EU CyberNet

Desafíos de la normativa de ciberseguridad en Latinoamérica

- Juan Pablo González Gutiérrez

EU CyberNet Expert Series
No 4
2025

Acerca de

Juan Pablo González Gutiérrez

Abogado de la Universidad Alberto Hurtado. Magíster en Derecho y Nuevas Tecnologías, Universidad de Chile. Cuenta con diversas certificaciones tales como: ISO 27.701, 27.701, 37.301, DPO, entre otras. Un especial agradecimiento a Sebastián Scheffer, egresado de la Universidad Alberto Hurtado, por el apoyo en la recopilación de información.

Desde noviembre de 2023, Juan Pablo forma parte del Grupo de Expertos EU CyberNet.

Resumen

El avance del marco normativo de ciberseguridad en América Latina está basado en regulaciones internacionales, especialmente aquella de índole europeo, pero aún existen algunos desafíos para adecuarlas a las realidades propias de la región. Para mejorar la protección de la ciberseguridad desde esta perspectiva es importante definir adecuadamente la gobernanza, sus infraestructuras críticas, establecer obligaciones claras para los sujetos regulados y proporcionar un sistema de sanciones claro. Finalmente, será crucial trabajar como región y contar con una participación activa de varios actores interesados en que la labor de ciertas organizaciones ha permitido ir reduciendo la fragmentación de las regulaciones y los enfoques dispares en la región.

1. Aspector Generales

El objetivo de esta nota es presentar el fenómeno de la elaboración de leyes de ciberseguridad en Latinoamérica, por ende, no busca analizar en detalle otras normativas relacionadas con la materia. Para ello, se tomó como punto de partida las estrategias o políticas de ciberseguridad de los siguientes países: Argentina [1], Belice [2], Brasil [3], Chile [4], Costa Rica [5], Guatemala [6], Jamaica [7], México [8], Panamá [9], Paraguay [10], Perú [11], Uruguay [12], Ecuador [13], República Dominicana [14], Trinidad y Tobago [15].

Del estudio realizado, uno puede indicar que existen elementos comunes en las políticas nacionales de ciberseguridad en los países de la región. Estos temas son:

- Gobernanza Nacional;
- Protección de la Infraestructura Crítica;
- Necesidad de avanzar en un marco normativo específico de la materia;
- Avanzar en la capacitación y cultura de ciberseguridad;
- Cooperación internacional.

Un punto que fue abordado de manera parcial en cada una de las estrategias fue lo relativo a la confianza digital y el resguardo de los derechos en el ciberespacio, (ej. Brasil, Guatemala, Jamaica, Paraguay y Trinidad y Tobago).

Esto ha provocado la producción de algunas normativas, ya sea a nivel legal o reglamentario, a saber: Chile (Ley N° 21.663, Marco de Ciberseguridad) [16], Uruguay (Decreto 66/025) [17], Colombia (Decreto N° 338) [18], El Salvador (Ley de Ciberseguridad y Seguridad de la Información (Decreto 143/2024) [19], y los proyectos de Ley de México [20] y Ecuador [21]. En el caso de República Dominicana, el Decreto 685-22, incorporó algunas medidas de ciberseguridad en el sector público, especialmente en la generación de políticas y gestión de riesgos informáticos [22]. No se identificaron otras regulaciones aprobadas o en avance de discusión parlamentaria.

