

PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE LA COMISIÓN PERMANENTE DEL HONORABLE CONGRESO DE LA UNIÓN EXHORTA RESPETUOSAMENTE AL PODER EJECUTIVO DEL ESTADO DE NUEVO LEÓN, A TRAVÉS DE LA SECRETARÍA DE SEGURIDAD PÚBLICA Y A LA POLICÍA CIBERNÉTICA DEL ESTADO, A IMPLEMENTAR DE MANERA URGENTE ESTRATEGIAS, ACCIONES Y MECANISMOS COORDINADOS PARA PREVENIR, ATENDER Y ERRADICAR LOS DELITOS CIBERNÉTICOS, ASÍ COMO A IMPLEMENTAR CAMPAÑAS PERMANENTES DE COMUNICACIÓN E INFORMACIÓN PARA DOTAR DE HERRAMIENTAS A LA POBLACIÓN A EFECTO DE MINIMIZAR EL ALTO IMPACTO DE ESTOS DELITOS EN LA ENTIDAD, PROCURANDO LA SEGURIDAD DE LAS Y LOS NEOLEONESES, A CARGO DE LAS DIPUTADAS Y DIPUTADOS DEL GRUPO PARLAMENTARIO DE MORENA.

Quienes suscriben, diputadas y diputados federales del Grupo Parlamentario de Morena en la LXV Legislatura de la Cámara de Diputados, con fundamento en lo dispuesto por los artículos 58 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, así como demás relativos y aplicables, sometemos a la consideración de esta Honorable Asamblea de la Comisión Permanente la siguiente Proposición con Punto de Acuerdo, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Las tecnologías informáticas que gozan de avances constantemente hacen más sencillas las transacciones, la conectividad, la interacción social a través de redes sociales, y, en general, facilitan el modo de vivir de las personas, poniendo de manifiesto la necesidad de la ciberseguridad, así como de autoridades que estén a la altura de poder implementarla, con el objeto de que socaven las agresiones virtuales y se prevenga la comisión de delitos cibernéticos.

De ahí que el avance tecnológico se aplique cada día más a la normalidad social, por lo que también surgen nuevos retos y riesgos a la seguridad ciudadana y a la seguridad gubernamental.

Con la integración de gran parte de los trámites privados y públicos, aplicaciones de comida, transporte y servicios bancarios, entre una infinidad de servicios digitalizados, se debe contar con programas de información permanente para la población y una autoridad a la altura que permitan evitar a la ciudadanía, los riesgos y situaciones que los hagan blancos fáciles de la ciberdelincuencia.

La operación de los criminales que usan los medios digitales como mecanismo para llegar a sus víctimas, resulta quirúrgica, dado que logran engañar a las y los neoleonenses con tácticas tales como la generación de páginas falsas de gobierno, en donde las personas proporcionan información personal pensando que accederán a apoyos, becas, programas sociales.

Un ejemplo de un fraude cibernético es la recepción de mensajes del “banco”, en donde le hacen creer a los usuarios que alguien está queriendo realizar transacciones y clonar sus datos bancarios; entonces, les indican que deben verificar su información a través de una aplicación, con la que les roban sus datos sensibles y dinero de su cuenta bancaria.

El sector financiero es uno de los más afectados por los delitos cibernéticos como el robo de identidad bancaria, la usurpación de identidad, los fraudes en compras electrónicas y el lavado de dinero a través de transacciones electrónicas, entre otros. Sin embargo, no es el único sector vulnerado por estos esquemas, pues existe la pornografía infantil, el abuso de menores, el acoso a través de medios digitales, el tráfico de personas y la corrupción de menores potenciada a través de herramientas cibernéticas.

Asimismo, las advertencias o amenazas generadas por medios digitales, como aquellas que van en contra del alumnado o algún plantel escolar, revelan que delitos de esta índole pueden infiltrar las aulas con holgada facilidad.

Si bien es una responsabilidad dual, donde el sector privado oferta servicios y productos por internet y medios digitales, mientras que el gobierno debe generar los esquemas necesarios para disminuir las prácticas delictivas en este rubro.

No debe dejarse de lado que las amenazas vinculadas al incremento del tráfico en internet, dado el confinamiento vivido recientemente a causa de la pandemia del SARS-COV-2, sólo logró exacerbar las estafas (phishing), el *malware* referido a *software* hostil, que potenció el *spyware* y el secuestro de información a personas y empresas (*ransomware*), accediendo a la información sensible de la ciudadanía.

Lamentablemente, el gobierno de Nuevo León no cuenta en la actualidad con instrumentos eficaces para que se acoten los delitos cibernéticos, ya que no han existido los ajustes requeridos para la nueva realidad tecnológica que se vive en el estado.

