Construcción de un ecosistema de confianza y seguridad digital

Sebastián M. Cabello
Mauricio Fernández
Mercedes Elaskar
Marcela Pallero
Federico Pereira
Diego Ros Rooney
Milagros Urtasun

NACIONES UNIDAS
CEPAL
Global Gateway
Alianza Digital UE-ALC
UE-ALC
ALIANZA DIGITAL
DIÁLOGOS POLÍTICOS

Gracias por su interés en esta publicación de la CEPAL

NACIONES UNIDAS

CEPAL

Si desea recibir información oportuna sobre nuestros productos editoriales y actividades, le invitamos a registrarse. Podrá definir sus áreas de interés y acceder a nuestros productos en otros formatos.

Deseo registrarme

Conozca nuestras redes sociales y otras fuentes de difusión en el siguiente link:

https://bit.ly/m/CEPAL

Documentos de Proyectos

Construcción de un ecosistema de confianza y seguridad digital

Sebastián M. Cabello
Mauricio Fernández
Mercedes Elaskar
Marcela Pallero
Federico Pereira
Diego Ros Rooney
Milagros Urtasun

NACIONES UNIDAS
CEPAL
Global Gateway
Alianza Digital UE-ALC
UE ALC
ALIANZA DIGITAL
DIÁLOGOS POLÍTICOS

Este informe fue preparado por Sebastián M. Cabello, Mauricio Fernández, Mercedes Elaskar, Marcela Pallero, Federico Pereira, Diego Ros Rooney y Milagros Urtasun, Consultores de la División de Desarrollo Productivo y Empresarial de la Comisión Económica para América Latina y el Caribe (CEPAL), bajo la coordinación de Sebastián Rovira, Oficial Superior de Asuntos Económicos, y Valeria Jordán y Alejandro Patiño, Oficiales de Asuntos Económicos, todos de la misma División. El documento se elaboró en el marco de la Alianza Digital Unión Europea-América Latina y el Caribe y contó con el financiamiento de la Unión Europea, a través de la estrategia Global Gateway.

El informe contó también con los aportes de Maria del Rosario Heras Carrasco, de la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), y de Jean-Marie Chenou, de Expertise France.

Publicación de las Naciones Unidas
LC/TS.2024/102
Distribución: L

Impreso en Naciones Unidas, Santiago
S.2400934[S]

Esta publicación debe citarse como: S. M. Cabello y otros, "Construcción de un ecosistema de confianza y seguridad digital", *Documentos de Proyectos* (LC/TS.2024/102), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2025.

Índice

Cuadros

Gráfico

Recuadros

Diagramas

Resumen

La protección de datos personales y la ciberseguridad se han convertido en elementos esenciales en el contexto digital actual, donde el manejo masivo de información sensible plantea desafíos significativos. Los gobiernos de América Latina y el Caribe (ALC) deben desarrollar marcos normativos robustos que no solo protejan la privacidad de los ciudadanos, sino que también fortalezcan la confianza pública en las instituciones y promuevan un entorno digital seguro.

Una de cada tres empresas de América Latina reportaron incidentes de ciberseguridad en 2023, lo que enfatiza la necesidad de una respuesta coordinada y efectiva (ESET, 2024). Por su parte, la falta de comprensión sobre la economía de datos, limita la innovación y la competencia. Este panorama sugiere que los gobiernos deben promover una cultura de gestión de datos que fomente el uso responsable y eficiente de la información, permitiendo así un crecimiento sostenible y la creación de nuevos modelos de negocio.

La protección de datos personales y la ciberseguridad están estrechamente vinculadas. Estos elementos son críticos para garantizar un entorno digital seguro y confiable en América Latina y el Caribe. La adecuada regulación y gestión del tratamiento de datos es esencial para salvaguardar la privacidad de las personas, mientras que la ciberseguridad aborda la gestión de un amplio rango de amenazas que ponen en riesgo la integridad de los sistemas de información y los datos personales.

Los esfuerzos por establecer marcos regulatorios han avanzado, como se evidencia en la promulgación de la Ley General de Protección de Datos en Brasil y la nueva Ley Marco de Ciberseguridaden Chile, que busca establecer una Agencia Nacional de Ciberseguridad. Estas iniciativas son pasos cruciales para mejorar la ciberseguridad y la protección de datos en la región, alineándose con estándares internacionales y promoviendo la cooperación entre países.

Se observa una disparidad significativa en el desarrollo de la ciberseguridad en los países. Entre 2017 y 2018, se desarrolló una primera generación de estrategias de ciberseguridad en América Latina y el Caribe. A partir de 2020, se inició una segunda ola de estrategias, impulsada en gran medida por la pandemia, que expuso a gobiernos y empresas a un aumento de ciberataques. En 2023, se observa un

proceso de consolidación con la implementación de estas estrategias y políticas en países como Brasil, Chile, Argentina y Costa Rica. Otros países, como Bolivia, Guyana, Honduras y Uruguay, están en proceso activo de elaboración de sus propias estrategias. Uruguay, por ejemplo, aprobó un Marco de Ciberseguridad en 2022, con una estrategia prevista para 2025.

De los 22 países que cuentan con legislación en protección de datos personales, todos cuentan con leyes vigentes que crean una autoridad de control encargada de monitorear el cumplimiento y la aplicación de la ley. Por otro lado, de los 11 países restantes que todavía no cuentan con una legislación, existen algunos como Surinam y Bolivia que están actualmente trabajando en proyectos de ley de protección de datos.

Al parecer, los países han iniciado sus esfuerzos regulatorios y normativos en materia de protección de datos con anterioridad a la ciberseguridad. Asimismo, existen casos como Brasil que se destacan por su enfoque integral, dado que ha venido trabajando de manera sostenida en ciberseguridad, asociando inmediatamente el tema de protección de datos personales.

Las fortalezas en América Latina y el Caribe incluyen una sólida base regulatoria establecida por la mayoría de los países y algunos espacios de cooperación regional. Además, se cuenta con capacidades técnicas que pueden impulsar una mejora regulatoria aún mayor, apoyadas por redes de cooperación internacional como la Red Iberoamericana de Protección de Datos y el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) de las Américas, lo que sugiere un entorno propicio para avanzar en la protección de datos y la seguridad digital.

Se identifican debilidades que afectan la efectividad de estas políticas y la falta de continuidad, además de cierta lentitud en la actualización de regulaciones. Además, la atención de los gobiernos y la asignación de presupuesto se ve desviada por otras prioridades, lo que limita el enfoque en la protección de datos y la ciberseguridad. La falta de sensibilización social sobre la importancia de proteger los datos también contribuye a este panorama. En este contexto, es fundamental que se implementen iniciativas de formación y sensibilización para fortalecer tanto la capacidad institucional como la cultura de ciberseguridad en la región.

La implementación de marcos normativos efectivos es esencial para enfrentar los desafíos contemporáneos y garantizar un entorno digital seguro y confiable que beneficie tanto a las empresas, los gobiernos y la sociedad en su conjunto. En un contexto donde el manejo de datos personales y la ciberseguridad son cada vez más críticos, es imperativo que los gobiernos desarrollen y fortalezcan regulaciones que protejan la privacidad de los individuos y la integridad de las operaciones comerciales. Esto no solo ayuda a prevenir ciberataques y filtraciones de datos, sino que también fomenta la confianza del público en las instituciones y los servicios digitales.

Introducción

En el contexto actual de constante evolución digital, la protección de datos personales y la ciberseguridad se han posicionado como elementos críticos. En respuesta al manejo masivo de información sensible, es crucial para los gobiernos asegurar que los marcos normativos sean robustos y efectivos. Estos no solo protegen la privacidad de los individuos, sino que también salvaguardan la integridad de las operaciones comerciales y financieras, fortalecen la confianza pública en las instituciones y promueven un entorno digital seguro y confiable para el desarrollo económico y social.

El objetivo principal de este trabajo, que se realiza en el marco de la Alianza Digital entre la Unión Europea y América Latina y el Caribe[1], es efectuar una revisión exhaustiva del marco normativo existente en materia de protección de datos personales y ciberseguridad en los 33 países de América Latina y el Caribe (ALC)[2]. Esta revisión se basa en referentes internacionales, y particularmente en los marcos normativos existentes en la Unión Europea. Específicamente, se realizó un análisis de las regulaciones de la Unión Europea en materia de protección de datos personales y de ciberseguridad que permitió una construcción de indicadores comprehensivos y acordes a estos estándares internacionales[3]. En consecuencia, se plantearon los siguientes objetivos secundarios: i) la sistematización de la información sobre las normativas estatales vigentes; ii) el desarrollo de un análisis que refleje el nivel de avance de estos aspectos en cada país; iii) la identificación de los principales desafíos que enfrentan los gobiernos para implementar políticas efectivas; y, iv) la elaboración de recomendaciones concretas para mejorar los marcos normativos y las políticas públicas relacionadas.

---

[1] La Alianza Digital Unión Europea-América Latina y el Caribe es un marco estratégico diseñado para fomentar una cooperación birregional significativa en un amplio espectro de cuestiones digitales. Esta alianza se centra en una visión de la economía y sociedad digitales que prioriza al ser humano. En este contexto, el presente estudio se desarrolla como un aporte clave que busca generar conocimiento y facilitar el intercambio de mejores prácticas, con el objetivo de promover un entorno digital más seguro.

[2] Antigua y Barbuda, Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Dominica, Ecuador, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, San Cristóbal y Nieves, San Vicente y las Granadinas, Santa Lucia, Surinam, Trinidad y Tobago, Uruguay y Venezuela.

[3] Este trabajo se realizó por el Dr. Tadas Jakstas.

Para lograr estos objetivos se empleó una metodología de relevamiento secundario. Esto implicó el análisis exhaustivo de políticas y legislaciones a través de fuentes de acceso público, como bases de datos gubernamentales, publicaciones académicas y documentos oficiales de entidades reguladoras. A partir de este relevamiento, el análisis se centró en la comparación de disposiciones legales, prácticas regulatorias y enfoques institucionales adoptados por cada país y por la Unión Europea. Se identificaron tendencias regionales, áreas de fortaleza y debilidades comunes, con el objetivo de ofrecer recomendaciones específicas que puedan fortalecer la protección de datos personales y la ciberseguridad en América Latina y el Caribe.

Para cada área de estudio, se han definido los ejes clave que conformarán el abordaje metodológico. Posteriormente, se identificaron variables dentro de estos ejes, las cuales fueron categorizadas en una escala del 0 al 3. Este enfoque ha permitido capturar de manera comparativa el grado de avance de los países en materia de ciberseguridad y tratamiento de datos personales.

En conclusión, este informe aspira a proporcionar un panorama detallado y actualizado sobre la situación normativa en la región, así como a servir como guía para promover políticas públicas más efectivas y adecuadas a los desafíos contemporáneos en materia de seguridad digital y protección de datos personales.

I. Desafíos críticos en la expansión de capacidades de ciberseguridad y la protección de datos personales

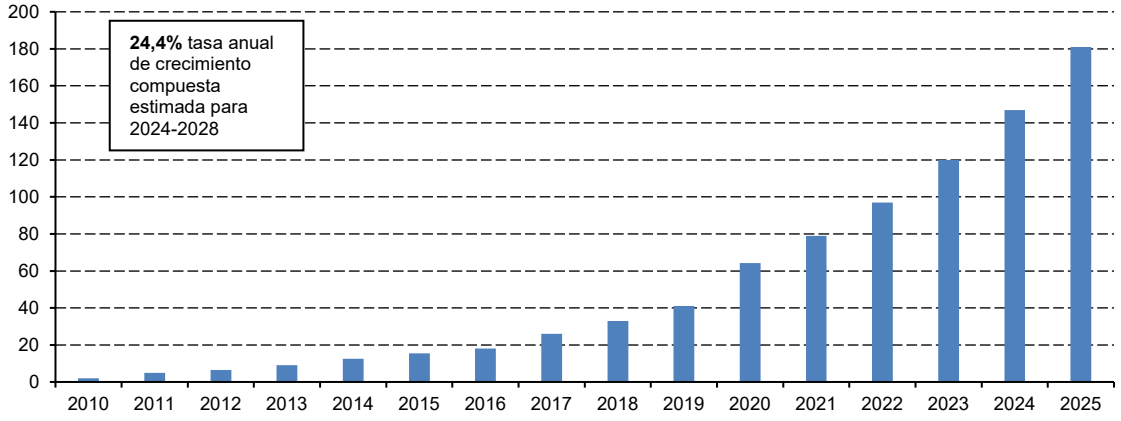
A. Revisión de los beneficios y riesgos de la economía de datos

El uso de datos ha experimentado un crecimiento exponencial en las últimas décadas, convirtiéndose en un recurso crucial para la toma de decisiones en diversos sectores, tanto privados como públicos. Se espera que esta tendencia se acelere aún más en los próximos años, impulsada por el desarrollo de la inteligencia artificial, el Internet de las cosas, la digitalización de trámites, y de otras tecnologías emergentes. Según la International Data Corporation (2024), se prevé que el volumen de datos creados anualmente aumente a una tasa anual de crecimiento compuesta (TACC) del 24,4% hasta 2028.

La economía de los datos se ha consolidado como un pilar esencial de la producción económica moderna, comparable a insumos tradicionales como la tierra, el capital y la mano de obra. Para 2025, se estima que el 50% de las actividades laborales actuales serán realizadas por máquinas, lo que destaca la creciente importancia de los datos en la automatización y la toma de decisiones (FMI, 2020).

Por ejemplo, se estima que las empresas que adoptan la toma de decisiones basada en datos pueden experimentar un incremento del 5-6% en su producción y productividad (Brynjolfsson et al., 2011). La Comisión Europea calcula que, incluso con un uso limitado de soluciones de análisis de grandes datos por parte de los 100 principales fabricantes de la UE, el crecimiento económico de la región podría aumentar anualmente en un 1,9% adicional (ESPC Strategic Notes, 2017). Para 2024, se estima que el valor económico de los flujos de datos en la nube para la UE sera de 77 mil millones de euros, y se prevé que aumente a 328 mil millones de euros para 2035 (European Comission, 2024). Para contextualizar este monto, el valor total de los flujos de datos basados en la nube en Europa en 2028 alcanzaría entonces el 1,8% del PIB de esta región. Además, el valor total actualmente supera el PIB de varios países europeos, por ejemplo, Bulgaria, Croacia, Estonia, Letonia y Lituania.

Gráfico 1
Evolución del volumen de datos a nivel mundial
(En Zettabytes)



Fuente: Elaboración propia a partir de IDC (2020) y Statista (2024).
Nota: Valores estimados.

Sin embargo, el mercado de datos enfrenta importantes desafíos. Solo el 19% de las empresas comprende el concepto de economía de datos, indicando una falta de entendimiento que puede limitar la innovación y la competencia (Pérez González et al., 2018). Además, las empresas tienden a acumular datos, lo que puede desalentar la competencia y limitar los beneficios sociales que podrían derivarse de un acceso más amplio a estos recursos.

En este contexto, los datos no solo son un recurso valioso, sino que también presentan desafíos significativos en términos de privacidad, competencia y seguridad. La creciente importancia de los datos ha llevado a los responsables de políticas a enfrentar una serie de retos, incluyendo la protección contra ciberataques y filtraciones de datos. Los ataques a infraestructuras críticas, empresas y gobiernos se han multiplicado, exponiendo información sensible y causando pérdidas económicas considerables.

Según los datos disponibles un 30% de las empresas en América Latina ha experimentado algún tipo de incidente en ciberseguridad en 2023 (ESET, 2024). En los últimos años, la incidencia de ataques digitales en la región ha aumentado, destacándose el malware[4], el ransomware[5] y el phishing[6] como los más frecuentes.

Este panorama ha elevado la relevancia y criticidad de la ciberseguridad y el tratamiento de datos, impulsando la implementación de nuevos marcos regulatorios y la creación de reguladores especializados en la protección de datos personales y la ciberseguridad. Ejemplos notables son la Ley General de Protección de Datos Personales (LGPD) en Brasil[7] de septiembre de 2020 que contempla una autoridad en la materia y la nueva Ley Marco sobre Cibserseguridad[8] en Chile, de abril de 2024. Esta última establece la Agencia Nacional de Ciberseguridad (Anci), un nuevo regulador encargado de supervisar y sancionar a las entidades que brindan servicios esenciales. En Argentina, en julio de 2024,

[4] Malware: programa malicioso que busca dañar a las computadoras y dispositivos móviles. Tienen como objetivo robar información personal, robar tarjetas de crédito y contraseñas, espiar, cobrar rescate en criptomonedas, bloquear equipos, destruir información, utilizar dispositivos para la minería de criptomonedas, mostrar publicidad no deseada.
[5] Ransomware: tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de varias maneras, cifrando la información, bloqueando la pantalla, etc.
[6] Phishing: quiere decir suplantación de identidad. Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.
[7] Lei Geral de Proteção de Dados Pessoais (LGPD).
[8] Ley 21663. Ley Marco de Ciberseguridad de Chile.

se creó la Agencia Federal de Ciberseguridad[9] que evaluará, planificará y desarrollará soluciones para la detección y contención de ciberataques contra la infraestructura informática crítica en el país, así como también de la capacitación del capital humano del Estado para la prevención de amenazas y fallas de seguridad. Se encuentra a cargo de la Secretaría de Inteligencia de Estado (SIDE).

Es fundamental destacar que la "revolución de los datos" no se limita únicamente al ámbito empresarial: el sector público y las organizaciones sin fines de lucro también están adoptando insumos basados en datos, bases de datos, análisis y plataformas en línea para reducir costos, mejorar la eficiencia y encontrar soluciones innovadoras para diversos desafíos sociales (OCDE, 2020). Este papel multifacético de los datos, y la necesidad de tomar decisiones políticas informadas que afectan a muchos ámbitos, subraya la importancia de conceptualizar y medir el valor de los datos. Junto con mantener un entorno de datos seguro y confiable, los gobiernos desempeñan un papel crucial en establecer las bases para una economía próspera impulsada por los datos.

Establecer marcos normativos sobre la protección de datos personales también es esencial para garantizar la confianza en el entorno digital y proteger los derechos de las personas. Estas regulaciones aseguran el manejo ético y seguro de la información personal, previniendo abusos y fortaleciendo la confianza ciudadana en la economía de datos. Además, promueven la transparencia y la rendición de cuentas, equilibrando el avance tecnológico con la protección de la privacidad.

B. Marco conceptual para analizar las políticas existentes de ciberseguridad y tratamiento de datos personales

Se busca proporcionar un marco claro y sistemático para evaluar las políticas existentes en estos dos ámbitos críticos. Este enfoque incluye la identificación y análisis de los elementos normativos e institucionales que influyen en la protección de datos personales y en la seguridad digital. Al establecer parámetros específicos para cada aspecto, se busca garantizar una evaluación estructurada, exhaustiva y coherente en todos los países, la que permita identificar fortalezas, debilidades y áreas de mejora en las políticas y prácticas vigentes.

