www.cybersecurityobservatory.org

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

Relatório de Cibersegurança

2020

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

www.cybersecurityobservatory.org

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

Relatório de Cibersegurança 2020

Copyright © 2020 Banco Interamericano de Desenvolvimento

Esta obra está licenciada sob uma licença Creative Commons IGO 3.0 Attribution-NonCommercial-NoDerivatives (CC-IGO BY-NC- ND 3.0 IGO) (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) e pode ser reproduzida para qualquer finalidade não comercial com crédito ao BID. É vedada a criação de obras derivadas.

Qualquer controvérsia relacionada ao uso das obras do BID que não possa ser solucionada amigavelmente será submetida a arbitragem de acordo com as regras da UNCITRAL. O uso do nome do BID e do logotipo do BID para qualquer finalidade que não seja para crédito ficará sujeito a um contrato de licença por escrito separado entre o BID e o usuário e não está autorizado como parte desta licença CC-IGO.

Observe que o link fornecido acima inclui termos e condições adicionais da licença.

As opiniões expressas nesta publicação são de responsabilidade dos autores e não necessariamente refletem as opiniões do Banco Interamericano de Desenvolvimento, de sua Diretoria ou dos países que representam, e tampouco da Organização dos Estados Americanos ou dos países que a compõem.

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Banco Interamericano de Desenvolvimento (BID)

Presidente

Luis Alberto Moreno

Coordenação do projeto

Miguel Porrúa

Equipe técnica

Ariel Nowersztern

Darío Kagelmacher

Santiago Paz

Pablo Libedinsky

Florencia Cabral

Benjamin Roseth

Organização dos Estados Americanos (OEA)

Secretário-Geral

Luis Almagro

Coordenação do projeto

Belisario Contreras

Equipe técnica

Kerry-Ann Barrett

Rolando Ramírez

Mariana Cardona Clavijo

Manuela Orozco Jaramillo

Nathalia Foditsch

Barbara Marchiori

Centro Global de Capacidade de Segurança Cibernética da Universidade de Oxford

Professor Sadie Creese

Professor Michael Goldsmith

Carolin Weisser Harris

Jakob Bund

Andraz Kastelic

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

ÍNDICE

9 Mensagens institucionais

10 Mensagem do Gerente do Setor de Instituições para o Desenvolvimento do BID
12 Mensagem da Secretária de Segurança Multidimensional da OEA

15 O que mudou desde o relatório de 2016?

19 Percepção dos especialistas

20 Tendências regionais na prontidão para a segurança cibernética, 2016–2020
/ Universidade de Oxford
24 A abordagem abrangente da UE para o enfrentamento das ameaças do ciberespaço
/ Serviço Europeu para a Ação Externa
28 Novas ameaças em segurança cibernética: implicações para a América Latina e o Caribe
/ Fórum Econômico Mundial
34 A necessidade de uma resposta harmonizada às ameaças cibernéticas: um roteiro
/ República da Estônia
38 Desenvolvendo Capacidades de Cibersegurança: desafios para a educação pós-ensino médio na América Latina e Caribe
/ Universidad de Chile

41 O modelo de maturidade da capacidade de cibersegurança

45 Perfis de países

46 Antígua e Barbuda
50 Argentina
54 Bahamas, Comunidade das
58 Barbados
62 Belize
66 Bolívia
70 Brasil
76 Chile
82 Colômbia
86 Costa Rica
90 Dominica
94 Equador
98 El Salvador
102 Granada
106 Guatemala
110 Guiana
114 Haiti
118 Honduras
122 Jamaica
126 México
130 Nicarágua
134 Panamá
138 Paraguai
144 Peru
148 República Dominicana
152 Santa Lúcia
156 São Cristóvão e Névis
160 São Vicente e Granadinas
164 Suriname
168 Trinidad e Tobago
172 Uruguai
176 Venezuela

181 Apêndice

182 Relação de CSIRTs
186 Países dotados ou em fase de elaboração de uma estratégia nacional de cibersegurança
187 Membros e observadores da Convenção de Budapeste
188 Acrônimos
191 Referências

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Mensagens institucionais

Mensagem de

Moisés J. Schwartz

Gerente do Setor de Instituições para o Desenvolvimento do BID

BID
Melhorando vidas

A crise desencadeada pela pandemia da Covid-19 no início de 2020 evidenciou nossa dependência de infraestruturas indispensáveis, que muitas vezes é invisível ou, na melhor das hipóteses, quase imperceptível para a maioria dos cidadãos.

Nossos artigos diários de primeira necessidade, como cadeias de suprimento de alimentos, meios de transporte, pagamentos e transações financeiras, atividades educacionais, procedimentos governamentais, serviços de emergência e até mesmo água e energia, figuram entre os muitos elementos essenciais com dependência crescente das tecnologias digitais, o que os deixa cada vez mais suscetíveis a ameaças cibernéticas.

As políticas de cibersegurança são fundamentais para proteger os direitos dos cidadãos no universo digital (inclusive a privacidade e a propriedade), bem como para fortalecer sua confiança na tecnologia digital e naturalidade em seu uso. Os crimes virtuais perfazem cerca de metade dos crimes contra a propriedade em todo o mundo. Em um contexto mais amplo, os números são ainda maiores. Os danos econômicos causados por ataques cibernéticos são estimados em mais de 1% do produto interno bruto (PIB) anual de alguns países, ao passo que alguns ataques à infraestrutura essencial podem provocar danos que podem atingir 6% do PIB anual.

Este estudo mostra que a região da América Latina e Caribe (ALC) não está suficientemente preparada para fazer frente aos ataques cibernéticos. Apenas sete dos 32 países estudados dispõem de um plano de proteção de infraestruturas críticas, enquanto 20 criaram equipes de resposta a incidentes de cibersegurança, as chamadas CERTs ou CSIRTs (do inglês Computer Emergency Response Team e Cybersecurity Incident Response Team, respectivamente). Isso limita sua capacidade de identificar e reagir aos ataques.

A identificação dos perigos no ciberespaço é o primeiro passo. A resposta a esses perigos é, em realidade, um desafio considerável para os países da ALC. Por exemplo, a análise de 22 dos países estudados revelou baixíssima capacidade para investigar os crimes cibernéticos, enquanto também enfrentam grandes dificuldades nos processos penais. Algumas das dificuldades referem-se ao ordenamento jurídico: um terço dos países não possui

um marco legal para tratar os crimes cibernéticos e apenas cinco ratificaram a Convenção de Budapeste, o principal instrumento de cooperação internacional para o enfrentamento dos crimes cibernéticos. A cooperação internacional é o segredo para o sucesso no enfrentamento desses crimes sem fronteiras.

Ainda que os governos da ALC estejam cientes da necessidade de proteger o espaço digital, do qual depende uma parcela tão grande do funcionamento adequado da sociedade, seus esforços para a adoção de políticas de segurança cibernética não avançaram com a urgência necessária. No início de 2020, apenas 12 países haviam aprovado uma estratégia nacional de cibersegurança (o que pode ser considerado uma vitória, considerando que apenas cinco países contavam com uma estratégia em 2016). Ademais, apenas 10 países instituíram uma entidade governamental centralizada para assumir a gestão nacional da segurança cibernética.

Por que os avanços são tão tímidos na região da ALC? Um dos fatores é a falta de capital humano qualificado. Estimativas colocam o déficit de profissionais de segurança cibernética na região em cerca de 600.000 trabalhadores, problema que se agrava ainda mais quando se consideram as disparidades de gênero, pois estima-se que menos de um quarto dos profissionais dessa área da segurança sejam mulheres. Diante dessa escassez, apenas 20 dos países estudados possuem algum programa de formação profissional em cibersegurança.

O Banco Interamericano de Desenvolvimento (BID) está colaborando de perto com os governos da ALC e com organismos multilaterais, como a Organização dos Estados Americanos (OEA), para superar esses desafios. Dado o atual crescimento do setor de segurança cibernética em escala mundial, a criação de políticas nos países da ALC oferece oportunidades econômicas, sobretudo nas condições atuais ocasionadas pela Covid-19 e à medida que a região começa a revitalizar sua economia na esteira da pandemia. A aplicação de políticas coesas de cibersegurança permitirá à região tirar proveito dos benefícios da Quarta Revolução Industrial com vistas a proteger os cidadãos e impulsionar a atividade econômica.

O BID agradece aos governos da Espanha e de Israel por seu apoio técnico e financeiro. Os dois países foram extremamente generosos ao compartilhar seus conhecimentos e experiências. O crime cibernético não respeita fronteiras e, por conseguinte, exige uma resposta global. Convido todos os países da América Latina e do Caribe a se tornarem modelos de cooperação e coordenação internacional em uma área tão relevante para nossa vida quotidiana. O BID assumiu um compromisso com esse objetivo e continuará a apoiar os governos da ALC em seus esforços para proteger os cidadãos das ameaças digitais.

Mensagem de

Farah Diva Urrutia

Secretária de Segurança Multidimensional da OEA

Desde 2004, a OEA vem enfatizando continuamente a segurança cibernética no hemisfério. A Organização se esforça para assegurar um ciberespaço aberto e seguro em todos os seus Estados-membros.

Com a publicação da edição 2020 do relatório "Cibersegurança: Riscos, avanços e o caminho a seguir na América Latina e Caribe", a OEA pretende oferecer uma descrição detalhada da capacidade dos países da América Latina e do Caribe (ALC) para combater o ciberterrorismo e assegurar um acesso mais seguro à Internet na região. Neste ano em particular, a pandemia da Covid-19 evidenciou o papel vital das tecnologias da informação e comunicação (TICs) na prestação de serviços essenciais e sua profunda integração em nossas sociedades.

A pandemia da Covid-19 nos apresenta a oportunidade de refletir sobre os avanços na expansão das TICs, conectividade da Internet e segurança cibernética no hemisfério. O aumento de nossa dependência do espaço digital durante a crise destaca a necessidade de extrair lições do que vem pela frente na transformação contínua de nossas sociedades e economias e na garantia da segurança cibernética no nível global.

Em sentido mais genérico, na última década aumentaram a frequência e a sofisticação dos ataques cibernéticos. O baixo custo e o risco mínimo envolvidos nesses crimes têm sido os principais fatores para seu crescimento. Com o simples uso de um computador com acesso à Internet, os criminosos digitais conseguem causar danos de vulto enquanto permanecem relativamente anônimos.

Cidadãos e instituições estão expostos à incerteza e à natureza imprevisível dos crimes cibernéticos. Dessa forma, é imperativo o enfrentamento dessas ameaças. Os esforços nesse sentido precisam ser de natureza multidimensional, tendo em vista que o desenvolvimento de uma sociedade digital resiliente exige diversos fatores. Políticas e ordenamentos jurídicos precisam ser ajustados, e todas as partes interessadas da sociedade civil, bem como dos setores público e privado, devem necessariamente trabalhar para criar uma cultura de consciência cibernética e formar profissionais qualificados. Logo, a estratégia de segurança cibernética constitui um esforço permanente e complexo.

Elaborado em colaboração com o Banco Interamericano de Desenvolvimento (BID) e o Centro Global de Capacidade em Segurança Cibernética da Universidade de Oxford, o presente relatório analisa a capacidade de segurança cibernética dos Estados-membros da OEA e os incentiva a adotar as normas mais recentes de cibersegurança, sem perder de vista a proteção dos direitos fundamentais de seus povos.

Tal como na edição anterior, o estudo analisa a maturidade cibernética de cada país nas cinco dimensões identificadas no Modelo de maturidade da capacidade de segurança cibernética das nações (CMM, na sigla em inglês): (i) Política e estratégia de cibersegurança; (ii) Cibercultura e sociedade; (iii) Educação, capacitação e competências em cibersegurança; (iv) Marcos legais e regulatórios; e (v) Normas, organizações e tecnologias.

São evidentes os avanços feitos na região, em grande medida com o apoio da OEA. O relatório de 2016, por exemplo, indicou que quatro em cada cinco países careciam de estratégias de segurança cibernética ou de um plano de proteção de infraestruturas críticas. Até o início de 2020, 12 países haviam aprovado estratégias nacionais de cibersegurança, inclusive Colômbia (2011 e 2016), Panamá (2013), Trinidad e Tobago (2013), Jamaica (2015), Paraguai (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) e Brasil (2020), com vários outros com o processo em andamento.

No que diz respeito à coleta e validação de dados realizadas por nossos Estados-membros, o relatório oferece um panorama do universo complexo e instável do espaço digital. Esperamos que este estudo propicie uma perspectiva que nos permita avaliar onde estamos, nos capacite a tomar decisões com base em evidências e melhore nossa compreensão coletiva dos desafios e oportunidades decorrentes da segurança cibernética em nossa região. As informações e análises contidas neste relatório ajudarão todas as partes interessadas — governos, setor privado, academia e sociedade civil — a trabalhar para construir um ciberespaço mais seguro, resiliente e produtivo em nosso hemisfério.

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

O que mudou desde o relatório de 2016?

Miguel Porrúa
Especialista Sênior em Governo Digital, Coordenador do Cluster de Dados e Governo Digital, **BID**

Belisario Contreras
Gerente do Programa de Cibersegurança da **OEA**

Em março de 2016, quando foi lançada a primeira edição do relatório "Cibersegurança: Estamos prontos na América Latina e Caribe?", a intenção do Banco Interamericano de Desenvolvimento (BID) e da Organização dos Estados Americanos (OEA) era fornecer aos países da América Latina e Caribe (ALC) não apenas um panorama da situação da segurança cibernética, mas também orientações sobre as próximas medidas a serem tomadas para fortalecer as capacidades nacionais de cibersegurança. Este foi o primeiro estudo do gênero, apresentando o estado da segurança cibernética com uma visão abrangente e contemplando todos os países da ALC.

Até a publicação do estudo, a região parecia não perceber a magnitude do problema. Enquanto isso, os ataques cibernéticos na região vêm aumentando, tendo como principal alvo as instituições financeiras da ALC. O aumento das atividades digitais gerado pela pandemia da Covid-19 na região expôs ainda mais as vulnerabilidades do seu espaço digital. O relatório sobre crimes cibernéticos ThreatMetrix identificou a América Latina como um foco da fraude na criação de contas, com cerca de 20% do volume total ante a média de 12,2% do setor como um todo.[1] Todos os anos, milhões de novos usuários da ALC se conectam à Internet pela primeira vez, o que, por sua vez, cria um mosaico de novos clientes não tão versados em tecnologia quanto os clientes digitais mais experientes. Essa dinâmica contribui para criar um ambiente de risco ampliado. Portanto, a ALC não apenas é um alvo para ataques dessa natureza, mas também uma fonte considerável deles.

A escalada no número de ataques cibernéticos estimulou um aumento no interesse pela cibersegurança na região. Um exemplo simples é que, entre março de 2016 e junho de 2019 a frequência de buscas da palavra cibersegurança em um dos mecanismos de busca mais populares da internet[2] saltou de 20 para 100.[3] Em outras palavras, a pesquisa pela palavra cibersegurança tornou-se cada vez mais popular entre os usuários da ALC. Coincidentemente, os usuários que pesquisaram o termo cibersegurança na ALC tenderam a pesquisar cursos e oportunidades de capacitação nessa área. Isso significa que mais pessoas na ALC estão cientes da importância da segurança cibernética e buscando formas de aprimorar seus conhecimentos.

Dado o aumento dos ataques cibernéticos, a OEA e o BID consideraram necessário reimplementar o Modelo de Maturidade da Capacidade de Segurança Cibernética das Nações (CMM), para medir o crescimento e desenvolvimento das capacidades de nossos Estados-membros para se defender das crescentes ameaças do espaço digital. Ambas as instituições estão satisfeitas em ver como a segurança cibernética conquistou importância na agenda política da região nos últimos anos, e como governos, cidadãos e empresas demonstram enorme interesse em saber mais sobre o assunto. A disponibilidade de mais profissionais qualificados tornou-se essencial para a criação e implantação das políticas e

medidas de cibersegurança necessárias para assegurar a resiliência dos países em face de ataques cibernéticos de sofisticação e complexidade crescentes. Tanto o BID quanto a OEA estão dando especial atenção a essa necessidade e oferecendo várias oportunidades para que os profissionais da ALC atualizem seus conhecimentos.

Este novo estudo nos concedeu uma visão renovada de nossa posição e das oportunidades que nossa região pode aproveitar. Por exemplo, embora os países da ALC tenham aprimorado suas capacidades de cibersegurança desde 2016, de acordo com o CMM o nível médio de maturidade da região ainda está entre 1 e 2, numa escala onde 1 significa Iniciante e 5 significa Dinâmico ou Avançado. Em outras palavras, a maioria dos países da ALC começou a formular iniciativas de cibersegurança, inclusive medidas de construção de capacidades. O mais importante é que algumas delas já estão em vigor; no entanto, elas estão sendo adotadas de forma pontual, sem coordenação entre as principais partes interessadas. O nível médio de maturidade da cibersegurança dos 32 países não deve ofuscar as conquistas da região nos últimos três anos.

Segundo a análise, o nível de maturidade da cibersegurança da sub-região do Cone Sul foi o maior em todas as cinco dimensões do CMM, com média entre 2 e 3. Ainda que "Marcos legais e regulatórios" tenha sido a dimensão mais desenvolvida, "Normas, organizações e tecnologias" teve a melhoria mais expressiva desde 2016. Vale ressaltar que todas as dimensões apresentam níveis semelhantes de maturidade da segurança cibernética, o que sugere que os países desta região estão adotando uma abordagem abrangente para a cibersegurança. O Uruguai foi avaliado com o nível de maturidade mais alto da região em quatro das cinco dimensões.

O Grupo Andino registrou um nível médio de maturidade em segurança cibernética de 2, o que revela a importância de concentrar os esforços de segurança cibernética para fortalecer a adoção de normas de cibersegurança e controles técnicos na região e para incentivar a divulgação responsável de informações. A Colômbia tem a segurança cibernética mais desenvolvida neste grupo, principalmente nas dimensões "Política e estratégia de cibersegurança" e "Cibercultura e sociedade".

América Central e México apresentaram um nível de maturidade médio de 2 nas dimensões "Cibercultura e Sociedade" e "Educação, capacitação e competências em cibersegurança", enquanto as dimensões "Política e estratégia de cibersegurança" e "Normas, organizações e tecnologias" estão abaixo desse nível. Assim como no Grupo Andino, a América Central e o México devem se concentrar na melhoria da implantação de normas de segurança cibernética e controles técnicos, bem como incentivar o desenvolvimento de um mercado de segurança cibernética. Chama a atenção o nível de maturidade entre 2 e 3 da dimensão "Marcos legais e regulatórios". O México ocupa a melhor posição da região, com nível de maturidade entre 2 e 3 em quase todas as dimensões. Finalmente, a região do Caribe registra nível de maturidade entre 1 e 2 em todas as dimensões. Contudo, embora, como em 2016, "Marcos legais e regulatórios" tenha sido a dimensão mais madura, "Política e Estratégia de Cibersegurança" foi a dimensão menos madura. A criação de uma estratégia nacional de cibersegurança proporciona aos países uma abordagem mais estratégica e abrangente para a solução e melhor compreensão dos desafios da segurança cibernética. Do mesmo modo, esse planejamento estratégico permite priorizar os objetivos e os investimentos em segurança cibernética. Cabe salientar que dois dos países com maior desenvolvimento em segurança cibernética na região, Trinidad e Tobago e Jamaica, possuem uma estratégia nacional nessa área.

Os grandes desafios da cibersegurança, como os da própria Internet, são de natureza global. Portanto, é inegável que os países da ALC precisam continuar promovendo maior cooperação mútua, mobilizando todos os atores relevantes, bem como instituindo um mecanismo de monitoramento, análise e avaliação de impactos no que se refere à cibersegurança em âmbito nacional e regional. Mais dados relativos à segurança cibernética permitiriam a introdução de uma cultura de gestão dos riscos cibernéticos, que precisa ser ampliada tanto no setor público quanto no privado.

Os países precisam estar preparados para se adaptar com rapidez ao ambiente dinâmico em que vivemos e tomar decisões com base em um mundo de ameaças em constante mutação. Para poder gerir esses riscos, nossos Estados-membros devem compreender o impacto e a probabilidade das ameaças cibernéticas a seus cidadãos, organizações e infraestruturas críticas nacionais. A passagem para o próximo nível de maturidade exigirá uma política de segurança cibernética abrangente e sustentável, respaldada pela agenda política nacional, com destinação de recursos financeiros e capital humano qualificado para sua execução.

A pandemia da Covid-19 vai passar, mas os eventos que exigirão o uso intensivo de tecnologias digitais para que o mundo possa seguir adiante continuarão a acontecer. Dessa forma, o desafio de proteger nosso espaço digital continuará a aumentar. O BID e a OEA têm a esperança de que esta edição do relatório ajude os países da ALC a entender melhor o estado atual de suas capacidades de segurança cibernética e seja útil para formulação de iniciativas políticas que permitam elevar seu nível de resiliência cibernética.

Percepção dos especialistas

Tendências regionais na prontidão para a cibersegurança, 2016–2020

Sadie Creese
Diretora do
Centro Global de Capacidade de Segurança Cibernética da Universidade de Oxford

Em 2015, a Organização dos Estados Americanos (OEA) foi a primeira organização do mundo a embarcar em um estudo amplo e profundo das capacidades de segurança cibernética de toda uma região, avaliando os desenvolvimentos na América Latina e Caribe.

Nesse contexto, a segunda rodada de avaliações de segurança cibernética apresentada neste relatório oferece uma perspectiva longitudinal dos avanços detalhados da capacidade de cibersegurança em toda a região, oferecendo uma oportunidade para que os governos façam um balanço sistemático de seus avanços à luz dos acontecimentos nas nações vizinhas. Essas percepções também podem ajudar os governos a otimizar seus esforços de acordo com os marcos identificados no nível estratégico, nas estratégias nacionais de segurança cibernética, nos planos de ação relacionados ou em outros programas de construção de capacidades em segurança cibernética. Ademais, esses dados fornecerão para os atores que fornecem recursos para a construção de capacidades outras percepções sobre o impacto que seus investimentos tiveram até o momento, o que permitirá a eles, e também a profissionais, pesquisadores, organismos internacionais e governos, identificar sucessos e melhores práticas em construção de capacidades. Não menos importante, esses dados longitudinais também facilitam a compreensão do valor das avaliações de capacidade na orientação das prioridades de políticas e investimentos.

O Modelo de Maturidade da Capacidade de Segurança Cibernética das nações (CMM), que serviu de base para os estudos regionais da OEA e do Banco Interamericano de Desenvolvimento (BID) em 2016 e 2020, adota uma metodologia abrangente que avalia a capacidade em cinco dimensões: Política e estratégia de cibersegurança; Cibercultura e sociedade; Educação, capacitação e competências em cibersegurança; Marcos legais e regulatórios; e Organizações e tecnologias. Para medir de forma confiável a capacidade de segurança cibernética, cada dimensão é subdividida em fatores, aspectos e indicadores, com cada nível avaliando a capacidade com granularidade progressiva.

O CMM foi desenvolvido pelo Centro Global de Capacidade de Segurança Cibernética (GCSCC) em 2013.

Para assegurar a atualização permanente do CMM e a existência de uma ferramenta poderosa que registre desenvolvimentos importantes, o modelo passa por revisões periódicas. Diante da evolução das necessidades de capacidade, torna-se necessário refletir esse progresso no modelo de modo a capturar os avanços de forma adequada e oferecer percepções sobre as possíveis próximas etapas para novas melhorias. Nesse sentido, o próprio modelo foi atualizado em fevereiro de 2017, em sintonia com os desafios de segurança dinâmicos e com base na experiência de implantação do modelo na prática.

Esta versão revista do modelo, usada no estudo de 2020, incorpora uma série de novos aspectos para análise, como o Modo de operação da capacidade de resposta a incidentes, Entendimento do usuário sobre a proteção de informações pessoais na Internet, Mecanismos de denúncia, Denúncia de incidentes cibernéticos pela mídia e redes sociais, Legislação de proteção de dados, Proteção das crianças na Internet, Legislação de proteção do consumidor, Legislação de propriedade intelectual; Cooperação formal e informal em questões de crimes cibernéticos, Qualidade de software, Controles técnicos de segurança e Controles criptográficos.

O presente estudo não apenas contribui com dados significativos para a comunidade internacional de segurança cibernética, mas também mostra o valor das avaliações de capacidade para orientar a estratégia, política e destinação de recursos nacionais e para a solução de dilemas de investimento em áreas de capacitação. Entre 2016 e 2020 (o período entre os dois estudos), em toda a América Latina e Caribe foram feitos avanços perceptíveis em todos os aspectos abrangidos pelo Modelo, como demonstra o aumento das pontuações de maturidade da capacidade. Os dados longitudinais dos dois estudos sugerem várias tendências e indicações de sinergia em diversos aspectos dos esforços de construção de capacidades.

Aspectos atinentes à dimensão Política e estratégia de cibersegurança avançaram mais do que aqueles de qualquer outra dimensão, indicando que uma abordagem estratégica sistemática da capacidade de segurança cibernética é reconhecida como algo importante. Além disso, os países que realizaram melhorias no conteúdo ou nos processos de desenvolvimento de sua estratégia nacional de cibersegurança constataram maiores avanços de forma generalizada, o que constitui um indicativo de que investir em uma abordagem estratégica gera resultados positivos para a segurança cibernética. Desde 2015, o número de países da região que adotaram uma estratégia nacional de cibersegurança (ENC) mais que dobrou. A Colômbia, que liderou os esforços nessa área ao desenvolver a primeira ENC na região, em 2011, está atualmente implementando a segunda iteração de sua ENC.

Melhorias significativas também foram registradas na promoção de uma mentalidade de segurança cibernética no âmbito dos governos e entre os usuários de internet. Embora não façam parte de uma campanha exclusiva de conscientização, consultas às diversas partes interessadas, realizadas para apoiar o desenvolvimento de estratégias nacionais de cibersegurança, promoveram a conscientização entre as organizações participantes acerca de suas respectivas atividades, responsabilidades e capacidades. Por sua vez, essa conscientização pode ser transmitida a outras pessoas e ajudar a desenvolver e manter capacidades nessa área. Avanços na organização e no conteúdo das estratégias se refletem em maior atenção às questões de segurança da tecnologia da informação e comunicação (TIC) por parte dos representantes do governo. No entanto, os dados sugerem que os dois grupos — servidores públicos e usuários de internet em geral — ainda estão atrás do setor privado e que a sensibilização dos usuários em geral para as questões de segurança como um todo continua comparativamente baixa. Nesse sentido, vale lembrar que o desenvolvimento da capacidade de segurança cibernética de um país continua sendo um esforço contínuo e de toda a nação, que, por definição, somente pode ter sucesso se contar com uma abordagem inclusiva que incorpore grupos vulneráveis de toda a sociedade.

É importante destacar que os usuários de países com legislação mais avançada e específica também declararam níveis mais elevados de confiança e segurança no uso da Internet, o que pode ser reflexo

de uma percepção de aumento na segurança que as leis específicas de segurança das TICs, legislação de proteção de dados e do consumidor e proteção das crianças na Internet (introduzidas como novas medidas no CMM revisto) trazem para a experiência dos internautas.

As pontuações de maturidade da Legislação substantiva sobre crimes cibernéticos praticamente se estabilizaram no período 2016–2020, possivelmente porque esse aspecto já conta com a pontuação média mais alta em toda a região. Esse avanço na legislação substantiva tem sido cada vez mais complementado por avanços na legislação processual de crimes cibernéticos, aspecto legal de maior atividade desde 2015. Ainda assim, a legislação substantiva registrará novos aumentos de capacidade em termos reais, uma vez que a aplicação é altamente dependente de disposições processuais.

A única exceção a esse progresso pronunciado na capacidade se deu nas avaliações da Coordenação de defesa cibernética. Contudo, essa coordenação também é uma questão delicada fora do continente americano. Mais do que em outros aspectos, acreditamos que as avaliações dos esforços de coordenação de defesa cibernética são limitadas pela sensibilidade das informações envolvidas e possível relutância em compartilhar dados importantes, fatores que também podem representar um impedimento para a coordenação em si.

Outras pesquisas comparativas sobre os dados longitudinais podem ajudar a entender melhor se avanços em áreas até então subpriorizadas poderiam catalisar avanços em outras áreas e, portanto, devem passar a ter prioridade. Todos os aspectos de Educação, capacitação e competências em cibersegurança, por exemplo, estão na metade inferior em termos de avanços. A escassez de mão de obra qualificada em segurança cibernética é um desafio quase universal. Ainda assim, sem custeio adequado para a formação e educação profissional, esse desequilíbrio entre oferta e demanda acarreta o risco de vir a limitar as conquistas de maturidade. A falta de uma base de competências para a sustentação da segurança cibernética também pode surtir efeitos negativos em cascata sobre os esforços de construção de capacidades em outras áreas. Essas considerações ressaltam a necessidade de conciliar investimentos em ganhos de maturidade no curto prazo para enfrentar ameaças de segurança imediatas, com planos de longo prazo para estimular competências e formação que deem contribuições substanciais e autossustentáveis para a cibersegurança nacional.

Divulgação responsável de informações foi o aspecto com o menor índice de maturidade na região. A abrangência e abordagem integrada do CMM possibilita uma maior contextualização das pontuações de cada aspecto. Nesse sentido, os riscos relacionados à ausência de um mecanismo institucionalizado de compartilhamento de informações sobre as vulnerabilidades detectadas e políticas sobre hackeamento ético podem ser agravados pelas pontuações igualmente baixas de capacidades de resposta interna, inclusive Organização da proteção de infraestruturas críticas, Gerenciamento de crises, Gerenciamento e resposta a riscos e Seguro contra crimes cibernéticos, que figuram na parte inferior e registraram poucas melhorias desde 2015.

Um objetivo importante de qualquer avaliação de CMM é identificar medidas que deram certo, mas também identificar as lacunas. A esse respeito, a OEA e todos os países participantes da região merecem reconhecimento por produzirem esse referencial atualizado e traçar um caminho que outras regiões podem seguir para ampliar a conscientização mais fundamentada de seus níveis de capacidade.

Além dos compromissos com o desenvolvimento da capacidade de segurança cibernética no nível nacional, a América Latina e o Caribe têm promovido iniciativas regionais vibrantes. Por exemplo, em 2016 foi lançado o CSIRT Américas, plataforma que permite a cooperação regional e o intercâmbio de informações entre os grupos de resposta a incidentes de cibersegurança governamentais e nacionais dos Estados-membros da OEA. Na esteira do ataque de ransomware WannaCry, em 2017, o CSIRT Américas intermediou a identificação e isolamento antecipado

de pontos críticos de infecção no continente americano para conter a disseminação do WannaCry na região. Para atenuar surtos futuros, a plataforma desenvolveu um repositório central de ferramentas para seus púbicos regionais a fim de prevenir e combater infecções por ransomware. Desde 2015, a própria comunidade de resposta a incidentes cresceu para 20 grupos nacionais de resposta a incidentes (CSIRTs) na região.

Desde 2016 equipes das Américas têm se capacitado, juntamente com suas contrapartes da Europa, África e Ásia, em exercícios anuais periódicos, organizados em parceria pela OEA, o Instituto Nacional de Segurança Cibernética da Espanha (INCIBE) e o Centro Nacional para a Proteção de Infraestruturas Críticas da Espanha. Em 2018, a OEA, o BID e o INCIBE organizaram o primeiro desafio conjunto de segurança cibernética especificamente para apoiar e estimular jovens talentos na Espanha e nas Américas a seguir carreira em áreas relacionadas à cibersegurança.

Em seu compromisso de fomentar a conformidade com as diretrizes de comportamento responsável no ciberespaço, identificadas pelos relatórios de consenso do Grupo de Especialistas Governamentais em Segurança da Informação da ONU, a OEA constituiu em 2017 um Grupo de Trabalho sobre Cooperação e Medidas de Fortalecimento da Confiança no Ciberespaço. Com o intercâmbio de melhores práticas com a Organização para a Segurança e Cooperação na Europa (OSCE), o grupo de trabalho elaborou dois conjuntos de medidas de fortalecimento da confiança, já adotadas pelos Estados-membros da OEA. Como parte dessas medidas, os Estados-membros resolveram compartilhar informações sobre políticas nacionais de segurança cibernética, estabelecer um ponto de contato nacional para discutir ameaças cibernéticas no nível regional, identificar um ponto de contato distinto em seus ministérios de relações exteriores para promover a cooperação internacional e o diálogo e viabilizar esses canais — conforme o caso — com plataformas e acordos para promover práticas que fortaleçam a estabilidade no espaço digital. Outros compromissos incluem o treinamento de diplomatas e servidores do governo em geral em questões de segurança cibernética e o fortalecimento de iniciativas de construção de capacidades por meio de campanhas de conscientização nos setores público e privado.

A OEA e o GCSCC mantêm uma relação especial. As duas organizações vêm colaborando desde a criação do CMM e realizaram implantações piloto conjuntas do modelo na Jamaica e na Colômbia em 2015 e uma avaliação no Brasil em 2018. Essa parceria estratégica foi formalizada em 2015, por meio de um memorando de entendimento. Por ser um parceiro de confiança, a OEA contribuiu ativamente no processo de revisão do CMM. A colaboração entre os dois organismos também se estende além do CMM e abrange iniciativas conjuntas em eventos que congregam partes interessadas, como o Fórum de Governança da Internet (IGF). Daqui por diante, a OEA e o GCSCC irão colaborar de perto no teste de um instrumento sobre danos cibernéticos, a ser implantado em conjunto com o CMM, bem como no estabelecimento de um polo regional na América Latina como parte de uma constelação global maior de centros regionais de capacidade em segurança cibernética.

A abordagem abrangente da UE para o enfrentamento das ameaças do ciberespaço

Pawel Herczynski
Diretor-Gerente de PCSD e Resposta a Crises
do Serviço Europeu para a Ação Externa

A cibersegurança é imprescindível para nossa prosperidade e segurança. As atividades digitais mal-intencionadas ameaçam não apenas nossas economias, mas também o próprio funcionamento de nossas democracias, nossas liberdades e nossos valores. O futuro de nossa segurança depende da transformação de nossa capacidade de nos proteger contra ameaças cibernéticas: tanto a infraestrutura civil quanto o aparato militar dependem de sistemas digitais seguros.

Esse fato foi reconhecido na Estratégia Global de Política Externa e Segurança da União Europeia (UE).[4] Com base também nas abordagens do Mercado Único Digital, da Estratégia Global, da Comunicação Conjunta ao Parlamento Europeu e ao Conselho "Resiliência, dissuasão e defesa: criar uma cibersegurança sólida para a UE",[5] a Agenda Europeia para a Segurança;[6] o Instrumento Conjunto de Combate a Ameaças Híbridas[7] e a Comunicação sobre o Lançamento do Fundo Europeu de Defesa,[8] a UE decidiu desenvolver maior resiliência e autonomia estratégica, ampliar as capacidades em termos de tecnologia e competências e formar um mercado único forte, bem como elaborar e implementar uma abordagem integrada da UE para a diplomacia cibernética no nível global.

Resiliência

Uma resiliência cibernética sólida demanda uma abordagem coletiva e abrangente. São necessárias estruturas eficazes para promover a cibersegurança e reagir a ataques digitais, não só nos Estados-membros da UE, mas também nas próprias instituições, agências e órgãos da União Europeia. Isso exige também uma abordagem mais abrangente e transversal de políticas para o desenvolvimento da resiliência cibernética e da autonomia estratégica, com um mercado único forte, grandes avanços na capacidade tecnológica da UE e ampliação expressiva do quadro de especialistas qualificados.

A Diretiva NIS, relativa a medidas para um nível comum elevado de segurança de redes e sistemas de informação,[9] desempenha uma função importantíssima no desenvolvimento de uma nova cultura de cibersegurança na UE. Graças a ela, os Estados-membros da UE trocam informações sobre incidentes cibernéticos, compartilham as melhores práticas de cibersegurança, cooperam e estão mais bem coordenados. O Grupo de Cooperação em NIS, criado pela diretiva, promove e facilita a cooperação estratégica e a troca de informações entre os Estados-membros

da UE. Segundo a Diretiva NIS, as operadoras de serviços essenciais (por exemplo, bancos, empresas de telecomunicações, concessionárias de energia, hospitais, etc.) são obrigadas a informar as autoridades nacionais quando são afetadas por incidentes graves de cibersegurança e contam com planos de avaliação para identificar os riscos. Em grande medida, a responsabilidade pela garantia da segurança dos sistemas de redes e informações cabe às operadoras de serviços essenciais e aos provedores de serviços digitais. Contudo, uma cultura de gerenciamento de riscos que envolva a avaliação de riscos e a adoção de medidas de segurança apropriadas aos riscos enfrentados deve ser fomentada e desenvolvida, por meio de requisitos regulatórios apropriados e práticas voluntárias do setor. Diante da sofisticação crescente das ameaças cibernéticas e dos incidentes de segurança cibernética em nossa economia e sociedade digitais, precisamos, mais do que nunca, de cooperação e intercâmbio de informações, bem como da combinação de diferentes competências e especialistas.

