Dip. Santiago Creel Miranda
Presidente de la Mesa Directiva
de la Cámara de Diputados del
H. Congreso de la Unión
P r e s e n t e

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL, A CARGO DE LA DIPUTADA GINA GERARDINA CAMPUZANO GONZÁLEZ, DEL GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL

La que suscribe, diputada federal Gina Gerardina Campuzano González, y las y los diputados integrantes del Grupo Parlamentario del Partido Acción Nacional (PAN) en la LXV Legislatura de la Cámara de Diputados, en ejercicio de la facultad que me otorga el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como lo dispuesto en los artículos 6, 77 y 78 del Reglamento de la Cámara de Diputados, someto a consideración de esta soberanía, la iniciativa con proyecto de decreto por el que se reforman los artículos 211 bis 1; el artículo 211 bis 2; y el artículo 211 bis 3; todos del Código Penal Federal, al tenor de la siguiente:

Exposición de Motivos

En México, en cuestiones de ciberseguridad, nuestro país está por debajo de países como Kenya, Sri Lanka, Brasil, Panamá, Chile o Nigeria. De acuerdo con el National Cibersecurity Index 2022, el índice de seguridad cibernética de México es de 37.66 puntos sobre 100, lo que ubicó al país en la posición 84 de 160 a nivel mundial.[i]

Estas cifras alarman tanto a dependencias gubernamentales como a las empresas. De acuerdo, con el estudio “El estado de Ransomware 2022”, de Sophos, indicó que, de 200 organizaciones en México, 74% fue víctima de ransomware, pagando un promedio de 482,446 dólares. Solo en 2021, este tipo de ataque creció 600% en México. [ii]

Recordemos que en la década de los 90 del siglo pasado, la cantidad de computadoras y sistemas que dependían de su conexión a internet eran muy pocos, sobre todo en países como el nuestro. Sin embargo, en sólo 25 años, prácticamente todas las actividades esenciales del mundo de lo privado y de lo público dependen en buena medida de lo que ocurre en la red.[iii]

De acuerdo con el Informe Global de Riesgos 2022, del Foro Económico Mundial, los ataques cibernéticos están considerados como la quinta amenaza o riesgo más importante a nivel internacional. Según sus datos, hay al menos 100 intentos cada minuto, por vulnerar algún sistema informático en el planeta; pero lo peor es que la intensidad de la búsqueda, ataques y vulnerabilidades detectadas crecen exponencialmente todos los años.[iv]

Asimismo, de acuerdo con la empresa de seguridad informática ESET, dos de cada tres personas afirman estar preocupada por incidentes relacionados con malware; solo 10% de las personas que han sido encuestadas por la empresa protege a sus dispositivos móviles con alguna solución de seguridad; 60% de los usuarios de internet están preocupados por el robo de información. Al menos el 50% de las personas que fueron encuestadas en 2022 sufrió algún incidente de ciberseguridad y alrededor del 60% asegura que el presupuesto asignado a su seguridad informática no es el suficiente.[v]

Parece ser que, por lo que está ocurriendo en nuestro país, el Gobierno de la República se encuentra justamente en el último de los supuestos expresados por usuarios individuales de todo el mundo. Con la enorme diferencia de que lo que se encuentra en juego en este caso es nada menos que la seguridad del Estado mexicano, así como la protección de servicios críticos para la población.[vi]

Hay muchas áreas súper sensibles del gobierno que hoy se encuentran en la red. Por ejemplo, cabe preguntarse si existe suficiente seguridad informática en el conjunto de instituciones del Sector Salud (IMSS; ISSSTE, y la Secretaría de Salud), en el resguardo de los expedientes clínicos digitales de sus pacientes. Lo mismo ocurre con los datos de que dispone COMPRANET de todas las personas que prestan servicios o venden productos para el sector público. ¿O qué decir de la aeronáutica civil, cuyos radares, por ejemplo, podrían en algún omento ser hackeados?.[vii]

La lista de espacios de riesgos es altísima. Por ello preocupa enormemente el hackeo masivo filtrado por “Gucamaya”, respecto de varios “terabites” de información, nada menos que de la Secretaría de la Defensa Nacional. Ya había habido alertas sobre la debilidad en el desempeño y seguridad informática de este gobierno con la caída del ya mencionado COMPRANET; y ahora también, con lo que parece ser un nuevo hackeo a la Secretaría de Comunicaciones y Transportes del Gobierno de la República, donde se han suspendido servicios y trámites “hasta nuevo aviso”. [viii]

De acuerdo con datos de FortiGuard Labs, en los primeros seis meses de 2022 México enfrentó al menos 80 millones de intentos de ciber ataques; esto hace un promedio de 444 mil casos por día, o bien, 7,400 intentos de ciber ataques cada minuto. En ese sentido, la empresa IQSec asegura que México se encuentra poco preparado para enfrentar con éxito estas amenazas en el corto plazo y por ello urge a una mejor regulación, pero también al desarrollo de una cultura de mayor prevención que permita prevenir, mitigar y revertir los ataques informáticos que ocurren a diario.[ix]

Al respecto es importante pensar, por ejemplo, en la edad que tienen los equipos informáticos con los que trabaja nuestro gobierno. Porque de ello depende el tipo de software que se usa. En efecto, por lo que sabemos a través de las disposiciones presupuestarias y administrativas del Gobierno de la República, la compra, renta o renovación de equipos de cómputo es una de las áreas que han sufrido mayores recortes. Y si esto es así, a medida en que los equipos envejecen, no sólo se tienen menores capacidades de trabajo, sino que las

vulnerabilidades se incrementan de manera muy relevante pues, al tener software envejecido, las posibilidades de que sea hackeado se incrementan exponencialmente, y eso lo sabe incluso cualquier hacker novato.[x]