El fenómeno de la ciberseguridad en Latinoamérica se puede ver influenciado en el último tiempo, debido a un aumento de ciberamenazas y especialmente, algunos vectores de ataques que no solo implican que los Estados cuenten con elementos técnicos para resguardar las amenazas cibernéticas, sino la necesidad de verlo como un asunto estratégico, en que la participación del sector privado se vuelve vital. En ese sentido, la Directiva Europea NIS1 sobre ciberseguridad, cumplió un rol importante – aunque insatisfactorio – en el proceso de impulsar las regulaciones de ciberseguridad en la región [23], ya que permitió tener una visión estratégica colocando énfasis en aquellos sectores críticos y la necesidad de avanzar en el reporte de incidentes cibernéticos, pero dejando varios aspectos a la decisión de cada país a través de la transposición de la Directiva, lo que provocó que estos lineamientos llegasen de manera indirecta a la región. Además, diversos instrumentos internacionales que han fomentado la cooperación internacional, también han promovido la discusión en Latinoamérica de la ciberseguridad desde un enfoque regulatorio, sin perjuicio que a diferencia de Europa, la falta de armonización en la región, ante una falta de un proceso similar a la transposición de la citada Directiva, como la fragmentación intrínseca de la regulación, la falta de recursos en algunos países y un planteamiento disímil han sido algunos de los factores que han propiciado el paulatino avance de la ciberseguridad a nivel de leyes en la región.

Ahora bien, la Directiva NIS2 (2022/20255) [24] y que si bien, actualmente, se encuentra en varios países europeos en procesos de transposición, sí ha tenido un rol importante en las normativas, tanto a nivel legal como reglamentario, que se han ido aprobando en la región y también aquellos proyectos de ley en proceso de discusión.

2. Gobernanza

a) Gobernanza en las estrategias o políticas nacionales de ciberseguridad.

A nivel de gobernanza establecida en las estrategias de ciberseguridad, el enfoque de los países analizados difiere, puesto que algunos han decidido mantener este asunto a nivel de Presidencia (ej. Argentina: Jefatura de Gabinete de Ministros, en particular, a través de la Dirección Nacional de Ciberseguridad; Brasil: Gabinete de Seguridad Institucional de la Presidencia; Guatemala: Ministerio de Gobernación; Perú: Presidencia del Consejo de Ministros, en la Secretaría de Gobierno Digital; y República Dominicana: Ministerio de la Presidencia a través de la Dirección Nacional de Inteligencia); otros en el Ministerio de la Seguridad Pública o Interior [ej. Belice: Ministerio de la Seguridad Nacional; México, en la Secretaría de la Seguridad y Protección Ciudadana, a través del CNPIC; y Trinidad y Tobago: Ministerio de Seguridad Interior (Ministery of Homeland Security)] y países como Costa Rica, Ecuador, Paraguay, Jamaica, Guatemala y Panamá, han entendido que es un tema que debe ser abordado desde las carteras gubernamentales de innovación (Ministerio de Innovación o aquel relacionado con la Transformación Digital).

En el caso de Colombia, en el decreto N°338 del 2022, se estableció un Modelo de Gobernanza de la Seguridad Digital, a través del Ministerio de Tecnologías de la Información y las Comunicaciones y cinco instancias de decisión, las cuales son:

1. Coordinación Nacional de Seguridad Digital;
2. Comité Nacional de Seguridad Digital;
3. Grupos de Trabajo de Seguridad Digital;
4. Las Mesas de Trabajo de Seguridad Digital;
5. Puestos de Mando Unificado de Seguridad Digital [18].

En el mismo sentido, en el caso de Uruguay, en el Decreto 66/025, establece un modelo de gobernanza dirigido por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (en adelante, AGESIC), entidad con autonomía técnica, pero dependiente de la Presidencia de Uruguay [17]. Finalmente, a nivel legal, es decir, de aquellos países que cuentan con una normativa aprobada, en Chile y El Salvador han optado por la creación de una autoridad estatal específica, funcionalmente descentralizada (Agencia Nacional de Ciberseguridad o ANCI – Chile) [16] y centralizada (Agencia de Ciberseguridad del Estado o ACE – El Salvador) [19] que permiten que el asunto sea liderado por una autoridad con niveles de independencia ya sea funcional o presupuestaria.

b) Gobernanza y aspectos estructurales de las normativas de ciberseguridad en la región.

