PROPOSICIÓN CON PUNTO DE ACUERDO, PARA EXHORTAR A LA SHCP A IMPLANTAR MEDIDAS EFICACES DE PREVENCIÓN, CONTROL Y SOLUCIÓN DE ATAQUES INFORMÁTICOS DEL GOBIERNO FEDERAL ANTE UN ESCENARIO DE CONSTANTES VULNERACIONES A INSTITUCIONES PÚBLICAS Y LA DEBILIDAD DERIVADA DE LA AUSENCIA DE UN PLAN NACIONAL EN LA MATERIA, A CARGO DEL DIPUTADO JOSÉ SALVADOR ROSAS QUINTANILLA, DEL GRUPO PARLAMENTARIO DEL PAN

El que suscrito, **José Salvador Rosas Quintanilla** , diputado federal del Grupo Parlamentario de Acción Nacional de la LXIV Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto por el artículo 6, numeral 1, fracción I, y 79 del Reglamento de la Cámara de Diputados, someto a consideración de esta asamblea la presente **proposición con punto de acuerdo por el que se exhorta a Arturo Herrera Gutiérrez, titular de Hacienda y Crédito Público, para la creación de una partida especial para el ejercicio fiscal 2020 que cumpla con el objetivo de no desatender las tareas de ciberseguridad del gobierno federal ante un escenario de constantes vulneraciones a instituciones públicas y la vulnerabilidad derivada de la ausencia de un plan nacional en la materia** , al tenor de las siguientes

Consideraciones

Los intentos de vulneración a la seguridad nacional se han tornado en una actividad constante por parte de diversos grupos delictivos, nacionales y extranjeros, que pasan por encima de la ciudadanía ante la expectativa de generar ganancias a cualquier costo. Al interior de nuestro territorio, el crimen organizado ha logrado sembrar el terror en localidades de diferentes regiones del país mediante su operación en actividades como el secuestro o el narcotráfico, expandiendo sus redes de reclutamiento y mermando el impacto positivo que las políticas gubernamentales pretenden obtener, especialmente en poblaciones vulnerables, las principales víctimas de esta clase de agrupaciones.

En paralelo al aumento de la violencia y las actividades criminales en el país, la adopción de las tecnologías de la información, como la internet, abrieron un mundo de posibilidades a la ciudadanía, las empresas y los gobiernos del mundo, al facilitar muchas de sus tareas mediante una red de comunicación remota, que puede ser actualizada en tiempo real, no demanda conocimientos técnicos complicados y puede ser utilizada desde dispositivos portátiles, lo que le da muchísimas ventajas respecto a otros medios, como la televisión o la radio.

Por desgracia, esta ampliación del "abanico de posibilidades" que las tecnologías nuevas siempre generan, también aumenta sus potenciales efectos negativos derivados de su empleo, como lo ha sido el uso de las frecuencias de radio por parte del narcotráfico o de las antenas de telecomunicaciones para la realización de sus respectivas actividades delictivas. Igualmente, la ciudadanía, con el paso del tiempo, se ha vuelto mucho más dependiente de estas tecnologías, donde cada aspecto de su vida diaria, como el manejo de su cuenta bancaria, la realización de trámites burocráticos y hasta el acceso a documentos de identificación personal, han sido digitalizados y almacenados en algún dispositivo conectado a la red, lo que vuelve ese contenido (data) muy atractivo para empresas y gobiernos, aunque ellos no sean los únicos interesados.

Con la intromisión a la privacidad que caracteriza a herramientas de esta clase, la delincuencia ha encontrado un nicho enorme a través de su forma digital, donde el robo sigue siendo una de las actividades predilectas entre los cibercriminales. Al año, los ataques perpetuados por el cibercrimen generan una pérdida alrededor de los 8 mil millones de dólares,[1] ante un escenario en el que el gobierno mexicano carece de un organismo especializado en labores de ciberseguridad. La falta de interés y la "austeridad republicana", en sus consecuencias no buscadas, han creado un panorama desfasado para las necesidades de seguridad nacional, al omitir la relevancia de la ciberseguridad respecto a amenazas internas y externas. Para septiembre de 2019, de acorde a información provista por *El Universal* , se estimaba que en lo que iba de la administración federal, se reportaron 45 millon 9 mil 188 intentos de

intervención,[2] cantidad que coloca a México como el segundo país con mayor cantidad de ciberataques entre los países latinoamericanos,[3] sólo detrás de Brasil.[4]

Al llevarlo al plano del peso de estos ciberataques, la ciudadanía es el principal objetivo, aunque hay ejemplos sumamente graves en la materia respecto a la seguridad digital de instituciones gubernamentales, con pasajes decepcionantes como la intervención al Sistema de Pagos Electrónicos Interbancarios del Banco de México (SPEI) en abril de 2018,[5] la filtración de información confidencial de la embajada de México en Guatemala en abril de 2019[6] y el reciente ataque que Petróleos Mexicanos sufrió en noviembre de 2019,[7] donde se solicitó la cantidad de 565 bitcoins (5 millones de dólares) para poder liberar los equipos secuestrados por ciberdelincuentes.