1. Ciberseguridad

La ciberseguridad engloba un conjunto de herramientas, políticas y prácticas diseñadas para proteger los sistemas de información y los datos de amenazas cibernéticas. Incluye la gestión de riesgos, la implementación de controles de seguridad, la capacitación en buenas prácticas y la respuesta a incidentes. La protección eficaz en este ámbito es crucial para salvaguardar a las personas, organizaciones y naciones de posibles ataques y vulnerabilidades. Esta protección incluye también la infraestructura física subyacente.

[9] Decreto 614/2024, que crea la Agencia Federal de Ciberseguridad (AFC).

Cuadro 1
Abordaje conceptual de la ciberseguridad

Parámetros de análisis	Descripción
Normativos	• Tipificación de ciberdelitos: determinar si existen leyes que tipifiquen los ciberdelitos o delitos informáticos, incluyendo la definición de qué constituye un delito cibernético y las sanciones aplicables. • Ley de ciberseguridad: revisar la existencia de una ley específica que aborde la ciberseguridad en su conjunto. Esta ley debe establecer directrices para la protección de sistemas de información, la gestión de riesgos y la coordinación institucional en el ámbito de la seguridad digital. • Estrategia de ciberseguridad: verificar si el país ha publicado una Estrategia Nacional de Ciberseguridad o seguridad digital que defina los objetivos y planes de acción para la protección de la infraestructura crítica y la gestión de amenazas cibernéticas.
Institucional	• Autoridad técnica: evaluar la existencia de una agencia o centro nacional de ciberseguridad encargado de la supervisión técnica y la coordinación de esfuerzos en materia de seguridad digital. Esta autoridad debe servir como el principal punto de contacto para el gobierno en cuestiones de ciberseguridad. • Órgano político: identificar la presencia de un órgano político, como un Ministerio o Secretaría, que tenga responsabilidades específicas en el ámbito de la ciberseguridad y coordine la implementación de políticas y estrategias a nivel gubernamental. • Equipos de respuesta: revisar la existencia y operatividad de equipos de respuesta a incidentes cibernéticos, como CERTs[a] o CSIRTs[b], que deben estar capacitados para manejar incidentes de seguridad y coordinar la respuesta ante ataques o vulnerabilidades.

Fuente: Elaboración propia.
[a] CERT: acrónimo que significa Computer Emergency Response Team o bien "Equipo de respuesta a emergencias informáticas". Un CERT es una organización responsable de coordinar la respuesta a incidentes de seguridad cibernética, como ataques cibernéticos, vulnerabilidades de seguridad, malware y otros incidentes relacionados con la ciberseguridad. Los CERT trabajan con organizaciones gubernamentales, empresas y organizaciones de la sociedad civil para detectar, analizar y responder a incidentes de seguridad cibernética. Además, los CERT proporcionan asesoramiento y recursos para ayudar a prevenir futuros incidentes.
[b] CSIRT: equipos de respuesta a incidentes de seguridad (CSIRT por las siglas de Computer Security Incident Response Team).

2. Tratamiento de datos personales

El tratamiento de datos personales se refiere a cualquier operación realizada con éstos, ya sea de forma automatizada o no. Esto incluye la recolección, registro, organización, modificación, uso, comunicación y/o eliminación de información sobre individuos identificados o identificables. La adecuada regulación y gestión del tratamiento de datos es esencial para proteger la privacidad de las personas y asegurar que las prácticas de manejo de datos cumplan con estándares legales y éticos.

Cuadro 2
Abordaje conceptual del tratamiento de datos personales

Parámetros de análisis	Descripción
Normativos	• Ley de Protección de Datos Personales: evaluar la existencia y el alcance de una legislación específica que regule el tratamiento de datos personales. La ley debe establecer los derechos de los individuos y las obligaciones de las entidades que manejan datos personales. • Otras reglamentaciones/normativas: identificar cualquier normativa complementaria o adicional que regule el tratamiento de datos, como regulaciones sectoriales o directrices emitidas por las autoridades de control. • Gobernanza de datos: revisar si existen documentos y recomendaciones emitidos por autoridades competentes que establezcan pautas para la gobernanza de datos y la coordinación institucional en la protección de datos personales.
Institucional	• Autoridad de aplicación: analizar la existencia, y si se encuentra nombrada, y el rol de una autoridad encargada de supervisar el cumplimiento de la normativa de protección de datos. Esta autoridad debe tener facultades claras y recursos adecuados para cumplir con sus responsabilidades de supervisión y regulación.

Fuente: Elaboración propia.

Recuadro 1
UE, CEPAL, OEA y RIPD promueven el desarrollo de un marco de protección de datos en América Latina y el Caribe

Unión Europea

La Unión Europea (UE) ha desempeñado un papel clave en el fortalecimiento de la protección de datos en América Latina y el Caribe (ALC) a través de su programa "Mejorando la Protección de Datos y Flujos de Datos ". Este programa ofrece asistencia técnica a los países de la región para la redacción y desarrollo de sus leyes de protección de datos, proporcionando apoyo bilateral durante los últimos ocho años. Países como Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Paraguay, Perú y Uruguay han recibido asistencia en este ámbito, lo que ha permitido la implementación de marcos normativos robustos y alineados con los estándares internacionales. Además, en el marco de la Alianza Digital, la UE, junto con la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), ha organizado diversas actividades y talleres sobre protección de datos, orientados a capacitar a funcionarios, compartir mejores prácticas y fomentar la cooperación regional en la creación de un entorno digital seguro y respetuoso con los derechos de las personas.

Comisión Económica para América Latina y el Caribe (CEPAL)

La Conferencia Ministerial sobre Sociedad de la Información y la Agenda Digital para América Latina y el Caribe (eLAC), bajo la coordinación de CEPAL, han sido un marco fundamental para el impulsar el desarrollo de políticas digitales en la región, y específicamente en el ámbito de la protección de datos personales. Desde el primer Plan de Acción sobre Sociedad de la Información acordado en Rio de Janeiro 2005, ya se reconocía la importancia de la protección de datos personales en el entorno digital, sentando las bases para futuras acciones.

Los planes de acción y las agendas digitales posteriores, acordados en 2008, 2010, 2013 2015, 2018, 2020 y 2022, han profundizado en la temática, promoviendo el fortalecimiento de marcos legales en protección de datos personales, la creación de autoridades de control y organismos independientes encargados de velar por el cumplimiento de la normativa, además de la importancia para facilitar el intercambio de experiencias y buenas prácticas entre los países de la región.

Organización de Estados Americanos

La Organización de Estados Americanos (OEA) a través de sus órganos se ha ocupado de la protección de los datos personales. La Asamblea General de la OEA desde 1966 ha aprobado resoluciones sobre la materia, instando a los Estados miembros a tomar determinadas acciones y en ocasiones confiriendo mandatos específicos a otros órganos de la Organización. En particular, es relevante destacar los siguientes hitos:

2000: se presentó el documento "El derecho de la información: acceso y protección de la información y datos personales en formato electrónico" en el Comité Jurídico Interamericano (CJI).

2012: el CIJ aprobó una "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas".

2015: el CIJ aprobó la "Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas".

2021: el CIJ aprobó las "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones".

Estos últimos principios tienen como objetivo principal establecer los fundamentos esenciales para una protección efectiva de datos. Los principios son[a]: 1. Finalidades legítimas y lealtad; 2. Transparencia y consentimiento; 3. Pertinencia y necesidad; 4. Tratamiento y conservación limitados; 5. Confidencialidad; 6. Seguridad de los datos; 7. Exactitud de los datos; 8. Acceso, rectificación, cancelación, oposición y portabilidad; 9. Datos personales sensibles; 10. Responsabilidad; 11. Flujo transfronterizo de datos y responsabilidad; 12. Excepciones; y, 13. Autoridades de protección de datos.

Red Iberoamericana de Protección de Datos

La Red Iberoamericana de Protección de Datos (RIPD) busca promover el desarrollo normativo sobre la protección de datos personales, y fomentar y fortalecer el intercambio de información entre el sector público y privado. La RIPD surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en junio de 2003, con la asistencia de representantes de 14 países iberoamericanos.

La red está conformada por las autoridades de protección de datos de Argentina, Brasil, Colombia, Costa Rica, Ecuador, México, Panamá, Perú, y Uruguay y el Consejo para la Transparencia de Chile a nivel regional y las autoridades de Andorra, España y Portugal.

Los países que poseen una ley vigente de protección de datos que no cuentan con una autoridad de control no pueden formar parte de la RIPD.

Desde la creación de la RIPD podemos destacar los siguientes hitos:

2010: compromiso de impulsar adopción de estándares regionales e internacionales para crear regulación con alta protección y facilitar el intercambio internacional (Declaración de México, 2010).

2013: la RIPD apoyó a las iniciativas de la OEA.

2015: compromiso de continuar desarrollando normas regionales para proteger datos personales y apoyar iniciativas de la OEA que permitan avances efectivos según estándares mínimos. (Declaración de Perú, 2015).

2016: propuesta para elaborar estandartes para la región (redactor INAI de México).

2017: en el marco del XVI Encuentro Iberoamericano de Santiago de Chile se aprueban los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[b], que han contado con el apoyo de la propia Comisión Europea.

2021: se aprobaron las cláusulas contractuales modelo para la transferencia internacional de datos personales de la Red Iberoamericana de Protección de Datos.

Los Estándares aprobados en 2017 buscan ser el modelo de referencia para la regulación futura en la región del derecho de protección de datos, así como para la revisión de las normas ya existentes para su actualización conforme a sus parámetros.

Fuente: Elaboración propia.

[a] OEA. Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, 2022.

[b] Red Iberoamericana de Protección de Datos. Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017.

II. Panorama regional sobre los diferentes enfoques en ciberseguridad y protección de datos personales

A. Marco metodológico para la evaluación del nivel de desarrollo de los países

A continuación, se presenta el abordaje metodológico empleado para analizar de manera comparativa el marco normativo de protección de datos personales y ciberseguridad en los países de América Latina y el Caribe. Este se basó principalmente en un análisis exhaustivo de fuentes secundarias de información, tales como bases de datos gubernamentales, publicaciones académicas, informes de organizaciones internacionales y documentos oficiales de entidades reguladoras.

Para asegurar un análisis comparativo, estructurado y riguroso, se definieron previamente los ejes clave que conforman un marco normativo robusto en cada país, además de tomar en cuenta la experiencia de la Unión Europea en la materia. Estos ejes incluyen disposiciones legales específicas, prácticas regulatorias y enfoques institucionales relacionados con la protección de datos y la ciberseguridad. Cada variable dentro de estos ejes fue evaluada utilizando una escala del 0 al 3, donde "0" indica un desarrollo inexistente o mínimo y "3" un desarrollo máximo. Esta clasificación permitió capturar de manera sistemática y objetiva el nivel de avance de cada país en estas áreas críticas.

El objetivo principal de este abordaje metodológico es proporcionar un panorama completo y actualizado que sirva como referencia para la formulación de políticas públicas y la mejora continua de los marcos normativos en la región. Este enfoque también facilita la identificación de tendencias regionales, así como de áreas de fortaleza y oportunidades de mejora en la protección de datos personales y la ciberseguridad en América Latina y el Caribe.

1. Ciberseguridad

Para la evaluación del nivel de desarrollo en ciberseguridad de los países de América Latina y el Caribe se realizó un análisis detallado de tres ejes clave y once variables específicas. Cada elemento y variable ha sido meticulosamente seleccionado para proporcionar una visión integral del marco institucional, del desarrollo de capacidades y de una cultura que promueva la ciberseguridad.

Cuadro 3
Variables para el análisis del nivel de desarrollo en ciberseguridad

Elemento	Variables	Descripción
Marco institucional	Estrategia y/o política nacional vigente	Evaluación de la existencia de una estrategia o política Nacional vigente que abarque la ciberseguridad o seguridad digital.
	Ley vigente	Análisis de la presencia de una ley nacional que regule la ciberseguridad y las infraestructuras críticas o servicios esenciales.
	Autoridad de aplicación	Verificación de la existencia de una autoridad estatal dedicada a aspectos de ciberseguridad o seguridad digital.
	Madurez y requerimientos legales para CERT/CSIRT	Evaluación del nivel de madurez en la implementación de equipos de respuesta ante incidentes (CERT/CSIRT) y los requisitos legales establecidos para su operación.
Capacidades	Gestión de crisis cibernética	Evaluación de las capacidades institucionales para manejar crisis cibernéticas.
	Gestión de infraestructura crítica	Análisis de la madurez en la protección de infraestructuras críticas frente a amenazas cibernéticas.
	Gestión de riesgos para infraestructura crítica o servicios esenciales	Evaluación de las acciones de notificación y gestión de riesgos frente a incidentes de ciberseguridad que afecten al país.
Cultura	Educación y programas de formación	Evaluación de la existencia de programas de formación y educación en ciberseguridad a nivel nacional.
	Programas de sensibilización	Análisis de campañas de sensibilización en ciberseguridad a nivel nacional.
	Coordinación internacional	Evaluación de las capacidades nacionales para la coordinación internacional en temas de ciberseguridad y seguridad digital.

Fuente: Elaboración propia.

Para la definición de estas variables de análisis, y como parte de la revisión bibliográfica, se estudiaron tres índices, desarrollados por organizaciones internacionales, que analizan el estado de situación de la ciberseguridad: ITU (2020)10, NCSI (2023)11 y BID/OEA (2019)12. Finalmente, los países fueron agrupados en tres categorías según los puntajes obtenidos en cada elemento y variable:

Cuadro 4
Categorías para el análisis del nivel de desarrollo en ciberseguridad

Categoría	Descripción
Madurez en desarrollo	Los países muestran avances sostenidos en la regulación a nivel nacional en ciberseguridad en las medidas de gestión de riesgos y seguridad de la información para la administración pública, algunos a través de decretos o leyes específicas sobre el tema. Se ha logrado avanzar en la protección de infraestructuras críticas y servicios esenciales, y muestras avances en las capacidades de respuesta ante incidentes y promueven la educación y en ciberseguridad.
Disparidad de esfuerzos	La regulación nacional no aborda las infraestructuras críticas o las aborda de manera inicial, existen acciones sostenida en alguna de las áreas base, pero no en todas las consideradas como respuesta ante incidentes o estrategia nacional. Existe cierto grado de avance en una de las áreas clave de ciberseguridad sin alcanzar un abordaje transversal al Estado. Hay, además, referencias a la necesidad de educación y sensibilización, pero no se reflejan en normativas nacionales.
Desarrollo inicial	Países tienen acciones solamente en algunos de los aspectos analizados, abordan a la ciberseguridad desde alguna de las áreas tradicionales sin dedicación de un organismo, con escaso nivel de avance en medidas de seguridad de la información para las administraciones públicas y capacidades de respuesta ante incidentes básicas o inexistentes. Hay países con equipo de respuesta ante incidentes y muestran poca campaña de sensibilización aún sin coordinación con otras áreas específicas. Existe escasa comprensión de la materia en su transversalidad.

Fuente: Elaboración propia.

[10] Índice de Ciberseguridad Global, UIT.
[11] NCSI National Cybersecurity Index.
[12] Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, BID/OEA.

En los anexos se incluye la matriz de análisis utilizada, detallando cada una de las variables evaluadas y sus respectivos criterios de puntuación.

2. Tratamiento de datos personales

Para la evaluación del nivel de desarrollo en tratamiento de datos personales de los países de América Latina y el Caribe se realizó un análisis detallado de cinco ejes clave y trece variables específicas. Cada uno de estos aspectos y variables ha sido seleccionado minuciosamente para proporcionar una evaluación integral en esta materia.

Cuadro 5
Variables para el análisis del nivel de desarrollo en tratamiento de datos personales

Elemento	Variables	Descripción
Institucional	Ley de protección de datos vigente	Evaluación de la existencia de una ley actualizada que regule el tratamiento de datos personales en el país y si está alineada con normas internacionales reconocidas.
	Autoridad de control	Análisis de la existencia de una autoridad estatal designada con poderes específicos para supervisar y asegurar el cumplimiento de las normativas de protección de datos personales.
Legitimación	Principios de protección de datos personales	Evaluación de los principios fundamentales considerados en la ley que deben ser seguidos durante el tratamiento de datos personales, como la finalidad, la proporcionalidad, la calidad de los datos, entre otros.
	Tratamiento lícito de los datos personales	Verificación de las bases legales claras y específicas que permiten el tratamiento lícito de los datos personales, asegurando que su procesamiento cumpla con los requisitos legales establecidos.
Regulación especial	Tratamiento de datos de menores	Evaluación de las disposiciones específicas para el tratamiento de datos personales de menores de edad, considerando su vulnerabilidad y los requisitos adicionales para su tratamiento.
	Categorías especiales de datos personales	Verificación de si la legislación contempla el tratamiento de categorías especiales de datos personales (como datos de salud, religión, u origen étnico) y si impone requisitos adicionales para su tratamiento lícito, debido a su naturaleza sensible.
Cumplimiento y derechos	Derechos de los titulares de datos	Examinación de si la legislación reconoce y garantiza derechos específicos para los titulares de datos personales, como el acceso, rectificación, cancelación y oposición (derechos ARCO), así como el derecho a la portabilidad de datos y la limitación del tratamiento.
	Responsable y encargado	Evaluación de si la legislación define claramente los roles y las responsabilidades de los responsables del tratamiento de datos personales (organizaciones o entidades que deciden sobre el tratamiento de los datos) y los encargados del tratamiento (entidades que tratan datos en nombre del responsable).
	Proactividad	Análisis sobre mecanismos de responsabilidad proactiva para fomentar prácticas de tratamiento de datos responsables y éticas, como la evaluación de impacto en la protección de datos (EIPD) y la consulta previa con la autoridad de protección de datos antes de llevar a cabo ciertas actividades de tratamiento de datos.
	Seguridad	Verificación sobre la obligación de implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdidas o destrucciones accidentales. Además, considera si establece procedimientos para la gestión de incidentes de seguridad que puedan comprometer la integridad de los datos personales.
	Regulación e implementación de garantías para la transferencia internacional	Análisis si la ley de protección de datos regula las transferencias internacionales de datos personales y si proporciona mecanismos para garantizar que dichas transferencias cumplan con las normativas de protección de datos, como decisiones de adecuación, cláusulas contractuales estándar o normas corporativas vinculantes.
Cultura y educación	Programas de sensibilización	Identificación de campañas o programas nacionales dirigidos a aumentar la conciencia y comprensión sobre la protección de datos personales entre la población en general y los actores involucrados en el tratamiento de datos.
	Educación y programas de formación en protección de datos personales y privacidad a nivel nacional	Identificación de programas formales de educación y capacitación en protección de datos personales y privacidad dirigidos a diversos sectores, incluyendo el público en general, empresas y entidades que manejan datos personales.

Fuente: Elaboración propia.

Finalmente, los países fueron agrupados en tres categorías según los puntajes obtenidos en cada variable.

