CARLOS GUERRERO ARGOTE

CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA

ANÁLISIS SOBRE LA ADHESIÓN Y EL PROCESO DE IMPLEMENTACIÓN EN COSTA RICA, GUATEMALA, PANAMÁ Y LA REPÚBLICA DOMINICANA

Autor: Carlos Guerrero Argote
Coordinadora: Lia P. Hernández Pérez
Revisión: Gabriel Cajigas
Colaboración: Michel Souza - Derechos Digitales
Diagramación: Juan Pablo Hoyos C.

Abril 2023

Queremos agradecer a las siguientes personas que proveyeron retroalimentación sobre las diferentes versiones del reporte, a través de entrevistas y comentarios remitidos por escrito. Su aporte ha sido invaluable para el resultado final:

Amalia Hernández (ISOC Honduras); Carlos Leonardo (CSIRT República Dominicana); César Moline (INDOTEL); Juan Ramón Anria (AIG Panamá); Michelle Souza (Derechos Digitales); Sara Fratti (Fundación Avina); y Silvia Batista (AIG Panamá).

IPANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

IPANDETEC Centroamérica es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

ÍNDICE

ÍNDICE

I. RESUMEN EJECUTIVO

1. SOBRE EL REPORTE

- El reporte analiza el proceso de adhesión e implementación del Convenio de Budapest en cuatro países de Centroamérica: Costa Rica, Guatemala, Panamá y República Dominicana.

- También provee una lectura crítica sobre el papel de la subregión en el contexto de la negociación de un nuevo tratado sobre ciberdelincuencia en las Naciones Unidas y qué agentes de influencia externa e interna deben ser tenidos en cuenta.

- Con base en las conclusiones, se plantea un conjunto de recomendaciones dirigidas a los gobiernos y la sociedad civil que permitan el avance de reformas impulsadas por consenso y con respeto de los derechos humanos.

- El objetivo final del reporte es dar a conocer la situación actual en los países analizados, así como identificar patrones, tendencias y otros elementos que mejoren la información disponible para los actores locales del ecosistema centroamericano.

2. SOBRE LAS CONCLUSIONES

- Se concluye que el impacto que el Convenio ha tenido en Centroamérica es profundo y se prolongará en el tiempo, incluso entre los países que no se han adherido o que están en vías de hacerlo.

- Se concluye que, salvo Guatemala, todos los países analizados presentan un gran avance en la implementación del Convenio y podrían ser un caso de estudio para Latinoamérica. Sin embargo, los reportes sobre la subregión todavía son escasos.

- Se concluye que, pese al aparente consenso frente a las reformas para la lucha contra la ciberdelincuencia de los últimos años, nuevos procesos de implementación del Convenio están siendo rechazados debido a posibles afectaciones a derechos humanos.

- Se concluye que la presión existente por sacar adelante la implementación ante un escenario de mayores riesgos para la ciberseguridad, podría alentar a los gobiernos de los países analizados a disminuir los espacios de diálogo, lo que es crítico frente a escenarios como la firma del Segundo Protocolo Adicional del Convenio.

3. SOBRE LAS RECOMENDACIONES

- Se recomienda la realización de iniciativas para mejorar la conciencia en la población sobre los peligros de la ciberdelincuencia. En el caso de los gobiernos, deben promover la creación de alianzas multisectoriales. En el caso de la sociedad civil, deben crear capacidades en públicos clave como activistas y periodistas.

- Se recomienda la realización de estudios más detallados sobre la experiencia centroamericana frente a la implementación del Convenio de Budapest, con el fin de identificar buenas prácticas a ser implementadas por otros gobiernos de la región o informar las estrategias de incidencia de la sociedad civil.

- Se recomienda el impulso de más espacios de diálogo de múltiples partes interesadas con el fin de que las reformas en el marco de implementación del Convenio de Budapest sean producto de un amplio consenso.

INTRODUCCÍON

Según datos del Banco Mundial, el acceso a Internet en el mundo ha mantenido una tasa de crecimiento sostenida con picos de explosión a lo largo de las dos últimas décadas. Así, aunque en el año 2000 el nivel de cobertura era apenas de 7%, en 2010 se cuadriplicó hasta llegar a 29% y finalmente en 2020 alcanzó un total de 60% (aproximadamente 4700 millones de personas). Latinoamérica ha experimentado un desarrollo similar, pasando de una cobertura de 4% en el año 2000, a una de 35% en 2010 y finalmente a 74% en 2020 (aproximadamente 655 millones de personas).[1]

Si bien las cifras anteriores cuentan una historia de progreso, la realidad es que a lo largo de estas dos décadas, la expansión del acceso no ha estado exenta de obstáculos, algunos de ellos relacionados al esfuerzo mismo de conectar a más personas, pero también otros surgidos a propósito de haber logrado dicha conexión. Los ciberataques, la difusión de noticias falsas y la violencia de género digital son algunos ejemplos de cómo el avance del acceso a Internet también ha creado o amplificado múltiples amenazas sobre las personas y las instituciones.

Una de estas amenazas son los ciberdelitos, una categoría que contiene diferentes elementos, entre ellos; los delitos informáticos, los delitos facilitados por la tecnología y otras situaciones en las que se afectan los medios informáticos y a las personas que los utilizan. En el contexto del crecimiento sostenido de la conectividad, el desarrollo de paradigmas como la transformación digital y el proceso de digitalización forzada iniciada en 2020 por la pandemia de COVID-19, distintas voces apuntan hacia los ciberdelitos como uno de los principales obstáculos para garantizar la seguridad y la paz a nivel global.

Debido a su naturaleza compleja, los ciberdelitos han requerido desde un inicio respuestas igual de complejas. La más importante de estas ha sido la creación del Convenio de Budapest, un tratado internacional que propone medidas para hacer interoperables los sistemas de justicia penal de los países miembros y facilitar la investigación y persecución transfronteriza. Si bien han existido otros esfuerzos, ninguno ha alcanzado el nivel de desarrollo del Convenio, que ha generado a su alrededor un ecosistema completo de iniciativas en materia investigación, intercambio de experiencias y creación de capacidades.

Publicado en 2001, durante más de dos décadas el Convenio ha impactado la forma en que los países del mundo enfrentan la ciberdelincuencia. Latinoamérica no ha sido ajena a esta situación y desde 2013 y en adelante varios países de la región lo han suscrito, iniciando o dando tracción a procesos de reforma para adaptarse a sus disposiciones. El alcance y situación actual de estos procesos han sido analizados en diferentes estudios, muchos de ellos liderados por los gobiernos y el sector privado, pero también por organizaciones de la sociedad civil, especialmente aquellas enfocadas en los derechos digitales.

1. Banco Mundial. Estadísticas de personas que usan Internet (2020). Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=map

Un ejemplo de lo anterior es un conjunto de ensayos dirigidos por la ONG Derechos Digitales en 2018 sobre el potencial impacto del Convenio en la región[2] y una actualización en 2022 sobre los procesos de reforma en curso y la participación de la sociedad civil en los mismos.[3] Una preocupación constante por parte de estos estudios es el potencial impacto negativo en los derechos humanos de cierto tipo de reformas, especialmente en materia de tipificación penal y técnicas de investigación, el cual se ve exacerbado por la ausencia de salvaguardas internacionales adecuadas como las que poseen miembros de otras regiones.

A pesar de tener una naturaleza más crítica, estos estudios permiten conocer el grado de implementación del Convenio y los cambios que ha producido y está produciendo en los países analizados. Esto no solo es insumo importante para la sociedad civil sino también para los hacedores de política pública, pues permite identificar aquellos factores de riesgo a tener en cuenta para avanzar sobre una reforma concertada y sostenible. Tal es así que el reporte de actualización de 2022 que mencionamos anteriormente incluyó recomendaciones dirigidas específicamente a los Estados y gobiernos nacionales.

Lamentablemente, tanto estos análisis como muchos de los que son llevados a cabo por gobiernos y el sector privado presentan carencias en torno al nivel de representación en la región. Dependiendo del enfoque y el objeto de análisis, cuando se estudia el impacto del Convenio en Latinoamérica, la subregión de Centroamérica suele estar subrepresentada, pese a presentar características diferenciales y ofrecer opciones interesantes de investigación, como el hecho de ser pionera en la tipificación de delitos informáticos o incluir a los países que más han avanzado en la implementación del Convenio.

Con el fin de cerrar esta brecha informativa, este reporte se propuso identificar y analizar el conjunto de actores, normas y procesos relacionados al Convenio de Budapest en cuatro países de Centroamérica: Costa Rica, Guatemala, Panamá y la República Dominicana. Para ello, se utilizaron insumos para contextualizar los hallazgos, entre ellos; estadísticas del Banco Mundial y otros organismos internacionales, reportes sobre ciberseguridad del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA)[4], documentos propios como la serie Centroamérica Cibersegura,[5] entrevistas con expertas y expertos, etc.

El objetivo final fue poner a disposición de todos los interesados, una herramienta actualizada de diagnóstico que informe y sea útil para la toma de mejores decisiones.

2.El conjunto de publicaciones se produjo en el marco del proyecto “Grupo de trabajo sobre ciberseguridad en América Latina”, gracias al trabajo conjunto de las organizaciones locales: Hiperderecho (Perú), IPANDETEC (Panamá), Fundación Karisma (Colombia), Red en Defensa de los Derechos Digitales (México) y TEDIC (Paraguay), bajo la coordinación de Derechos Digitales, y gracias al apoyo de Ford Foundation. Disponibles en: https://www.derechosdigitales.org/?s=budapest
3. Bruna Martins dos Santos. Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf
4. BID y OEA. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (Informe Ciberseguridad 2016). Disponible en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf
5. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf

III. SOBRE EL CONVENIO DE BUDAPEST Y SU IMPACTO EN LATINOAMÉRICA

En esta sección, se presenta un recuento sucinto sobre el Convenio de Budapest, desde su creación hasta el momento actual, incluyendo sus protocolos y el reciente tratado en materia de ciberdelincuencia que se gesta en las Naciones Unidas. Luego se analizan las interacciones del Convenio con países de Latinoamérica y el impacto que este ha tenido, a partir de diferentes estudios sobre la región.