La razón de dichas vulneraciones están asociadas a la falta de mecanismos serios y eficientes de ciberseguridad, donde la falta de una agenda nacional integral en la materia es una de las principales casusa de ello, al igual que uno organismo especializado para el cumplimiento de ésta función. La existencia de Equipos de Respuesta ante Emergencias Informáticas (CERT),[8] como el de la UNAM o la Policía Federal,[9] ya no son suficientes para la realización de la labor, donde esfuerzos desarticulados de los sectores público y privado no devendrán en resultados consistentes en la materia. Ante un escenario de amenazas digitales de origen global, donde la procedencia de los intentos de intervención han provenido de países tan variados como Rusia, China, Croacia, India, Cuba,[10] muestran que nuestra estrategia debe de ser implementada de la manera más pronta posible, donde no podemos presentar esquicio alguno de rezago con los métodos, medidas y herramientas usadas por países potencia en el ramo, ya que la ofensiva de la delincuencia será tan buena como la mejor invención disponible o desarrollable, donde las desigualdades en el acceso y uso de estas tecnologías podrían dejar vulnerable a México.

Sobre esto, la necesidad de contar con los recursos necesarios para cumplir con labores de ciberseguridad resulta indispensable, los cuales hoy en día son limitados ante una postura de eficiencia y austeridad en las actividades gubernamentales, por lo que garantizar la salvaguarda de los fondos disponibles y la operación adecuada de cada una de estas instituciones es prioritario, lo que genera un ambiente de codependencia entre una lógica de austeridad y la protección de los fondos planeados. Así, demandar la existencia de un monto dedicado exclusivamente a labores de ciberseguridad, requiere de que ésta sea el presupuesto suficiente para gestar y consolidar un trabajo serio en la materia, el cual debe de ser considerado en el ejercicio fiscal del año 2020, donde la Secretaría de Hacienda y Crédito Público debe de comprometerse para asignar la cantidad indispensable para garantizar las funciones, donde la exposición de una justificación, más allá de la previamente realizada, parece trivial ante la obviedad del problema y los muchos problemas que hoy en día estamos travesando ante la constante vulneración de nuestra seguridad por parte actores públicos y privados que sacan ventaja de estas tecnologías con total impunidad.

Por ello, presento ante esta honorable asamblea, la siguiente proposición con:

Punto de Acuerdo

Único. La honorable Cámara de Diputados exhorta a Arturo Herrera Gutiérrez, titular de Hacienda y Crédito Público, para que implemente medidas eficientes y eficaces de prevención, control y solución de ataques informáticos del gobierno federal ante un escenario de constantes vulneraciones a instituciones públicas y la vulnerabilidad derivada de la ausencia de un plan nacional en la materia.

Notas

1 Itzel Castañares. (2019). Ciberataques cuestan alrededor de 8 mil mdd a México, 2 de Diciembre de 2019, de El Financiero.Sitioweb:https://www.elfinanciero.com.mx/tech/ciberataques-cuestan-alrededor-de-8-mil-mdd-a-mexico

2 Pedro Villa y Caña. (2019). Hackers acechan información del Estado; van 45 millones de intentos, 2 de Diciembre de 2019, de El Universal. Sitio web:

https://www.eluniversal.com.mx/nacion/hackers-acechan-in formacion-del-estado-van-45-millones-de-intentos

3 Karen Julibeth. (2019). México, de los más vulnerables a ciberataques por falta de cultura e inversión, 2 de Diciembre de 2019, de Milenio. Sitio web: https://www.milenio.com/negocios/mexico-uno-de-los-paises-mas-vulnerabl es-a-ciberataques-en-al.com.mx/nacion/hackers-acechan-informacion-del-e stado-van-45-millones-de-intentos

4 Ídem

5 Cristóbal Martínez Riojas. (2018). Caso SPEI: la cronología del hackeo al sistema financiero mexicano, 2 de Diciembre de 2019, de Expansión. Sitio web:

https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano

6 Redacción. (2019). Hackea embajada de México y publica datos de pasaportes en Twitter, 2 de Diciembre de 2019, de Milenio. Sitio web: https://www.milenio.com/tecnologia/hackea-embajada-mexico-publica-datos-pasaportes-twitter

7 Redacción de Reuters. (2019). "Plantas operan, pozos trabajan"; mexicana Pemex no pagará a hackers: secretaria Energía, 2 de Diciembre de 2019, de Reuters. Sitio web: https://mx.reuters.com/article/petroleo-mexico-hackers-idMXL2N27T1EL

8 Rodrigo Riquelme. (2018). ¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?, 2 de Diciembre de 2019, de El Economista. Sitio web: https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuest a-ante-Emergencias-Informaticas-CERT-20180122-0009.html

9 Ídem

10 Pedro Villa y Caña. (2019). Hackers acechan información del Estado; van 45 millones de intentos, 2 de Diciembre de 2019, de El Universal. Sitio web: https://www.eluniversal.com.mx/nacion/hackers-acechan-informacion-del-estado-van-45-millones-de-intentos

Dado en el Palacio Legislativo de San Lázaro, a 11 de febrero de 2020.

Diputado José Salvador Rosas Quintanilla (rúbrica)