PARLAMENTO ANDINO

RECOMENDACIÓN No. 540

PARA QUE LOS PAÍSES ANDINOS FIRMEN Y RATIFIQUEN EL CONVENIO SOBRE LA CIBERDELINCUENCIA DEL CONSEJO EUROPEO ("CONVENIO DE BUDAPEST") Y SUS PROTOCOLOS ADICIONALES

La Plenaria del Parlamento Andino, reunida a los veintiocho (28) días del mes de agosto de 2025, en el marco de su Período Ordinario de Sesiones, realizado en la ciudad de Bogotá D.C., República de Colombia

CONSIDERANDO

Que, el Acuerdo de Cartagena establece que el Parlamento Andino es el órgano deliberante de la Comunidad Andina, y tiene dentro de sus atribuciones la promoción y orientación del proceso de integración subregional andina, así como participar en la generación normativa del proceso mediante sugerencias a los órganos del Sistema sobre temas de interés común, y promover la armonización de las legislaciones de los países miembros.

Que, el ciberdelito es “una forma de delincuencia transnacional en constante evolución. Su complejidad, al ocurrir en el ciberespacio, se ve agravada por la creciente participación de grupos delictivos organizados. Los autores del ciberdelito y sus víctimas pueden estar ubicados en diferentes regiones, y sus efectos pueden extenderse a sociedades de todo el mundo, lo que pone de relieve la necesidad de implementar una respuesta urgente, dinámica e integrada” (UNODC, s.f)

Que, la Agenda 2030 para el Desarrollo Sostenible reconoce que el desarrollo económico y la institucionalidad democrática dependen, cada vez más, de entornos digitales seguros. En ese marco, el Objetivo de Desarrollo Sostenible (ODS) 9 resalta la necesidad de “construir infraestructuras resistentes, promover la industrialización inclusiva y sostenible y fomentar la innovación”, todo lo cual requiere de infraestructuras digitales seguras y esto va a depender de fuertes medidas de ciberseguridad, capaces de sostener un crecimiento económico y tecnológico. A su vez, el ODS 16, orientado a consolidar instituciones eficaces, responsables e inclusivas, demanda mecanismos de ciberseguridad que garanticen la integridad de los datos personales, procesos electorales seguros y la prevención de delitos informáticos.

Que, la importancia de la ciberseguridad es crucial para los Estados, pues compromete la protección de sus infraestructuras críticas. En este contexto, el Foro Económico Mundial señala que "los ciberataques a infraestructuras esenciales, como redes eléctricas, hospitales o sistemas de agua, representan una amenaza creciente para la seguridad nacional"(World Economic Forum & Accenture, 2024), puntualizando de esta manera que las consecuencias pueden ir desde pérdidas económicas hasta crisis sociales.

Que, la Organización de las Naciones Unidas establece que “la seguridad cibernética es un componente indispensable para la paz y el desarrollo sostenibles en la era digital″(ONU, 2022), por lo que se debe garantizar la protección de información de vital importancia y alta sensibilidad; tal es el caso de los datos confidenciales de millones de ciudadanos que manejan los gobiernos, donde cualquier filtración puede generar la desconfianza pública y poner en peligro la integridad de las instituciones.

Que, se experimenta un crecimiento muy significativo en la cantidad y en la gravedad de los ciberataques a nivel mundial. En el tercer trimestre del año 2024, el promedio semanal de ciberataques por organización ascendió a 1,876 casos semanales; es decir, un aumento del 75 % en comparación con el mismo período del año anterior. Los sectores más afectados son el educativo y de investigación, el gubernamental y militar, así como el de salud. Esta situación pone de manifiesto el uso de tácticas cada vez más sofisticadas por parte de la delincuencia, y subraya la urgente necesidad de fortalecer la ciberseguridad a nivel global. (Check Point Research, 2025).

Que, en los últimos meses el panorama digital mundial está siendo testigo de ataques cibernéticos representativos que han comprometido servicios críticos tales como sistemas de atención médica. Un ejemplo de ello es el ciberataque al sistema de salud de los Estados Unidos en febrero del año 2024, que afectó a más de 100 millones de pacientes, causando la interrupción masiva de la atención en farmacias y hospitales (Reflectiz, 2024). En esa misma línea, el gobierno francés denunció ese mismo año haber sido objeto de ataques que incluyeron entidades gubernamentales, financieras y deportivas, en el contexto de los Juegos Olímpicos de París (Vandal, 2025).

