CIBERSEGURIDAD EN AMÉRICA LATINA:

Estrategias nacionales en 2024

Derechos Digitales
AMÉRICA LATINA

CIBERSEGURIDAD EN AMÉRICA LATINA:
Estrategias nacionales en 2024

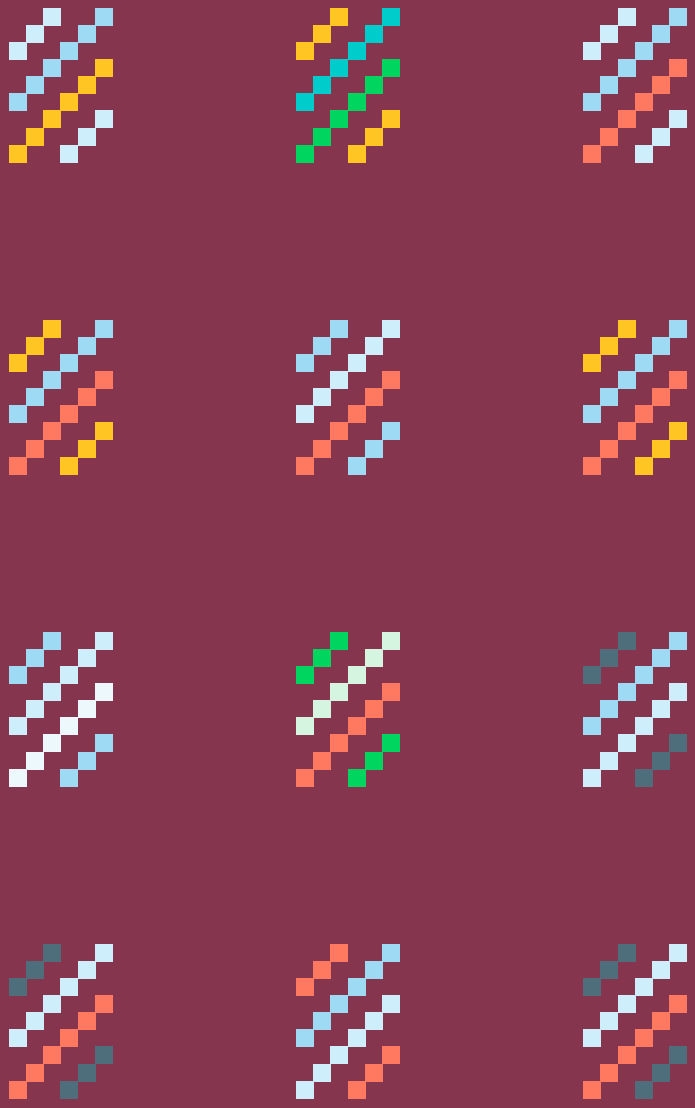
Esta publicación fue creada por Derechos Digitales, una organización independiente sin fines de lucro, fundada en 2005, que tiene como misión la defensa, promoción y desarrollo de los derechos humanos en entornos digitales en América Latina.

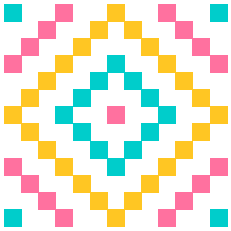
Autor: Juan Carlos Lara
Traducción al inglés y portugués: Dafne Melo
Diseño: Comunas Unidas

Diciembre, 2024.

Esta publicación fue posible para Derechos Digitales como miembro de la Colaborativa CYRILLA.

ÍNDICE





RESUMEN EJECUTIVO

La ciberseguridad se ha convertido en un tema prioritario para los gobiernos de América Latina, dado el incremento de amenazas digitales y la creciente dependencia de las infraestructuras tecnológicas. Este informe da cuenta superficialmente de la existencia de políticas y estrategias nacionales de ciberseguridad de la región, identificando los puntos comunes y desafíos que persisten en su implementación.

