PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE LA COMISIÓN PERMANENTE DEL HONORABLE CONGRESO DE LA UNIÓN EXHORTA RESPETUOSAMENTE AL EJECUTIVO FEDERAL Y A LAS 32 ENTIDADES FEDERATIVAS EN MATERIA DE CIBERSEGURIDAD Y ESTRATEGIA DIGITAL A CARGO DE LA DIPUTADA NÉLIDA IVONNE SABRINA DÍAZ TEJEDA, DEL GRUPO PARLAMENTARIO DEL PRI.

La que suscribe, diputada **Nélida Ivonne Sabrina Díaz Tejeda**, integrante del Grupo Parlamentario del Partido Revolucionario Institucional en la LXV Legislatura del Honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 6, numeral 1, fracción I, y 79, numeral 2, del Reglamento de la Cámara de Diputados; y 58 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, somete a consideración de esta Honorable asamblea la siguiente **Proposición con Punto de Acuerdo por el que la Comisión Permanente del honorable congreso de la unión exhorta respetuosamente al ejecutivo federal y a las 32 entidades federativas en materia de ciberseguridad y estrategia digital,** al tenor de la siguiente:

Exposición de Motivos

El hackeo masivo a la Secretaría de la Defensa Nacional (SEDENA) por parte del grupo “Guacamaya” en septiembre de 2022, así como otros eventos de similar magnitud ha mostrado el estado de vulnerabilidad en materia de ciberseguridad en el que se encuentra actualmente México.

A pesar de la inversión por parte de SEDENA de más de 340 millones de pesos en la creación de su Centro de Operaciones del Ciberespacio, parece ser que las políticas implementadas no han sido suficientemente eficientes y deja en claro que aún tenemos un largo camino que recorrer.[1]

Actualmente México se encuentra en el lugar 84 de 160 por debajo de países como Perú, Colombia y Jamaica de acuerdo con el Índice de Ciberseguridad Nacional (NCSI), siendo el país latinoamericano con mayor número de ataques cibernéticos, debido a esto SEDENA no es la primera institución gubernamental atacada, y no es el primer ataque grave del país. [2]

Es importante destacar que las principales estrategias con las que cuentan tanto el gobierno como la ciudadanía se centran en la prevención, acceso a la información y la consolidación de una cultura general de ciberseguridad. No obstante, esta materia se encuentra en permanente evolución y existe preocupación ante el aumento de

[1] Forbes. Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque, recuperado de: https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/
[2] NCSI. México, recuperado de: https://ncsi.ega.ee/country/mx/

riesgos, amenazas y ataques informáticos sofisticados, generalmente acompañados de nuevas formas y técnicas para aprovechar vulnerabilidades y en muchos casos aprovechándose del desconocimiento de las personas usuarias, permitiendo así el incremento de conductas delictivas a través de estos medios.

Para octubre de 2022 se habían registrado alrededor de 85 mil millones de intentos de ciberataques en México, un aumento del 40% en comparación con 2021. El director de Investigación de Telecomunicaciones de IDC: Worldwide Security Governance 2022 en México enfatizó: "cada vez más, las empresas están adoptando medidas o políticas de ciberseguridad para no ser víctimas de *ransomware*, *phishing* o cualquier intento de ciberataque a la infraestructura de las empresas, a los clientes internos y externos o a los socios comerciales", señalando también que la inversión hacía la mejora de la ciberseguridad aunque puede probar ser costosa, supera en beneficios la alternativa, tomando en consideración las pérdidas de negocio, costos legales, compensación de víctimas, desacreditación de marca, entre otros, que han sido reportado por empresas impactadas.[3]

Esta problemática también se exacerba ante una falta de recursos, financiamiento e inversión por parte del gobierno, que no ha logrado mantenerse al día con las actualizaciones necesarias para asegurar la protección de datos efectiva, así como el combate de ciberataques. Actualmente en el país se cuenta con expertos en ciberseguridad que no están siendo aprovechados eficientemente y esta falta de financiamiento e inversión, no les permite poner en práctica sus conocimientos.[4]

Uno de los métodos preferidos en México para estos ciberataques, es el "ransomware", un tipo de software que permite al atacante secuestrar datos que solamente podrán ser liberados al pago de una suma de dinero. En 2019, PEMEX fue la víctima de un ciberataque en el cual 180,000 archivos fueron secuestrados por 4.9 millones de dólares, convirtiéndolo en el segundo rescate más grande desde 2016, sin embargo, el rescate no fue pagado. De esta manera también en 2022 la Lotería Nacional y la Plataforma Nacional de Transparencia también fueron atacados.[5]

---

[3] IDC. México Registra Más De 85 Mil Millones De Intentos De Ciberataques En Lo Que Va Del 2022: IDC, recuperado de: https://www.idc.com/getdoc.jsp?containerId=prLA49766122#:~:text=M%C3%A9xico%20tiene%20el%20primer%20lugar,lugar%20con%206.3%20mil%20millones.