Que los países de la región andina también son blanco de ciberataques, tal es el caso de Colombia, que en 2024 concentró el 17 % de los ataques registrados en América Latina, convirtiéndose en el país más atacado de la región (Forbes Colombia, 2024). Por otro lado, en Perú se han reportado incidentes de ciberseguridad dirigidos a bancos y otras entidades financieras, al punto que en octubre del año 2024 un ataque a los servidores internos de un conocido banco causó la filtración de los datos personales de más de 3 millones de usuarios (Segura, 2025). En los últimos años, Chile ha evidenciado un preocupante aumento en los intentos de ciberataques. Informes recientes señalan que en 2023 se registraron 6 000 millones de intentos, cifra que se incrementó a 27 600 millones en 2024 (Channel News–EMB, 2025). En el caso de Ecuador, los sectores financieros, de telecomunicaciones y gubernamental, por su alto valor estratégico, se han convertido en los objetivos más frecuentes de los ciberataques.

Que, la creciente sofisticación y alcance transnacional de los ciberataques exige respuestas coordinadas entre Estados, organismos internacionales y entidades especializadas en ciberseguridad, con la finalidad de proteger infraestructuras críticas, datos sensibles y la integridad de las instituciones públicas y privadas. En este contexto, cabe destacar que, en 2018, la Asamblea de las Naciones Unidas reconoció que “…los Estados deben estudiar la mejor manera de cooperar para intercambiar información,

prestarse asistencia mutua, enjuiciar la utilización de las TIC con fines terroristas y delictivos y aplicar otras medidas de cooperación para hacer frente a esas amenazas." (ONU, 2018).

Que, considerando los cambios provocados por la digitalización y el desarrollo de nuevas redes informáticas, y con el fin de proteger a la ciudadanía frente a la ciberdelincuencia, el Consejo Europeo establece el 23 de noviembre de 2001, el Convenio sobre la Ciberdelincuencia (CETS N.º 185), conocido como "Convenio de Budapest". Este instrumento tiene como objetivo "incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos" (Consejo Europeo, 2001, p. 3).

Que, el Convenio de Budapest busca "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, garantizando la tipificación como delito de dichos actos, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable" (Consejo de Europeo, 2001).

Que, el Convenio de Budapest, está compuesto por cuatro capítulos a través de los cuales se abordan los siguientes temas:

i) Disposiciones Generales (Terminología). Define conceptos clave como "sistema informático", "datos informáticos", "proveedor de servicios" y "datos de tráfico", con el propósito de armonizar el lenguaje jurídico y facilitar la cooperación internacional.

ii) Medidas que deben adoptarse a nivel nacional. Establece las obligaciones que deben asumir los Estados para adaptar su legislación penal interna, tipificando delitos como: el acceso e interceptación ilícita, ataques a la integridad de sistemas, fraude y falsificación informática, distribución de pornografía infantil y delitos contra la propiedad intelectual. También establece procedimientos procesales para la investigación y recolección de evidencia digital.

iii) Cooperación internacional. Promueve la asistencia mutua entre Estados en investigaciones transfronterizas, incluyendo allanamientos, incautaciones, conservación de datos y extradición. Se establece además la Red 24/7, en donde cada parte establecerá un punto de contacto para garantizar asistencia inmediata en casos de ciberdelito.

iv) Clausulas finales. Contiene cláusulas jurídicas que regulan el funcionamiento del Convenio. Establece las normas sobre firma, ratificación, entrada en vigor y adhesión al Convenio.

Que, el Convenio de Budapest sobre la Ciberdelincuencia entró en vigor el 1 de julio de 2004, tras la ratificación de 5 estados firmantes. Actualmente[1], ha sido ratificado por un total de 80 países, 45 de ellos son Estados miembros del Consejo Europeo y 35 son Estados no miembros. De este último grupo, 9 de ellos son países latinoamericanos, entre los cuales se encuentra Chile, Colombia, Ecuador y Perú[2].

Que, a fin de promover la actualización del Convenio de Budapest y propiciar su aplicación efectiva, así como el intercambio de información y el examen de futuras enmiendas se creó el Comité de la Convención sobre Delitos Cibernéticos (T-CY), el cual representa a los Estados Parte del Convenio de Budapest. Que el T- CY es el "Principal espacio de intercambio de información sobre la implementación y uso del Convenio y tiene el mandato para elaborar protocolos adicionales al texto original para articular nuevas cuestiones y demandas de los Estados miembros en la lucha contra la ciberdelincuencia" (Martins dos Santos, 2022, p.8).