Cuadro 6
Categorías para el análisis del nivel de desarrollo en tratamiento de datos personales

Categoría	Descripción
Madurez en desarrollo	Países que poseen normativas de protección de datos personales alineadas con estándares internacionales, indicando un desarrollo avanzado en principios, derechos de los titulares y regulación de transferencias internacionales. Aunque algunos países necesitan fortalecer los mecanismos para el tratamiento lícito de datos personales, existe un potencial para mejorar la educación y sensibilización sobre protección de datos mediante la implementación de más programas y campañas.
Regulación en proceso	Países que teniendo una base normativa sólida, aún no han establecido una autoridad de control o su implementación está pendiente. Necesitan mejorar la claridad y precisión en aspectos clave como los principios, derechos de los titulares y los mecanismos de tratamiento lícito. La falta de programas de sensibilización y educación sobre protección de datos para autoridades y ciudadanos representa una oportunidad de mejora.
Vacío normativo	Países que muestran un bajo desarrollo en normativa, sensibilización y educación sobre protección de datos personales. La mayoría carece de legislación vigente en esta área, con solo unos pocos países que tienen proyectos de ley en estudio. No se evidencian programas o campañas de sensibilización sobre protección de datos para autoridades o ciudadanos civiles, subrayando la necesidad urgente de un mayor impulso en la creación de marcos legales y actividades educativas.

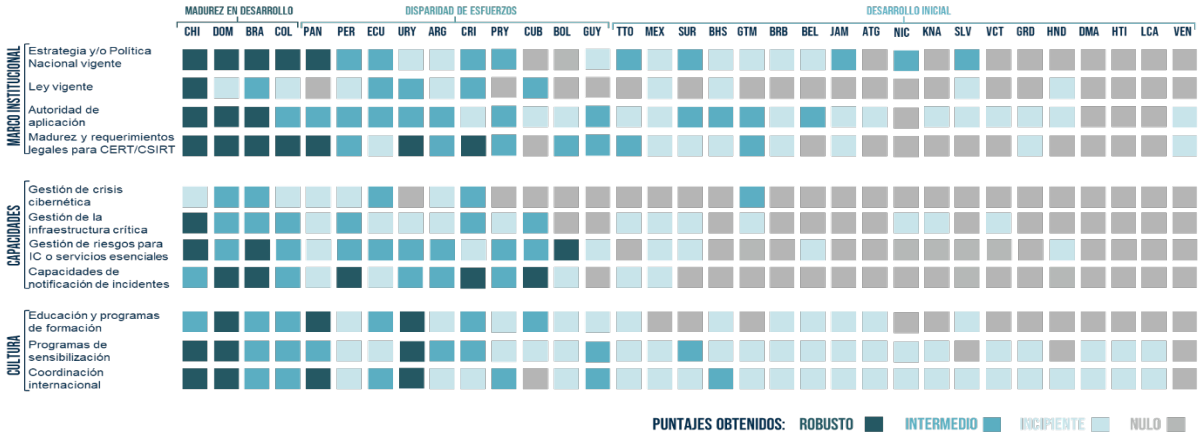
Fuente: Elaboración propia.

En los anexos se incluye la matriz de análisis utilizada, detallando cada una de las variables evaluadas y sus respectivos criterios de puntuación.

B. Estado de situación sobre la ciberseguridad

Se presenta un análisis del estado de desarrollo institucional y normativo de la ciberseguridad en los 33 países de la región. Esta evaluación se enfoca en tres ejes de análisis: marco institucional, capacidades y cultura. Para cada una de ellas, y como se observa en la siguiente ilustración, se han puntuado las principales variables de análisis con el objetivo de reflejar el estado de situación actual de cada país. Es importante resaltar que el relevamiento explora más allá de lo que está presente o no en la legislación, ya que también revisa la naturaleza de las instituciones encargadas, las prácticas administrativas y los lineamientos estratégicos de los gobiernos en esta materia. Esto se debe a que la ciberseguridad no sólo se establece en las reglas formales sino también en las informales (Kasim y Maharazu, 2023).

Diagrama 1
Grado de desarrollo de la ciberseguridad en los países de America Latina y el Caribe



Fuente: Elaboración propia.

En el caso de Brasil cabe señalar que, a pesar de no contar con una ley específica en ciberseguridad, se apoya en varios instrumentos estratégicos como la Política Nacional de Seguridad de la Información (2018), la Política Nacional de Ciberseguridad (2023) y la Estrategia Nacional de Ciberseguridad, además de leyes clave como el Marco Civil de Internet (Ley N° 12.965 de 2014), que establece principios para la seguridad digital, y la Ley N° 12.737 de 2012, que tipifica delitos informáticos. También destaca la Ley N° 11.829 de 2008, enfocada en combatir la pornografía infantil en línea, y la Ley N° 14.811 de 2024, centrada en proteger a menores frente a violencia en entornos digitales. En el ámbito legislativo, se tramita la Propuesta de Enmienda Constitucional N° 3 de 2020, que eleva la ciberseguridad a nivel constitucional, y proyectos como el N° 428 de 2024, que busca reforzar la ciberseguridad en servicios económicos, y el proyecto N° 177 de 2024, que propone una campaña contra ciberdelitos relacionados con inteligencia artificial. Este marco demuestra la evolución de Brasil en seguridad digital, aunque persisten retos en la implementación.

1. Marco institucional

Respecto a la existencia de una estrategia y/o política nacional vigente, se observa un alto grado de disparidad entre los países de la región, con algunos ya habiendo desarrollado y publicado su segunda estrategia de ciberseguridad mientras otros no muestran avance alguno. Este punto es sumamente importante ya que estas políticas son instrumentos claves para el desarrollo de una agenda proactiva en ciberseguridad. Es importante destacar que en este estudio se entiende que políticas de ciberseguridad funcionan como lineamientos generales en las agendas de ciberseguridad de los países, mientras que las estrategias de ciberseguridad son las herramientas de aplicación.

Entre 2017 y 2018, se observa una primera generación de estrategias de ciberseguridad, pero con escaso peso administrativo. A partir del 2020 comienza una segunda ola de estrategias en países de América Latina y el Caribe, en gran parte motivadas por la pandemia, la cual amplificó la exposición de los gobiernos y las empresas a ciberataques. Por otro lado, 2023 marca el comienzo de consolidación con segundas estrategias y políticas en países con un mayor grado de desarrollo, como Brasil, Chile, Argentina y Costa Rica. Otros países como Bolivia, Guyana, Honduras y Uruguay se encuentran en proceso activo de elaboración. Uruguay posee un Marco de Ciberseguridad aprobado en 2022 que funciona como marco de referencia en la materia. Se estima que la estrategia acompañante será publicada en 2025. Por otro lado, los países principalmente de la subregión del Caribe, como ser Haití, Cuba, Santa Lucía, San Cristóbal y Nieves, no evidencian ningún proceso activo.

Diagrama 2
Línea de tiempo de estrategias y políticas de ciberseguridad

Fuente: Elaboración propia.

En cuanto a la existencia de autoridad de aplicación, la mayoría de los países de la región posee una autoridad que lleva adelante algún tipo de agenda en Ciberseguridad. Sin embargo, su grado de madurez varía. Solo Brasil, Chile y Republica Dominicana poseen autoridades especializadas en la

materia, de carácter técnico, que atienden funciones de manera integral que contribuyen y se coordinan con otras políticas. Brasil con el Gabinete de Seguridad Institucional (GSI[13]), Republica Dominicana con el Centro Nacional de Ciberseguridad (CNCS[14]) y Chile con la Unidad de Coordinación de Ciberseguridad[15] del Ministerio del interior y Seguridad Pública. Además, Chile se encuentra en proceso de creación de la Agencia Nacional de Ciberseguridad creada por la Ley Marco recientemente aprobada.

Se puede ver que 12 países cuentan con un organismo que atiende funciones de ciberseguridad en el marco de una política más amplia. Por ejemplo, Argentina cuenta con la Dirección Nacional de Ciberseguridad dependiente de la Secretaría de Innovación Pública[16], similar a la Dirección de Ciberseguridad del Ministerio de Tecnologías de la Información y Comunicación (MITIC) en Paraguay. También en este nivel se observan agencias como Agesic[17] en Uruguay. Asimismo, la mayoría de los países de la región poseen una autoridad que atiende alguna de las funciones de ciberseguridad. En estos casos se observan autoridades que llevan adelante estas atribuciones en ciberseguridad pero con poca coordinación interministerial y baja constancia política. Finalmente, se observan cuatro países que no poseen ningún área con funciones de ciberseguridad asignada: Nicaragua, Dominica, Haití y Santa Lucía.

Recuadro 2
Ley de ciberseguridad en Chile: el único caso en la región

El 26 de marzo de 2024, se promulgó la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. La Ley es un hito en la región ya que es la primera legislación de esta naturaleza. Busca garantizar la protección y continuidad de los servicios esenciales en caso de ciberataques, aplicando obligaciones a las empresas tanto privadas como públicas.

La Ley Marco considera servicios esenciales a las siguientes actividades:

- Generación, transmisión o distribución eléctrica.
- Transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento.
- Telecomunicaciones e infraestructura digital.
- Servicios digitales y servicios de tecnología de la información gestionados por terceros.
- Transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva.
- Banca, servicios financieros y medios de pago.
- Administración de prestaciones de seguridad social.
- Servicios postales y de mensajería.
- Prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos.
- La producción y/o investigación de productos farmacéuticos.

Además, se consideran servicios esenciales a aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional o los prestados bajo concesión de servicio público. La ANCI podrá calificar otros servicios como esenciales mediante resolución o consulta pública.

Los operadores de servicios esenciales deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional). Se consideran incidentes significativos a aquellos que interrumpan la continuidad de un servicio esencial o afecten la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales.

Fuente: Elaboración propia con base en Ministerio del Interior y Seguridad Público de Chile (2024).

[13] Gabinete de Segurança Institucional. La GSI/PR, a pesar de ser el principal órgano con competencias en la materia, no es el único, también existen otros órganos, como la Agencia Nacional de Telecomunicaciones y el Ministerio de Justicia y Seguridad Pública, que también tienen competencias sobre el tema.

[14] CNCS. Centro Nacional de Ciberseguridad de República Dominicana.

[15] Unidad de Ciberseguridad de Chile.

[16] Recientemente se ha creado en Argentina la Agencia Federal de Ciberseguridad, bajo la esfera del Sistema Nacional de Inteligencia. Sin embargo, no ha sido aún especificado hasta qué punto esta nueva Agencia reemplaza a la ya existente Dirección ni cuántas de sus funciones absorberá.

[17] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay.

Diagrama 3
Madurez y requerimientos legales para el CERT/CSIRT

Niveles de madurez	Países	Ejemplos
7 países cuentan con un CERT/CSIRT de gobierno con mandato por norma nacional que le asigna rol y responsabilidades.	Uruguay, Panamá, Chile, Costa Rica, República Dominicana, Brasil y Colombia.	**BRASIL** ha establecido una Red Federal, un Plan Federal y al CTIR como Equipo de Respuesta ante incidentes como coordinador y concentrador, el cual es miembro de la Red de CSIRT de las Américas.
7 países poseen un CSIRT cuyo rol y responsabilidades están definidos en una normativa, pero no tiene un nivel jerárquico nacional para brindar servicios a todo el Estado Nacional.	Guyana, Guatemala, Bolivia (Estado Plurinacional de), Trinidad y Tobago, Argentina, Paraguay y Perú.	**GUYANA** estableció su CSIRT por Decisión de la Jefatura de Gabinete. El equipo funcionó como una unidad dentro del Ministerio del Interior hasta Sep 30, 2016. Ahora está bajo el ámbito de la Autoridad Nacional de Gestión de Datos dentro de la Oficina del Primer Ministro.
8 países poseen un CSIRT, pero su rol y responsabilidades no están definidos en el marco legal.	Venezuela (República Bolivariana de), Bahamas, Barbados, Jamaica, Suriname, México, Ecuador y Granada.	**JAMAICA** cuenta con un CIRT bajo la esfera de la Oficina del Primer Ministro. Sin embargo, su creación fue dispuesta solo a través de la Estrategia de Ciberseguridad de 2015.
12 países no poseen un CERT/CSIRT.	Antigua y Barbuda, Dominica, Santa Lucía, Haití, Honduras, Cuba, Saint Kitts y Nevis, San Vincente y las Granadinas, Bélice, El Salvador y Nicaragua.	

Fuente: Elaboración propia.

Evaluando la madurez y los requerimientos legales para los equipos de respuesta CERT/CSIRTs se observa que solo 7 países en la región cuentan con un CERT/CSIRT de gobierno con mandato por norma nacional que le asigna rol y responsabilidades: Uruguay, Panamá, Chile, Costa Rica, Republica Dominicana y Colombia. Por ejemplo, Brasil ha establecido una Red Federal, un Plan Federal y al CTIR, miembro de la Red de CSIRT de las Américas[18], como coordinador.

Por otro lado, 7 países poseen un CSIRT cuyo rol y responsabilidades están definidos en una normativa, pero no tiene un nivel jerárquico nacional para brindar servicios a todo el Estado Nacional. Este es el caso de Argentina, Guyana, Guatemala, Bolivia, Trinidad y Tobago, Paraguay y Perú. Por ejemplo, Guyana estableció su CSIRT por Decisión de la Jefatura de Gabinete. El equipo funcionó como una unidad dentro del Ministerio del Interior hasta el 30 de Septiembre de 2016 pero ahora se encuentra bajo la órbita de la Autoridad Nacional de Gestión de Datos dentro de la Oficina del Primer Ministro.

Finalmente, 8 países, entre los que se encuentran Venezuela, Bahamas, Argentina y otros, poseen un CSIRT pero su rol y responsabilidades no están definidos en el marco legal. Por ejemplo, Jamaica cuenta con un CIRT bajo la esfera de la Oficina del Primer Ministro. Sin embargo, su creación fue dispuesta solo a través de la Estrategia de Ciberseguridad[19] de 2015. El resto de los países relevados no poseen un CERT/CSIRT.

[18] Red de los Equipos de Respuestas ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los Estados Miembros de la Organización de los Estados Americanos.

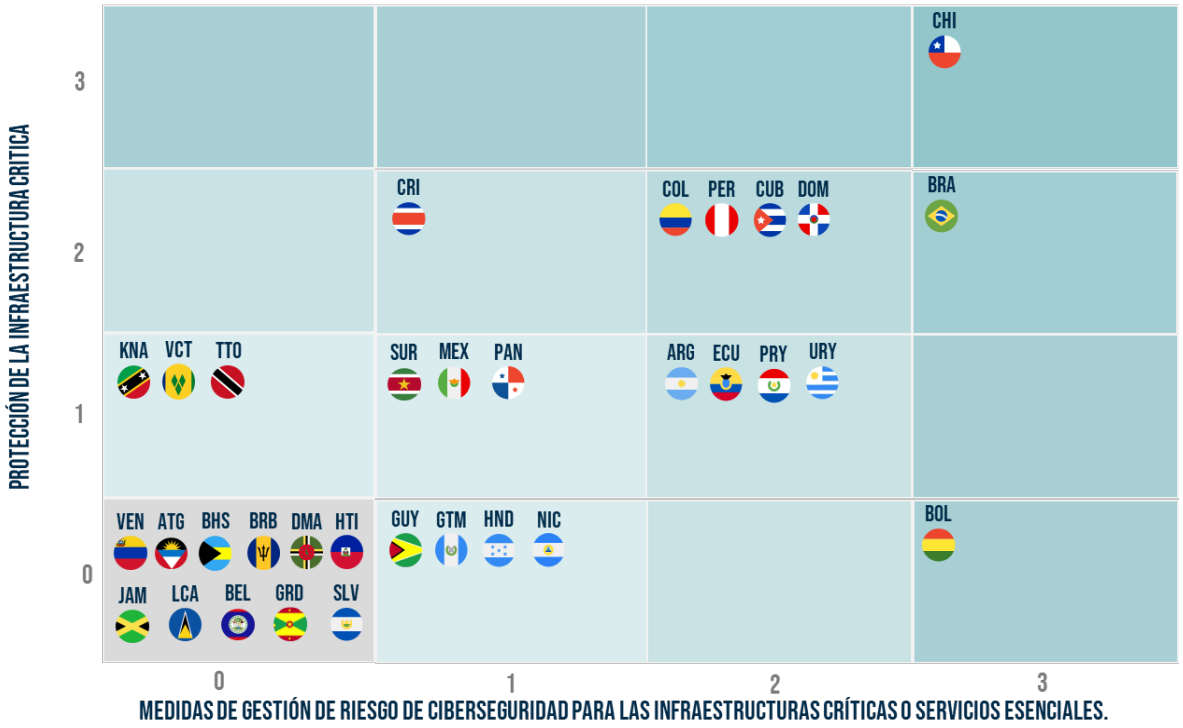
[19] Estrategia Nacional de Seguridad Cibernética (2015) de Jamaica, desarrollada con el apoyo técnico del Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA).

2. Capacidades

El eje de análisis "Capacidades" evalúa cuatro variables, entre las que se encuentra la gestión de la infraestructura críticas, por un lado, y medidas de gestión de riesgo de ciberseguridad para las Infraestructuras críticas o servicios esenciales, por el otro. Se observa que existe cierta correlación entre ambas variables: aquellos países que presentan un nivel alto de madurez en la protección de su infraestructura critica también presentan avances en las medidas de gestión de riesgos.

Chile, por ejemplo, cuenta con ley para las infraestructuras críticas en las que las define y asigna su protección a la defensa nacional. Además, la reciente Ley Marco aborda específicamente sus aspectos tecnológicos y cibernéticos. Asimismo, el país ha avanzado aún antes de su Ley Marco en brindar requisitos de ciberseguridad para varios sectores, como por ejemplo para el sector eléctrico, el sector de las telecomunicaciones, el sector de la salud y para la Administración Pública en general. Por su parte, Brasil ha establecido una política Nacional de Infraestructuras Críticas y ha incluido en su Política Nacional de Ciberseguridad[20] la protección de los aspectos cibernéticos de los sectores ya definidos en la Política principal. Por otro lado, también ha implementado requisitos mínimos para la Administración pública Federal desde 2021, para el sector de telecomunicaciones y el sector aeronáutico, desde la Agencia de Aviación Civil.

Diagrama 4
Correlación entre protección de la infraestructura y medidas de gestión de riesgos



Fuente: Elaboración propia.

[20] Decreto Nº 11.856, del 26 de diciembre de 2023 de Brasil.

Otra de las variables evaluadas en este eje corresponde a la gestión de la cibercrisis. Cabe destacar que es en este aspecto donde la región se encuentra más rezagada, identificando solo niveles de desarrollo intermedios e incipientes. Solo 10 países abordan algún aspecto de cibercrisis, mientras que el resto de los 23 países no evidencian ningún tipo de desarrollo en la materia. En los primeros lugares se identificaron los casos de Brasil, Republica Dominicana, Costa Rica, Guatemala y Ecuador.

Brasil en 2019 creó por decreto la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno para abordar temas que exceden el alcance de Ministerios. En particular se indican los temas Seguridad de la Información, la ciberseguridad y las infraestructuras críticas. Por otra parte, en la Estrategia Nacional[21] de Republica Dominicana se contempla la resiliencia de las infraestructuras. Además, el gobierno ha realizado simulacros de crisis cibernética con impacto en desastres nacionales. Ecuador, en su Política Nacional, aborda como uno de los objetivos la gestión de la crisis de ciberseguridad. Además, en la Estrategia Nacional de Ciberseguridad[22] se contempla en el Pilar 2, Objetivo 2.1: "Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para las crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional". Impulsada en gran parte por los ciberataques de 2022, la Comisión Nacional de Emergencia de Costa Rica emitió en Junio de ese mismo año el Plan General de la Emergencia de Ciberataques[23], cuyo objetivo es desarrollar las accionas y servicios necesarios para contener y prevenir nuevos ataques en contra de los Sistemas de Información del Estado.