Analizando las leyes que han sido aprobadas a la fecha en la materia – Chile y El Salvador – se puede identificar que ambas han sido influenciadas directamente por la Directiva Europea NIS2 – sobre medidas destinadas a garantizar un elevado nivel común de ciberseguridad de la Unión Europea (2022/2055) (24), que buscó fortalecer aspectos de la Directiva Europea NIS1 (2016/1148), especialmente en lo relativo a:

(a) ampliar el ámbito de aplicación a sectores críticos, incluyendo a 18 sectores esenciales e importantes;
(b) la terminología de infraestructura crítica u operaciones de servicios esenciales es reemplazada por entidades esenciales e importantes, lo que es tremendamente relevante en materia de pequeñas y medianas empresas;
(c) los sujetos obligados, se consideran en relación a su tamaño y sector económico en el cual se encuentran, a diferencia de lo que proponía NIS1, fomentando la discreción de cada país;
(d) se establecen plazos específicos para la notificación de incidentes (24 horas para una notificación inicial; con una posterior a 72

horas y cierre del incidente);
(e) a nivel de sanciones, se establecen específicamente de hasta un 2% del volumen global de la entidad;
(f) a nivel de cooperación internacional, se creó el EU-CyClone para la mejora de inteligencia de amenazas;
(g) aborda tanto las obligaciones de la Alta Dirección como la necesidad de evaluar riesgos de terceras partes y proveedores, dentro de la cadena de suministro.

En ese sentido, ambas leyes latinoamericanas, coinciden en los siguientes temas:
(a) crean una Agencia de Ciberseguridad (art. 10 y siguientes ley chilena, art. 7 y siguientes ley salvadoreña);
(b) abordan principios claves para la interpretación de la autoridadadministrativa y judicial, tales como: seguridad por diseño, confidencialidad, integridad, resiliencia, cooperación y proporcionalidad (art. 3 ley chilena, art. 3 ley salvadoreña);
(c) tienen un enfoque preventivo, exigiendo a los sujetos obligados que deban realizar evaluaciones de riesgos de ciberseguridad y planes de continuidad, simulacros y reportes, aunque la normativa del Salvador, tiene un foco en la gestión de incidentes de ciberseguridad, mientras que la normativa chilena solo se centra en cuanto al deber general de los servicios esenciales;
(d) finalmente, define a los sujetos y obligaciones, ya sean infraestructuras críticas (nomenclatura de la normativa de El Salvador, art. 2, 4, 5 y 6) u operadores de importancia vital (nomenclatura de la normativa Chilena, art. 4 al 9).

No obstante ello, las regulaciones tienen algunas diferencias, tales como:
(a) la ANCI es un órgano descentralizado (art. 10 ley chilena), mientras que la ACE es un órgano centralizado (art.7 ley salvadoreña);
(b) la normativa de El Salvador, se aplica a las entidades públicas y entidades que tengan alguna incidencia en la infraestructura crítica (art. 2 ley salvadoreña), frente a la norma chilena que se aplica a los servicios esenciales y operadores de importancia vital, que pueden ser públicos o privados (art. 1 y 4 ley chilena);
(c) la normativa chilena tiene un foco multisectorial y de coordinación regulatoria; mientras que la de El Salvador, solo tiene un foco de implementación estatal centralizada;
(d) en cuanto al reporte de incidentes, la normativa chilena tiene plazos definidos (3 horas, para alerta; 72 horas, para un reporte de evaluación; y 15 días un informe, todo regulado en el art. 9 ley chilena), mientras que la otra regulación, no lo indica expresamente;
(e) la ANCI puede solicitar acceso a sistemas de los sujetos obligados únicamente con orden judicial en casos críticos (art. 11, letra k ley chilena); mientras que la ACE tiene facultades más amplias y puede acceder sin necesidad de una orden judicial (art. 8 y 16 de la ley salvadoreña);
(f) la normativa chilena, tiene un foco en el riesgo, entendiendo no sólo aquel que se genera en el sector público, sino especialmente en el sector privado; ahora bien, la normativa salvadoreña se aplica a entidades públicas y tiene una aplicación indirecta para aquellos privados, cuando exista afectación a infraestructura crítica;
(g) finalmente, la ACE tiene facultades sancionatorias y de auditoría amplias, mientras que la ANCI solo las puede ejercer en casos específicos, por ejemplo, en procesos de incidentes de impacto significativo o ante operadores de importancia vital.