Uma medida para melhorar a resposta do direito penal aos ataques cibernéticos foi tomada em 2013, com a adoção da Diretiva sobre ataques contra sistemas de informação,[10] que estipulou regras mínimas relativas à definição de infrações e sanções penais na área de ataques contra sistemas de informação e previa medidas operacionais para melhorar a cooperação entre as autoridades. A Diretiva propiciou avanços sensíveis na criminalização dos ataques cibernéticos a um nível comparável nos vários Estados-membros, o que facilita a cooperação internacional das autoridades policiais na investigação desse tipo de crimes. Dada a inexistência de fronteiras da Internet, a estrutura para a cooperação internacional proporcionada pela Convenção de Budapeste do Conselho da Europa contra a Criminalidade Cibernética[11] enseja a oportunidade de usar de um padrão jurídico ideal nas diversas legislações nacionais que tratam de crimes cibernéticos. Neste momento, está sendo explorado o possível acréscimo de um protocolo à convenção, o que também poderia oferecer uma oportunidade útil para abordar a questão do acesso transfronteiriço a evidências eletrônicas.

Pesquisa e desenvolvimento

Por meio da cooperação, combinação da experiência da UE em cibersegurança e elaboração de um roteiro europeu comum de pesquisa e inovação (P&I) em cibersegurança e de uma estratégia europeia para o setor de segurança cibernética, o continente pode colaborar para o crescimento desse setor e do ecossistema de cibersegurança, o que resultará também na ampliação da capacidade de cibersegurança da UE. É por esse motivo que, em 2016, a Comissão Europeia firmou um contrato de parceria público-privada (cPPP) com a Organização Europeia de Segurança Cibernética (ECSO, na sigla em inglês). O cPPP é determinante na estruturação e coordenação dos recursos setoriais de segurança digital na Europa. Ele inclui um amplo leque de atores, desde PMEs inovadoras até produtores de componentes e equipamentos, operadoras de serviços essenciais e institutos de pesquisa, todos reunidos sob a égide da ECSO. Como parte de seu programa de pesquisa e inovação Horizonte 2020, a UE comprometeu-se a investir até € 450 milhões nesta parceria. Em contrapartida, o setor precisa investir o triplo nas mesmas áreas. Como uma próxima etapa ambiciosa, em setembro de 2018 foi proposto uma nova regulação para estabelecer uma rede de centros nacionais de coordenação de cibersegurança e o novo Centro Europeu de Competências Setoriais, Tecnológicas e de Pesquisa em Cibersegurança. Essa proposta está sendo discutida pelos co-legisladores da UE. O Centro é considerado uma forma de enfrentar a fragmentação do ecossistema de cibersegurança da Europa, solucionar a falta de competências e conhecimentos especializados em cibersegurança, combinar os recursos europeus e coordenar os esforços para o fortalecimento das capacidades de cibersegurança da UE e permitir aos mercados da UE desenvolver produtos e serviços com competitividade mundial. O Centro lançará as bases para uma Europa digital segura, equacionando todos os desafios futuros de cibersegurança decorrentes de tecnologias emergentes (por exemplo, Internet das coisas, inteligência artificial, quantum, HPCs, blockchain) e usadas em setores essenciais (por exemplo, transporte, energia, saúde, finanças, produção e defesa). Ele também definirá e executará os investimentos apropriados

em segurança cibernética para o próximo Programa Quadro Financeiro Plurianual da UE (MFF, na sigla em inglês).

Construção de capacidades

A estabilidade cibernética global depende da capacidade local e nacional de todos os países de prevenir e reagir a incidentes cibernéticos e investigar e processar casos de crimes cibernéticos. O apoio aos esforços de desenvolvimento de resiliência nacional nos países em desenvolvimento aumentará o nível de cibersegurança em escala mundial, com consequências positivas para a UE. O combate às ameaças cibernéticas, em rápida evolução, sugere a necessidade de esforços para o desenvolvimento de formação, políticas e legislação, bem como equipes de resposta a emergências em computadores (CERTs) e unidades de crimes cibernéticos com funcionamento eficiente em todos os países do mundo.

Desde 2013, a UE vem liderando internacionalmente a construção de capacidades em cibersegurança vinculando sistematicamente esses esforços a sua cooperação para o desenvolvimento. A UE continuará a fomentar um modelo de construção de capacidades baseado em direitos, em consonância com a abordagem Digital4Development.[12] As prioridades para construção de capacidades serão os países vizinhos da UE e os países em desenvolvimento com crescimento acelerado da conectividade e rápido surgimento de ameaças. Os esforços da UE serão complementares à sua agenda de desenvolvimento à luz da Agenda 2030 para o Desenvolvimento Sustentável e dos esforços gerais de construção de capacidades institucionais.

Em junho de 2018, a UE também definiu sua abordagem sobre construção de capacidades em cibersegurança quando o Conselho, em suas conclusões sobre as Diretrizes de Construção de Capacidade Cibernética Externa da UE, lembrou que a construção de capacidades em cibersegurança está se tornando um dos temas mais importantes da agenda da política internacional de cibersegurança e enfatizou o papel dessa construção de capacidades nos países e regiões parceiros como elemento constitutivo estratégico dos esforços de diplomacia cibernética da União Europeia.

Diplomacia cibernética

Orientada pelos valores básicos e direitos fundamentais da União Europeia, como a liberdade de expressão e o direito à privacidade e proteção de dados pessoais, bem como a promoção de um espaço digital aberto, livre e seguro, a política internacional de cibersegurança da UE tem o intuito de enfrentar o desafio, em constante evolução, de promover a estabilidade no universo cibernético mundial, bem como de contribuir para a autonomia estratégica da Europa no espaço digital. Dado o caráter global das ameaças, a formação e manutenção de alianças e parcerias sólidas com outros países é fundamental para a prevenção e dissuasão de ataques cibernéticos, que são cada vez mais importantes para a estabilidade e segurança internacionais. Em seus compromissos bilaterais, multilaterais e regionais, a UE dará prioridade ao estabelecimento de um marco estratégico para a estabilidade e a prevenção de conflitos no espaço digital. A UE defende com firmeza a posição de que o direito internacional, em particular a Carta das Nações Unidas, se aplica ao ciberespaço. Como complemento ao direito internacional vinculante, a UE endossa as normas, regras e princípios voluntários não vinculantes de comportamento responsável do Estado, articulados pelo Grupo de Peritos Governamentais da ONU. Ela também estimula o desenvolvimento e implementação de medidas regionais de construção de confiança, tanto na Organização para a Segurança e Cooperação na Europa como em outras regiões. No nível bilateral, os diálogos sobre questões cibernéticas[13] são também promovidos e complementados por esforços para mediar a cooperação com outros países, com vistas a reforçar os princípios de diligência prévia e responsabilidade do Estado no espaço digital. A UE ressalta também que a segurança cibernética não é um pretexto para a proteção do mercado e a restrição de direitos e liberdades fundamentais, inclusive a liberdade de expressão e o acesso à informação. Uma abordagem integrada da

cibersegurança requer respeito aos direitos humanos. Nesse sentido, a UE destaca a importância do envolvimento de todas as partes interessadas na governança da Internet.

Adotado em 2017, o instrumento para uma reação diplomática conjunta da UE a atividades digitais mal-intencionadas (a "caixa de ferramentas da diplomacia cibernética"[14]) estabelece as medidas no âmbito da Política Comum de Assuntos Externos e de Segurança, inclusive medidas restritivas, que podem ser adotadas para fortalecer a resposta da UE a atividades que prejudiquem seus interesses políticos, econômicos e de segurança. O instrumento constitui um passo importante no desenvolvimento das capacidades de sinalização e resposta no nível da UE e dos Estados-membros.

Conclusão

A prontidão da UE para questões cibernéticas é fundamental para o Mercado Único Digital e para a nossa União de Segurança e Defesa. É imperiosa a ampliação da cibersegurança europeia e o enfrentamento das ameaças a alvos civis e militares. Nessa empreitada desafiadora, contamos também com o apoio de nossos parceiros globais. A única forma de proporcionar um espaço digital aberto, seguro e protegido para todos é a união, resiliência e capacidade de proteção eficaz de nosso povo por meio da antecipação de possíveis ameaças cibernéticas e incidentes de cibersegurança, desenvolvimento de sólida resiliência em nossas estruturas e defesa, ágil recuperação de eventuais ataques cibernéticos e dissuasão dos responsáveis.

Novas ameaças em segurança cibernética: implicações para a América Latina e o Caribe

Nayia Barmpaliou,
Diretora de Políticas e Iniciativas Públicas
do Centro de Cibersegurança do Fórum Econômico Mundial

Cibersegurança na era da hiperconectividade e das pandemias

A pandemia da Covid-19 marcou um ponto de inflexão fundamental em nossa trajetória global e acentuou como nunca nossa dependência da infraestrutura digital. Embora tenha exposto deficiências estruturais inerentes a vários sistemas de nossa sociedade, como saúde, economia, emprego e educação, esta crise também evidenciou o papel catalisador da tecnologia na forma como enfrentamos coletivamente a pandemia.

Em um intervalo de três meses, testemunhamos a aceleração da transformação digital anteriormente prevista para ocorrer em três anos.[15] Nossa transição para a era do "digital de tudo" remodelou profundamente nossa vida profissional e pessoal. Mesmo no ambiente mais disruptivo da pandemia, a Internet e a infraestrutura digital global possibilitaram a prestação de serviços essenciais, permitiram a continuidade do funcionamento das empresas e mantiveram cada um de nossos contatos sociais. O resultado dessa transição foi o drástico aumento de uma superfície de ataques cibernéticos em um ecossistema digital de vulnerabilidades já amplificadas que abarca mais de 20 bilhões de dispositivos conectados à Internet das coisas (IoT) em todo o mundo.[16]

Mesmo antes da pandemia, as violações de segurança cibernética e os vazamentos de dados estavam se tornando obstáculos para a economia digital. Os criminosos cibernéticos exploram rapidamente os novos vetores de ataque e tiram proveito das lacunas na cooperação policial internacional dada a natureza inerentemente transnacional de suas atividades desonestas. Por sua vez, invariavelmente o risco de ataques cibernéticos contra infraestruturas essenciais e de fraude ou roubo de dados encabeça a lista de preocupações de empresários de todo o mundo. De acordo com o Relatório de Riscos Globais do Fórum Econômico Mundial de 2020,[17] o risco de ataques cibernéticos contra infraestruturas críticas e fraude ou roubo de dados foi classificado entre os dez principais riscos de maior probabilidade de ocorrência, ao passo que o recente relatório Covid-19 Risks Outlook[18] (Perspectivas dos Riscos da Covid-19, em tradução livre) identificou os ataques cibernéticos como a terceira maior preocupação devido à nossa atual migração prolongada e sustentada para modelos de

trabalho digital. Os dados disponíveis corroboram essas preocupações; estima-se que os danos dos crimes digitais atinjam a cifra de US$ 6 trilhões até 2021, o que equivale ao PIB da terceira maior economia do mundo.[19] Além do custo financeiro, os crimes e ataques cibernéticos minam a confiança do usuário na economia digital. Pesquisas indicam que menos de 50% da população mundial com acesso à Internet acredita que a tecnologia irá melhorar suas vidas, demonstrando uma crescente e profunda falta de confiança em relação à privacidade de dados.[20]

Essas tendências são particularmente pertinentes para a região da América Latina e Caribe (LAC) que, nos últimos cinco anos, testemunhou uma expansão tremenda no uso de tecnologias da informação e comunicação (TIC). Conforme a região está se movendo cada vez mais na direção da economia digital, aumenta a necessidade de intensificar a confiança digital. Em uma economia cada vez mais orientada por dados, os protocolos de gestão dos riscos de segurança digital e proteção da privacidade constituem responsabilidades compartilhadas por governos, setor privado e usuários individuais.[21] Além da elevação da construção de capacidades em segurança cibernética na agenda de desenvolvimento da região, graças aos esforços articulados e intensificados do Banco Interamericano de Desenvolvimento (BID) e da Organização dos Estados Americanos (OEA) nos últimos anos, a necessidade de integrar a segurança cibernética e o combate aos crimes cibernéticos às estratégias e políticas digitais da região também foi registrada no nível mais alto como parte da Proposta de Agenda Digital para a América Latina e o Caribe.[22]

Uma questão transversal na política nacional

A penetração do espectro digital em todas as áreas da atividade humana e os níveis inéditos de inovação e interdependência tecnológica tornaram impossível tratar a segurança cibernética de forma isolada, como uma questão técnica ou uma área de política distinta. Nos últimos anos, a segurança cibernética quebrou o teto de vidro dos compartimentos técnicos e se encontra no cruzamento de várias disciplinas e áreas: acesso e conectividade digital, resiliência, justiça penal, diplomacia, segurança e defesa internacional, economia e comércio digital, bem como novas tecnologias. Com os países tentando colher os benefícios da Quarta Revolução Industrial, a segurança cibernética foi elevada à condição de zeitgeist da política global. Isto acarretou um aumento expressivo na adoção ou revisão de estratégias nacionais de cibersegurança, que utilizam uma abordagem de consideração do governo como um todo ou, por vezes, da sociedade como um todo, bem como a criação ou adaptação da legislação nacional sobre crimes cibernéticos, sobretudo em países em desenvolvimento que não tinham uma legislação pertinente em vigor.

Este relatório traz evidências promissoras de que os governos da região da ALC deram passos importantes no desenvolvimento e eficácia de suas estratégias nacionais de cibersegurança, que também serviram como veículos para melhorar a cultura e as práticas nacionais nessa área desde a última pesquisa, realizada em 2016. Além disso, quatro países da América Latina e Caribe aderiram à Convenção do Conselho da Europa sobre a Criminalidade Cibernética (a Convenção de Budapeste), cujo objetivo é adotar uma política criminal comum contra os crimes cibernéticos, oferecendo uma estrutura comum para a legislação nacional cooperação internacional adequadas.

Falha de mercado e oportunidade para a cibersegurança na economia digital

Embora gere grandes inovações, o rápido avanço das tecnologias digitais também cria novas vulnerabilidades em um ritmo mais acelerado do que o de suas proteções. Até o momento, o descompasso entre o lançamento no mercado e a implementação de medidas de segurança continua a ser uma questão predominante, com as forças do mercado exercendo pressão para a criação de novos produtos de tecnologia sem incentivos para priorizar os recursos de segurança desde o início do seu desenvolvimento.[23]

É impressionante que, a despeito da evolução no comportamento do consumidor em relação às crescentes preocupações com privacidade e segurança, a mudança nos objetivos do mercado não esteja

sendo suficientemente rápida e é inevitável que leve a diferentes experiências em intervenções e regimes regulatórios. Por enquanto, constatamos que a falta generalizada de uma abordagem de incorporação da segurança já na fase de desenvolvimento das tecnologias gerou uma tendência a regimes voluntários de certificação de segurança cibernética para produtos de TIC, como, por exemplo, na UE e em Singapura, além de outros países com foco específico na IoT. Na outra ponta do espectro, essa falha de mercado fez a segurança cibernética despontar como um dos setores mais diversificados e de maior crescimento em todo o mundo. Antes da crise da Covid-19, previa-se que os gastos mundiais com produtos e serviços de cibersegurança aumentariam 88% nos próximos oito anos.[24] A retração econômica causada pela pandemia pode levar à consolidação desse mercado. No caso da ALC, à medida que a região conquista mais maturidade em segurança cibernética, é importante que as estratégias nacionais para sua implantação considerem medidas que limitem o risco do aumento da superfície de ataque e se inspirem em modelos existentes ou em regimes voluntários.

O imperativo estratégico da segurança cibernética no setor empresarial

A noção de que a estratégia de segurança cibernética é parte integrante da estratégia do setor empresarial ganhou mais tração e aplicação efetiva nas empresas nos últimos cinco anos, em parte devido à publicidade em torno de algumas violações de segurança em grande escala, bem como ao aumento de considerações jurídicas e regulatórias, inclusive a entrada em vigor, em maio de 2018, do Regulamento Geral sobre a Proteção de Dados da UE (GDPR), que tem abrangência global significativa. Em termos práticos, esse tem sido um fator importante para que dirigentes e diretorias de empresas compreendam melhor os riscos cibernéticos de seu modelo operacional e encontrem o equilíbrio certo entre proteção da segurança de seus ativos, mitigação de perdas e manutenção da lucratividade em um ambiente competitivo. Essa maior conscientização entre os dirigentes das empresas constitui um primeiro passo crucial para capacitar o processo decisório bem fundamentado nas empresas para o planejamento da segurança cibernética, mecanismos de resposta e investimentos. O lançamento do Manual de Supervisão de Riscos Cibernéticos para Diretorias de Empresas pela Organização dos Estados Americanos e a Aliança de Segurança da Internet em 2019,[25] marcou um esforço consultivo considerável para promover essa conscientização na região da ALC entre as partes interessadas de diretorias de empresas, altos executivos, governos e academia, bem como para adaptar a orientação às especificidades regionais.

Paralelamente a isso, com as empresas de maior porte investindo mais em segurança cibernética e inovação em segurança, análises recentes indicam um aumento expressivo nos ataques direcionados a pequenas e médias empresas (PMEs). Essa dinâmica cria um risco considerável para o ecossistema digital, sobretudo considerando que as PMEs não dispõem de recursos financeiros para fazer investimentos maciços em segurança cibernética ou simplesmente não têm a cultura de segurança como um item de destaque em suas agendas. Na realidade, os desafios enfrentados pelas PMEs em termos de falta de recursos financeiros ou cultura de segurança para proteger seu ambiente digital são bastante diferentes daqueles das organizações maiores. Refletindo essa realidade no contexto regional da ALC, cabe observar que, de acordo com a Organização para Cooperação e Desenvolvimento Econômico, 99,5% da estrutura econômica da região é composta por micro, pequenas e médias empresas.[26] A ampliação da conscientização sobre o tema e a promoção do esmero em segurança cibernética básica nas PMEs da região deve ser uma prioridade crucial nos próximos anos.

Novas tecnologias remodelam o cenário da segurança cibernética e das políticas

As “velhas” e “novas” tecnologias não estão apenas remodelando o setor e o cenário da cibersegurança, mas também questionando em termos mais gerais os mecanismos tradicionais de funcionamento da sociedade. A convergência de tecnologias da informação com tecnologias operacionais e sistemas legados já representa grandes desafios em todo o ecossistema

digital. O surgimento de novas tecnologias e suas aplicações, como inteligência artificial, big data, redes 5G, computação na nuvem, Internet das Coisas e computação quântica, está contestando drasticamente nosso pensamento convencional em relação ao futuro da economia digital. Por um lado, elas oferecem oportunidades imensas de eficiência e inovação, mas, por outro, também ampliam a superfície de ataque e podem criar riscos desconhecidos para a segurança e a privacidade de dados. Por esse motivo, empresas e governos precisam trabalhar em conjunto para desenvolver uma compreensão sólida dos novos riscos relacionados à segurança cibernética, dos pontos de vista operacional, de risco e de políticas. Parte do desafio será promover a confiança entre as diferentes partes interessadas do ecossistema, para reduzir o atrito nos atuais modelos regulatórios e de garantia. Para os países da região da América Latina e Caribe e para outras economias emergentes, é importante que essas novas questões de segurança sejam tratadas de forma a não exacerbar as barreiras de acesso aos benefícios dessas novas tecnologias.

A cibersegurança em uma arquitetura global fragmentada e polarizada

Na era de uma ordem global multipolar e multiconceitual, o contexto geopolítico e social não só influencia o desenvolvimento da tecnologia, mas é também afetado por ela. Por um lado, o surgimento de novas tecnologias tem o potencial de remodelar profundamente as dinâmicas e alianças geopolíticas, ao passo que hoje a convergência das novas tecnologias com as aplicações tradicionais desempenha um papel determinante na intensificação das tensões existentes em relação aos valores para a governança da Internet aberta e descentralizada em contraste com a soberania digital ou o uso do espaço digital como um lugar de concorrência estratégica. Essa polarização pode comprometer tanto a segurança no espaço digital quanto a confiança para a cooperação global contra desafios comuns de segurança cibernética. As abordagens divergentes das principais ciberpotências em relação à aplicação do direito internacional no espaço digital — que estão em discussão nos fóruns relevantes da ONU[27] — refletem um ambiente internacional bastante conflituoso, ainda mais exacerbado pelos clamores por autonomia digital estratégica, mesmo que ela seja difícil de alcançar num contexto de transformações tecnológicas aceleradas e cadeias de valor globais.

Nesse cenário, as organizações regionais têm se posicionado como as principais interessadas na promoção da estabilidade, segurança e esforços de construção de confiança no espaço digital, na forma de medidas de fortalecimento da confiança. A região da ALC também demonstrou avanços consideráveis nesse sentido com o estabelecimento, em 2017, do Grupo de Trabalho da OEA sobre Cooperação e Medidas de Fortalecimento da Confiança no espaço digital pelo Comitê Interamericano contra o Terrorismo.[28]

Necessidade de mudança de paradigma na cooperação público-privada

Ao longo do tempo, a natureza intrinsecamente complexa e distribuída do ecossistema digital, aliada às múltiplas dimensões das políticas cibernéticas públicas e empresariais, criou uma arquitetura de partes interessadas extremamente complexa. A digitalização transformou nossa sociedade em um sistema de sistemas, no qual as funções essenciais são distribuídas entre as partes interessadas públicas e privadas em pontos dispersos e com interdependências complexas. Portanto, os últimos anos nos ensinaram que, para superar as barreiras e alcançar a verdadeira eficiência, a cooperação público-privada em segurança cibernética exige um pensamento fora dos formatos tradicionais e rígidos. Para lidar com essa maior complexidade e essa responsabilidade compartilhada, precisamos de uma nova geração de parcerias público-privadas que invalidem o "pensamento compartimentado" e adotem uma abordagem sistêmica na navegação pela dinâmica composta de fatores políticos, tecnológicos, econômicos, sociais e geopolíticos, que molda o cenário de riscos de segurança cibernética e suas interdependências. Ao acelerar sua transformação digital, os países da região da América Latina e Caribe têm a oportunidade de incorporar esse raciocínio sistemático em sua

arquitetura de cooperação público-privada para que ele possa ser um fator de diferenciação para sua resiliência cibernética.

Conclusão

A complexidade da segurança cibernética é um exemplo claro da inadequação de nossa atual arquitetura global fragmentada para o seu propósito no século XXI. O efeito catalisador da pandemia da Covid-19 sobre a economia colocou uma pressão imensa sobre nosso ambiente digital para que ele permaneça seguro, resiliente e eficiente. A cibersegurança é um componente essencial que permite essa conectividade sem precedentes, de sorte que esse novo normal reafirmou seu valor como um bem público mundial.

Além da proteção operacional de sistemas e redes, a segurança cibernética é, e continuará a ser, essencial para assegurar a integridade e resiliência da interconexão de processos governamentais, empresariais e socioeconômicos que estão no topo de nosso ecossistema de tecnologias de complexidade contínua. O enfrentamento generalizado do risco cibernético exige esforços e adaptação contínuos. O presente relatório oferece percepções importantes sobre os esforços feitos no nível nacional na região da ALC, registrando e quantificando o avanço dos países em diferentes dimensões da segurança cibernética desde a revisão de 2016, além de demonstrar a melhoria da postura da região nessa área ao longo do tempo. Esse trabalho pode servir como uma ferramenta inestimável para que os responsáveis por decisões nos setores público e privado identifiquem as intervenções prioritárias à medida que avancem na melhoria do estado da segurança cibernética na região da ALC por meio de colaboração nacional, regional e internacional articulada e escalável.

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

A necessidade de uma resposta harmonizada às ameaças cibernéticas: um roteiro

Sven Mikser,
Ministro da Relações Exteriores da
República da Estônia

Ao longo da última década, surgiram no espaço digital diversas ameaças que exigem a atenção de governos de todo o mundo. Três das questões mais prementes de cibersegurança internacional envolvem a instabilidade crescente causada pelos crimes cibernéticos, invasões em redes críticas com o uso de meios cibernéticos e operações cibernéticas com motivação política. Todos esses elementos foram ou estão sendo implementados nas agendas políticas de países de todo o mundo. Contudo, a priorização das questões delineadas difere muito de um Estado para outro, o que indica uma maior necessidade de harmonização dos esforços dos países para ampliar sua segurança cibernética. A questão, portanto, é como incentivar os Estados a cooperar em uma área que convencionalmente seria considerada uma questão interna.

Uma forma de enfrentar os novos desafios entre os Estados seria adotar uma abordagem internacional que se concentrasse na harmonização das capacidades de segurança cibernética. Devido ao nível elevado de interconexão dos países no espaço digital, a estabilidade de um estado afeta o bem-estar de todos ao seu redor. Portanto, uma abordagem regional poderia estimular o envolvimento de muitos países na construção das capacidades de segurança cibernética. Muitas organizações regionais tomaram iniciativas para solucionar a questão. Por exemplo, há vários anos a Organização dos Estados Americanos (OEA) vem organizando oficinas para o desenvolvimento de capacidades em segurança cibernética. Esses eventos são de particular importância para lançar as bases para o desenvolvimento de sólidas capacidades no nível nacional por meio da ampliação da conscientização sobre as novas ameaças cibernéticas e o desenvolvimento de possíveis mecanismos de enfrentamento. Levando em consideração os primeiros esforços com que vários atores contribuíram para promover a conscientização sobre segurança cibernética na América Latina e Caribe (ALC), outras medidas para se conseguir um espaço digital mais estável e próspero poderiam ter como base o fortalecimento da cooperação regional em segurança cibernética.

Veremos a seguir uma explanação de como a cooperação regional e os valores comuns em segurança

cibernética ajudariam os países a superar as três principais ameaças destacadas acima, com algumas sugestões sobre como avançar a partir do estado atual de desenvolvimento.

Como as capacidades de segurança cibernética harmonizadas internacionalmente podem garantir um espaço digital mais seguro?

Dado que os crimes possibilitados pelo espaço digital não respeitam fronteiras, a cooperação regional na construção de capacidades é imprescindível para reagir ao crime organizado cibernético e conter os ataques cibernéticos antes que eles fujam ao controle. Os incidentes de cibersegurança ocorridos em 2017 e 2018 demonstraram o risco de aumento dos danos financeiros e do número de pessoas e países afetados. Já testemunhamos operações criminosas cibernéticas de proporções inéditas, que paralisaram o bom andamento de economias nacionais, direcionadas especificamente a alguns dos pilares centrais de sua economia, como os setores industrial e bancário.

A conscientização de especialistas técnicos, políticos e policiais pode ajudar a diminuir a vulnerabilidade dos países aos crimes cibernéticos. A natureza dos atos criminosos que ocorrem no ciberespaço está mudando com rapidez, razão pela qual os países precisam investir mais na educação de suas forças policiais, sistemas judiciais e outras instituições governamentais competentes. A adaptação às novas circunstâncias também é essencial para o desenvolvimento de parcerias público-privadas confiáveis. O compartilhamento de informações entre o setor privado, o setor público e as instituições governamentais já pode ser verificados em alguns países, mas é menos perceptível em outros. A harmonização regional dos ordenamentos jurídicos para enfrentar os crimes cibernéticos e das melhores práticas policiais pode contribuir para a segurança e estabilidade regionais no espaço digital.

Além do aumento da incidência de crimes cibernéticos, o roubo de propriedade intelectual com o uso de meios cibernéticos se tornou mais comum em muitas partes do planeta. O nível de sofisticação do roubo de propriedade intelectual torna impossível evitar atribuir sua autoria a um ator estatal.

Alguns dos programas de malware usados dão sinais de origem regional e são desenvolvidos especificamente para atingir determinadas regiões do mundo. Esse é um dos motivos pelos quais a cooperação regional no combate ao roubo de propriedade intelectual com o uso de meios cibernéticos deve ser considerada parte de uma abordagem internacional harmonizada capitaneada pelos países.

Essas atividades têm como pano de fundo operações de influência política conduzidas no espaço digital, que agora podem representar uma séria preocupação para os países democráticos. Em 2018, foram realizadas eleições presidenciais nas três maiores democracias: Brasil, Colômbia e México. Embora a cobertura dos meios de comunicação indique apenas uma fraca disseminação de desinformação durante as campanhas eleitorais e períodos de votação, é bastante provável que, nos próximos anos, a questão da interferência eleitoral permaneça na agenda da maioria dos países democráticos. Interferência eleitoral, campanhas de desinformação e segurança da infraestrutura de votação são consideradas áreas de preocupação no que se refere à disseminação da influência política em países estrangeiros. Aproveitando o alcance da mídia digital, alguns países estrangeiros podem continuar a tentar sabotar as instituições democráticas e a formulação de políticas na região. A mudança da opinião pública por meio da mídia virtual tornou-se uma parte persistente da atividade política contemporânea, que é particularmente visível em época de eleições, de modo que as estruturas para o seu enfrentamento devem existir antes de uma eleição.

Uma abordagem regional para harmonizar o nível de capacidade de segurança cibernética

A promoção das políticas de segurança cibernética no nível regional deve começar com o desenvolvimento de elementos constitutivos nacionais. Uma estratégia nacional de cibersegurança pode funcionar como o

principal instrumento de conscientização e planejamento em cada Estado. As estratégias de segurança cibernética existentes podem oferecer uma série de exemplos e lições.

Alguns dos países que lançaram suas estratégias ainda na década de 2000 testemunharam em primeira mão os acontecimentos ao longo do tempo, oferecendo uma visão estratégica da segurança cibernética. Na Estônia, a segurança cibernética se tornou uma parte permanente do trabalho cotidiano de diversos ministérios e instituições do Estado. Seu principal efeito foi uma coordenação de políticas intra-Estado profundamente arraigada nas estruturas da formulação de políticas estratégicas do Estado. Embora a ênfase na primeira estratégia de cibersegurança da Estônia tenha surgido de um caso de campanha híbrida devido aos eventos de 2007 em Tallinn e se tenha tornado parte da reação à crise, as duas estratégias posteriores se concentraram mais amplamente no fortalecimento da resiliência cibernética e das capacidades.

O desenvolvimento de uma política de segurança cibernética é um processo contínuo. Entre outros objetivos estratégicos, a terceira estratégia de cibersegurança da Estônia (2019–2021) tratou a educação cibernética como uma das áreas onde devem ser feitos mais investimentos no futuro. A dimensão cibernética também foi incorporada à legislação nacional de resposta a crises. Algumas das melhores práticas que temos para dar continuidade ao trabalho no nível nacional envolvem o aprimoramento da coordenação nacional e dos mecanismos de troca de informações, a superação da defasagem entre os especialistas e os principais decisores nacionais nos setores público e privado e a criação de instituições e estruturas de coordenação de segurança cibernética. Essas práticas ainda fazem parte do nosso trabalho atual.

Como as atividades mal-intencionadas com o uso de meios cibernéticos podem facilmente se propagar de um país para outro, é impossível haver investigações eficazes sem cooperação internacional. Como sabemos, um número crescente de nossos sistemas nacionais de informação e infraestruturas críticas depende da segurança de nossas redes. Uma estratégia de segurança cibernética que englobe todo o governo — inclusive possíveis medidas preventivas, legislação nacional que trate dos crimes cibernéticos e cooperação operacional internacional — deve ser um dos requisitos de maior destaque para evitar atividades que explorem as vulnerabilidades das infraestruturas críticas.

Caminhos a seguir para a cooperação regional na América Latina e Caribe

A ampliação da cooperação regional para desenvolver uma visão comum e aprender com as melhores práticas de outros Estados é fundamental para harmonizar as capacidades de segurança cibernética dos países. Diversos Estados-membros da OEA adotaram com sucesso legislações penais com disposições sobre crimes relacionados a TI, bem como estratégias de segurança cibernética. Além das disposições legais, muitos países já aderiram à Convenção de Budapeste contra os Crimes Cibernéticos. Dos pontos de vista nacional e internacional, a Convenção de Budapeste oferece um marco jurídico internacional abrangente e confiável para o combate aos crimes cibernéticos e, durante suas quase duas décadas de existência, tornou-se um instrumento de referência global. Assim, a Convenção de Budapeste passou a ser um modelo preferencial para muitos países na promoção de suas próprias legislações nacionais, formação de cooperação internacional e intercâmbio de evidências eletrônicas.

Dado que as ameaças cibernéticas estão ficando mais sofisticadas, é responsabilidade dos Estados assegurar que as atividades dos criminosos não passem despercebidas. Iniciativas legislativas e de políticas, juntamente com medidas de construção de capacidades, constituem elementos fundamentais para o combate às ameaças surgidas no espaço digital, inclusive a conduta dos criminosos. A implantação de legislação pertinente e a adoção de métodos estratégicos irão sustentar a eficácia do trabalho realizado em prol da justiça penal no nível nacional e da cooperação internacional entre os

Estados da OEA, sob os auspícios de dispositivos do direito internacional.

A conscientização acerca das ameaças cibernéticas no nível político é apenas o primeiro passo para o desenvolvimento de capacidades de segurança cibernética mais harmonizadas no âmbito regional. A adoção e aplicação de políticas nacionais de segurança cibernética propiciaria desenvolvimento econômico e político mais seguro e estável na região, além de contribuir para a estabilidade local e global do espaço digital. Atores regionais na ALC, como a OEA, já contribuíram para esse processo. É chegada a hora de uma implementação mais prática.

Desenvolvendo Capacidades de Cibersegurança:

desafios para a educação pós-ensino médio na América Latina e Caribe

UNIVERSIDAD DE CHILE

Prof. Pablo Ruiz Tagle-Vial
Reitor da Faculdade de Direito da **Universidade do Chile**
Prof. Daniel Álvarez Valenzuela
Coordenador Acadêmico do Centro de Estudos em Direito da Ciência da Informação da Faculdade de Direito da **Universidade do Chile**

Nos últimos anos, vários países da América Latina e Caribe presenciaram e foram vítimas do número crescente de ameaças à segurança cibernética que afetaram não apenas instituições públicas e privadas, mas também os cidadãos desses países. O aumento das ameaças à segurança cibernética é evidenciado pelo número de ataques registrados, bem como pelo seu nível de intensidade e sofisticação.

O diagnóstico das causas atribuídas ao surgimento das ameaças cibernéticas é conhecido por todos. Na versão anterior deste relatório, publicada em 2016,[29] constatou-se que o nível de crescimento das tecnologias digitais da região, os processos incipientes de transformação digital que esses países estão empreendendo e a dependência gerada pela tecnologia foram fatores que contribuíram para o aumento dos riscos e ameaças à segurança digital enfrentados pelos países da região.

Além do acima exposto, a versão anterior deste relatório também esclarece como os países da ALC estão mal preparados para enfrentar novos cenários de risco para a segurança de seus habitantes e, consequentemente, para a proteção efetiva de seus direitos, questão que se manifestou em todas as dimensões analisadas no Modelo de Maturidade da Capacidade de Segurança Cibernética das Nações (CMM) desenvolvido pelo Centro Global de Capacidade de Segurança Cibernética da Universidade de Oxford.[30]

Na versão atual do relatório, o nível de maturidade dos países em educação, capacitação e construção de capacidades continua extremamente desigual, o que não nos surpreende, dadas as imensas disparidades econômicas, sociais e culturais existentes entre os diversos países da ALC, como veremos a seguir.

Por um lado, temos um grupo de países — que representa um terço do total dos países analisados — que aumentou consideravelmente suas classificações em áreas como educação e capacitação nos últimos anos, atingindo o nível médio de maturidade. Esse é o caso do Uruguai, que atingiu um nível de maturidade

estratégica na área de formação profissional, bem como o da Guiana, que aumentou sua classificação em quase todas as áreas avaliadas.

Esse grupo de países também inclui Argentina, Chile, Colômbia, Costa Rica, México, Paraguai, República Dominicana e Trinidad e Tobago, que, coincidentemente, são os países que contam com uma política ou estratégia nacional de cibersegurança, total ou parcial e que criaram uma oferta educacional, tanto pública como privada, que contempla a formação especializada em cibersegurança, dos pontos de vista técnico e jurídico.

Por outro lado, o presente relatório observa o progresso marginal ou sua ausência no nível de maturidade de dois terços dos países da ALC nos quesitos educação, capacitação e desenvolvimento de competências em segurança cibernética. Nesses países, a oferta de formação especializada em segurança digital é inexistente ou incipiente e, quando existe, costuma considerar apenas a dimensão técnica da segurança cibernética.

Esses resultados nos convidam a repensar as estratégias que cada um desses países, bem como suas organizações públicas e privadas, deve adotar para melhorar seus níveis atuais de maturidade, promovendo mecanismos de cooperação internacional tanto no nível regional como no sub-regional. Por exemplo, países que conseguiram promover e melhorar sua oferta educacional poderiam auxiliar aqueles que estão em situação menos vantajosa.

Como já foi dito várias vezes, o fator humano é e continuará a ser um elemento fundamental para o sucesso de qualquer estratégia, de sorte que as instituições pós-ensino médio desempenham um papel fundamental nesse sentido. Do nosso ponto de vista, os desafios que enfrentamos são múltiplos e exigem soluções complexas e diferenciadas em função da realidade política, econômica e social dos diversos países que compõem a região.