Que, el aumento de la xenofobia y el racismo cometidos a través de sistemas informáticos llevó a que, en enero de 2003, se publicara el *Primer Protocolo Adicional del Convenio sobre la Ciberdelincuencia (CETS N.º 189).* Este incluye disposiciones sustantivas, procesales y de cooperación internacional, para abarcar los delitos de propaganda racista o de xenofobia en línea, además ofrece una definición de "material racista y xenófobo", y proporciona un conjunto de herramientas para reprimir la difusión de este tipo de contenidos a través de los sistemas informáticos (Consejo Europeo, 2003). Este Protocolo entró en vigor en marzo del 2006, y ha sido ratificado y adoptado por 38 países, incluidos los Estados miembros del Parlamento Andino, con excepción de Bolivia.

Que, con el objetivo de continuar mejorando "la cooperación en materia de ciberdelincuencia y la capacidad de las autoridades de justicia penal para reunir pruebas en formato electrónico de un delito penal a efectos de investigaciones o procedimientos penales específicos mediante instrumentos adicionales relacionados con una asistencia mutua más eficiente y otras formas de cooperación entre las autoridades competentes; la cooperación en casos de emergencia, y la cooperación directa entre las autoridades competentes y los proveedores" (Consejo Europeo, 2023a, p. 208), en noviembre de 2021 el Consejo Europeo adoptó el *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (CETS N.º 224),* el cual fue abierto a la firma de los Estados en mayo de 2022.

Que, el *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas*, busca hacer frente a los diferentes desafíos y complejidades para obtener pruebas electrónicas que

[1] Al 10.06.2025

[2] Cuadro de firmas y ratificaciones del Convenio sobre la Ciberdelincuencia https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

pueden estar almacenadas en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas. En ese sentido, establece disposiciones e instrumentos orientados a fortalecer la cooperación y la divulgación de pruebas digitales relativas a ciberdelincuencia y a otros delitos que son cometidos por los proveedores de servicios en jurisdicciones extranjeras, pero con poderes coercitivos restringidos a los límites nacionales. Todo ello lo hace a través de un sistema sólido de salvaguardias de los derechos humanos y del estado de derecho, incluida la protección de datos personales (Consejo Europeo, s.f).

Que, este Protocolo se divide en cuatro capítulos. El primero establece la finalidad y su ámbito de aplicación, el cual abarca no solo delitos de ciberdelincuencia, sino cualquier infracción penal que implique pruebas en formato electrónico, incorpora definiciones adicionales relevantes, además de incluir un artículo sobre el uso de la lengua para facilitar la cooperación internacional superando barreras lingüísticas. El segundo capítulo contiene las principales medidas de cooperación reforzada. El tercer capítulo establece las condiciones y salvaguardias e incluye salvaguardias específicas para la protección de los datos personales. Finalmente, el capítulo cuarto contiene las disposiciones finales (Consejo Europeo, 2022a).

Que, las Decisiones 2022/722 y 2023/436 del Consejo de la Unión Europea autorizan a los Estados miembros a firmar y ratificar el Protocolo, estableciendo también las reservas y declaraciones necesarias para su aplicación conforme al derecho comunitario (Consejo Europeo, 2022b; 2023b).

Que, el *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia*, ha sido firmado por 48 países[3]; sin embargo, solo ha sido ratificado por dos, por lo que aún no ha entrado en vigor. En el caso de los países andinos, este Convenio ha sido firmado por Colombia, Chile y Perú; no obstante, aún no ha sido ratificado por ninguno de ellos[4].

Que, con el objetivo de promover la ratificación e implementación del *Segundo Protocolo Adicional al Convenio de Budapest sobre la Ciberdelincuencia* por parte de los Estados miembros de la Unión Europea y otros Estados Parte del Convenio de Budapest se instaura en 2024 el *proyecto "CyberSPEX (2024 - 2026): Cooperación reforzada sobre pruebas electrónicas por parte de los Estados miembros de la UE a través del Segundo Protocolo del Convenio de Budapest".* Este proyecto viene siendo implementado de forma conjunta por la Unión Europea y el Consejo Europeo a través de la Oficina del Programa sobre Ciberdelincuencia del Consejo Europeo (C-PROC).

---

[3] Al 10.06.2025.