1. BREVE HISTORIA DEL CONVENIO DE BUDAPEST

La Convención sobre el cibercrimen, también conocida como el Convenio de Budapest sobre cibercrimen o simplemente el Convenio de Budapest es un tratado negociado en el seno del Consejo de Europa, abierto a firma el 23 de septiembre de 2001 y vigente desde el 1 de julio de 2004. Se le reconoce como el primer instrumento internacional creado con el fin de combatir los delitos informáticos, así como los delitos facilitados por la tecnología a través de un mandato de estandarización de las normas penales en su parte sustantiva y procesal, y la implementación de mecanismos de cooperación internacional entre los países miembros.

Según su sitio web informativo, el Convenio de Budapest cuenta actualmente con 68 países miembros y 19 países observadores (de un total de 193), siendo que la mayoría de estos últimos han sido invitados a adherirse y se encuentran en diferentes etapas de dicho proceso. En Latinoamérica, los miembros, enumerados por orden cronológico de adhesión, son: República Dominicana (2013), Panamá (2014), Chile (2017), Costa Rica (2017), Argentina (2018), Paraguay (2018), Perú (2019), Colombia (2020) y Brasil (2022). En calidad de observadores se encuentran Ecuador, Guatemala, México y Uruguay.[6]

Más de dos décadas después de su lanzamiento, el Convenio de Budapest sigue siendo el único tratado de su tipo que agrupa a países de todas las regiones y es un elemento casi siempre presente cuando se discuten políticas públicas en el ámbito de la ciberseguridad. No obstante, su vigencia no se sostiene solo en su singularidad, sino también en el universo de programas, iniciativas y otros desarrollos que han surgido en su interior, como es el caso del Programa GLACY+, el Proyecto Octopus; y el Primer y Segundo Protocolo Adicional al Convenio.

Pese a todo lo anterior, el Convenio de Budapest también tiene detractores. Países como China, India y Rusia se han negado a adherirse, aduciendo que no participaron en su redacción y por lo tanto sus intereses no se ven reflejados en el texto. Además, muchas de las disposiciones sobre cooperación internacional, que fueron pensadas por sus miembros originales desde su alto nivel de confianza y cooperación previa, son percibidas como contrarias a la soberanía digital.[7] Al ser estos y otros países reacios a implementar dichos mecanismos, la universalidad a la que el Convenio aspira se ve comprometida.

6. Consejo de Europa. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Disponible en: https://www.coe.int/en/web/cybercrime/parties-observers
7. Internet Society. Navigating Digital Sovereignty and its Impact on the Internet. Disponible en: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf

Con el fin de superar el problema anterior, durante la última década ciertos países han impulsado la idea de que se necesita un nuevo tratado contra la ciberdelincuencia, el cual además debe ser elaborado por un organismo multilateral. Como respuesta a ello, tras años de estudios previos y diálogo en comisiones y grupos de trabajo, durante su 74° período de sesiones en 2019, la Asamblea General de las Naciones Unidas emitió la Resolución N° 74/247, en la que dispuso la creación un Comité Intergubernamental con el fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.[8]

Si bien se espera que el proceso de las Naciones Unidas se vea influenciado por las experiencias producidas durante la aplicación del Convenio de Budapest, todavía no resulta claro en qué medida ambos instrumentos convivirán si es que el tratado de las Naciones Unidas finalmente es aprobado y suscrito por una mayoría importante de países. Esto último, así como los alcances del nuevo tratado, son temas de especial interés para los países de la región, tanto los que han suscrito el Convenio de Budapest como los que están en proceso de hacerlo.

2. EL CONVENIO DE BUDAPEST Y SU IMPACTO EN LATINOAMÉRICA

Actualmente son 9 los países de Latinoamérica que han suscrito y ratificado el Convenio de Budapest, siendo Brasil el último de ellos. Por otro lado, Ecuador, Guatemala, México y Uruguay han sido invitados a firmar y se encuentran en el proceso de adoptar diferentes medidas que implementen o permitan la implementación futura del Convenio. En tanto, Bolivia, Cuba, El Salvador, Honduras, Nicaragua y Venezuela no han mostrado interés en adherirse, no han formalizado dicho interés o no han recibido la invitación del Consejo de Europa para adherirse.

El impacto del Convenio sobre Latinoamérica se suele medir a partir de su capacidad para influir en la forma cómo los países enfrentan los delitos informáticos y los delitos facilitados por la tecnología, incluso antes de iniciado el proceso de adhesión y ratificación. Sin embargo, es importante señalar que dicha influencia está atravesada por dos hechos: el primero es que ninguno de los países de la región participó en la negociación del Convenio; y el segundo es que la realidad de Latinoamérica es muy distinta a la de los miembros originales (Canadá, Estados Unidos de América, Japón y la Unión Europea).

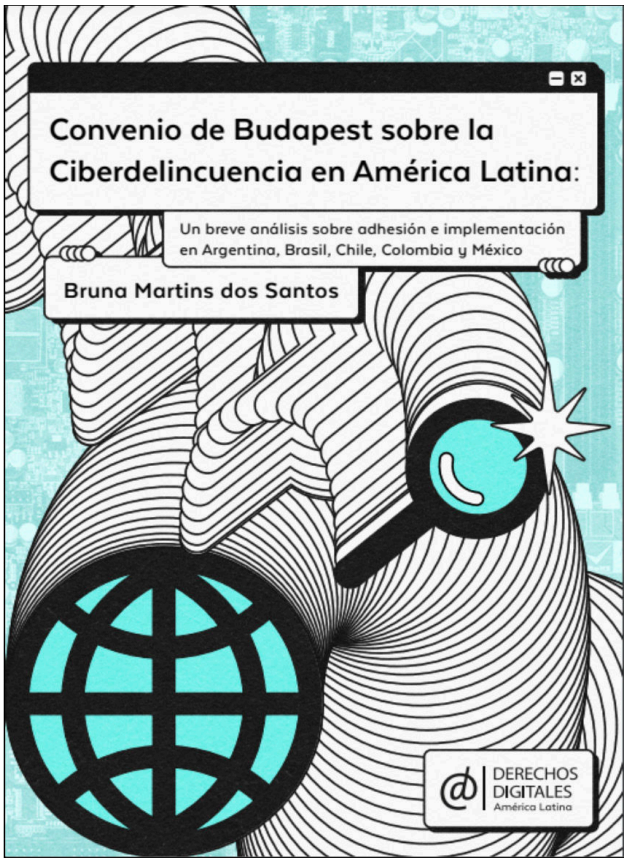
Que los países de la región no hayan participado en la negociación tiene como consecuencia directa que la forma en que la legislación penal se aplica no haya permeado el texto del Convenio, generando potenciales problemas de adaptación o la inaplicabilidad de algunos delitos o medidas procesales a nivel local. Así mismo, que las realidades entre estos y los miembros originales del Convenio sean muy diferentes en ámbitos relevantes (economía, institucionalidad, tecnología), plantea la cuestión de que, aún si se lograra la estandarización de las normas penales y los mecanismos de cooperación internacional, no está garantizado que los cambios serán efectivos y/o sostenibles en el tiempo.

8. Naciones Unidas. Resolución aprobada por la Asamblea General el 27 de diciembre de 2019: Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/32/PDF/N1944032.pdf?OpenElement

En un conjunto de ensayos sobre el futuro impacto del Convenio de Budapest en la región coordinado por Derechos Digitales durante 2018, se identificaron varios problemas comunes.[9]

El más frecuente fue la dificultad para crear o adaptar el catálogo de delitos o las medidas procesales propuestas por el Convenio, sin que esto signifique un menoscabo de los principios y garantías de derechos humanos. Un reporte más reciente de 2022 promovido por la misma organización acerca del proceso de implementación refuerza las conclusiones de los trabajos anteriores y añade un problema adicional; la celeridad y poca transparencia de las reformas legislativas e institucionales que se vienen realizando.[10]

En dos estudios de 2016 y 2020 sobre la ciberseguridad en América Latina y el Caribe, el Banco Interamericano de Desarrollo (BID) en conjunto con la Organización de Estados Americanos (OEA) analizaron a los países según su nivel de desarrollo. El reporte de 2016 identificó que la mayoría de países de Latinoamérica presentaban un importante atraso en todos los indicadores evaluados.



En la revisión de 2020 el panorama general había mejorado, especialmente el indicador de Marcos Legales, algo atribuido al impacto del Convenio de Budapest, aún en aquellos países no adherentes. Sin embargo, la falta de capacidades en ciberseguridad se citó como un obstáculo para lograr mayores avances.[12]

Mediciones internacionales como el Global Cybersecurity Index de la Unión Internacional de Telecomunicaciones (UIT)[13] y el National Cybersecurity Index de la organización e-Governance Academy (eGA)[14] consideran la adhesión al Convenio de Budapest como una medida que en sí misma representa un avance y mejora la puntuación del país evaluado. Esto se debe a que parece haber consenso en que las obligaciones derivadas del Convenio estimulan la creación de legislación penal efectiva para combatir los ciberdelitos; propician la modernización de las instituciones de justicia; y ayudan a crear o actualizar los mecanismos de cooperación para las investigaciones y operaciones internacionales.

9. Derechos Digitales. Ensayos del Grupo de trabajo sobre ciberseguridad en América Latina. Disponibles en: https://www.derechosdigitales.org/?s=budapest
10. Bruna Martins dos Santos. Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf
11. BID y OEA. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (Informe Ciberseguridad 2016). Disponible en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf
12. BID y OEA. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe
13. UIT. Global Cybersecurity Index. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
14. e-Governance Academy. National Cybersecurity Index. Disponible en: https://ncsi.ega.ee/

Teniendo en cuenta que la mayoría de países de Latinoamérica se han adherido muy recientemente al Convenio, todavía faltan muchos años para poder calibrar mejor su influencia en la región. Sin embargo, de la información que existe actualmente sobre los procesos de adecuación y el estado general de la ciberseguridad es posible concluir que los próximos años serán claves para identificar y prevenir posibles impactos negativos, particularmente en los derechos humanos y la sostenibilidad de las reformas.

IV. ANÁLISIS DEL IMPACTO DEL CONVENIO DE BUDAPEST EN CENTROAMÉRICA

En esta sección, se presenta un análisis sobre el impacto del Convenio de Budapest en 4 países de la subregión de Centroamérica: Costa Rica, Guatemala, Panamá y República Dominicana. Este análisis está estructurado a partir de tres dimensiones; el contexto previo, el proceso de adhesión y la implementación del Convenio. Se adiciona un cuadro resumen al final de cada país analizado.