No caso dos países abrangidos por este relatório e que estão nos estágios iniciais de maturidade, parece inevitável a busca pelo desenvolvimento de programas especializados de graduação e pós-graduação em tecnologia da informação e segurança cibernética, com ênfase no desenvolvimento das competências necessárias para uma formação técnica de qualidade. Como já ocorreu no passado, a cooperação internacional, bem como as parcerias público-privadas, pode desempenhar um papel fundamental na identificação e priorização das necessidades mais prementes de cada país.

Além de fortalecer e expandir suas especializações nos cursos de graduação e pós-graduação, os países que se encontram atualmente no estágio Formativo ou passaram para o estágio Estabelecido devem iniciar processos de inovação curricular para a incorporação do conteúdo mínimo que qualquer profissional deve adquirir na área de tecnologia da informação e segurança digital, e certamente incluindo a perspectiva de gênero, a fim de permitir que outras lacunas recém-identificadas sejam eliminadas. Entre os conteúdos mínimos que podem ser identificados hoje, podemos citar o gerenciamento de riscos, regulamentação de tecnologias, proteção de dados pessoais e crimes informáticos, entre outros.

De modo semelhante, é necessário fomentar o desenvolvimento de programas multidisciplinares que permitam a formação integral de profissionais capazes de compreender a tarefa de suas respectivas disciplinas de um ponto de vista mais amplo. Esse é um fator essencial na transição para uma sociedade digital que vários de nossos países estão vivenciando, o que requer não apenas especialistas profissionais e técnicos na área de tecnologia da informação e segurança cibernética, mas também profissionais de ciências sociais, inclusive nos campos do direito, ciência política, ciência econômica e comunicação social, entre outros. Nesta área não podemos deixar de mencionar os programas de pós-graduação que a Universidade do Chile oferece há décadas em sua Escola de Engenharia[31] e, mais recentemente, em sua Faculdade de Direito,[32] iniciativas que, desde o início, consideraram o enfoque multidisciplinar como um aspecto essencial da formação de pós-graduação especializada.

Os países que estão no estágio de maturidade Estabelecido exigem um compromisso maior de suas

universidades e instituições de ensino superior com a pesquisa e desenvolvimento, por meio de esforços públicos e privados, em vários aspectos relacionados à segurança cibernética, como a criptografia e suas diversas aplicações, o estudo de modelos e técnicas de análise de incidentes, o uso de inteligência artificial e redes neurais na solução de problemas complexos e aplicações de segurança, entre outros. A pesquisa pode ser baseada em informações coletadas pelas autoridades nacionais de segurança cibernética, pela plataforma do Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT) das Américas, administrado pela OEA, e pelas empresas especializadas que atuam em cada país.

O círculo virtuoso gerado por esse intercâmbio contínuo de informações — com as devidas medidas técnicas, jurídicas, de confidencialidade e de segurança — permitirá a alguns desses países passar aos estágios de maturidade Estratégica e Dinâmica. Assim, a oferta educacional, treinamento e pesquisa estarão direcionados para as reais necessidades e objetivos estratégicos de cada país, de acordo com as definições adotadas nas respectivas políticas ou estratégias nacionais de cibersegurança, ao mesmo tempo mantendo um sistema de identificação e gerenciamento de riscos compatível com os tipos de ameaças e vulnerabilidades que enfrentam.

Finalmente, o desafio que enfrentamos como instituições de ensino superior deve ser visto, ao menos pelas instituições públicas ou estatais, como um desafio nacional que, ao ser superado, nos proporcionará um espaço digital livre, aberto, seguro e resiliente, beneficiando diretamente as pessoas e o pleno exercício de seus direitos fundamentais no ciberespaço.

O modelo de maturidade das capacidades de cibersegurança

Em consulta a mais de 200 especialistas internacionais de governos, sociedade civil e academia, o Centro Global de Capacidade de Segurança Cibernética (GSCC) da Universidade de Oxford desenvolveu o Modelo de Maturidade da Capacidade de Segurança Cibernética das Nações (CMM).[33] A finalidade do CMM é fornecer uma avaliação do nível de maturidade das capacidades de cibersegurança de um país, atribuindo um estágio específico que corresponda ao seu grau de concretização da cibersegurança. Os cinco estágios de maturidade, que são atribuídos por meio de uma avaliação, vão desde o mais básico (Iniciante) até o mais avançado (Dinâmico).

Os cinco estágios são definidos[34] a seguir (ver Figura 1):

- ***Iniciante:*** Nesse estágio, a maturidade em segurança cibernética é inexistente ou possui caráter bastante embrionário. Pode haver discussões iniciais sobre construção de capacidades em cibersegurança, mas não foram tomadas providências concretas. Não há indícios observáveis da capacidade de segurança cibernética neste estágio.

- ***Formativo:*** Alguns aspectos começaram a crescer e a ser formulados, mas podem ser pontuais, desorganizados, mal definidos ou simplesmente novos. No entanto, as evidências desses aspectos podem ser claramente demonstradas.

- ***Estabelecido:*** Os elementos do aspecto existem e estão funcionando. Entretanto, não há considerações criteriosas da alocação relativa dos recursos. Poucas decisões de trade-off foram tomadas em relação ao investimento relativo neste aspecto. Contudo, o aspecto é funcional e definido.

- ***Estratégico:*** Nesse estágio, foram feitas escolhas acerca dos indicadores importantes do aspecto e quais são menos importantes para a organização ou país em questão. O estágio Estratégico reflete o fato de que essas escolhas foram feitas, condicionadas às circunstâncias específicas do Estado ou organização.

- ***Dinâmico:*** Neste estágio, há mecanismos claros para alterar a estratégia conforme as circunstâncias, como a sofisticação tecnológica do ambiente da ameaça, conflito global ou uma mudança significativa em uma área de preocupação (por exemplo, crime cibernético ou privacidade). As organizações dinâmicas desenvolveram métodos para alterar as estratégias com rapidez. Processo decisório ágil, remanejamento de recursos e atenção constante ao ambiente em evolução são características deste estágio.

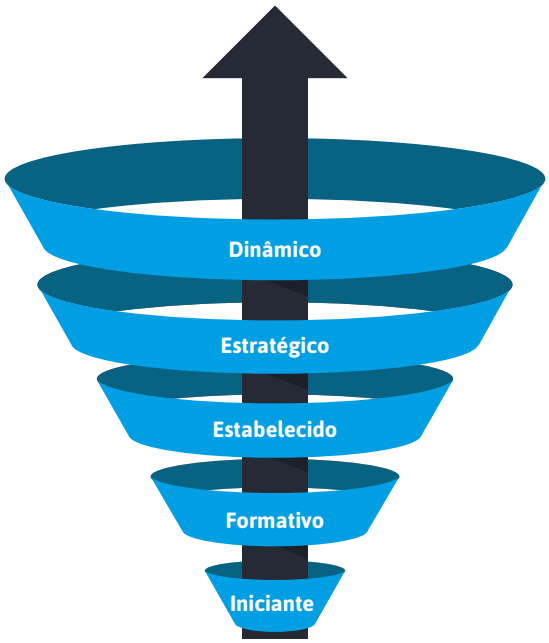


Figura 1: Os cinco estágios da maturidade

A avaliação dos níveis de maturidade é dividida em cinco dimensões (ver Figura 2), que correspondem a aspectos essenciais e específicos da cibersegurança: (i) Política e estratégia de cibersegurança; (ii) Cibercultura e sociedade; (iii) Educação, capacitação e competências; (iv) Marcos legais e regulatórios; e e (v) Normas, organizações e tecnologias. Esses aspectos são subdivididos em um conjunto de fatores que descrevem e definem o que significa possuir capacidade de segurança cibernética em cada dimensão e indicam como aumentar a maturidade.

A tabela a seguir detalha os fatores que compõem as dimensões:

Dimensão 1 Política e Estratégia de Cibersegurança (Criação da estratégia de segurança cibernética e resiliência)	**D1.1** Estratégia Nacional de Cibersegurança **D1.2** Resposta a incidentes **D1.3** Proteção de infraestruturas críticas (IC) **D1.4** Gerenciamento de crises **D1.5** Ciberdefesa **D1.6** Redundância de comunicações
Dimensão 2 Cibercultura e Sociedade (Incentivo a uma cultura de segurança cibernética responsável na sociedade)	**D2.1** Mentalidade de cibersegurança **D2.2** Confiança e segurança na Internet **D2.3** Compreensão do usuário sobre a proteção de informações pessoais na Internet **D2.4** Mecanismos de Denúncia **D2.5** Mídia e redes sociais
Dimensão 3 Educação, capacitação e competências em cibersegurança (Desenvolvimento de conhecimentos em cibersegurança)	**D3.1** Conscientização **D3.2** Marco para a educação **D3.3** Marco para a formação profissional

Dimensão 4 Marcos legais e regulatórios (Criação de marcos jurídicos e regulatórios eficazes)	**D4.1** Marcos jurídicos **D4.2** Sistema de justiça penal **D4.3** Estruturas formais e informais de cooperação para o combate aos crimes cibernéticos
Dimensão 5 Normas, organizações e tecnologias (Controle dos riscos por meio de normas, organizações e tecnologias)	**D5.1** Observância de normas **D5.2** Resiliência da infraestrutura da Internet **D5.3** Qualidade do software **D5.4** Controles técnicos de segurança **D5.5** Controles criptográficos **D5.6** Mercado de cibersegurança **D5.7** Divulgação responsável

Figura 2: As cinco dimensões do CMM

Os dados primários usados neste relatório foram coletados por meio de um instrumento on-line distribuído a todos os Estados-membros da Organização dos Estados Americanos (OEA). Os dados coletados foram objeto de referência cruzada com uma pesquisa secundária e de consulta aos Estados-membros para a validação dos resultados declarados. Com o CMM como referencial, este relatório apresenta os resultados da análise de capacidade de cibersegurança da América Latina e Caribe com base em dados validados até dezembro de 2019. Cada perfil de país termina com uma tabela-resumo que lista as cinco dimensões e seus respectivos níveis de maturidade de acordo com os relatórios de 2016 e 2020.

Os valores de 2016 usados foram atualizados para refletir a edição revista do Modelo de Maturidade da Capacidade de Segurança Cibernética das Nações (CMM). Todas as avaliações realizadas na publicação de 2016 continuam inalteradas, exceto pela inclusão de novos indicadores.

Perfis de Países

Antígua e Barbuda

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Apesar de Antígua e Barbuda não ter adotado formalmente uma estratégia nacional de cibersegurança nem criado um CSIRT nacional, foram dados passos importantes para abordar a segurança cibernética no nível nacional. Em 2017, o governo criou o cargo de Diretor de Cibersegurança do Ministério da Informação, Radiodifusão, Telecomunicações e Tecnologia da Informação e nomeou um titular para o cargo em novembro do mesmo ano.

No que se refere a atividades de segurança cibernética, em março de 2016 Antígua e Barbuda participou da 2ª Reunião de Partes Interessadas do Caribe sobre Cibersegurança e Cibercrimes, organizada pela União de Telecomunicações do Caribe (CTU) em conjunto com o Secretariado da Comunidade Britânica, ocasião em que foi apresentado um plano de ação regional de segurança cibernética.[35] O plano de ação abrange áreas como capacitação, legislação, capacidade técnica e atividades policiais.[36] Além disso, em maio de 2017, Antígua e Barbuda sediou a Semana e Simpósio sobre TICs que, entre outros tópicos, discutiu segurança e crimes cibernéticos.[37] O país também colabora ativamente com organismos internacionais e regionais como a INTERPOL e a CARICOM IMPACS para a investigação de crimes digitais. Além disso, o Ministério da Informação, Radiodifusão, Telecomunicações e Tecnologia da Informação tinha em seu orçamento para o exercício de 2017 uma referência à contratação de especialistas para tratar de questões de segurança cibernética e da criação de um CSIRT.[38]

Apesar de limitados, Antígua e Barbuda tem alguns serviços de segurança cibernética prestados pelo setor privado. No entanto, o envolvimento do setor privado e da sociedade civil nas questões de segurança cibernética parece ser limitado, embora algumas empresas tenham começado a priorizar essa modalidade de segurança por meio da identificação de práticas de alto risco e se capacitando em cibersegurança.[39]

Antígua e Barbuda faz parte da campanha internacional STOP.THINK.CONNECT, que promove práticas seguras na Internet.[40] Quanto à disponibilidade de capacitação formal em segurança cibernética, embora não haja cursos específicos, o Instituto Internacional de Tecnologia de Antígua e Barbuda oferece cursos de graduação em TI e ciências da computação.[41] Em junho de 2013, o governo incluiu uma TIC nacional na sua política educacional.

O país dispõe de legislação sobre crimes eletrônicos e proteção de dados desde 2013. Mais especificamente, a Lei de Crimes Eletrônicos prevê a "prevenção e punição de crimes eletrônicos e ilícitos afins". A Lei de Proteção de Dados também promulgada em 2013, prevê a proteção das informações privadas armazenadas em bancos de dados públicos e privados e abrange tanto a proteção de dados pessoais quanto a transparência no seu processamento. [42]

Também houve avanços expressivos na oferta aos cidadãos de um número limitado de serviços governamentais virtuais, como a renovação da carteira de habilitação.[43] Em janeiro de 2018, Antígua e Barbuda sediou a Cúpula e Simpósio do Governo do Século 21, que trataram das formas mais eficazes de usar as TIC para a oferta e prestação de serviços aos seus cidadãos.[44] Este evento mostra a disposição de continuar avançando no desenvolvimento de suas capacidades de governo eletrônico.

Indicadores: Antígua e Barbuda

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia	■□□□□	■□□□□
Organização	■□□□□	■■□□□
Conteúdo	■□□□□	■□□□□
1-2 Resposta a incidentes		
Identificação de incidentes	■□□□□	■□□□□
Organização	■□□□□	■■□□□
Coordenação	■□□□□	■□□□□
Modo de funcionamento	□□□□□	■□□□□
1-3 Proteção de infraestruturas críticas (IC)		
Identificação	■■□□□	■■□□□
Organização	■□□□□	■■□□□
Gestão e resposta a riscos	■□□□□	■□□□□
1-4 Gerenciamento de crises		
Gerenciamento de crises	■□□□□	■□□□□
1-5 Ciberdefesa		
Estratégia	■□□□□	■□□□□
Organização	■□□□□	■□□□□
Coordenação	■□□□□	■□□□□
1-6 Redundância de comunicações		
Redundância de comunicações	■□□□□	■□□□□

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo	■□□□□	■■□□□
Setor privado	■■□□□	■■□□□
Usuários	■□□□□	■■□□□
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet	■□□□□	■■□□□
Confiança do usuário nos serviços de governo eletrônico	■□□□□	■■□□□
Confiança do usuário nos serviços de comércio eletrônico	■■□□□	■■□□□
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet	□□□□□	■□□□□
2-4 Mecanismos de denúncia		
Mecanismos de denúncia	□□□□□	■□□□□
2-5 Mídia e redes sociais		
Mídia e redes sociais	□□□□□	■■□□□

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Argentina

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Nos últimos anos, a Argentina adotou várias medidas para implementar políticas e mudanças administrativas e regulatórias nos seus setores de telecomunicações, Internet e tecnologia. Em 2017, a promulgação do Decreto n° 577/2017 levou à criação do Comitê de Segurança Cibernética, vinculado à Secretaria de Governo de Modernização da Chefia do Gabinete de Ministros, que contou com representantes do Ministério da Defesa e do Ministério da Segurança, a fim de dar continuidade ao desenvolvimento de uma estratégia nacional de cibersegurança.[46] Está em tramitação um projeto de lei administrativa que ampliará a composição do Comitê de Segurança Cibernética. A estratégia nacional de cibersegurança foi aprovada por meio da resolução 829/2019, que criou "a Unidade Executora"[47] no âmbito do Comitê de Segurança Cibernética, vinculada à Secretaria de Modernização da Nação, e convidou as províncias e a Cidade Autônoma de Buenos Aires para aderir à estratégia.[48]

Por meio de um empréstimo baseado em políticas (PBL, na sigla em inglês) aprovado em 2019, o BID auxilia o governo argentino na adoção de políticas relacionadas a infraestruturas críticas, segurança de dados pessoais e boas práticas no uso de TICs, com ações específicas para o fortalecimento das capacidades nacionais de cibersegurança.[49] Além de reforçar os laços internacionais e suas políticas de segurança cibernética, a Argentina firmou uma parceria com os Estados Unidos para criar um grupo de trabalho destinado a melhorar a cooperação em segurança cibernética.[50] Foram assinados convênios com países como Espanha e Chile e estão em análise memorandos de entendimento com Coreia, Rússia e China.[51]

A Argentina também criou um Programa Nacional de Infraestruturas Críticas para a Informação e Cibersegurança (ICIC), instituído pela Resolução JGM n° 580/2011, com vistas à criação e adoção de um marco regulatório para definir e proteger a infraestrutura estratégica e crítica dos setores público e privado, bem como de organizações interjurisdicionais.[52] Entre outras funções, o ICIC abriga o CSIRT nacional. Embora o ICIC-CERT não seja membro do CSIRT Américas, o BA-CSIRT (CSIRT da Cidade de Buenos Aires) é membro e pode se beneficiar da rede.

Embora o ICIC colabore com o setor privado, um relatório da PwC revelou que 53% das empresas pesquisadas na Argentina não têm uma estratégia geral de segurança cibernética, 61% não contam com um plano de contingência de resposta a incidentes e apenas 46% dispõem de um programa de segurança para os funcionários.[53]

Há várias oportunidades para os argentinos darem continuidade à sua formação em segurança cibernética, em universidades públicas e privadas e em cursos oferecidos pela sociedade civil. Além disso, o BA-CSIRT oferece capacitação e palestras de conscientização para ensinar as partes interessadas sobre segurança cibernética e uso de TICs. Quanto à legislação, em 2008 a Argentina promulgou a Lei n° 26.388, que alterou o código penal de modo a abranger os crimes cibernéticos.[54] Além disso, a Lei n° 26.904 incorporou ao código penal o aliciamento de menores pela Internet.

Danos a infraestruturas críticas e outros crimes serão tipificados em um projeto de lei a ser enviado em breve ao Congresso Nacional.[55] A adesão da Argentina à Convenção de Budapeste do Conselho da Europa sobre Crimes Cibernéticos foi ratificada em junho de 2018.[56]

A Lei n° 25.326, aprovada em 2000, trata da proteção de dados pessoais.[57] Na realidade, a Argentina foi um dos primeiros países do continente americano a instituir um marco regulatório para a proteção de dados pessoais, e desde então o fortaleceu e atualizou. Ela é um dos poucos países das Américas que participa da Convenção do Conselho da Europa para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais.[58] Em 2018, foi apresentado um projeto de lei que altera a Lei n° 25.326, com vistas a atualizar o atual marco regulatório.

A Argentina tem dois decretos sobre governo eletrônico: o Decreto n° 378/2005, que descreve a estratégia de governo eletrônico para ampliar as TICs com o intuito de melhorar a prestação e oferta de serviços governamentais[59] e o Decreto n° 87/2017, mais recente, para a criação de uma plataforma digital para facilitar a interação entre a população e o Estado.[60] O Decreto n° 996/2018 criou a Agenda Digital da Argentina, que envolve "o desenvolvimento de competências em segurança cibernética para gerar confiança nos ambientes digitais."[61]

Indicadores: Argentina

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Bahamas
(Comunidade das)

Habitantes
*Ref.:Banco Mundial**

Assinaturas de telefone celular
*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet
*Ref.:UIT***

Em 2014, o Governo da Comunidade das Bahamas iniciou esforços para o desenvolvimento de uma estratégia nacional de cibersegurança que contemplava a criação do CSIRT nacional.[62] A elaboração da estratégia de segurança cibernética e o estabelecimento de um CSIRT nacional são essenciais, visto que os crimes cibernéticos vêm aumentando nos últimos anos, apesar do país ter registrado uma redução geral dos crimes graves.[63] Embora a estratégia ainda não tenha sido adotada, em 2017 a Corporação Policial das Bahamas combinou a Seção de Rastreamento e Apreensão da Unidade de Repressão às Drogas com a Seção de Crimes Comerciais da Unidade Central de Detetives para criar a Unidade de Segurança Cibernética.[64] Essa unidade atua agora de forma centralizada em todo o país e tem a incumbência de proteger seu espaço digital.

Depois que o país foi classificado na 129ª posição no Índice Global de Cibersegurança (GCI, na sigla em inglês), os líderes do setor privado expressaram a necessidade de melhorias na prontidão cibernética do país.[65] Embora existam provedores de serviços e cursos sobre segurança cibernética no setor privado, persiste a necessidade geral de maior envolvimento do setor privado visando a proteção ativa contra ataques cibernéticos.

Em 2003, as Bahamas aprovaram legislação sobre crimes cibernéticos e proteção de dados, especificamente a Lei de Uso Indevido de Computadores e a Lei de Proteção de Dados. A primeira oferece um panorama completo dos atos ilícitos, bem como dos aspectos processuais das ações penais referentes a crimes cibernéticos,[66] ao passo que a segunda abrange as definições e procedimentos a serem observado pelos controladores de dados públicos e privados.[67] Além disso, o governo adotou a Lei de Comunicações e Transações Eletrônicas (2006).

O BID tem promovido e incentivado o fortalecimento das políticas e medidas de segurança cibernética nas Bahamas.

Por meio de um empréstimo intitulado Transformação Digital Governamental para Fortalecer a Competitividade, aprovado em 2018, o BID está prestando assistência técnica e financeira à agenda digital do país, que inclui um componente específico de segurança cibernética.[68]

O governo eletrônico faz parte da Declaração de Política das Bahamas sobre Comércio Eletrônico e da Agenda Digital das Bahamas de 2003, do Ministério das Finanças, com o objetivo de facilitar o intercâmbio de informações entre todos os ministérios e órgãos relacionados.[69] Já o projeto de 2016 do Plano de Desenvolvimento Nacional 2040 vai um passo além e descreve a necessidade de uma "estratégia de atendimento ao cidadão em guichê único".[70] Atualmente, o governo presta alguns serviços on-line por meio do portal de serviços eletrônicos para empresas, cidadãos/residentes e não residentes.[71]

Programas educacionais com foco em segurança cibernética não são comuns nas Bahamas. Embora o Instituto de Negócios e Tecnologia das Bahamas ofereça uma graduação em Tecnologia de Escritório de Negócios, não há cursos de graduação específicos em segurança cibernética.[72] O Instituto de Serviços Financeiros das Bahamas também oferece um Certificado Avançado em Segurança Cibernética; contudo, esse programa dura apenas três meses.[73] Finalmente, quanto aos esforços nacionais de conscientização, em maio de 2018 a Câmara de Comércio e Confederação de Empregadores das Bahamas (BCCEC, na sigla em inglês) realizou um Fórum de Segurança Cibernética e, em junho de 2018, o Banco Central das Bahamas organizou um seminário sobre segurança da informação para, entre outros temas, promover a conscientização em cibersegurança e crimes cibernéticos.[74] Em dezembro de 2019, o Governo das Bahamas e o BID realizaram uma conferência conjunta para o intercâmbio de experiências internacionais em segurança cibernética.

Indicadores: Bahamas (Comunidade das)

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Barbados

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Governo de Barbados está dando início a um diálogo com as partes interessadas para a criação de uma estratégia nacional de cibersegurança.[75] Esse processo de múltiplas partes interessadas se abre para receber contribuições de uma série de atores, permitindo assim o desenvolvimento de uma estratégia que atenda às necessidades de muitos intervenientes. Ademais, apesar de não dispor de uma estratégia de segurança cibernética, Barbados conta com um CSIRT nacional subordinado à Unidade de Telecomunicações do Ministério da Inovação, Ciência e Tecnologia Inteligente. O CSIRT também é integrante do CSIRT Américas, e se beneficia da natureza colaborativa da plataforma. O BID está cooperando com o Governo de Barbados para viabilizar suas iniciativas e políticas de segurança cibernética, que fortalecerão a capacidade do país para gerir as ameaças cibernéticas. Como resultado da operação de empréstimo "Programa de Modernização do Setor Público", aprovada em novembro de 2019, o BID está prestando assistência técnica e financeira à agenda digital do país, que prevê apoio específico para a segurança cibernética.[76]

No Fórum de Governança da Internet, realizado em Barbados em junho de 2017, houve destaque para a necessidade de mais campanhas de conscientização dos cidadãos, pois havia o consenso de que, apesar dos esforços de empresas do setor privado para tornar a segurança cibernética uma prioridade, os cidadãos podem não estar cientes das ameaças a que estão expostos ao usar a Internet.[77] É interessante observar que o Departamento de Processamento de Dados, a Unidade de Telecomunicações, a Força de Defesa e a Corporação de Investimento e Desenvolvimento de Barbados (BIDC na sigla em inglês) uniram forças com o Centro Israelense de Defesa Cibernética do Caribe (CICCD na sigla em inglês) para promover a conscientização sobre os riscos da segurança cibernética e sua importância para o país, principalmente à luz do novo Regulamento Geral sobre a Proteção de Dados (GDPR) da UE, que pode levar a multas elevadas em casos de violação da segurança cibernética de qualquer instituição que lide com informações de cidadãos da UE.[78] Além disso, apesar de existirem alguns provedores de serviços de segurança cibernética no setor privado, estes são limitados.[79]

Barbados tem a Lei de Uso Indevido de Computadores, que abrange legislação substantiva e processual sobre crimes cibernéticos.[80] Além disso, o país tem hoje projetos de lei sobre proteção e privacidade de dados, como o projeto da Lei de Proteção de Dados, que se aplicará a qualquer controlador de dados estabelecido em Barbados ou que use equipamentos situados no país para o processamento de dados.[81]

Barbados conta com uma estratégia de governo eletrônico de 2006, cuja visão é "empoderar os cidadãos de Barbados por meio da melhoria da funcionalidade, velocidade, eficiência, qualidade e variedade de serviços e informações fornecidos pelo governo".[82] O governo eletrônico também é mencionado em parte do Plano Estratégico Nacional de TICs 2010–2015, como uma ferramenta por meio da qual o governo pode se tornar um modelo para o uso de TICs na prestação de serviços. O Plano de TICs também requer um comitê diretor para supervisionar a implantação de uma política de governo eletrônico.[83] O primeiro-ministro anunciou em 2017 que uma estratégia de governo digital estava em processo de lançamento a fim de fornecer um roteiro para o trabalho que ainda precisa ser feito para a digitalização dos serviços prestados pelo governo.[84] Assim, Barbados está prestes a ter um caminho claro na direção da governança eletrônica. Além disso, Barbados deu grandes passos em tecnologias de ponta, como a tecnologia de blockchain, e vem realizando projetos para a implantação de uma rede de pagamentos digital.[85]

Finalmente, uma das próximas etapas delineadas em 2017 no Fórum de Governança da Internet foi a criação de uma parceria do Ministério da Educação, Ciência, Tecnologia e Inovação com a Internet Society, a Unidade de Telecomunicações e a Universidade das Índias Ocidentais com vistas a promover o conhecimento sobre o funcionamento da Internet desde a infância.[86] Quanto à educação complementar, não há cursos de graduação em segurança cibernética, embora a Universidade das Índias Ocidentais ofereça graduação em ciência da computação.[87]

Indicadores: Barbados

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Belize

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Governo de Belize está desenvolvendo atualmente uma estratégia nacional de cibersegurança por meio de um processo com múltiplas partes interessadas: a Força-Tarefa Nacional de Segurança Cibernética (CSTF, na sigla em inglês). A CSTF é encarregada de elaborar a estratégia nacional de cibersegurança por meio de um processo de consulta às partes interessadas do país. Além disso, Belize desenvolveu novas iniciativas relacionadas à tecnologia da informação, inclusive uma política nacional destinada a expandir os serviços de governo eletrônico no país. Na tentativa de promover a conscientização sobre os riscos e oportunidades relacionados à segurança cibernética, em abril de 2017 a Comissão de Serviços de Utilidade Pública de Belize (PUC, na sigla em inglês) organizou o Primeiro Simpósio Nacional sobre Cibersegurança na Cidade de Belize. Um dos objetivos do simpósio foi identificar as próximas etapas para a formulação de uma agenda de segurança e crimes cibernéticos, de modo que o país está prestes a deflagrar o processo.

A despeito da falta geral de conscientização e envolvimento do setor privado em relação à segurança cibernética em Belize, o Simpósio sobre Cibersegurança foi um impulso no sentido de ampliar a conscientização sobre a importância da segurança cibernética. A participação das forças policiais, das comunidades judiciária e jurídica, do governo e do setor privado é sinal da crescente importância do assunto para todas as partes.[88] A oferta de educação e capacitação em segurança cibernética continua a ser feita por empresas privadas. Não há cursos de graduação em segurança cibernética nas universidades de Belize, embora a Faculdade de Ciência e Tecnologia da Universidade de Belize ofereça o bacharelado em tecnologia da informação.[89]

Visando fortalecer a mentalidade de segurança cibernética, o Escritório Central de Tecnologia da Informação (CITO, na sigla em inglês) promove a conscientização sobre segurança cibernética entre as diferentes instituições governamentais, por meio do envio de pesquisas mensais com dicas e práticas recomendadas sobre segurança cibernética. O CITO também criou uma pesquisa para melhorar a notificação de incidentes cibernéticos entre as instituições públicas. A Unidade de TI do Departamento de Polícia de Belize também empreendeu esforços consideráveis para melhorar sua capacidade de reação a incidentes por meio da criação de um laboratório de criminalística. Atualmente, Belize tem quatro leis relacionadas à segurança cibernética: (i) a Lei de Telecomunicações, (ii) a Lei de Provas Eletrônicas, (iii) a Lei de Propriedade Intelectual e (iv) a Lei de Interceptação de Comunicações, mas não conta com legislação sobre privacidade e proteção de dados.[90] Já o Departamento de Polícia de Belize tem uma parceria com a Internet Watch Foundation para denunciar casos de pornografia infantil. No entanto, a falta de uma lei abrangente sobre crimes cibernéticos dificulta o julgamento de crimes cometidos no meio digital.[91] Há necessidade de atualizar a legislação do país e a estrutura de aplicação da lei para poder criminalizar e processar tais atos. O governo vem analisando as leis de crimes cibernéticos de países semelhantes para desenvolver sua própria legislação, que permita um processo mais eficiente para persecução de crimes cibernéticos.

Há um plano abrangente de governo eletrônico, que detalha o roteiro de criação e implantação, para atingir a visão de governo eletrônico do país, de "um governo integrado e colaborativo que preste serviços públicos seguros e de qualidade que conectem e empoderem as pessoas".[92] No entanto, até o momento ainda não foi implantado um portal de governo eletrônico.

Indicadores: Belize

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 — Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 — Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 — Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Bolívia

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Nos últimos anos, a Bolívia deu os primeiros passos para melhorar a segurança cibernética do país com a aprovação pelo Senado, em 2017, de uma lei que define o desenvolvimento de uma estratégia nacional de cibersegurança como prioritário para o país.[93] Além disso, o Decreto Supremo n° 2.514, de setembro de 2015, determinou a criação da Agência de Governo Eletrônico e de Tecnologias da Informação e Comunicação (AGETIC), com o objetivo de conduzir o processo de desenvolvimento e implantação de governo eletrônico e TICs visando a transformação da gestão pública e a construção da soberania científica e tecnológica do Estado Plurinacional da Bolívia.[94]

O Decreto Supremo n° 2.514 criou também o Centro de Gestão de Incidentes Informáticos (CGII), com a missão de proteger informações críticas para o Estado e promover a conscientização da segurança para prevenir e reagir a incidentes de segurança.[95] Adicionalmente, o CGII faz parte da plataforma CSIRT Américas, desenvolvida pela OEA, cujo objetivo é promover a colaboração, intercâmbio, incentivo e participação em projetos técnicos entre os CSIRTs nacionais, de defesa, de polícia e de governo dos países membros.[96]

O setor privado boliviano é atuante na área de cibersegurança. Diversas empresas oferecem serviços de cibersegurança e segurança e, de forma geral, o setor privado tem consciência da existência da segurança cibernética.[97]

Não há legislação específica sobre crimes cibernéticos ou proteção de dados pessoais, mas a legislação existente pode ser aplicada aos casos de crime cibernético, 98 acesso à informação[99] e outras questões correlatas. Do mesmo modo, uma seção separada sobre proteção de privacidade foi incorporada à constituição de 2009.

Na área de governo eletrônico, a Bolívia tomou medidas importantes para elaborar um plano para a implantação do governo eletrônico de 2017 a 2025.O objetivo desse plano é modernizar e tornar mais transparente a gestão pública do país, além de gerar e estabelecer um mecanismo tecnológico para ampliar a participação e a conscientização da sociedade com o uso das TICs pela população.[100] Além disso, em 2018 foi aprovada uma lei com a finalidade de "estabelecer as condições e responsabilidades para o pleno acesso e exercício da cidadania digital" na Bolívia.[101]

Existem cursos de graduação sobre temas relacionados à segurança cibernética. Há também oportunidades nos setores público e privado para formação em governo eletrônico e segurança cibernética.

Indicadores: Bolívia

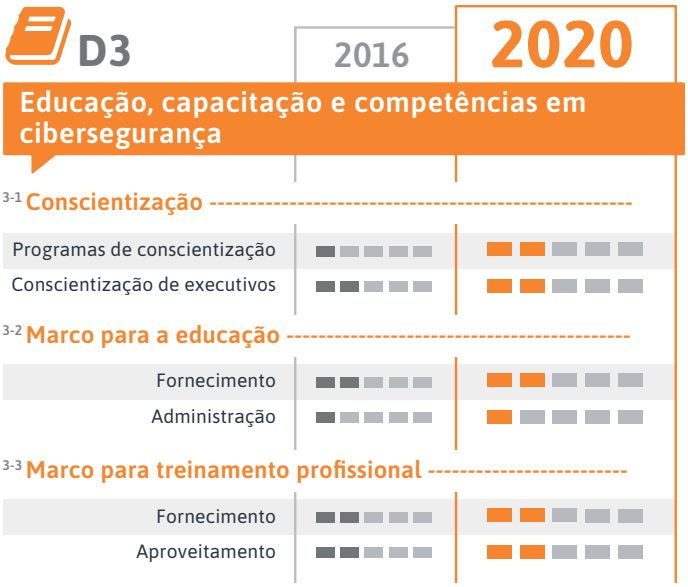
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

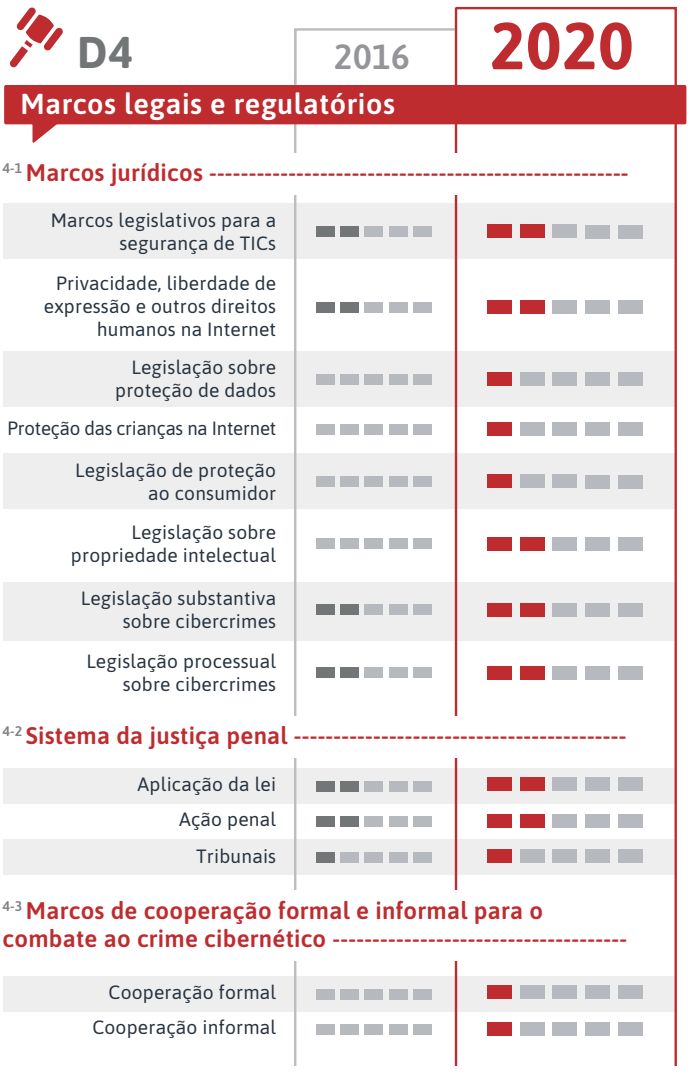
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

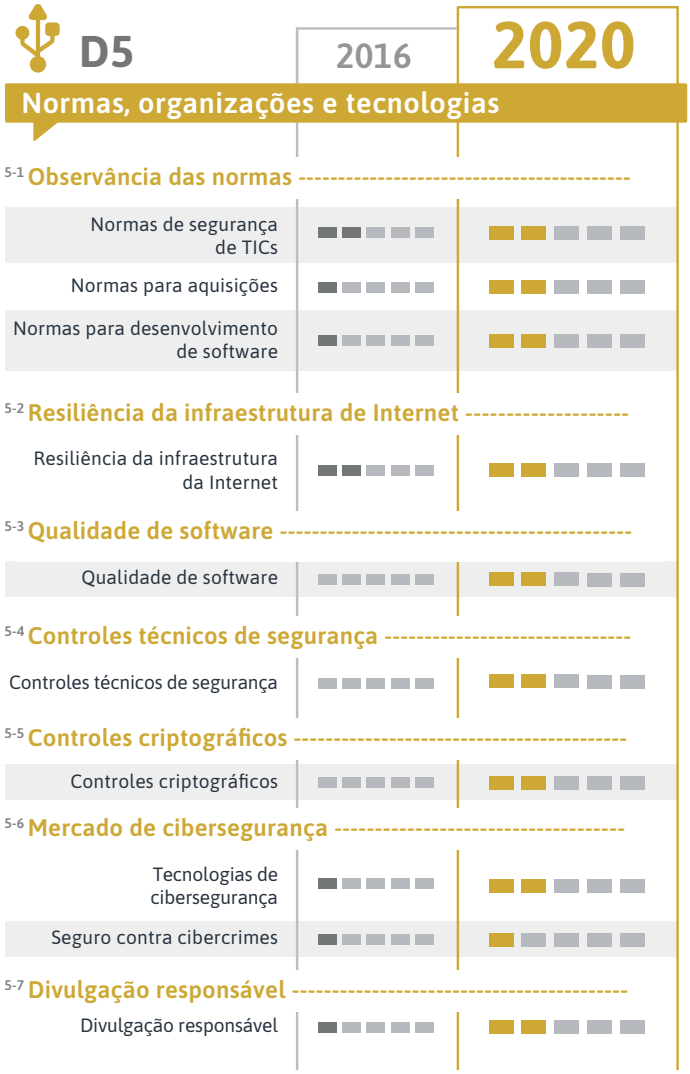
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Brasil

Habitantes

*Ref.:Banco Mundial**

2017

207.833.831

Assinaturas de telefone celular

*Ref.:UIT***

2017

218.255.041

Pessoas com acesso à Internet

2017

140.228.155

Penetração da Internet

*Ref.:UIT***

2017

67%

Em 5 de fevereiro de 2020, foi publicado o Decreto Federal nº 10.222 (o "Decreto"), que aprova a Estratégia Nacional de Segurança Cibernética.[102] Mais especificamente, o Decreto visa orientar a abordagem do Brasil à cibersegurança e prevê medidas para aumentar sua resiliência contra ameaças cibernéticas e fortalecer seu desempenho no plano internacional. O Decreto também cria um modelo de governança centralizado no nível nacional para promover a articulação entre os diferentes atores da área, criar um conselho nacional de cibersegurança e estimular verificações internas de conformidade de cibersegurança em entidades públicas e privadas.