Por otro lado, otros países con un desarrollo más incipiente abordan algún aspecto necesario para gestionar una crisis nacional originada en un incidente de ciberseguridad pero no completan los requisitos como normas legales u organismo con asignación y capacidades específicas. Chile, por ejemplo, posee un consejo interministerial, algo necesario para abordar una crisis cibernética, pero no lo define entre las funciones de atención de este. Argentina, por su parte, ha publicado una resolución desde el Ministerio de Seguridad sobre tratamiento de incidentes relevantes. Sin embargo, no se observa vinculación con la Autoridad de Ciberseguridad. Por otro lado, Panamá y Perú han realizado simulacros de crisis cibernéticas, demostrando comprensión de la necesidad de abordar la materia, aunque ninguno de los dos posee normativa relativa a la materia u organismos con responsabilidad específica en su gestión.

En materia de notificación de incidentes, el grado de avance en la región es mayor. Cinco países tienen directrices normativas sobre la notificación o atención ante incidentes para la Administración Pública Nacional (APN) e Infraestructuras Críticas: Brasil, Perú, Cuba, Costa Rica y Republica Dominicana.

Otros cinco países tienen directrices normativas sobre la notificación o atención ante incidentes solo para la Administración Pública Nacional: Chile, Argentina, Colombia, Paraguay y Uruguay. Paraguay, por ejemplo, según el Decreto 2274/2019[24], existe la obligación de notificar incidentes para las entidades de la APN. Las instituciones del sector público están obligadas a comunicar y denunciar ante el MITIC todos los incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional, siguiendo los procedimientos reglamentados por el Ministerio.

Finalmente, cinco países de la región se encuentran en un nivel incipiente de desarrollo en materia de notificación de incidentes. Entre estos se encuentran Panamá, Trinidad y Tobago, Ecuador, Bolivia y México. Panamá, por ejemplo, no cuenta con una normativa específica en la materia. Sin embargo, en el CSIRT se pueden reportar incidentes. No existen plazos para dicho reporte, ni un procedimiento específico establecido. Otro caso ilustrativo es el de México, en donde la Guardia Nacional emitió un protocolo de gestión de incidentes para la Administración Pública Nacional (APN) pero que no tiene peso administrativo.

---

[21] Estrategia Nacional de Desarrollo 2030 de República Dominicana.
[22] Estrategia Nacional de Ciberseguridad (2020) de Ecuador.
[23] Plan General de la Emergencia de Ciberataques (2022) de Costa Rica.
[24] Decreto No. 2274. Por el cual se reglamenta la Ley No. 6207, del 22 de octubre de 2018 'Que crea el Ministerio de Tecnologías de la Información y Comunicación y establece su Carta Orgánica', Paraguay.

Por último, son 18, de los 33 países, que cuentan no cuentan con capacidad en materia de notificación de incidentes. Estos son países principalmente de la región Caribe, excluyendo a los ya mencionados previamente en esta sección.

Diagrama 5
Capacidades en materia de notificación de incidentes a nivel nacional

Nivel de desarrollo en notificación de incidentes	Países
Robustez en capacidades para notificación de incidentes: 5 países tienen directrices normativas sobre la notificación o atención ante incidentes para la Administración Pública Nacional (APN) e Infraestructuras Críticas.	República Dominicana Brasil, Perú, Cuba y Costa Rica
Intermedios en capacidades para notificación de incidentes: 5 países tienen directrices normativas sobre la notificación o atención ante incidentes para la APN.	Chile, Argentina Colombia, Paraguay y Uruguay
Incipientes en notificación de incidentes: 5 países sólo tienen algún lineamiento sobre la notificación o atención ante incidentes.	Panamá, Trinidad y Tabago, Ecuador Bolivia (Estado Plurinacional de) y México
Nula capacidad en materia de notificación de incidentes: 18 países no tienen ningún tipo de lineamiento en materia de notificación de incidentes.	Suriname, Bahamas, Guatemala, Barbados, Belice, Jamaica, Antigua, Nicaragua, Saint Kitts y Nevis, El Salvador, San Vincente y las Granadinas, Granada, Honduras, Dominica, Haití, Santa Lucía, Venezuela y Guyana

Fuente: Elaboración propia.

3. Cultura

El último eje de análisis "Cultura" describe la situación en la que se encuentra la región en materia de educación y sensibilización en ciberseguridad. El relevamiento muestra que existen varios programas de sensibilización, aunque con baja constancia. Sin embargo, el mayor déficit se encuentra en la disponibilización de programas de educación y formación de cuadros técnicos.

Los casos más destacados son Republica Dominicana y Chile. El primero, por ejemplo, tiene como objetivo estratégico promover la cultura y la educación en materia de ciberseguridad. Además, el Centro Nacional de Ciberseguridad (CNCS) ha creado una trayectoria de formación en seguridad digital. El CNCS es activo también en campañas de sensibilización: elabora boletines y material de difusión en materia de sensibilización de ciberseguridad. Además, lidera el grupo de trabajo de medidas de fomento de la confianza en el ciberespacio. Por su parte, durante los últimos años la Coordinación Nacional de Ciberseguridad de Chile ha organizado diversos eventos orientados a sensibilizar y formar a la sociedad en aspectos centrales de la ciberseguridad. Además, el CSIRT posee un blog técnico en el que comparten recomendaciones para la gestión de riesgos y elaboración de planes de ciberseguridad, principalmente orientados a empresas que posean infraestructuras de información.

Uruguay ha realizado importantes avances en capacitación y sensibilización en ciberseguridad a través de iniciativas lideradas por Agesic. El 14 de diciembre de 2022, se presentó la primera currícula técnica en Ciberseguridad del país, desarrollada en colaboración con la Facultad de Ingeniería (Instituto de Computación) y la Fundación Julio Ricaldoni, con el apoyo del BID. Este programa académico ofrece a las personas con educación secundaria completa la posibilidad de formarse o reconvertirse profesionalmente en ciberseguridad. La currícula es flexible y de acceso libre, para que las instituciones educativas puedan adaptarla según sus propuestas académicas y las demandas del mercado, además de facilitar la continuidad en estudios de grado y posgrado. Paralelamente, Agesic publica en su sitio

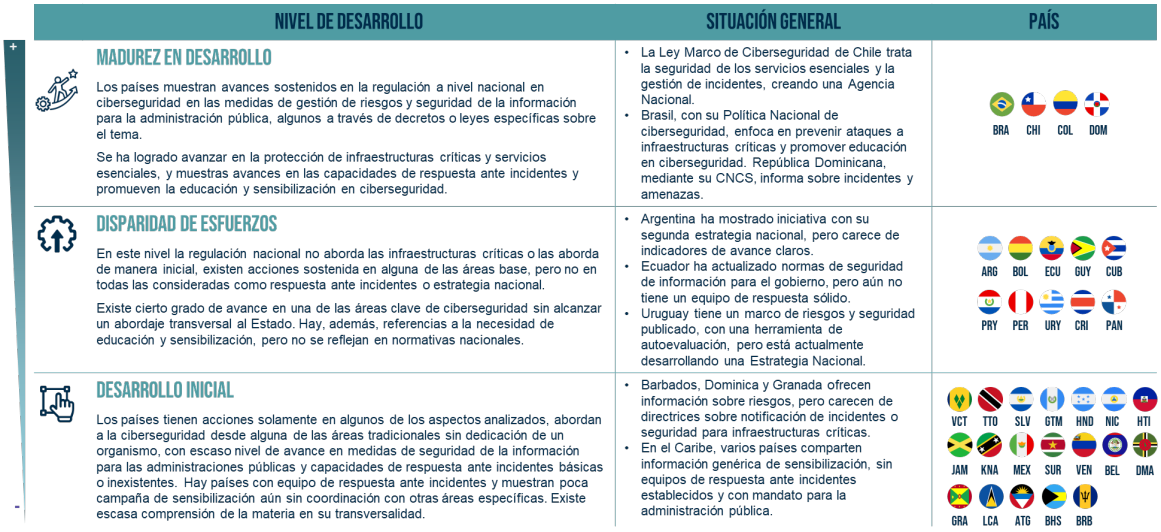
web una oferta académica actualizada sobre carreras terciarias, cursos, certificaciones, posgrados y especializaciones en ciberseguridad. Asimismo, desarrolla campañas de sensibilización, como "Seguro te Conectás", que proporciona información y recomendaciones prácticas para pequeñas empresas y emprendedores, así como materiales para promover el manejo seguro de la información personal. Estas acciones reflejan el compromiso de Uruguay con la formación técnica y la promoción de una cultura de ciberseguridad en todos los sectores de la sociedad.

A nivel de coordinación regional, es importante notar el trabajo de la Comunidad del Caribe (Caricom[25]). A partir de 2023, a través de su Agencia de Implementación para el Crimen y la Seguridad, ha organizado eventos regionales de sensibilización y formación regional sobre ciberseguridad en los países miembros de Caricom. Estos cursos regionales están dirigidas a altos funcionarios, ministros de gobierno, parlamentarios, responsables políticos y público en general.

C. Análisis sobre el nivel de desarrollo de la ciberseguridad

Tal como se ha presentado previamente, a partir del relevamiento se logran identificar tres niveles de desarrollo o madurez en ciberseguridad: madurez en desarrollo, disparidad de esfuerzos y desarrollo inicial.

Diagrama 6
Categorías según el nivel de desarrollo en ciberseguridad



Fuente: Elaboración propia.

Madurez en desarrollo: Los países muestran avances sostenidos en la regulación a nivel nacional de la ciberseguridad en las medidas de gestión de riesgos y seguridad de la información para la administración pública, algunos a través de decretos o leyes específicas sobre el tema. En estos casos, se ha logrado avanzar en la protección de infraestructuras críticas y servicios esenciales, y se pueden apreciar avances en las capacidades de respuesta ante incidentes. Por ejemplo, mediante su Ley Marco de Ciberseguridad Chile aborda la ciberseguridad de los servicios esenciales y la obligación de gestionar incidentes de ciberseguridad, así como la creación de una Agencia Nacional. Brasil, con su Política Nacional de Ciberseguridad adopta como principio la prevención de incidentes y ciberataques dirigidos

[25] CARICOM: Caribbean Community.

a infraestructuras críticas, y como objetivo desarrollar educación y formación técnico-profesional en ciberseguridad. República Dominicana, a través del Centro Nacional de Ciberseguridad (CNCS) publica e informa estadísticas sobre incidentes y amenazas. Finalmente en Colombia, principalmente a partir de 2022, se emitieron una serie de decretos destinados a abordar la Ciberseguridad de forma integral en toda la administración pública como, por ejemplo, el Decreto 338 de 2022[26] que, entre otras cosas, desarrolló un conjunto de medidas para la gestión de incidentes de manera coordinada y las herramientas necesarias para llevarla a cabo.

Disparidad de esfuerzos: La regulación nacional no aborda las infraestructuras críticas o las aborda de manera superficial, existen acciones sostenida en alguna de las áreas base pero no en todas las consideradas como pueden ser la respuesta ante incidentes o las estrategias nacionales. Además, se tiene cierto grado de avance en una de las áreas clave de Ciberseguridad sin alcanzar un abordaje transversal al Estado. Existen referencias a la necesidad de educación y sensibilización, pero no se reflejan en normativas nacionales. Por ejemplo, países como Argentina, con su segunda Estrategia Nacional, han mostrado iniciativa. No obstante, no se observan indicadores de avance de la Estrategia. Argentina también ha emitido lineamientos en materia de respuesta ante incidentes, pero no se encuentra información de acciones consistentes realizadas.

Por otro lado, Ecuador ha actualizado sus normas en materia de seguridad de la información para gobierno sin establecer un equipo de respuesta fuerte. Uruguay tiene un marco de riesgos y seguridad publicado y una herramienta de autoevaluación. Sin embargo, sólo recientemente ha comenzado a abordar una Estrategia Nacional.

Desarrollo inicial: los países en Desarrollo inicial tienen acciones solamente en algunos de los aspectos analizados, abordan a la ciberseguridad desde alguna de las áreas tradicionales sin dedicación de un organismo. Cuentan con escaso nivel de avance en medidas de seguridad de la información para las administraciones públicas y capacidades de respuesta ante incidentes básicas o inexistentes.

En esta categoría, se observan algunos países con equipos de respuesta ante incidentes pero sin requerimientos legales para el funcionamiento de estos. Otros directamente no poseen equipos. Por ejemplo, países como Barbados, Dominica y Granada publican información sobre sensibilización en riesgos, pero carecen de lineamientos en notificación de incidentes o medidas de seguridad para infraestructuras críticas. Además, estos países en general no tienen equipos de respuesta ante incidentes establecidos con su alcance definido con mandato para la administración pública.

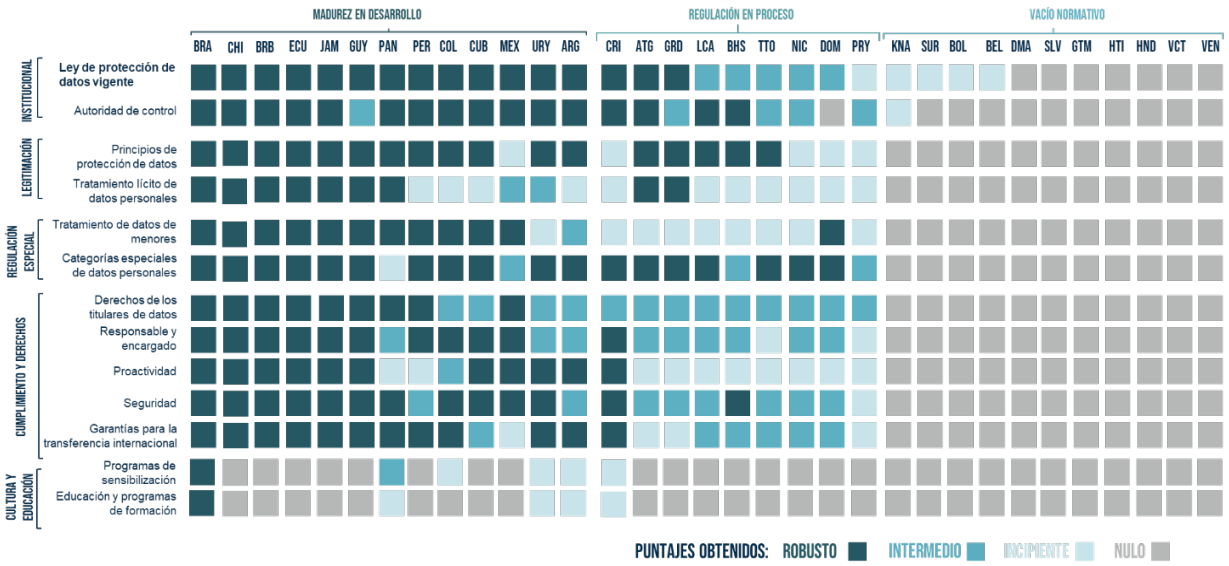
San Cristóbal y Nieves sancionó en 2018 su Ley de Protección de Datos. Sin embargo, esta aún no ha entrado en vigor. Debido a esto, no se han implementado ninguna de las medidas que la legislación considera. Un ejemplo de esto es la pendiente creación del Comisario de Información que cumpliría el rol de autoridad de control.

D. Estado de situación sobre el tratamiento de datos personales

Esta evaluación se enfoca en cinco ejes de análisis que permiten identificar tres tipos de avances sobre el tratamiento de datos personales en la región. En la siguiente ilustración, se presenta un mapa de calor que refleja la puntuación otorgada a cada país según ciertos elementos y el contenido de su legislación, categorizándolos finalmente en uno de los tres niveles de desarrollo identificados: madurez en desarrollo, regulación en proceso y vacío normativo.

[26] Decreto 338 de 2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias deGobernanza de Seguridad Digital y se dictan otras disposiciones" de Colombia.

Diagrama 7
Grado de desarrollo del tratamiento de datos personales en los países de América Latina y el Caribe



Fuente: Elaboración propia.

Como se observa en la ilustración, Barbados, Brasil, Ecuador y Jamaica son los países mejor posicionados. Poseen un nivel de desarrollo de su legislación robusto sobre ciertos factores institucionales, de legitimación, de regulación especial y de cumplimiento y derechos. Asimismo, en una gran parte de los países no se logró identificar iniciativas vinculadas a fortalecer la cultura y la educación en este ámbito. Es decir, no se han identificado programas públicos de sensibilización o de formación en tratamiento de datos personales vigentes. Algunas excepciones al respecto son Brasil, Panamá, Uruguay, Argentina y Costa Rica.

1. Institucional

El eje "Institucional" tiene como objetivo destacar la existencia de normativa específica en materia de protección de datos personales, incluyendo la previsión de una autoridad de control y su efectiva operación. Se evalúa si existe una ley vigente que regule el tratamiento de datos personales en el país, asegurando su alineación con normas internacionales, y si hay una autoridad estatal con facultades específicas para supervisar el cumplimiento de esta regulación. Según el relevamiento realizado, 22 de los 33 países de la región cuentan con una legislación actualizada en protección de datos personales.

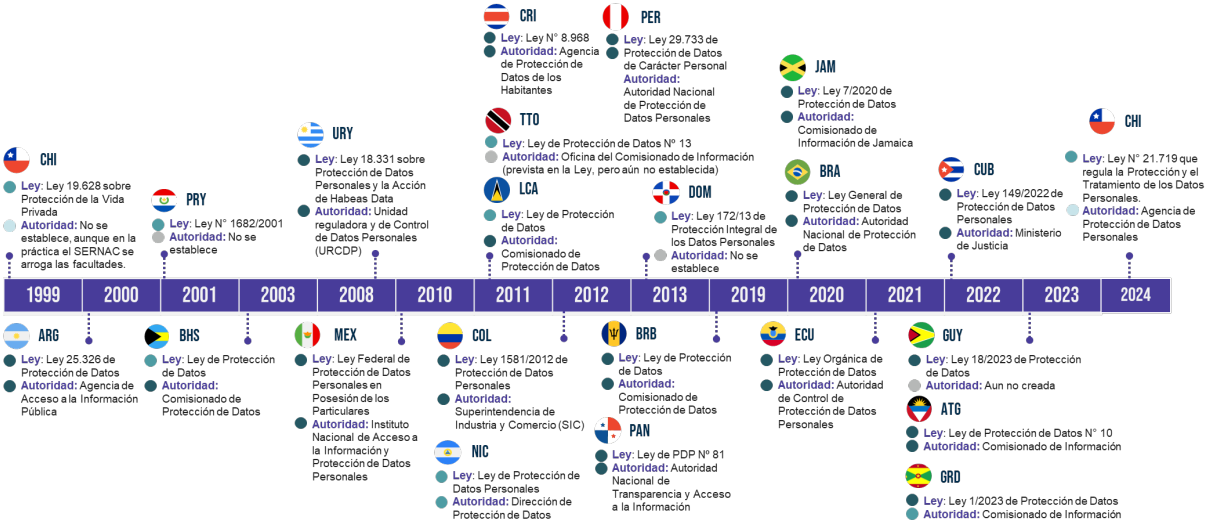
Argentina, Chile, Uruguay, México, Perú, Colombia, Barbados, Panamá, Brasil, Jamaica, Ecuador, Cuba y Guyana son los países mejor posicionados ya que poseen leyes de protección de datos personales alineada con normas internacionales. Por ejemplo, la Ley 18/2023 de Protección de Datos de Guyana[27] fue aprobada en 2023. Esta posee principios, derechos e institutos de protección de datos acordes y alienados con la normativa internacional.

