**HONORABLE ASAMBLEA**

A la Comisión de Relaciones Exteriores de la LXIV Legislatura de la Cámara de Diputados le fue turnada, para su estudio y dictamen, la Proposición con Punto de Acuerdo, por el que se exhorta a la Secretaría de Relaciones Exteriores a promover, en el seno de la Comunidad de Estados Latinoamericanos y Caribeños, los acuerdos diplomáticos apropiados para la elaboración y firma de un Convenio Latinoamericano de Ciberseguridad.

La Comisión de Relaciones Exteriores, con fundamento en lo dispuesto por los artículos 39 y 45, numeral 6, incisos e) y f), de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; 80, numeral 1, fracción VI; 82, numeral 1, y 85 del Reglamento de la Cámara de Diputados, y habiendo analizado el contenido de la proposición con punto de Acuerdo, somete a consideración de esta Honorable Asamblea el presente dictamen, al tenor de lo siguiente:

# ANTECEDENTES

1. Con fecha 23 de febrero de 2021, la Diputada María Eugenia Hernández Pérez, integrante del Grupo Parlamentario de Morena, presentó la Proposición con Punto de Acuerdo que exhorta a la Secretaría de Relaciones Exteriores (S.R.E.), a promover en el seno de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), los acuerdos diplomáticos apropiados para la elaboración y firma de un Convenio Latinoamericano de Ciberseguridad.
2. En la misma fecha, la Proposición con Punto de acuerdo fue turnada para su estudio y dictamen a la Comisión de Relaciones Exteriores.

**CONTENIDO DE LA PROPOSICIÓN**

La Diputada expone textualmente en sus consideraciones lo siguiente:

*“Primera. – Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe.*

*El estudio Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe1 pone en evidencia que la región de América Latina y el Caribe aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio. Únicamente 7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica, y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT, según sus siglas en inglés. Esto limita la capacidad de identificar ataques y responder oportunamente a los mismos.*

*Identificar un peligro cibernético es tan sólo el primer paso. Tomar medidas contra las amenazas y crímenes del ciberespacio es un reto aún mayor para nuestros países. En 22 de los países analizados se considera que hay pocas capacidades para investigar los delitos que se cometen en el ciberespacio. Más aún, que dichos delitos resulten en juicio es todavía un reto mayor.*

*El reciente reporte de la Organización de los Estados Americanos (OEA) evalúa en 5 dimensiones los esfuerzos en los Estados Americanos por atender el fenómeno de la ciberseguridad las cuales son:*

*1. Política y Estrategia de Seguridad Cibernética*

*2. Cultura Cibernética y Sociedad*

*3. Formación, Capacitación y Habilidades de Seguridad Cibernética*

*4. Marcos Legales y Regulatorios*

*5. Estándares, Organizaciones y Tecnologías*

*Al respecto, es importante señalar que México, en la Dimensión 4 (Marcos Legales y Regulatorios), en la subdimension: Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético ha sido evaluado con 2 puntos de 5 donde 5 es la calificación más alta, y donde 2 es una calificación baja, como se ilustra en la siguiente imagen:*

**

*Dicho grafico nos muestra que México requiere mejorar sus instrumentos legales de cooperación formal para atender el fenómeno de la ciberseguridad.*

*Segunda. - Cooperación Internacional como Política Exterior.*

*Hay más de 4,000 millones de personas en el mundo conectadas a internet y esa cifra aumenta diariamente. Ante este escenario, en el que cada día son más necesarias las tecnologías emergentes para realizar cualquier actividad cotidiana, la ciberseguridad se convierte en algo imprescindible para poder garantizar la seguridad de las Tecnologías de la Información y de la Comunicación. Cuando se produce un ciberataque no suele afectar a un solo país y aunque así suceda, en muchas ocasiones el ataque es realizado desde otro lugar del mundo.*

