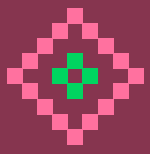
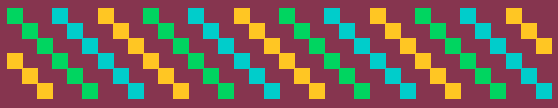
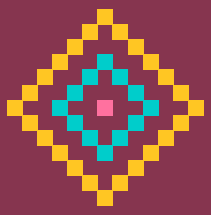






SEGURANÇA CIBERNÉTICA NA AMÉRICA LATINA:

Estratégias nacionais em 2024

Derechos Digitales
AMÉRICA LATINA

SEGURANÇA CIBERNÉTICA NA AMÉRICA LATINA:
Estratégias nacionais em 2024

Esta publicação foi criada por Derechos Digitales, uma organização independente sem fins lucrativos fundada em 2005, cuja missão é defender, promover e desenvolver os direitos humanos em ambientes digitais na América Latina.

Autor: Juan Carlos Lara
Tradução para inglês e português: Dafne Melo
Projeto gráfico: Comunas Unidas

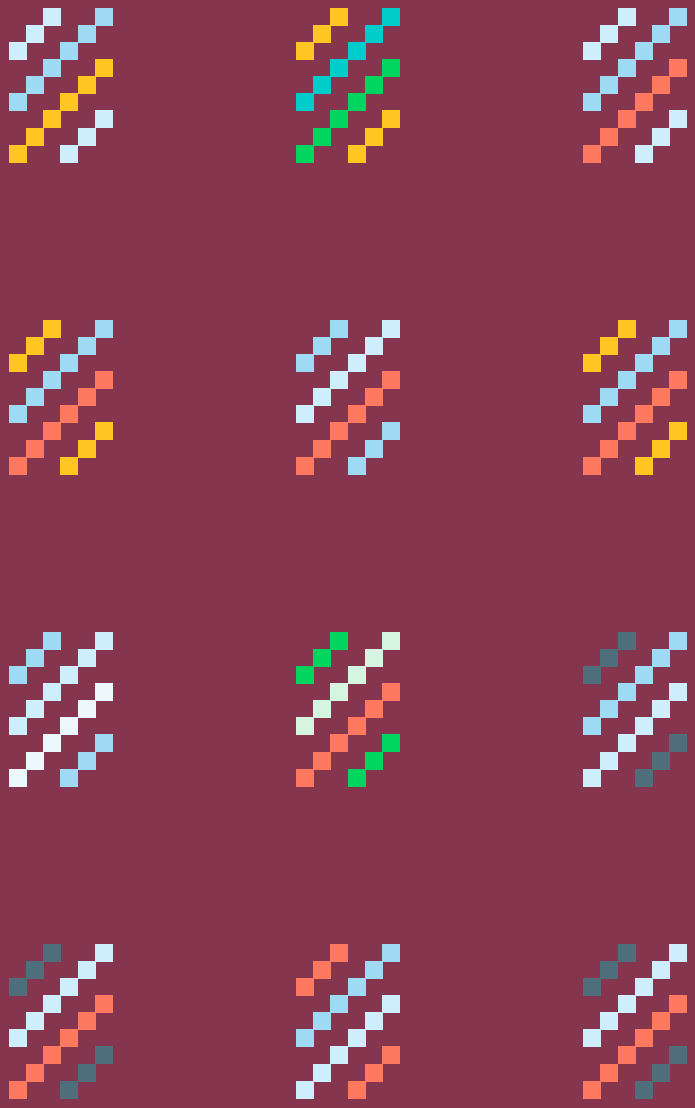
Dezembro, 2024.

Esta publicação foi possível para Derechos Digitales como membro da Colaborativa CYRILLA.

Derechos Digitales
AMÉRICA LATINA

CYRILLA

SUMÁRIO



RESUMO EXECUTIVO

A segurança cibernética se tornou um tema prioritário para os governos da América Latina, dado o aumento de ameaças digitais e a crescente dependência de infraestruturas tecnológicas. Este relatório descreve de forma breve a existência de políticas e estratégias nacionais de segurança cibernética na região, identificando pontos comuns e desafios que persistem em sua implementação.