O Brasil conta com numerosos CSIRTs, que vão desde entidades governamentais até instituições acadêmicas e do setor privado. A depender da função da CERT, essas entidades podem estar envolvidas exclusivamente na gestão da segurança dos sistemas, aplicar as diretrizes de segurança cibernética ou ser responsáveis pela coordenação de esforços entre as autoridades nacionais e as esferas municipais.

A maturidade da capacidade do Brasil para proteger as infraestruturas críticas difere entre os operadores públicos e privados dessas infraestruturas. Todas as instituições federais são obrigadas a realizar avaliações de risco cibernético, que são atualizadas anualmente com base nas lições aprendidas em grandes incidentes. Entre as partes interessadas de infraestruturas críticas públicas estão empresas de telecomunicações e instituições de transportes, energia e finanças, que cooperam e se articulam por meio de canais formais de comunicação com o Ministério da Defesa. Políticas e procedimentos claramente definidos são seguidos por todas as instituições públicas com base nas informações fornecidas pela ferramenta de consciência situacional da CERT nacional. A CERT nacional (CERT.br) continua a ser a principal entidade responsável pelo tratamento das notificações de incidentes no nível nacional e das atividades nas redes brasileiras.

Ainda está por ser criado um programa nacional de conscientização sobre segurança cibernética, a ser capitaneado por uma organização designada (de qualquer setor), que aborde uma grande variedade de dados demográficos. Contudo, o governo reconheceu a necessidade de priorizar a segurança cibernética em todas as suas instituições, e um número crescente de usuários e partes interessadas dos setores público e privado são considerados como detentores de conhecimento genérico de como as informações pessoais são manuseadas no meio virtual e empregam boas práticas (proativas) de segurança cibernética para proteger suas informações pessoais online.

O Marco Civil da Internet (Lei nº 12.965) foi desenvolvido por meio de um processo de consulta multilateral com o objetivo de regulamentar o uso da Internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para os usuários de internet. No entanto, o Brasil não dispõe de uma lei específica para a proteção de dados ou da privacidade[1], mas conta com diversos dispositivos da constituição federal:[103] o Código Penal,[104] o Código de Defesa do Consumidor[105] e o Marco Civil para a Proteção da Privacidade na Internet.

Chama a atenção que alguns aspectos dos processos governamentais e estruturas institucionais tenham sido criados em resposta aos riscos à segurança cibernética, mas as iniciativas são baseadas principalmente em determinados órgãos de destaque. Em termos gerais, a cultura de segurança cibernética no Brasil varia conforme a região do país e os diversos setores do governo e da economia. O setor financeiro e o setor de TI estão mais avançados em cibersegurança por serem alvos frequentes e, portanto, estão investindo mais na área. Não obstante, a sociedade como um todo ainda carece de uma mentalidade de segurança cibernética. Os usuários podem estar cientes dos riscos de segurança cibernética, mas muitas vezes deixam de agir da forma adequada no dia a dia.

A necessidade de aprimorar a educação em segurança cibernética nas escolas e universidades foi

[1] As informações expressas no perfil do País refletem a situação do momento da coleta dos dados. Desde então, o Brasil aprovou uma lei de proteção de dados em agosto de 2018(1). Também, em dezembro de 2018, a medida provisória 869/2018(2), emendou a Lei de Proteção de Dados e criou a Autoridade Nacional de Proteção de Dados, se consolidando na lei 13.853, de 8 de julho de 2019(3). Em decorrência dessas emendas, a Lei de Proteção de Dados (LGPD) do Brasil só entrou em vigor em setembro de 2020(4), ainda sem os artigos referentes às punições, que só entram em vigor em agosto de 2021.
(1) https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.
(2) http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869impressao.htm.
(3) http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm.
(4) https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/lei-geral-de-protecao-de-dados-entra-em-vigor.

identificada por importantes partes interessadas do governo e do setor privado. Qualificações para segurança cibernética e educadores nessa área estão prontamente disponíveis. Cursos especializados em ciências da computação são oferecidos em nível universitário. Profissionais do setor público fazem cursos profissionais de TI no exterior e recebem certificados de TIC com o aval de instituições internacionais, como Certificação Profissional em Segurança de Sistemas de Informação (CISSP) e Gestor Certificado em Segurança da Informação (CISM).

Finalmente, o governo federal adota uma estrutura de divulgação de vulnerabilidades. As organizações estabeleceram processos formais para divulgar automaticamente informações e a CERT nacional recebe essas informações e fornece relatórios completos sobre como lidar com os incidentes.

Indicadores: Brasil

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Chile

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Chile lançou sua Política Nacional de Cibersegurança em abril de 2017, com o objetivo de atingir os seguintes objetivos até o ano 2022: (i) contar com uma infraestrutura de informação robusta e resiliente; (ii) fazer com que o Estado garanta os direitos das pessoas no ciberespaço; (iii) elaborar uma estratégia de segurança cibernética baseada na educação, boas práticas e responsabilidade na gestão de tecnologias digitais, estabelecendo relações de cooperação em cibersegurança com outros atores; e (iv) fomentar o desenvolvimento de um setor de cibersegurança para atender a seus objetivos estratégicos.[106] Além disso, em 2018, de acordo com a Política Nacional de Cibersegurança, o presidente da república nomeou um assessor presidencial que o informa diretamente sobre as questões de segurança cibernética, e a Subsecretaria do Interior foi reestruturada para dar cumprimento às medidas descritas na referida política por meio da Unidade de Coordenação de Cibersegurança (Resolução Isenta n° 5.006).

Naquele ano, esse assessor promoveu uma série de medidas relacionadas aos objetivos estratégicos, uma dos quais foi o fortalecimento do CSIRT governamental vinculado ao Ministério do Interior e Segurança Pública,[107] de acordo com a Política Nacional de Cibersegurança.[108] Além disso, em março de 2018, foi aprovada a Política Nacional de Ciberdefesa, sendo criada uma unidade específica para a coordenação da defesa nacional, vinculada ao Ministério da Defesa, e outra para os setores industriais/estratégicos, vinculada ao Ministério da Fazenda. Por meio do recém-aprovado Programa de Fortalecimento da Gestão Estratégica da Segurança Pública no Chile, o BID e o Governo do Chile comprometeram-se a incluir um componente específico para reforçar a gestão estratégica da segurança pública com o intuito de assegurar "um espaço digital aberto, seguro e resiliente".[109] Paralelamente a isso, o BID apoia o governo chileno com assessoria técnica na avaliação dos níveis de prontidão e resposta em segurança cibernética, com o objetivo de identificar, planejar e projetar melhorias. O CSIRT do Governo do Chile também é membro do CSIRT Américas, o que permite o acesso a todas as informações que a plataforma oferece, inclusive a troca dinâmica de informações por meio da Plataforma de Compartilhamento de Informações sobre Malware e Compartilhamento de Ameaças (MISP) instalada na rede hemisférica.

O governo também coordena os órgãos reguladores financeiros em segurança cibernética e risco operacional em geral por meio do Grupo de Trabalho sobre Continuidade Operacional do Conselho de Estabilidade Financeira. O grupo tem como missão analisar os riscos operacionais da infraestrutura do mercado financeiro e de seus participantes e principais usuários, inclusive bancos, corretoras de valores, fundos de pensão e seguradoras, e propor as mudanças jurídicas e regulatórias necessárias para atenuar esses riscos e seus efeitos sobre o sistema financeiro. Os integrantes desse grupo de trabalho são do Ministério da Fazenda, do Banco Central do Chile, da Comissão do Mercado Financeiro e da Superintendência de Pensões, e costumam se reunir uma vez por mês. Uma das medidas para atingir o primeiro objetivo da estratégia de segurança cibernética é identificar e priorizar as infraestruturas de informação críticas do país. De acordo com a estratégia, "serão consideradas críticas, entre outras, a infraestrutura de informação dos setores de energia, telecomunicações, serviços de saneamento, saúde, serviços financeiros, segurança pública, transporte, administração pública, proteção e defesa civil".[110]

A estratégia também determina que o Ministério do Interior e Segurança Pública crie um grupo de trabalho permanente para estabelecer um marco regulatório paras infraestruturas críticas do Chile.[111] A estratégia determina ainda que "deve ser avaliada a pertinência de se criar um CSIRT de infraestruturas críticas". O setor privado, o setor acadêmico e a sociedade civil também têm sido atores ativos, auxiliando na elaboração da estratégia nacional de cibersegurança após a realização de uma consulta pública.[112]

A recém-criada Aliança Chilena de Cibersegurança reúne organizações públicas e privadas, bem como instituições acadêmicas, para, entre outras coisas, promover a educação e o uso responsável da tecnologia e gerar canais de comunicação entre o setor privado e o governo.[113] Entretanto, após os ataques cibernéticos de 2018, houve uma preocupação maior por parte das empresas, e as organizações do setor privado podem precisar fortalecer suas redes e sistemas.[114] Em todo caso, existem vários provedores de serviços de segurança cibernética no Chile.

O marco jurídico chileno está passando por modificações associadas aos crimes relacionados à computação e à proteção de dados pessoais. Contudo, na área de crimes cibernéticos, a Lei n° 19.223, de 1993, penaliza quem pratica atividades ilícitas em sistemas de informação.[115] Para a proteção de dados pessoais, o Chile aprovou a Lei n° 19.628.[116] Além disso, em 2018 foi aprovada uma reforma do inciso 4 do artigo 19 da Constituição Política da República do Chile, que reconheceu o direito à honra e à vida privada e introduziu a proteção de dados pessoais.[117] Atualmente, estão em tramitação no Congresso dois projetos de lei, um que modifica os regulamentos de Proteção de Dados Pessoais (Boletim n° 11.144-07118) e outro que adapta os regulamentos chilenos à Convenção de Budapeste sobre Crimes Cibernéticos, além de fazer modificações em outros órgãos jurídicos (Boletim n° 12.192-25[119]). Finalmente, existem iniciativas jurídicas em matérias financeiras — alterações na Lei Geral dos Bancos na área de risco operacional e a incorporação de regras específicas de Informação sobre Incidentes Operacionais (RAN 20-8) e Gestão da Continuidade de Negócios (RAN 20-9) da Comissão para o Mercado Financeiro (CMF).

Cabe observar que o governo assumiu o compromisso de apresentar o projeto do Marco de Cibersegurança até o final de 2019. Além dos esforços jurídicos nesta área, tem-se trabalhado na modificação dos órgãos reguladores com a finalidade de aperfeiçoar os padrões de segurança cibernética na administração do Estado e articular eficazmente as funções do Comitê Interministerial de Cibersegurança.

As Nações Unidas classificaram o Chile como o segundo país mais desenvolvido em termos de governo eletrônico na América Latina e Caribe em 2018.[120] Adicionalmente, o tema do governo digital faz parte da Agenda Digital 2020, que consiste em "um roteiro que define os próximos passos para alcançar uma política de desenvolvimento inclusiva e sustentável com o uso de Tecnologias de Informação e Comunicação (TICs)".[121] O governo eletrônico é um dos eixos da Agenda Digital 2020, juntamente com os Direitos para o Desenvolvimento Digital, a Conectividade Digital, a Economia Digital e as Competências Digitais.[122] Em 24 de janeiro de 2019, foi emitida uma Instrução Presidencial sobre Transformação Digital que previa quatro linhas de ação: Identidade Digital, Filas Zero, Papel Zero e Coordenação e Monitoramento.[123] Em 11 de novembro de 2019, foi publicada a Lei n° 21.180, sobre Transformação Digital,[124] que prevê uma reforma abrangente nos procedimentos administrativos no âmbito do Estado, instituindo o formato eletrônico para atos administrativos, além de promover o uso de plataformas de interoperabilidade entre os órgãos da administração pública, a criação de um repositório digital e a rastreabilidade de todas as comunicações entre os órgãos da administração do Estado.

Programas com a temática de segurança cibernética nos níveis de graduação, pós-graduação e especialização são oferecidos pelas universidades públicas e privadas no Chile. Há outras iniciativas em andamento, como a do Ministério da Educação, cujo projeto Internet Segura tem como objetivo "disponibilizar ferramentas a adultos para que possam acompanhar crianças e jovens em sua jornada digital" e "dar orientação às escolas de ensino fundamental e médio, de uma perspectiva mais pedagógica, para que possam formar cidadãos digitais conscientes de seus direitos e deveres".[125] Desde a promulgação da Política Nacional de Cibersegurança, tem sido promovido o desenvolvimento de diversos programas de educação continuada e pós-graduação nessa área, com uma abordagem tanto técnica como jurídica, com vistas a fortalecer os recursos humanos capacitados nessas questões.

Indicadores: Chile

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Colômbia

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

A Colômbia adotou uma segunda política nacional de segurança cibernética em 2016, cinco anos após a introdução da primeira.[126] O objetivo geral da política é fortalecer a capacidade do Estado para reagir às ameaças de segurança e a defesa cibernética do país. A nova política de segurança cibernética visa reforçar ainda mais as capacidades de todas as partes interessadas a fim de identificar, administrar, tratar e mitigar os riscos de segurança no meio digital.[127] Uma das principais contribuições da nova política é a criação da função de Coordenador Nacional de Segurança Digital, vinculada à Presidência da República da Colômbia.

Da mesma forma, o governo criou a principal entidade responsável por questões intersetoriais de segurança cibernética, o Comitê de Segurança Digital, que é dirigido pelo Coordenador Nacional de Segurança Digital.[128] Além disso, no âmbito de suas políticas de gestão e desempenho,[129] o governo incluiu pela primeira vez a política de segurança cibernética como parte integrante da operação estratégica de entidades públicas e privadas.

Simultaneamente, o Ministério de Tecnologia e Comunicações (MinTIC) implementou o Modelo de Segurança e Privacidade da Informação nos níveis nacional e local para auxiliar na gestão e adoção de normas e boas práticas para proteger ativos de informações críticas, infraestruturas tecnológicas e sistemas de informação e comunicação, fomentando assim o aprimoramento contínuo.

A Colômbia também criou a colCERT, uma equipe nacional de resposta a incidentes com computadores, atualmente subordinada ao Ministério da Defesa Nacional, a quem cabe a reação inicial aos incidentes cibernéticos e a proteção das infraestruturas cibernéticas nacionais críticas (ICCN).[130] Adicionalmente, foi desenvolvido um plano para fortalecer a proteção da infraestrutura digital crítica, utilizando o Guia para identificação de infraestruturas cibernéticas nacionais críticas (ICCN), que se somou aos planos setoriais de proteção da ICCN.[131] A fim de promover a transformação digital da Colômbia, no final de 2018 o BID aprovou o Programa para a Melhoria da Conectividade e Digitalização da Economia por meio de um empréstimo baseado em políticas (PBL, na sigla em inglês).[132] O programa especifica iniciativas para fortalecer os recursos nacionais de segurança cibernética. Embora o governo tenha adotado medidas significativas para proteger o espaço digital do país com as duas políticas de segurança cibernética, o setor privado (sobretudo as pequenas e médias empresas) ainda tem um longo caminho a percorrer para se preparar para as ameaças cibernéticas atuais.

Os colombianos têm amplas oportunidades de dar continuidade a seus estudos em segurança cibernética, tanto na graduação quanto na pós-graduação. Adicionalmente, o MinTIC concedeu bolsas de estudo a servidores públicos nas áreas de cibersegurança e ciberdefesa.[133] O MinTIC também patrocina cursos e capacitação em segurança cibernética para os diversos setores do funcionalismo público relacionados às TICs.[134] Diversos programas de formação foram conduzidos em colaboração com outras instituições, como o MinTIC, a OEA e a Citi Foundation, beneficiando 40 estudantes de engenharia de baixa renda.[135] Finalmente, a campanha "En TIC Confío" (Confio na TIC) do MinTIC visa promover e aumentar a conscientização sobre o uso responsável da Internet e das TICs.[136]

Os crimes cibernéticos estão previsto na Lei n° 1.273, de 2009, que altera o código penal de modo a tipificar esses crimes.[137] Visando a proteção e privacidade de dados, em 2012 a Colômbia promulgou a Lei n° 1581.[138] Adicionalmente, a Colômbia conta com um departamento designado para a proteção de dados pessoais[139] que, entre outras responsabilidades, tem a incumbência de assegurar o cumprimento de todas as normas relacionadas à proteção de dados e de informar os usuários de seus direitos relativos à proteção de dados pessoais. Essa lei se aplica a bancos de dados públicos e privados.

A Colômbia é membro da INTERPOL e da Europol[140] e priorizou sua participação no contexto internacional.[141] Além disso, a Lei n° 1928, promulgada em 24 de julho de 2018, aprovou a Convenção de Budapeste sobre Crimes Cibernéticos[142] e depositou o instrumento de adesão em 16 de março de 2020.

A política de governo eletrônico[143] está prevista no Decreto n° 1.008, de 2018. De acordo com esse decreto, entende-se por política de governo eletrônico "o uso e a exploração de tecnologias de informação e comunicação para consolidar um Estado competitivo, proativo e inovador, e cidadãos que geram valor público em um ambiente de confiança digital".

Indicadores: Colômbia

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Costa Rica

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Em 2017, o Ministério da Ciência, Tecnologia e Telecomunicações da Costa Rica apresentou a estratégia nacional de cibersegurança do país, que objetiva desenvolver um marco para orientar as ações do país no que se refere ao uso seguro das TICs, envidar esforços de articulação e cooperação entre as partes interessadas e promover medidas de conscientização, prevenção e mitigação de riscos com o uso de TICs.[144] Apesar do lançamento recente da estratégia nacional de cibersegurança, a Costa Rica já havia adotado medidas significativas para proteger seu espaço digital. Em 2012, por meio do Decreto nº 37.052, foi criado, no âmbito do Ministério, um CSIRT nacional para coordenar todas as matérias atinentes a segurança cibernética e da informação entre as diferentes partes interessadas e formar uma equipe de especialistas em segurança de TICs, com vistas a prevenir e responder a incidentes cibernéticos contra instituições governamentais.[145] O CSIRT-CR também é membro da rede CSIRT Américas.

A estratégia nacional define infraestruturas críticas como "sistemas e redes de informação que, em caso de falha, podem ter um sério impacto sobre a saúde, segurança física e operacional, economia e bem-estar dos cidadãos ou o funcionamento eficaz do governo e da economia do país." A estratégia também descreve a necessidade de definir as infraestruturas críticas do país e criar um comitê de formulação de políticas, composto por membros de entidades públicas e privadas que tenham sido classificadas como infraestruturas críticas.

O conhecimento do setor privado sobre questões de cibersegurança parece limitado, mas, a partir de 2017, começaram a proliferar empresas com foco no fornecimento de soluções e serviços de segurança cibernética.[146] Os costarriquenhos têm muitas oportunidades dar continuidade aos estudos em segurança cibernética, e algumas universidades oferecem programas de capacitação e certificação mais curtos.[147] Também foram realizados diversos eventos de capacitação em colaboração com instituições internacionais, como a capacitação oferecida pelo Centro Nacional de Criptologia da Espanha para servidores públicos e formação profissional em colaboração com a OEA e a Citi Foundation.[148]

Em 2012, a Costa Rica aprovou o Decreto Legislativo nº 9.048, que reformou o código penal e introduziu formalmente disposições relativas a crimes cibernéticos.[149] Algumas pessoas argumentam que essa medida não é suficiente, porque há problemas com a aplicação do marco, além de não ser exaustiva e deixar sem regulamentação crimes como o golpe do "chupa-cabra" (furto de dados do cartão de crédito), aliciamento infantil (fazer amizade com uma criança com a intenção de abuso) e perseguição/assédio no meio digital.[150] Em 2017, o país aderiu à Convenção de Budapeste sobre Crimes Cibernéticos e a outras convenções, e agora está desenvolvendo uma estratégia nacional de combate aos crimes cibernéticos.

No que se refere à privacidade e à proteção de dados, o país conta com a Lei nº 8.968, que dispõe sobre a proteção da pessoa contra o processamento de dados pessoais.[151] Essa lei se aplica a bancos de dados públicos e privados. Desde 2010, a Costa Rica conta com um projeto de estratégia de governo eletrônico, com vistas a se tornar referência na América Latina em termos de serviços de governo eletrônico com foco no cidadão, transparência no atendimento e interconexão das instituições governamentais com base em um ambiente favorável às TICs e o estabelecimento de uma sociedade igualitária e protegida.[152]

Indicadores: Costa Rica

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Administração

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Dominica

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

A Dominica ainda não implantou uma estratégia nacional de cibersegurança, mas elaborou um projeto em colaboração com a OEA, a Iniciativa de Crimes Cibernéticos da Comunidade e o Conselho da Europa. Esse projeto de estratégia define quatro pilares: (i) Governo e Legislação para fortalecer a capacidade de gerir os mecanismos de segurança cibernética e processar os criminosos cibernéticos; (ii) Cooperação entre as Partes Interessadas para atribuir as responsabilidades de segurança cibernética entre todas as partes afetadas; (iii) Construção de capacidades e Conscientização para assegurar a existência de profissionais com formação técnica suficiente para trabalhar na área de segurança cibernética; e (iv) Considerações Técnicas, que prevê a criação de um CSIRT nacional. Além disso, o projeto de estratégia define como infraestruturas críticas a rede elétrica, comunicações, métodos de execução financeira, águas e esgotos, transporte, alfândega, autoridades portuárias e domínio nacional de nível superior (ccTLD).

As oportunidades para os dominicanos fazerem capacitação em segurança cibernética são bastante limitadas. Embora não haja oferta de cursos específicos sobre questões cibernéticas em nível nacional, o Dominica State College oferece bacharelado em ciência da computação e TI.[153] Em parceria com a República da Índia, o governo também abriu o Centro de Excelência em TICs para oferecer aos cidadãos a oportunidade de aprender sobre essas tecnologias. Como próximo passo, o diretor de telecomunicações pretende explorar a criação de um Centro de Excelência em Cibersegurança.[154]

A Dominica promulgou recentemente diversas leis relacionadas ao espaço digital, como a Lei de Provas Eletrônicas (2010),[155] a Lei de Declarações Eletrônicas (2013),[156] a Lei de Transferência Eletrônica de Fundos (2013),[157] e a Lei de Transações Eletrônicas (2013).[158] Em relação à criminalização dos crimes cibernéticos, a Dominica possui o Projeto de Lei de Crimes Eletrônicos de 2013, que prevê a "prevenção e punição de crimes eletrônicos e ilícitos afins", mas que ainda não foi sancionado. Do mesmo modo, há o Projeto de Lei de Proteção de Dados que irá reger a proteção de informações privadas processadas por órgãos públicos e privados. No entanto, assim como o Projeto de Lei de Crimes Eletrônicos, o Projeto de Lei de Proteção de Dados ainda está sendo apreciado com vistas a sua aprovação.

Indicadores: Dominica

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Equador

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Embora ainda não disponha de uma estratégia de segurança cibernética, o Equador fez avanços expressivos no aprimoramento de suas capacidades cibernéticas, como a criação de um grupo de trabalho para a formulação de uma estratégia nacional de cibersegurança, iniciativa respaldada pela criação da EcuCERT, a equipe nacional de resposta a incidentes cibernéticos vinculada à Agência de Regulação e Controle das Telecomunicações (ARCOTEL).[165] Além disso, desde 2018 o BID vem prestando assessoria técnica ao Equador para identificar, avaliar e planejar os níveis de prontidão em segurança cibernética nacional a fim de lançar as bases técnicas, estratégicas, regulatórias e de governança para o governo usar na formulação da estratégia de segurança cibernética. É importante observar que a EcuCERT é filiada ao CSIRT Américas, de forma que pode se beneficiar da rede de colaboração, intercâmbio, incentivo e participação em projetos técnicos entre CSIRTs nacionais, de defesa, polícia e governo dos países membros. Adicionalmente, a Diretoria de Arquitetura Tecnológica e Segurança da Informação é responsável pela coordenação da segurança cibernética do país e tem como uma de suas tarefas a elaboração, avaliação, coordenação e gestão de programas governamentais de segurança cibernética.[166]

Embora haja a prestação de alguns serviços de segurança cibernética pelo setor privado, parece existir a necessidade de melhorar a conscientização e prontidão para enfrentar ameaças nessa área. Um estudo da Deloitte, realizado em 2018, revelou que 50% das empresas "implementaram um programa de conscientização dos funcionários sobre segurança cibernética". Em todo caso, o estudo apurou que "70% das organizações declaram não ter certeza da eficácia de seu processo de resposta a incidentes de cibersegurança" e o orçamento para essa área é o empecilho mais importante para as organizações.[167]

As universidades públicas e privadas oferecem alguns cursos e há oportunidades de capacitação voltadas para segurança cibernética e outros temas importantes relacionados às TICs. Contudo, o Equador enfrenta atualmente uma carência de profissionais de segurança cibernética.[168]

A Lei nº 2002-67, que dispõe sobre comércio eletrônico, assinaturas eletrônicas e mensagens de dados, penaliza os crimes cibernéticos e indica as reformas pertinentes do código penal. Já os artigos 229 a 234 do código penal[169] estabelecem o marco para o enquadramento de crimes contra ativos de sistemas de informação e comunicação.[170] Há previsão constitucional para a proteção e privacidade de dados.[171] A constituição determina que os cidadãos têm direito à proteção dos seus dados pessoais. Existem leis e regulamentos relacionados à proteção de dados pessoais, mas não uma lei específica sobre o assunto. Entretanto, existe atualmente um projeto de lei sobre a proteção da privacidade de dados pessoais,[172] que até o momento não foi transformado em lei.[173] Paralelamente, o Sistema Nacional de Registro de Dados Públicos (SINARDAP) está criando grupos de trabalho para analisar o anteprojeto que será apresentado à Assembleia Nacional.[174]

Em outra frente, o Equador estabeleceu o Plano de Governo Eletrônico 2014–2017, cujo objetivo é executar um modelo de governo eletrônico sustentável e inclusivo, que leve em consideração aspectos políticos, sociais e ambientais, com o intuito de consolidar um governo próximo, aberto, eficiente e eficaz.[175] Esse plano foi atualizado com o Plano Nacional de Governo Eletrônico 2018–2021, que considera os diferentes aspectos do primeiro e determina o que precisa ser aperfeiçoado.[176]

Finalmente, a Lei do Sistema Nacional de Compras Públicas, modificada em 2018, exige a segurança da informação durante todo o processo de compras e criou o Serviço Nacional de Compras Públicas (SERCOP), órgão autônomo responsável, entre outras coisas, pela definição das políticas e condições para o uso de informações e ferramentas eletrônicas e pela modernização das ferramentas relacionadas ao sistema eletrônico de compras públicas e de pregões eletrônicos.[177]

Indicadores: Equador

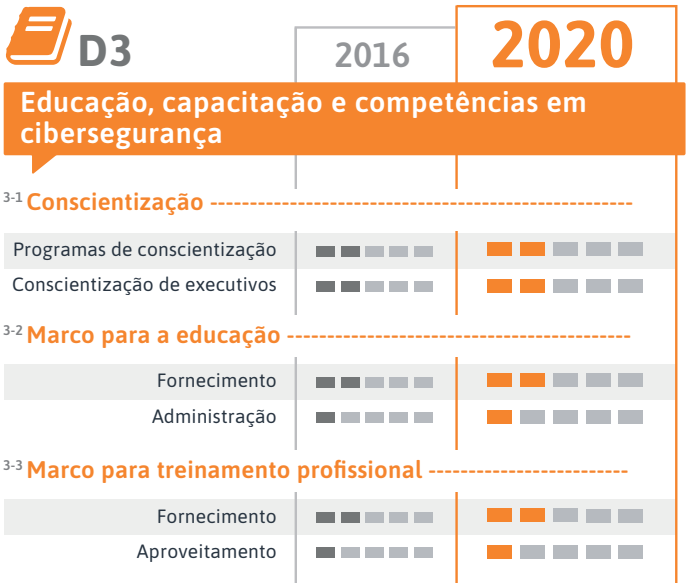
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

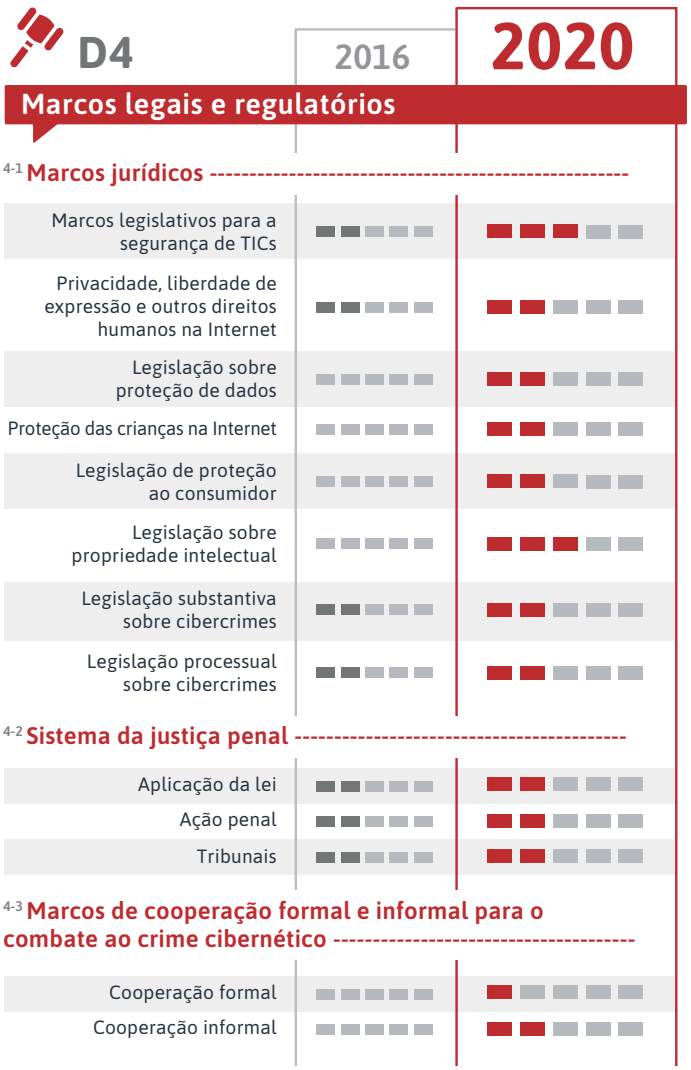
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

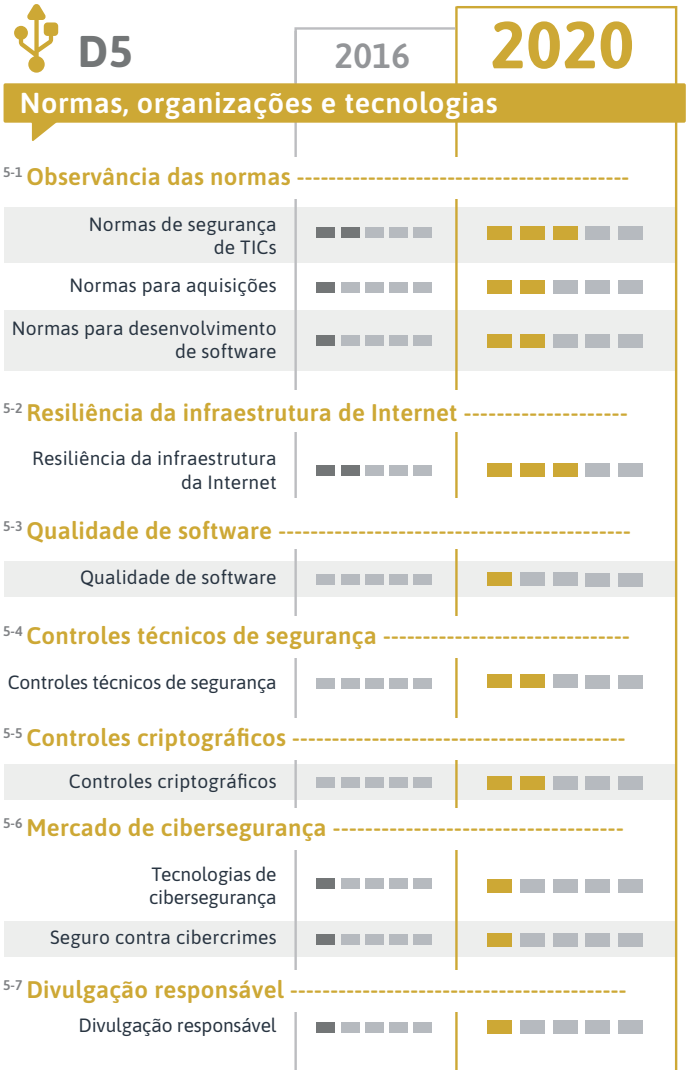
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



El Salvador

Habitantes
*Ref.:Banco Mundial**

Assinaturas de telefone celular
*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet
*Ref.:UIT***

Embora El Salvador não possua uma estratégia nacional de segurança cibernética, um dos objetivos da Estratégia de Governo Eletrônico 2018–2022[178] é dispor de uma Política Nacional de Segurança Cibernética, como "resultado de um processo de consulta envolvendo especialistas internacionais, instituições acadêmicas, instituições governamentais, o setor privado e organizações da sociedade civil".[179] O país tem um CSIRT reconhecido nacionalmente, o SalCERT, incumbido de responder a incidentes de segurança cibernética e articular-se com outras equipes de resposta.

Nos últimos anos, o país fez o intercâmbio de conhecimentos sobre temas como proteção de infraestruturas críticas e aperfeiçoamento da segurança cibernética com Israel, Coreia, Espanha e Equador, entre outros.[180]

O setor privado de El Salvador participa da oferta de serviços de segurança cibernética, desde análises até capacitações. No que se refere à educação em segurança cibernética, há oportunidades de estudo em algumas universidades, e algumas empresas privadas oferecem cursos de formação.[181] As empresas também tomaram conhecimento da existência de uma carência nessa área nas instituições de ensino superior.

A área em que El Salvador fez grandes avanços foi na legislação relativa aos crimes cibernéticos. Em 2016, foi aprovada a Lei Especial contra Crimes Informáticos com o objetivo de proteger os direitos legais contra delitos cometidos por meio das TICs, bem como a prevenção de crimes cometidos contra dados armazenados, processados e/ou transferidos.[182]

Os Artigos 24° a 26° do Decreto n° 260 da Lei Especial contra Crimes Informáticos referem-se à proteção contra o uso, comercialização, transferência e divulgação indevida de dados pessoais. Já o Decreto n° 133[183] da Lei da Assinatura Eletrônica protege os dados pessoais necessários para o trabalho dos prestadores de serviços. No entanto, não há uma legislação abrangente sobre o assunto, de modo que a proteção de dados e a privacidade não são tratadas de forma adequada.

