de noviembre de cada año, como "Día Nacional de la Ciberseguridad".

TRANSITORIOS

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

Dado en el salón de sesiones de la Comisión Permanente, a 5 de agosto de 2020

DIPUTADA MARÍA EUGENIA HERNÁNDEZ PÉREZ

Referencias

[i] Consultado en julio de 2020, disponible en: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[ii] International Organization for Standardization (ISO), norma ISO/IEC 27032, consultado en julio de 2020, disponible en: https://www.iso27001security.com/html/27032.html

[iii] Cabe señalar que esta y otras ideas se retoman de mi Iniciativa con proyecto de Decreto por el que se adicionan las fracciones XIV y XV al artículo 5; una fracción VI al artículo 6; todos de la Ley de Seguridad Nacional, en materia de ciberseguridad. La Iniciativa la presenté en enero de 2020.

[iv] Consultado en julio de 2020, disponible en: https://www.elfinanciero.com.mx/economia/hackers-sustraen-400-mdp-de-bancos

[v] Consultado en julio de 2020, disponible en: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

[vi] Convenio sobre cibercriminalidad [Budapest, 23.XI. 2001], consultado en julio de 2020, disponible en: http://documentostics.com/documentos/convenio_cibercriminalidad.pdf

[vii] El 73% de las organizaciones en México han sufrido incidentes en la nube pública: estudio Sophos, consultado en julio 2020, disponible en: http://cio.com.mx/el-73-de-las-organizaciones-en-mexico-han-sufrido-incidentes-en-la-nube-publica-estudio-sophos/