O documento destaca a diversidade de abordagens na região, com estratégias variadas em termos de alcance, maturidade e capacidade de implementação. Em alguns casos, como Argentina e Equador, as estratégias estão bem definidas, mas enfrentam desafios em sua implementação devido à falta de recursos técnicos e humanos. Em outros, como o Peru, a falta de formalização de documentos limita o impacto dos esforços de segurança cibernética.

Esta análise conclui que, para avançar em direção a um ambiente digital seguro e resiliente, é essencial priorizar a colaboração regional, fortalecer as capacidades locais e alinhar as estratégias nacionais aos padrões internacionais. Os principais desafios identificados incluem a necessidade de fortalecer as capacidades técnicas nacionais, a coordenação multissetorial e a cooperação internacional. Além disso, a região precisa progredir na criação de marcos regulatórios específicos que apoiem estratégias nacionais e na promoção de uma cultura de segurança cibernética entre a população.

1. INTRODUÇÃO

A segurança cibernética na América Latina evoluiu de forma desigual, refletindo uma diversidade de contextos nacionais e prioridades estratégicas. Este documento mapeia políticas e estratégias de segurança cibernética adotadas ou em desenvolvimento em diferentes países da região, desde aquelas formalizadas e em plena implementação até esforços iniciais de planejamento e consulta. Integrar perspectivas nacionais e internacionais é essencial para entender o panorama regional.

Esta análise não considera em profundidade os marcos institucionais e legais que sustentam as estratégias, como as ações concretas propostas para enfrentar as crescentes ameaças cibernéticas. No Brasil, com sua consolidada estratégia E-Ciber, até casos como Honduras e El Salvador, onde os avanços são incipientes, evidencia-se uma falta significativa de capacidades e recursos que influi na efetividade das políticas. Tal disparidade demanda esforços de envergaduras muito diferentes.

O objetivo do texto é proporcionar uma visão integral da segurança cibernética na América Latina em 2024, avaliando as conquistas alcançadas, as áreas que requerem atenção urgente e as oportunidades para fortalecer a cooperação regional. Essa perspectiva permitirá aos atores envolvidos desenhar repostas mais coordenadas e eficazes diante das ameaças emergentes no ciberespaço.

2. ESTRATÉGIAS NACIONAIS DE SEGURANÇA CIBERNÉTICA NA AMÉRICA LATINA

2.1. Argentina: *Segunda Estratégia Nacional de Segurança Cibernética*

A Argentina fez progressos significativos em sua abordagem à segurança cibernética com a implementação da Segunda Estratégia Nacional de Segurança Cibernética, aprovada pela Resolução 44/2023 da Secretaria de Inovação Pública em setembro de 2023[1]. Elaborado pelo Comitê Nacional de Segurança Cibernética, o documento estabelece diretrizes nacionais para a proteção do ciberespaço, com o objetivo de prevenir ações que possam afetar a administração do Estado, organizações, serviços essenciais e a população em geral.

A nova estratégia aborda questões como a incorporação de perspectivas de gênero e direitos humanos, atenção a setores vulneráveis e considerações específicas relacionadas a desenvolvimentos tecnológicos emergentes, como Internet das Coisas (IoT), 5G e serviços em nuvem. Além disso, concentra-se na soberania digital e promove a governança colaborativa envolvendo diversas partes interessadas.

O documento inclui oito Princípios Orientadores, nomeadamente: paz e segurança no ciberespaço; respeito aos direitos humanos e liberdades fundamentais; capacitação e fortalecimento federal; cooperação internacional; cultura de segurança cibernética e

(1) Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

responsabilidade compartilhada; reforço do desenvolvimento socioeconômico; segurança para pessoas em situações vulneráveis ou historicamente discriminadas; perspectiva de gênero e direitos humanos.