[4] Cuadro de firmas y ratificaciones del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (CETS n.º 224) disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

Que, el Parlamento Andino ha venido desarrollando esfuerzos normativos significativos en materia de prevención y respuesta frente a los delitos cibernéticos. Entre ellos, la aprobación del *Marco Normativo que establece la Estrategia Andina para Combatir el Acoso Cibernético entre Niños, Niñas y Adolescentes* (Recomendación N.º 452), que orienta a los Estados miembros en la formulación de políticas públicas para enfrentar esta problemática, priorizando la protección de los derechos de la niñez y adolescencia. Asimismo, se encuentra en curso la actualización del *Marco Normativo para el Fortalecimiento de la Ciberseguridad en la Región Andina* (Recomendación N.º 454), cuyo propósito es armonizar los marcos legislativos nacionales, fortalecer las capacidades institucionales y promover un entorno digital seguro y resiliente. Además de proteger a la ciudadanía, al sector privado y sector público de amenazas cibernéticas e informáticas, fomentando la prosperidad social, el crecimiento económico y la maximización de los beneficios de las Tecnologías de la Información y de la Comunicación.

A estos esfuerzos se suma la elaboración del documento *Lineamientos de Política de Seguridad Integral para los Países de la Región Andina*, aprobado mediante Resolución N.º 8 del Parlamento Andino del 2024, el cual consolida la producción normativa del Parlamento Andino relacionada con la seguridad humana desde un enfoque integral, incluido lo referente a ciberseguridad y delitos informáticos.

Que, estas acciones reflejan el compromiso del Parlamento Andino con el desarrollo de un ciberespacio confiable y constituyen una base complementaria que refuerza la necesidad de avanzar hacia la adopción del Convenio de Budapest y sus Protocolos Adicionales, en aras de una cooperación internacional eficaz frente a las amenazas cibernéticas transnacionales.

Que, la ciberdelincuencia ha trascendido fronteras y viene evolucionando con gran rapidez, razón por la cual la cooperación internacional se ha convertido en un componente esencial para una respuesta eficaz y coordinada. La persecución de estos delitos no solo requiere de marcos normativos comunes, canales ágiles de intercambio de información, sino de mecanismos de asistencia mutua entre Estados. Por tanto, la ratificación del Convenio de Budapest sobre la Ciberdelincuencia y sus Protocolos Adicionales por parte de los Estados miembros del Parlamento Andino no solo fortalecerá sus capacidades internas para enfrentar amenazas digitales. Además, permitiría integrarse a una red global de cooperación judicial y técnica, facilitando investigaciones transnacionales, el acceso a pruebas electrónicas y la protección de los derechos fundamentales en el entorno digital.

Por los considerandos antes expuestos, y de conformidad a sus atribuciones reglamentarias, la Plenaria del Parlamento Andino:

RECOMIENDA

ARTÍCULO PRIMERO: Instar a los países de la región andina que aún no han firmado ni ratificado el Convenio sobre la Ciberdelincuencia del Consejo Europeo (Convenio de Budapest) a que procedan a su pronta firma y ratificación. Asimismo, exhortar a aquellos Estados que ya han ratificado dicho Convenio a que suscriban y ratifiquen los Protocolos Adicionales adoptados en el marco de este, en tanto constituyen instrumentos esenciales para fortalecer la cooperación internacional en la lucha contra los delitos informáticos, y mejorar la respuesta regional frente a los desafíos de la ciberseguridad.

ARTÍCULO SEGUNDO: Exhortar a los países de la región andina a adecuar su legislación interna a las disposiciones del Convenio de Budapest y sus Protocolos Adicionales, promoviendo marcos legales eficaces y compatibles con los estándares internacionales en materia de ciberseguridad.

ARTÍCULO TERCERO: Solicitar a las autoridades competentes de los países andinos, incluidos los Ministerios de Justicia, del Interior, de Defensa y de Tecnologías de la Información; las fiscalías especializadas en delitos informáticos; el Poder Judicial; las unidades de investigación criminal; las instituciones a cargo del registro civil y de identificación ciudadana; y otros organismos pertinentes, que establezcan acciones coordinadas para el diseño e implementación de programas de capacitación, cooperación técnica y fortalecimiento institucional, orientados al mejoramiento de las capacidades de investigación, persecución y juzgamiento de los delitos informáticos, al uso eficaz de la evidencia electrónica, y al fortalecimiento de la cooperación interinstitucional, internacional y con el sector privado, en línea con los estándares del Convenio de Budapest y su Segundo Protocolo.

Dada y suscrita a los 28 días del mes de agosto de 2025.

Notifíquese y publíquese.

PARLAMENTO ANDINO PRESIDENCIA

P.A. SARA KATTYA CONDORI
Presidenta

DR. EDUARDO CHILIQUINGA MAZÓN
Secretario General

PARLAMENTO ANDINO SECRETARIA GENERAL