El documento destaca la diversidad de enfoques en la región, con estrategias que varían en términos de alcance, madurez y capacidad de ejecución. En algunos casos, como en Argentina y Ecuador, las estrategias están bien definidas pero enfrentan desafíos en su implementación debido a la falta de recursos técnicos y humanos. En otros, como en Perú, la falta de formalización de los documentos limita el impacto de los esfuerzos en ciberseguridad.

Este análisis concluye que, para avanzar hacia un entorno digital seguro y resiliente, es fundamental priorizar la colaboración regional, fortalecer las capacidades locales y alinear las estrategias nacionales con los estándares internacionales. Entre los principales desafíos identificados se encuentran la necesidad de fortalecer las capacidades técnicas nacionales, la coordinación multisectorial y la cooperación internacional. Además, la región necesita avanzar en la creación de marcos regulatorios específicos que respalden las estrategias nacionales y en la promoción de una cultura de ciberseguridad entre la ciudadanía.

1. INTRODUCCIÓN

La ciberseguridad en América Latina ha evolucionado de manera desigual, reflejando una diversidad de contextos nacionales y prioridades estratégicas. El presente documento es un mapeo de las políticas y estrategias de ciberseguridad adoptadas o en proceso de desarrollo en distintos países de la región, desde aquellas formalizadas y en plena implementación hasta los esfuerzos iniciales de planificación y consulta. La integración de perspectivas nacionales e internacionales resulta esencial para entender el panorama regional.

Este análisis omite considerar en profundidad los marcos institucionales y legales que sustentan las estrategias, como las acciones concretas propuestas para enfrentar las crecientes amenazas cibernéticas. Desde Brasil, con su consolidada estrategia E-Ciber, hasta casos como Honduras y El Salvador, donde los avances son incipientes, se evidencia una brecha significativa en capacidades y recursos que influye en la efectividad de las políticas. Dicha disparidad amerita un esfuerzo de muy diferente envergadura.

El objetivo del texto es proporcionar una visión integral de la ciberseguridad en América Latina en 2024, evaluando los logros alcanzados, las áreas que requieren atención urgente y las oportunidades para fortalecer la cooperación regional. Esta perspectiva permitirá a los actores involucrados diseñar respuestas más coordinadas y eficaces frente a las amenazas emergentes en el ciberespacio

2. ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN AMÉRICA LATINA

2.1. Argentina: *Segunda Estrategia Nacional de Ciberseguridad*

Argentina ha avanzado significativamente en su enfoque hacia la ciberseguridad con la implementación de la Segunda Estrategia Nacional de Ciberseguridad, aprobada por la Resolución 44/2023 de la Secretaría de Innovación Pública en septiembre de 2023[1]. Elaborada por el Comité Nacional de Ciberseguridad, el documento establece las directrices nacionales para la protección del ciberespacio, con el objetivo de prevenir acciones que puedan afectar a la administración del Estado, organizaciones, servicios esenciales y a la ciudadanía en general.

La nueva estrategia aborda temas como la incorporación de la perspectiva de género y derechos humanos, la atención a sectores vulnerables, y consideraciones específicas relacionadas con desarrollos tecnológicos emergentes como Internet de las Cosas (IoT), 5G y servicios en la nube. Además, se enfoca en la soberanía digital y promueve una gobernanza colaborativa que involucra a múltiples partes interesadas.

El documento incluye ocho Principios Rectores, a saber: Paz y seguridad en el ciberespacio, respeto por los derechos humanos y libertades fundamentales, construcción de capacidades y fortalecimiento federal, cooperación internacional, cultura de ciberseguridad y responsabilidad

(1) Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

compartida, fortalecimiento del desarrollo socioeconómico, seguridad para personas en situación de vulnerabilidad o históricamente discriminadas, perspectiva de género y derechos humanos.

En tanto, los objetivos a los que están supeditadas las 42 medidas mencionadas son: fortalecimiento del sistema institucional para abordar la ciberseguridad a nivel federal; protección de las infraestructuras críticas nacionales; protección y recuperación de sistemas de información del sector público; fortalecimiento de capacidades de prevención, detección y respuesta; concientización, capacitación y educación en ciberseguridad; desarrollo de un marco normativo acorde a los desafíos digitales; cooperación internacional en ciberseguridad; fomento de la industria nacional de ciberseguridad.