Os objetivos a que estão sujeitas as 42 medidas mencionadas são: fortalecer o sistema institucional para abordar a segurança cibernética no nível federal; proteção de infraestruturas críticas nacionais; proteção e recuperação de sistemas de informação do setor público; reforçar as capacidades de prevenção, detecção e resposta; conscientização, treinamento e educação em segurança cibernética; desenvolvimento de um quadro normativo alinhado com os desafios digitais; cooperação internacional em segurança cibernética; fomento à indústria nacional de segurança cibernética.

2.2. Brasil: *E-Ciber*

A Estratégia Nacional de Segurança Cibernética, a "E-Ciber", foi aprovada pelo Decreto nº 10.222, de fevereiro de 2020[2], com o propósito de consolidar a liderança regional do Brasil em cibersegurança. Ela está inserida na Política Nacional de Segurança da Informação, estabelecida pelo Decreto nº 9.637 de dezembro de 2018, que define princípios e objetivos para a segurança da informação na administração pública federal. A E-Ciber foi desenvolvida com a participação de mais de quarenta órgãos governamentais, instituições privadas e do setor acadêmico, e tem como objetivo principal fortalecer a segurança cibernética no país, melhorando a resiliência das infraestruturas críticas e os serviços públicos nacionais.

A visão da Estratégia Nacional de Segurança Cibernética é tornar o Brasil "um país de excelência em segurança cibernética". Para tal, três objetivos estratégicos principais foram definidos: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira a ameaças cibernéticas; e fortalecer o papel do Brasil em segurança cibernética no cenário internacional. Isso parece estar de acordo com a toada do governo de Jair Bolsonaro, em cujo mandato a Estratégia foi aprovada.

As ações estratégicas da política incluem fomentar a cooperação nacional e internacional para o intercâmbio de informações sobre ameaças cibernéticas; desenvolver capacidades de prevenção, monitoramento e respostas diante de incidentes cibernéticos; proteger a infraestrutura crítica de informações com uma abordagem integral; promover a conscientização pública sobre a importância da segurança cibernética; estabelecer programas de treinamento técnico em segurança cibernética; incentivar a pesquisa e o desenvolvimento de soluções tecnológicas avançadas; participar ativamente de fóruns internacionais relacionados à segurança cibernética.

A E-Ciber tinha um horizonte de validade que se estendia até 2023. Em junho de 2023, já sob outra gestão, foi anunciada a extensão da vigência da estratégia até 2024[3]. Uma nova política, que entrará em vigor posteriormente, já está sendo elaborada.

---

(2) Disponível em: 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 junho de 2023. Disponível em: https://convergenciadigital.com.br/seguranca/governo-prorroga-por-um-ano-a-estratgia-nacional-de-segurana-ciberntica/

2.3. Chile: *PNCS 2023-2028*

A primeira Política Nacional de Segurança Cibernética (PNCS, na sigla em espanhol) foi implementada entre 2017 e 2022, lançando as bases para um ciberespaço mais seguro. Posteriormente, em 4 de dezembro de 2023, foi publicado no Diário Oficial da União o novo PNCS para o período 2023-2028[4]. O Comitê Interministerial de Segurança Cibernética (CICS, na sigla em espanhol) tem sido o órgão responsável pelo desenvolvimento e coordenação dessas políticas, assegurando a colaboração entre diversas entidades governamentais e privadas, bem como os processos de audiências e consultas públicas prévias à conclusão de cada PNCS.

A PNCS 2023-2028 mantém cinco objetivos fundamentais já presentes em sua antecessora: infraestrutura resiliente; direitos das pessoas; cultura de segurança cibernética; coordenação nacional e internacional; promoção da indústria e da investigação científica. Além disso, incorpora quatro objetivos transversais: abordagem de direitos humanos; perspectiva de gênero; desenvolvimento sustentável; cooperação internacional.

Em um avanço significativo para as PNCS, a Lei Marco sobre Segurança Cibernética e Infraestrutura Crítica da Informação foi promulgada em março de 2024, criando a Agência Nacional de Segurança Cibernética (ANCI, na sigla em espanhol). Esse órgão é responsável por regular, supervisionar e sancionar todos os organismos públicos e privados que prestam serviços essenciais, fortalecendo as instituições de segurança cibernética no Chile.