3. Equipo ante respuesta de incidentes (CSIRT o CERT)

Otro elemento importante, es el avance de capacidades técnicas en la región, y por ende, destacar la creación de equipos de respuesta ante incidentes cibernéticos (CSIRT o CERT), especialmente aquellos países reconocidos en varias de las estrategias nacionales de ciberseguridad (ej. Chile, Paraguay, Trinidad y Tobago, Jamaica, Costa Rica, República Dominicana, Panamá, Brasil).

En la región, hay diferencias en los avances regulatorios vinculados al establecimiento de los CSIRT o CERT, por lo cual es menester

analizar su reconocimiento en distintos niveles, dado que algunos países han optado por reconocerlo vía legal o reglamentaria. Por ejemplo, a nivel legal, la ley chilena crea un CSIRT Nacional que actúa como una arquitectura multinivel y coordinadora con los CSIRT Sectoriales como el del área de la Defensa (art. 24 a 32 ley chilena).

A diferencia de la normativa de El Salvador, que no lo indica explícitamente y, por ende, se entiende que la ACE asume operaciones tanto operativas como de coordinación técnica en la gestión y tratamiento de incidentes cibernéticos (art. 8 ley salvadoreña). A nivel reglamentario, hay varios países que reconocen la existencia de Equipos ante Respuesta de Incidentes, tales como Colombia, Uruguay, Perú, Brasil, Ecuador, República Dominicana, entre otros, con algunas diferencias. En Colombia, República Dominicana y Uruguay, hay una arquitectura multinivel, en un CSIRT o CERT Nacional, otros sectoriales; y, en Colombia, sectoriales críticos, cuya regulación incluye sus definiciones, funciones, obligaciones y enfoque de coordinación y cooperación con los órganos de la Administración del Estado, las instituciones públicas y privadas (art. 2.2.21.1.1.3, 2.2.21.1.5.1 a 2.2.21.1.5.10 del decreto 338-2022 colombiano; art. 3, 7, 8, 9 y 13 del decreto 66/025 uruguayo; art. 3° del decreto 685-22 de República Dominicana). En cambio, en los otros países, sólo hay reconocimiento de su existencia, más no el detalle de funciones, atribuciones, obligaciones, etc.

A nivel de estrategias nacionales, se reconoce en la mayoría de los países de la región latinoamericana sin que se establezca en ella, salvo en casos como el de Belice, donde actualmente sólo está contemplado como parte de una iniciativa regional llamada CSIRT-SICA (25), sin que exista una mención a nivel legal o reglamentario al respecto.

La relevancia de contar con un CSIRT es realizar un seguimiento y analizar las ciberamenazas, las vulnerabilidades y los incidentes a escala nacional, difundir alertas tempranas sobre amenazas, responder a incidentes y prestar asistencia a las entidades esenciales e importantes, recopilar información forense y realizar un análisis de riesgos e incidentes, entre otros, tomando como referencia lo señalado en la normativa europea (NIS2).

Por lo tanto, tienen un rol vital para entregar información relevante sobre amenazas cibernéticas que son cada vez más dinámicas, y unido a iniciativas regionales (ej. CSIRT Américas o LACNIC CSIRT), fomentan identificar un escenario de riesgos informáticos para que los países puedan compartir, adoptar oportunamente, estrategias frente a un entorno dinámico de riesgos en el ciberespacio.

