Proposición con Punto de Acuerdo por el que se exhorta a la Secretaría de Seguridad y Protección Ciudadana, para que implemente acciones de protección y prevención contra los delitos cibernéticos relacionados con COVID-19, así como estrategias de combate eficientes.

Quien suscribe, **Ivonne Liliana Álvarez García,** Diputada Federal integrante del Grupo Parlamentario del Partido Revolucionario Institucional de la LXIV Legislatura, con fundamento en lo dispuesto en los artículos 78, fracción III, de la Constitución Política de los Estados Unidos Mexicanos y 58 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someto a consideración de esta Honorable Asamblea, la siguiente proposición con Punto de Acuerdo, al tenor de la siguiente:

Exposición de motivos

La pandemia por COVID-19 ha obligado a millones de personas de todo el mundo a resguardarse en sus hogares para evitar mayores tasas de contagio y que el virus se salga de control. Hemos presenciado cómo la gran mayoría de las ciudades del orbe han quedado prácticamente deshabitadas por meses enteros y esta situación extraordinaria también ha provocado que algunos delitos también disminuyan. Sin embargo, hay algunos delitos que, por su naturaleza, se han incrementado aprovechando la crisis sanitaria, entre estos se encuentran los de tipo cibernético.

Para la Organización Internacional de Policía Criminal (INTERPOL), el concepto ciberdelincuencia se refiere a delitos contra computadoras y sistemas de

información, con el objetivo de lograr acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo.[1]

La ciberdelincuencia surge a raíz del uso expandido de las nuevas tecnologías de la información y los ataques pueden realizarse contra individuos, empresas e incluso gobiernos. Delitos como el robo, el fraude y el tráfico ilegal en sus diferentes modalidades ahora se benefician de los medios electrónicos para maximizar sus beneficios en un mundo cada vez más interconectado por el ciberespacio.

De acuerdo con el Secretario General de la INTERPOL, Jürgen Stock, el crimen organizado ha aprovechado la situación de pandemia para aumentar sus ganancias. Se ha detectado un incremento sustantivo en el tráfico y venta ilícita de medicamentos apócrifos, falsas vacunas o productos que prometen curar o prevenir el COVID-19, [2] así como el fraude y robo cibernético, lo que pone en riesgo la salud, la vida y el patrimonio de millones de personas en todo el mundo.[3]

El *phishing*, *Vishing y SMShing,* son métodos de fraude y extorsión en los que se envían correos electrónicos, llamadas telefónicas o mensajes de texto falsos a determinadas personas pretendiendo ser una fuente legítima, como una institución bancaria o gubernamental, un sitio comercial en línea, una empresa e incluso organizaciones civiles, con el objetivo de inducir a la persona a revelar información personal y financiera.[4]

[1] Ciberdelincuencia, INTERPOL, en: https://www.interpol.int/es/Delitos/Ciberdelincuencia
[2] COVID-19: The global threat of fake medicines, INTERPOL, en: file:///C:/Users/ivank/Downloads/COVID-19-The%20Global%20Threat%20of%20Fake%20Medecines.pdf
[3] Campaign Will highlight top threats and offer advice to #WashYourCyberHands, INTERPOL, en: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats
[4]

El *ramsomware*, es otra de las herramientas implementadas por la ciberdelincuencia, con el uso de un programa se toma como rehenes cibernéticos a instituciones como hospitales, servicios médicos y farmacéuticas, impidiendo el acceso a sus activos digitales o archivos hasta que se pague un rescate monetario.

La Organización Mundial de la Salud (OMS), por ejemplo, se vio obligada a colocar una alerta en su página institucional debido a la existencia de una nueva forma de estafa tipo *phishing*, donde los hackers envían a cuentas de correo electrónico de todo el mundo información falsa y alertas sanitarias haciéndose pasar por dicho organismo, con el objetivo de recolectar la información personal y las contraseñas de las personas.[5]

La INTERPOL también emitió una advertencia en marzo pasado sobre las estafas y fraudes financieros asociados con el COVID-19, entre los que se encuentran la compra de equipo de protección personal defectuoso, estafas telefónicas y en línea que exigen el pago para la atención de algún pariente hospitalizado y correos electrónicos de *phishing* como el identificado por la OMS.

Ese mismo mes, la Oficina de las Naciones Unidas contra las Drogas y el Crimen (UNODC), advirtió sobre correos electrónicos de *phishing* que contienen virus *malware* incrustados en aplicaciones, direcciones electrónicas o documentos que vulneran los equipos para acceder a información personal y financiera a través de los dispositivos móviles de las personas.

[5] COVID-19 and crime. A response develops at the UN, Global Initiative, en: https://globalinitiative.net/wp-content/uploads/2020/06/Covid-19-and-crime-A-response-develops-at-the-UN.pdf

Pero los delitos cibernéticos no son los únicos que se han incrementado con la crisis por COVID-19, también la propagación de desinformación o noticias falsas (*fake news*) han aumentado centrándose en el tema de la pandemia teniendo efectos negativos en la sociedad. La divulgación de teorías de la conspiración e información falsa, por ejemplo, ha motivado ataques contra el personal de salud, contra instituciones gubernamentales y la negación de la existencia del coronavirus. ´

En nuestro país hemos sido testigos de las consecuencias que pueden tener las *fake news*, hospitales violentados, clínicas quemadas, personal médico agredido, caos y saqueos, etc. La desinformación se propaga principalmente a través de las redes sociales por lo que es necesario implementar campañas de combate contra la desinformación utilizando estas mismas redes para ofrecer información verídica y oportuna.

Dado el grado de conectividad digital que existe a nivel global en la actualidad, la ciberdelincuencia no conoce fronteras físicas ni virtuales. Millones de personas, gobiernos, instituciones y organizaciones están siendo afectadas actualmente por este delito, por lo que se hace necesario tomar acciones de prevención y protección contra delitos cibernéticos a nivel nacional, así como estrategias de combate a este problema.

Por lo anteriormente expuesto, someto a la consideración de esta Soberanía la siguiente Proposición con:

PUNTO DE ACUERDO

ÚNICO. La Comisión Permanente del H. Congreso de la Unión exhorta a la Secretaría de Seguridad y Protección Ciudadana, para que implemente acciones de protección y prevención contra los delitos cibernéticos relacionados con COVID-19, así como estrategias de combate eficientes.

Dado en el salón de sesiones del Palacio Legislativo de San Lázaro, sede de la Cámara de Diputados del H. Congreso de la Unión, al día 28 de junio del año 2020.

ATENTAMENTE