Embora a PNCS 2023-2028 estabeleça diretrizes claras, o plano de ação detalhado que especifica as medidas e os prazos para atingir os objetivos propostos ainda não foi publicado. Espera-se que esse documento suplementar seja lançado em breve para orientar a implementação efetiva da política.

2.4. Colômbia: *Políticas de Confiança e Segurança Digital*

Em 2016, o país adotou a Política Nacional de Segurança Digital por meio do documento CONPES 3854, estabelecendo as bases para um ambiente digital mais seguro e confiável. Posteriormente, em 2020, foi publicada a Política Nacional de Confiança e Segurança Digital (CONPES 3995)[5], cujos objetivos são: fortalecer as capacidades de segurança digital da população, do setor público e do setor privado do país; atualizar a estrutura de governança da segurança digital para aumentar seu nível de desenvolvimento; analisar a adoção de modelos, padrões e marcos em segurança digital, com ênfase em novas tecnologias.

Em consonância com esses esforços, o governo colombiano propôs a criação da Agência Nacional de Segurança Digital e Assuntos Espaciais, uma entidade técnica e especializada que terá como objetivo planejar, articular e gerenciar os riscos de segurança digital no país, bem como fortalecer a confiança e segurança no mundo digital. Tal projeto de lei foi submetido ao Congresso em julho de 2023 e avançou em seu processo legislativo, sendo aprovado em primeira sessão em novembro do mesmo ano. A Agência será responsável por coordenar ações na área de segurança cibernética, incluindo a proteção de infraestruturas

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

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

críticas de informação, a resposta a incidentes cibernéticos e a promoção de uma cultura de segurança digital na sociedade colombiana.

Todos esses são esforços parte de uma estratégia de nível político para potencializar as capacidades de segurança cibernética da Colômbia[6], que, além da criação da Agência, inclui o fortalecimento do Centro Colombiano de Resposta a Incidentes Cibernéticos (ColCERT), a criação de um centro de segurança cibernética em Caldas, e a melhoria da formação e capacitação de especialidades em segurança cibernética.

2.5. Costa Rica: *Estratégia Nacional de Segurança Cibernética 2023-2027*

Em 2017, a Costa Rica implementou sua primeira Estratégia Nacional de Segurança Cibernética, estabelecendo uma estrutura para proteger sua infraestrutura crítica e promover uma cultura de segurança digital. Entretanto, dado o aumento das ameaças cibernéticas e a evolução tecnológica, foi reconhecida a necessidade de sua atualização. Em novembro de 2023, o Ministério da Ciência, Inovação, Tecnologia e Telecomunicações (MICITT, na sigla em espanhol) apresentou a nova Estratégia Nacional de Segurança Cibernética 2023-2027[7], com o objetivo de fortalecer a resiliência do país contra ameaças cibernéticas e garantir um ambiente digital seguro para a população.

A Estratégia Nacional de Segurança Cibernética 2023-2027 se articula em torno de cinco pilares fundamentais: governança e coordenação; marcos legais e normativas; proteção de infraestruturas e resiliência cibernética; educação, treinamento e conscientização; cooperação e alianças. Esses pilares procuram estabelecer um quadro de atuação abrangente que permita prevenir e mitigar riscos e ameaças no ambiente digital, fomentar a inovação e o desenvolvimento de soluções de segurança cibernética, reforçar a capacidade de resposta a incidentes e promover uma sólida cultura de segurança na sociedade costarriquenha.

Em termos de organização, o MICITT lidera a implementação da estratégia em coordenação com o Centro de Resposta a Incidentes de Segurança Informática (CSIRT-CR), que opera um componente essencial dessa estratégia, como ente encarregado de coordenar a segurança cibernética e de informação no país. A estratégia incorpora a participação ativa de instituições públicas, empresas privadas, sociedade civil e academia, garantindo uma abordagem multissetorial para o fortalecimento da segurança cibernética no país.