Além do desenvolvimento da Estratégia de Governo Eletrônico 2018–2022,[184] El Salvador tomou algumas medidas concretas para implementar o governo eletrônico, como o lançamento da versão preliminar do Sistema de Gestão Administrativa Integrada, bem como da Política Nacional de Dados Abertos que aderiu ao novo Datos.gob.sv, portal que abriga mais de 20 bases de dados públicos.[185] Além disso, em 2016 foi criado o Escritório de Governo Eletrônico, responsável pela articulação de iniciativas com instituições públicas, e está em funcionamento desde o início de 2017[186] uma plataforma para facilitar o intercâmbio de informações governamentais seguindo as diretrizes de segurança.[187]

Indicadores: El Salvador

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Granada

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Em 2014, a Comissão Nacional de Regulamentação de Telecomunicações de Granada sinalizou que estava trabalhando com o governo para definir uma estratégia de segurança cibernética, o que também permitiria a criação de um CSIRT nacional.[188] No entanto, até o momento não houve mais notícias a respeito. Nesse sentido, o governo tem investido em vários projetos relacionados às TICs, como "One Tablet One Child" ("um tablet para cada criança", em tradução livre), do Ministério da Educação, além de um banco de dados centralizado para facilitar a oferta de serviços governamentais on-line aos cidadãos. Fora isso, há poucas evidências de articulação entre o governo e os proprietários de ativos críticos de infraestrutura.[189]

Em termos gerais, a sociedade civil e o setor privado têm conhecimento e consciência limitados sobre a segurança cibernética. Sem mecanismos de denúncia, é muito difícil dar visibilidade aos crimes cibernéticos. No quesito educação e capacitação, a formação em TI faz parte da Estratégia de TICs de Granada, cujo objetivo é ser "centrada no cidadão, com foco na oferta de níveis melhores de atendimento ao cliente e maior satisfação do cidadão". Contudo, ainda são muito limitadas as oportunidades locais de capacitação específicas em segurança cibernética.

Em 2013, Granada adotou o Projeto de Lei de Crimes Eletrônicos, que visa incluir os crimes eletrônicos no código penal. O projeto de lei define crimes específicos, bem como o procedimento para investigá-los.[190] Embora não disponha de legislação para a proteção e privacidade de dados, Granada faz parte da Organização dos Estados do Caribe Oriental, que possui uma Lei de Proteção de Dados aplicável à forma como os dados são processados nos Estados-membros.[191]

Granada tem uma estratégia de governo eletrônico como parte da Estratégia de TICs 2006–2010.[192] Além disso, o país também é integrante da Estratégia de Governo Eletrônico da CARICOM 2014, cujo objetivo é oferecer melhorias sustentáveis à prestação de serviços públicos com o uso de TICs.[193] Contudo, há poucas evidências que sugiram que tenham sido feitos avanços na prestação de serviços públicos eletrônicos.[194]

Indicadores: Granada

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Guatemala

Habitantes

*Ref.:Banco Mundial**

2017

16.087.418

Assinaturas de telefone celular

*Ref.:UIT***

2017

19.986.482

Pessoas com acesso à Internet

2017

10.456.822

Penetração da Internet

*Ref.:UIT***

2017

65%

Juntamente com a República Dominicana, a Guatemala é o país mais recente da região a ingressar no grupo de nações com estratégias nacionais de cibersegurança. Em junho de 2018, o governo lançou sua estratégia nacional de segurança cibernética, com o objetivo de fortalecer as capacidades da nação, criando assim o ambiente e as condições necessárias para garantir a participação, o desenvolvimento e o exercício dos direitos humanos no espaço digital.[195] Além disso, o CSIRT-gt da Guatemala é uma equipe de resposta a incidentes sob a supervisão do Ministério do Interior[196] e membro da rede CSIRT Américas.

Embora a Guatemala ainda não tenha uma definição formal de infraestrutura crítica, uma das etapas estabelecidas no eixo legislativo da estratégia de segurança é criar, aprovar e implementar uma Lei de Infraestruturas Críticas para identificar e analisar as principais características dos setores que prestam serviços essenciais e definir medidas de prevenção, proteção e recuperação contra ameaças.

A Guatemala tem vários prestadores de serviços de segurança cibernética, bem como uma CERT para o setor privado.[197] Além disso, algumas empresas têm procurado promover a conscientização sobre segurança cibernética.[198] Da mesma forma, o Capítulo Guatemala da Internet Society conta com um grupo de trabalho que, entre outras coisas, visa promover a conscientização sobre segurança cibernética e oferecer oficinas sobre gerenciamento de incidentes.[199]

Embora não haja muitas oportunidades para dar continuidade à educação superior em segurança cibernética, estão disponíveis algumas opções de educação complementar. Já a estratégia nacional de cibersegurança apresenta um eixo educacional com o objetivo de aumentar a oferta de educação e capacitação em segurança cibernética para atender à demanda técnica e profissional de todos os setores. Também houve vários eventos de capacitação oferecidos pelo governo em parceria com outras entidades, como a oficina sobre ameaças cibernéticas[200] ou a formação para o primeiro CSIRT em colaboração com a OEA.[201]

A Guatemala está em processo de elaboração de legislação específica para crimes cibernéticos. No entanto, a Iniciativa Legislativa nº 5.254, de 2017, "prevê a aprovação de uma lei contra os crimes cibernéticos".[202] O projeto de lei "visa ordenar medidas de prevenção e punição de atos ilícitos cometidos no meio digital, com o uso de dispositivos tecnológicos, mensagens de dados, sistemas ou dados computacionais, bem como medidas de proteção contra exploração, pornografia e outras formas de abuso sexual a menores e que são executados por meio de sistemas informatizados".[203] De modo similar, há uma iniciativa legislativa para a proteção e privacidade de dados, que se aplicará a bancos de dados dos setores público e privado.[204]

A Guatemala ainda não dispõe de uma estratégia de governo eletrônico, mas este é um dos eixos de ação da Comissão Presidencial de Gestão Pública Aberta e Transparência, que tem como missão apoiar as ações dos ministérios e instituições do poder executivo para dar continuidade à aplicação das medidas oriundas das convenções internacionais sobre transparência, governo eletrônico, combate à corrupção e governo aberto.[205]

Com o apoio da OEA e do Conselho da Europa, a Lei de Combate ao Crime Cibernético foi apresentada em março de 2017. Em abril de 2020, a Guatemala foi convidada a aderir à Convenção de Budapeste.

Indicadores: Guatemala

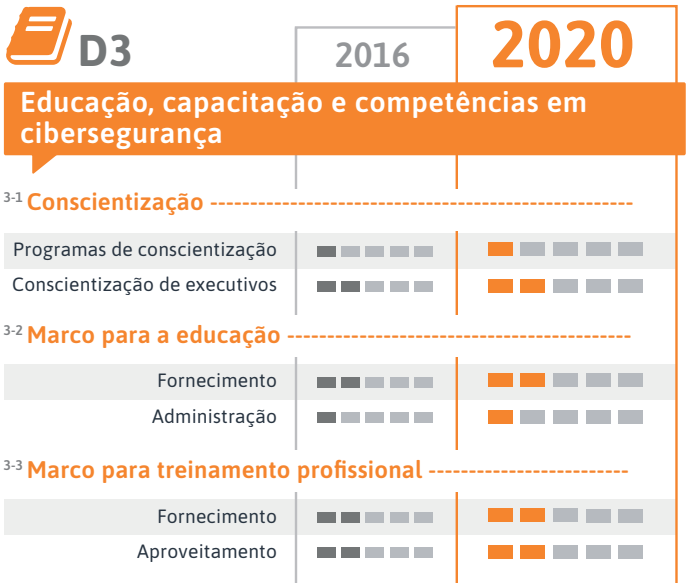
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

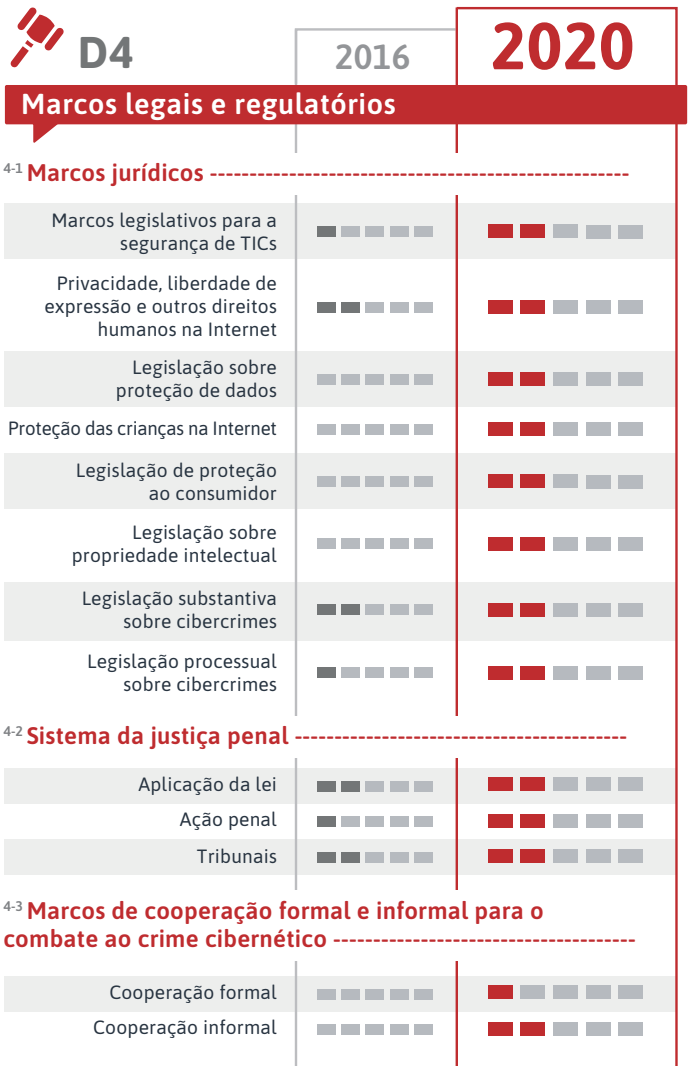
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

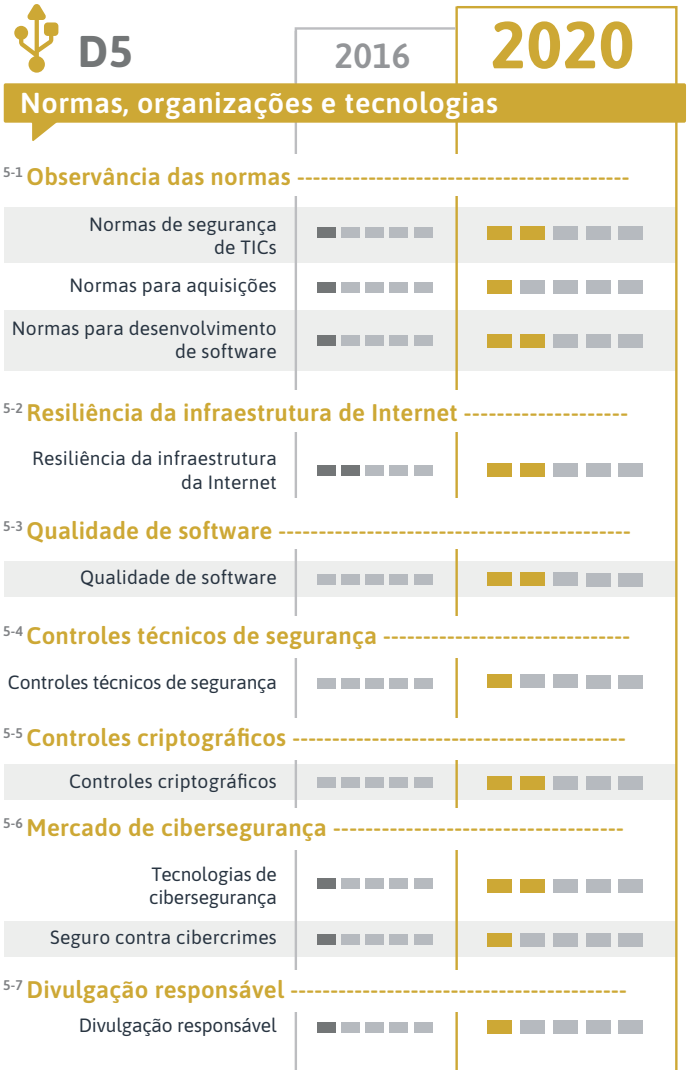
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Guiana

Habitantes

*Ref.:Banco Mundial**

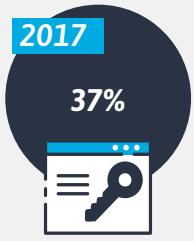
Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***



Em março de 2019, foi criado o Grupo de Trabalho Nacional sobre Estratégia de Cibersegurança para elaborar uma estratégia nacional sob a orientação da OEA. Como parte dessa iniciativa, e em parceria com a OEA, foi realizada uma consulta nacional às partes interessadas em julho de 2019. Um anteprojeto de estratégia está sendo apreciado no momento. Em 2013, o país instituiu seu CSIRT nacional, o CIRT.GY,[206] com a missão de "melhorar a prontidão e resposta da segurança cibernética nacional por meio de medidas de segurança proativas e mecanismos de compartilhamento de informações". Os serviços são oferecidos aos setores público e privado, bem como a integrantes da sociedade civil afiliados à Guiana. O CIRT.GY é vinculado ao Ministério das Telecomunicações Públicas.[207] Além disso, o CIRT.GY é membro do CSIRT Américas, aproveitando a natureza colaborativa dessa rede, e também firmou parceria com outras CERTs na Estônia, Colômbia e Países Baixos.

Ainda não há no mercado muitos provedores privados de serviços de cibersegurança e o foco da segurança cibernética para executivos está na fase reativa. No entanto, a segurança cibernética está se transformando em tema mais frequente nas discussões em nível gerencial. Por outro lado, as instituições da sociedade civil ainda não estão cientes da importância das boas práticas nessa área.[208]

A Guiana oferece algumas oportunidades de capacitação em segurança cibernética. Há alguns cursos de bacharelado em ciência da computação e TI. Apesar de não existir um programa exclusivo sobre segurança cibernética, um curso de pós-graduação em Segurança de Redes é oferecido no recém-lançado Centro de Excelência em Tecnologia da Informação, resultado de um acordo bilateral entre o Governo da Índia e o Governo da Guiana. Esse programa inicialmente era voltado para o setor público, mas há planos de ampliar o público-alvo para incluir o setor privado.

O governo tomou várias medidas para promover a conscientização sobre a segurança cibernética. Em abril de 2019, a Guiana se beneficiou de uma campanha de conscientização e sensibilização pública elaborada pelo Programa de Segurança Cibernética do Reino Unido, cujo fator determinante foi o lançamento do site www.getsafeonline.gy.[209]

Em setembro de 2019, o Ministério das Telecomunicações Públicas colaborou com a Get Safe Online para organizar uma oficina de treinamento em conscientização sobre segurança cibernética, tendo como participantes 124 servidores públicos de 50 órgãos. Mais adiante, em outubro de 2019, em comemoração ao mês de conscientização sobre segurança cibernética, foi realizada uma campanha nacional de conscientização pública com entrevistas pelo rádio, anúncios nas redes sociais e sessões de conscientização em instituições de ensino médio e superior, bem como no setor público.

No que tange aos crimes cibernéticos, em 2017 a Força Policial da Guiana, em colaboração com o setor privado, abriu um centro de segurança cibernética com o objetivo de instruir a polícia, a comunidade empresarial e a população a reagir aos crimes cibernéticos.[210] Em janeiro de 2019, a Força Policial da Guiana formalizou a criação de uma unidade de crimes cibernéticos para investigar e processar crimes cometidos com o uso de tecnologias da computação. A legislação de crimes cibernéticos foi promulgada em 2018, após dois anos de tramitação.[211, 212] A legislação abrange uma série de crimes cibernéticos e métodos de sanção.[213] A Guiana ainda não aprovou legislação sobre privacidade e proteção de dados.[214]

A estratégia de governo eletrônico da Guiana tem como fundamento a Estratégia de Desenvolvimento do Estado Verde: Visão 2040. Essa é a política nacional de desenvolvimento da Guiana para um período de 20 anos, que reflete a visão e os princípios orientadores de sua agenda verde. O objetivo central é o desenvolvimento que proporcione melhor qualidade de vida para todos os guianenses, derivada das riquezas naturais do país: sua diversidade humana e abundância de recursos naturais (terra, água, florestas, minerais e agregados, biodiversidade). O uso correto das TICs pode melhorar a vida de todos os guianenses e, portanto, constitui um componente transversal da Estratégia de Desenvolvimento do Estado Verde: Visão 2040. As TICs têm o potencial de dotar os serviços governamentais de mais alcance, eficiência e interatividade, bem como de atuar como estímulo à atividade de novas empresas ecológicas.[215]

Indicadores: Guiana

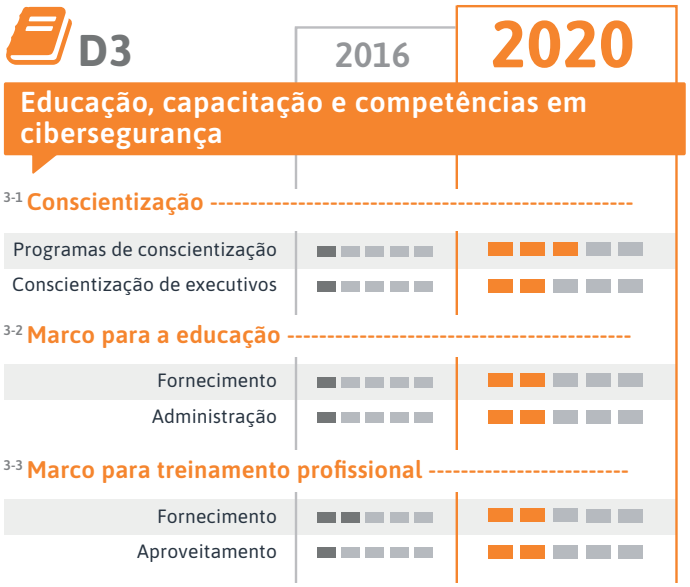
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

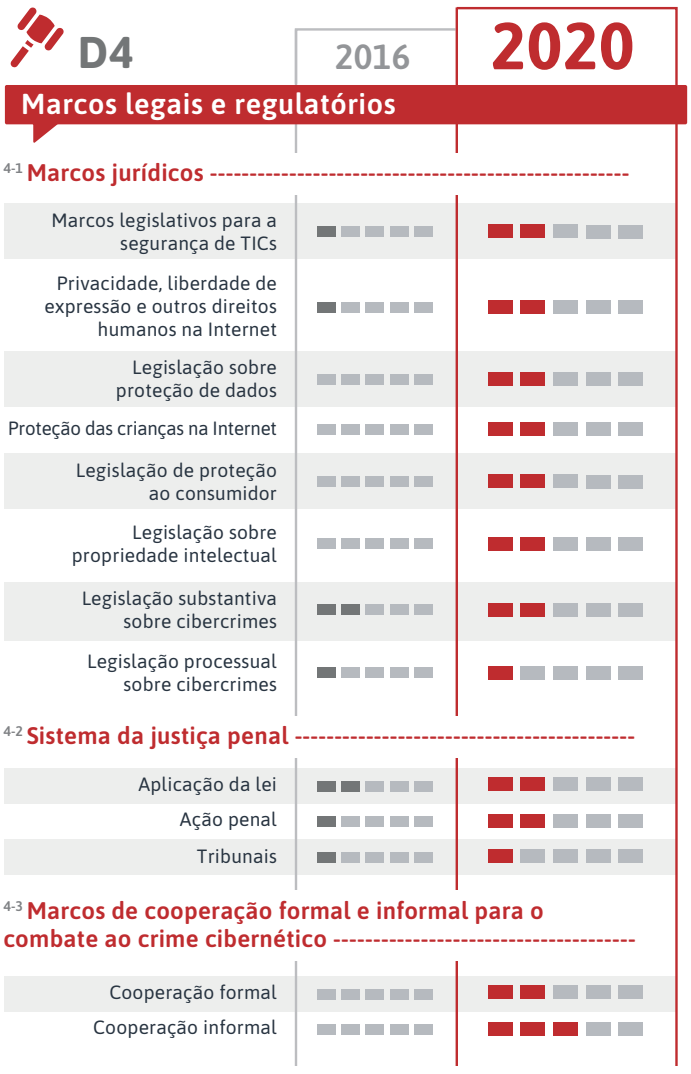
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

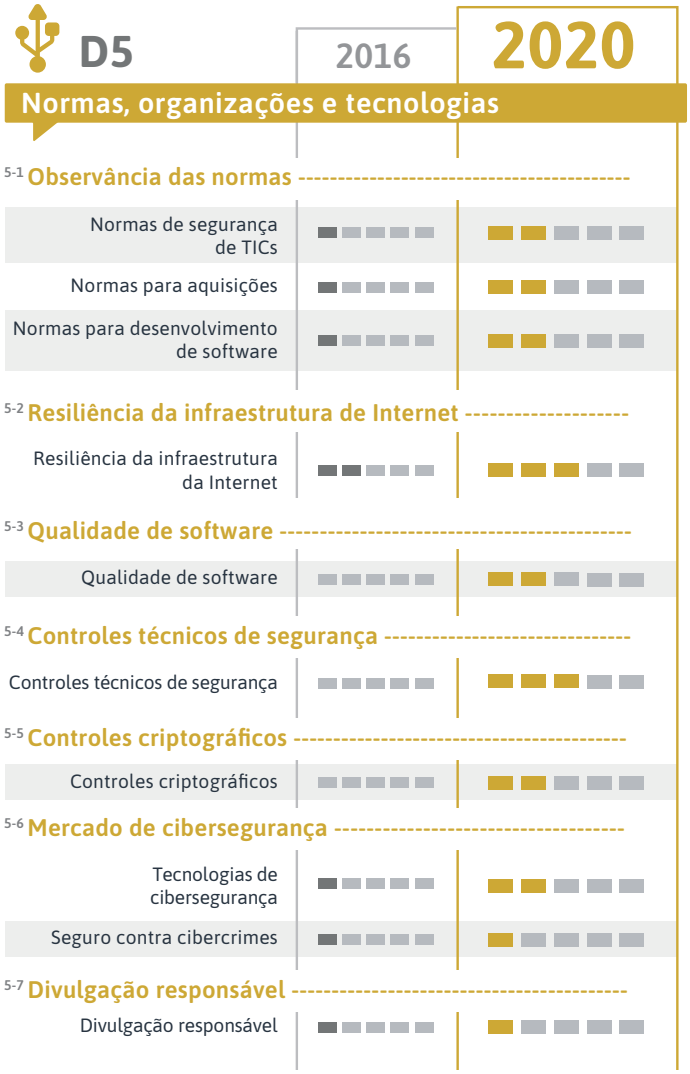
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Haiti

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Haiti não possui uma estratégia nacional de cibersegurança nem um CSIRT nacional. Contudo, o governo está ciente da importância crescente da segurança cibernética e tomou medidas nesse sentido. Em 2015, o Ministério de Obras Públicas, Transportes e Comunicações constituiu um grupo de trabalho sobre cibersegurança e crimes cibernéticos (GTCSC), com a missão de desenvolver e aplicar uma estratégia nacional de cibersegurança. Em 2016, esse grupo apresentou um seminário a respeito de projetos de lei sobre cibersegurança, crimes cibernéticos, interceptação de comunicações e transações e evidências eletrônicas, com participantes do setor bancário, operadoras de telefonia celular, provedores de serviços de Internet, a polícia nacional, o Ministério da Segurança Pública e outras instituições de Estado, várias entidades da Universidade de Estado do Haiti e os presidentes das comissões permanentes de telecomunicações, informação e comunicação das duas casas do parlamento.[216] Em maio de 2018, uma delegação do Centro de Informação de Redes da América Latina e Caribe se reuniu com o diretor geral do Conselho Nacional de Telecomunicações (CONATEL) para discutir, entre outros assuntos, a colaboração para a criação de um CSIRT nacional.[217]

No setor privado, há a preocupação de que as instituições públicas e privadas não estejam cientes dos riscos para seus sistemas; elas deveriam fazer uma "auditoria tecnológica" periódica para identificar as eventuais vulnerabilidades.[218] À medida que os haitianos intensificam o uso pessoal e profissional das redes, o risco cibernético aumenta, o que gera a necessidade de políticas e legislação para regulamentar o espaço digital, algo que o país ainda não possui.[219] Em termos gerais, o setor privado parece ter boa consciência da importância da cibersegurança. Ademais, há atores envolvidos na realização de eventos de conscientização e na condução de oficinas e capacitações em segurança cibernética, como a Haiti Cybercon.[220]

Há oferta de cursos sobre segurança cibernética, embora não existam graduações específicas nessa área. Entretanto, o Haiti enviou participantes para capacitações organizadas pela OEA em 2017 e 2018, como o Summer Bootcamp organizado pela OEA e o INCIBE e para a Oficina Sub-regional sobre Proteção de Infraestruturas Críticas, no Panamá.[221]

No momento, o Haiti ainda não possui legislação sobre crimes cibernéticos nem sobre proteção de dados e privacidade.[222] No entanto, a legislação sobre crimes cibernéticos está em processo de desenvolvimento, conforme demonstrado pelo seminário de 2016 para a apresentação de projetos de lei sobre o tema. Há poucos indícios de desenvolvimento de legislação referente à proteção e privacidade de dados.

Embora o Haiti careça de uma estratégia específica de governo eletrônico, parte de seu Plano de Desenvolvimento Estratégico 2030 versa sobre a modernização digital da administração pública.[223] O país conta com uma plataforma de governo integrada,[224] mas ainda não oferece serviços de governo eletrônico a seus cidadãos.[225]

Indicadores: Haiti

D1 Política e Estratégia de Cibersegurança

2016 | 2020

1-1 Estratégia nacional de cibersegurança

- Desenvolvimento da estratégia
- Organização
- Conteúdo

1-2 Resposta a incidentes

- Identificação de incidentes
- Organização
- Coordenação
- Modo de funcionamento

1-3 Proteção de infraestruturas críticas (IC)

- Identificação
- Organização
- Gestão e resposta a riscos

1-4 Gerenciamento de crises

- Gerenciamento de crises

1-5 Ciberdefesa

- Estratégia
- Organização
- Coordenação

1-6 Redundância de comunicações

- Redundância de comunicações

D2 Cibercultura e Sociedade

2016 | 2020

2-1 Mentalidade de cibersegurança

- Governo
- Setor privado
- Usuários

2-2 Confiança e segurança na Internet

- Confiança e segurança do usuário na Internet
- Confiança do usuário nos serviços de governo eletrônico
- Confiança do usuário nos serviços de comércio eletrônico

2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet

- Compreensão do usuário sobre proteção de informações pessoais na Internet

2-4 Mecanismos de denúncia

- Mecanismos de denúncia

2-5 Mídia e redes sociais

- Mídia e redes sociais

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Honduras

Habitantes

*Ref.:Banco Mundial**

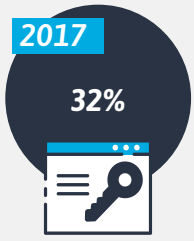
Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***



Honduras desenvolveu o projeto de Lei Nacional de Segurança Cibernética e Medidas de Proteção contra Atos de Ódio e Discriminação na Internet e Redes Sociais, que identifica a necessidade de criar uma estratégia nacional de cibersegurança e de um comitê interinstitucional de cibersegurança, responsável pela formulação e implementação da estratégia.[226] Honduras também chegou a um acordo com Israel em 2016 para a cooperação com foco no "fortalecimento das capacidades de prevenção, defesa e reação a possíveis ataques cibernéticos a instituições governamentais, gestoras de infraestrutura e serviços críticos".[227] Por outro lado, por meio do programa "Transformação Digital para Maior Competitividade", o BID e o Governo de Honduras estão colaborando para modernizar a rede de segurança cibernética do país.[228]

Honduras ainda não dispõe de um CSIRT nacional, mas há entidades privadas que prestam serviços de resposta a incidentes. Embora ainda haja muito a ser feito em termos de provedores de serviços de cibersegurança, as principais empresas do setor privado começaram a priorizar o assunto e a tomar medidas nesse sentido.[229]

O governo hondurenho adotou várias ações para fortalecer as oportunidades de formação em segurança cibernética para seus servidores públicos e as forças armadas. Para começar, as Forças Armadas de Honduras assinaram um acordo com o México que é "o marco para melhorar as áreas de cooperação em capacitação naval e militar, formação e educação, segurança e defesa nacional, segurança cibernética e defesa cibernética".[230] Além disso, a CONATEL, a Comissão Nacional de Telecomunicações, organizou uma oficina de dois dias sobre segurança cibernética como parte de uma estratégia nacional,[231] e, embora limitada, há oferta de cursos sobre segurança cibernética, inclusive cursos introdutórios virtuais gratuitos.

Honduras conseguiu alguns avanços em termos de legislação. O Congresso está examinando a Lei de Segurança Cibernética, vinculada à Lei Nacional de Segurança Cibernética e Medidas de Proteção contra Atos de Ódio e Discriminação na Internet e Redes Sociais. Para proteger os dados e a privacidade, o projeto de lei sobre a proteção de informações pessoais foi aprovado no Congresso Nacional após o terceiro e último debate, em abril de 2018.[232] Essa nova lei se aplica a bancos de dados dos setores público e privado.[233]

No que se refere ao avanço da tecnologia, o governo eletrônico constitui um dos quatro eixos estratégicos da Agenda Digital de Honduras 2014–2018. O objetivo é promover as TICs para criar um novo modelo de administração pública visando melhorar a prestação de serviços e informações, bem como aumentar a eficiência, eficácia e transparência do setor público. As principais iniciativas são a criação de uma rede governamental que compreende um portal governamental, um call center, um sistema eletrônico de compras públicas, um portal de negócios, um guichê para o sistema aduaneiro eletrônico, um banco de dados governamental e um sistema nacional de certificação digital.[234]

Indicadores: Honduras

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Jamaica

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Em janeiro de 2015, a Jamaica divulgou sua estratégia nacional de cibersegurança com quatro objetivos principais: definição de medidas técnicas para a proteção e resposta eficientes a ataques cibernéticos, ampliação dos recursos humanos e construção de capacidades na área de segurança da informação, aperfeiçoamento do marco regulatório e ampliação da educação e conscientização da população sobre a segurança cibernética.[235] Como parte das medidas técnicas e de capacitação, a Jamaica estabeleceu um CSIRT nacional (JaCIRT), subordinado ao Ministério da Ciência, Energia e Tecnologia (MSET), para monitorar o espaço digital da Jamaica e coordenar a reação a incidentes cibernéticos.[236] O JaCIRT é membro do CSIRT Américas e, portanto, tem acesso a toda a rede de CSIRTs filiados. Além disso, no orçamento de 2018–2019, a Jamaica destinou verbas específicas a diversas iniciativas de segurança cibernética dos Ministério da Segurança Nacional e da Ciência, Energia e Tecnologia.[237]

A estratégia de segurança cibernética nacional da Jamaica também definiu as infraestruturas críticas nacionais como "sistemas e ativos, sejam físicos ou virtuais, tão essenciais que sua incapacitação ou destruição teria um impacto debilitante sobre a segurança, a segurança econômica nacional e a saúde ou segurança pública nacional, ou qualquer combinação destas".[238] Elas podem incluir "redes de água e esgoto, agricultura, sistemas de saúde, serviços de emergência, tecnologia da informação e telecomunicações, operações bancárias e finanças, energia (elétrica e eólica), transporte (aéreo, rodoviário, portuário), entidades postais e de frete".[239] Assim, a estratégia atribuiu o papel principal na proteção das infraestruturas críticas nacionais ao MSET, eGov Jamaica e operadores de infraestruturas críticas.

O governo jamaicano adotou medidas significativas para aprimorar a segurança cibernética do país, porém muitas empresas ainda não têm planos de resposta a incidentes cibernéticos.[240] Além disso, com o objetivo de educar a sociedade civil como parte da estratégia nacional de cibersegurança, o governo lançou, em colaboração com o setor privado, um programa de conscientização pública sobre segurança cibernética.[241] Com efeito, a própria estratégia de segurança cibernética destaca a importância da participação do setor privado em atividades de segurança cibernética e na proteção de recursos públicos e privados.

Para o ensino superior em cibersegurança, há alguns provedores privados que oferecem capacitações, e o governo ofereceu várias sessões e oficinas (alguns em colaboração com o JaCIRT) a servidores do governo e ao setor privado para desenvolver habilidades e conhecimentos em cibersegurança.[242]

A Jamaica conta com um sólido marco regulatório para crimes cibernéticos. A Lei de Crimes Cibernéticos de 2010[243] prevê "sanções penais para o uso indevido de sistemas informatizados ou dados e o abuso de meios eletrônicos para efetuar transações e facilitar a investigação e a persecução de crimes cibernéticos".[244]

Essa lei foi alterada em 2015, após uma revisão abrangente envolvendo não apenas as partes interessadas locais, mas também atores internacionais.[245] Além disso, está em tramitação no parlamento a Lei de Proteção de Dados, destinada a proteger "a privacidade de determinados dados e questões correlatas". A Lei de Proteção de Dados será aplicada a controladores de dados públicos e privados, proporcionando assim uma legislação abrangente sobre proteção e privacidade de dados.[246]

A Jamaica também desenvolveu o Plano Setorial de TICs 2009–2030[247] e uma Política de TICs, aprovada em 2011.[248] A Lei de Identificação e Registro Nacional, aprovada em 2017, está sendo aplicada com o apoio do BID[249] e "visa abrigar suas informações biográficas, biométricas e demográficas em ambientes autônomos altamente seguros".[250]

Indicadores: Jamaica

D1 Política e Estratégia de Cibersegurança

2016 | 2020

1-1 Estratégia nacional de cibersegurança

- Desenvolvimento da estratégia
- Organização
- Conteúdo

1-2 Resposta a incidentes

- Identificação de incidentes
- Organização
- Coordenação
- Modo de funcionamento

1-3 Proteção de infraestruturas críticas (IC)

- Identificação
- Organização
- Gestão e resposta a riscos

1-4 Gerenciamento de crises

- Gerenciamento de crises

1-5 Ciberdefesa

- Estratégia
- Organização
- Coordenação

1-6 Redundância de comunicações

- Redundância de comunicações

D2 Cibercultura e Sociedade

2016 | 2020

2-1 Mentalidade de cibersegurança

- Governo
- Setor privado
- Usuários

2-2 Confiança e segurança na Internet

- Confiança e segurança do usuário na Internet
- Confiança do usuário nos serviços de governo eletrônico
- Confiança do usuário nos serviços de comércio eletrônico

2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet

- Compreensão do usuário sobre proteção de informações pessoais na Internet

2-4 Mecanismos de denúncia

- Mecanismos de denúncia

2-5 Mídia e redes sociais

- Mídia e redes sociais

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

México

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O México apresentou sua estratégia nacional de cibersegurança em 2017, com o objetivo principal de identificar e definir as ações de segurança cibernética aplicáveis às áreas social, econômica e política, para permitir que os cidadãos e organizações públicas e privadas usem as TICs de forma responsável em prol do desenvolvimento sustentável do Estado mexicano.[251] As infraestruturas críticas de informação são definidas na estratégia nacional de cibersegurança como aquelas consideradas estratégicas por estarem vinculadas à prestação de serviços públicos essenciais, podendo sua deterioração comprometer a segurança nacional. Há alguns anos que o México instituiu um CSIRT nacional, o CERT-MX, para prevenir e atenuar ameaças cibernéticas.[252] O CERT-MX está subordinado à Polícia Federal e faz parte da rede CSIRT Américas.

Com os crimes cibernéticos sendo uma preocupação crescente, organizações mexicanas que realizam projetos de transformação digital identificaram que, em 96% dos casos (91% no nível global), os grupos de interesse de decisores (diretores executivos) incluíam equipes de segurança e privacidade e 44% (53% no nível global) incluíam estruturalmente no planejamento e orçamento de projetos a gestão proativa dos riscos cibernéticos e da privacidade como uma consideração importante.[253]

Existem muitas oportunidades para os mexicanos darem continuidade a seus estudos sobre segurança cibernética, com opções em nível de graduação e de pós-graduação. Além disso, o governo já promoveu diversos eventos sobre cibersegurança, como o Fórum de Cibersegurança, com ênfase no setor financeiro,[254] e o curso básico sobre cibersegurança para servidores públicos oferecido pela Polícia Federal.[255]

O México não tem uma lei específica sobre crimes cibernéticos, mas o Artigo 211 do código penal aborda esse tipo de delitos.[256] No entanto, essas disposições são limitadas e apresentam lacunas, o que dificulta o combate ao crime cibernético. No que se refere à proteção e privacidade de dados, existem duas leis distintas: uma para bancos de dados públicos e outra para bancos de dados privados.[257]

Como parte do Plano de Desenvolvimento Nacional 2013–2018, o México lançou uma estratégia digital nacional, com o objetivo inicial de "ampliar a digitalização do México"[258] por meio do fomento à "implantação e expansão da infraestrutura de telecomunicações, bem como a adoção e o uso de TICs pela população para aproveitar seus benefícios".[259] Essa transformação visa forjar uma nova relação entre a sociedade e o governo, centrada na experiência do cidadão como usuário dos serviços públicos por meio da adoção das TICs no poder público. Atualmente, o México disponibiliza a seus cidadãos o portal gob.mx, que oferece, entre outros, serviços de identificação, saúde e vistos.[260]

Indicadores: México

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Nicarágua

Habitantes

*Ref.:Banco Mundial**

2017

6.384.855

Assinaturas de telefone celular

*Ref.:UIT***

2017

8.179.876

Pessoas com acesso à Internet

2017

1.779.015

Penetração da Internet

*Ref.:UIT***

2017

28%

A Nicarágua está em processo de formulação de uma estratégia nacional de cibersegurança, que conterá em seus eixos, entre outros, a criação de um centro de resposta a incidentes de cibersegurança e a atualização dos marcos jurídicos, administrativos, penais e processuais com o intuito de permitir a prevenção, investigação, julgamento e punição de crimes cibernéticos.