*Parte del problema se inicia muchas veces en la propia ley: en un tercio de los países en América no existe un marco legal sobre los delitos informáticos y únicamente 5 países de esta región se han adherido al Convenio Sobre Ciberdelincuencia, mejor conocido como Convenio de Budapest, que facilita la cooperación internacional en la lucha contra el crimen informático. Frente a un delito que no conoce fronteras, trabajar de la mano con otros países es un factor indispensable para el éxito, ante esta situación se han establecido convenios y acuerdos internacionales para hacer frente a los ciberataques, el ciberterrorismo y la ciberdelincuencia de manera coordinada.*

*Algunos de estos Acuerdos y Convenios2 de colaboración más relevantes son:*

*• Acuerdo de Colaboración UE y OTAN – junio de 2018*

*• Paris Call for Trust and Security in CyberSpace – noviembre de 2018.*

*• Cybersecurity Tech Accord – abril de 2018.*

*• Convenio sobre Ciberdelincuencia (Convenio de Budapest) – 2001.*

*Todos estos acuerdos de cooperación internacional en su mayoría han sido firmados en y por países de Europa, sin embargo, en América Latina no existe aún algún instrumento regional de este tipo que le ayude a los países de esta región a hacer frente a los ciberataques, el ciberterrorismo y la ciberdelincuencia de manera coordinada.*

*Tercera. - Presidencia a tempore del CELAC por parte de México.*

*Según su página3 , la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) es un mecanismo intergubernamental para el diálogo y el acuerdo político, que incluye permanentemente treinta y tres países de América Latina y el Caribe. Es un foro regional que reúne a toda América Latina y el Caribe. La CELAC aspira a ser una voz única de toma de decisiones en el ámbito político y la cooperación en apoyo de los programas de integración regional. Fue creada con el compromiso de avanzar en el proceso gradual de integración regional, unidad y equilibrio cuidadoso de la diversidad política, económica, social y cultural de América Latina y el Caribe de 650 millones de personas. Desde su lanzamiento en diciembre de 2011, la CELAC ha ayudado a profundizar el diálogo respetuoso entre todos los países de la región en áreas tales como desarrollo social, educación, desarme nuclear, agricultura familiar, cultura, finanzas, energía y medio ambiente.*

*A partir del 7 de enero del 2020, México cuenta con la Presidencia pro tempore del mecanismo intergubernamental, y el pasado jueves 24 de septiembre del 20204 , los representantes de las 33 naciones miembros de la Comunidad de Estados Latinoamericanos y Caribeños acordaron por unanimidad reelegir a México en la presidencia pro tempore de esa instancia para el periodo 2021-2022. Por ello, es importante considerar que el hecho de tener la Presidencia de la CELAC y formar parte del Consejo de Seguridad de las Naciones Unidas este 2021, constituyen dos factores estratégicos para que México pueda proponer la creación de un Convenio Latinoamericano de Ciberseguridad.*

*Cuarta. - Plan de Trabajo 2020 de la CELAC*

*El gobierno mexicano en la Cumbre del CELAC en enero del 2021 presento su Plan de trabajo para 20215 . La propuesta de Plan de Trabajo, aceptada por la Cumbre, propone el desarrollo de 14 proyectos con la intención de obtener 14 resultados concretos. Esto implica plantearse metas concretas y bien definidas para fomentar el intercambio y articulación políticos entre los países miembros del CELAC. El Plan tiene teóricamente una amplia perspectiva, los proyectos propuestos buscan armonizar al sector público en la región atendiendo ejes muy particulares como: corrupción, gestión sustentable, ciencia tecnología e innovación, cooperación internacional entre otros. Sin embargo, temas como la inclusión del sector privado en dichos proyectos, los efectos del cambio tecnológico exponencial, o las capacidades en materia de ciberseguridad son escasamente mencionados.*