4. Colaboración entre diversos actores interesados

A nivel de la colaboración nacional entre las instituciones público – privadas, sociedad civil y academia, es importante destacar algunos aspectos de ambas regulaciones:

Respecto a la colaboración nacional, en Chile es posible observar ello, por ejemplo, a través de la composición del Consejo Multisectorial sobre Ciberseguridad, organismo consultivo en ciberseguridad vinculado a la ANCI, integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, que serán personas destacadas en ciberseguridad, donde dos provienen del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil (art. 20 a 22 de la ley chilena, regulado en detalle en el decreto 276) (26). En cambio, en otros casos, tales como Colombia – mediante vía reglamentaria – y El Salvador, dicha participación es más limitada. En Colombia, en la conformación del Comité Nacional de Seguridad Digital, habrá representantes de las autoridades vinculadas a la infraestructura crítica cibernética o de servicios esenciales (art. 2.2.21.1.3.5 del decreto 338-2022 colombiano).). Y, en El Salvador, no hay una mención expresa en relación con la participación de la sociedad civil en la ACE u

otro organismo. Otros casos de participación limitada se pueden visualizar en los proyectos de ley en México y Ecuador. Por ejemplo, en México, en la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la seguridad de la información (CITICSI), donde representantes de industrias, expertos, académicos, o la sociedad civil, sólo tendrían una participación si son invitados por la comisión en las sesiones, con derecho a voz, pero no a voto (art. 9 y 10 del proyecto de ley) [20]. Mismo caso en Ecuador, en el Comité Nacional de Seguridad Digital (art. 24 y 30 del proyecto de ley de abril 2025) [21]. Sin perjuicio de lo anterior, del análisis de los países antes mencionados, destaca la importancia de la colaboración interna general, especialmente en la promoción y ejecución de programas de capacitación y educación, fomentando canales que permitan comunicar posibles ciberataques, donde el rol público-privado es relevante para la construcción de confianza.

Finalmente, en el caso de República Dominicana la Comisión Técnica Especializada de Ciberseguridad que asesora el Centro Nacional de Ciberseguridad que apoya al Consejo de Seguridad y Defensa Nacional, está conformado por varios representantes del sector público, para tener una visión disciplinaria del asunto, abordando áreas desde la defensa interior, las telecomunicaciones, financiero, tecnologías de la información y la educación superior (art. 3° decreto 612-24) [27].

5. Cooperación internacional

Respecto a la cooperación internacional en ciberseguridad, ésta ocurre en el impulso de iniciativas conjuntas, que permiten el intercambio de conocimiento y el fomento de la capacitación y educación en ciberseguridad dentro de la región. Un ejemplo de lo anterior en los países de la Latinoamérica radica en el Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4), que es un centro regional de educación y capacitación en ciberseguridad, el cual convoca a eventos vinculados a la ciberseguridad de forma periódica [28].

Otra forma relevante de cooperación internacional es posible de observar en los equipos de respuesta ante incidentes cibernéticos de Latinoamérica (CSIRT o CERT), en particular, en la generación de redes activas de colaboración e intercambio de información en dichos equipos a nivel regional, a través de iniciativas tales como CSIRT Américas Network [29] (que establece parámetros de madurez de los CSIRT, a nivel de organización, aspectos humanos, herramientas y procesos), o el Foro de Respuesta a Incidentes y Equipos de Seguridad – FIRST – [30] (consistente en una plataforma para centros de respuesta a incidentes, que les permite un intercambio de información, experiencias prácticas y herramientas en ciberseguridad), lo que fomenta y permite contar con información de amenazas cibernéticas actualizadas y oportuna para identificar fenómenos cibernéticos en la región y en ciertas industrias específicas.