2.6. Equador: *ENC*

No dia 3 de agosto de 2022, o país apresentou sua primeira Estratégia Nacional de Segurança Cibernética (ENC, na sigla em espanhol), elaborada pelo Ministério das Telecomunicações e Sociedade da Informação (MINTEL, na sigla em espanhol). Essa estratégia visa proporcionar aos cidadãos um acesso mais seguro aos serviços digitais e fortalecer a proteção dos seus dados pessoais, num contexto de implementação recente da sua primeira lei nacional integral sobre esta última matéria.

---

(6) "Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad", MINTIC, 19 jul. 2023. Disponível em: 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) Disponível em: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

A ENC está estruturada em seis eixos de ação: governança e coordenação nacional; resiliência cibernética; combate ao crime cibernético; defesa cibernética nacional e inteligência cibernética; habilidades e capacidades de segurança cibernética; cooperação internacional.

A implementação da ENC envolve a participação ativa de diversas instituições públicas e privadas, bem como a colaboração com organizações internacionais especializadas em segurança cibernética. O MINTEL lidera a coordenação dessas ações, trabalhando em conjunto com entidades como o Comitê Nacional de Segurança Cibernética para garantir uma abordagem integral e eficaz à proteção do ciberespaço equatoriano.

2.7. Guatemala: *Estratégia Nacional de Segurança Cibernética*

A Guatemala publicou sua Estratégia Nacional de Segurança Cibernética em 20 de junho de 2018[8], a qual foi elaborada pelo Ministério de Governação em colaboração com vários atores nacionais e internacionais. O processo de elaboração incluiu consultas e validações com mais de 160 representantes de diferentes setores da sociedade guatemalteca, buscando fortalecer a segurança no ciberespaço e proteger os dados pessoais dos cidadãos.

A estratégia se articula em torno dos seguintes eixos fundamentais: fortalecimento de capacidades; proteção de infraestrutura crítica; marco legal e regulatório; conscientização e educação; cooperação internacional. Inclui também planos de ação específicos com medidas concretas, embora não detalhe seu número total.

A implementação da estratégia enfrentou desafios, principalmente devido à ausência de um arcabouço legal específico que respalde as ações propostas. Apesar disso, esforços têm sido empreendidos para formar o Comitê Nacional de Segurança Cibernética, responsável por coordenar e monitorar políticas nessa área. A validade da estratégia está sujeita a revisões periódicas para adaptação às novas ameaças e avanços tecnológicos no campo digital.

2.8. México: *ENCS*

O México publicou sua Estratégia Nacional de Segurança Cibernética (ENCS, na sigla em espanhol) em novembro de 2017, desenvolvida em colaboração com a Organização dos Estados Americanos (OEA)[9]. O processo de desenvolvimento da ENCS, denominado "Rumo a uma Estratégia Nacional de Segurança Cibernética", ocorreu de março a outubro de 2017 e promoveu espaços de diálogo, discussão e aprendizagem por meio de fóruns e oficinas que envolveram diversos atores da sociedade mexicana.

A ENCS estabelece cinco objetivos estratégicos: proteger a sociedade e seus direitos; preservar a prosperidade econômica do país; manter a ordem pública, a paz e a segurança nacional; fortalecer a cooperação internacional e promover um governo digital confiável. Além disso, baseia-se em princípios orientadores como a perspectiva dos direitos humanos, uma abordagem baseada na gestão de riscos e colaboração multidisciplinar e de diferentes atores.

Desde sua publicação, a implementação da ENCS enfrentou desafios, incluindo a necessidade de harmonizar esforços entre diversas instituições e setores. Apesar desses

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

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

desafios, houve progresso na promoção de uma cultura de segurança cibernética e no treinamento de pessoal especializado. A vigência da estratégia está sujeita a revisões periódicas para se adaptar à constante evolução do ambiente digital e às novas ameaças cibernéticas.