*Partiendo de las cifras del National Cybersecurity Index6 de la E-Governance Academy (Institución líder en la evaluación de capacidades de ciberseguridad), y el Global Cybersecurity Index, de la Unión Internacional de Telecomunicaciones, es evidente que la región Latinoamérica aún se encuentra por detrás de Europa, América del Norte y Asia en cuanto a la preparación a atender el fenómeno de la ciberseguridad. Latinoamérica está enfocando sus esfuerzos en la seguridad cibernética e introduciéndola en su agenda como un tema principal. Sin embargo, tales esfuerzos han sido desarticulados7 , por lo que persiste un desequilibrio en la situación de cada país, tanto en términos de desarrollo como de implementación de políticas de seguridad cibernética.*

*En este contexto, es evidente que existen condiciones para promover que se incluya en la agenda de LA CELAC, la celebración de un Convenio Latinoamericano de Ciberseguridad . Tal proyecto es definitivamente pertinente y se convertiría en un mecanismo regional que unificaría criterios y acciones, ejes temáticos y líneas de acción concretas, para enfrentar el fenómeno de la ciberseguridad en América Latina.*

*Quinta. – Características generales del Convenio Latinoamericano de Ciberseguridad*

*El proyecto de Convenio Latinoamericano de Ciberseguridad, tendrá que incorporar los temas cruciales en materia de definiciones, identificación y tipificación de los delitos informáticos, disposiciones comunes, estrategias de cooperación regional e internacional, combate a las organizaciones cibercriminales trasnacionales, derechos humanos y derechos A.R.C.O.,*

*Del mismo modo, ese Convenio deberán abordar el tema de la privacidad de la información y promover la soberanía de cada Estado y de la región en general. El gobierno de México, a través de la Secretaría de Relaciones Exteriores, puede promover la elaboración conjunta y firma del Convenio Latinoamericano de Ciberseguridad, con base en el liderazgo renovado de nuestro país en la región Latinoamérica y el Caribe.*

*La estructura y el contenido específico de esta propuesta de Convenio Latinoamericano de Ciberseguridad, deberá definirse a partir de una metodología de trabajo diseñada por la propia CELAC, con base en las particularidades del fenómeno de la ciberdelincuencia en la región latinoamericana. En todo caso es importante que, a manera de orientación y referencia se considere la experiencia y el trabajo realizado en otras regiones del mundo, que se expresa en los Acuerdos y Convenios antes citados:*

*• Acuerdo de Colaboración UE y OTAN – junio de 2018*

*• Paris Call for Trust and Security in CyberSpace – noviembre de 2018.*

*• Cybersecurity Tech Accord – abril de 2018.*

*• Convenio sobre Ciberdelincuencia (Convenio de Budapest) – 2001.*

*En definitiva, la elaboración multilateral de un Convenio Latinoamericano de Ciberseguridad, auspiciado por la CELAC, encuentra buenas posibilidades de realización. Tanto la necesidad imperiosa de contar con in Instrumento regional para hacer frente al desafío de la ciberdelincuencia, como la posición de liderazgo de México, hacen viable que prospere la propuesta en este tenor.*

*Con base en lo anteriormente expuesto, someto a la consideración de esta soberanía, la siguiente Proposición con*

*Punto de Acuerdo*

*Único. – La Cámara de Diputados del Congreso de la Unión exhorta respetuosamente a la Secretaria de Relaciones Exteriores, a promover en el seno de la Comunidad de Estados Latinoamericanos y Caribeños, los acuerdos diplomáticos apropiados para la elaboración y firma de un Convenio Latinoamericano de Ciberseguridad”.*

Una vez establecidos los antecedentes y el objetivo de la proposición, los integrantes de la Comisión de Relaciones Exteriores que suscriben el presente dictamen, exponen las siguientes:

**CONSIDERACIONES**

**PRIMERA.** El aumento de la conectividad a Internet hace que un número cada vez mayor de personas estén conectadas en un espacio en gran parte público y transnacional, y proporciona una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación en maneras en que nunca hubiéramos podido imaginar hace muy poco tiempo.

Esto es particularmente cierto en América Latina y el Caribe, donde más de la mitad de nuestra población ya está en línea y la tasa de crecimiento de usuarios de Internet se encuentra entre las más altas del mundo.