1. COSTA RICA

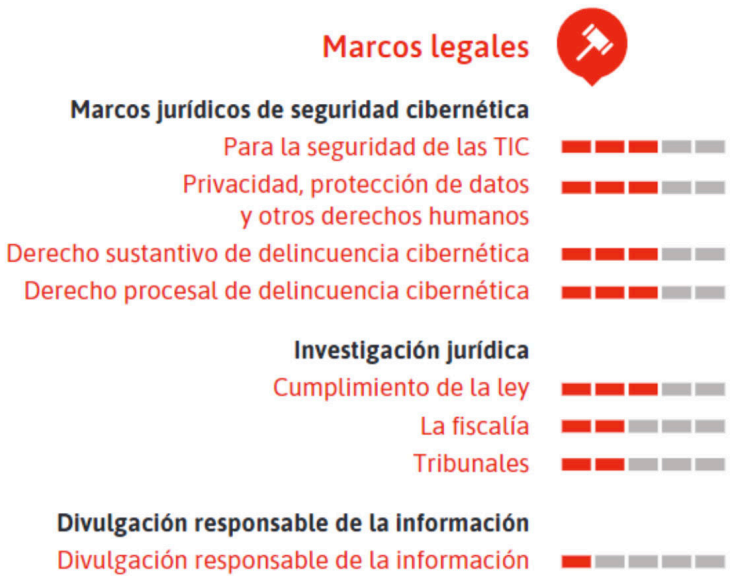
Costa Rica es un país de la subregión de Centroamérica con un sistema de gobierno presidencialista y unitario. Posee una población de aproximadamente 5.139.053 personas. El porcentaje de penetración de Internet se sitúa en más del 81%.[15]

1.1 CONTEXTO PREVIO

Según el reporte Centroamérica Cibersegura de 2020, de forma previa a la adhesión al Convenio de Budapest, Costa Rica ya había llevado a cabo múltiples reformas de carácter legal, técnicas y organizativas en materia de ciberseguridad.[16] Respecto de las reformas legales, en 2001 se aprobó la Ley N° 8148 que incluyó por primera vez en el Código Penal los delitos de violación de comunicaciones electrónicas (196 bis), estafa o fraude informático (217 bis) y alteración de datos y sabotaje Informático (229 bis). Años después, en 2012 la Ley N° 9048 modificó los delitos de corrupción (167), violación de correspondencia o comunicaciones (196), violación de datos personales (196 bis), extorsión (214), estafa informática (217 bis), daño informático (229 bis) y espionaje (288). También creó los delitos de suplantación de identidad (230), espionaje informático (231), instalación o propagación de programas informáticos maliciosos (232), suplantación de páginas electrónicas (233), facilitación del delito informático (234), narcotráfico y crimen organizado (235) y difusión de información falsa (236).

En el reporte de 2016 coordinado por el BID y la OEA sobre el estado de la ciberseguridad en América Latina y el Caribe, es posible destacar que Costa Rica presentaba un estado relativamente avanzado en el indicador de Marcos Legales, constituido principalmente por legislación penal en materia de delitos informáticos y efectividad de los actores del sistema de justicia. En 5 de los 8 subindicadores se encontraba en la categoría de "establecido", en 2 de ellos en la categoría de "formativo" y solo 1 en la categoría de "inicial".[17]

15. Banco Mundial. Estadísticas de personas que usan Internet. Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USERZS?end=2020&start=2020&view=map
16. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf
17. Estas clasificaciones, que se utilizarán a lo largo de esta sección, corresponden al "Modelo de Madurez de la Capacidad de Ciberseguridad" desarrollado por la Universidad de Oxford y aplicado en los reportes 2016 y 2020 del BID y la OEA. De menor a mayor desarrollo estas clasificaciones son: "Inicial", "Formativo", "Establecido", "Estratégico" y "Dinámico".



En cuanto al nivel de desarrollo técnico, en 2010 se creó la Comisión Nacional de Seguridad en Línea (CNSL), encargada de diseñar políticas para el buen uso del Internet y las tecnologías digitales. Además, en 2012 entró en operaciones el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR).

Fuente: Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016 (BID/OEA)

Pese a estos avances, el reporte del BID/OEA de 2016 destacó que si bien se estaba extendiendo el uso de normativas ISO, como la ISO/IEC 27001 sobre Sistemas de Gestión de Seguridad de la Información (SGSI), la adopción de las mismas no era frecuente. Todos estos factores hacían que casi todos los subindicadores del indicador Tecnologías estuviera clasificado como “formativo”.

Finalmente, a nivel organizativo, gran parte de las iniciativas en materia de ciberseguridad fueron lideradas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), incluyendo la redacción de la Estrategia Nacional de Ciberseguridad publicada en 2017.[18] Para el reporte del BID/OEA, el contar con una entidad ejerciendo el liderazgo de manera sostenida permitiría en el futuro una producción de políticas públicas coherentes y con capacidad de alcanzar a todos los actores tanto del sector público como privado.

1.2 PROCESO DE ADHESIÓN

Según consta en los archivos de la Asamblea de Costa Rica, este país fue invitado a adherirse al Convenio de Budapest en 2007. Tras dicha invitación, en 2012 el Poder Ejecutivo presentó ante la Asamblea el Proyecto de Ley N° 18484, Aprobación de la adhesión al Convenio sobre la ciberdelincuencia, dando inicio a su trámite legislativo. En la Exposición de Motivos del proyecto se señaló que la adhesión era necesaria para combatir los delitos informáticos ya que impulsará cambios necesarios en la legislación penal costarricense.

18. MICITT. Estrategia Nacional de Ciberseguridad de Costa Rica. Disponible en: https://www.micitt.go.cr/wp-content/uploads/2022/05/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-Oficial.pdf

Es interesante observar que uno de los argumentos que sostienen dicha necesidad es la reiterada negativa de los Estados Unidos de América a negociar un Convenio interamericano sobre ciberdelincuencia al interior de la OEA.[19]

Entre 2012 y 2016, el proyecto pasó por sucesivos períodos de revisión y solicitud de opiniones a diferentes actores, entre ellos la Cámara de Tecnologías de Información y Comunicación-CAMTIC, perteneciente al sector privado. Durante este tiempo, se produjeron las reformas del Código Penal a partir de la Ley N° 9048, así como la creación del CSIRT-CR. Finalmente, en 2017 la Asamblea aprobó la propuesta, que en su texto final había incorporado dos declaraciones interpretativas sobre los artículos 10 y 24 del Convenio relacionados al uso de obras protegidas por derechos de autor y la extradición de nacionales, respectivamente.

Este estudio no ha encontrado información públicamente disponible sobre reacciones negativas o posturas críticas sobre la adhesión de este país al Convenio. Sin embargo es posible presumir la existencia de condiciones para un diálogo abierto y participativo, no sólo debido al tiempo transcurrido entre la presentación de la propuesta por parte del Ejecutivo y su aprobación en la Asamblea, sino a que iniciativas similares en ese período como la Estrategia Nacional de Ciberseguridad de 2017 del MICITT contaron con procesos abiertos de consulta pública.

1.3 IMPLEMENTACIÓN

Oficialmente, Costa Rica se convirtió en miembro del Convenio de Budapest en el año 2017. En el año 2018, fue elegido como beneficiario del Programa GLACY+, una iniciativa de apoyo del Consejo de Europa para la implementación del Convenio.

Como parte del programa, se realizó un análisis de la situación del país y se identificaron objetivos de trabajo prioritarios. Una de las conclusiones de este ejercicio fue la necesidad de "(...) promover la coherencia en la legislación sobre ciberdelincuencia y evidencia electrónica armonizando las disposiciones nacionales con las disposiciones del Convenio de Budapest, el estado de derecho y los derechos humanos, incluidas las normas de protección de datos"[20]

Siempre en el marco de GLACY+, durante los siguientes años Costa Rica ha sido parte de diferentes talleres organizados por el Consejo de Europa para crear capacidades entre los actores del sistema de justicia. En la misma línea de esfuerzos, en 2018 se propuso el Proyecto de Ley N° 21187, Ley para combatir la ciberdelincuencia, que se sustenta en la implementación del Convenio e incluye acciones como la creación de una Comisión Nacional de Lucha contra la Ciberdelincuencia, la elaboración de una Estrategia Nacional de Lucha contra la Ciberdelincuencia, así como nuevas modificaciones al Código Penal. Dicha iniciativa actualmente sigue pendiente de discusión en la Asamblea.

19. Revisar el Expediente Digital de la Ley N° 9452 en el repositorio de la Asamblea. Disponible en: http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaLeyes.aspx
20. Consejo de Europa. Reporte de actividades realizadas en el marco del Proyecto GLACY+ en Costa Rica. Disponible en: https://rm.coe.int/reporte-actividades-en-costa-rica-glacy-/16808f231e

En el reporte de 2020 del BID/OEA se verifica una mejora de Costa Rica en todos los indicadores, siendo que en los de Política y Estrategia, Marcos Legales y Cultura Cibernética y Sociedad, la mejora podría atribuirse al impacto de la adhesión al Convenio de Budapest. Pese a ello y a esfuerzos específicos desarrollados en el marco de GLACY+, el indicador de Tecnologías sigue presentando poco avance, manteniéndose casi todos los subindicadores en la categoría de "inicial". La conclusión del reporte que señala que las infraestructuras digitales y la adopción de estándares de seguridad son débiles en Costa Rica es consistente con los devastadores ataques de ransomware que ha sufrido este país recientemente.[21]

Cabe resaltar que en mayo de 2022 se abrió a firma el Segundo Protocolo Adicional al Convenio, que busca ser una base legal para mejorar la cooperación y divulgación de evidencia electrónica entre los países miembros.