2.2. Brasil: *E-Ciber*

La Estrategia Nacional de Seguridad Cibernética o "E-Ciber" fue aprobada por el Decreto Nº 10.222, en febrero de 2020[2], con el propósito de consolidar el liderazgo regional de Brasil en ciberseguridad. Se enmarca en la Política Nacional de Seguridad de la Información, establecida por el Decreto Nº 9.637 de diciembre de 2018, que define principios y objetivos para la seguridad de la información en la administración pública federal. La E-Ciber fue desarrollada con la participación de más de cuarenta organismos gubernamentales, instituciones privadas y del sector académico, y tiene como objetivo principal fortalecer la seguridad cibernética en el país, mejorando la resiliencia de las infraestructuras críticas y los servicios públicos nacionales.

La visión de la Estrategia Nacional de Seguridad Cibernética de Brasil es convertir al país "en un país de excelencia en seguridad cibernética". Para alcanzar esta visión, se definieron tres objetivos estratégicos fundamentales: hacer de Brasil un país más próspero y confiable en el entorno digital; aumentar la resiliencia brasileña frente a las amenazas cibernéticas; y fortalecer el rol de Brasil en seguridad cibernética en el escenario internacional. Esto parece ir en línea con el carácter del gobierno de Jair Bolsonaro durante cuyo mandato se aprobó la Estrategia.

Las acciones estratégicas de la política incluyen fomentar la cooperación nacional e internacional para el intercambio de información sobre ciberamenazas; desarrollar capacidades de prevención, monitoreo y respuesta ante incidentes cibernéticos; proteger las infraestructuras críticas de información con un enfoque integral; promover la concientización pública sobre la importancia de la ciberseguridad; establecer programas de capacitación técnica en seguridad cibernética; incentivar la investigación y el desarrollo de soluciones tecnológicas avanzadas; y participar activamente en foros internacionales relacionados con la seguridad cibernética.

E-Ciber tenía un horizonte de vigencia que se extendía hasta el año 2023. En junio de 2023, ya bajo una administración distinta, se anunció la extensión de la vigencia de la estrategia hasta el año 2024[3] Queda pendiente una nueva política que rija con posterioridad, en la que ya se estaría trabajando.

---

(2) Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

(3) "Governo prorroga por um ano a Estratégia Nacional de Segurança Cibernética", Convergência Digital, 6 de junio de 2023. https://convergenciadigital.com.br/seguranca/governo-prorroga-por-um-ano-a-estratgia-nacional-de-segurana-ciberntica/

2.3. Chile: *PNCS 2023-2028*

La primera Política Nacional de Ciberseguridad (PNCS) se implementó entre 2017 y 2022, estableciendo las bases para un ciberespacio más seguro. Posteriormente, el 4 de diciembre de 2023, se publicó en el Diario Oficial la nueva PNCS para el período 2023-2028[4]. El Comité Interministerial sobre Ciberseguridad (CICS) ha sido el órgano encargado de la elaboración y coordinación de estas políticas, asegurando la colaboración entre diversas entidades gubernamentales y privadas, como también los procesos de audiencias y consultas públicas previos a la finalización de cada PNCS.

La PNCS 2023-2028 mantiene cinco objetivos fundamentales ya presentes en su antecesora: infraestructura resiliente, derechos de las personas, cultura de ciberseguridad, coordinación nacional e internacional, y fomento a la industria e investigación científica. Además, incorpora cuatro objetivos transversales: enfoque de derechos humanos, perspectiva de género, desarrollo sostenible, y cooperación internacional.

En un avance significativo para las PNCS, en marzo de 2024 se promulgó la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, que crea la Agencia Nacional de Ciberseguridad (ANCI). Este organismo rector es responsable de regular, fiscalizar y sancionar a todos los organismos públicos y privados que presten servicios esenciales, fortaleciendo la institucionalidad en materia de ciberseguridad en Chile.