[27] Ley 18/2023 de Protección de Datos de Guyana.

Otros países poseen legislaciones que, si bien no son específicas de protección de datos personales, determinan ciertas obligaciones respecto a la gestión y recolección de datos. Este es el caso, por ejemplo, de Paraguay. La Ley N° 1682/2001[28] (modificada por la Ley N° 1969/2002[29] y la Ley N° 5543/2015[30]) regula la información privada, el uso de datos personales con fines crediticios y establece obligaciones generales respecto del uso de estos.

En la siguiente línea del tiempo se observan las legislaciones vigentes en la región, las autoridades encargadas de la protección de datos personales y los puntajes obtenidos.

Diagrama 8
Línea del tiempo de legislaciones de protección de datos personales vigentes



Fuente: Elaboración propia.

De los 22 países que poseen legislación en la materia, todos tienen leyes vigentes que establecen la creación de una autoridad de control que ejerza funciones de monitoreo de cumplimiento y aplicación de la ley. Existen algunos países como Chile, Guyana, Granada, Trinidad y Tobago y Nicaragua, en los cuales la ley dispone la creación de una autoridad de control específica pero la misma aún no ha sido creada o esta en proceso de creación. De los 11 países restantes, Surinam y Bolivia poseen al momento del presente informe proyectos de ley de protección de datos bajo estudio del Congreso. Es importante destacar también el caso de San Cristóbal y Nieves ya que el país ha aprobado en 2018 su Ley de Protección de Datos, pero ésta todavía no ha entrado en vigor. Asimismo, Chile promulgó el 25 de noviembre de 2024 la Ley 21719 que regula la Protección y el Tratamiento de los Datos Personales, creando además la Agencia de Protección de Datos Personales.

2. Legitimación

El eje "Legitimación" releva y refleja los principios rectores contenidos en la normativa de protección de datos, lo cuales rigen las actividades de tratamiento y deberán utilizarse como guía y orientación respecto de la recolección, tratamiento, y almacenamiento de los datos personales. Asimismo, analiza

[28] Ley Nº 1682 que reglamenta la información de carácter privado de Paraguay, aprobada en 2001.
[29] Ley nº 1.969 que modifica, amplía y deroga varios artículos de la ley nº 1682/2001 "que reglamenta la información de carácter privado" de Paraguay, aprobada en 2022.
[30] Ley nº 5543 que modifica los artículos 5° y 9° de la ley nº 1.682/01 "que reglamenta la información de carácter privado", modificado por la ley nº 1.969/02 de Paraguay, aprobada en 2015. La protección de datos se refiere principalmente a regulaciones y políticas, mientras que la ciberseguridad tiene un componente operativo más diverso y complejo que dificulta su implementación.

la aplicación de los principios y los mecanismos de licitud contenidos en la regulación que permiten el tratamiento lícito de los datos personales. Estos mecanismos refieren a las bases legales que respaldan la legitimidad del tratamiento. Es decir que al momento de recolectar los datos personales y llevar adelante las actividades de tratamiento, los responsables deberán basarse en las bases legales enumeradas en la legislación para legitimar el procesamiento de datos. En particular, se releva si la ley de protección de datos personales prevé principios de protección de datos personales aplicables al tratamiento de datos y si esta prevé mecanismos de licitud para el tratamiento de los datos personales.

A partir de los puntajes obtenidos, los países se han agrupado en 4 categorías distintas. En primer lugar, 12 países (36%) se encuentran en la categoría de "Sin Cobertura". Esto significa que no disponen de leyes de protección de datos personales, o que la regulación vigente no contempla principios claros para el tratamiento de datos personales. Este es el caso de Surinam, Venezuela, Belice, Dominica, El Salvador, Guatemala, Honduras, San Cristóbal y Nieves, San Vicente y las Granadinas, Bolivia, Haití y Paraguay.

Bolivia, por ejemplo, ha intentado normar sin éxito el uso de datos personales en el país. Este país posee un anteproyecto de Ley de Protección de datos Personales[31] que fue presentado en el Congreso en diciembre de 2021, con solicitud de reposición para tratamiento en marzo y diciembre de 2023. En marzo de 2023, se socializó un nuevo Anteproyecto de Ley de Protección de Datos Personales, sin embargo no llegó a ser presentado para tratamiento ante la Cámara de Diputados. De igual forma, Surinam posee un proyecto de ley de Protección de Datos bajo estudio. El proyecto de ley se presentó a la Asamblea Nacional de Surinam en 2018 y fue examinado por el Comité de Relatores el 21 de enero de 2021. El Comité formuló varias preguntas y solicitó comentarios. Sin embargo, no ha habido más avances desde entonces, y sigue siendo examinado en la Asamblea Nacional.

Por otro lado, 3 países (9%) están clasificados en la categoría de "Principios Básicos". Esto se debe a que Costa Rica, Nicaragua y República Dominicana consideran únicamente el consentimiento de los titulares como el principio fundamental para el tratamiento lícito de los datos. Por ejemplo, el artículo 5 de la Ley N° 8.968[32] de Costa Rica establece el principio de consentimiento informado, el cual es luego desarrollado en el Capítulo II del Decreto Reglamentario. Bajo esta regulación, el único mecanismo de licitud válido para el tratamiento de datos personales es el consentimiento del titular. La ley prevé excepciones específicas. En Nicaragua, el artículo 6 de la Ley de Protección de Datos Personales[33] prevé que el tratamiento de datos personales podrá realizarse únicamente con el consentimiento previo, expreso e informado del titular del dato. A diferencia de Costa Rica, esta legislación prevé excepciones específicas para el uso del consentimiento.

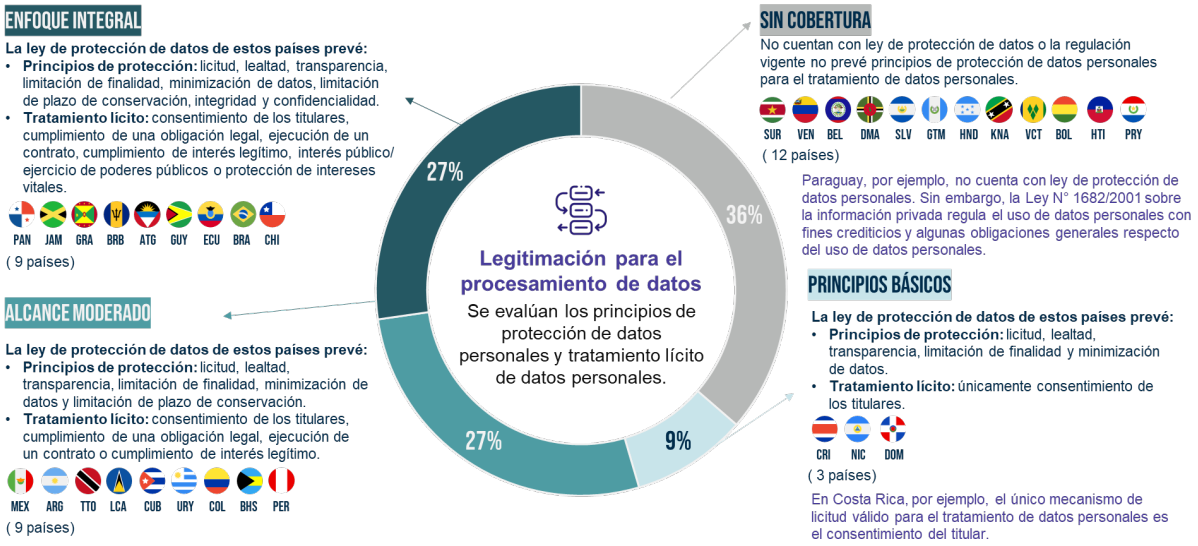
Además, 9 países (27%) han sido incluidos en la clasificación de "Alcance Moderado". De esta manera, México, Argentina, Trinidad y Tobago, Santa Lucia, Cuba, Uruguay, Colombia, Bahamas y Perú profundizan en los principios de protección de datos y los elementos que permiten considerar el tratamiento como lícito. En Perú, el Título 1 de la Ley 29.733[34] de Protección de Datos de Carácter Personal establece los principios rectores de la ley. En particular, determina ocho principios a ser aplicados: legalidad, consentimiento, finalidad y minimización, proporcionalidad, calidad y limitación del plazo de conservación, seguridad (integridad y confidencialidad), disposición de recuso, y nivel de protección adecuado.

Finalmente, 9 países (27%) se encuentran en la categoría de "Enfoque Integral", ya que sus legislaciones abarcan ampliamente los principios de protección de datos. Este es el caso de Panamá, Jamaica, Granada, Barbados, Antigua y Barbuda, Guyana, Ecuador, Brasil y Chile. Por ejemplo, la Parte II

[31] Anteproyecto de Ley de Protección de Datos Personales de Bolivia, socializado en 2023.
[32] Ley n.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales de Costa Rica, aprobada en 2011.
[33] Ley n.º 787 de Nicaragua, aprobada en 2012.
[34] Ley n.º 29.733 de Protección de Datos de Carácter Personal de Perú, aprobada en 2011.

de la Ley de Protección de Datos N° 10/2023[35] de Antigua y Barbuda prevé los principios generales de protección de datos. Así, determina 7 principios dentro de los que se incluyen divulgación (junto a las limitaciones para compartir datos), seguridad y confidencialidad, limitación de plazo de conservación, integridad de los datos y acceso. Además, establece un principio general de protección de datos que prevé los mecanismos legales para el procesamiento lícito de los datos personales, así como también incluye el principio de limitación de licitud, finalidad, y minimización. Asimismo, el principio de notificación y elección establece la obligación de brindar información clara a los titulares sobre las características de las actividades de tratamiento.

Diagrama 9
Niveles de desarrollo para el eje "legitimación"



Fuente: Elaboración propia.

En cuanto a los principios, la gran mayoría de las legislaciones en la región incorporan de manera consistente los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, así como la limitación del plazo de conservación, la integridad y la confidencialidad. Sin embargo, países como México, Costa Rica, Nicaragua, República Dominicana y Paraguay establecen una serie de principios rectores, pero sus legislaciones no contemplan todos los principios estudiados.

En lo que respecta a mecanismos de licitud, el relevamiento evidencia que existe una disparidad en los mecanismos previstos por las distintas legislaciones. Sin embargo, es posible afirmar que predomina en la región el consentimiento como principal y único mecanismo de licitud para el tratamiento de datos personales. Esto se demuestra en que 13 países de la región, dentro de los cuales es posible incluir a Argentina, Colombia, Bahamas y Uruguay, establecen que el único mecanismo de licitud válido para el procesamiento de datos personales es el consentimiento previo del titular de los datos.

Otras regulaciones más recientes (sancionadas desde 2018 hasta la fecha) como son las de Brasil, Ecuador y Barbados entre otras, prevén no solo el consentimiento como mecanismo de licitud sino también cumplimiento de una obligación legal, ejecución de un contrato, cumplimiento del interés legítimo, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, y para proteger intereses vitales del interesado o de otra persona física.

[35] Ley n.º10/2023 de Protección de Datos de Antigua y Barbuda, aprobada en 2023.

3. Regulación especial

El eje de "Regulación especial" busca relevar y reflejar la existencia de requisitos específicos para la recolección y tratamiento de datos personales de menores y datos sensibles. En particular, se identifica si la legislación vigente en materia de protección de datos personales prevé normativa específica en materia de tratamiento de datos de menores y si prevé el tratamiento de categorías especiales de datos personales o requisitos especiales para su tratamiento lícito. Además, se incluye el relevamiento de condiciones especiales de licitud para el tratamiento de datos sensibles y datos de menores de edad.

Diagrama 10
Requisitos específicos para la recolección y tratamiento de datos personales

Fuente: Elaboración propia.

En materia de datos sensibles, se evidencia que todas las normativas de la región prevén una definición de categoría especial de datos o datos sensibles y requisitos especiales para la licitud de su tratamiento (a excepción de Panamá, México, Bahamas y Paraguay). Por ejemplo, en Trinidad y Tobago, se consideran diversos mecanismos de licitud para el tratamiento de datos sensibles como el tratamiento con fines estadísticos y de investigación, tratamiento en interés de la aplicación de la ley y de la seguridad nacional, y el tratamiento para determinar el acceso a los servicios sociales.

Por su parte, la ley de protección de datos[36] de Panamá no prevé una definición de categoría especial de datos ni requisitos para la licitud de su tratamiento, mientras que las regulaciones de México, Bahamas y Paraguay prevé una definición de categoría especial de datos, pero no prevén requisitos especiales para la licitud de su tratamiento.

En lo que respecta al tratamiento de datos de menores de edad la normativa no es uniforme. La regulación de datos de menores define, en general, que se entiende por menores de edad y cuál es la edad límite bajo la cual los niños son considerados menores de edad y se encuentran amparados por la regulación. Asimismo, al momento de regular el tratamiento de datos de menores las diversas normativas establecen los mecanismos de licitud específicos que posibilitan el tratamiento de los datos personales, como consentimiento parental.

Algunas regulaciones de datos personales contienen normativa específica para el tratamiento de datos de menores como Chile, Brasil, Jamaica y Barbados, mientras que algunas regulaciones no tratan el supuesto especifico, pero si existen documentos de gobernanza como en el caso de Argentina.

[36] Ley n.º 81 de Protección de Datos Personales de Panamá, aprobada en 2019.

Por ejemplo, en la regulación de Perú, los menores entre 14 y 18 años podrán dar su consentimiento para el tratamiento de sus datos, siempre que la información sobre el tratamiento sea proporcionada de manera comprensible para ellos. Por su parte, el Reglamento 285 de Panamá detalla que la información dirigida a menores debe ser redactada de manera clara, simple y fácil de comprender. Además, el tratamiento de sus datos debe contar con la autorización del tutor del menor. En Cuba y Argentina el consentimiento es otorgado por los menores de acuerdo con el concepto de autonomía progresiva. Es decir, depende de la edad y el grado de madurez.

4. Cumplimiento y derechos

El eje "Cumplimiento y derechos" busca relevar y reflejar las obligaciones concretas de cumplimiento impuestas a todo aquel que se involucre en el tratamiento de datos personales en pos de cumplir con los principios de protección de datos y los derechos de los titulares de datos. Estos indicadores incluyen obligaciones generales y acciones específicas requeridas a los responsables y encargados de tratamiento, así como también el relevamiento de los mecanismos provistos por la normativa para cumplir y documentar el cumplimiento de la normativa de protección de datos aplicable.

Diagrama 11
Medidas de proactividad y/o seguridad incorporadas por los países de América Latina y el Caribe

Fuente: Elaboración propia.

En materia de derechos, se ha estudiado si la legislación vigente otorga derechos específicos a los titulares de datos. En particular, 10 países de la región poseen legislaciones vigentes que contemplan únicamente los derechos de acceso, rectificación, cancelación y oposición (ARCO, por sus siglas en inglés). Este es el caso de México, donde la Ley Federal de Protección de Datos Personales en Posesión

de los Particulares[37] de México prevé los derechos de acceso, rectificación y supresión. Otros países contemplan estos derechos, así como también el derecho de oposición, portabilidad, limitación del tratamiento, y derecho de oponerse a ser objeto de decisiones individuales automatizadas. Por ejemplo, la legislación de Barbados incorpora los siguientes derechos: portabilidad, limitar el procesamiento que pueda causar daños al titular, limitar el procesamiento con fines de marketing directo y a no ser objeto de decisiones automatizadas. La Ley de Protección de Datos Personales[38] de Nicaragua se destaca ya que prevé los derechos a solicitar información y al olvido digital además de los derechos ARCO.

Luego, se analizaron los distintos roles y obligaciones a los responsables y encargados de tratamiento. La puntuación máxima en este caso refleja las legislaciones que definen los distintos roles y especifican las obligaciones del responsable y encargado del tratamiento de los datos. Como normal general, los países que contienen una definición específica de los roles coinciden en definir al responsable como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento y al encargado como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Respecto de los resultados y la revisión realizada, 11 países, dentro de los cuales podemos identificar a Ecuador, Cuba, Chile y Costa Rica, establecen una definición específica de los roles de responsable y encargado y listado de obligaciones de cada uno. Por ejemplo, en Chile la Ley 21.719 de Protección de Datos Personales define claramente los roles del responsable y el encargado del tratamiento de datos personales, y establece de manera explícita sus deberes y obligaciones.

Países como Antigua y Barbuda, Trinidad y Tobago y Dominica, entre otros, no establecen una definición específica de responsable y encargado, así como tampoco especifica las obligaciones de estos. La legislación de Antigua y Barbuda[39], por ejemplo, define al "usuario de datos" como una persona que, sola o conjuntamente o en común con otras personas, procesa cualquier dato personal o tiene el control o autoriza el procesamiento de cualquier dato personal. Si bien esta definición podría atribuirse al rol de responsable de tratamiento, la ley no prevé una definición específica de encargado de tratamiento. En lo que respecta a las obligaciones, no prevé artículos específicos en los cuales se determine las obligaciones de cada una de las partes. Las obligaciones son generales de cumplimiento con todo lo dispuesto por la ley, pero no existe un listado claro y específico de las obligaciones de cada una de las partes (responsable y encargado).

Finalmente, en países como México la legislación define al responsable y al encargado del tratamiento de datos personales, así como los deberes y las obligaciones de cada uno. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares[40] define al responsable como la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. El encargado, en cambio, es la persona física o jurídica que sola o juntamente con otras trate datos personales por cuenta del responsable. La autoridad de control emitió guías para guiar el comportamiento de estos. En el Decreto Reglamentario[41], por ejemplo, se establecen los deberes y obligaciones del encargado. Cabe resaltar también la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017.

En materia de proactividad, se ha investigado si la legislación vigente prevé la existencia de mecanismos de responsabilidad proactiva en la regulación de protección de datos personales. La responsabilidad proactiva debe ser entendida como el principio que impone al responsable y/o encargado la responsabilidad del cumplimiento de los principios y obligaciones de la ley y ser capaz de

---

37 Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, aprobada en 2010.
38 Ley n.º 787 de Nicaragua, aprobada en 2012.
39 Ley n.º10/2023 de Protección de Datos de Antigua y Barbuda, aprobada en 2023.
40 Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, aprobada en 2010.
41 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, aprobado en 2011.

demostrarlo. Si bien los medios de cumplimiento de la legislación no resultan taxativos, los mecanismos de responsabilidad proactiva estudiados en el presente son: la obligación de nombrar un delegado de Protección de Datos, obligación de notificar incidentes de seguridad, obligación de implementar medidas de protección de datos por diseño y por defecto, obligación de llevar adelante evaluaciones de impacto y obligación de llevar adelante un registro de actividades de tratamiento.