A diferencia del Convenio, este nuevo protocolo ha suscitado reacciones críticas desde la sociedad civil, que ve con preocupación que las nuevas disposiciones debiliten las protecciones existentes sobre derechos como la privacidad y habiliten un uso desproporcionado de la información obtenida durante las investigaciones. No obstante, en junio de ese mismo año Costa Rica firmó el protocolo sin reservas.[22]

Fuente: Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. (BID/OEA)

1.4 CUADRO DE RESUMEN

COSTA RICA	
¿El país ha firmado y ratificado el Convenio de Budapest?	Sí, el país ha firmado y ratificado el Convenio de Budapest en 2017.
¿Presentó reservas u otras observaciones?	Sí, presentó dos observaciones interpretativas sobre los artículos 10 y 24 del Convenio de Budapest.
¿Se han presentado normas para la implementación?	Sí, se ha presentado el Proyecto de Ley N° 21187, Ley para combatir la ciberdelincuencia.
¿Ha firmado el Segundo Protocolo Adicional?	Sí, se firmó en 2022 sin reservas.

21. BBC News. "Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-61516874
22. Electronic Frontier Foundation (EFF) y AlSur. Evaluando el nuevo protocolo al convenio sobre ciberdelincuencia en América Latina. Disponible en: https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam-es.pdf
23. Banco Mundial. Estadísticas de personas que usan Internet. Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=map
24. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf

2. GUATEMALA

Guatemala es un país de la subregión de Centroamérica con un sistema de gobierno republicano, democrático, representativo y organizado. Posee una población de aproximadamente 17.109.746 personas. El porcentaje de penetración de Internet se sitúa en más del 51%.[23]

2.1 CONTEXTO PREVIO

Según el reporte Centroamérica Cibersegura de 2020, Guatemala ha implementado muy pocas reformas de carácter legal, técnicas y organizativas en materia de ciberseguridad y actualmente no es parte del Convenio de Budapest.[24]

Respecto de las reformas legales, a través del Decreto 33-96 de 1996 se introdujo en el Código Penal los delitos informáticos de destrucción de registros informáticos (274-A), alteración de programas (274-B), reproducción de instrucciones o programas de computación (274-C), registros prohibidos (274-D), manipulación de información (274-E), uso de información (274-F) y programas destructivos (274-G). Sin embargo, debido a la ambigüedad de su redacción y a su desfase progresivo, no parecen haber sido efectivos. El reporte de 2016 del BID/OEA coincide con esta apreciación cuando señala sobre Guatemala que "(...) hasta que no se cuente con una legislación integral sobre delincuencia cibernética, el sistema judicial tendrá dificultades para procesar los casos eficazmente".

En cuanto al nivel de desarrollo técnico, durante 2006 diferentes entidades del sector público y privado unieron esfuerzos para poner en funcionamiento un Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-GT).[25] Lamentablemente esta iniciativa, que habría operado de manera ad hoc por un tiempo, finalmente se desactivó al no contar con un marco legal adecuado ni recursos, dejando al país sin un CSIRT público hasta la actualidad. A esto hay que añadir que el nivel de adopción de medidas de seguridad de la información también es bajo, en todos los sectores.

Finalmente, a nivel organizativo, no existe una entidad que dirija los esfuerzos en materia de ciberseguridad, sino un conjunto de entidades que actúan en función a competencias directa o indirectamente relacionadas. Por ejemplo, está el IV Viceministerio de Tecnologías de Información y Comunicaciones que ha llevado a cabo diferentes planes y estrategias de digitalización, incluyendo la Estrategia Nacional de Seguridad Cibernética de 2018. También se encuentra el Ministerio de Defensa que sostuvo la iniciativa CSIRT-GT durante su breve período de existencia.

Estas carencias institucionales se reflejan en la baja calificación del reporte 2016 del BID/OEA en el indicador de Política y Estrategia en donde se aprecia que todos los subindicadores se encuentran en la categoría de "inicial".[27]

25. UIT. 4a sesión–Vigilancia Vigilancia, precaución y respuesta respuesta a incidentes: Taller Regional sobre Marcos para la Ciberseguridad y la Protección de la Infraestructura básica de la Información (Presentación CSIRT-GT). Disponible en: https://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/clark-CSIRT-guatemala-buenos-aires-oct-07.pdf
26. Ministerio de Gobernación. Estrategia Nacional de Seguridad Cibernética. Disponible en: https://web.archive.org/web/20180731012903/https://mingob.gob.gt/wp-content/uploads/2018/06/version-digital.pdf
27. Estas clasificaciones, que se utilizarán a lo largo de esta sección, corresponden al "Modelo de Madurez de la Capacidad de Ciberseguridad" desarrollado por la Universidad de Oxford y aplicado en los reportes 2016 y 2020 del BID y la OEA. De menor a mayor desarrollo estas clasificaciones son: "Inicial", "Formativo", "Establecido", "Estratégico" y "Dinámico".

2.2 PROCESO DE ADHESIÓN

Guatemala fue invitada a adherirse al Convenio de Budapest en 2020. Tras dicha invitación, no se ha presentado ante el Congreso de la República de Guatemala ninguna iniciativa desde el Poder Ejecutivo para su ratificación. Sin embargo, esto no ha impedido que este ejerza cierta influencia en el ecosistema local. Por ejemplo, en 2017 se presentó el Proyecto de Ley N° 5254 para reformar el Código Penal en materia de delitos informáticos, tomando como referencia el texto del Convenio. Así mismo, en 2018 se presentó el Proyecto de Ley N° 5239 que, entre otras cosas, proponía la creación del delito de Terrorismo Cibernético y finalmente en 2019 también el Proyecto de Ley N° 5601 que incluía múltiples reformas a nivel legal e institucional sobre ciberdelitos.

Algunos de los proyectos anteriores recibieron comentarios por parte del Consejo de Europa a través del acercamiento entre el Programa GLACY+ y el Foro de presidentes y presidentas de Poderes Legislativos de Centroamérica y el Caribe (FOPREL), del cual es parte Guatemala.[28] De hecho, el Proyecto de Ley N° 5601, cuyo texto podría considerarse el más cercano al estándar propuesto por el Convenio de Budapest, se convirtió brevemente en ley en agosto de 2022 bajo el nombre de Decreto N° 39-2022, pero fue derogado un mes más tarde debido a fuertes protestas por parte de la sociedad civil provocadas por la posible instrumentalización de la ley como herramienta para afectar la libertad de expresión e información.[29]

2.3 IMPLEMENTACIÓN

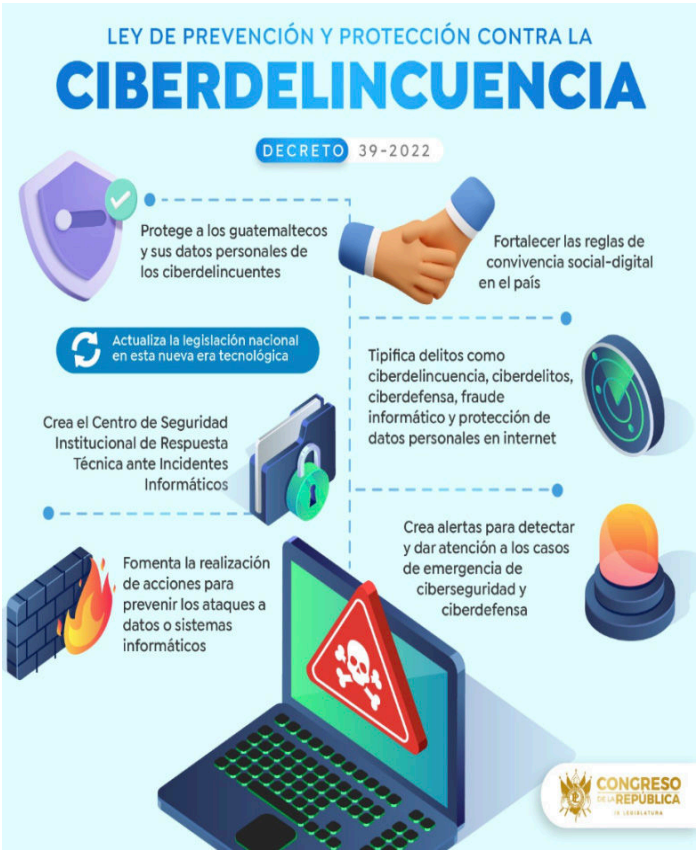
El reporte de 2020 del BID/OEA precisa que si bien desde el año 2018 Guatemala cuenta con una Estrategia Nacional de Seguridad Cibernética, se requieren reformas en todos los niveles.

Pese a ello, hasta la fecha muy pocas de las propuestas formuladas por dicha Estrategia parecen estar llevándose a cabo, salvo algunas excepciones como es el caso de la creación del Comité Nacional de Seguridad Cibernética (CONCIBER) llevada a cabo en 2021, que está a cargo de la Secretaría de Inteligencia Estratégica del Estado.

Es posible afirmar que si Guatemala finalmente ratifica el Convenio de Budapest y eventualmente hace lo mismo con sus protocolos adicionales, el camino de la implementación en el país será costoso y accidentado. Costoso porque el país presenta mucho atraso en todos los indicadores evaluados por los reportes del BID/OEA, entre los que se encuentran varios directamente ligados a la adecuación y efectividad exigida por el Convenio.

Accidentado porque la urgencia de llevar a cabo las reformas podría provocar que los espacios de discusión legislativa se limiten o sean de plano inexistentes, provocando situaciones como la que desencadenó la derogación del Decreto N° 39-2022.

28. FOPREL. Misión Consultiva y Taller de Trabajo sobre ciberdelito y prueba electrónica y la implementación del Convenio de Budapest en los países que forman parte del FOPREL. Disponible en: https://foprel.digital/wp-content/uploads/2022/04/07-REPORTE-CIBERDELITO-GLACY.pdf
29. Prensa Libre. Congreso oficializa que se archiva el decreto 39-2022 que contenía la Ley contra la ciberdelincuencia. Disponible en: https://www.prensalibre.com/guatemala/politica/congreso-oficializa-que-se-archiva-el-decreto-39-2022-que-contenia-la-ley-contra-la-ciberdelincuencia-breaking/



Fuente: Congreso de la República de Guatemala

2.3 CUADRO DE RESUMEN

GUATEMALA	
¿El país ha firmado y ratificado el Convenio de Budapest?	No, el país ha sido invitado a firmar en 2020, pero todavía no formaliza la firma y ratificación.
¿Presentó reservas u otras observaciones?	No, hasta que no se produzca la firma y ratificación, no se sabe si se presentarán reservas u observaciones
¿Se han presentado normas para la implementación?	Sí, se han presentado los Proyectos de Ley N° 5254 de 2017, N° 5239 de 2018 y N° 5601 de 2019 (actualmente archivado).
¿Ha firmado el Segundo Protocolo Adicional?	No, pues no se ha firmado y ratificado el tratado principal.