No se puede ignorar que la creciente conectividad y dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente la exposición al riesgo a una gran cantidad de actividades y actores relacionados con la delincuencia y seguridad.

Como lo ha señalado Ulrick Beck, vivimos en una sociedad del riesgo. La globalización y las nuevas tecnologías, nos proporcionan satisfactores y nuevas herramientas, pero también nos exponen a mayores amenazas globales.

Los incidentes y ataques cibernéticos, en particular los que se realizan con intención criminal, están aumentando en frecuencia y sofisticación. Las agencias gubernamentales y las empresas han llegado a reconocer la necesidad de tener fuertes marcos, medidas y capacidades de seguridad cibernética, así como contar imperiosamente con cooperación e intercambio de información.

En la actualidad se entiende que el delito cibernético no reconoce fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas. De hecho, está avanzando de manera importante.

Solo por poner un ejemplo de la región latinoamericana, México está dentro de los diez países que más ataques cibernéticos recibe a nivel mundial.

**SEGUNDA.** Para la Organización de los Estados Americanos (OEA) el **costo de los incidentes** **ocasionados por el cibercrimen** a nivel mundial, pasará de 3 mil millones de dólares en 2015, a 6 mil mdd, en 2021. La ciberdelincuencia ocasiona pérdidas de 575 millones de dólares al año, lo que representa un 0.5% del PIB mundial. En América Latina los daños por este concepto equivalen a 90 millones de dólares anuales.

El dato más revelador es que los ciberataques a escala global, equivalentes a 3 mil millones de dólares anuales, han rebasado los ingresos del narcotráfico, según Adrián Acosta, oficial de Cibercrimen en la Oficina Regional de Interpol para América del Sur. Sin embargo, la ciberseguridad no recibe tanta atención por parte de autoridades y políticas públicas como sí ocurre con el trasiego de enervantes.

En México, 33 millones de consumidores fueron víctimas de delitos cibernéticos y las pérdidas ascendieron a 7.7 millones de dólares (*Norton Cyber Security Insights* 2017). Los usuarios de *smartphones* y *laptops* son los más propensos a ser víctimas de ciberdelitos. Esta situación se ha agudizado durante la emergencia sanitaria por Covid-19, debido a necesidad y, por lo tanto, a la vulnerabilidad del trabajo remoto.

Según la *Global State of Information Security Survey* 2018 de *PwC*, México es el segundo país más ciberatacado de América Latina, sólo detrás de Brasil. Las afectaciones pueden incluir interrupción del negocio, pérdida de información, de ingresos y daños a la infraestructura tecnológica.

La economía y la ubicación geoestratégica de México son un objetivo atractivo para las actividades cibernéticas ilícitas. Por un lado, está disfrutando de una considerable inversión extranjera directa y un sólido crecimiento del PIB y, por otro lado, sigue siendo relativamente vulnerable en ciberseguridad y ciberseguridad[[1]](#footnote-1).

**TERCERA.** Como lo menciona la proponente en los antecedentes de su proposición, es la **Organización de los Estados Americanos** **(OEA)** la instancia internacional que ha abordado el tema de la “política y estrategia de seguridad cibernética” en sus distintas dimensiones.

En efecto, la Organización de los Estados Americanos (OEA) ha estado comprometida con temas de seguridad cibernética y delincuencia cibernética, fomentando y apoyando la labor de los Estados Miembros para fortalecer su capacidad para proteger a las personas, las economías y la infraestructura crítica contra la delincuencia cibernética y otros ataques o incidentes cibernéticos.

Lo anterior es así porque la Organización de Estados Americanos (OEA) fue fundada, entre otros, con el objetivo de lograr "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia".

La OEA, para realizar los principios en que se funda y cumplir sus obligaciones regionales de acuerdo con la Carta de las Naciones Unidas, establece dentro de sus principales propósitos el de “afianzar la paz y la seguridad del Continente”.