De los 22 países de la región que poseen legislación en materia de protección de datos, solo 11 contemplan la mayoría de estos mecanismos. Por ejemplo, México incorpora el principio de responsabilidad, y determina que para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines. En particular, en lo que respecta a mecanismos de responsabilidad proactiva, se establece la notificación de vulnerabilidad de seguridad que afecten datos personales. Asimismo, la autoridad de control emitió una Guía para la elaboración de evaluaciones de impacto a la privacidad y una Guía de recomendaciones para el manejo de incidentes de seguridad de datos personales[42].

Además, se relevó el contenido y obligaciones en materia de seguridad de los datos personales. En particular, si la legislación prevé la obligación de establecer medidas de seguridad y mecanismos sobre cómo implantar las medidas y sobre gestión de incidentes de seguridad que afecten datos personales. 21 de los 22 países de la región que poseen normativa de protección de datos personales prevén el principio y obligación de seguridad de los datos personales y la necesidad de implementar medidas de seguridad para garantizar la confidencialidad e integridad de los datos personales objeto de tratamiento. Sin embargo, no todos ellos contemplan la obligatoriedad y/o recomendación de notificar incidentes de seguridad. Solo 11 países de la región poseen legislaciones vigentes que prevé la necesidad de incorporar medidas de seguridad y mecanismos de gestión de incidentes. Por ejemplo, la legislación de Colombia prevé el principio de seguridad mientras que la Superintendencia de Industria y Comercio imparte las instrucciones relacionadas con las medidas de seguridad necesarias.

Por último, se analizó la inclusión de regulación específica sobre transferencias internacionales y la existencia de garantías para la transferencia internacional. En particular, se ha analizado la inclusión de los siguientes mecanismos en la legislación: i) decisiones de adecuación, ii) cláusulas modelo de transferencia y iii) Normas Corporativas Vinculantes.

Como resultado de este análisis, se identificaron 12 países de la región poseen legislaciones vigentes que prevén de manera específica los mecanismos para la transferencia de datos bajo estudio. Por su parte, 6 países de la región dentro de los cuáles podemos identificar a Cuba, Bahamas y Trinidad y Tobago, prevén regulación específica de transferencias pero no incorporan mecanismos específicos para la transferencia.

En la región, es relevante resaltar a Uruguay, Argentina y Perú que han incorporado en su legislación interna las cláusulas modelo de transferencia emitidas por la Red Iberoamericana de Protección de Datos. Por otro lado, cabe destacar que Argentina y Uruguay son los únicos dos países de ALC que han sido declarados países con legislación adecuada de protección de datos personales por la Unión Europea (a efectos del Artículo 45[43] de RGPD[44]).

---

[42] Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2016), Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

[43] Artículo 45 RGPD.

[44] RGPD: Reglamento general de protección de datos de la Unión Europea.

La legislación de Argentina, por ejemplo, regula sobre transferencias internacionales. En particular el artículo 12 de la ley prohíbe las transferencias internacionales a países no adecuados. Esta prohibición es subsanada por el artículo 12 del Decreto Reglamentario 1558/2001[45] el cual determina que se podrá realizar transferencias a países no adecuados con el consentimiento expreso de los titulares. De la misma forma, otorga facultades a la autoridad para determinar cuáles son los países considerados adecuados.

Por medio de la Disposición 60/2016[46] la autoridad determinó cuales son las autoridades adecuadas a las cuales se podrá realizar transferencias de forma legítima bajo el artículo 12 de la Ley 25.326, luego la Resolución 34/2019 incorpora al Reino Unido de Gran Bretaña e Irlanda del Norte a la lista de países adecuados luego del Brexit. Asimismo, a través de esta disposición la autoridad emitió las cláusulas modelo para las transferencias internacionales de datos personales para la cesión de datos personales (responsable a responsable) y para el encargo de servicios de procesamiento (responsable a encargado).

Luego, a través de la Resolución 198/2023[47], la Agencia de Acceso a la Información Pública incorporó al derecho interno las cláusulas modelo de transferencia emitidas por la Red Iberoamericana de Protección de Datos. Por último, a través de la Resolución 159/2018[48] la Agencia de Acceso a la Información Pública emitió una guía para la redacción, aprobación e implementación de Normas Corporativas Vinculantes.

5. Cultura y educación

El eje "Cultura y educación" busca reflejar el nivel de desarrollo de la cultura de protección de datos en los países analizados y las medidas y políticas concretas de los distintos gobiernos y autoridades en la promoción del conocimiento de la normativa en materia de protección de datos. En particular, se releva la existencia de campañas de sensibilización en materia protección de datos y la existencia de formación en protección de datos personales y privacidad a nivel nacional. En este último eje podemos ver que la región posee, en general, un desarrollo muy bajo. Esto deja en evidencia que la existencia de regulación en la materia puede no ser suficiente y se requieren esfuerzos específicos de educación a fin de lograr una completa y efectiva aplicación de la normativa sancionada. Solo cuatro países de la región, Uruguay, Argentina, Panamá y Colombia, incorporan elementos de sensibilización y formación sobre tratamiento de datos en el marco de sus legislaciones de protección de datos personales.

En Uruguay desde 2013, la autoridad de control de Uruguay (URCDP[49]) viene desarrollando campañas de sensibilización. La campaña más reciente se realizó en 2024 bajo el nombre de "Competencia digital. Tus datos, tu huella", organizada por Agesic y URCDP, esta campaña busca promover la ciudadanía digital en Uruguay, haciendo especial énfasis en la protección de datos personales. La iniciativa incentiva la colaboración entre docentes y estudiantes, quienes participan en cursos, talleres, capacitaciones y juegos diseñados para sumar puntos en representación de su centro educativo. De esta manera, el concurso combina el aprendizaje lúdico con el fortalecimiento de la cultura digital y la protección de datos en las comunidades educativas del país.

Por su parte, la autoridad de Colombia ha organizado en 2024 un espacio de reflexión sobre la reforma al régimen de datos en Colombia. En Argentina, distintas entidades públicas, como la Defensoría del Pueblo de la Ciudad de Buenos Aires, han implementado campañas dirigidas a la sociedad civil para concientizar sobre la importancia de proteger los datos personales. Por último, en el

---

45 Decreto 1558/2001 - Apruébase la reglamentación de la Ley Nº 25.326 de Argentina, aprobado en 2001.
46 Disposición 60 - E/2016 de Argentina, aprobada en 2016.
47 Resolución 198/2023 de Argentina, aprobada en 2023.
48 Resolución 159/2018 de Argentina, aprobada en 2018.
49 Unidad Reguladora y de Control de Datos Personales de Uruguay.

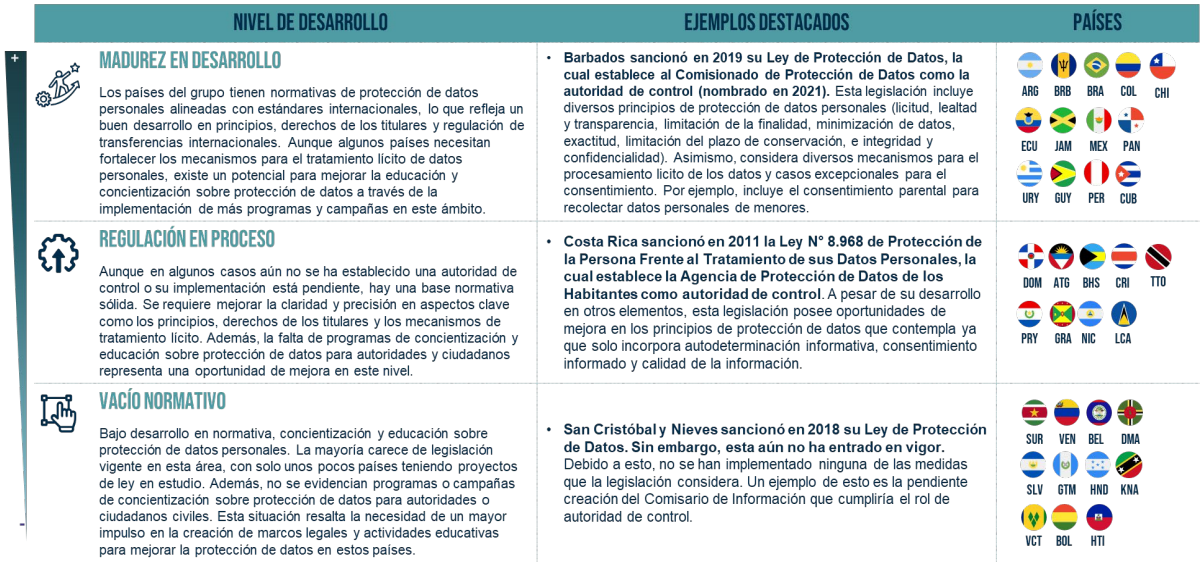
caso de Panamá, se ha promovido programas y foros de sensibilización en materia de protección de datos personales desde 2020. Sin embargo, estos están dirigidos en general a entidades públicas y privadas, dejando de lado a la sociedad civil.

En el marco de la Alianza Digital, la Unión Europea organizó un curso de sensibilización sobre la protección de datos personales en el sector de la salud en 2024, dirigido a las autoridades de Costa Rica, Panamá y República Dominicana. El curso permitió a los participantes adquirir conocimientos sobre los estándares internacionales de protección de datos y explorar mejores prácticas para garantizar la confidencialidad y seguridad de la información de los pacientes, promoviendo un entorno de salud digital más seguro y confiable.

E. Análisis sobre los niveles de desarrollo del tratamiento de datos personales

En base a los resultados del análisis de cada uno de los 33 países de la región a la luz de los ejes descriptos, tal como mencionamos anteriormente, hemos podido agrupar a los países en tres grupos de desarrollo: vacío normativo, regulación en proceso y madurez en desarrollo.

Diagrama 12
Categorías según el nivel de desarrollo en tratamiento de datos personales



Fuente: Elaboración propia.

Implementación consolidada: en base a la información relevada, los países que integran este grupo poseen una normativa de protección de datos personales en línea con la normativa internacional. En muchos casos, la normativa aplicable al tratamiento de datos se encuentra en la ley específica, así como también en regulaciones y normativa complementaria emitida por las autoridades de control.

Este grupo posee un gran desarrollo en materia de derechos de los titulares, mecanismos de cumplimiento y responsabilidad proactiva y regulación en materia de transferencias internacionales. Si bien los países cuentan con un gran desarrollo en la materia, es posible evidenciar la falta de mecanismos aplicables para el tratamiento lícito de datos personales toda vez que muchos de los países prevén únicamente al consentimiento de los titulares de datos como condición de licitud para el tratamiento de datos personales.

Por último, en materia de educación y sensibilización, algunos de los países evidencian algún tipo de medidas o políticas en esas áreas, pero aún queda mucho desarrollo en materia de sensibilización, educación y cultura de protección de datos. En otros casos, no se han encontrado evidencias de programas públicos o campañas de sensibilización y educación en materia de protección de datos personales para autoridades públicas o ciudadanos civiles.

Estos países son: Argentina, Barbados, Brasil, Chile, Colombia, Cuba, Ecuador, Guyana, Jamaica, México, Panamá, Perú y Uruguay.

Regulación en proceso: en base a la información relevada, todos los países que se encuentran en este nivel poseen una normativa específica en materia de protección de datos personales. Sin embargo, en algunos casos, la normativa vigente no contempla la creación y puesta en funcionamiento de una autoridad de control especifica o bien lo hace pero lo misma aún no ha sido creada.

Asimismo, la normativa de protección de datos vigente en los países que forman parte de este nivel carece de previsiones claras y precisas en algunos puntos importantes como los derechos de los titulares, los mecanismos de licitud del tratamiento, mecanismos de seguridad e implementación de la responsabilidad proactiva y regulación especial sobre transferencias internacionales.

Por último, no se han encontrado evidencias de programas públicos o campañas de sensibilización y educación en materia de protección de datos personales para autoridades públicas o ciudadanos civiles.

Estos países son: Costa Rica, Antigua y Barbuda, Granada, Santa Lucia, Bahamas, Trinidad y Tobago, Nicaragua, República Dominicana y Paraguay.

Vacío normativo: en base a la información relevada, este grupo de países posee poco o nulo desarrollo en materia de normativa, sensibilización y educación sobre protección de datos personales. La gran mayoría de estos países no poseen legislación vigente en materia de protección de datos personales, y solo algunos de estos poseen proyectos de ley bajo estudio. De la misma forma, no se han encontrado evidencias de programas públicos o campañas de sensibilización y educación para autoridades públicas o ciudadanos civiles.

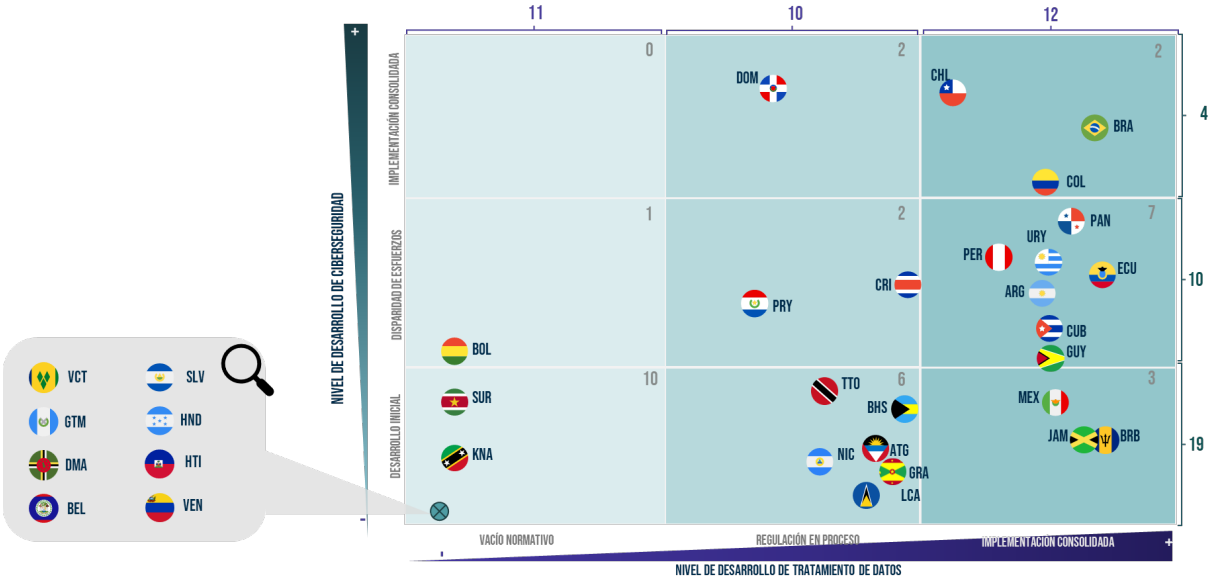
Estos países son: Belice, Bolivia, Dominica, El Salvador, Guatemala, Haití, Honduras, San Cristóbal y Nieves, San Vicente y las Granadinas, Surinam y Venezuela.

F. Diferencias en el nivel de desarrollo de la ciberseguridad y el tratamiento de datos personales en América Latina y el Caribe

Existe una notoria diferencia entre el nivel de desarrollo del abordaje de la ciberseguridad frente al de datos personales en la región. La protección de datos personales fue abordada en los ámbitos legislativos mucho antes que los debates en ciberseguridad, existiendo además una definición más amplia en materia de ciberseguridad que complica el establecimiento de autoridades que coordinen a todos los actores involucrados.

Otra de las diferencias es que en ciberseguridad el componente técnico y su abordaje es mucho más complejo que la regulación de protección de datos personales. Un punto de encuentro no obstante es cuando se aborda el principio de seguridad del dato, ya que este punto en indivisible de la ciberseguridad, en ese sentido se destacan países como Colombia o Brasil que han tenido en cuenta esta característica en sus marcos regulatorios.

Diagrama 13
Niveles de desarrollo de la ciberseguridad y tratamiento de datos personales en América Latina y el Caribe



Fuente: Elaboración propia.

Como se puede ver en la ilustración anterior, mientras que únicamente 4 países se encuentran con un nivel de desarrollo de implementación consolidada en ciberseguridad, son 13 los que se encuentran con ese mismo nivel de desarrollo avanzado en el tratamiento de los datos personales.

1. Diferencias entre tratamiento de datos personales y la ciberseguridad

Las áreas de trabajo de la ciberseguridad son múltiples y diversas dentro de las estructuras gubernamentales, además de transversal a la sociedad en su conjunto en su implementación, incluyendo a la educación, el desarrollo de marcos normativos, la constitución de nuevas instituciones de gobernanza, la cooperación y colaboración internacional hasta los aspectos técnicos concretos entre otras temáticas. Esta diversidad implica una complejidad inherente para los países ya que deben establecer una coordinación de las políticas y sus programas a nivel nacional que requiere asignarles a las instituciones de gobernanza un liderazgo político de jerarquía y una asignación presupuestaria que les permita concretar lo planificado.

En materia de protección de datos personales, si bien es un tema transversal, en general se ha establecido un foco más concreto en la regulación, que con variaciones siguen, en la región, el modelo europeo en los países más desarrollados en la materia.

Es así que, en materia de protección de datos personales, los países reconocen la necesidad de una ley que aborde los problemas actuales y una autoridad independiente, mientras que la gobernanza en materia de ciberseguridad no se enmarca en un solo modelo. Sin embargo, se destaca Chile con su Ley Marco de Ciberseguridad y la creación de una Agencia Nacional.

2. Trayectoria regulatoria

Al parecer los países han iniciado de manera más temprana su trayectoria sobre sus esfuerzos regulatorios en materia de protección de datos personal antes que el tratamiento de la ciberseguridad. Los debates legislativos y la sanción de leyes o la inclusión de la protección de datos personales en otras leyes tienen un mayor recorrido en la región, con los ejemplos de Chile y Argentina desde fines de los 90´s e inicios de los 2000, sin dejar de mencionar que adicionalmente han actualizado su marco regulatorio.

Por otro lado, en ciberseguridad las regulaciones a nivel nacional y en particular los proyectos legislativos han logrado tener un éxito moderado, cómo es el caso de Chile en 2024.

En el caso de la ciberseguridad cabe mencionar que si bien la Directiva NIS (Networks and Information Systems), con requisitos para los países de la Unión Europea es de 2016, el mismo año que el Reglamento General de Protección de Datos Europeo, no surgió en principio como un modelo a seguir tal como sucedió en datos personales. También puede mencionarse que ya en 2024 entra en vigor la Directiva NIS2[50] que actualiza la versión anterior bajo la denominación de Directiva de ciberseguridad.

En ALC, países como Chile, Uruguay y Argentina han adoptado el término ciberseguridad, mientras que Perú, Colombia y Ecuador, por mencionar algunos se han orientado a Seguridad Digital en su regulación.