Es importante mencionar que no todos los países están en todas las iniciativas regionales, a saber: Chile, Brasil, Perú, Argentina, Bolivia, Paraguay, México, Trinidad y Tobago, Jamaica no están en LAC4. Paraguay, Bolivia, Belice, y Jamaica no están en FIRST. Belice no está en CSIRT Americas Network. Sin perjuicio de ello, existen algunos países en la región que tienen una participación más activa en algunas de las iniciativas regionales tales como Chile, Uruguay, Brasil y Colombia, lo cual contribuye significativamente en la cooperación y colaboración internacional sobre ciberseguridad. Por último, es relevante destacar la iniciativa regional de CSIRT-SICA, que integra a varios Estados de Centroamérica, que ha permitido apoyar a países como Belice, que se encuentran avanzando en la creación de capacidades en estas materias. Por ejemplo, Belice lidera esta iniciativa de un CSIRT Regional, que busca elaborar una estrategia regional de ciberseguridad 2024-2026 [25].

6. Sujetos obligados y régimen infraccional

Este es un tema clave que permite determinar claramente quiénes son los sujetos regulados y, además, si existe alguna infracción en caso de incumplimiento. A nivel de leyes ya publicadas en la región, la normativa Chilena, distingue entre aquellos prestadores de servicios esenciales, que en el sector público son aquellos organismos del Estado o concesionarios de servicios públicos, o instituciones privadas de ciertos sectores. De este grupo de instituciones – generalmente – serán nombrados algunos operadores de importancia vital cada 3 años (art. 4 a 6 ley chilena). A su vez, la normativa salvadoreña, reconoce que la infraestructura crítica está conformada por sectores como: telecomunicaciones, energía, transporte, agua, salud, seguridad pública, y finanzas, pero no se indica los plazos de declaración (art. 2 y 4 de la ley salvadoreña). Importante es indicar que varios de los sectores coinciden con aquellos reconocidos en la Directiva Europa NIS2 (art. 2 y 3).

A nivel infraccional, tanto la normativa chilena como salvadoreña establecen una tipificación de aquellas infracciones leves, graves y gravísimas (o muy graves de esta última), que están centradas en aspectos tales como el incumplimiento de las obligaciones técnicas, no colaborar proveyendo información durante un incidente con la autoridad de ciberseguridad o, derechamente, no notificar incidentes (art. 38 y 39 ley chilena; art. 18 a 21 ley salvadoreña). El rango de multa en la normativa chilena en un rango entre 350.000 a 1.400.000 USD (art. 40 ley chilena), mientras que la norma salvadoreña establece un rango de multa entre 1 (365 USD) a 10 salarios mínimos mensuales (leves), 11 a 50 salarios mínimos mensuales (graves) y 51 a 100 salarios mínimos mensuales – 36.500 USD (muy graves) (art. 22 a 24 de la ley salvadoreña, respectivamente); además, incluye otras sanciones, tales como la amonestación escrita (leves, art. 22 ley salvadoreña), despido o destitución del cargo (graves y muy graves, art. 23 y 24 de la ley salvadoreña), y la imposibilidad de pertenecer al sector público por 10 años posteriores a la imposición de la sanción (art. 25 ley salvadoreña). En ambas regulaciones, se establece un procedimiento administrativo con derecho a defensa y es instruido – por oficio o denuncia – por las agencias de ciberseguridad, respectivamente (art. 11 letra o), 41 a 47 ley chilena; art. 28 ley salvadoreña).

En el proyecto de Ley de Ecuador, en su versión abril 2025, existe una tipificación de las faltas en leves, graves y gravísimas, cuya sanción corresponde a multas desde 5 (2.350 USD) a 20 (9.400 USD) salarios básicos unificados (art. 70 a 73 del proyecto de ley ecuatoriano). En cambio, si bien el proyecto de ley Federal sobre Ciberseguridad en México no contempla una tipificación de infracciones en leves, graves y gravísimas, sí refiere a infracciones por incumplimientos de aspectos similares a los mencionados anteriormente. Y las sanciones aluden a multas de mil (5.800 USD) a veinte mil (11.6000 USD) veces el valor diario de la Unidad de Medida y Actualización (UMA), por parte de la Agencia Nacional de Ciberseguridad de México (art. 62 a 64 del proyecto de ley mexicano).