En 2004 los Estados Miembros de la **OEA** aprobaron la **Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética**, que abogaba por un esfuerzo coordinado de múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio y proporcionaba un marco inicial para cultivar y guiar tal enfoque.

La OEA ha alentado a sus miembros a implementar los principios del **Convenio de Budapest** sobre Delito Cibernético y a considerar su adhesión al tratado, sin embargo, solo Argentina, Chile, Costa Rica, Colombia, Panamá, República Dominicana y recientemente, también Paraguay y Perú han solicitado su adhesión al Convenio. Las razones son múltiples y diversas, inciden básicamente en las carencias tecnológicas para estar al nivel de adoptar las estrategias que el Convenio de Budapest establece, así como de los mecanismos legales para imponer las sanciones propuestas por la comisión de delitos como accesos ilegales, interrupciones ilícitas de servicios, robos de datos, interrupción de sistemas, utilización indebida de aparatos, falsificación informática, fraude informático, pornografía infantil y delitos en materia de derechos de autor y propiedad intelectual.

Cabe mencionar, que los integrantes de esta Comisión dictaminadora, durante el desarrollo de la Décima Reunión Ordinaria, celebrada el 28 de noviembre de 2019, votaron, por unanimidad, a favor de un dictamen con punto de acuerdo por el que se exhorta al titular de la Secretaría de Relaciones Exteriores a impulsar el instrumento de adhesión para que el Estado mexicano forme parte del Convenio sobre Ciberdelincuencia, conocido como el Convenio de Budapest; sin embargo, se encuentra pendiente su trámite en la Mesa Directiva de la Cámara de Diputados, por lo que consideramos que la suscripción del presente dictamen representará un aporte importante en la tarea de impulsar los mecanismos e implementar las políticas necesarias para fortalecer la seguridad cibernética de México y América Latina.

**CUARTA.** Si bien es cierto que México, al ostentar la **presidencia *pro tempore* de la Comunidad Latinoamericana de Estados Latinoamericanos y Caribeños (CELAC)**, ha tenido la oportunidad de fortalecer su liderazgo y así lo ha ejercido para lograr importantes consensos en la región, también lo es que, en materia de seguridad y de manera específica, en el tema de ciberseguridad, el espacio idóneo lo es la Organización de Estados Americanos, por tratarse, en primer término, de una organización internacional con personalidad jurídica propia y una estructura organizacional específica, que le permite impulsar distintas iniciativas como la que se plantea, a diferencia de la CELAC que es, hasta el día de hoy, un foro regional de concertación política, pero sin la estructura formal de una organización internacional.

Por lo tanto, esta dictaminadora considera pertinente modificar el punto de acuerdo en el sentido de que el espacio en el que se impulse un Convenio Latinoamericano de Ciberseguridad, sea en el seno de la Organización de Estados Americanos (OEA), en los siguientes términos:

Único. La Cámara de Diputados del H. Congreso de la Unión exhorta respetuosamente al titular de la Secretaría de Relaciones Exteriores para que proponga, en el seno de la organización de Estados Americano (OEA), el tema de la ciberseguridad, para su análisis y debate, a fin de que, de ser viable, se impulse la suscripción de un Convenio Latinoamericano de Ciberseguridad.

En virtud de lo expuesto, esta Comisión dictaminadora somete a consideración del pleno el siguiente

**ACUERDO**

**Único.** La Cámara de Diputados del H. Congreso de la Unión exhorta respetuosamente al titular de la Secretaría de Relaciones Exteriores para que proponga, en el seno de la organización de Estados Americano (OEA), el tema de la ciberseguridad, para su análisis y debate, a fin de que, de ser viable, se impulse la suscripción de un Convenio Latinoamericano de Ciberseguridad.

Dado en el Palacio Legislativo de San Lázaro el 30 de marzo de 2021.

1. [Estrategia Nacional de Ciberseguridad - Proceso](https://www.proceso.com.mx/opinion/2020/7/30/estrategia-nacional-de-ciberseguridad-246953.html) [↑](#footnote-ref-1)