Aunque la PNCS 2023-2028 establece directrices claras, aún no se ha publicado el plan de acción detallado que especifica las medidas y plazos para alcanzar los objetivos propuestos. Se espera que este documento complementario sea divulgado próximamente para orientar la implementación efectiva de la política.

2.4. Colombia: *Políticas de Confianza y Seguridad Digital*

En 2016, el país adoptó la Política Nacional de Seguridad Digital mediante el documento CONPES 3854, estableciendo las bases para un entorno digital más seguro y confiable. Posteriormente, en 2020, se publicó la Política Nacional de Confianza y Seguridad Digital (CONPES 3995)[5], cuyos objetivos son: fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo; y analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

En línea con estos esfuerzos, el Gobierno colombiano ha propuesto la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, una entidad técnica y especializada que tendrá como objetivo planificar, articular y gestionar los riesgos de seguridad digital en el país, así como fortalecer la confianza y seguridad en el ámbito digital. Este proyecto de ley fue radicado ante el Congreso en julio de 2023 y ha avanzado en su trámite legislativo, siendo aprobado en primer debate en noviembre del mismo año. La Agencia

(4) Disponible en: https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf?utm_source=chatgpt.com

(5) Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

será responsable de coordinar las acciones en materia de ciberseguridad, incluyendo la protección de infraestructuras críticas de información, la respuesta a incidentes cibernéticos y la promoción de una cultura de seguridad digital en la sociedad colombiana.

Todos estos son esfuerzos de una estrategia a nivel político para potenciar las capacidades en ciberseguridad de Colombia[6], que además de la creación de la Agencia, incluye al fortalecimiento del Centro Cibernético de Respuesta a Incidentes de Colombia (ColCERT), el nacimiento de un centro de ciberseguridad en Caldas, y la mejora de la capacitación y entrenamiento de especialidades en ciberseguridad..

2.5. Costa Rica: *Estrategia Nacional de Ciberseguridad 2023-2027*

En 2017, Costa Rica implementó su primera Estrategia Nacional de Ciberseguridad, estableciendo un marco para proteger sus infraestructuras críticas y promover una cultura de seguridad digital. Sin embargo, ante el incremento de ciberamenazas y la evolución tecnológica, se reconoció la necesidad de actualizar esta estrategia. En noviembre de 2023, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) presentó la nueva Estrategia Nacional de Ciberseguridad 2023-2027[7], con el objetivo de fortalecer la resiliencia del país frente a las amenazas cibernéticas y garantizar un entorno digital seguro para la ciudadanía.

La Estrategia Nacional de Ciberseguridad 2023-2027 se articula en torno a cinco pilares fundamentales: gobernanza y coordinación; marcos legales y normativas; protección de infraestructuras y ciberresiliencia: educación, capacitación y concientización; y cooperación y alianzas. Estos pilares buscan establecer un marco de acción integral que permita prevenir y mitigar los riesgos y amenazas en el entorno digital, fomentar la innovación y el desarrollo de soluciones en ciberseguridad, fortalecer la capacidad de respuesta ante incidentes y promover una cultura de seguridad sólida en la sociedad costarricense.

En términos de orgánica, el MICITT lidera la implementación de la estrategia en coordinación con el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR), que opera componente esencial de esta estrategia, como ente encargado de coordinar la seguridad cibernética y de información en el país. La estrategia incorpora la participación activa de instituciones públicas, empresas privadas, la sociedad civil y la academia, garantizando un enfoque multisectorial para el fortalecimiento de la ciberseguridad en el país.

2.6. Ecuador: *ENC*

El 3 de agosto de 2022, el país presentó su primera Estrategia Nacional de Ciberseguridad (ENC), elaborada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Esta estrategia busca proporcionar a los ciudadanos un acceso más seguro a los servicios digitales y fortalecer la protección de sus datos personales, en un contexto de reciente puesta en vigencia de su primera ley nacional integral en esa última materia.