2.9. Nicarágua: *Estratégia Nacional de Segurança Cibernética 2020-2025*

A Nicarágua aprovou sua Estratégia Nacional de Segurança Cibernética 2020-2025 por meio do Decreto Presidencial nº 24-2020, publicado em 29 de setembro de 2020[10]. Essa estratégia foi desenvolvida pelo Instituto Nicaraguense de Telecomunicações e Serviços Postais (TELCOR, na sigla em espanhol) e pelo Ministério das Relações Exteriores, com o objetivo de garantir o uso soberano, seguro e confiável do ciberespaço no país.

A estratégia se fundamenta em quatro princípios orientadores: garantir a soberania e proteger os direitos da população no ciberespaço; gestão de riscos e capacidade de resiliência; proteção e defesa do ciberespaço; e cooperação internacional. Além disso, está estruturada a partir de cinco objetivos estratégicos: fortalecer a governança da segurança cibernética; proteger infraestruturas críticas de informação; desenvolver capacidades nacionais de segurança cibernética; promover uma cultura de segurança cibernética na sociedade; fomentar a cooperação internacional em segurança cibernética.

A implementação da estratégia está prevista para o período 2020-2025, com avaliações periódicas para adaptá-la às necessidades do país e às ameaças emergentes no ambiente digital. No entanto, sua aplicação tem levantado preocupações entre organizações de direitos humanos e setores da sociedade civil, que temem que ela possa ser usada para restringir a liberdade de expressão e aumentar o controle governamental sobre o ciberespaço, como ocorreu em relação à polêmica Lei de Delitos Cibernéticos no país.

2.10. Panamá: *Estratégia Nacional de Segurança Cibernética 2021-2024*

O Panamá publicou sua Estratégia Nacional de Segurança Cibernética 2021-2024 em 15 de dezembro de 2021, por meio da Resolução nº 17 da Autoridade Nacional para Inovação Governamental (AIG, na sigla em espanhol)[11]. Essa estratégia atualiza a Estratégia Nacional de Segurança Cibernética de 2013, refletindo a evolução das tecnologias da informação e comunicação, e a necessidade de fortalecer a segurança no ciberespaço panamenho.

A estratégia é estruturada em torno de quatro pilares fundamentais: proteger a privacidade e os direitos fundamentais das pessoas no ciberespaço; dissuadir e punir comportamentos criminosos no ciberespaço; fortalecer a segurança e a resiliência da infraestrutura crítica do país; promover uma cultura nacional de segurança cibernética.

Para a implementar da estratégia, a AIG coordenou workshops e campanhas de conscientização, como "Panamá Cibersegurança", com o objetivo de promover uma cultura social de segurança cibernética. Além disso, o papel do CSIRT Panamá como equipe nacional para resposta a incidentes de segurança da informação foi fortalecido,

(10) Disponível em: https://legislacion.asamblea.gob.ni/indice.nsf/c3639d8c1d72577006256fe800533609/e9e4a6071fa07177062585b9005fd3db

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

sendo responsável por prevenir, identificar e resolver ataques cibernéticos que afetam a infraestrutura crítica do país. A estratégia vigorará até 2024, com avaliações periódicas para adaptação a novas ameaças e avanços tecnológicos.

2.11. Paraguai: *Plano Nacional de Segurança Cibernética*

O Paraguai adotou seu Plano Nacional de Segurança Cibernética em 2017, a partir da aprovação do Decreto nº 7052/17[12]. Esse plano foi desenvolvido sob a liderança da Presidência da República, por meio da então Secretaria Nacional de Tecnologias da Informação e Comunicação (SENATICs, na sigla em espanhol), em coordenação com o Ministério das Relações Exteriores (MRE) e com o apoio da OEA. O processo de elaboração envolveu vários setores, incluindo o setor privado e a sociedade civil, com o objetivo de estabelecer políticas públicas que fortaleçam a segurança de ativos críticos e promovam um ciberespaço seguro e resiliente.

O plano está estruturado em várias linhas de ação: sensibilização e cultura; pesquisa, desenvolvimento e inovação; proteção de infraestruturas críticas; capacidade de resposta a incidentes cibernéticos; capacidade de investigação e busca; coordenação nacional. Além disso, define objetivos específicos e um plano de ação para a implementação da política nacional de segurança cibernética, com a participação de entidades governamentais, setor privado, academia e sociedade civil.