3. PANAMÁ

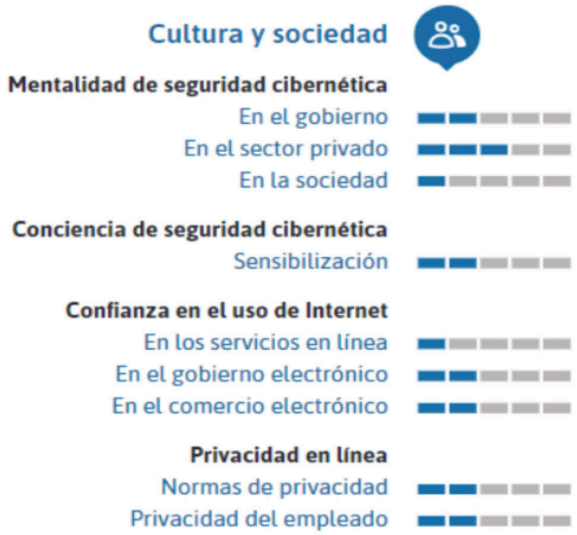
Panamá es un país de la subregión de Centroamérica con un sistema de gobierno unitario, republicano, democrático y representativo. Posee una población de aproximadamente 4.381.583 personas. El porcentaje de penetración de Internet se sitúa en más del 64%.[30]

3.1 CONTEXTO PREVIO

Según el reporte Centroamérica Cibersegura de 2020, de forma previa a la adhesión al Convenio de Budapest, Panamá ya había llevado a cabo múltiples reformas de carácter legal, técnicas y organizativas en materia de ciberseguridad.[31]

Respecto de las reformas legales, se aprobó un nuevo Código Penal mediante la Ley N° 14 del 18 de mayo de 2007, que incluyó modificaciones para sancionar el uso de medios informáticos como en los delitos contra el honor (195), agravantes del hurto (214), estafa y otros fraudes (220 y 226), daños (236), delitos financieros (243), revelación de secretos empresariales (288), delitos de contrabando y defraudación aduanera (288-C), así como la creación de una sección específica de delitos informáticos contenida en el Título VIII bajo el nombre de Delitos contra la Seguridad Jurídica de los Medios Electrónicos (289 al 292).

En el reporte de 2016 del BID/OEA se destaca el avance de Panamá en diferentes indicadores, especialmente en el de Cultura y Sociedad.



En cuanto al nivel de desarrollo técnico, mediante el Decreto Ejecutivo N° 709 del 26 de septiembre de 2011 se creó el Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño (CSIRT-Panamá) bajo la supervisión de la Autoridad Nacional para la Innovación Gubernamental (AIG). No obstante, el reporte del BID/OEA de 2016 señaló en su evaluación que la adopción de estándares de seguridad y el nivel de coordinación entre los actores todavía era bajo, siendo que la mayoría de subindicadores del indicador Tecnología se encontraban en la categoría de "inicial".[32]

30. Banco Mundial. Estadísticas de personas que usan Internet. Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=map
31. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf
32. Estas clasificaciones, que se utilizarán a lo largo de esta sección, corresponden al "Modelo de Madurez de la Capacidad de Ciberseguridad" desarrollado por la Universidad de Oxford y aplicado en los reportes 2016 y 2020 del BID y la OEA. De menor a mayor desarrollo estas clasificaciones son: "Inicial", "Formativo", "Establecido", "Estratégico" y "Dinámico".

Finalmente, a nivel organizativo, en el año 2013, la AIG promovió la publicación de la primera Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica, un documento guía compuesto por 36 tareas distribuidas en seis pilares fundamentales, efectiva mediante Resolución N° 21 de 2013.[33] Uno de estos pilares fue el de "prevenir y detener las conductas delictivas en el ciberespacio o el uso de este para cualquier tipo de delitos o actos ilícitos".

3.2 PROCESO DE ADHESIÓN

Según los archivos de la Asamblea Nacional de Panamá, en 2013 el Poder Ejecutivo presentó el Proyecto de Ley N° 595, dando inicio a su trámite legislativo.[34] La aprobación por parte de la Asamblea se logró el mismo año y no implicó la formulación de reservas ni observaciones, siendo finalmente promulgado bajo la Ley N° 79 del 22 de octubre 2013, Por la cual se aprueba el Convenio sobre la Ciberdelincuencia, hecho en Budapest, el 23 de noviembre de 2001. Este estudio no ha encontrado información públicamente disponible sobre reacciones negativas o posturas críticas sobre la adhesión de este país al Convenio. Sin embargo, debido al corto tiempo entre la presentación de la propuesta por el Ejecutivo y su aprobación en la Asamblea, es posible que los espacios de diálogo hayan sido limitados.

3.3 IMPLEMENTACIÓN

Oficialmente, Panamá se convirtió en miembro del Convenio de Budapest en el año 2014. A partir de esa fecha, se han presentado hasta cuatro iniciativas en la Asamblea Nacional de Diputados con el fin de implementar el Convenio. Las más recientes son el Proyecto de Ley N° 558 de 2017, Que modifica y adiciona artículos al Código Penal, relacionados con el cibercrimen, presentado por el Ministerio Público y el Proyecto de Ley N° 555 de 2021, Que crea la Unidad Policial especializada en delitos informáticos en la República de Panamá y modifica el Código Penal. Actualmente ambas siguen pendientes de discusión en la Asamblea.

En el reporte de 2020 del BID/OEA se verifica una mejora de Panamá en la mayoría de indicadores, con la excepción del indicador de Formación, Capacitación y Habilidades de Seguridad Cibernética, que no ha avanzado significativamente desde 2016. A propósito de ello, a través de la Resolución N° 17 del 10 de septiembre de 2021 se aprobó la Estrategia Nacional de Ciberseguridad para el período 2021-2024 que contiene varias propuestas para mejorar la oferta educativa en ciberseguridad.[35] Finalmente, si bien Panamá no forma parte del grupo de países del Programa GLACY+, en años recientes se han producido diferentes talleres organizados por el Consejo de Europa para evaluar la situación del país y asesorar la implementación del Convenio.[36]

33. Consejo Nacional para la Innovación Gubernamental. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica. Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf
34. Asamblea Nacional. Acta N° 3 Comisión de Relaciones Exteriores, correspondiente al 27 de agosto de 2013. Disponible en: https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_ACTAS/2010_ACTAS/2013_ACTAS/2013_ACTAS_COMISION/2013_COMISION/2013_08_27_A_COMI_RELACIONES.pdf
35. Consejo Nacional para la Innovación Gubernamental. Estrategia Nacional de Ciberseguridad para el período 2021-2024. Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/29434_A/88864.pdf
36. Consejo de Europa. Panama and the Convention on Cybecrime: GLACY+ workshop on domestic legislation. Disponible en: https://www.coe.int/en/web/cybercrime/-/panama-and-the-convention-on-cybecrime-glacy-workshop-on-domestic-legislation

Cabe resaltar que en mayo de 2022 se abrió a firma el Segundo Protocolo Adicional al Convenio, que busca ser una base legal para mejorar la cooperación y divulgación de evidencia electrónica entre los países miembros.

A diferencia del Convenio, este nuevo protocolo ha suscitado reacciones críticas desde la sociedad civil, que ve con preocupación que las nuevas disposiciones debiliten las protecciones existentes sobre derechos como la privacidad y habiliten un uso desproporcionado de la información obtenida durante las investigaciones.[37] Panamá todavía no ha firmado el nuevo protocolo.

3.4 CUADRO DE RESUMEN

PANAMÁ	
¿El país ha firmado y ratificado el Convenio de Budapest?	Sí, el país ha firmado y ratificado el Convenio de Budapest en 2014.
¿Presentó reservas u otras observaciones?	No, no presentó reservas ni observaciones.
¿Se han presentado normas para la implementación?	Sí, se han presentado los Proyectos de Ley N° 558 de 2017, Que modifica y adiciona artículos al Código Penal, relacionados con el cibercrimen, presentado por el Ministerio Público y el Proyecto de Ley N° 555 de 2021, Que crea la Unidad Policial especializada en delitos informáticos en la República de Panamá y modifica el Código Penal.
¿Ha firmado el Segundo Protocolo Adicional?	No, no se ha firmado todavía.

4. REPÚBLICA DOMINICANA

República Dominicana es un país de la subregión de Centroamérica con un sistema de gobierno presidencialista y representativo. Posee una población de aproximadamente 10.953.714 personas. El porcentaje de penetración de Internet se sitúa en más del 77%.[38]

37. Electronic Frontier Foundation (EFF) y AlSur. Evaluando el nuevo protocolo al convenio sobre ciberdelincuencia en América Latina. Disponible en: https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam-es.pdf
38. Banco Mundial. Estadísticas de personas que usan Internet (2020). Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=map
39. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf

4.1 CONTEXTO PREVIO

Según el reporte Centroamérica Cibersegura de 2020, de forma previa a la adhesión al Convenio de Budapest, República Dominicana ya había llevado a cabo múltiples reformas de carácter legal, técnicas y organizativas en materia de ciberseguridad.[39] Respecto de las reformas legales, en el año 2007 se aprobó la Ley N° 53-07 sobre Crímenes y Delitos de Alta Tecnología cuyo objetivo fue prevenir y sancionar los delitos informáticos y los delitos facilitados por la tecnología, como los delitos de códigos de acceso (5), acceso Ilícito (6), acceso Ilícito para servicios a terceros (7), dispositivos fraudulentos (8), interceptación e lintervención de datos o señales (9), daño o alteración de datos (10), sabotaje (11), atentado contra la vida de la persona (12), robo mediante la utilización de alta tecnología (13), obtencion ilicita de fondos (14), estafa (15), chantaje (16), robo de identidad (17), de la falsedad de documentos y firmas (18), uso de equipos para invasion de privacidad (19), comercio ilícito de bienes y servicios (20), difamación (21), injuria pública (22), atentado sexual (23), pornografía infantil (24), delitos relacionados a la propiedad intelectual y afines (25), delitos de telecomunicaciones (26), crimenes y delitos contra la Nacion (27) y actos de terrorismo (29). Además se establecen medidas de carácter procesal y reorganiza las funciones de diferentes entidades del sector público.

