República del Ecuador

Ministerio de Gobierno

**CRITERIO TÉCNICO**
**CONVENIO SOBRE LA CIBERDELINCUENCIA**

## 1. ANTECEDENTES

El *Convenio sobre la Ciberdelincuencia* o *Convenio de Budapest* es el primer tratado multilateral que se refiere al combate a los delitos cibernéticos: aprobado el 23 de noviembre de 20021 por el Consejo de Europa, entró en vigor el 1 de julio de 2004.

El Artículo 37 del mencionado Convenio establece, en su parte pertinente: "*Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a los Estados firmantes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración*".

Por otro lado, los días 11 y 12 de septiembre de 2018, el Ministerio del Interior (ahora Gobierno), participó en el *Taller de Cibercrimen* que tuvo lugar en Viena, bajo la Presidencia del Ecuador del *Grupo G77*. Durante este espacio, se presentaron los avances a nivel nacional, con especial énfasis en los desafíos registrados para prevenir, combatir e investigar los delitos cibernéticos dado el marco normativo vigente. En dicho foro, se tomó conocimiento de la oportunidad y alcance que reviste la *Convención sobre Ciberdelincuencia*, como también, otras iniciativas en curso, particularmente el interés de determinados países de alcanzar un instrumento universal, jurídicamente vinculante en esta materia.

Posterior, el Ministerio de Gobierno, por medio de sus áreas técnicas como de la Policía Nacional del Ecuador, participaron en las distintas reuniones y espacios promovidos por el Ministerio de Relaciones Exteriores y Movilidad Humana, cuyo objetivo consistió en concientizar a las instituciones nacionales sobre las necesidades de fortalecer, organizar y articular la cooperación en materia de Ciberseguridad, a través del ente rector del relacionamiento internacional. Es así que, el 31 de enero de 2019, se atendió la convocatoria realizada por la Subsecretaría de Asuntos Multilaterales, en la cual, las áreas técnicas de nivel ministerial y policial, expusieron sus criterios sobre la necesidad de robustecer el marco normativo, por medio de una posible adhesión al *Convenio de Budapest*. Otras instituciones se sumaron a este criterio, ante los cual la Cancillería impulsó una serie de acercamientos y manifestaciones de interés ante socio estratégicos en esta materia.

Por ello, Ecuador expresó su interés por ingresar al *Convenio de Budapest*, en mayo de 2019, tras una consulta realizada por parte del Gobierno ecuatoriano al Consejo de Europa, lo que le permitió ser calificado como país prioritario para recibir apoyo para su adhesión al Convenio. Ante ello, se viene recibiendo cooperación a través de *Glacy +*, el cual es un Proyecto de la Unión Europea y del Consejo de Europa para contribuir a fortalecer las capacidades de los Estados respecto de legislación, política y estrategias para afrontar el cibercrimen.

La cooperación, a través de *Glacy +*, ha permitido la realización de varias acciones y talleres, como parte de ello el "*Taller de Legislación sobre Ciberdelito y Evidencia Electrónica en Ecuador*" realizado los días 28 y 29 de mayo del 2020, el cual constituyó uno de los principales

*interceptación ilegal de datos*, el *ataque a la integridad de sistemas informáticos*, *la circulación de información restringida* y la *interceptación de las comunicaciones o datos informáticos*.

Además de estas codificaciones, existen Planes Nacionales que abordan la temática del delito cibernético, particularmente la *Política Nacional de Ciberseguridad*, aprobada en 2021, por parte del Gabinete Sectorial de Seguridad (GSS).

## 3. CRITERIO Y ANÁLISIS TÉCNICO

### 3.1. Diversificación de los riesgos y amenazas en el ciberespacio

En el mundo más de 4.100 millones de usuarios tienen acceso a internet (ITU 2019), esto representa más de la mitad de la población mundial.[1] En el caso de las nuevas tecnologías de la información y comunicación, su creciente democratización ha traído consigo cambios y retos permanentes, al constituirse como uno de los pilares del mundo globalizado[2].

El avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo[3]. Es así que un número creciente de personas y grupos obtienen ventajas de la rapidez, conveniencia y anonimato que brinda el Internet para perpetrar una serie de actividades delictivas que no conocen fronteras físicas, representando amenazas reales para las víctimas a nivel global.[4] Si en el pasado el delito cibernético era perpetrado principalmente por individuos o por pequeños grupos, en la actualidad, se estarían configurando patrones novedosos bajo los cuales operan concertadamente redes delictivas muy complejas en el ciberespacio, que reúnen a individuos en distintos países en tiempo real, para cometer delitos a una escala sin precedentes (Interpol 2017).

Entre los principales delitos cibernéticos, se destacan la piratería que afecta a la propiedad intelectual, así también ataques con códigos maliciosos como por ejemplo ataques de denegación de servicios (DoS, DDoS), que constituyen amenazas a la seguridad de los gobiernos, negocios e individuos y suponen un desafío para los organismos y agencias encargadas de la aplicación de la

---

[1] Uno de cada tres de estos usuarios es menor de 18 años y accede al internet en su mayoría a través del teléfono celular. Niños niñas y adolescentes en el mundo están en línea alrededor de dos horas al día entre semana y aproximadamente el doble de tiempo el fin de semana.

[2] Las Tecnologías de la Información y de la comunicación (TIC) son fundamentales para la democratización del conocimiento. Es decir, las TIC constituyen un elemento indispensable de cara a las proyecciones de desarrollo social de los países, de los grupos sociales y de los individuos (Lugo, 2010, IIPE, 2014).

[3] El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado, e incluyendo a la sociedad civil. Según Naciones Unidas, en el mundo los cibercrímenes (o ciberdelitos) llegaría a representar un costo de 600 mil millones USD (ONUDC, 2016).

[4] Un impacto primario del delito cibernético es financiero, considerando que puede incluir muchos tipos diferentes de actividades delictivas con fines de lucro, incluidos ataques de ransomware, fraude por correo electrónico e internet y fraude de identidad, así como intentos de robo de cuentas financieras, tarjetas de crédito u otra información de tarjetas de pago. No obstante, también se ven afectadas las personas y los Estados.

deepweb y darkweb han permitido la consolidación de comercialización de material pornográfico, de armas, de drogas, prostitución y tráfico de personas. De este modo, se han creado verdaderos mercados ilícitos virtuales y anónimos dentro del internet, los cuales se han convertido en maneras más seguras de delinquir.

En definitiva, prácticamente todos los delitos comunes se han potenciado con el uso de internet, de las tecnologías comunicacionales y las técnicas de anonimato. Delitos como la extorsión, anteriormente se lo consideraba ligado al secuestro de las personas o al robo de sus bienes tangibles, pero al momento se dan extorsiones en línea, ejerciendo presión a la víctima sobre su información personal y digital, amenazándola con difundir o eliminar su información, obteniendo réditos económicos a cambio de no publicarla.

3.2. Riesgos en línea: escenario nacional

Según la encuesta multipropósito TIC 2019, realizada por el Instituto Ecuatoriano de Estadísticas y Censos (INEC) el porcentaje de hogares con acceso a internet se ha incrementado en los últimos años, en 2019 el 45.5% de hogares a nivel nacional tuvieron acceso a internet.

Esta misma encuesta indica que los niños, niñas y adolescentes entre 5 y 17 años, utilizan el internet principalmente desde su hogar (64.5%), desde centros de acceso público (15%) y desde su institución educativa (13.1%). En menor medida lo usan en el trabajo o en otros lugares.

En cuanto al uso de teléfono celular inteligente, en 2019 el 12.2% de personas que tienen teléfono celular inteligente, son niños, niñas y adolescentes entre 5 y 15 años de edad, frente a 1,2% de niños, niñas y adolescentes entre 5 y 15 años de edad que tenían teléfono celular inteligente en el año 2012.

En medio de la pandemia por COVID19, niños, niñas y adolescentes se vieron volcados al uso de plataformas y entonos virtuales para el desarrollo de clases en línea, realidad que se mantendrá en los próximos meses y que incrementa el riesgo y la vulnerabilidad de esta población a la ciberdelincuencia.