Em 2024, o Ministério das Tecnologias de Informação e Comunicação (MITIC, na sigla em espanhol), através da Direção-Geral de Segurança Cibernética e Proteção de Informação (DGCPI, na sigla em espanhol) e do CERT-PY, iniciou o processo de atualização da estratégia nacional para o período 2024-2028, novamente com a apoio da OEA. Esse processo inclui mesas de diálogo e trabalho com os principais atores do ecossistema nacional de segurança cibernética, buscando consolidar uma política pública atualizada que responda aos desafios emergentes no campo digital.

2.12. República Dominicana: *Estratégia Nacional de Segurança Cibernética 2030*

A República Dominicana aprovou sua Estratégia Nacional de Segurança Cibernética 2030 por meio do Decreto nº 313-22, de 14 de junho de 2022[13], com horizonte de vigência até 31 de dezembro de 2030. Essa estratégia visa fortalecer o marco nacional de segurança cibernética, fomentando a criação de ambientes seguros, confiáveis e resilientes que promovam uma sociedade digital inclusiva e que respeite os direitos fundamentais.

A estratégia é estruturada em torno de vários eixos principais: fortalecimento do marco regulatório; desenvolvimento de capacidades e habilidades em segurança cibernética; proteção de infraestruturas críticas de informação; gestão de riscos e resposta a incidentes cibernéticos; conscientização e cultura de segurança cibernética e cooperação nacional e internacional.

Para sua implementação, foi criado um Conselho Diretor presidido pelo Ministério da Presidência, que coordena as ações do Centro Nacional de Segurança Cibernética (CNCS,

(12) Disponível em: https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

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

na sigla em espanhol). O CNCS é responsável por executar as políticas e planos derivados da estratégia, incluindo a operação do CSIRT-RD, a equipe nacional de resposta a incidentes cibernéticos. A estratégia prevê avaliações periódicas para adaptação a novas ameaças e avanços tecnológicos, garantindo a proteção do ciberespaço dominicano e a confiança digital de seus cidadãos e cidadãs.

3. OS PROCESSOS DE FORMULAÇÃO DE ESTRATÉGIAS EM CURSO

Os demais países da região não têm estratégias ou políticas nacionais sobre segurança cibernética, embora em muitos casos tenham medidas aplicáveis a nível federal ou regulações relacionadas. Em vários desses casos, estratégias ou políticas nacionais foram anunciadas ou estão em elaboração.

Embora El Salvador ainda não tenha um texto definitivo, sua Estratégia Nacional de Segurança Cibernética está sendo desenvolvida para fortalecer a proteção da informação digital e da infraestrutura crítica do Estado, como um compromisso com a Agenda Digital 2020-2030[14]. Porém, em 2024 o país aprovou a Lei de Segurança Cibernética e da Informação, que estabelece princípios, um marco legal e diretrizes para estruturar, regular, auditar e fiscalizar medidas de segurança cibernética em instituições públicas. Essa lei obriga a implementação de sistemas de gestão da segurança cibernética, a elaboração de estratégias de segurança informática e a manutenção de registros atualizados das ações executadas na área.

Honduras também não tem uma estratégia nacional ou CSIRT, o que limita sua capacidade de enfrentar incidentes cibernéticos e proteger sua infraestrutura digital. O Plano de Governo Digital de Honduras 2023-2026[15] inclui a criação de uma Estratégia e Plano de Ação Nacional de Segurança Cibernética, bem como a criação de uma equipe para incidentes cibernéticos.

O Peru tem um documento de trabalho intitulado Estratégia Nacional de Segurança e Confiança Digital 2021-2026, elaborado pela Secretaria de Governo Digital da Presidência do Conselho de Ministros (PCM, na sigla em espanhol)[16]. O documento propõe uma estrutura abrangente para fortalecer a segurança cibernética e promover a confiança no ambiente digital, articulada em torno de eixos como cultura de segurança; desenvolvimento de capacidades; proteção de ativos críticos, padrões, serviços digitais e estrutura legal. Entretanto, o documento não foi adotado como política oficial.