---

(6) "Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad", MINTIC, 19 de julio de 2023. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276939:Ministro-TIC-presenta-la-estrategia-de-cuatro-puntos-para-hacer-de-Colombia-una-potencia-en-Ciberseguridad

(7) Disponible en: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%20 10Nov2023%20SPA.pdf

La ENC se estructura en seis ejes de acción: gobernanza y coordinación nacional, resiliencia cibernética, lucha contra la ciberdelincuencia, ciberdefensa nacional y ciberinteligencia, habilidades y capacidades de ciberseguridad, cooperación internacional.

La implementación de la ENC implica la participación activa de diversas instituciones públicas y privadas, así como la colaboración con organismos internacionales especializados en ciberseguridad. El MINTEL lidera la coordinación de estas acciones, trabajando en conjunto con entidades como el Comité Nacional de Ciberseguridad, para garantizar un enfoque integral y efectivo en la protección del ciberespacio ecuatoriano.

2.7. Guatemala: *Estrategia Nacional de Seguridad Cibernética*

Guatemala publicó su Estrategia Nacional de Seguridad Cibernética el 20 de junio de 2018[8], elaborada por el Ministerio de Gobernación en colaboración con diversos actores nacionales e internacionales. El proceso de elaboración incluyó consultas y validaciones con más de 160 representantes de distintos sectores de la sociedad guatemalteca, buscando fortalecer la seguridad en el ciberespacio y proteger los datos personales de los ciudadanos.

La estrategia se articula en torno a los siguientes ejes fundamentales: fortalecimiento de capacidades, protección de infraestructuras críticas, marco legal y regulatorio, concientización y educación, cooperación internacional. Además, incluye planes de acción específicos con medidas concretas, aunque no detalla su número total.

La implementación de la estrategia ha enfrentado desafíos, principalmente debido a la ausencia de un marco legal específico que respalde las acciones propuestas. A pesar de ello, se han realizado esfuerzos para conformar el Comité Nacional de Seguridad Cibernética, encargado de coordinar y dar seguimiento a las políticas en esta materia. La vigencia de la estrategia está sujeta a revisiones periódicas para adaptarse a las nuevas amenazas y avances tecnológicos en el ámbito digital.

2.8. México: *ENCS*

México publicó su Estrategia Nacional de Ciberseguridad (ENCS) en noviembre de 2017, elaborada con la colaboración de la Organización de los Estados Americanos (OEA)[9]. El proceso de desarrollo de la ENCS, denominado "Hacia una Estrategia Nacional de Ciberseguridad", se llevó a cabo de marzo a octubre de 2017, promoviendo espacios de diálogo, discusión y aprendizaje mediante foros y talleres que involucraron a diversos actores de la sociedad mexicana.

La ENCS establece cinco objetivos estratégicos: proteger la sociedad y sus derechos, preservar la prosperidad económica del país, mantener el orden público, la paz y la seguridad nacional, fortalecer la cooperación internacional, y promover un gobierno digital confiable. Además, se basa en principios rectores como la perspectiva de derechos humanos, enfoque basado en gestión de riesgo, y colaboración multidisciplinaria y de múltiples actores.

(8) Disponible aquí: https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf

(9) Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Desde su publicación, la implementación de la ENCS ha enfrentado desafíos, incluyendo la necesidad de armonizar esfuerzos entre diversas instituciones y sectores. A pesar de estos retos, se han realizado avances en la promoción de una cultura de ciberseguridad y en la capacitación de personal especializado. La vigencia de la estrategia está sujeta a revisiones periódicas para adaptarse a las constantes evoluciones del entorno digital y las nuevas amenazas cibernéticas.

2.9. Nicaragua: *Estrategia Nacional de Ciberseguridad 2020-2025*

Nicaragua aprobó su Estrategia Nacional de Ciberseguridad 2020-2025 mediante el Decreto Presidencial Nº 24-2020, publicado el 29 de septiembre de 2020[10]. Esta estrategia fue desarrollada por el Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR) y el Ministerio de Relaciones Exteriores, con el objetivo de garantizar un uso soberano, seguro y confiable del ciberespacio en el país.