En el reporte de 2016 coordinado por el BID y la OEA sobre el estado de la ciberseguridad en América Latina y el Caribe, se observa que República Dominicana presenta un alto nivel de desarrollo en el indicador de Marcos Legales, constituido principalmente por legislación penal en materia de delitos informáticos y efectividad de los actores del sistema de justicia. En comparación con los otros países analizados en este reporte, es el único que posee 4 subindicadores en las categorías de “Estratégico” y “Dinámico”.[40] Esto se debería a que la Ley N° 53-07 habría adoptado gran parte de las propuestas del Convenio de Budapest.

En cuanto al nivel de desarrollo técnico, a partir de la Ley N° 53-07 se creó la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT), el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), y la División de Investigaciones de Delitos Informáticos (DIDI). Hasta la creación del CSIRT nacional, la DICAT operó de manera ad hoc como entidad coordinadora de la respuesta a incidentes de ciberseguridad. Sin embargo, según el reporte del BID/OEA de 2016 la adopción de estándares de seguridad de la información y otras medidas era bajo en el sector público. Finalmente, a nivel organizativo, gran parte de las iniciativas en materia de ciberseguridad fueron lideradas por diferentes entidades en el ámbito de sus competencias.

Entre ellas se encuentran los miembros del CICDAT; el Ministerio Público, Ministerio de Defensa, Ministerio de Interior y Policía, la Policía Nacional, la Dirección Nacional de Control de Drogas (DNCD), el Departamento Nacional de Investigaciones (DNI), el Instituto Dominicano de las Telecomunicaciones (INDOTEL), la Superintendencia de Bancos de la República Dominicana, el Consejo Nacional para la Niñez y la Adolescencia (CONANI), y el Instituto Tecnológico de las Américas (ITLA). Posteriormente a estas entidades se sumaría la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC).

37. Electronic Frontier Foundation (EFF) y AlSur. Evaluando el nuevo protocolo al convenio sobre ciberdelincuencia en América Latina. Disponible en: https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam-es.pdf
38. Banco Mundial. Estadísticas de personas que usan Internet (2020). Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=map
39. IPANDETEC. Centroamérica Cibersegura. Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf

4.2 PROCESO DE ADHESIÓN

Según consta en los archivos del Congreso Nacional de República Dominicana, este país fue invitado a adherirse al Convenio de Budapest en 2008, una acción previsible luego de la reforma dispuesta por la Ley N° 53-07. Cuatros años después, mediante Resolución N° 158-12 de 2012, el Congreso ratificó la adhesión sin reservas ni observaciones. También durante 2012 se aprobó mediante la Ley N° 1-12, la Estrategia Nacional de Desarrollo 2030, cuyo artículo 16 estableció que las políticas públicas deberán tener en cuenta la promoción del uso de las tecnologías de información y comunicación.[41] Este estudio no ha encontrado información públicamente disponible sobre reacciones negativas o posturas críticas sobre la adhesión de este país al Convenio. Sin embargo es posible presumir la existencia de condiciones para un diálogo abierto y participativo, no sólo debido al tiempo transcurrido entre la presentación de la propuesta por parte del Ejecutivo y su aprobación en el Congreso, sino a que iniciativas similares en ese período como la Estrategia Nacional de Desarrollo 2030 y otras de similar naturaleza contaron con procesos abiertos de consulta pública.

4.3 IMPLEMENTACIÓN

Oficialmente, República Dominicana se convirtió en miembro del Convenio de Budapest en 2013. A partir de allí, ocurrieron varios hechos importantes. En 2016 el país fue elegido como beneficiario del Programa GLACY+, una iniciativa de apoyo para la implementación del Convenio. Como parte del programa, se realizó un análisis de la situación del país y se identificaron objetivos de trabajo prioritarios.[42] Ese mismo año, el INDOTEL empezó la redacción de una Estrategia Nacional de Ciberseguridad. Finalmente, mediante el Decreto Nº 258/2016 se lanzó el Proyecto República Digital que contenía disposiciones sobre ciberseguridad.[43]

En 2018 se produjo una nueva sucesión de hitos relevantes. En 2018, mediante Decreto N° 230-18, se aprobó la Estrategia Nacional de Ciberseguridad 2018-2021 trabajada por INDOTEL cuya participación fue abierta y pública.[44] En aplicación de dicha estrategia se produjo la creación de nuevas entidades con competencias en materia de ciberseguridad, entre ellas el Centro Nacional de Ciberseguridad (CNCS) y el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD). En 2022, se publicó mediante Decreto N° 313-22 una nueva versión bajo el nombre de Estrategia Nacional de Ciberseguridad 2030 que amplía aún más el ecosistema de ciberseguridad, incluyendo medidas específicas para prevenir y sancionar los ciberdelitos.[45]

40. Estas clasificaciones, que se utilizarán a lo largo de esta sección, corresponden al "Modelo de Madurez de la Capacidad de Ciberseguridad" desarrollado por la Universidad de Oxford y aplicado en los reportes 2016 y 2020 del BID y la OEA. De menor a mayor desarrollo estas clasificaciones son: "Inicial", "Formativo", "Establecido", "Estratégico" y "Dinámico".
41. Ministerio de Economía, Planificación y Desarrollo. Estrategia Nacional de Desarrollo 2030. Disponible en: https://mepyd.gob.do/mepyd/wp-content/uploads/archivos/end/marco-legal/ley-estrategia-nacional-de-desarrollo.pdf
42. Diario Libre. Incorporarán a Dominicana al proyecto GLACY +. Disponible en: https://www.diariolibre.com/actualidad/tecnologia/incorporaran-a-dominicana-al-proyecto-glacy-HE5006801
43. Consejo de Europa. Accesión de la República Dominicana al Convenio del Consejo de Europa sobre ciberdelincuencia (CONVENIO DE BUDAPEST/ETS-185). Disponible en: https://rm.coe.int/3148-1-1-3-cy-caribbean-3-9h00-domrep-bc-c-peguero/168094f062
44. Presidencia de República Dominicana. Estrategia Nacional de Ciberseguridad 2018-2021. Disponible en: https://cncs.gob.do/wp-content/uploads/2020/02/Decreto-230-18.pdf
45. Presidencia de República Dominicana. Estrategia Nacional de Ciberseguridad 2030. Disponible en: https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

Entre la ratificación del Convenio de Budapest y la actualidad, además de las reformas señaladas anteriormente, no se han producido otras reformas importantes sino hasta muy poco, cuando el Poder Ejecutivo presentó en junio de 2022 un proyecto de ley contra la ciberdelincuencia, con el que buscaba reformar completamente la Ley N° 53-07 de 2007, incluyendo la creación de nuevos delitos y desarrollando las competencias de diferentes entidades como el DICAT, la DIDI y el CNCS.[46] Sin embargo, días después, el Ejecutivo retiró el proyecto debido a críticas recibidas por posibles vulneraciones a la libertad de expresión en el texto de la iniciativa.[47] Mientras se define la situación de dicha iniciativa, en junio de 2022 se aprobó la Estrategia Nacional de Ciberseguridad 2030 ya mencionada y en noviembre el Decreto 685-22 que establece las medidas de notificación obligatoria de incidentes e intercambio de inteligencia de amenazas.

Cabe resaltar que en mayo de 2022 se abrió a firma el Segundo Protocolo Adicional al Convenio, que busca ser una base legal para mejorar la cooperación y divulgación de evidencia electrónica entre los países miembros.

A diferencia del Convenio, este nuevo protocolo ha suscitado reacciones críticas desde la sociedad civil, que ve con preocupación que las nuevas disposiciones debiliten las protecciones existentes sobre derechos como la privacidad y habiliten un uso desproporcionado de la información obtenida durante las investigaciones.[48] No obstante, en enero de 2023 República Dominicana firmó el protocolo sin reservas.

4.4 CUADRO DE RESUMEN

REPÚBLICA DOMINICANA	
¿El país ha firmado y ratificado el Convenio de Budapest?	Sí, el país ha firmado y ratificado el Convenio de Budapest en 2013.
¿Presentó reservas u otras observaciones?	No, no presentó reservas ni observaciones.
¿Se han presentado normas para la implementación?	Sí, en 2022 se presentó un Proyecto de Ley sobre ciberdelincuencia, pero luego se retiró.
¿Ha firmado el Segundo Protocolo Adicional?	No, no se ha firmado todavía.

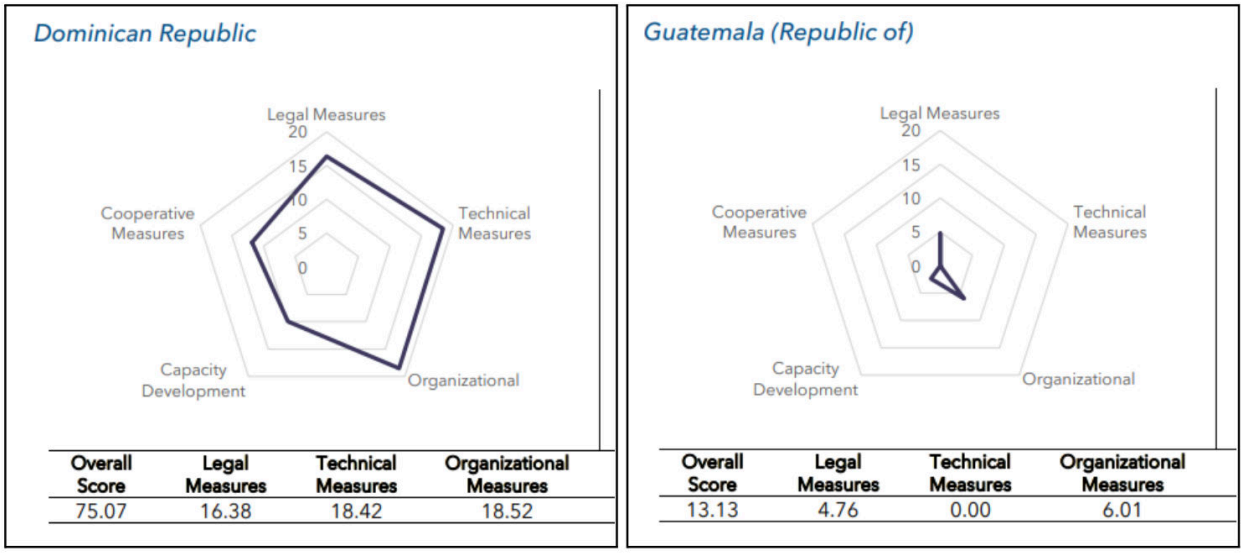
46. DPL News. República Dominicana | El Poder Ejecutivo somete proyecto de ley contra la ciberdelincuencia. Disponible en: https://dplnews.com/republica-dominicana-el-poder-ejecutivo-somete-proyecto-de-ley-contra-la-ciberdelincuencia/
47. Sociedad Interamericana de Prensa. Preocupa a la SIP auge de proyectos anti libertad de prensa en República Dominicana. Disponible en: https://www.sipiapa.org/notas/1215241-preocupa-la-sip-auge-proyectos-anti-libertad-prensa-republica-dominicana
48. Electronic Frontier Foundation (EFF) y AlSur. Evaluando el nuevo protocolo al convenio sobre ciberdelincuencia en América Latina. Disponible en: https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam-es.pdf

V. MÁS ALLÁ DE BUDAPEST: PERSPECTIVAS PARA CENTROAMÉRICA A PROPÓSITO DEL TRATADO SOBRE CIBERDELINCUENCIA EN LAS NACIONES UNIDAS

En esta sección, se presenta un análisis prospectivo a partir del proceso de creación de un nuevo tratado contra la ciberdelincuencia que se viene realizando al interior de las Naciones Unidas.