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

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

(16) Referência da página da Secretaria de Governo e Transformação Digital. Disponível em: https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital

O Uruguai está desenvolvendo sua Estratégia Nacional de Segurança Cibernética 2024-2030, liderada pela Agência de Governo Eletrônico e Sociedade da Informação e do Conhecimento (Agesic, na sigla em espanhol)[17]. A estratégia é estruturada em torno de seis pilares: governança e regulação; proteção de infraestrutura crítica; capacidades técnicas e humanas; educação e conscientização; gestão de riscos; e cooperação nacional e internacional. Sua elaboração inclui consultas públicas e oficinas multissetoriais, integrando as perspectivas dos principais atores para projetar uma estrutura abrangente de segurança cibernética. Esse esforço complementa a recente entrada em vigor da Lei 20.327, que estabelece disposições para prevenir e punir crimes informáticos. No momento do encerramento deste relatório, não havia uma versão final da Estratégia.

A Venezuela tomou medidas para consolidar uma Estratégia Nacional de Segurança Cibernética, embora não possua um documento formalizado. Em agosto de 2024, o governo criou o Conselho Nacional de Segurança Cibernética por meio do Decreto nº 42.939, com o objetivo de coordenar as políticas nessa área, assessorar o Poder Executivo e propor regulações específicas[18]. O ciberespaço foi declarado de interesse público e estratégico, o que enfatiza a necessidade de medidas para proteger infraestruturas críticas e garantir a soberania digital. Apesar da ausência de uma estratégia integrada, o país conta com um Sistema Nacional de Segurança de Informática, sob a supervisão da Superintendência de Serviços de Certificação Eletrônica (SUSCERTE, na sigla em espanhol), que busca estabelecer padrões e condições para o uso seguro das tecnologias da informação e comunicação.

4. ANÁLISE

O cenário da segurança cibernética na América Latina reflete uma diversidade de abordagens e níveis de maturidade na implementação de estratégias nacionais. Países como Argentina e Brasil avançaram na formalização de políticas que buscam fortalecer a resiliência contra ameaças cibernéticas, enquanto nações como Honduras e Peru ainda não consolidaram marcos estratégicos oficiais, o que pode limitar sua capacidade de resposta a incidentes digitais.

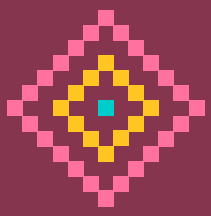
A influência de organizações internacionais, especialmente a Organização dos Estados Americanos, tem sido decisiva no fornecimento de assessoria e apoio técnico para a elaboração dessas estratégias. Seu acompanhamento permitiu que diversos países estruturassem planos alinhados aos padrões globais, além de receberem suporte técnico quanto aos objetivos e medidas propostas. Mais importante ainda, esse acompanhamento nos permite considerar que, apesar da dispersão de órgãos e instrumentos, seus conteúdos podem estar promovendo uma visão regional coerente sobre segurança cibernética.

(17) "Cocreación de la Estrategia Nacional de Ciberseguridad", Agesic, 10 de setembro 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. Disponível em: http://mippci.gob.ve/index.php/2024/08/20/gaceta-oficial-creado-consejo-nacional-de-ciberseguridad/

A implementação efetiva dessas políticas enfrenta desafios significativos. A falta de recursos especializados, tanto humanos quanto tecnológicos, e a ausência de estruturas legais robustas dificultam a implementação de medidas específicas. Além disso, a rápida evolução das tecnologias e táticas empregadas por agentes maliciosos exige atualização e adaptação constantes das estratégias nacionais.

É fundamental que os países da região fortaleçam a cooperação internacional e regional, compartilhando experiências e boas práticas para enfrentar ameaças comuns. Assim, integrar a segurança cibernética às agendas nacionais de desenvolvimento e promover uma cultura de segurança digital entre os cidadãos são aspectos essenciais para construir um ambiente digital mais seguro e resiliente na América Latina.



www.derechosdigitales.org