Atualmente, a Unidade de Crimes Cibernéticos da Polícia Nacional atende aos incidentes de segurança cibernética em conjunto com a Unidade Especializada contra o Crime Organizado do Ministério Público e outras instituições especializadas na área. Com relação à legislação sobre segurança cibernética, a Nicarágua dispõe do seguinte marco jurídico:

1) Constituição Política da República: protege os sistemas de comunicação nacionais e a administração e gestão do espectro radioelétrico e de satélites.

2) Lei nº 983 (Lei da Justiça Constitucional): regulamenta o recurso de Habeas Data.

3) Lei nº 919 (Lei de Segurança Soberana): identifica ameaças à segurança soberana, inclusive ataques externos contra a segurança cibernética.

4) Lei nº 787 (Lei de Proteção de Dados Pessoais):[261] protege o tratamento automatizado de dados pessoais da sociedade nicaraguense a fim de assegurar a autodeterminação informacional.

5) Lei nº 641 (Código Penal):[262] tipifica alguns comportamentos de crimes cibernéticos.

As instituições públicas fortaleceram suas capacidades orientadas para a segurança cibernética por meio de equipamentos e formação especializados. O setor privado expandiu sua oferta de serviços de segurança cibernética, que inclui serviços públicos e privados de proteção na nuvem.

Com relação ao acesso às tecnologias da informação, após a implantação do Eixo do Programa Nacional de Desenvolvimento Humano 2018–2021, que prevê a promoção da ciência, tecnologia e inovação, a execução do Programa Nacional de Banda Larga teve continuidade com o apoio do BID. Esse programa facilitou o acesso dos municípios remotos do país aos serviços de telecomunicações, fortalecendo assim a conectividade do sistema nacional de saúde e de agricultura.

A expansão do acesso às tecnologias de informação permitiu a ampliação das carreiras e cursos técnicos por meios remotos, valendo-se da educação virtual. Também foram implementados serviços on-line e procedimentos públicos.

De acordo com estatísticas do Instituto de Telecomunicações e Serviços Postais da Nicarágua (TELCOR), em 2017 havia 8.179.876 assinantes de telefonia celular registrados, com uma cobertura de banda larga fixa de 92%, banda larga móvel de 98% e cobertura móvel 3G de 100% do território nacional.

Indicadores: Nicarágua

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

	2016	2020
3-1 Conscientização		
Programas de conscientização	■□□□□	■□□□□
Conscientização de executivos	■□□□□	■■□□□
3-2 Marco para a educação		
Fornecimento	■□□□□	■□□□□
Administração	■□□□□	■□□□□
3-3 Marco para treinamento profissional		
Fornecimento	■□□□□	■■□□□
Aproveitamento	■□□□□	■■□□□

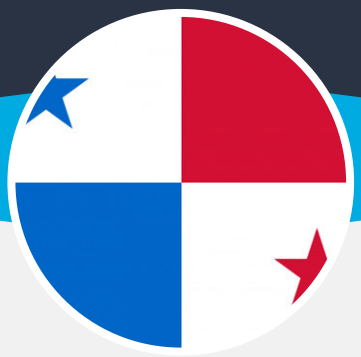
D4 Marcos legais e regulatórios

	2016	2020
4-1 Marcos jurídicos		
Marcos legislativos para a segurança de TICs	■□□□□	■■□□□
Privacidade, liberdade de expressão e outros direitos humanos na Internet	■■□□□	■■□□□
Legislação sobre proteção de dados	□□□□□	■■□□□
Proteção das crianças na Internet	□□□□□	■■□□□
Legislação de proteção ao consumidor	□□□□□	■■□□□
Legislação sobre propriedade intelectual	□□□□□	■■□□□
Legislação substantiva sobre cibercrimes	■□□□□	■■□□□
Legislação processual sobre cibercrimes	■■■□□	■■■□□
4-2 Sistema da justiça penal		
Aplicação da lei	■□□□□	■■□□□
Ação penal	■□□□□	■□□□□
Tribunais	■□□□□	■□□□□
4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético		
Cooperação formal	□□□□□	■□□□□
Cooperação informal	□□□□□	■□□□□

D5 Normas, organizações e tecnologias

	2016	2020
5-1 Observância das normas		
Normas de segurança de TICs	■□□□□	■□□□□
Normas para aquisições	■■□□□	■■□□□
Normas para desenvolvimento de software	■□□□□	■■□□□
5-2 Resiliência da infraestrutura de Internet		
Resiliência da infraestrutura da Internet	■□□□□	■■□□□
5-3 Qualidade de software		
Qualidade de software	□□□□□	■■□□□
5-4 Controles técnicos de segurança		
Controles técnicos de segurança	□□□□□	■□□□□
5-5 Controles criptográficos		
Controles criptográficos	□□□□□	■■□□□
5-6 Mercado de cibersegurança		
Tecnologias de cibersegurança	□□□□□	■■□□□
Seguro contra cibercrimes	□□□□□	■□□□□
5-7 Divulgação responsável		
Divulgação responsável	■□□□□	■□□□□

Panamá



Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Panamá adotou sua estratégia de segurança cibernética em março de 2013, com a edição da Resolução nº 21,[263] a Estratégia Nacional de Cibersegurança e Proteção das Infraestruturas Críticas, com o slogan "Panamá, confiável no espaço digital: Trabalho de todos".[264] Os pilares da estratégia de segurança cibernética são proteção da privacidade, prevenção e repressão de crimes no espaço digital, fortalecimento das infraestruturas críticas, promoção do desenvolvimento do setor privado, ampliação da cultura de cibersegurança, capacitação, inovação e adoção de padrões e melhoria da capacidade dos órgãos públicos de responder a incidentes.

Um dos aspectos da cibersegurança que se destaca na estratégia é a proteção das infraestruturas críticas, "vitais para o bem-estar da população, os serviços básicos, o funcionamento das organizações governamentais e privadas, o bem-estar econômico e a qualidade de vida do povo",[265] e que necessitam de "proteção abrangente".

Em 2011, por meio do Decreto Executivo nº 709, foi criado o CSIRT Panamá, no âmbito da Autoridade Nacional para Inovação Governamental como o grupo nacional de reação a incidentes em computadores.[266] Além de prevenir, tratar, identificar e solucionar incidentes de segurança cibernética, o CSIRT Panamá também tem a tarefa de ampliar o conhecimento geral do país sobre o tema.[267] Para fortalecer essas capacidades, o Governo do Panamá e o BID comprometeram-se a apoiar iniciativas específicas de segurança cibernética por meio do empréstimo Programa Panamá On-line, aprovado em 2016.[268] Além disso, o CSIRT Panamá é integrante do CSIRT Américas e, portanto, pode se beneficiar de tudo o que a rede tem a oferecer.

Existem, no Panamá, provedores do setor privado que oferecem uma gama de serviços de segurança cibernética, desde segurança de banco de dados até um leque de cursos de formação. Paralelamente a isso, há grandes oportunidades para os cidadãos panamenhos darem continuidade a seus estudos sobre segurança cibernética e tecnologias da informação, inclusive programas de mestrado. Para incentivar o estudo da segurança cibernética, a Autoridade Nacional para Inovação Governamental, em colaboração com o Citi e a OEA, ofereceu no passado bolsas de estudo para a formação em segurança cibernética, a fim de reduzir a escassez de profissionais da área na região.[269] Além disso, o CSIRT Panamá oferece capacitação permanente em segurança cibernética para os profissionais dos departamentos de tecnologia de instituições governamentais.[270]

Em termos de legislação, o código penal do Panamá traz algumas disposições que tratam dos crimes cibernéticos.[271] Já o projeto de Lei nº 558, de 2017,[272] visa modificar o código penal para "cumprir os padrões internacionais de segurança cibernética", inclusive a Convenção de Budapeste sobre Crimes Cibernéticos, aprovada pelo Panamá em 2013.[273]

Existe um projeto de lei para a proteção de dados pessoais que, quando aprovado, será aplicável aos setores público e privado.[274] Finalmente, em seu Plano Estratégico de Governo 2015–2019 e na Agenda Digital 2014–2019, o Panamá conta com uma estratégia de governo eletrônico e outras diretrizes importantes relacionadas à segurança cibernética e à governança de TICs.[275]

Indicadores: Panamá

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

Paraguai

Habitantes

Ref.:Banco Mundial*

Assinaturas de telefone celular

Ref.:UIT**

Pessoas com acesso à Internet

Penetração da Internet

Ref.:UIT**

Em abril de 2017, o Paraguai aprovou seu Plano Nacional de Cibersegurança e formou sua Comissão Nacional de Cibersegurança com representantes de diferentes instituições públicas, com o objetivo de adotar medidas de segurança cibernética para garantir e fomentar o uso seguro e confiável das TICs, bem como o progresso e a inovação no país.[276] O plano também define claramente sete linhas de ação (conscientização e cultura, pesquisa, desenvolvimento e inovação, proteção das infraestruturas críticas, capacidade de resposta a incidentes cibernéticos, capacidade de investigar e processar crimes cibernéticos, administração pública e sistema nacional de cibersegurança), tudo com muita clareza em relação às etapas subsequentes. O plano foi elaborado como um complemento para instituir iniciativas na área de segurança cibernética. O CSIRT nacional do Paraguai (CERT-PY) é membro da rede CSIRT Américas.[277]

Com o objetivo de expandir a capacidade do país, em 2018 o BID aprovou o empréstimo Programa de Apoio à Agenda Digital, que inclui ações e componentes específicos para assegurar o fortalecimento da estrutura nacional de segurança cibernética.[278]

O Plano Nacional de Segurança Cibernética também define infraestrutura crítica como "sistemas e ativos, sejam físicos ou virtuais, essenciais para a manutenção de funções sociais vitais, saúde, integridade física, segurança e o bem-estar social e econômico da população, cuja interrupção ou destruição teria um impacto debilitante na segurança nacional, gerando uma cascata de efeitos negativos que afetariam gravemente o país." [279] Isso evidenciou a necessidade de cooperação entre os setores público e privado na proteção da infraestrutura crítica do país.

Embora haja provedores desses serviços no setor privado, a estratégia de segurança cibernética visa ampliar a conscientização sobre a importância da adoção de boas práticas de segurança cibernética no setor privado. Em 2017, ainda não existiam empresas do setor privado com a certificação ISO 27001, norma internacional de segurança da informação que, em novembro de 2017, foi adotada como o padrão paraguaio pelo Instituto Nacional de Tecnologia e Normalização, por meio de um comitê composto por representantes de instituições públicas, empresas privadas, associações de consumidores e universidades.[280] Contudo, o setor privado participou da elaboração do Plano Nacional de Cibersegurança e da definição da norma paraguaia ISO 27001, o que indica disposição para participar mais e criar consciência da importância da segurança cibernética.

Em outubro de 2018, foi criado o Ministério das Tecnologias da Informação e Comunicações (MITIC), no qual se estabeleceu a Segurança Cibernética e a Proteção da Informação como eixo estratégico. Por meio da Direção-Geral de Cibersegurança e Proteção da Informação, o MITIC tem hoje as seguintes funções e atribuições, determinadas pela Lei de Criação do MITIC nº 6.207/2018:

- Desenvolvimento de um ecossistema digital seguro, confiável e resiliente, incluindo os setores público, privado, acadêmico e os cidadãos
- Políticas para a proteção de informações pessoais e governamentais
- Proteção de sistemas, redes, processos e informações de órgãos e entidades estatais
- Planos e estratégias de cibersegurança no nível nacional
- Autoridade em cibersegurança, prevenção, gestão e controle de incidentes cibernéticos
- Definição e proteção das infraestruturas tecnológicas críticas

O MITIC oferece diversos cursos de TI gratuitos online, disponíveis para qualquer pessoa que conte com um computador e acesso à Internet, inclusive alguns sobre segurança da informação. Além disso, diversos programas de formação são oferecidos por universidades e empresas de segurança, e há oportunidades limitadas de graduação em segurança cibernética. O governo também realizou campanhas de capacitação, com o intuito de educar a população sobre a segurança cibernética.[281]

Da mesma forma, a Direção-Geral de Cibersegurança e Proteção da Informação tem várias iniciativas e oferece diversos serviços, inclusive alertas e boletins de segurança, gerenciamento de incidentes cibernéticos, auditorias de vulnerabilidades de sistema governamental, diagnósticos de segurança para instituições governamentais e atividades de conscientização e capacitação para cidadãos, empresas, governo, academia e outros setores.

Em 2011, por meio da Lei nº 4.439/11, o Paraguai modificou e ampliou o conjunto de atos passíveis de punição previstos na Lei nº 1.160/97 (Código Penal), que se refere a determinados artigos que descrevem condutas ilícitas adotadas por meio do uso de tecnologia cuja essência está na sua natureza computacional, mais conhecidos como crimes cibernéticos.[282]

Também figura na legislação nacional do Paraguai a Lei nº 1.682, que trata de informações de caráter privado e cujo objetivo é regulamentar a "coleta, armazenamento, processamento e publicação de dados ou características pessoais".[283]

Em 2017, com a Lei nº 5.994/17, o Paraguai aderiu à Convenção de Budapeste sobre Crimes Cibernéticos e seu Protocolo Adicional, cujo objetivo principal é "aplicar uma política penal comum destinada a proteger a sociedade contra os crimes cibernéticos, sobretudo por meio da adoção de legislação adequada e da promoção da cooperação internacional".[284] Atualmente, na qualidade de Estado participante dessa convenção, o Paraguai é beneficiário do Programa GLACY+ (Ação Global Ampliada contra o Cibercrime), executado pelo Conselho da Europa em conjunto com a União Europeia, a fim de auxiliar os países-membros na adoção efetiva e na harmonização da convenção com uma legislação nacional positiva, por meio da promoção de estratégias legislativas contra os crimes cibernéticos e da construção de capacidades para funcionários do judiciário e cooperação jurídica internacional. Em dezembro de 2019, o país recebeu o Comitê do Conselho da Europa, composto por consultores especializados na área de cibercrimes, para realizar uma missão inicial de avaliação da situação do país na luta contra os crimes cibernéticos, com o objetivo de definir as diretrizes a serem seguidas por meio de um plano de trabalho com os diversos atores envolvidos nessa área.

O Ministério Público possui uma Unidade Especializada em Crimes Cibernéticos composta por um Promotor Adjunto, um Promotor Delegado e três unidades penais na capital, bem como agentes especializados em crimes cibernéticos nos principais departamentos, com vistas a intervir em denúncias de atos de natureza eletrônica passíveis de punição. Paralelamente a isso, ele conta com um gabinete de apoio técnico à gestão fiscal, a quem cabe prestar assistência e apoio técnico com o objetivo de conduzir pesquisas que envolvam o uso de tecnologia eletrônica ou da computação. Por sua vez, a Polícia Nacional também possui uma divisão especializada no combate a crimes cibernéticos, que atua em parceria com o Ministério Público.

Por meio do Instituto de Altos Estudos Estratégicos, o Ministério da Defesa está passando por um processo de inovação e adaptação, que exige profissionais especializados e, em 2019, implantou o Programa de Especialização em Ciberdefesa e Cibersegurança Estratégica como forma de capacitar seu pessoal na criação de estratégias de combate a novas ameaças existentes no espaço digital, sinal de que a modernidade chegou à instituição, que terá sua primeira turma de graduados.

O país também possui um projeto da Estratégia Nacional de TIC/Agenda Digital, que "se enquadra nos objetivos do Plano Nacional de Desenvolvimento do Paraguai 2030." [285] Os eixos da Agenda Digital são: (i) governo eletrônico; (ii) inclusão, apropriação e uso; e (iii) inovação e competitividade. A Lei nº 4.989/13 é outro instrumento importante na formulação de políticas de TIC.[286] Da mesma forma, várias normas e diretrizes de segurança cibernética foram adotadas no setor governamental, inclusive as seguintes:

- Controles Críticos de Cibersegurança, com base nos Controles CIS, aprovados pela Resolução SENATIC nº 115/2018.[287]

- Critérios Mínimos de Segurança para o Desenvolvimento e Aquisição de Software, aprovado pela Resolução MITIC nº 699/2019.[288]

- Diretrizes de Cibersegurança para Canais Oficiais de Comunicação do Estado, aprovadas pela Resolução MITIC nº 432/2019.[289]

Indicadores: Paraguai

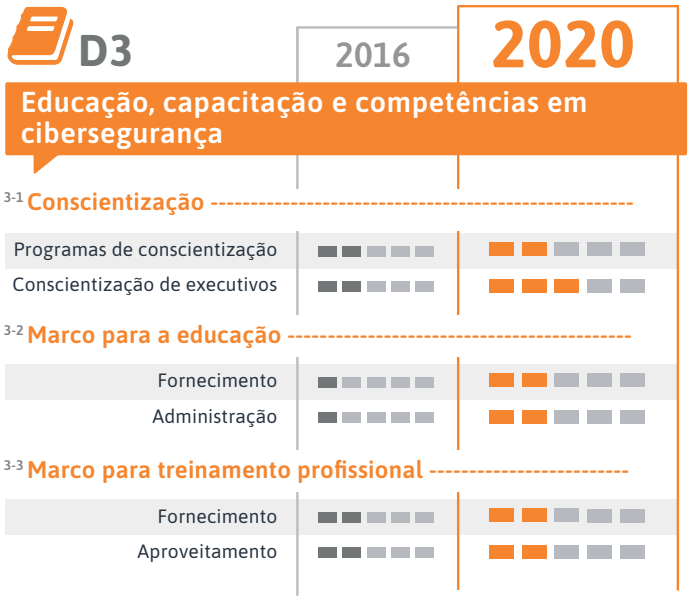
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia	■■□□□	■■■□□
Organização	■■□□□	■■□□□
Conteúdo	■□□□□	■■■□□
1-2 Resposta a incidentes		
Identificação de incidentes	■■■□□	■■■□□
Organização	■■■□□	■■■□□
Coordenação	■■□□□	■■■□□
Modo de funcionamento	□□□□□	■■□□□
1-3 Proteção de infraestruturas críticas (IC)		
Identificação	■□□□□	■□□□□
Organização	■□□□□	■□□□□
Gestão e resposta a riscos	■□□□□	■□□□□
1-4 Gerenciamento de crises		
Gerenciamento de crises	■□□□□	■■□□□
1-5 Ciberdefesa		
Estratégia	■□□□□	■■□□□
Organização	■□□□□	■■■□□
Coordenação	■□□□□	■□□□□
1-6 Redundância de comunicações		
Redundância de comunicações	■■□□□	■□□□□

D2 Cibercultura e Sociedade

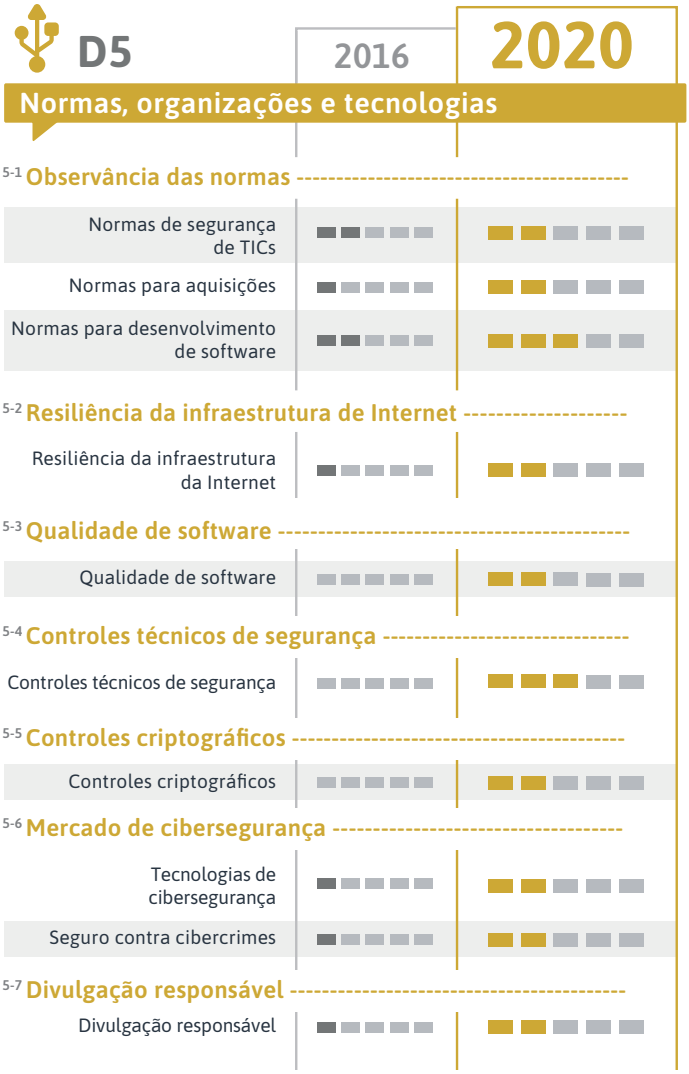
	2016	2020
2-1 Mentalidade de cibersegurança		
Governo	■■□□□	■■□□□
Setor privado	■■□□□	■■□□□
Usuários	■■□□□	■■□□□
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet	■■□□□	■■□□□
Confiança do usuário nos serviços de governo eletrônico	■■□□□	■■□□□
Confiança do usuário nos serviços de comércio eletrônico	■■□□□	■■□□□
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet	□□□□□	■■□□□
2-4 Mecanismos de denúncia		
Mecanismos de denúncia	□□□□□	■■□□□
2-5 Mídia e redes sociais		
Mídia e redes sociais	□□□□□	■■□□□

D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios

D5 Normas, organizações e tecnologias



CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Peru

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Peru ainda não possui uma estratégia nacional de cibersegurança, mas tem uma Política Nacional de Cibersegurança que, entre outras coisas, destaca a necessidade de criar uma estratégia nacional e um comitê nacional dedicados à questão.[290]

A Lei nº 30.618, de 2017, define cibersegurança como a "situação de confiança no ambiente digital, diante das ameaças que afetam as capacidades nacionais, por meio do gerenciamento de riscos e da aplicação de medidas de cibersegurança e capacidades de ciberdefesa, alinhadas à consecução dos objetivos do Estado".[291] A lei também estipula que a Diretoria Nacional de Inteligência tem a responsabilidade de "desenvolver atividades e definir procedimentos que visem alcançar a segurança cibernética na sua área de competência".[292]

O Decreto Supremo nº 106-2017-PCM "aprova o Regulamento de Identificação, Avaliação e Gerenciamento de Riscos de Ativos Críticos Nacionais", que são "recursos, infraestruturas e sistemas essenciais e indispensáveis à manutenção e desenvolvimento das capacidades nacionais ou que se destinem a cumprir essa finalidade".[293]

O Peru conta com um CSIRT nacional, o PeCERT, com o objetivo de articular a prevenção, tratamento e resposta a incidentes de segurança cibernética de instituições do setor público, bem como desenvolver estratégias, práticas e mecanismos necessários para atender às necessidades de segurança da informação do Estado.[294] O PeCERT é vinculado ao Escritório Nacional de Governo Eletrônico e Tecnologia da Informação (ONGEI) e filiado à rede CSIRT Américas. Além disso, segundo o Centro de Segurança Cibernética Industrial, o Peru está preparando uma lei para a proteção da infraestrutura crítica.[295] Por meio do empréstimo Projeto para Melhorar e Expandir os Serviços de Apoio à Prestação de Serviços Nacionais para Cidadãos e Empresas, o Governo do Peru e o BID comprometeram-se a fomentar projetos específicos para fortalecer a situação da segurança cibernética nacional.[296]

Há vários provedores privados de serviços de segurança cibernética no Peru e alguns deles também oferecem capacitação na área. Há oportunidades nas universidades para os peruanos darem continuidade a seus estudos sobre segurança cibernética, e também ocorreram eventos relacionados ao tema organizados por associações independentes. O governo peruano também tomou a iniciativa de organizar eventos de segurança cibernética, como o Congresso Internacional sobre Desafios e Gestão na Segurança Digital, em junho de 2018, organizado pela Direção Nacional de Inteligência e a Secretaria de Governo Eletrônico.[297]

A questão do governo eletrônico é importante para o Peru, cuja Lei do Governo Eletrônico "visa estabelecer a estrutura de governança do governo eletrônico para o gerenciamento adequado da identidade digital, serviços digitais, arquitetura digital, interoperabilidade, segurança cibernética e dados, bem como o regime jurídico aplicável à transversalidade do uso de tecnologias digitais na digitalização de processos e na prestação de serviços digitais por entidades da administração pública nas três esferas de governo".[298] Além disso, o Peru declarou "estratégias, ações, atividades e iniciativas de interesse nacional para o desenvolvimento do governo eletrônico, inovação e economia digital no Peru com enfoque territorial"[299] em 2018,[300] além de aprovar as "diretrizes para a formulação do Plano de Governo Eletrônico".[301]

No que tange à legislação, a Lei nº 30.096 contém disposições substantivas sobre crimes de computador[302], e a Lei nº 27.309 incorpora os crimes computacionais ao código penal do país.[303] Adicionalmente, a Lei nº 29.733 se aplica à proteção de bancos de dados públicos e privados.[304]

Indicadores: Peru

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

República Dominicana

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Em junho de 2018, o Governo da República Dominicana emitiu o Decreto n° 230-18, de adoção de sua Estratégia Nacional de Cibersegurança 2018–2021.[159] Esse decreto visa estabelecer mecanismos de segurança cibernética adequados para a proteção do Estado, seus habitantes e, em termos mais gerais, a segurança e o desenvolvimento nacionais.

Ademais, a estratégia nacional faz parte do Programa República Digital, criado pelo Decreto n° 258-16,[160] e propõe 4 objetivos gerais, 13 objetivos específicos e 37 linhas de ação contidas em seus quatro pilares: (i) Marco Legal e Fortalecimento Institucional; (ii) Proteção das Infraestruturas Críticas Nacionais e Infraestrutura de TI do Governo; (iii) Educação e Cultura Nacional de Cibersegurança; e (iv) Parcerias Nacionais e Internacionais. Desenvolvidos com a participação do setor privado esses pilares têm a finalidade de estabelecer um mecanismo de diálogo e cooperação entre todos os setores da sociedade a fim de promover as melhores práticas, identificar problemas comuns e desenvolver soluções adequadas para o enfrentamento das ameaças cibernéticas.

Enquadrado na estratégia nacional, o pilar Proteção das Infraestruturas Críticas Nacionais e Infraestrutura de TI do Governo tem como objetivos gerais: "Assegurar o funcionamento contínuo e a proteção das informações armazenadas nas infraestruturas críticas nacionais e infraestrutura de TI relevante do Estado." Para alcançar esse objetivo, suas linhas de ação consideram a criação do CSIRT-RD, que contribuirá para melhorar a articulação intersetorial e institucional para a proteção dos sistemas de informação e das infraestruturas nacionais essenciais e de TI do Estado e do setor privado.

A estratégia nacional considera a criação de alianças estratégicas públicas e privadas, tanto no nível local como internacional, com o objetivo de fortalecer a cooperação e sincronizar esforços para reagir a incidentes relacionados a segurança cibernética. Dessa forma, ela pretende ampliar a participação do setor privado e da sociedade civil nas questões dessa área. O objetivo fundamental do pilar Parcerias Nacionais e Internacionais centra-se no desenvolvimento da cooperação intersetorial nos níveis local e internacional, com o objetivo de compartilhar informações sobre incidentes, ameaças, melhores práticas, eventos de diretivas e iniciativas para melhorar a resiliência cibernética do país.

A República Dominicana possui legislação específica que tipifica os crimes cibernéticos na Lei n° 53-07[161], que trata de crimes e delitos na área de alta tecnologia. Na mesma linha está a Lei n° 172-13,[162] cujo objetivo é a "proteção integral dos dados pessoais registrados em arquivos, registros públicos, bancos de dados e outros meios técnicos de processamento de dados para a geração de relatórios, sejam públicos ou privados". Além disso, a constituição de 2010 concede a todas as pessoas[163] o direito de acessar quaisquer dados a seu respeito e de solicitar à autoridade judicial competente que atualize, retifique ou destrua dados que possam afetar ilicitamente os seus direitos.[164]

A República Dominicana oferece oportunidades de estudos em segurança cibernética a seus cidadãos, e estão previstas medidas para desenvolver uma cultura nacional de segurança cibernética entre toda a população, bem como para fortalecer a segurança cibernética em todos os níveis educacionais, desde o ensino fundamental até os níveis de graduação, pós-graduação e mestrado.

Indicadores: República Dominicana

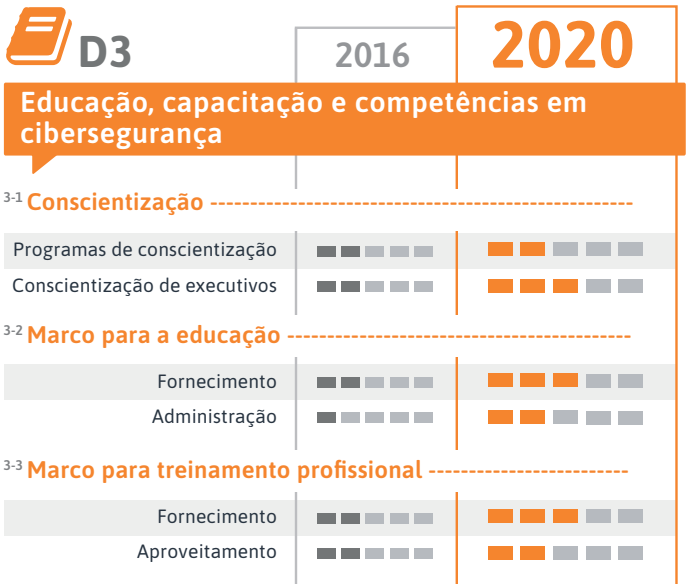
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

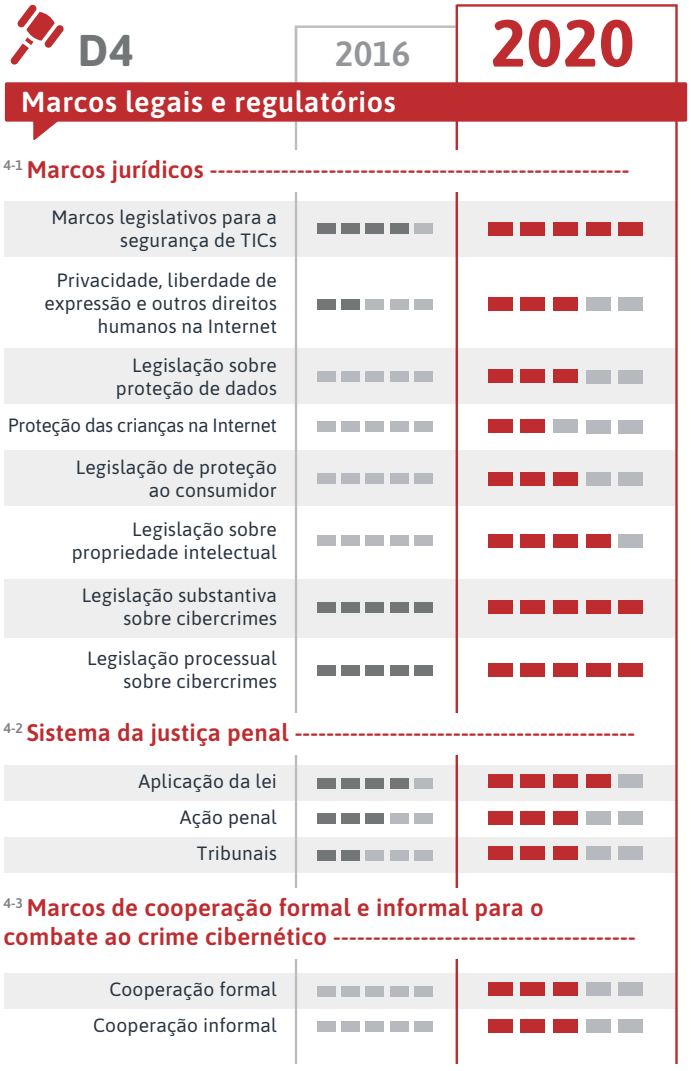
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

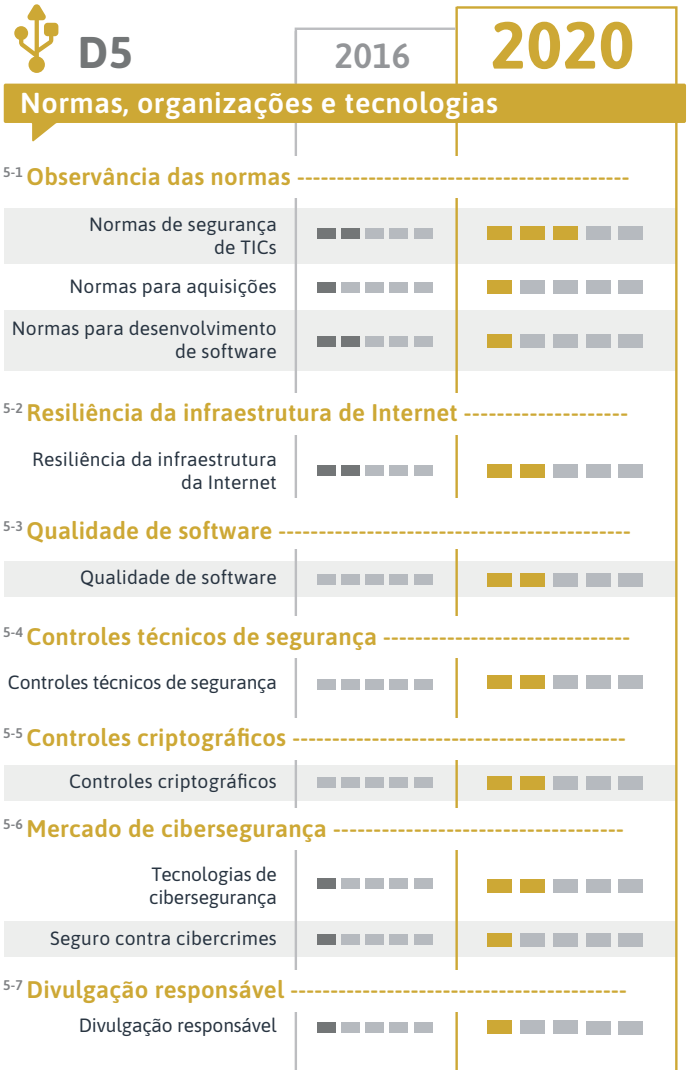
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Santa Lúcia

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Por meio do Departamento de Serviço Público, o governo de Santa Lúcia está tomando medidas para desenvolver a resiliência a ataques cibernéticos, criando assim um ambiente mais seguro para suas operações e intercâmbio de dados. O Data Center do Governo, gerenciado pelos Serviços de Tecnologia da Informação do Governo (GITS) conseguiu a certificação ISO 27001:2013 em 2015.[314] A renovação estava prevista para abril de 2018, mas não se concretizou devido a restrições. Atualmente, a Divisão de Modernização do Setor Público (DPSM) do Departamento de Serviço Público contratou os serviços de uma consultoria para auxiliar o GITS na preparação para a recertificação de seu data center dentro da norma ISO 27001:2013.

Por intermédio da Divisão de Modernização do Setor Público, o Departamento de Serviço Público deu início a um exercício para atualizar a Política e a Estratégia Setorial Nacional de TICs. O intuito dessa estratégia é traçar o caminho a seguir para a implantação das TICs em todos os setores a fim de modernizá-los, criar novas oportunidades de negócios e fomentar a inovação. Foi realizada uma consulta de uma semana com um grupo representativo de partes interessadas do governo, setor privado e sociedade civil. Foram formados grupos de trabalho para examinar cada setor e fazer recomendações. Um setor importantíssimo é a segurança nacional, que terá a segurança cibernética como foco principal.

Também houve apoio à Força Policial Real de Santa Lúcia por parte do governo francês a fim de auxiliar na capacitação de recursos humanos em segurança cibernética por meio de várias iniciativas de formação.