[4] Forbes. Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque, recuperado de: https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/

[5] SEGOB. Ransomware, recuperado de: https://www.gob.mx/gncertmx/articulos/ransomware#:~:text=Actualmente%2C%20los%20delincuentes%20utilizan%20t%C3%A9cnicas,para%20que%20la%20v%C3%ADctima%20entregue, Forbes. Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque, recuperado de: https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/, El Economista. El rescate por el hackeo a Pemex es el segundo mayor por ransomware, recuperado de: https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

Una de las fracciones más preocupantes de una ciberseguridad carente es la importancia que hoy en día representan los sistemas financieros transaccionales, los Sistemas de pago de Banxico (SPEI), manejan en un día 4.2 millones de transacciones, con un monto promedio de $1,100 pesos por persona, si de alguna manera debido a un ciberataque o una falla grave en el sistema por falta de ciberseguridad que causara su caída, Banxico se enfrenta a una pérdida aproximadamente de 147 millones de pesos cada hora.[6] Es imprescindible contar con políticas de ciberseguridad que permitan afrontar el aumento de estos ciberataques eficientemente.

Solo en 2021, los ataques por ransomware crecieron 600% en México, y seguirán creciendo junto con otros tipos de ataques cibernéticos, ya que actualmente existe una gran cantidad de softwares disponibles o puntos débiles donde se puede atacar, con los responsables encontrando cada vez maneras más sofisticadas para hacerlo.[7]

En este aspecto, nuestro país comenzó con la implementación de una Estrategia Nacional de Ciberseguridad, publicada en noviembre de 2017 y que define objetivos y ejes transversales, plasma los principios rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además señala el modelo de gobernanza para la implementación, seguimiento y evaluación de dicha Estrategia, no obstante presenta avances mínimos en su implementación.[8]

Adicionalmente, el Gobierno Federal creó la Estrategia Digital Nacional 2021-2024 que incluye entre otras disposiciones promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales que contempla la evaluación de seguridad en las instituciones para la detección de amenazas y mejorar la gestión de riesgos de seguridad de la información, así como proponer la adopción de acciones clave para fortalecer los mecanismos de seguridad de la información que prevengan riesgos y amenazas a la información e infraestructura institucional.[9]

---

[6] IDC. México Registra Más De 85 Mil Millones De Intentos De Ciberataques En Lo Que Va Del 2022: IDC, recuperado de: https://www.idc.com/getdoc.jsp?containerId=prLA49766122#:~:text=M%C3%A9xico%20tiene%20el%20primer%20lugar,lugar%20con%206.3%20mil%20millones.

[7] El Economista. El rescate por el hackeo a Pemex es el segundo mayor por ransomware, recuperado de: https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

[8] El Ceo. Austeridad y falta de estrategia de AMLO aumentan riesgos en ciberseguridad. 9 de febrero 2023. Recuperado de: https://elceo.com/tecnologia/austeridad-y-falta-de-estrategia-de-amlo-aumentan-riesgos-en-ciberseguridad/

[9] Gobierno de México. Estrategia Digital Nacional 2021-2024. Publicada en el D.O.F. el 06/09/2021. Recuperado de: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc

Ambas estrategias requieren implementarse no solo a nivel federal, pero replicarse a nivel local, en tanto el riesgo de vulnerabilidad informática en las entidades es aún mayor. Esto se ha visto en casos como el ocurrido a finales de 2022 donde la Secretaría de Finanzas de San Luis Potosí sufrió un ataque cibernético pese a que se logró contener la propagación del virus[10], esto demuestra el riesgo latente que existe para otras entidades.

Dada la relevancia que ocupa el tema en la actualidad, resulta fundamental que tanto sociedad y gobierno comprendamos el valor de la ciberseguridad como un habilitador para el desarrollo del potencial de la digitalización del país y una pieza clave para el desarrollo sostenible de México y el mundo y el gobierno de la República juega un papel fundamental para lograr este cometido pero también corresponde a los gobiernos estatales reforzar sus sistemas y alinearse con ambas estrategias nacionales.

Por lo anteriormente expuesto, se presenta el siguiente:

Punto de Acuerdo

PRIMERO. - La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente al Ejecutivo Federal para que informe a esta soberanía el estado que guarda la implementación de la Estrategia Nacional de Ciberseguridad y la Estrategia Digital Nacional.

SEGUNDO. - La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a las 32 entidades federativas a realizar las adecuaciones normativas, presupuestales y programáticas necesarias para garantizar la ciberseguridad y servicios digitales en sus gobiernos.

Atentamente

Dip. Nélida Ivonne Sabrina Díaz Tejeda

Dado en el salón de sesiones de la Comisión Permanente del H. Congreso de la Unión, a 22 de mayo de 2024.

[10] El Universal, San Luis Potosí. Hackean Secretaría de Finanzas de San Luis Potosí; suspenden servicios. 04/11/2022. Recuperado: https://sanluis.eluniversal.com.mx/cartera/sufre-hackeo-secretaria-de-finanzas-de-san-luis-potosi-suspenden-servicios