3. Diferencias en enfoque y componente jurídico

La protección de datos personales, como se ha mencionado, tiene un recorrido en el tratamiento regulatorio de varios años que cuenta con doctrina y jurisprudencia, mientras que la ciberseguridad ha sido recién en los últimos años que tomado impulso en el debate legal en la región. En materia de ciberseguridad el componente más fuerte ha sido el tecnológico/técnico y los marcos jurídicos pasaron a un segundo plano.

En la gran mayoría de los países se han establecidos requisitos mínimos para la seguridad de la información para las administraciones públicas de orden nacional. Estas normativas se basan en estándares técnicos internacionales.

4. Bajo nivel de desarrollo normativo y de sensibilización en ciberseguridad

Solo Chile cuenta con legislación específica de ciberseguridad en ALC. Los bajos niveles de sensibilización se retroalimentan con la falta de legislaciones claras, surgiendo un ciclo de falta de conciencia y ausencia de legislación. Varios países, 16 de los 33, cuentan con estrategias nacionales de ciberseguridad con distintos niveles de efectividad. Se observó que los países más avanzados en su nivel de madurez son aquellos en los que existe una mayor sensibilización sobre la necesidad de políticas públicas sobre esta materia.

Tal como pasó con Chile, y también en varios países de la Unión Europea, se espera que el paso siguiente al establecimiento de las Estrategias o Políticas Nacionales sea la discusión de leyes que aborden esta temática.

Recuadro 3
Brasil se destaca por su enfoque integral

Brasil ha sancionado su Ley de protección de datos personales en 2018, con entrada en vigor en 2020, adoptando los principios actualizados en la materia, mientras que ha venido trabajando en distintos aspectos de la ciberseguridad como la consolidación de una red federal de atención de incidentes o un centro de ciberseguridad para los organismos de gobierno. Si bien no tiene una ley promulgada, su decreto para el establecimiento de una política nacional y la creación de un Comité multisectorial en 2023 merecen destacarse como un abordaje integral en materia de ciberseguridad y protección de datos.

En el caso de Colombia también se encuentran evidencias de adoptar un enfoque de ciberseguridad y privacidad tanto en su modelo de políticas para la administración pública, y una autoridad de protección de datos personales activa.

Fuente: Elaboración propia.

[50] NIS2: Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2).

5. Interrelación entre protección de datos y ciberseguridad

El principio de seguridad del dato es clave para la protección de las personas en materia de datos personales y muchos otros aspectos. Para su efectivo cumplimiento es necesaria la implementación de medidas de ciberseguridad que abordan la seguridad de las infraestructuras, las redes, los sistemas de información y a la información como objetivos.

Esta interrelación es más evidente cuando los incidentes de ciberseguridad afectan a datos personales en cuyo caso podrían verse involucradas instituciones y/o regulaciones de ambas materias. Sería deseable tener esta perspectiva al momento de delinear los modelos de gobernanza.

III. Ciberseguridad y protección de datos personales: áreas clave de mejora para un desarrollo sostenido

A. Regulación y capacidades técnicas como base para la promoción de la ciberseguridad y tratamiento de datos personales

El relevamiento realizado permite identificar, aunque con la disparidad ya descripta, patrones comunes que permiten destacar tanto las fortalezas y oportunidades como las debilidades y amenazas que la ciberseguridad y el tratamiento de datos personales presentan en ALC.

Cuadro 7
Matriz FODA de ciberseguridad y tratamiento de datos personales

Aspectos positivos		Aspectos negativos
Factores intrínsecos	Fortalezas: • Sólida base regulatoria • Capacidades técnicas disponibles • Existencia de autoridades de aplicación	Debilidades: • Falta de continuidad en las políticas públicas • Lentitud en la actualización regulatoria • Atención de los gobiernos desviada por otras prioridades • Falta de demanda de la ciudadanía
Factores extrínsecos	Oportunidades: • Aprender de la experiencia de otros países • Aumentar la consciencia tanto de la ciudadanía como de los responsables políticos	Amenazas: • Velocidad con la que se implementan nuevos servicios digitales • Rápido avance tecnológico • Alcance y la complejidad de los ciberataques

Fuente: Elaboración propia.

Como fortalezas, se han identificado las siguientes:

- La mayoría de los países han establecido una sólida base regulatoria para el tratamiento de datos, lo que constituye un paso fundamental tanto para profundizar en este aspecto como para garantizar la ciberseguridad. Esta preocupación es compartida por la sociedad civil, lo cual se refleja en la existencia de numerosas organizaciones dedicadas a este fin.
- Se observa un conjunto de capacidades técnicas disponibles que podrían impulsar y promover una mejora regulatoria aún mayor. Además, se han identificado redes de cooperación internacional, como la Red Iberoamericana de Protección de Datos, el CSIRT de las Américas (de la OEA), las iniciativas de la Alianza Digital UE-ALC, así como Caricom.
- Una fortaleza institucional destacada es la existencia de autoridades de control de la ciberseguridad en 29 de los 33 países, lo que subraya el compromiso regional con este tema.

En contraposición a estas fortalezas, se han identificado las siguientes debilidades:

- La falta de continuidad en las políticas públicas es evidente en varios países. gubernamentales, lo que dificulta la implementación de medidas consistentes en materia de datos y ciberseguridad.
- La lentitud en la actualización regulatoria es otro desafío significativo, donde los procesos para adaptar las regulaciones a los avances tecnológicos suelen ser prolongados y poco ágiles.
- Además, la atención de los gobiernos se desvía por otras prioridades, como urgencias políticas y económicas, lo que resulta en una falta de enfoque en la protección de datos y la ciberseguridad.
- La falta de demanda de la ciudadanía y la escasa sensibilización social sobre la importancia de proteger los datos también contribuyen a este panorama (Mendoza, 2020).

Asimismo, se han identificado posibles amenazas:

- La velocidad con la que se implementan nuevos servicios digitales representa una amenaza, ya que puede superar la capacidad de las organizaciones para garantizar la seguridad y protección de los datos.
- El rápido avance tecnológico supone un desafío constante, ya que las medidas de protección de datos y ciberseguridad pueden quedar rezagadas frente a las nuevas vulnerabilidades y métodos de ataque que surgen con frecuencia.
- Las amenazas cibernéticas no conocen fronteras y pueden afectar a organizaciones de todo el mundo. Esto amplifica el alcance y la complejidad de los ciberataques, dificultando la defensa y la mitigación de riesgos.

Finalmente, en consideración de las fortalezas y diversas debilidades y amenazas y el estado actual de situación en la región es posible identificar las siguientes oportunidades:

- Existe la oportunidad de aprender de la experiencia de otros países a nivel internacional e incluso de algunos países dentro de la región.
- Es posible aprovechar esta situación para aumentar la conciencia tanto de la ciudadanía como de los responsables políticos, y continuar fortaleciendo las capacidades a través de iniciativas de formación. Por ejemplo, a través de la implementación de programas de capacitación específicos para servidores públicos que aborden las necesidades actuales en materia de protección de datos personales y ciberseguridad. Cabe, resaltar el apoyo que la Alianza Digital UE-ALC esta desarrollando en esta materia como ya se indicó.

B. Líneas de acción para que la región continúe su trayectoria de desarrollo en ciberseguridad y tratamiento de datos

A partir del relevamiento realizado en los capítulos anteriores, se identificaron los principales hallazgos, barreras y oportunidades de mejora encontradas en la región para el desarrollo de las capacidades en ciberseguridad y en el tratamiento de datos personales.

1. Ciberseguridad

A pesar de que la región sigue presentando desafíos significativos en temas de ciberseguridad, los países muestran una base alentadora para su desarrollo e implementación adecuada.

Cuadro 8
Oportunidades de mejora de la ciberseguridad en América Latina y el Caribe

Situación general	Descripción	Oportunidad de mejora
Falta de terminología común podría dificultar el diálogo y la cooperación internacional	• Estrategias Nacionales de seguridad digital muestran diversidad en terminología y alcance sin definiciones explícitas. • Normativas con debate legislativo (Chile, Ecuador, Argentina, Perú) ofrecen definiciones claras. • "Ciberseguridad" es el término más utilizado pero carece de consenso y definición precisa. • Falta de consenso podría dificultar la cooperación internacional y reducir efectividad. • Inclusión de términos no técnicos en las políticas será crucial para alcanzar objetivos comunes en esfuerzos internacionales.	Analizar las diferencias y los estudios sobre las terminologías adoptadas por los países y establecer consensos, con la finalidad de superar diferencias de enfoques o terminología que promuevan políticas centradas en la cooperación y colaboración.
Débiles capacidades en Protección de Infraestructuras críticas y servicios esenciales	• Protección de infraestructuras críticas y servicios esenciales desde la ciberseguridad es abordada de manera incipiente en regulaciones nacionales. • Chile y Brasil, más avanzados en esta temática, han abordado la materia primero desde la Defensa Nacional. • Posteriormente, los aspectos digitales relacionados se incluyen en las normativas nacionales.	Abordar la protección de la infraestructura crítica y los servicios esenciales desde la ciberseguridad en función de la criticidad de los servicios para los Estados. Esto implica identificar las amenazas potenciales, evaluando sus posibles impactos y tomando medidas para mitigar riesgos. Aprovechar buenas prácticas internacionales en esta área.
La gestión de las crisis originadas en un incidente de ciberseguridad es de las capacidades menos consideradas junto a las iniciativas legislativas en ciberseguridad	• Importancia de una coordinación efectiva entre agencias de seguridad de la información y gestión de incidentes madura para construir capacidades en la gestión de cibercrisis. • Cuando un incidente alcanza un nivel crítico, se requiere que un comité de crisis preestablecido tome acciones planificadas. Aunque los equipos de respuesta a incidentes están presentes en la mayoría de los países de la región sur, más del 50% carece de gestión de cibercrisis y proyectos de ley en ciberseguridad, y no hay iniciativas de debate nacional al respecto.	A medida que mejoren las capacidades en la gestión de incidentes y se fortalezca la cooperación entre agencias, será deseable articular los esfuerzos para prepararse en el análisis de situaciones, la elaboración de planes de acción y la toma de decisiones durante crisis originadas en incidentes.
Son aún incipientes las capacidades en gobernanza en ciberseguridad	• La región debe seguir esforzándose por establecer instituciones, normas, políticas y procedimientos que promuevan una estrategia coordinada en ciberseguridad, involucrando a todas las partes interesadas. Colombia ejemplifica esto con su Decreto 338/2022, mientras que Chile lo describe implícitamente en su Ley Marco. Destaca a su vez el caso de Rep. Dominicana, que cuenta con una Estrategia de Ciberseguridad emitida por decreto presidencial y un Centro Nacional de Ciberseguridad, de naturaleza técnica, con un marco de gobernanza altamente avanzado en términos relativos a sus pares regionales.	Se recomienda iniciar por la selección de una estrategia adecuada para la gobernanza que se adapte a cada necesidad que contempla un plan de crecimiento en capacidades y despliegue con objetivos concretos y planes factibles.

Situación general	Descripción	Oportunidad de mejora
Escasas acciones para la promoción de la educación y cultura en ciberseguridad	• Falta de apoyo a la educación y promoción de la cultura en ciberseguridad. • Escasas campañas de difusión sobre programas formativos y oportunidades en diversas áreas. • Estados deben impulsar la difusión, elaboración, análisis, investigación y producción de material educativo en ciberseguridad. • Esta promoción puede ser realizada por los Estados mismos y/o en colaboración con el sector privado. • Algunos países, como Chile y Uruguay, reconocen un déficit de profesionales en ciberseguridad. • Las iniciativas para implementar acciones concretas aún están en sus etapas iniciales.	Trabajar colaborativamente con el sector público y privado para orientar en los distintos roles en ciberseguridad y las posibilidades de formación, así como para difundir información sobre programas de formación.
Privacidad y ciberseguridad en los países más consolidades en ciberseguridad	• Convergencia en esfuerzos nacionales cuando un incidente de ciberseguridad afecta datos personales, servicios digitales o infraestructuras. • Países avanzados incorporan referencias a la seguridad y privacidad: Ley Marco de Chile; Protección de datos personales en la Política Nacional de Brasil; Decreto de la Estrategia de la República Dominicana; y Modelo de Seguridad y Privacidad en la Política de Gobierno Digital de Colombia. • Reconocimiento de la vinculación necesaria entre ciberseguridad, privacidad y protección de datos.	Promover y fortalecer esta tendencia para que los incidentes que afectan a datos personales puedan ser analizados por su impacto en los derechos de las personas y también desde los aspectos técnicos para evitar futuras ocurrencias.

Fuente: Elaboración propia.

2. Tratamiento de datos personales

En ALC se tienen 22 países con leyes de protección de datos personales vigentes pero, a pesar de este nivel de desarrollo y esfuerzos en la normativa, la sensibilización aún permanece baja.

Cuadro 9
Oportunidades de mejora en el tratamiento de datos personales en América Latina y el Caribe

Situación general	Descripción	Oportunidad de mejora
Variación subregional	• Respecto a los países puntuados como robustos: • 8 de los 12 países de América del Sur posee normativa de protección de datos alineada, en ciertos aspectos, con normativa internacional. • 9 de los 15 países del Caribe poseen normativa de protección de datos personales. • 2 de los 8 países de América Central poseen normativa de protección de datos alineada con normativa internacional.	Fomentar la cooperación regional y el intercambio de buenas prácticas a través de foros y mesas de trabajo sobre protección de datos personales. Aquellos países que aún no cuentan con normativas de protección de datos pueden tomar como referencia los progresos de otros países y considerar las oportunidades y obstáculos que enfrentaron estos países.
Carencia en los mecanismos de licitud	• 22 de los 33 países en la región que poseen normativa vigente en materia de protección de datos, 13 prevén únicamente al consentimiento como mecanismos de licitud para el tratamiento de datos.	La incorporación de otros mecanismos de licitud como la ejecución de un contrato o la satisfacción de interés legítimo facilitarían la transparencia y la posibilidad de decisión de los titulares de datos. Además, brindarían más posibilidades para el tratamiento legitimo.
Menores desprotegidos	• 11 de los 33 países de la región posee normativa que establece de manera clara la regulación para el tratamiento de datos de menores de edad.	Hay un incremento en la exposición de los datos personales de menores debido a las redes sociales. Incluir cuidados específicos para menores de edad y limitar la influencia excesiva o con fines ilícitos permite una presencia digital segura. Los menores suelen desconocer los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales por lo que mecanismos específicos de control y consentimiento los protegería. Esto contempla campañas de capacitación y programas formativos a familias y/o menores además de programas que permitan verificar la edad del menor antes de acceder a determinados contenidos.

Situación general	Descripción	Oportunidad de mejora
sensibilización para la protección	• 22 de los 33 países de la región posee normativa vigente de protección de datos personales. Sin embargo, solo algunos demuestran desarrollos en materia de sensibilización y educación.	Una baja sensibilización dificulta la aplicación de los preceptos legales. El desarrollo de programas de sensibilización y educación y políticas en esta materia promovería la implementación y el cumplimiento de la normativa.
Clausulas para la Transferencia internacional	• 12 de los 15 países de la región con legislación de protección de datos caracterizada como "robusta" incluyen amplias garantías para la transferencia internacional de datos. Es decir que las normativas prevén de forma expresa mecanismos de adecuación los cuales pueden incluir algunos de los siguientes: i) decisiones de adecuación, ii) cláusulas modelo de transferencia y/o iii) Normas Corporativas Vinculantes.	La falta de armonización puede generar complejidades adicionales para las empresas que operan en múltiples jurisdicciones. Trabajar en la estandarización de los criterios y procedimientos para la transferencia internacional de datos podría facilitar el cumplimiento normativo y promover un entorno empresarial más eficiente y transparente.

Fuente: Elaboración propia.

Bibliografía

ABIresearch (2024), *Data generation by manufacturing industry*. https://www.abiresearch.com/news-resources/chart-data/manufacturing-industry-amount-of-data-generated/.

Banco Interamericano de Desarrollo, Organización de Estados Americanos, Centro Global de Capacidad en Seguridad Cibernética, & Universidad de Oxford (2020), *Reporte de ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean.

Brynjolfsson, E., & otros (2011), *Strength in numbers: How does data-driven decision-making affect firm performance?* SSRN. https://doi.org/10.2139/ssrn.1928616.

E-governance academy de Estonia (2023, septiembre), *NCSI - National Cybersecurity Index*. https://ncsi.ega.ee/ncsi-index/.

ESPC Strategic Notes (2017), *Enter the data economy: EU policies for a thriving data ecosystem* (Issue 21). https://www.espc-strategic-notes.com.

European Commission (2024), *Data flow and economic value EU framework: Modelling update and data collection*. https://digital-strategy.ec.europa.eu/en/library/data-flow-and-economic-value-eu-framework-modelling-update-and-data-collection.

European Parliament (2022), *Measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555.

ESET (2024), *ESET Security Report (ESR): Informe anual sobre el estado de la seguridad en las empresas de América Latina*. https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-2024-es.pdf.

IDC (2024), *Worldwide IDC global datasphere forecast, 2024–2028: AI everywhere, but upsurge in data will take time*.

Informe de implementación política nacional de ciberseguridad 2017-2022 chilena https://ciberseguridad.gob.cl/documents/3/Evaluaci%C3%B3n_PNCS_2017-2022.pdf.

Kasim, M. (2023), Rethinking the impact of informal organizational rules on organizational cybersecurity. *Cybersecurity for Decision Makers*, 317-326.

Ministerio del Interior y Seguridad Pública de Chile (2024), Ley 21663 Firma Electrónica. Ley Marco de Ciberseguridad. Abril 2024.

Parlamento Europeo y Consejo de la Unión Europea (2016), *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).* Diario Oficial de la Unión Europea, L 119, 1–88.

Pérez González, D., Solana-González, P., & Trigueros Preciado, S. (2018), *Economía del dato y transformación digital en pymes industriales: Retos y oportunidades*. https://documents.worldbank.org/en/publication/documentsreports/documentdetail/099400004112257749/p1754970d6c6420f00ab5905f7004ba9c2f.

Política Nacional de Ciberseguridad de Chile. https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf.

Presentación del Proyecto de Ley de Protección de Datos Personales. https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales.

Red Iberoamericana de Protección de Datos (2017), *Estándares de Protección de Datos de los Estados Iberoamericanos.* Aprobado en el marco del XV Encuentro Iberoamericano de Protección de Datos.