México contaba, en la extinta Policía Federal, con una sólida división de policía cibernética; pero con su paso a la Guardia Nacional, no se sabe bien a bien si sus capacidades se mantuvieron o incluso mejoraron; si el personal adscrito a esa división se protegió y se trasladó en buenas condiciones laborales, porque lo que sabían y saben, es sumamente delicado para la seguridad del Estado y su población. [xi]

Como puede verse, los frentes que se abren en este tema son inmensos; porque el uso intensivo del internet se aceleró tremendamente con la pandemia, con lo que ello implica, para bien, pero también en términos de riesgos y amenazas, sobre todo en ámbitos que entran en el ámbito de lo infame, como la explotación sexual infantil o la trata de personas. Y ante todo ello, urge una auténtica política de Estado en la materia. [xii]

Como legisladores debemos analizar, reformar y actualizar la Ley, para fortalecer y establecer mayores sanciones, que permitan prevenir, mitigar y revertir los ataques informáticos que ocurren a diario, para que el Estado mexicano pueda perseguir este tipo de actos en contra de sus instituciones, y brindar mayor seguridad informática para el Estado y su población.

Es por lo anterior que la presente Iniciativa propone que se reforme el artículo 211 bis 1, con el objeto de establecer que al que sin autorización vulnere, modifique, destruya, amenace o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de siete meses a tres años de prisión y de doscientos a cuatrocientos días multa.

Asimismo, se considera necesario reformar el artículo 211 bis 2, para establecer que el que sin autorización vulnere, modifique, destruya, amenace o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Por último, se propone reformar el artículo 211 bis 3, para establecer que al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente vulnere, modifique, amenace, destruya o provoque pérdida de información que contengan, se le impondrán de tres a nueve años de prisión y de trescientos a novecientos días multa.

En Acción Nacional como legisladores coincidimos en que conforme avanza la tecnología, también deben avanzar las estrategias de ciberseguridad y contar con un marco regulatorio sólido, que, de mayor protección y preservación de la información, evitando en lo posible o minimizando cualquier riesgo o amenaza a la integridad física de la población y de las instituciones.

Por las consideraciones expuestas, someto a consideración del Pleno de esta Soberanía, la Iniciativa con Proyecto de

DECRETO POR EL QUE SE REFORMAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL

ÚNICO. Se reforman los artículos 211 bis 1; el artículo 211 bis 2; y el artículo 211 bis 3; todos del Código Penal Federal, para quedar en los siguientes términos:

Artículo 211 bis 1.- Al que sin autorización **vulnere,** modifique, destruya, **amenace** o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de **siete** meses a **tres** años de prisión y de **doscientos** a **cuatrocientos** días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de **nueve meses** a **tres años** de prisión y de **ciento cincuenta** a **trescientos** días multa.

Artículo 211 bis 2.- Al que sin autorización **vulnere**, modifique, destruya, **amenace** o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **nueve** meses a **tres** años de prisión y de **trescientos** a **quinientos** días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de **cinco** a **doce** años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de **cinco** a **once** años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, **vulnere,** obstaculice, **amenace**, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente **vulnere**, modifique, **amenace**, destruya o provoque pérdida de información que contengan, se le impondrán de **tres** a **nueve** años de prisión y de trescientos a novecientos días multa.

Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de

dos a **cinco** años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de **cinco** a **doce** años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

TRANSITORIOS

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

Palacio Legislativo de San Lázaro, a 01 de febrero de 2023.

DIPUTADA GINA GERARDINA CAMPUZANO GONZÁLEZ
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÒN NACIONAL

[i] Ginger Jabbour, México sin antivirus: hay falta de inversión en ciberseguridad, Tecnología, Expansión, consultado el 22 de noviembre de 2022 en https://expansion.mx/tecnologia/2022/08/18/ciberseguridad-en-mexico-falta-de-inversion#:~:text=En%20cuestiones%20de%20ciberseguridad%2C%20M%C3%A9xico,de%20160%20a%20nivel%20mundial.
[ii] Ibídem.
[iii] Saúl Arellano, Investigador del PUED-UNAM, La seguridad informática no es un juego, México Social La Cuestión Social en México, consultado por última vez el 21 de noviembre de 2022 en https://www.mexicosocial.org/seguridad-informatica/
[iv] Ibídem.
[v] Ibídem.
[vi] Saúl Arellano, Investigador del PUED-UNAM, La seguridad informática no es un juego, México Social La Cuestión Social en México, consultado por última vez el 21 de noviembre de 2022 en https://www.mexicosocial.org/seguridad-informatica/
[vii] Ibídem.
[viii] Ibídem.
[ix] Saúl Arellano, Investigador del PUED-UNAM, La seguridad informática no es un juego, México Social La Cuestión Social en México, consultado por última vez el 21 de noviembre de 2022 en https://www.mexicosocial.org/seguridad-informatica/
[x] Ibídem.
[xi] Ibídem.
[xii] Saúl Arellano, Investigador del PUED-UNAM, La seguridad informática no es un juego, México Social La Cuestión Social en México, consultado por última vez el 21 de noviembre de 2022 en https://www.mexicosocial.org/seguridad-informatica/