A Lei de Uso Indevido de Computadores, de 2011, entrou em vigor em 6 de julho de 2018, e a Lei de Transações Eletrônicas[315] e Dados e Privacidade[316] foi aprovada pelo Parlamento de Santa Lúcia em 2011.[317]

Além disso, a DPSM constituiu grupos de trabalho com a Força-Tarefa de Governo Eletrônico para desenvolver um Roteiro de CSIRT e uma Política e Estratégia de Cibersegurança. Uma vez concluídos, eles serão analisados e encaminhados para aprovação e custeio.

À medida que o Governo de Santa Lúcia evolui para uma posição mais centrada no cidadão, por meio da adoção de iniciativas importantes de TICs, as ameaças cibernéticas ficam ainda mais palpáveis. Nesse sentido, a DPSM também está participando do programa Resposta a Incidentes Cibernéticos: Capacitação, na Comunidade Britânica. Esse é um esforço para assegurar que o governo disponha dos sistemas, capacidades e apoio corretos para desenvolver, manter e ampliar um CSIRT. Também cabe observar que todos os projetos da DPSM têm um foco bastante grande na segurança, de modo a assegurar a proteção das TICs e dos recursos de dados. A DPSM também contratou os serviços de uma consultoria jurídica para examinar a legislação em vigor, identificar lacunas, fazer recomendações e, em alguns casos, redigir legislação pertinente para ser apreciada e adotada pela procuradoria-geral.

Indicadores: Santa Lúcia

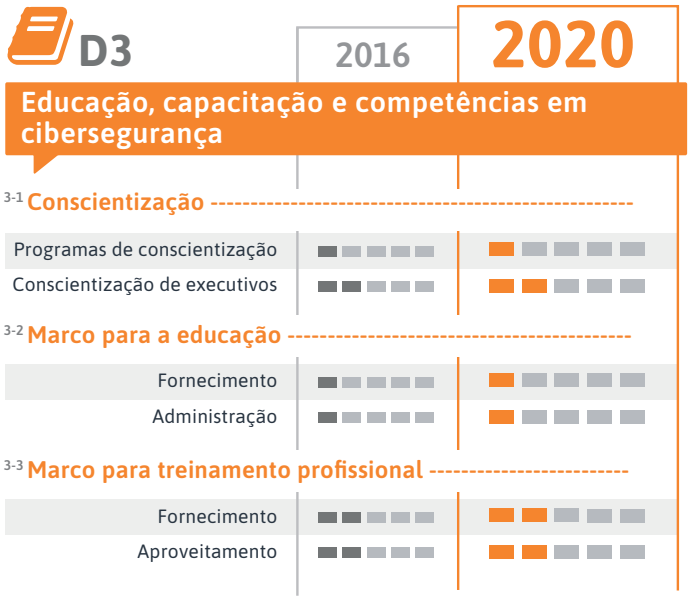
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

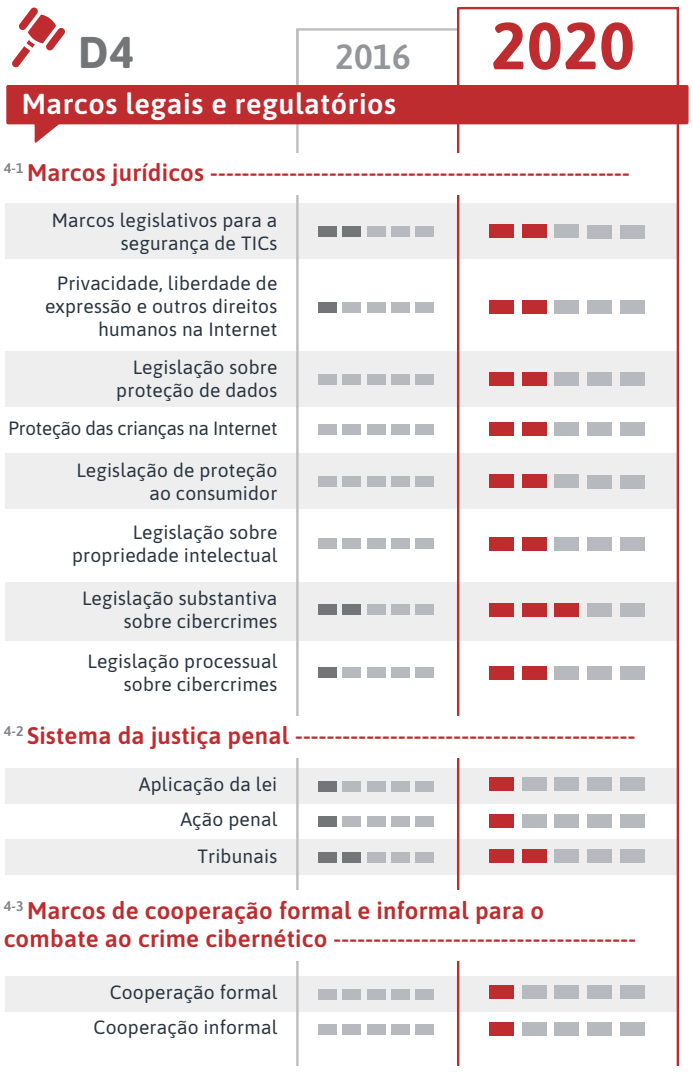
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

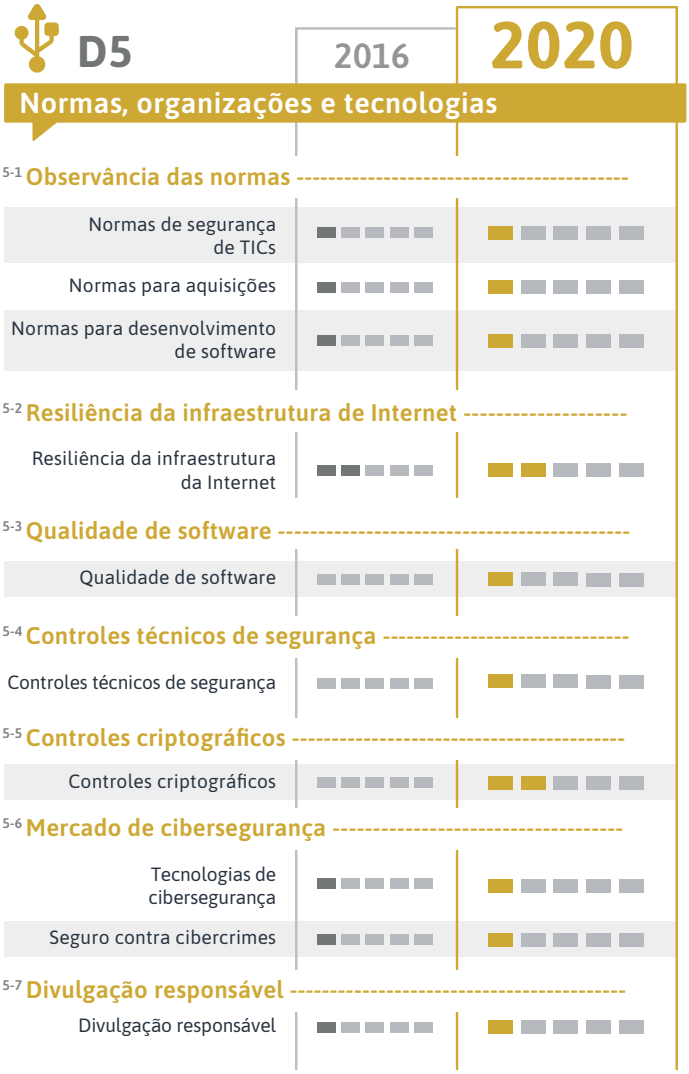
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



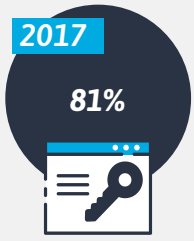
São Cristóvão e Nevis

Habitantes
*Ref.:Banco Mundial**

Assinaturas de telefone celular
*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet
*Ref.:UIT***



São Cristóvão e Névis ainda não criou uma estratégia nacional de cibersegurança nem estabeleceu um CSIRT nacional. No entanto, o governo está ciente da importância crescente da segurança cibernética para a segurança nacional como um todo e está trabalhando para constituir um CSIRT nacional. Ademais, o desenvolvimento de uma estratégia nacional de cibersegurança e de um plano para sua implantação, o estabelecimento de um comitê nacional de segurança cibernética, a realização de entrevistas com as partes interessadas e a análise de pesquisas que avaliem as necessidades atuais também são medidas nas quais o país está trabalhando.

A cibersegurança foi um dos principais pontos da agenda de uma reunião realizada pelo Conselho de Ministros do Sistema de Segurança Regional em 2017, presidida pelo primeiro-ministro de São Cristóvão e Névis.[305] Na reabertura do Centro de TICs, declarações públicas do primeiro-ministro deixaram claro que a segurança cibernética deve ser uma prioridade para o país.[306] Finalmente, o orçamento de 2018 menciona o agora reformulado Centro de TICs, um projeto de infraestrutura de rede de governo eletrônico e um projeto de segurança cibernética.[307]

Embora limitados, há provedores de serviços de segurança cibernética no setor privado do país, alguns oferecendo serviços técnicos e outros serviços de conscientização e formação. Não obstante, o setor privado está começando a priorizar a segurança cibernética e a tomar medidas nesse sentido. No nível nacional, o governo facilitou alguns programas de capacitação em segurança cibernética para servidores públicos, como a capacitação em risco da ISO-31000.[308] No entanto, ainda não há oportunidades de fazer cursos de nível superior em segurança cibernética.

São Cristóvão e Névis já conta com legislação sobre crimes cibernéticos, como a Lei de Crimes Eletrônicos de 2009, que trata tanto de ilícitos relacionados a crimes eletrônicos quanto do procedimento para processá-los.[309] A nova Lei de Proteção de Dados, promulgada em 2018, é bastante semelhante à da Organização dos Estados do Caribe Oriental e se aplica às informações mantidas pelo setor público e pelo setor privado.[310]

O governo eletrônico faz parte do Plano Estratégico Nacional de Tecnologias da Informação e Comunicação (TIC), de 2006, e visa aproveitar as TICs para fins de prestação de serviços e informações pelo governo.[311] Em 2016, por meio de uma parceria público-privada, foi lançado um novo portal eletrônico governamental, com a promessa de aumentar a eficiência nos trâmites com o setor público. Além disso, o portal também conectaria diferentes ministérios e órgãos governamentais para facilitar o compartilhamento de informações.[312] Está prevista a formulação de uma estratégia digital nacional e um aumento na implementação de sistemas de informação interconectados. Prevê-se também a implantação de uma nova arquitetura empresarial no governo, com um desenho orientado para a segurança, interoperabilidade e serviços.[313]

Indicadores: São Cristóvão e Nevis

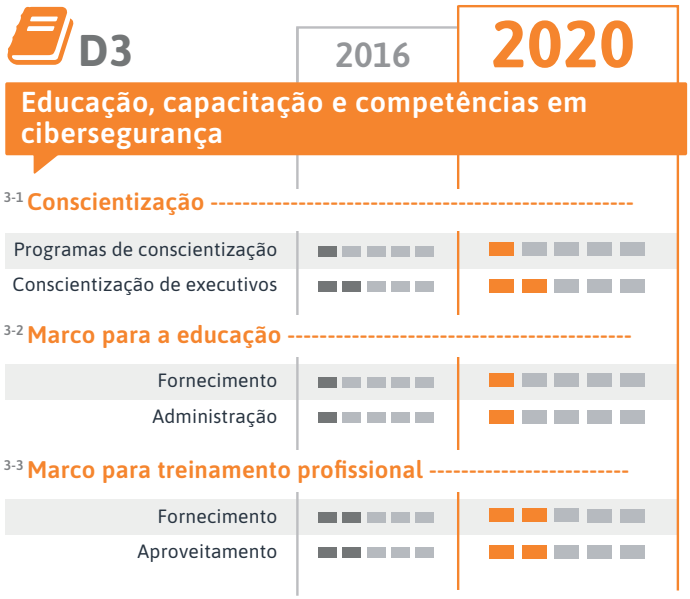
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

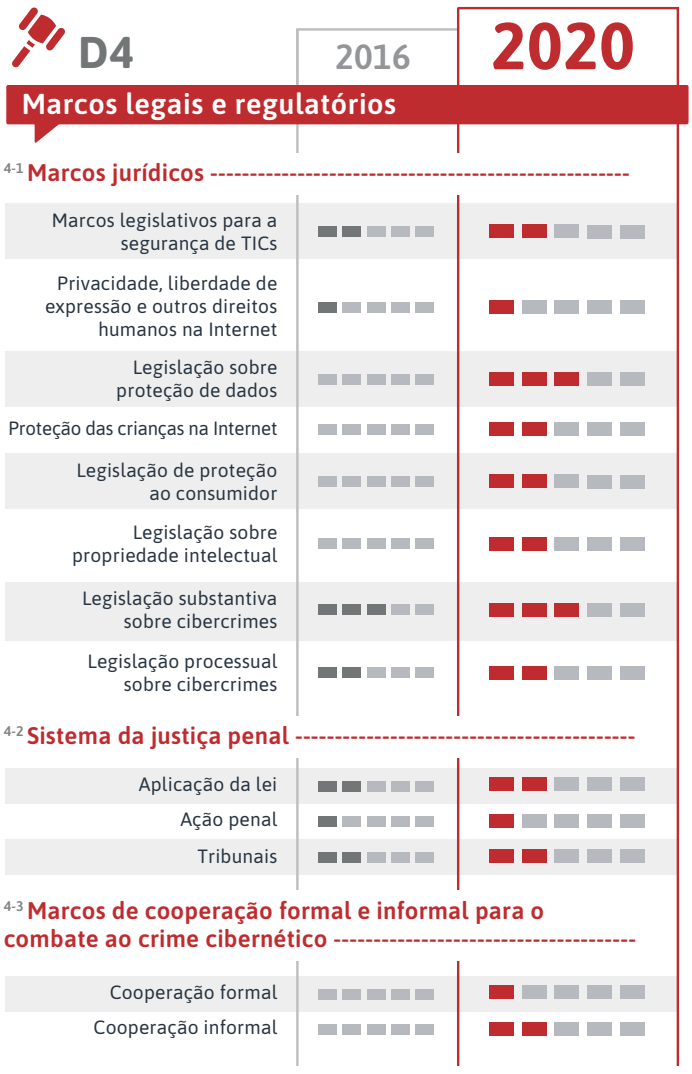
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

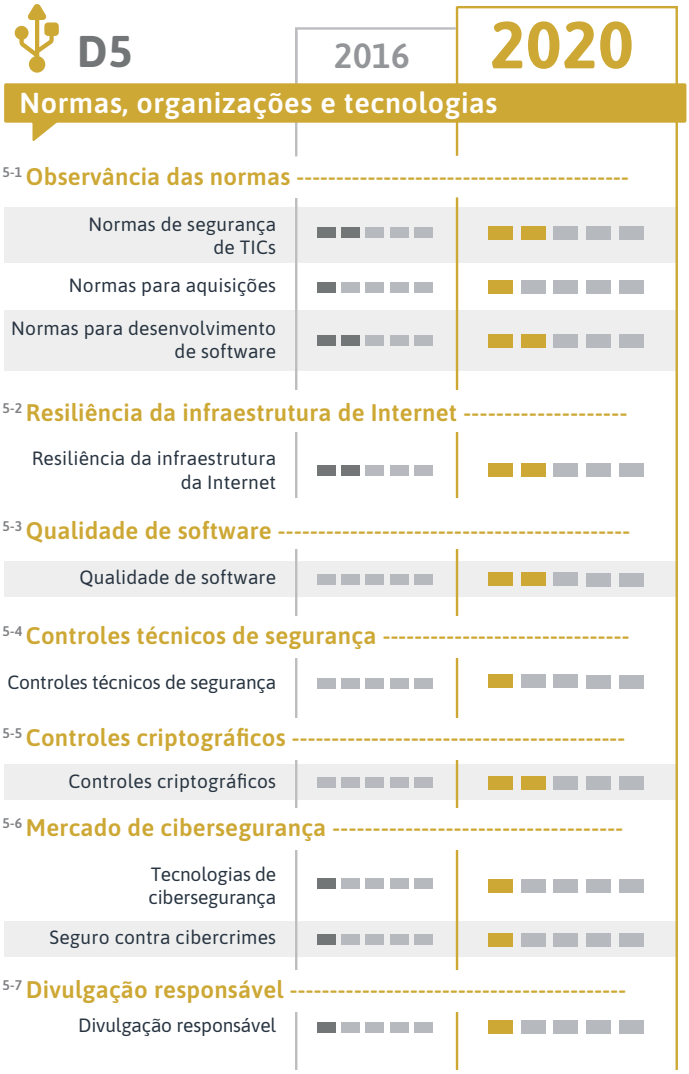
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



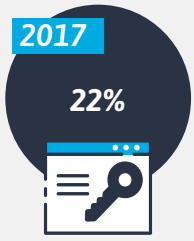
São Vicente e Granadinas

Habitantes
*Ref.:Banco Mundial**

Assinaturas de telefone celular
*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet
*Ref.:UIT***



Recentemente, São Vicente e Granadinas adotou medidas para reforçar sua cibersegurança, apesar da ausência de uma estratégia nacional de segurança cibernética. Como exemplo da crescente atenção à cibersegurança, em dezembro de 2017 foi realizado um simpósio nacional sobre o assunto.[318] O simpósio, que atraiu participantes de toda a região do Caribe Oriental, foi considerado um passo em direção a uma abordagem mais coordenada da segurança cibernética, com discussões desde iniciativas de educação e capacidade técnica até a promoção da conscientização enfatizando as ações para a criação de um CSIRT, que ainda não existe no país.[319]

Há alguma presença de provedores de serviços de cibersegurança do setor privado e as oportunidades de formação em segurança cibernética são limitadas, mas o governo está ciente do importante papel que a educação desempenha na cibersegurança, especificamente nos níveis escolar e comunitário.[320] Por fim, aparentemente o governo não proporcionou oportunidades de capacitação em segurança cibernética, embora tenha enviado representantes a vários eventos de formação organizados pela OEA, como a formação internacional em crimes cibernéticos sobre a preservação de provas digitais e investigações baseadas na Internet, apresentado em colaboração com o Departamento de Estado dos EUA em 2016, e a Oficina Sub-regional sobre a Proteção de Infraestruturas Críticas: Cibersegurança e Proteção de Fronteiras em 2017. Em maio de 2017, a Internet Society abriu um capítulo em São Vicente e Granadinas com o objetivo de promover uma Internet aberta e confiável.[321]

Embora o país já tivesse leis sobre cibersegurança, inclusive a Lei de Provas Eletrônicas de 2004 e a Lei de Transações Eletrônicas de 2015,[322] não havia nenhuma lei específica tratando de crimes cibernéticos. Entretanto, em agosto de 2016, os legisladores sancionaram a Lei de Crimes Cibernéticos,[323] proporcionando ao país uma legislação substantiva e processual para enfrentar os crimes cibernéticos de forma mais eficaz.[324]

Entre 2012 e 2015, São Vicente e Granadinas teve um Plano de Estratégia de Desenvolvimento de Governo Eletrônico, que delineava as medidas necessárias para o programa "fornecer uma infraestrutura tecnológica comum estável e segura, que observe um conjunto de políticas e normas para a conexão com essas infraestruturas comuns e seu uso".[325] Além disso, o governo eletrônico faz parte da Estratégia e Plano de Ação Nacional de Tecnologia da Informação e Comunicação do país.[326]

Indicadores: São Vicente e Granadinas

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

	2016	2020
3-1 Conscientização		
Programas de conscientização	■□□□□	■□□□□
Conscientização de executivos	■■□□□	■■□□□
3-2 Marco para a educação		
Fornecimento	■□□□□	■□□□□
Administração	■□□□□	■□□□□
3-3 Marco para treinamento profissional		
Fornecimento	■□□□□	■■□□□
Administração	■■□□□	■■□□□

D4 Marcos legais e regulatórios

	2016	2020
4-1 Marcos jurídicos		
Marcos legislativos para a segurança de TICs	■■□□□	■■□□□
Privacidade, liberdade de expressão e outros direitos humanos na Internet	■□□□□	■■□□□
Legislação sobre proteção de dados	□□□□□	■■■□□
Proteção das crianças na Internet	□□□□□	■■□□□
Legislação de proteção ao consumidor	□□□□□	■■□□□
Legislação sobre propriedade intelectual	□□□□□	■■□□□
Legislação substantiva sobre cibercrimes	■■■□□	■■■□□
Legislação substantiva sobre cibercrimes	■□□□□	■■□□□
4-2 Sistema da justiça penal		
Aplicação da lei	■□□□□	■□□□□
Ação penal	■□□□□	■□□□□
Tribunais	■■□□□	■■□□□
4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético		
Cooperação formal	□□□□□	■□□□□
Cooperação informal	□□□□□	■□□□□

D5 Normas, organizações e tecnologias

	2016	2020
5-1 Observância das normas		
Normas de segurança de TICs	■□□□□	■□□□□
Normas para aquisições	■□□□□	■□□□□
Normas para desenvolvimento de software	■□□□□	■□□□□
5-2 Resiliência da infraestrutura de Internet		
Resiliência da infraestrutura da Internet	■■□□□	■□□□□
5-3 Qualidade de software		
Qualidade de software	□□□□□	■□□□□
5-4 Controles técnicos de segurança		
Controles técnicos de segurança	□□□□□	■□□□□
5-5 Controles criptográficos		
Controles criptográficos	□□□□□	■■□□□
5-6 Mercado de cibersegurança		
Tecnologias de cibersegurança	■□□□□	■□□□□
Seguro contra cibercrimes	□□□□□	■□□□□
5-7 Divulgação responsável		
Divulgação responsável	■□□□□	■□□□□

Suriname

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Suriname ainda não aprovou uma estratégia nacional de cibersegurança, mas, no final de 2014, o governo iniciou o processo de criação de uma estratégia em colaboração com a OEA. Além disso, a Visão de TICs 2020 do Suriname requer a melhoria da segurança cibernética e a promoção da conscientização sobre as ameaças cibernéticas.[327] Ainda não há um CSIRT nacional, mas este está sendo desenvolvido pela Diretoria de Segurança Nacional.

Há empresas que prestam serviços de segurança cibernética no Suriname, embora tais serviços sejam limitados. Ademais, as oportunidades de formação superior em segurança cibernética são limitadas; o governo está começando a oferecer formações na área e também tem recebido apoio de organismos internacionais para realizar capacitações técnicas e discussões sobre segurança cibernética.[328]

Em julho de 2019, o Governo do Suriname instalou oficialmente o Comitê Nacional de Segurança Cibernética. Devido ao aumento dos ataques cibernéticos e dos crimes cibernéticos no Suriname, faz-se necessário o aprimoramento das infraestruturas de TI devido à contínua digitalização do mundo. Em conexão com isso, a Diretoria de Segurança Nacional criou esse comitê com as seguintes tarefas:

- Atualizar o plano estratégico de cibersegurança,
- Implementar o plano estratégico de cibersegurança, e
- Instituir o CSIRT nacional.

O Suriname lançou sua campanha de conscientização sobre segurança cibernética por meio de infomerciais, mídias sociais, programas de rádio e televisão e sites oficiais.

Recentemente, o país incorporou os crimes cibernéticos à sua legislação, além de avançar na elaboração de um projeto de lei sobre privacidade e proteção de dados, que ainda está em tramitação no parlamento. Em dezembro de 2018, o parlamento aprovou uma legislação de identificação eletrônica (E-ID).

O Suriname conta com uma estratégia de governo eletrônico que visa aperfeiçoar o atendimento à sociedade por meio do funcionamento mais eficiente do governo com a implantação de novos recursos digitais. Para implementá-la, o Governo do Suriname instaurou a Comissão de Governo Eletrônico, priorizando a melhoria dos serviços de governo para governo, governo para empresas e governo para cidadãos.[329]

Indicadores: Suriname

D1 Política e Estratégia de Cibersegurança

2016 | 2020

1-1 Estratégia nacional de cibersegurança

- Desenvolvimento da estratégia
- Organização
- Conteúdo

1-2 Resposta a incidentes

- Identificação de incidentes
- Organização
- Coordenação
- Modo de funcionamento

1-3 Proteção de infraestruturas críticas (IC)

- Identificação
- Organização
- Gestão e resposta a riscos

1-4 Gerenciamento de crises

- Gerenciamento de crises

1-5 Ciberdefesa

- Estratégia
- Organização
- Coordenação

1-6 Redundância de comunicações

- Redundância de comunicações

D2 Cibercultura e Sociedade

2016 | 2020

2-1 Mentalidade de cibersegurança

- Governo
- Setor privado
- Usuários

2-2 Confiança e segurança na Internet

- Confiança e segurança do usuário na Internet
- Confiança do usuário nos serviços de governo eletrônico
- Confiança do usuário nos serviços de comércio eletrônico

2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet

- Compreensão do usuário sobre proteção de informações pessoais na Internet

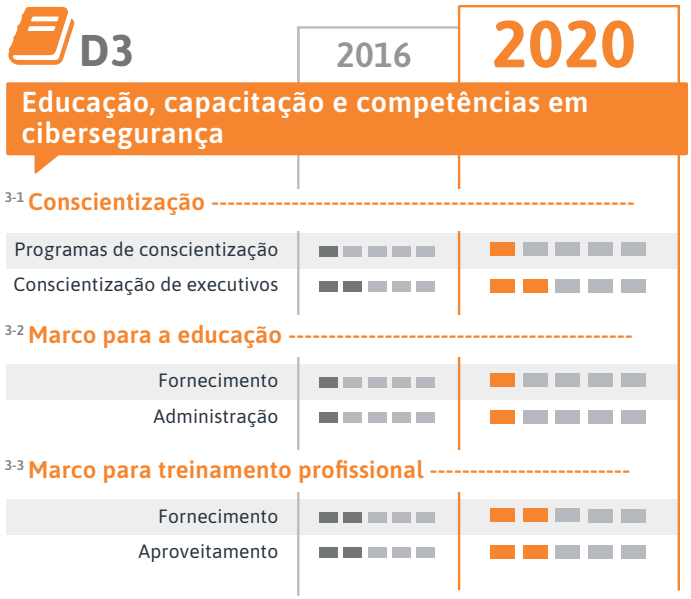
2-4 Mecanismos de denúncia

- Mecanismos de denúncia

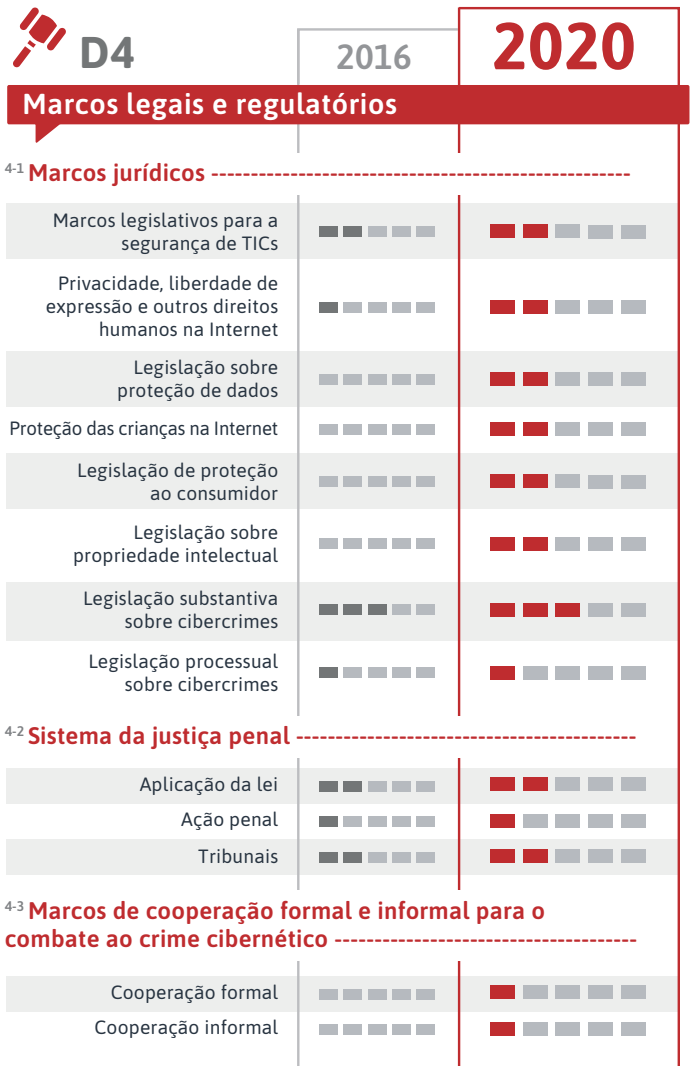
2-5 Mídia e redes sociais

- Mídia e redes sociais

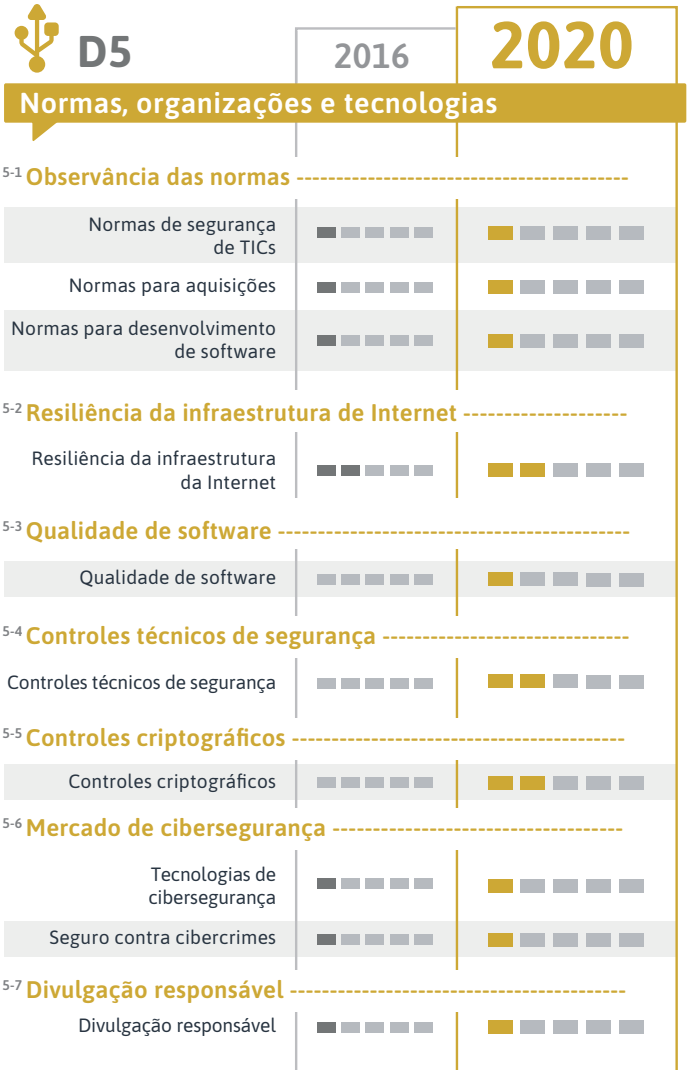
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Trinidad e Tobago

Habitantes
*Ref.:Banco Mundial**

Assinaturas de telefone celular
*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet
*Ref.:UIT***

Trinidad e Tobago lançou sua estratégia nacional de cibersegurança em 2012, com o objetivo geral de criar um ambiente digital seguro para seus cidadãos por meio do desenvolvimento das capacidades de proteção e gerenciamento de incidentes de cibersegurança, bem como da educação da população sobre as melhores práticas para possibilitar atenuar ao máximo os riscos. Além disso, a estratégia determina cinco áreas principais a serem abordadas: governança, gestão de incidentes, colaboração, cultura e legislação.[330] Como parte da área de gestão de incidentes, o país instituiu o CSIRT nacional por intermédio do Ministério de Segurança Nacional.[331] O TTCSIRT também é membro do CSIRT Américas, permitindo assim a colaboração internacional. A estratégia também define a necessidade de uma agência exclusiva para se encarregar da segurança cibernética do país. Para a criação dessa agência, foi proposto um projeto de "lei que disponha sobre a criação da Agência de Segurança Cibernética de Trinidad e Tobago e assuntos afins". Entretanto, até o momento esse projeto de lei não foi aprovado.

A estratégia de segurança cibernética define infraestruturas críticas como "sistemas informatizados, dispositivos, redes, programas informatizados e dados informatizados tão essenciais para o país que a incapacitação, destruição ou interferência em tais sistemas e ativos teria um impacto debilitante na segurança, defesa ou relações internacionais do Estado".[332] Contudo, ela não definiu a responsabilidade pela proteção das infraestruturas críticas, mas simplesmente menciona que a colaboração entre o governo, o setor privado e a academia é necessária para protegê-las contra incidentes cibernéticos.

Há alguns provedores de serviços de segurança cibernética no setor privado, mas a falta de envolvimento desse setor é generalizada. O projeto de lei da Agência de Segurança Cibernética de Trinidad e Tobago defende a intensificação da cooperação entre a população e o setor de segurança cibernética, mas só agora a segurança cibernética está começando a ser encarada como uma prioridade.[333]

Ainda que não haja ampla oferta de cursos universitários de segurança cibernética, as instituições de ensino superior de Trinidad e Tobago estão começando a introduzir esses cursos. Adicionalmente, há oportunidades oferecidas pelo governo, como a oficina de capacitação em segurança cibernética, ministrada pelo Ministério do Planejamento e Desenvolvimento, onde estudantes de nível médio e superior e profissionais de TI podem aprender os conceitos básicos da segurança cibernética.[334]

Com relação à legislação de crimes cibernéticos, o país aguarda a aprovação de "um projeto de lei para a tipificação de ilícitos relacionados a crimes cibernéticos e questões afins". Esse projeto de lei oferece uma definição completa de vários crimes cibernéticos, bem como a forma de repressão a tais crimes. A Lei nº 13 de 2011 dá proteção à privacidade e informações pessoais.[335] Essa lei é aplicável a todos os "que manuseiam, armazenam ou processam informações pessoais pertencentes a outrem".