La creación en 2019 del Comité Intergubernamental para elaborar un tratado sobre ciberdelincuencia por parte de las Naciones Unidas representa una nueva e interesante oportunidad para los países de Centroamérica en materia de lucha contra los delitos informáticos y los delitos facilitados por la tecnología. Por un lado, será la primera vez que los países de la región participarán de la negociación de un instrumento de esta naturaleza, a diferencia de lo ocurrido con el Convenio de Budapest. Por el otro, tendrán la oportunidad de influir en el texto final, de tal manera que este refleje sus intereses.

Por supuesto, la situación anterior se verá además afectada por múltiples factores internos y externos que es preciso tener en cuenta. En el caso de los factores internos está el hecho de que, según diferentes reportes internacionales, la mayoría de los países de Centroamérica presenta un importante retraso en el desarrollo de medidas legales, técnicas y organizativas en materia de ciberseguridad, incluyendo aquellas relacionadas a la lucha contra los ciberdelitos. Estas carencias hacen suponer que su capacidad de participar e influir en la negociación será menor que la de aquellos países o bloques con mayor desarrollo, incluso dentro de la misma subregión.



Overall Score	Legal Measures	Technical Measures	Organizational Measures
75.07	16.38	18.42	18.52

Overall Score	Legal Measures	Technical Measures	Organizational Measures
13.13	4.76	0.00	6.01

Fuente: Global Cybersecurity Index 2020 (UIT)

Otro factor interno es la extrema vulnerabilidad de los gobiernos latinoamericanos frente a ciberataques que comprometen infraestructuras críticas. Esto hace prever que aquellos países que hayan experimentado casos traumáticos, tendrán una mayor propensión a exigir medidas más represivas y aceptar controles más laxos para el tratado que se está negociando. El hecho de que luego de los ataques de ransomware sufridos por el gobierno de Costa Rica, este haya suscrito el Segundo Protocolo del Convenio de Budapest casi inmediatamente y sin reservas es un ejemplo de esta situación a la que pueden verse arrojados los hacedores de política pública de otros países centroamericanos.

Entre los factores externos está la afinidad política e ideológica. En el contexto de la negociación del nuevo tratado en las Naciones Unidas, centros de poder como China, Estados Unidos de América, Rusia y la Unión Europea poseen una gran capacidad de influencia y tienen posturas encontradas sobre la lucha contra los ciberdelitos. Por ejemplo, Estados Unidos es partidario de establecer mecanismos para que los gobiernos puedan realizar solicitudes de información a empresas de otros países de manera directa en el curso de una investigación penal. En tanto, China y Rusia sostienen que el nuevo tratado debería incluir nuevos delitos, entre ellos algunos relacionados con la libertad de expresión.

Otro factor externo a tener en cuenta es la influencia de la cooperación internacional, especialmente la que se da a través de iniciativas relacionadas a la lucha contra el cibercrimen. Por ejemplo, es previsible que los países de Centroamérica que hayan suscrito y ratificado el Convenio de Budapest o sean beneficiarios de proyectos como GLACY+ tengan posiciones más afines a las de otros miembros del Convenio, especialmente los países de la Unión Europea. Algo similar en el caso de los Estados Unidos de América, respecto de aquellos países que participen activamente de los programas sobre ciberseguridad impulsados por el Comité Interamericano contra el Terrorismo (CICTE) de la OEA.

Dicho todo lo anterior y teniendo en cuenta los diferentes niveles de desarrollo en materia de ciberseguridad de los países analizados en este reporte y los demás que conforman la subregión (El Salvador, Honduras y Nicaragua), es posible afirmar que una de las claves para que Centroamérica logre influir y ver representados sus intereses el proceso de negociación del nuevo tratado pasará por el nivel de coordinación interna que puedan lograr. Escapa de este reporte profundizar qué espacios podrían ser más propicios para ello, pero a partir de esta investigación, dos buenos candidatos parecen ser el FOPREL y el Sistema de la Integración Centroamericana (SICA).

Aunque tanto el FOPREL[49] como el SICA[50] han dado algunos pasos para acoger la discusión sobre la ciberdelincuencia en Centroamérica, también se debe señalar que de momento ninguno de ellos ha sido perceptiblemente activo durante las tres rondas de negociación que ya se han realizado en las Naciones Unidas. En contraste, otros bloques como la Comunidad del Caribe (CARICOM), la Unión Europea, la Unión Africana y un conglomerado liderado por Rusia (que incluye a Bielorrusia, Burundi, China, Nicaragua y Tayikistán) han presentado múltiples documentos con observaciones y comentarios al Comité Intergubernamental encargado de elaborar el nuevo tratado.

49. FOPREL. Foro Regional de las Américas sobre la cooperación en materia de ciberdelincuencia y pruebas electrónicas. Disponible en: https://foprel.digital/foro-regional-de-las-americas-sobre-la-cooperacion-en-materia-de-ciberdelincuencia-y-pruebas-electronicas/
50. SICA. SICA: Analizan la respuesta del derecho penal frente al ciberdelito. Disponible en: https://www.sica.int/noticias/sica-analizan-la-respuesta-del-derecho-penal-frente-al-ciberdelito_1_128479.html

VI. CONCLUSIONES

En esta sección, se presentan las conclusiones del reporte, que a su vez justifican un conjunto de recomendaciones para los actores locales del ecosistema digital centroamericano, las cuales se encuentran en la siguiente sección.

1. EL IMPACTO DEL CONVENIO EN CENTROAMÉRICA ES SIGNIFICATIVO Y SEGUIRÁ CRECIENDO

El Convenio de Budapest ha generado un impacto significativo en la forma cómo los países centroamericanos enfrentan el fenómeno de la ciberdelincuencia, incluso con muchos años de anticipación al proceso de adhesión e implementación del mismo. Dicho impacto se percibe en la forma cómo se han tipificado los delitos informáticos y los delitos facilitados por la tecnología de los países analizados pues la mayoría siguen un patrón similar al propuesto por el Convenio. También en la creación de entidades públicas especializadas (CSIRTs, policías informáticas), que estudios sobre ciberseguridad como los del BID/OEA atribuyen al efecto de proyectos derivados como GLACY+, que ha llegado a interactuar con espacios de diálogo y cooperación subregionales como el FOPREL y el SICA.

Además de su influencia actual, es previsible que el Convenio de Budapest se mantenga como la referencia más importante para la subregión en los próximos años, no solo debido a que sigue siendo el único tratado de su tipo, sino también a que a lo largo de su existencia ha ejercido igual influencia en otras partes del mundo. Según un reporte del Consejo de Europa sobre el avance de las legislaciones contra los ciberdelitos publicado en 2023, aproximadamente 160 países (de un total de 193) han utilizado el Convenio como guía o fuente principal para sus procesos de reforma, aún sin ser adherentes del mismo.[51] En ese sentido, todo apunta a que su impacto seguirá creciendo, incluso en el contexto de una futura aprobación del nuevo tratado que se está negociando en las Naciones Unidas.

2. LA IMPLEMENTACIÓN DEL CONVENIO ESTÁ MUY AVANZADA EN LOS PAÍSES ANALIZADOS

Salvo Guatemala, que aún no se adhiere y está muy por detrás, los otros países centroamericanos analizados son adoptantes tempranos del Convenio, siendo la República Dominicana el primer país de la región de Latinoamérica en haberlo suscrito en 2013. Esto significa que todos ellos presentan procesos avanzados de implementación, en los cuales es posible identificar elementos comunes: La existencia de iniciativas para reformar la legislación penal sobre ciberdelincuencia; el reforzamiento de las instituciones de cooperación internacional; y la inclusión de la lucha contra los ciberdelitos como un componente importante en estrategias y planes nacionales en materia de ciberseguridad y gobierno digital.

51. Consejo de Europa. The global state of cybercrime legislation 2013 – 2023: A cursory overview. Disponible en: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137

Tanto el Global Cybersecurity Index 2020 de la UIT[52] y el National Cybersecurity Index de eGA[53] ubican a Costa Rica, Panamá y la República Dominicana en las posiciones más altas a nivel regional en materia de lucha contra los ciberdelitos. Al presentar un mayor avance, estos parecen ideales para explorar lo que podría ocurrir en otros países de Latinoamérica que han suscrito el Convenio de Budapest de manera más reciente. Pese a ello, la mayoría de estudios suelen obviar a Centroamérica y se enfocan en países con mayor población o desarrollo general, pese a que varios de estos todavía se encuentran en las primeras etapas de la adhesión o implementación del Convenio.[54]

3. PESE A LOS CONSENSOS PREVIOS, REFORMAS RECIENTES ESTÁN GENERANDO CONFLICTOS

Si bien los procesos de adhesión e implementación del Convenio en los países analizados parecen haber permitido la existencia de espacios abiertos al diálogo y la participación de múltiples partes interesadas, dichos espacios no parecen haber alcanzado a sectores sensibles, especialmente en la sociedad civil. Esto explicaría por qué recientes iniciativas de reforma penal en Guatemala y la República Dominicana han enfrentado el rechazo de activistas y medios de comunicación, que parecen percibir en estos cambios, peligros para derechos que se ejercen a través de medios y entornos digitales como la libertad de expresión e información.