Por último, no existe un criterio uniforme a nivel de régimen infraccional y sancionatorio ante incumplimientos de deberes de informar incidentes cibernéticos, que sí se encuentra presente en las normativas chilena y salvadoreña. A su vez, en el caso de Uruguay, el Decreto 66/025 le otorga atribuciones a la AGESIC para apercibir a las entidades obligadas que incumplan la normativa, pero no establece sanciones específicas. Sin embargo, en los otros países analizados (por ej., Perú, Jamaica, Belice etc.) no hay una normativa específica que sancione los incumplimientos generales por incidentes cibernéticos, sino que las sanciones están reducidas a la remisión normativa a leyes de delitos informáticos-cibernéticos.

7. Conclusiones y reflexiones

Del análisis realizado, sin que sea exhaustivo, uno puede destacar algunos aspectos:

- El proceso legislativo en ciberseguridad en la región latinoamericana ha avanzado para alinearse con los estándares internacionales, especialmente en varios elementos de la Directiva NIS2, pero principalmente de acuerdo a sus realidades locales. En ese sentido, Chile y El Salvador cuentan con una normativa aprobada y publicada que, a su vez, ha sido tomada como referencia por otros países que han ido avanzando en sus procesos de construcción de normativa interna a través de Proyectos de Ley. Sin perjuicio de que ciertos asuntos técnicos (ej. CSIRT) se ha avanzado a través de vía reglamentaria.

- Uno de los aspectos claves en aquellos países que están construyendo sus normativas internas, además de la gobernanza, sería un procedimiento para la calificación de sectores esenciales o críticos, siendo especialmente cuidadoso de buscar un equilibrio entre la carga regulatoria para aquellos sujetos regulados y su nivel de madurez.

- La aplicación de sanciones es otro aspecto a destacar en las normativas analizadas, debiendo ser un elemento clave de discutirse internamente por su necesidad de entender la relevancia del asunto, sin que exista un criterio uniforme en la región.

- La colaboración regional, a través de mecanismos como CSIRT Américas o LACNIC CSIRT, permiten fortalecer las capacidades de respuesta a través de la generación de redes para intercambiar información y lograr establecer adecuadas medidas para mitigar los riesgos informáticos. Por ello, si bien ha existido una disparidad en el nivel de participación activa de algunos países de la región frente a otros en dichos mecanismos de cooperación internacional (por ej., Chile, Uruguay, Brasil y Colombia tienen mayor participación activa que Belice o Jamaica), iniciativas regionales como CSIRT-SICA en Centroamérica, constituyen una herramienta fundamental en la cooperación internacional hacia países desaventajados como Belice o Jamaica, en la elaboración de estrategias regionales de ciberseguridad, que contemplan la creación de un CSIRT Regional.

- Para concluir, cada país, de acuerdo a sus procesos internos de discusión parlamentaria, debe indagar en los presentados para satisfacer sus necesidades y condiciones internas, tomando como referencias las normativas ya aprobadas y especialmente, los estándares internacionales, pero sin tener el anhelo de abordar materias respecto de las cuales no se cuente con capacidades técnicas previamente instaladas.