Sin duda, la tecnología y la experiencia digital, tiene muchos aspectos positivos, sin embargo, la exposición al mundo digital sin un entorno seguro, implica muchos riesgos, en particular, para niños, niñas y adolescentes: desde trastornos relacionados con el juego, riesgos financieros, recopilación y monetización de datos personales, ciberacoso, ciberbulling, discursos de odio, racismo, violencia y exposición a conductas o contenidos inapropiados, entre otros.[7]

En este contexto, la cibercriminalidad es una de las *nuevas amenazas* que enfrenta el Ecuador y el mundo, que genera muchas inquietudes y se ha convertido en un gran reto para los gobiernos que deben buscar mecanismos integrales para que niños, niñas y adolescentes accedan de manera

[7] La exposición de niños, niñas y adolescentes a contenido inapropiado o información inexacta, puede ocasionar que adopten conductas autolesivas, destructivas o violentas, así como limitar su entendimiento del mundo que les rodea. Contenidos orientados a la manipulación de niños, niñas y adolescentes, pueden influir en su desarrollo, formación de opiniones, valores y hábitos.

el COIP), con el propósito de viabilizar una adaptación y armonización de las leyes y tipologías actuales con aquellas más comunes del delito cibernético a nivel internacional, y así abrir el espacio a la formulación y ejecución de nuevos mecanismos y herramientas de investigación adaptadas a la realidad del fenómeno.

Por ello, con los antecedentes establecidos respecto del *Convenio de Budapest*, cuyo objetivo busca proteger a las sociedades frente a delitos informáticos, mejorar las técnicas de investigación y cooperación internacional; y dadas las necesidades en esta materia a nivel nacional, particularmente de las instituciones de cumplimiento de la Ley (Fiscalía, Policía), adquiere especial relevancia y oportunidad el impulsar todas las acciones y mecanismos vigentes, entre ellos el de cooperación internacional, para que el marco normativo actual ecuatoriano tipifique delitos asociados al entorno cibernético, en línea con buenas prácticas que han adoptado otros Estados, luego de su adhesión al *Convenio de Budapest*.

**En este sentido, el criterio técnico es favorable a emprender, de manera coordinada e interinstitucional, los distintos procesos y pasos necesarios para que el Ecuador puede alcanzar una adhesión plena al *Convenio de Budapest*.**

## 4. RECOMENDACIONES

Se recomienda mantener la articulación con otros poderes del Estado, tanto en el ámbito judicial como legislativo, éste último en particular puesto que una posible adhesión requiere de reformas normativas como se ha identificado.

Enfrentamos nuevos retos y desafíos como consecuencia de la diversificación de actividades por parte de los grupos de delincuencia organizada, que requieren una actuación y respuesta sistémica ante la corrupción; la trata de personas; el tráfico ilícito de migrantes; el tráfico ilícito de armas de fuego, municiones y explosivos; los delitos ambientales; la extorsión; y, el lavado de activos, al igual que delitos cibernéticos -con creciente impacto en la economía, en los derechos humanos y en la privacidad de las personas. La cooperación internacional tiene, en ese contexto, un rol estratégico, pues permite generar un proceso permanente de aprendizaje e intercambio de conocimientos y experiencias con países con los cuales compartimos desafíos similares, particularmente en el ámbito de la seguridad pública, debido a que enfrentamos amenazas comunes.

De este modo, dado el escenario de riesgos y amenazas en el entorno cibernético, se requiere continuar fortaleciendo y diversificando los mecanismos de cooperación con otras instituciones competentes en materia de ciberseguridad (de países como de organismos internacionales), con el acompañamiento del ente rector del relacionamiento internacional, para adaptar, crear y desarrollar nuevas herramientas y capacidades cooperativas de prevenir y enfrentar los delitos cibernéticos.

Quito, 21 de septiembre de 2021

JOHN ESTEBAN GAME VILLACIS

**Aprobado: Subsecretaría de Seguridad Ciudadana**

Elaborado: Dirección contra la Delincuencia Organizada y sus Delitos Conexos