Muestra de lo anterior es que la frecuencia de delitos como el fraude, el robo de identidad y de datos personales, así como el acoso, ha crecido de manera exponencial en la entidad, siendo que de 2020 a 2021, el número de reportes de ciberdelitos aumentó en 56%. Así, en 2020, se dieron en total 5 mil 505 casos, mientras que en 2021, fueron 8 mil 616¹.

De acuerdo con la empresa de ciberseguridad Metabase Q, el ransomware es el ciberfraude que más se intensificó en 2021 en Nuevo León, con un aumento de 400 por ciento, siendo las pequeñas y medianas empresas (Pymes) las más afectadas². Lamentablemente, la prevención de fraudes e incidentes cibernéticos que ponen en riesgo a la población del estado, no ha sido prioridad del gobierno en turno que no ha implementado eficientemente campañas de información y asesoría.

Para el gobierno de Nuevo León, la protección de las infraestructuras públicas y privadas debe ser una prioridad, sobre todo las de aquellas consideradas por su importancia como estratégicas y críticas, al tiempo que debe cuidar a la ciudadanía de a pie a través de

¹ <https://www.milenio.com/politica/comunidad/en-nuevo-leon-aumentan-un-56-los-ciberdelitos>

² <https://www.elfinanciero.com.mx/monterrey/2022/05/16/alertan-por-nueva-amenaza-cibernetica-en-nuevo-leon/>

acciones coordinadamente implementadas para desarticular células *criminales que operan en la red*.

La Secretaría de Seguridad Pública del estado de Nuevo León cuenta con una policía cibernética que tiene la misión de prevenir y combatir los delitos en los que se utilicen medios electrónicos y tecnológicos, mediante el ciberpatrullaje en la web, el análisis de sistemas, ingeniería social, equipos informáticos y de telecomunicaciones³.

Esta unidad técnica, tiene la obligación de prevenir y combatir los delitos en los que se utilizan medios electrónicos y tecnológicos, mediante el análisis de sistemas, ingeniería social, equipos informáticos y de telecomunicaciones⁴, sin embargo, dado los resultados, su actuar no ha sido efectivo.

Derivado de lo anterior, el gobierno del estado de Nuevo León, encabezado por Samuel García Sepúlveda, debe generar estrategias y mecanismos coordinados y eficaces en contra de los delitos cibernéticos, que rindan resultados positivos, incentivando una regulación que no limite las comunicaciones privadas, pero procure y salvaguarde la seguridad de las y los neoleoneses. Asimismo, requiere de la aplicación efectiva de campañas permanentes de comunicación para dotar de herramientas a la población a efecto de minimizar el alto impacto de este tipo de delitos, dado que hoy por hoy, el gobierno estatal se ha visto rebasado.

La convergencia de las áreas de ciberseguridad del estado debe complementarse y fortalecerse con esfuerzos, recursos y visión de miras, establecer puntos de vinculación, mapeo de riesgos, coordinación analítica, investigación de fraudes, resguardo de equipo crítico, entre otros, para atender en forma integral amenazas, eliminar riesgos, y desarrollar habilidades institucionales en beneficio de las y los neoleoneses.

³ <https://www.nl.gob.mx/campanas/conoce-que-tipo-de-delitos-investiga-la-policia-cibernetica-y-denuncia#:~:text=Contacta%20a%20la%20Unidad%20de,se%20trata%20de%20un%20incidente>.

⁴ <https://www.posta.com.mx/nuevo-leon/general-nuevo-leon/nuevo-leon-cuenta-con-una-policia-cibernetica-lo-sabias/19867>

Por lo anteriormente expuesto, sometemos a consideración de esta Honorable Asamblea, el siguiente:

PUNTO DE ACUERDO

PRIMERO. La Comisión Permanente del Honorable Congreso de la Unión exhorta respetuosamente al Poder Ejecutivo del estado de Nuevo León, a través de la Secretaría de Seguridad Pública y la Policía Cibernética de la entidad, a implementar de manera urgente estrategias, acciones y mecanismos coordinados para prevenir, atender y erradicar los delitos cibernéticos cometidos en el estado, procurando la seguridad de las y los neoleoneses.

SEGUNDO. La Comisión Permanente del Honorable Congreso de la Unión exhorta respetuosamente al Poder Ejecutivo del estado de Nuevo León, a través de la Secretaría de Seguridad Pública y la Policía Cibernética del Estado a implementar campañas permanentes de comunicación e información para dotar de herramientas a la población a efecto de minimizar el alto impacto de los delitos cibernéticos en la entidad, en beneficio de las y los neoleoneses.

Dado en el Pleno de la Comisión Permanente, el 13 de junio de 2022.