La estrategia se fundamenta en cuatro principios rectores: garantía de la soberanía y protección de los derechos de los ciudadanos en el ciberespacio, gestión de riesgos y capacidad de resiliencia, protección y defensa del ciberespacio, y cooperación internacional. Además, se estructura en cinco objetivos estratégicos: fortalecer la gobernanza de la ciberseguridad, proteger las infraestructuras críticas de información, desarrollar capacidades nacionales en ciberseguridad, promover una cultura de ciberseguridad en la sociedad, y fomentar la cooperación internacional en materia de ciberseguridad.

La implementación de la estrategia está prevista para el período 2020-2025, con evaluaciones periódicas para adaptarse a las necesidades del país y a las amenazas emergentes en el ámbito digital. Sin embargo, su aplicación ha suscitado preocupaciones entre organizaciones de derechos humanos y sectores de la sociedad civil, quienes temen que pueda ser utilizada para restringir la libertad de expresión y aumentar el control gubernamental sobre el ciberespacio, como ha ocurrido a propósito de la polémica Ley de Ciberdelitos de ese país.

2.10. Panamá: *Estrategia Nacional de Ciberseguridad 2021-2024*

Panamá publicó su Estrategia Nacional de Ciberseguridad 2021-2024 el 15 de diciembre de 2021, mediante la Resolución Nº 17 de la Autoridad Nacional para la Innovación Gubernamental (AIG)[11]. Esta estrategia actualiza la Estrategia Nacional de Seguridad Cibernética de 2013, reflejando la evolución de las tecnologías de la información y comunicación y la necesidad de fortalecer la seguridad en el ciberespacio panameño.

La estrategia se estructura en cuatro pilares fundamentales: proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio, disuadir y castigar el comportamiento criminal en el ciberespacio, fortalecer la seguridad y la resiliencia de la infraestructura crítica de la nación, y fomentar una cultura nacional de ciberseguridad.

(10) Disponible en: https://legislacion.asamblea.gob.ni/indice.nsf/c3639d8c1d72577006256fe800533609/e9e4a6071fa07177062585b9005fd3db

(11) Disponible en: http://www.gacetaoficial.gob.pa/pdfTemp/29434_A/88864.pdf

Para su implementación, la AIG ha coordinado talleres y campañas de concientización, como "Panamá Cibersegura", dirigidas a promover una cultura de ciberseguridad en la sociedad. Además, se ha fortalecido el rol del CSIRT Panamá como equipo nacional de respuesta a incidentes de seguridad de la información, encargado de prevenir, identificar y resolver ataques cibernéticos que afecten la infraestructura crítica del país. La estrategia está vigente hasta 2024, con evaluaciones periódicas para adaptarse a las nuevas amenazas y avances tecnológicos.

2.11. Paraguay: *Plan Nacional de Ciberseguridad*

Paraguay adoptó su Plan Nacional de Ciberseguridad en 2017, aprobado mediante el Decreto Nº 7052/17[12]. Este plan fue desarrollado bajo el liderazgo de la Presidencia de la República, a través de la entonces Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), en coordinación con el Ministerio de Relaciones Exteriores (MRE) y con el apoyo de la OEA. El proceso de elaboración involucró a diversos sectores, incluyendo el sector privado y la sociedad civil, con el objetivo de establecer políticas públicas que fortalezcan la seguridad de los activos críticos y promuevan un ciberespacio seguro y resiliente.

El plan se estructura en varios ejes de acción: sensibilización y cultura, investigación, desarrollo e innovación, protección de infraestructuras críticas, capacidad de respuesta ante incidentes cibernéticos, capacidad de investigación y persecución, y coordinación nacional. Además, define objetivos específicos y un plan de acción para la ejecución de la política nacional de ciberseguridad, con la participación de entidades gubernamentales, el sector privado, la academia y la sociedad civil.