Bibliografía

[1] Estrategia Nacional de Ciberseguridad en Argentina. Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904
[2] Estrategia Nacional de Ciberseguridad 2020-2030, Belice. Disponible en: https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf
[3] Decreto N° 11.856, de 26 de diciembre de 2023, que establece la Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad. Disponible en: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289
[4] Política Nacional de Ciberseguridad 2023-2028, Chile. Disponible en: https://anci.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf
[5] Estrategia Nacional de Ciberseguridad 2023-2027, Costa Rica. Disponible en: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf
[6] Estrategia Nacional de Seguridad Cibernética, Guatemala. Disponible en: http://conciber.gob.gt/wp-content/uploads/2022/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf
[7] Estrategia Nacional de Seguridad Cibernética, Jamaica. Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Jamaica%20National%20Cyber%20Security%20Strategy%20(Spanish).pdf
[8] Estrategia Nacional de Ciberseguridad, México. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
[9] Estrategia Nacional de Ciberseguridad 2021-2024, Panamá. Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/29434_A/88864.pdf
[10] Plan Nacional de Ciberseguridad, Paraguay. Disponible en: https://afyonluoglu.org/PublicWebFiles/strategies/America/Paraguay%202017%20National%20Cyber%20Security%20Strategy.pdf
[11] Estrategia Nacional de Seguridad y Confianza Digital 2021-2026, Perú. Disponible en: https://www.enap.edu.pe/wp-content/uploads/transformacion/Tema4/1.Estrategia_Nacional_de_Seguridad_y_Confianza_Digital.pdf
[12] Estrategia Nacional de Ciberseguridad del Uruguay 2024-2030. Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-del-uruguay-2024-2030/estrategia
[13] Estrategia Nacional de Ciberseguridad del Ecuador, 2022-2025. Disponible en: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf
[14] Estrategia Nacional de Ciberseguridad 2021-2030, República Dominicana. Disponible en: https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf
[15] Estrategia Nacional de Seguridad Cibernética, Trinidad y Tobago. Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(Spanish).pdf
[16] Ley N°21.663 en Chile, Ley Marco de Ciberseguridad. Disponible en: https://www.bcn.cl/leychile/navegar?i=1202434&f=2025-03-01
[17] Decreto N°66 de 2025 de Uruguay, relativo a la determinación de los cometidos de la dirección de seguridad de la información de la agencia para el desarrollo del gobierno de gestión electrónica y la sociedad de la información y del conocimiento (AGESIC). Disponible en: https://www.impo.com.uy/bases/decretos/66-2025
[18] Decreto N°338 de 2022 en Colombia, que establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
[19] Decreto N°143, que establece la Ley de Ciberseguridad y Seguridad de la Información en El Salvador. Disponible en: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/5BD19CFF-F658-4770-8391-8493916A3129.pdf
[20] Proyecto de Ley Federal de Ciberseguridad en México, 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf
[21] Proyecto de ley orgánica de protección digital en Ecuador, 2025. Disponible en: https://www.asambleanacional.gob.ec/es/noticia/101493-proyectos-de-ley-sobre-proteccion-digital-y-de
[22] Decreto N°685-22 en República Dominicana, Decreto de notificación obligatorio de incidentes e intercambio de inteligencia de amenazas. Disponible en: https://cncs.gob.do/wp-content/uploads/2022/12/Decreto-685-22.pdf
[23] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Disponible en: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng
[24] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas para garantizar un elevado nivel común de ciberseguridad en la Unión, por la que se modifica el Reglamento (UE) n.° 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[25] Plan de acción de la Estrategia Regional de Ciberseguridad de SICA 2024-2026. Disponible en: https://www.sica.int/erdi/proyectos
[26] Decreto N°276 en Chile, que aprueba reglamento que establece normas para el funcionamiento del Consejo Multisectorial sobre Ciberseguridad. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1211058&idParte=0
[27] Decreto 612-24 en República Dominicana, Decreto de reorganización de competencias en ciberseguridad y creación del Instituto Criptográfico Nacional. Disponible en: https://cncs.gob.do/decreto-612-24/
[28] Centro de Competencia Cibernética de América Latina y el Caribe (LAC4). Disponible en: https://www.lac4.eu/
[29] CSIRT Américas Baseline, 2025. Disponible en: https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1191&lang=2
[30] Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST). Disponible en: https://www.first.org/

Desafíos de la normativa de ciberseguridad en Latinoamérica
Juan Pablo González Gutiérrez

EU CybetNet Expert Series, No 4, 2025

EU CyberNet

Funded by
the European Union