Es preciso notar además que, pese a que en estos dos casos la resistencia se debió a cuestiones puntuales dentro de las reformas, las medidas de resistencia han tenido como consecuencia la paralización total de los procesos. Esto es problemático por diferentes motivos. Para empezar, significa un retroceso sobre los consensos previos en torno a las acciones adoptadas para enfrentar los ciberdelitos. También afectan la capacidad de ambos para implementar los compromisos derivados de la fase previa (Guatemala) y posterior (República Dominicana) a la adhesión al Convenio. Finalmente, ponen a estos países en una situación de mayor vulnerabilidad institucional, especialmente a Guatemala, que presenta un atraso generalizado según los estudios citados en este reporte.

4. LA PRESIÓN SOBRE LOS GOBIERNOS PODRÍA DEBILITAR EL DIÁLOGO DE MÚLTIPLES PARTES

Hasta enero de 2023, se tenía que 5 de los 9 países de Latinoamérica adherentes al Convenio, ya habían firmado el Segundo Protocolo Adicional: Chile (2022), Colombia (2022), Costa Rica (2022); Argentina (2023) y República Dominicana (2023). Tal como se ha mencionado anteriormente, organizaciones de la sociedad civil alrededor del mundo han llamado la atención sobre ese protocolo, pues ven con preocupación que sus disposiciones debiliten las protecciones existentes sobre derechos como la privacidad y habiliten un uso desproporcionado de la información obtenida durante las investigaciones. Tal es así que durante su etapa de consulta en 2019, estas organizaciones emitieron un comunicado exigiendo mayores garantías.[55]

52. UIT. Global Cybersecurity Index. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
53. e-Governance Academy. National Cybersecurity Index. Disponible en: https://ncsi.ega.ee/
54. Solo por mencionar algunas cifras, para la medición 2020 de la UIT, la República Dominicana ocupaba el quinto lugar en la región de las Américas, por encima de Argentina, Chile y Colombia. En la medición de eGA, los países analizados en este reporte menos Guatemala presentan mejores indicadores en la categoría "Fight against cybercrime" que Brasil y México.
55. IPANDETEC. Modificaciones al Protocolo del Convenio de Budapest. Disponible en: https://www.ipandetec.org/2019/02/21/protocolo-del-convenio-de-budapest/

VII. RECOMENDACIONES PARA LOS ACTORES LOCALES DEL ECOSISTEMA DIGITAL CENTROAMERICANO

En esta sección, se presenta un conjunto de recomendaciones para los actores locales del ecosistema digital centroamericano, las cuales se basan en las conclusiones de la sección anterior. En general, las recomendaciones apuntan hacia aquellos actores mejor posicionados para accionar frente a las oportunidades y desafíos identificados a lo largo del reporte.

1. INICIATIVAS EDUCATIVAS PARA UNA MAYOR CONCIENCIACIÓN EN MATERIA DE LUCHA CONTRA CIBERDELITOS

1.1 GOBIERNOS

- Los gobiernos de Centroamérica deberían poner un mayor énfasis en la concienciación sobre los riesgos en el uso de las tecnologías de información y comunicación. Esto permitirá interiorizar entre la población la importancia de las acciones del Estado frente a la ciberdelincuencia, entre ellas la adhesión e implementación del Convenio de Budapest.
- Las iniciativas de este tipo deberían considerar los diferentes públicos a los que se dirigen, debiendo hacer énfasis en aquellos que resultan más vulnerables a los ciberdelitos como los niños, niñas y adolescentes, y las mujeres. De la misma manera con aquellas personas que realizan actividades sensibles empleando las tecnologías digitales como los defensores de derechos humanos y los periodistas.
- El diseño y ejecución de estas iniciativas podrían ser una oportunidad para crear grupos de trabajo multisectorial con participación público-privada, no solo para mejorar su alcance y sostenibilidad sino para que se creen y fortalezcan relaciones entre los participantes, mejorando la capacidad de diálogos futuros.

1.2 SOCIEDAD CIVIL

- Las organizaciones de sociedad civil de Centroamérica con experiencia y especialización en ciberdelitos (como es el caso de las que tratan derechos digitales), deberían promover la capacitación de otras organizaciones en estos temas, a través de talleres, eventos y otros espacios con el fin de mejorar su capacidad de involucramiento desde sus respectivas agendas.
- Un grupo de especial interés para la creación de capacidades en estos temas deberían ser los activistas de derechos humanos, los periodistas y los medios de comunicación. Esto mejoraría el entendimiento y la incidencia de estos grupos frente a iniciativas legislativas en materia de ciberdelitos que pudieran afectar realmente derechos como la libertad de expresión e información.

2. CENTROAMÉRICA COMO CASO DE ESTUDIO PARA LA REGIÓN DE LATINOAMÉRICA

2.1 GOBIERNOS

- Los gobiernos de Centroamérica deberían reconocer que están en una posición privilegiada frente al desarrollo de medidas contra la ciberdelincuencia, en gran parte debido a su temprana adhesión al Convenio de Budapest y a los procesos de reforma que han experimentado durante los últimos años. Esto debería estimularlos a ser más activos en compartir su experiencia a nivel regional y subregional.

- Los casos de estudio de Costa Rica, Guatemala, Panamá y la República Dominicana pueden arrojar lecciones valiosas y buenas prácticas a ser implementadas por otros gobiernos de la región. En ese sentido, debería estimularse la producción de estudios y análisis más detallados sobre dichas experiencias.

2.2 SOCIEDAD CIVIL

- Las organizaciones de sociedad civil de Centroamérica deberían promover más investigaciones sobre el proceso de implementación del Convenio de Budapest en los países centroamericanos, con el fin de identificar patrones, tendencias y otros elementos que informen y faciliten las acciones de incidencia en la región en materia ciberdelincuencia, con énfasis en el Segundo Protocolo Adicional del Convenio.

3. ESPACIOS PERMANENTES DE DIÁLOGO DE MÚLTIPLES PARTES INTERESADAS

3.1 GOBIERNOS

- Los gobiernos de Centroamérica deberían promover espacios permanentes de diálogo de múltiples partes interesadas, especialmente en relación al proceso de adhesión e implementación del Convenio de Budapest. En la medida en que existan públicos más concientizados y la sociedad civil esté mejor preparada para participar de estos espacios, será más sencillo avanzar en las reformas necesarias y evitar situaciones como las vistas en Guatemala y República Dominicana.

3.2 SOCIEDAD CIVIL

- Las organizaciones de sociedad civil de Centroamérica deberían exhortar a los gobiernos a establecer espacios permanentes de diálogo y exigir que en estos se incluya a activistas de derechos humanos, periodistas y medios de comunicación, con el fin de que cualquier reforma en materia de ciberdelitos sea discutida y consensuada antes de ser aprobada.

- En ausencia de estos espacios, las organizaciones deberían exhortar a los gobiernos a participar de espacios de diálogo ya constituidos en donde se aborden temas relacionados a la ciberdelincuencia. Algunos de los que existen en Centroamérica son: La Reunión Regional Preparatoria del Foro de Gobernanza de Internet (LACIGF) y los Foros Locales de Gobernanza de Internet.[56]

56. A la fecha y según el sitio web de la Secretaría del Foro de Gobernanza de Internet de las Naciones Unidas, todos los países analizados cuentan con foros locales. Disponible en: https://www.intgovforum.org/en/content/national-igf-initiatives

VII. ANEXOS

En esta sección, se presentan los anexos del reporte, entre ellos el apartado con la metodología, la relación de personas que contribuyeron al reporte y finalmente una pequeña biografía sobre el investigador principal.

1. METODOLOGÍA

Este reporte se ha escrito a partir del desarrollo de tres fases. En la primera fase, se han recopilado fuentes bibliográficas de distinto orden (artículos, reportes, noticias, leyes, etc), las cuales se han analizado para lograr una comprensión integral del estado de la ciberseguridad en Centroamérica, con énfasis en los países analizados y su relación con el Convenio de Budapest. En la segunda fase se han realizado entrevistas con actores de los ecosistemas digitales locales con el fin de contrastar los hallazgos de la primera fase. En la tercera fase se ha producido un borrador con los hallazgos y conclusiones. En cuanto a la estructura del reporte, se ha utilizado como modelo el informe "Convenio de Budapest sobre la ciberdelincuencia en América Latina Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México" publicado en 2022 por la organización Derechos Digitales.[57]

Como componente original, se han incluido múltiples gráficos tomados de las fuentes bibliográficas con el fin de ofrecer contexto y mayor profundidad a los contenidos expuestos.

2. AGRADECIMIENTOS

Queremos agradecer a las siguientes personas que proveyeron retroalimentación sobre las diferentes versiones del reporte, a través de entrevistas y comentarios remitidos por escrito. Su aporte ha sido invaluable para el resultado final:

Amalia Hernández (ISOC Honduras); Carlos Leonardo (CSIRT República Dominicana); César Moline (INDOTEL); Gabriel Cajiga (Cajigas & Co); Juan Ramón Anria (AIG Panamá); Lía Hernández (IPANDETEC); Marión Brancesco (Legal Hackers Costa Rica); Michelle Souza (Derechos Digitales); Sara Fratti (Fundación Avina); y Silvia Batista (AIG Panamá).

3. SOBRE EL AUTOR

Carlos Guerrero es abogado por la Universidad Nacional Mayor de San Marcos (Perú) y tiene una Maestría en Legaltech y Derecho Digital por la Universidad de Salamanca (España). Entre 2016 y 2020 fue Director de Políticas Públicas de la ONG Hiperderecho. En 2021 fue Director Adjunto del Instituto para la Sociedad de la Información y la Cuarta Revolución Industrial de la Universidad La Salle. Actualmente asesora a la Secretaría de Gobierno y Transformación Digital del Perú en ciberseguridad y derechos digitales. Su portafolio de investigaciones puede consultarse en: www.carlosguerrero.pe.

57. Bruna Martins dos Santos. Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

IPANDETEC

CENTROAMÉRICA