En 2024, el Ministerio de Tecnologías de la Información y Comunicación (MITIC), a través de la Dirección General de Ciberseguridad y Protección a la Información (DGCPI) y el CERT-PY, inició el proceso de actualización de la estrategia nacional para el período 2024-2028, nuevamente con el apoyo de la OEA. Este proceso incluye mesas de diálogo y trabajo con actores clave del ecosistema de ciberseguridad nacional, buscando consolidar una política pública actualizada que responda a los desafíos emergentes en el ámbito digital.

2.12. República Dominicana: *Estrategia Nacional de Ciberseguridad 2030*

La República Dominicana aprobó su Estrategia Nacional de Ciberseguridad 2030 mediante el Decreto Nº 313-22, de 14 de junio de 2022[13], con un horizonte de vigencia hasta el 31 de diciembre de 2030. Esta estrategia tiene como objetivo fortalecer el marco nacional de ciberseguridad, fomentando la creación de entornos digitales seguros, confiables y resilientes que promuevan una sociedad digital inclusiva y respetuosa de los derechos fundamentales.

La estrategia se estructura en varios ejes fundamentales: fortalecimiento del marco normativo, desarrollo de capacidades y competencias en ciberseguridad, protección de infraestructuras críticas de información, gestión de riesgos y respuesta a incidentes cibernéticos, concientización y cultura de ciberseguridad, y cooperación nacional e internacional.

(12) Disponible en: https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

(13) Disponible en: https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

Para su implementación, se ha establecido un Consejo Directivo presidido por el Ministerio de la Presidencia, que coordina las acciones del Centro Nacional de Ciberseguridad (CNCS). El CNCS es responsable de ejecutar las políticas y planes derivados de la estrategia, incluyendo la operación del CSIRT-RD, el equipo nacional de respuesta a incidentes cibernéticos. La estrategia prevé evaluaciones periódicas para adaptarse a las nuevas amenazas y avances tecnológicos, asegurando la protección del ciberespacio dominicano y la confianza digital de sus ciudadanos.

3. LOS PROCESOS DE FORMULACIÓN DE ESTRATEGIAS EN CURSO

Los demás países de la región no cuentan con estrategias o políticas nacionales sobre ciberseguridad, sin perjuicio de contar, en varios casos, con medidas aplicables a nivel de gobierno central o bien regulación relacionada. En varios de estos casos, las estrategias o políticas nacionales han sido anunciadas o están en elaboración.

Aunque El Salvador no cuenta aún con un texto definitivo, está en desarrollo su Estrategia Nacional de Ciberseguridad para fortalecer la protección de la información digital y la infraestructura crítica del Estado, como compromiso de la Agenda Digital 2020-2030[14]. No obstante, durante 2024 el país ha aprobado la Ley de Ciberseguridad y Seguridad de la Información, que establece principios, un marco legal y lineamientos para estructurar, regular, auditar y fiscalizar las medidas de ciberseguridad en las instituciones públicas. Esta ley obliga a implementar sistemas de gestión de ciberseguridad, elaborar estrategias de seguridad informática y mantener registros actualizados de las acciones ejecutadas en este ámbito.

Honduras tampoco cuenta con una estrategia ni con un CSIRT nacional, lo que limita su capacidad para enfrentar incidentes cibernéticos y proteger su infraestructura digital. En el Plan de Gobierno Digital de Honduras 2023-2026[15] se compromete la emisión de una Estrategia Nacional de Ciberseguridad y un Plan de Acción, además de la creación de un equipo para incidentes cibernéticos.

El Perú cuenta con un documento de trabajo titulado Estrategia Nacional de Seguridad y Confianza Digital 2021-2026[16], elaborado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM). El documento propone un marco integral para fortalecer la ciberseguridad y promover la confianza en el entorno digital, articulándose en ejes como cultura de seguridad, desarrollo de capacidades, protección de activos críticos, estándares, servicios digitales y marco jurídico. Sin embargo, el documento no ha sido adoptado como política oficial.