Unión Internacional de Telecomunicaciones (2020), *Global cybersecurity index*. Ginebra, Suiza. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Anexo

Cuadro A1
Variables para el relevamiento del tratamiento de datos personales

Variable	Descripción	Criterio de puntuación			
		0	1	2	3
Ley de protección de datos vigente	El indicador releva información sobre la existencia de una ley vigente que regule el tratamiento de datos personales en el país y su alineación con normas internacionales.	El país no posee ley ni proyectos de ley de protección de datos personales.	El país posee proyectos de ley en materia de protección de datos personales.	El país posee ley en materia de protección de datos personales que no encuentra alineada con las normas internacionales.	El país posee ley de protección de datos personales alineada con normas internacionales.
Autoridad de control	El indicador releva información sobre la existencia de una autoridad estatal a la cual se le asignan facultades específicas para la supervisión del cumplimiento de la regulación de datos personales.	El país no posee normativa que brinde facultades de supervisión en materia de cumplimiento de la ley de protección de datos personales y no existe otra autoridad con facultades para llevar a cabo el monitoreo de cumplimiento.	El país no posee normativa que brinde facultades de supervisión en materia de cumplimiento de la ley de protección de datos personales, sin embargo, existe otra autoridad que toma las facultades para llevar a cabo el monitoreo de cumplimiento.	La ley de protección de datos personales otorga facultades a una autoridad específica para la supervisión de la ley, pero la autoridad aún no ha sido constituida.	La ley de protección de datos personales define y otorga facultades a una autoridad específica para la supervisión de la ley, y la autoridad ha sido constituida y ejerce la función de control.
Principios de protección de datos personales	El indicador releva si la ley de protección de datos personales prevé principios de protección de datos personales aplicables al tratamiento de datos.	El país no posee ley de protección de datos, y no hay otra regulación que prevé principios de protección de datos personales para el tratamiento de datos personales.	La Ley de protección de datos vigente prevé licitud, lealtad, transparencia, limitación de finalidad y minimización de datos.	La Ley de protección de datos vigente prevé licitud, lealtad, transparencia, limitación de finalidad y minimización de datos además de limitación de plazo conservación.	La Ley de protección de datos vigente prevé licitud, lealtad, transparencia, limitación de finalidad y minimización de datos además de limitación de plazo conservación además de integridad y confidencialidad.
Tratamiento lícito de los datos personales	El indicador releva si la ley de protección de datos personales prevé mecanismos de licitud para el tratamiento de los datos personales. En particular, estos mecanismos refieren a las bases legales que respaldan la legitimidad del tratamiento. Al momento de recolectar los datos personales y llevar adelante las actividades de tratamiento, los responsables deberán basarse en las bases legales enumeradas en la legislación para legitimar el procesamiento de datos.	El país no posee ley de protección de datos, y no hay otra regulación que prevé principios de protección de datos personales para el tratamiento de datos personales.	La ley de protección de datos vigente prevé únicamente al consentimiento de los titulares de datos como condición de licitud para el tratamiento de datos personales.	La ley de protección de datos vigente prevé las siguientes condiciones de licitud: i) Consentimiento de los titulares de datos; ii) Cumplimiento de una obligación legal; iii) Ejecución de un contrato; iv) Cumplimiento del interés legítimo.	La ley de protección de datos vigente prevé las siguientes condiciones de licitud: i) Consentimiento de los titulares de datos; ii) Cumplimiento de una obligación legal; iii) Ejecución de un contrato; iv) Cumplimiento del interés legítimo; v) Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos; vi) Para proteger intereses vitales del interesado o de otra persona física.
Tratamiento de datos de menores	El indicador releva si la ley de protección de datos personales prevé normativa específica en materia de tratamiento de datos de menores.	El país no posee ley de protección de datos, y no hay otra regulación que prevé reglas para el tratamiento de datos de menores.	La ley de protección de datos vigente no prevé condiciones específicas sobre el tratamiento de datos personales de menores.	La ley de protección de datos vigente no prevé normativa sobre el tratamiento de datos personales de menores pero existen documentos de gobernanza sobre el tratamiento de datos personales de menores.	La ley de protección de datos vigente prevé condiciones sobre la edad del menor o condiciones sobre el tratamiento de datos personales de menores.
Categorías especiales de datos personales	El indicador revela si la legislación vigente en materia de protección de datos personales prevé el tratamiento de categorías especiales de datos personales y si prevé requisitos especiales para su tratamiento lícito.	El país no posee ley de protección de datos, y no hay otra regulación que prevé y determine el tratamiento de categorías especiales de datos personales.	El país posee una la ley de protección de datos vigente, pero la misma no prevé una definición de categoría especial de datos ni requisitos para la licitud de su tratamiento.	La ley de protección de datos vigente prevé una definición de categoría especial de datos, pero no prevé requisitos especiales para la licitud de su tratamiento.	La ley de protección de datos vigente prevé una definición de categoría especial de datos y prevé requisitos especiales para la licitud de su tratamiento.

Variable	Descripción	Criterio de puntuación			
		0	1	2	3
Derechos de los titulares de datos	El indicador releva si la legislación vigente en materia de protección de datos personales otorga derechos específicos a los titulares de datos.	El país no posee ley de protección de datos, y no hay otra regulación que prevé derechos específicos en materia de datos personales.	La ley de protección de datos vigente no otorga derechos a los titulares de datos.	La ley de protección de datos vigente otorga a los titulares únicamente los derechos de acceso, rectificación y supresión.	La ley de protección de datos vigente otorga a los titulares los derechos de acceso, rectificación y supresión, así como también otros derechos, dentro de los cuales es posible identificar el derecho de oposición, derecho de portabilidad, limitación del tratamiento, información y derecho a oponerse a ser objeto de decisiones individuales automatizadas.
Responsable y encargado	El indicador releva si la legislación vigente si la legislación vigente en materia de protección de datos personales prevé distintos roles y obligaciones a los responsables y encargados de tratamiento.	El país no posee ley de protección de datos, y no hay regulación que prevé y determines los roles de responsable y encargado.	La ley de protección de datos vigente no prevé una definición del rol del responsable y el encargado de tratamiento.	La ley de protección de datos vigente prevé una definición del rol del responsable y el encargado de tratamiento, pero no específica de forma expresa los deberes y obligaciones de cada uno.	La ley de protección de datos vigente prevé una definición del rol del responsable y el encargado de tratamiento, y específica de forma expresa los deberes y obligaciones de cada uno.
Proactividad	El indicador releva si la legislación vigente en materia de protección de datos personales prevé la existencia de mecanismos de responsabilidad proactiva en la regulación de protección de datos personales.	El país no posee ley de protección de datos, y no hay otra guías o recomendaciones que prevean la obligación y/o recomendación de implementar medidas de responsabilidad proactiva.	La ley de protección de datos vigente no prevén medidas de responsabilidad proactiva concretas.	La ley de protección de datos vigente prevé la obligación de nombrar un Delegado de Protección de Datos y obligación de notificar incidentes de seguridad.	La ley de protección de datos vigente prevé la obligación de nombrar un Delegado de Protección de Datos, obligación de notificar incidentes de seguridad, obligación de implementar medidas de protección de datos por diseño y por defecto, obligación de llevar adelante evaluaciones de impacto y obligación de llevar adelante un registro de actividades de tratamiento.
Seguridad	El indicador releva si la legislación vigente en materia de protección de datos personales prevé la existencia de la obligación de establecer medidas de seguridad y mecanismos sobre cómo implantar las medidas y sobre gestión de incidentes de seguridad que afecten datos personales.	El país no posee ley de protección de datos y no hay otra regulación respecto de medidas de seguridad para el tratamiento de datos personales.	La ley de protección de datos personales no prevé la obligación de medidas de seguridad en el tratamiento de datos personales.	La ley de protección de datos personales prevé la obligación de adoptar medidas de seguridad en el tratamiento de datos personales, pero no prevé mecanismos de gestión de incidentes de seguridad que afecten datos personales.	La ley de protección de datos personales prevé la obligación de adoptar medidas seguridad en el tratamiento de datos personales y prevé mecanismos de gestión de incidentes de seguridad que afecten datos personales.
Regulación e implementación garantías necesarias para la transferencia internacional	El indicador releva si la ley de protección de datos vigente establece regulación específica en materia de transferencias internacionales y en tal caso, si prevé la implementación de mecanismos de adecuación para llevar adelante la transferencia como lo son las decisiones de adecuación, cláusulas modelo de transferencia y las Normas Corporativas Vinculantes.	El país no posee ley de protección de datos y no hay otra regulación respecto de medidas de transferencia internacional de datos personales.	La ley de protección de datos personales vigente no prevé regulación a específica en materia de transferencias internacionales.	La ley de protección de datos vigente prevé regulación sobre transferencias internacionales, pero no establece medidas o mecanismos para garantizar que las transferencias sean realizadas de acuerdo con la legislación nacional. La autoridad de aplicación tampoco ha sancionado regulación complementaria en materia de mecanismos de adecuación.	La ley de protección de datos vigente prevé regulación sobre transferencias internacionales y la misma establece medidas o mecanismos para garantizar que las transferencias sean realizadas de acuerdo con la legislación nacional. La ley prevé de forma expresa mecanismos de adecuación los cuales pueden incluir algunos de los siguientes: i) decisiones de adecuación, ii) cláusulas modelo de transferencia y/o iii) Normas Corporativas Vinculantes.

Variable	Descripción	Criterio de puntuación			
		0	1	2	3
Programas de sensibilización	El indicador releva la existencia de campañas de sensibilización en materia protección de datos a nivel nacional.	El país no evidencia campañas de sensibilización en materia de protección de datos personales.	El país tiene alguna campaña en materia de sensibilización en protección de datos personales.	El país realiza o realizó varias campañas sobre sensibilización en protección de datos personales.	El país evidencia la coordinación de campañas de sensibilización dirigida a diferentes públicos (niños, adultos mayores, escolares, empleados, PYMES, etc.).
Educación y programas de formación en protección de datos personales y privacidad a nivel nacional	El indicador releva la existencia de formación en protección de datos personales y privacidad a nivel nacional.	El país no tiene ningún tipo de promoción o acción sobre la necesidad de formación, programas o cursos en materia de protección de datos personales y privacidad.	El país tiene algún tipo de promoción o acción sobre la necesidad de formación, realiza programas o cursos en materia de protección de datos personales y privacidad.	El país tiene programas de formación o cursos en materia de protección de datos personales y privacidad.	El país evidencia de trabajar en protección de datos personales y privacidad con el ministerio o área de Educación y programas de formación para empleados públicos con distintos contenidos técnicos.

Fuente: Elaboración propia.

Cuadro A2
Variables para el relevamiento de ciberseguridad

Variable	Descripción	Criterio de puntuación			
		0	1	2	3
Estrategia y/o Política Nacional de ciberseguridad vigente	El indicador releva información sobre la existencia de una estrategia o política nacional que contempla la ciberseguridad o a la seguridad digital.	El país no posee estrategia y/o política nacional de ciberseguridad o de seguridad digital ni proyectos en tratamiento.	El país ha elaborado algún proyecto de estrategia y/o política nacional , o ha recibido asistencia internacional pero no se ha implementado todavía.	El país tiene una Estrategia o Política en implementación.	EL país tiene una Estrategia o política en implementación con indicadores de avance, transparencia.
Ley de ciberseguridad vigente	El indicador releva información sobre la existencia de una ley que contempla la ciberseguridad o a la seguridad digital y las infraestructuras críticas o servicios esenciales.	El país no posee ley ni proyectos en tratamiento de ciberseguridad o de seguridad digital y la protección de las infraestructuras críticas o servicios esenciales.	El país ha elaborado algún proyecto de ley sin debates o trascendencia, y la protección de las infraestructuras críticas o servicios esenciales.	El País tiene un proyecto de ley en tratamiento o existen debates legislativos sobre ciberseguridad y la protección de las infraestructuras críticas o servicios esenciales.	El país posee ley sobre ciberseguridad o seguridad digital y contempla la protección de infraestructuras críticas y servicios esenciales aprobada.
Autoridad de aplicación	El indicador releva información sobre la existencia de una autoridad estatal que aborda aspectos de ciberseguridad o seguridad digital.	El país no cuenta con organismo que atiende alguna función de ciberseguridad.	El país cuenta con un organismo que atiende alguna de las funciones de ciberseguridad de manera aislada.	El país cuenta con un organismo que atiende funciones de ciberseguridad en el marco de una política más amplia, no como una función independiente que contribuye con muchas otras políticas.	El país cuenta con un organismo que atiende funciones de manera integral en ciberseguridad como una función independiente que contribuye y se coordina con otras políticas.
Madurez y requerimientos legales para el CERT/CSIRT	El indicador releva información sobre la madurez del país en el despliegue de CERTS/CSIRT y los requerimientos establecidos para su establecimiento.	El país no posee un CSIRT o CERT.	El país posee un CSIRT de gobierno pero su rol y responsabilidades no están definidos en el marco legal.	El país posee un CSIRT de gobierno cuyo rol y responsabilidades están definidos en el marco legal pero no tiene un nivel jerárquico para atender al gobierno.	El marco legal define el rol y las responsabilidades del CERT o CSIRT nacional y / o pertenece a FIRST.
Gestión de ciber crisis	El indicador releva las capacidades institucionales para la gestión de crisis cibernética.	El país no posee capacidades para la gestión de crisis cibernética.	El país posee algunos lineamientos en gestión de crisis cibernética pero sus funciones y responsabilidades no están definidas en el marco legal.	El país posee una entidad de gestión de crisis cibernética cuyas sus funciones y responsabilidades están en curso de definición.	El país tiene una entidad de gestión de crisis cibernética y establece una líneas directrices sobre funciones y responsabilidades de la gestión de crisis, actividades de gestión de crisis, procedimientos de gestión de crisis, y canales de comunicación.

Variable	Descripción	Criterio de puntuación			
		0	1	2	3
Gestión de la infraestructura crítica	El indicador muestra la madurez en materia de atención a la ciberseguridad de las infraestructuras críticas.	El país no tiene ningún tipo de lineamiento sobre protección de infraestructuras críticas.	El país tiene algún tipo de lineamiento o requerimiento sobre protección de infraestructuras críticas.	El país tiene una norma (formal) con definiciones y requerimiento sobre protección de infraestructuras críticas.	El país tiene una norma (formal) y un organismo que atiende la protección de infraestructuras críticas.
Capacidades en materia de notificación ante incidentes a nivel nacional	El Indicador releva las acciones de notificación ante incidentes de ciberseguridad que afecte a la Nación.	El país no tiene ningún tipo de lineamiento sobre la notificación o atención ante incidentes.	El país tiene algún tipo de lineamiento sobre la notificación o atención ante incidentes.	El país tiene lineamiento sobre la notificación o atención ante incidentes para la Administración Pública Nacional.	El país tiene lineamiento sobre la notificación o atención ante incidentes para la Administración Pública Nacional e Infraestructuras críticas.
Medidas de gestión de riesgo de ciberseguridad para las Infraestructuras críticas o servicios esenciales.	El Indicador releva las acciones de gestión de riesgo ante incidentes de ciberseguridad que afecte a la Nación (análisis de riesgo, gestión de incidentes, continuidad de las actividades, seguridad de la cadena de suministros, evaluación de las medidas de gestión de riesgo, prácticas de ciber higiene, criptografía, recursos humanos, autenticación y comunicación seguras).	El país no tiene ningún tipo de lineamiento sobre la gestión de riesgo ante incidentes de ciberseguridad.	El país tiene algún tipo de lineamiento sobre la gestión de riesgo ante incidentes de ciberseguridad pero no incluyen todas las siguientes dimensiones:(análisis de riesgo, gestión de incidentes, continuidad de las actividades, seguridad de la cadena de suministros, evaluación de las medidas de gestión de riesgo, prácticas de ciber higiene, criptografía, recursos humanos, autenticación y comunicación seguras).	El país tiene lineamiento sobre la gestión de riesgo ante incidentes que incluyen el análisis de riesgo, la gestión de incidentes, la continuidad de las actividades, la seguridad de la cadena de suministros, la evaluación de las medidas de gestión de riesgo, las prácticas de ciber higiene, el uso de criptografía, la seguridad de los recursos humanos, y el uso de autenticación y comunicación seguras, pero so aplican para la Administración Pública Nacional.	El país tiene establecida unas medidas de gestión de riesgo de ciberseguridad que incluyen el análisis de riesgo, la gestión de incidentes, la continuidad de las actividades, la seguridad de la cadena de suministros, la evaluación de las medidas de gestión de riesgo, las prácticas de ciber higiene, el uso de criptografía, la seguridad de los recursos humanos, y el uso de autenticación y comunicación seguras, para todas las infraestructuras críticas o servicios esenciales.
Educación y programas de formación en ciberseguridad a nivel nacional	El indicador releva la existencia de formación en ciberseguridad a nivel nacional.	El país no tiene ningún tipo de promoción o acción sobre la necesidad de formación, programas o cursos en materia de ciberseguridad.	El país tiene algún tipo de promoción o acción sobre la necesidad de formación, realiza programas o cursos en materia de ciberseguridad.	El país tiene programas de formación o cursos en materia de ciberseguridad.	El país evidencia de trabajar en ciberseguridad con el ministerio o área de Educación y programas de formación para empleados públicos con distintos contenidos técnicos.
Programas de sensibilización	El indicador releva la existencia de campañas de sensibilización en materia ciberseguridad a nivel nacional.	El país no evidencia campañas de sensibilización en materia de ciberseguridad.	El país tiene alguna campaña en materia de sensibilización en ciberseguridad.	El país realiza o realizó varias campañas sobre sensibilización en ciberseguridad.	El país evidencia la coordinación de campañas de sensibilización dirigida a diferentes públicos (niños, adultos mayores, escolares, empleados, PYMES, etc.).
Coordinación internacional	El indicador releva las capacidades nacionales para la coordinación internacional en materia de ciberseguridad o seguridad digital.	El país no evidencia coordinación o participación en foros internacionales en ningún aspectos de los temas relativos con Ciberseguridad.	El país evidencia alguna coordinación o participación en foros internacionales en algún aspectos (Cibercrimen, CSIRT, ITU, Celac, Mercosur, etc.) de los temas relativos con Ciberseguridad.	El país realiza alguna coordinación o participación formal en foros internacionales en algún aspectos (Cibercrimen, Educación, FIRST, ITU, Celac, Mercosur, etc.) de los temas relativos con Ciberseguridad.	El país realiza una coordinación o participación formal continua en foros internacionales en más de un ámbito (Cibercrimen, Educación, FIRST, ITU, Celac, Mercosur, etc.) relativos con Ciberseguridad.

Fuente: Elaboración propia.

Este documento presenta un análisis exhaustivo del estado de la protección de datos personales y la ciberseguridad en los 33 países de América Latina y el Caribe. A través de una revisión detallada de la situación actual, se determinan los desafíos clave, como el aumento de los incidentes de ciberseguridad y la falta de comprensión sobre cuestiones relacionadas con la economía de datos, así como los avances en materia normativa y regulatoria, y se destacan las disparidades existentes entre los distintos países.

Se adopta un enfoque integral, al evaluar tanto las fortalezas como las debilidades de la región mediante un marco conceptual que define los ámbitos de análisis de la ciberseguridad y la protección de datos personales. Asimismo, se discuten aspectos cruciales, como la necesidad de una mayor continuidad en el ámbito de las políticas, la sensibilización social y el desarrollo de capacidades técnicas.

El documento concluye con una serie de recomendaciones concretas para mejorar la solidez de los marcos normativos sobre protección de datos y ciberseguridad en la región y promover un entorno digital seguro y confiable que impulse el desarrollo y la confianza en el ámbito digital.

CEPAL

Comisión Económica para América Latina y el Caribe (CEPAL)
Economic Commission for Latin America and the Caribbean (ECLAC)
www.cepal.org

LC/TS.2024/102