(14) Disponible en: https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf

(15) Disponible en: https://www.diger.gob.hn/sites/default/files/2024-02/Plan%20de%20Gobierno%20Digital%20Honduras.pdf

(16) Referenciado en el sitio de la Secretaría de Gobierno y Transformación Digital, disponible en: https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital

Uruguay está en proceso de desarrollar su Estrategia Nacional de Ciberseguridad 2024-2030, liderada por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic)[17]. La estrategia se estructura en seis pilares: gobernanza y regulación, protección de infraestructuras críticas, capacidades técnicas y humanas, educación y concienciación, gestión de riesgos, cooperación nacional e internacional. Su elaboración incluye consultas públicas y talleres multisectoriales, integrando las perspectivas de actores clave para diseñar un marco integral de ciberseguridad. Este esfuerzo complementa la reciente entrada en vigor de la Ley 20.327, que establece disposiciones para prevenir y sancionar delitos informáticos. A la fecha de cierre de este informe no había una versión definitiva de la Estrategia.

Venezuela ha dado pasos hacia la consolidación de una Estrategia Nacional de Ciberseguridad, aunque no cuenta con un documento formalizado. En agosto de 2024, el gobierno creó el Consejo Nacional de Ciberseguridad mediante el Decreto N° 42.939, con el objetivo de coordinar las políticas en esta materia, asesorar al Ejecutivo y proponer regulaciones específicas[18]. El ciberespacio fue declarado de interés público y estratégico, enfatizando la necesidad de medidas para proteger las infraestructuras críticas y garantizar la soberanía digital. A pesar de la falta de una estrategia integrada, el país cuenta con un Sistema Nacional de Seguridad Informática, bajo la supervisión de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), que busca establecer estándares y condiciones para un uso seguro de las tecnologías de información y comunicación.

4. ANÁLISIS

El panorama de la ciberseguridad en América Latina refleja una diversidad de enfoques y niveles de madurez en la implementación de estrategias nacionales. Países como Argentina y Brasil han avanzado en la formalización de políticas que buscan fortalecer la resiliencia frente a amenazas cibernéticas, mientras que naciones como Honduras y Perú aún no han consolidado marcos estratégicos oficiales, lo que podría limitar su capacidad de respuesta ante incidentes digitales.

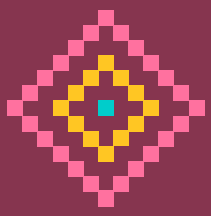
La influencia de organismos internacionales, especialmente la Organización de los Estados Americanos, ha sido determinante en la asesoría y el apoyo técnico para la elaboración de estas estrategias. Este acompañamiento ha permitido a varios países estructurar planes alineados con estándares globales, además de contar con soporte técnico respecto de objetivos y medidas propuestas. Más relevantemente, ese acompañamiento permite considerar que, a pesar de la dispersión de órganos e instrumentos, sus contenidos pueden estar promoviendo una visión regional coherente en materia de ciberseguridad.

(17) "Cocreación de la Estrategia Nacional de Ciberseguridad", Agesic, 10 de septiembre de 2024. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/cocreacion-estrategia-nacional-ciberseguridad

(18) "Gaceta Oficial: Creado Consejo Nacional de Ciberseguridad", ISCOM, 20 de agosto de 2024. http://mippci.gob.ve/index.php/2024/08/20/gaceta-oficial-creado-consejo-nacional-de-ciberseguridad/

La implementación efectiva de estas políticas enfrenta desafíos significativos. La carencia de recursos especializados, tanto humanos como tecnológicos, y la falta de marcos legales robustos dificultan la ejecución de medidas concretas. Además, la rápida evolución de las tecnologías y las tácticas empleadas por actores maliciosos exigen una constante actualización y adaptación de las estrategias nacionales.

Es imperativo que los países de la región fortalezcan la cooperación internacional y regional, compartiendo experiencias y buenas prácticas para enfrentar amenazas comunes. Asimismo, la integración de la ciberseguridad en las agendas nacionales de desarrollo y la promoción de una cultura de seguridad digital entre los ciudadanos son aspectos clave para construir un entorno digital más seguro y resiliente en América Latina.



www.derechosdigitales.org