Embora o país não disponha de uma estratégia específica de governo eletrônico, ela faz parte do Plano Nacional de TIC "FastForward II", que está atualmente em fase de projeto. Um dos objetivos estratégicos deste plano é melhorar a prestação de serviços públicos e uma de suas estratégias é aumentar a eficiência do governo. Trinidad e Tobago já tem um portal governamental, o ttconnect.gov.tt, que oferece uma série de serviços, mas pretende expandir os serviços eletrônicos disponíveis para os consumidores.[336]

Indicadores: Trinidad e Tobago

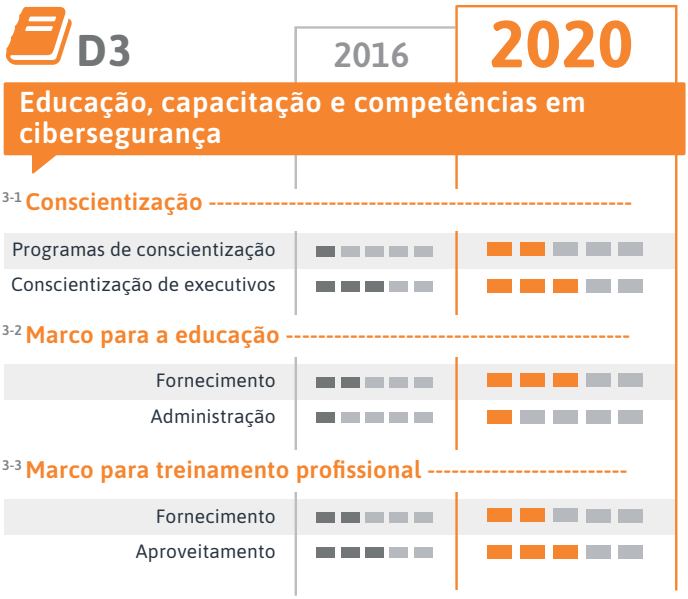
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

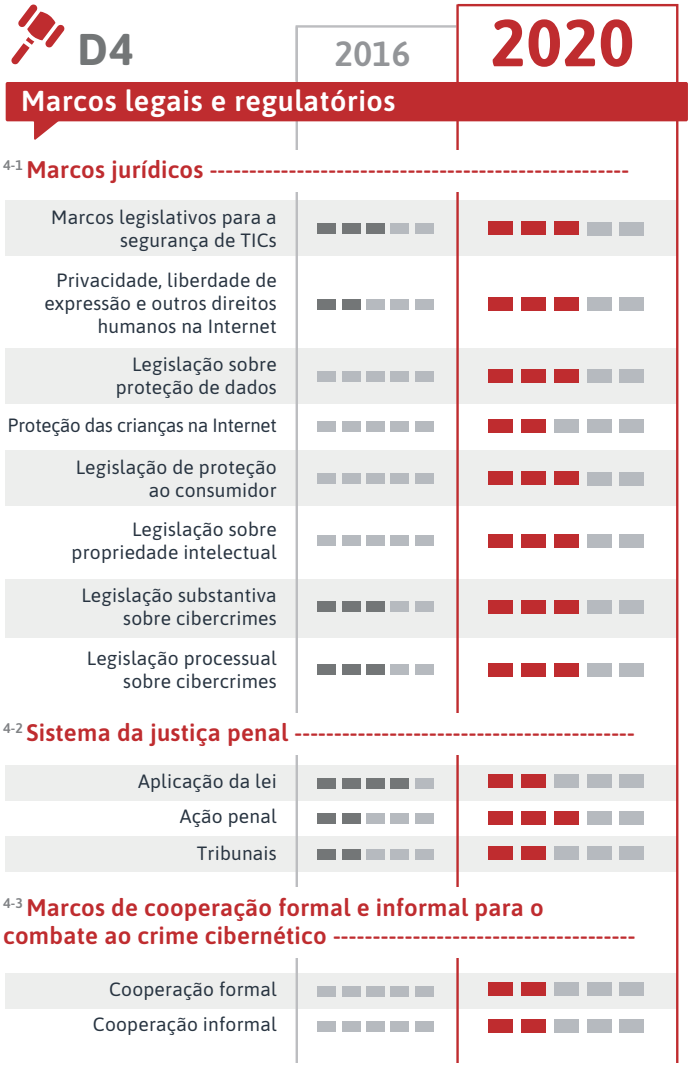
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

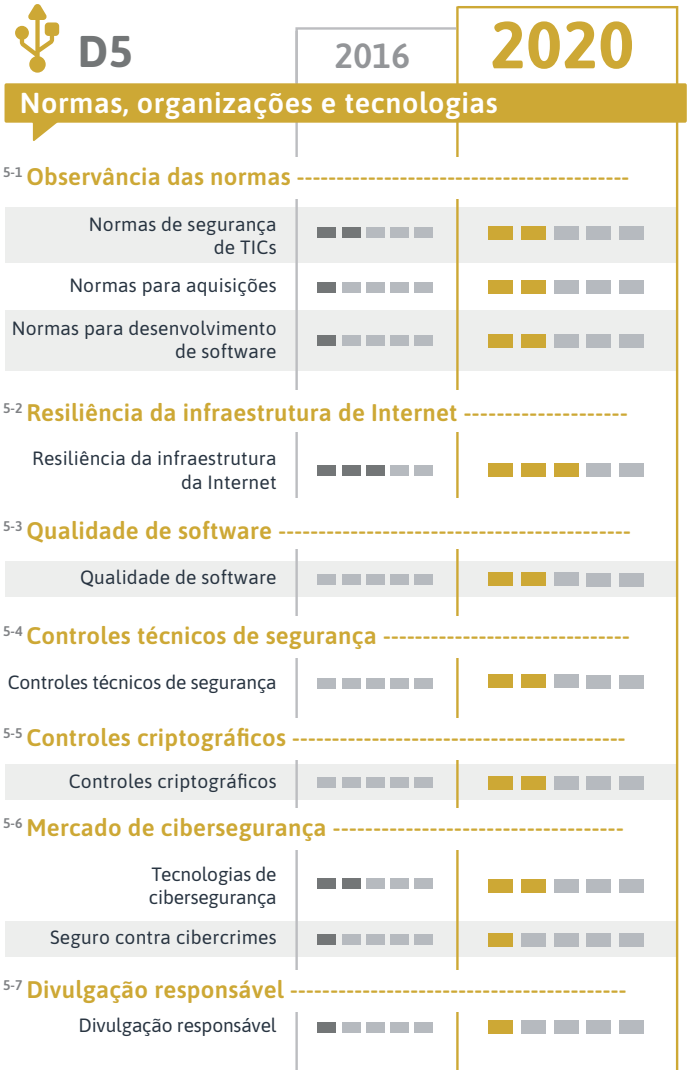
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Uruguai

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

O Uruguai possui um marco de segurança cibernética, embora não seja uma estratégia nacional de cibersegurança. O documento é uma estrutura organizada com referência às normas internacionais aplicáveis aos regulamentos nacionais para a melhoria da segurança cibernética de infraestruturas críticas e entidades públicas.[337] O Uruguai também conta com um CSIRT nacional, o CERTuy, vinculado à Agência para o Governo Eletrônico e à Sociedade da Informação e do Conhecimento (AGESIC).[338] Por meio do projeto Fortalecimento da Segurança Cibernética no Uruguai, o país tornou-se o primeiro da região a ter acesso a assistência técnica e financeira por meio de uma operação de empréstimo do BID voltada exclusivamente para o fortalecimento da segurança cibernética no nível nacional.[339] Por sua vez, a AGESIC recebeu assessoria técnica coordenada pelo BID para a criação de um Centro Nacional de Treinamento em Segurança Cibernética e apoio ao Centro de Operações de Segurança do Governo (GSOC). O CERTuy também é membro da rede CSIRT Américas, de modo que pode aproveitar ao máximo a natureza colaborativa dessa rede.

Embora o Uruguai não defina as infraestruturas críticas nacionais, a responsabilidade por sua proteção recai sobre o D-CSIRT, o CSIRT subordinado ao Ministério da Defesa de acordo com o Decreto n° 36/015, que o criou.[340] Além disso, o orçamento da AGESIC para 2018 destinou um volume considerável de recursos para o fortalecimento da segurança da informação.[341]

O Uruguai conta com alguns provedores de serviços de segurança cibernética e parece haver uma boa consciência geral das questões de segurança cibernética por parte do setor privado, mas o governo parece estar fornecendo uma parcela maior dos serviços e treinamentos na área. O governo oferece cursos de cibersegurança e ciberdefesa em nível iniciante para integrantes dos setores público e privado.[342] O CERTuy também dispõe de uma série de guias e manuais de melhores práticas em seu site, que fornece recursos para quem deseja ficar mais informado sobre a segurança cibernética.[343] No conjunto, há várias universidades que oferecem formação e cursos de segurança cibernética.

No que tange ao marco legal e regulatório, há alguns projetos de lei sobre crime cibernético, voltados tanto para a legislação substantiva quanto a processual, para a persecução dos crimes cibernéticos após sua comprovação.[344] Por outro lado, o país possui legislação sobre proteção de dados pessoais e privacidade, na forma da Lei n° 18.331, que se aplica a bases de dados dos setores público e privado.[345] O Uruguai tem o Plano de Governo Eletrônico 2020 objetiva criar valor público por meio de serviços que atendam às necessidades, expectativas e preferências dos cidadãos de forma aberta, colaborativa, inteligente, eficiente, integrada e confiável.[346]

O governo eletrônico foi incluído na Agenda Digital 2020 como parte do pilar relacionado à inovação na relação entre o governo e seus cidadãos.[347] Atualmente, o Uruguai conta com um portal governamental que oferece uma série de serviços para acompanhar o andamento de diversos processos e agendar horários em instituições governamentais, para o uso de assinaturas eletrônicas e para obter informações relevantes.[348]

Indicadores: Uruguai

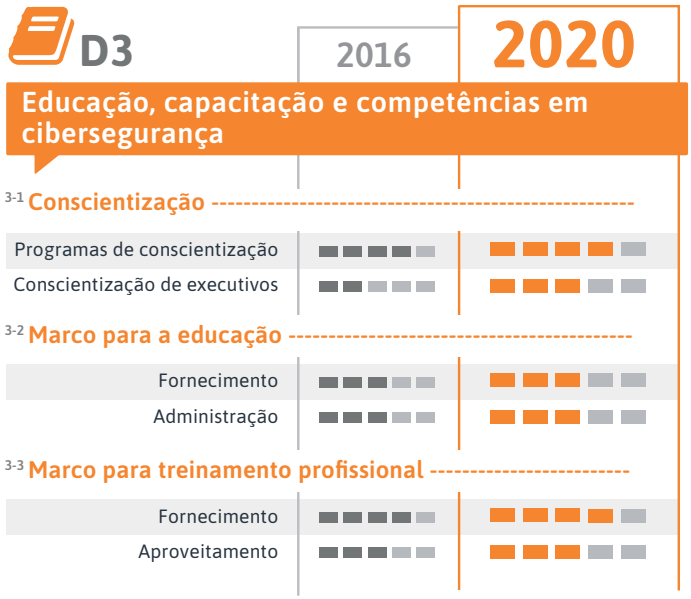
D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia	3	4
Organização	3	4
Conteúdo	2	3
1-2 Resposta a incidentes		
Identificação de incidentes	4	4
Organização	4	5
Coordenação	4	5
Modo de funcionamento	0	4
1-3 Proteção de infraestruturas críticas (IC)		
Identificação	2	2
Organização	2	3
Gestão e resposta a riscos	2	3
1-4 Gerenciamento de crises		
Gerenciamento de crises	2	3
1-5 Ciberdefesa		
Estratégia	2	3
Organização	3	3
Coordenação	3	3
1-6 Redundância de comunicações		
Redundância de comunicações	3	4

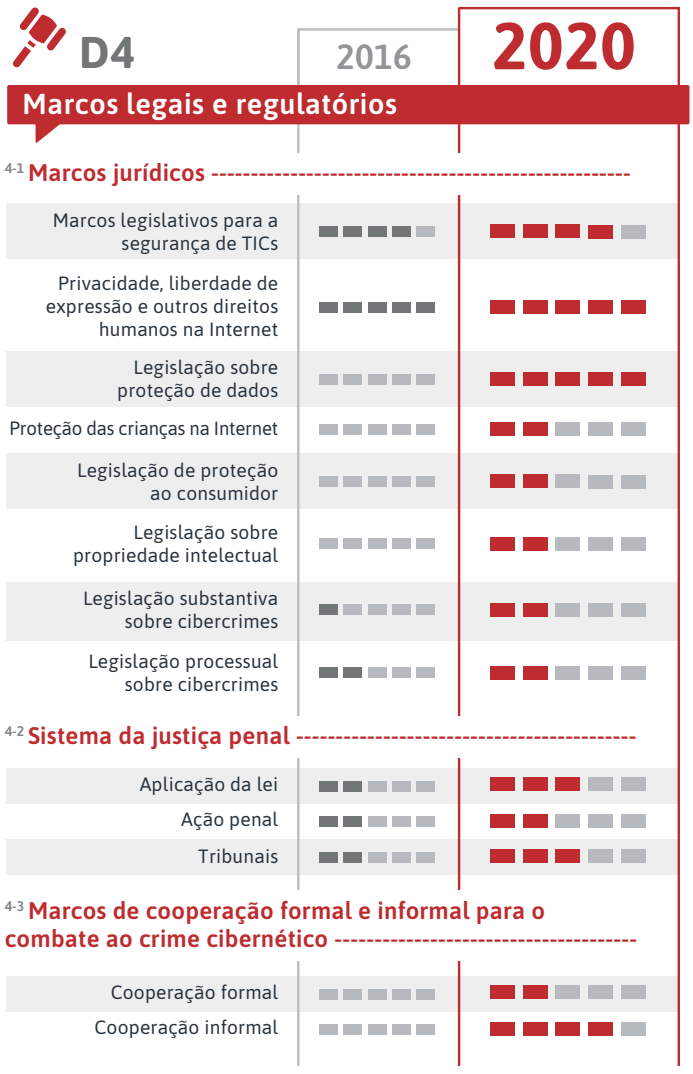
D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo	4	5
Setor privado	3	3
Usuários	3	3
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet	4	5
Confiança do usuário nos serviços de governo eletrônico	5	5
Confiança do usuário nos serviços de comércio eletrônico	4	4
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet	0	5
2-4 Mecanismos de denúncia		
Mecanismos de denúncia	0	4
2-5 Mídia e redes sociais		
Mídia e redes sociais	0	4

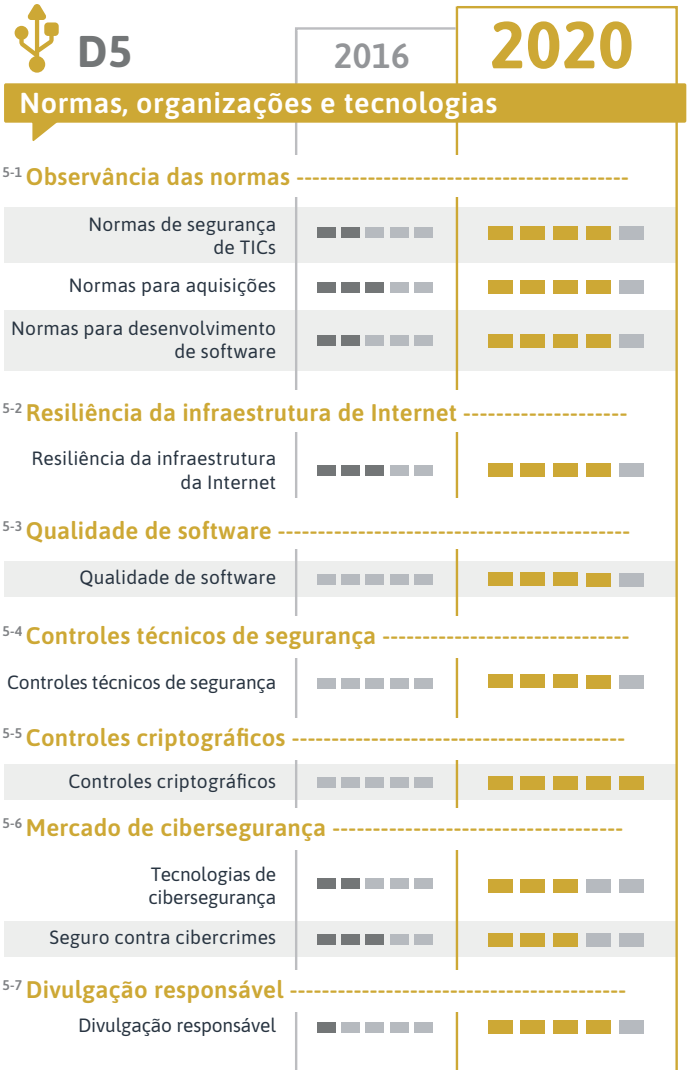
D3 Educação, capacitação e competências em cibersegurança



D4 Marcos legais e regulatórios



D5 Normas, organizações e tecnologias



Venezuela

Habitantes

*Ref.:Banco Mundial**

Assinaturas de telefone celular

*Ref.:UIT***

Pessoas com acesso à Internet

Penetração da Internet

*Ref.:UIT***

Segundo dados de 2017, a Venezuela não possui uma estratégia nacional de cibersegurança. Contudo, existe um sistema nacional de cibersegurança sob a responsabilidade da Superintendência de Serviços de Certificação Eletrônica (SUSCERTE), conforme disposto no Artigo n° 54 da Lei de Governo Eletrônico.[349] O objetivo desse sistema é criar condições que gerem confiança no uso das TICs nas mãos dos detentores do poder e adotar medidas que forneçam níveis de segurança adequados para elas.[350] A SUSCERTE também é a sede do CSIRT nacional da Venezuela, o VenCERT, cujo objetivo principal é "prevenir, detectar e gerenciar os incidentes gerados nos sistemas de informação do Estado e nas infraestruturas críticas da nação por meio do gerenciamento de vulnerabilidades e incidentes de segurança cibernética".[351]

Uma das incumbências do VenCERT é oferecer capacitação em segurança cibernética.[352] Durante a conferência internacional Venezuela Digital 2017, o superintendente da SUSCERTE ressaltou que, em 2017, 687 pessoas foram capacitadas em segurança cibernética na Venezuela.[353] Embora não pareça haver muitas oportunidades para os venezuelanos darem continuidade a seus estudos especificamente em segurança cibernética, há muitas opções em temas afins, como ciência da computação ou engenharia de sistemas.

Algumas empresas privadas prestam serviços de segurança da informação. Entretanto, o número de empresas e o alcance dos serviços que elas oferecem são limitados. Ademais, parece haver uma falta generalizada de conhecimento por parte do setor privado em relação à segurança cibernética, em que pese algumas empresas de destaque terem começado a priorizar a segurança cibernética.

Quanto à legislação, a Venezuela introduziu a Lei Especial contra Delitos Informáticos em 2001, com o objetivo de proteger os sistemas que usam tecnologias da informação, bem como prevenir e punir os crimes cometidos contra tais sistemas ou com o seu uso.[354] Contudo, não há legislação sobre proteção de privacidade e de dados,[355] embora os artigos da constituição se refiram ao direito à "proteção da honra, vida privada, privacidade, autoimagem, confidencialidade e reputação" (Artigo 60) e "acesso às informações e dados sobre a pessoa ou seu patrimônio em registros oficiais ou privados"[356] (Artigo 28).

Indicadores: Venezuela

D1 Política e Estratégia de Cibersegurança

	2016	2020
1-1 Estratégia nacional de cibersegurança		
Desenvolvimento da estratégia		
Organização		
Conteúdo		
1-2 Resposta a incidentes		
Identificação de incidentes		
Organização		
Coordenação		
Modo de funcionamento		
1-3 Proteção de infraestruturas críticas (IC)		
Identificação		
Organização		
Gestão e resposta a riscos		
1-4 Gerenciamento de crises		
Gerenciamento de crises		
1-5 Ciberdefesa		
Estratégia		
Organização		
Coordenação		
1-6 Redundância de comunicações		
Redundância de comunicações		

D2 Cibercultura e Sociedade

	2016	2020
2-1 Mentalidade de cibersegurança		
Governo		
Setor privado		
Usuários		
2-2 Confiança e segurança na Internet		
Confiança e segurança do usuário na Internet		
Confiança do usuário nos serviços de governo eletrônico		
Confiança do usuário nos serviços de comércio eletrônico		
2-3 Compreensão do usuário sobre a proteção de informações pessoais na Internet		
Compreensão do usuário sobre proteção de informações pessoais na Internet		
2-4 Mecanismos de denúncia		
Mecanismos de denúncia		
2-5 Mídia e redes sociais		
Mídia e redes sociais		

D3 Educação, capacitação e competências em cibersegurança

2016 | 2020

3-1 Conscientização

- Programas de conscientização
- Conscientização de executivos

3-2 Marco para a educação

- Fornecimento
- Administração

3-3 Marco para treinamento profissional

- Fornecimento
- Aproveitamento

D4 Marcos legais e regulatórios

2016 | 2020

4-1 Marcos jurídicos

- Marcos legislativos para a segurança de TICs
- Privacidade, liberdade de expressão e outros direitos humanos na Internet
- Legislação sobre proteção de dados
- Proteção das crianças na Internet
- Legislação de proteção ao consumidor
- Legislação sobre propriedade intelectual
- Legislação substantiva sobre cibercrimes
- Legislação processual sobre cibercrimes

4-2 Sistema da justiça penal

- Aplicação da lei
- Ação penal
- Tribunais

4-3 Marcos de cooperação formal e informal para o combate ao crime cibernético

- Cooperação formal
- Cooperação informal

D5 Normas, organizações e tecnologias

2016 | 2020

5-1 Observância das normas

- Normas de segurança de TICs
- Normas para aquisições
- Normas para desenvolvimento de software

5-2 Resiliência da infraestrutura de Internet

- Resiliência da infraestrutura da Internet

5-3 Qualidade de software

- Qualidade de software

5-4 Controles técnicos de segurança

- Controles técnicos de segurança

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de cibersegurança

- Tecnologias de cibersegurança
- Seguro contra cibercrimes

5-7 Divulgação responsável

- Divulgação responsável

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

BID
Melhorando vidas

OEA
Mais direitos para mais pessoas

Apêndice

Relação de CSIRTs

Países dotados ou em fase de elaboração de uma estratégia nacional de cibersegurança

Membros e observadores da Convenção de Budapeste

Acrônimos

Referências

CSIRTs

Tipo de CSIRT

- Governo
- Acadêmico
- Nacional
- Militar
- Polícia

Relação de CSIRTs

Argentina

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Governo	BACSIRT	https://www.ba-csirt.gob.ar/	Cidade de Buenos Aires	Sim
Acadêmico	CERTUNLP	http://www.cespi.unlp.edu.ar/cert	Universidade Nacional de la Plata	Sim

Barbados

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CIRT_BB	N/A	Centro Nacional de Resposta a Incidentes de Segurança Cibernética de Barbados	Sim

Bolívia

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CSIRT-Bolivia	http://www.csirt.gob.bo/	N/A	Sim

Chile

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Governo	CSIRTGob.cl	http://www.csirt.gob.cl/	Ministério do Interior e da Segurança Pública	Sim

Colômbia

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	colCERT	http://www.colcert.gov.co/	Ministério da Defesa	Sim
Militar	CCOC-ARMADA	https://ccoc.mil.co	Comando Conjunto Cibernético	Sim

Costa Rica

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CSIRT-CR	https://www.micit.go.cr/	Ministério da Ciência, Tecnologia e Telecomunicações	Sim

República Dominicana

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CSIRT-RD	https://csirt.gob.do/	Presidência da República	Sim

Equador

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	EcuCERT	https://www.ecucert.gob.ec/	Agencia de Regulação e Controle das Telecomunicações do Equador	Sim
Militar	COCIBER	N/A	Comando de Ciberdefesa	Sim

Guatemala

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CSIRT-gt	https://www.cert.gt/	Ministério de Governo	Sim

Guiana

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CIRT.GY	https://cirt.gy/	Ministério da Segurança Pública	Sim

Jamaica

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	JA-CIRT	https://www.mset.gov.jm/cyber-incident-response-team-jacirt	Ministério da Ciência, Energia e Tecnologia	Sim

México

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CERT-MX	https://www.gob.mx/sspc	Comissão Nacional de Segurança	Sim
Militar	SEDENA-CSIRT	https://www.gob.mx/sedena	Secretaria da Defesa Nacional	Sim
Militar	CSIRT-SEMAR	https://www.gob.mx/semar	Secretaria da Marinha	Sim

Panamá

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CSIRT-Panamá	https://cert.pa/	Autoridade Nacional para a Inovação Governamental	Sim

Paraguai

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CERT-PY	https://www.cert.gov.py/	Ministério da Tecnologia da Informação e Comunicações	Sim

Peru

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Militar	CITELE_EP	http://www.ejercito.mil.pe/cotele/	Comando de Telemática do Exército do Peru	Sim
Militar	CSTPERU	https://fap.mil.pe/	Comando Conjunto das Forças Armadas do Peru	Sim
Militar	CSIRT-MGP	N/A	Marinha de Guerra do Peru	Sim

Suriname

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	SurCIRT (En proceso)	www.gov.sr	Serviço Central de Inteligência e Segurança	Sim

Trinidad e Tobago

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	TTCSIRT	http://ttcsirt.gov.tt/	Ministério da Segurança Nacional	Sim

Estados Unidos da América

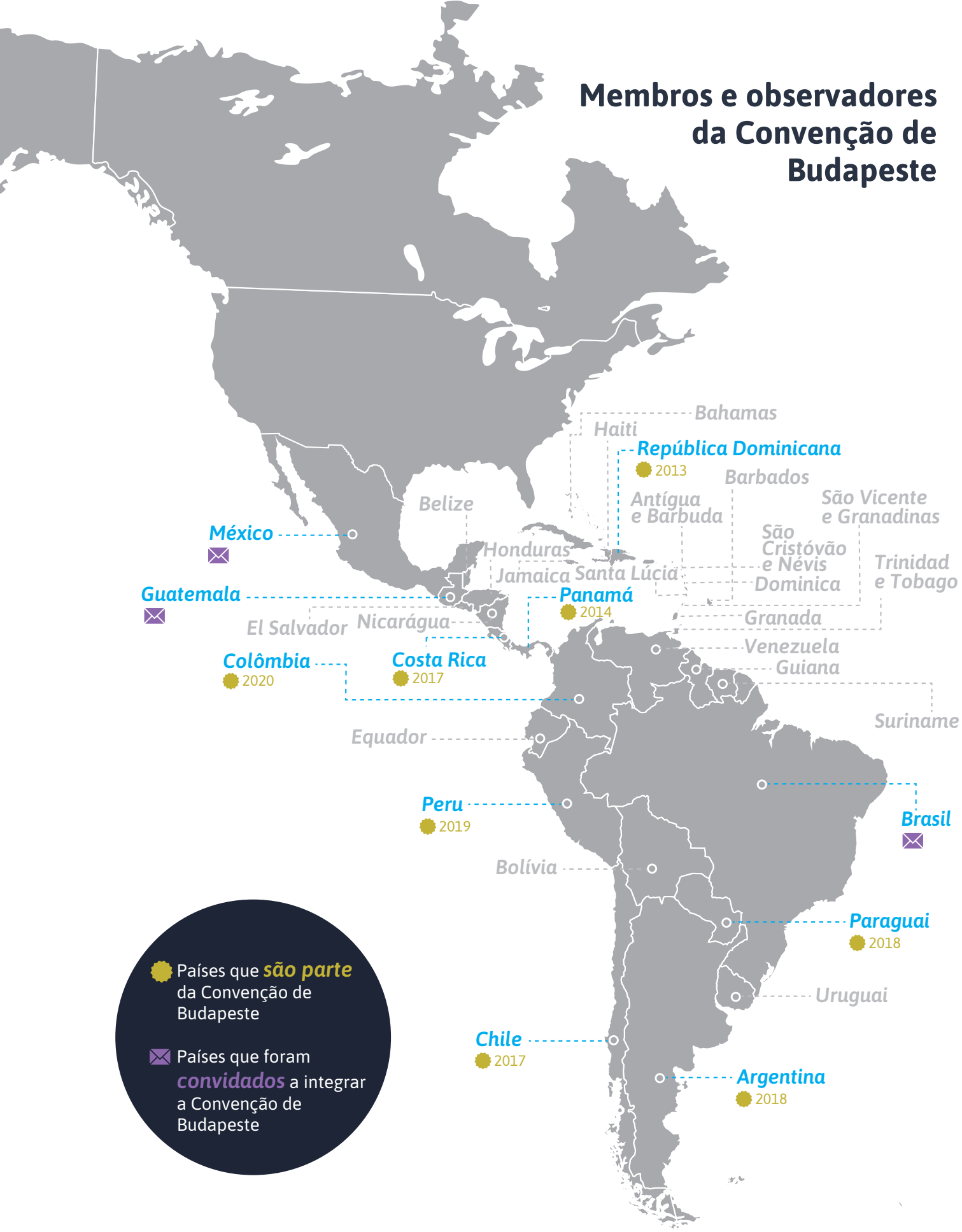
Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CISA	https://us-cert.cisa.gov/	Departamento da Segurança Nacional (DHS)	Sim

Uruguai

Tipo	CSIRT	Site do CSIRT	Instituição hospedeira	CSIRT Américas
Nacional	CERTuy	https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/	Agência do Governo Eletrônico, da Sociedade da Informação e do Conhecimento	Sim
Militar	DCSIRT	https://www.gub.uy/ministerio-defensa-nacional/	Ministério da Defesa Nacional	Sim

Países dotados ou em fase de elaboração de uma estratégia nacional de cibersegurança

Membros e observadores da Convenção de Budapeste



Países que **são parte** da Convenção de Budapeste

Países que foram **convidados** a integrar a Convenção de Budapeste

Acrônimos

AGESIC
Agência de Governo Eletrônico e da Sociedade da Informação e Conhecimento do Uruguai

AGETIC
Agência de Governo Eletrônico de Tecnologias da Informação e Comunicação da Bolívia

ARCOTEL
Agência de Regulação e Controle das Telecomunicações do Equador

BA-CSIRT
CSIRT da Cidade de Buenos Aires

BID
Banco Interamericano de Desenvolvimento

CARICOM
Comunidade do Caribe

ccTLD
Domínio nacional de nível superior ou Domínio de topo de código de país

CERT
Equipe de Resposta a Emergências de Computadores

CERT.br
CERT nacional do Brasil

CERT-MX
CSIRT nacional do México

CERT-PY
CSIRT nacional do Paraguai

CERTuy
CSIRT nacional do Uruguai

CGII
Centro de Gestão de Incidentes Informáticos da Bolívia

CICCD
Centro Israelense de Defesa Cibernética do Caribe

CIRT.GY
CSIRT nacional da Guiana

CISM
Gerente Certificado em Segurança da Informação (ISACA)

CISSP
Profissional Certificado em Segurança de Sistemas de Informação (ISC2)

CITO
Escritório Central de Tecnologia da Informação de Belize

CMF
Comissão para o Mercado Financeiro do Chile

CMM
Modelo de maturidade da capacidade de segurança cibernética das nações

COE
Conselho da Europa

colCERT
CERT nacional da Colômbia

CONATEL
Conselho Nacional de Telecomunicações do Haiti

CONATEL
Conselho Nacional de Telecomunicações de Honduras

CSIRT
Grupo de Resposta a Incidentes de Segurança em Computadores

CSIRT-CR
CSIRT nacional da Costa Rica

CSIRT-gt
CSIRT nacional da Guatemala

CSIRT-RD
CSIRT nacional da República Dominicana

CSTF
Força-Tarefa Nacional de Segurança Cibernética de Belize

D-CSIRT
CSIRT do Ministério da Defesa do Uruguai

DPSM
Divisão de Modernização do Setor Público de Santa Lúcia

ECSO
Organização Europeia de Segurança Cibernética

EcuCERT
CSIRT nacional do Equador

E-ID
Identificação eletrônica

Europol
Agência da União Europeia para a Cooperação Policial

GCI
Índice Global de Cibersegurança

GCSCC
Centro Global de Capacidade de Segurança Cibernética

GDPR
Regulamento Geral sobre a Proteção de Dados da União Europeia

GITS
Serviços de Tecnologia da Informação do Governo de Santa Lúcia

GLACY+
Ação Global Ampliada contra o Cibercrime

GSOC
Centro de Operações de Segurança Governamental

GTCSC
Grupo de trabalho de segurança e crimes cibernéticos do Haiti

HPC
Computador de alto desempenho

IC
Infraestrutura crítica

ICCN
Infraestrutura cibernética nacional crítica

ICIC
Programa Nacional de Infraestruturas Críticas de Informação e Cibersegurança da Argentina

INCIBE
Instituto Nacional de Segurança Cibernética da Espanha

INTERPOL
Organização Internacional de Polícia Criminal

JaCIRT
CSIRT nacional da Jamaica

MFF
Programa Quadro Financeiro Plurianual da UE

MICITT
Ministério da Ciência, Tecnologia e Telecomunicações da Costa Rica

MinTIC
Ministério da Tecnologia e Comunicações da Colômbia

MISP
Plataforma de compartilhamento

de informações sobre malware e compartilhamento de ameaças

MITIC
Ministério de Tecnologias da Informação e Comunicações do Paraguai

MPTC
Ministério de Obras Públicas, Transporte e Comunicações do Haiti

MSET
Ministério da Ciência, Energia e Tecnologia da Jamaica

NIS
Sistemas de redes e informação

OEA
Organização dos Estados Americanos

ONGEI
Escritório Nacional de Governo Eletrônico e Informática do Peru

OSCE
Organização para a Segurança e Cooperação na Europa

PBL
Empréstimo baseado em políticas

PeCERT
CSIRT nacional do Peru

PMEs
Pequenas e médias empresas

PPPc
Parceria público-privada contratual

PUC
Comissão de Serviços Públicos de Belize

PwC
PricewaterhouseCoopers

P&I
Pesquisa e inovação

SalCERT
CSIRT nacional de El Salvador

SERCOP
Serviço Nacional de Contratações Públicas do Equador

SINARDAP
Sistema Nacional de Registro de Dados Públicos do Equador

SUSCERTE
Superintendência de Serviços de Certificação Eletrônica da Venezuela

TELCOR
Instituto de Telecomunicações e Serviços Postais da Nicarágua

TIC
Tecnologia da Informação e Comunicação

TTCSIRT
CSIRT nacional de Trinidad e Tobago

UE
União Europeia

UIT
União Internacional de Telecomunicações

UNGGE
Grupo de Especialistas Governamentais das Nações Unidas

VenCERT
CSIRT nacional da Venezuela

Referências

1. ThreatMetrix Cybercrime Report: An Interview (November 2019).
https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/.

2. www.trends.google.com.

3. Os números representam o interesse da busca em relação ao ponto mais alto do gráfico para uma determinada região e horário. Um valor de 100 é a popularidade máxima do termo. Um valor de 50 significa que o termo é meio popular. Um valor de 0 significa que não há dados suficientes para esse termo.

4. Consultar https://eeas.europa.eu/topics/eu-global-strategy_en.

5. Comissão Europeia. 2017. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Disponível em
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en.

6. Comissão Europeia. 2015. The European Agenda on Security. Disponível em:
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

7. Comissão Europeia. 2016. Joint Framework on countering hybrid threats: a European Union response. Disponível em
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

8. Comissão Europeia. 2017. Launching the European Defence Fund. Disponível em
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0295&from=EN.

9. Diretiva (UE) n° 2.016/1148 do Parlamento e do Conselho Europeu, de 6 de julho de 2016, relativa a medidas para um elevado nível comum de segurança de redes e sistemas de informação em toda a União.

10. Diretiva n° 2013/40/EU do Parlamento e do Conselho Europeu, de 12 de agosto de 2013, relativa a ataques contra sistemas de informação.

11. A Convenção sobre Crime Cibernético é o primeiro tratado internacional sobre crimes cometidos pela Internet e outras redes de computadores, tratando especificamente de violações de direitos autorais, fraude relacionada a computadores, pornografia infantil e violações de segurança de redes. Em 2017, 55 governos haviam retificado ou se integrado à Convenção do Conselho da Europa sobre Crimes Cibernéticos.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

12. Comissão Europeia. 2017. Digital4Development: mainstreaming digital technologies and services into EU Development Policy. Disponível em:
https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF.

13. Em setembro de 2017, a UE conduziu diálogos cibernéticos com os Estados Unidos, China, Japão, República da Coreia e Índia.

14. Ver http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

15. Hintermann, Francis. 2020. 3 Powerful Ways the Pandemic Is Changing Research Forever. Disponível em
https://www.accenture.com/us-en/blogs/accenture-research/3-powerful-ways-the-pandemic-is-changing-research-forever.

16. International Data Corporation. 2019. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Disponível em
https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

17. WEF (Fórum Econômico Mundial) 2020. The Global Risks Report 2020. Disponível em
https://www.weforum.org/reports/the-global-risks-report-2020.

18. WEF (Fórum Econômico Mundial). 2020. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. Disponível em
https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications.

19. Cybersecurity Ventures. 2019. The 2019 Official Annual Cybercrime Report. Disponível em
https://www.herjavecgroup.com/resources/2019-official-annual-cybercrime-report/.

20. WEF (Fórum Econômico Mundial). 2018. Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Disponível em http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf.

21. OCDE(Organização para a Cooperação e o Desenvolvimento Econômico). 2019. Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives. Paris: OECD Publishing. Disponível em https://doi.org/10.1787/8bb3c9f1-en.

22. ECLAC. 2018. Proposed Digital Agenda for Latin America and the Caribbean (eLAC2020). Sixth Ministerial Conference on the Information Society in Latin America and the Caribbean. Disponível em https://repositorio.cepal.org/bitstream/handle/11362/43464/S1800206_en.pdf.

23. WEF (Fórum Econômico Mundial) 2020. Incentivizing responsible and secure innovation: Principles and guidance for investors. Disponível em https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-a-framework-for-entrepreneurs-and-investors.

24. AustCyber. 2019. Australia's Cyber Security Sector Competitiveness Plan 2019: Driving Growth and Global Competitiveness. Disponível em https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

25. OEA (Organization of American States) and ISA (Internet Security Alliance). 2019. Cyber-Risk Oversight Handbook for Corporate Boards. Disponível em https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf.

26. OCDE et al. 2019. Latin American Economic Outlook 2019: Development in Transition. Paris: OECD Publishing. Disponível em https://doi.org/10.1787/8bb3c9f1-en.

27. O Grupo de Especialistas Governamentais para a Promoção do Comportamento Responsável do Estado no Espaço Digital no Contexto da Segurança Internacional (GGE), instituído pela Resolução n° 73/266 da Assembleia Geral da ONU, e o Grupo de Trabalho Aberto sobre Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional (OEWG), instituído pela Resolução n° 73/27 da Assembleia Geral da ONU.

28. Inter-American Committee against Terrorism. 2017. Resolution CICTE / RES. 1/17 Establishment of a Working Group on Measures of Promotion of Cooperation and Trust in Cyberspace. Adopted at the 17th plenary session, held on April 7, 2017. Disponível em https://www.oas.org/en/sms/cicte/session_2017.asp.

29. BID: 2016. Disponível em https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

30. https://www.oxfordmartin.ox.ac.uk/cyber-security/.

31. https://www.dcc.uchile.cl/seguridad.

32. http://postgrados.derecho.uchile.cl/diploma-ciberseguridad-pf/.

33. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0.

34. Fonte: Centro Global de Capacidade de Segurança Cibernética.

35. https://technewstt.com/caribbean-cybersecurity-dev/.

36. https://www.caricom.org/media-center/communications/news-from-the-community/caribbean-nations-sign-off-on-cyber-crime-action-plan.

37. https://www.thecaribbeanradio.com/antigua-barbuda-to-host-ict-week-and-symposium/; https://today.caricom.org/2017/03/01/antigua-and-barbuda-to-host-ctu-ict-week-and-symposium/.

38. https://ab.gov.ag/pdf/budget/2017_Budget_Summary.pdf.

39. Pesquisa on-line da OEA

40. https://stopthinkconnect.org.ag/.

41. https://abiit.edu.ag/programs/.

42. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf.

43. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf.

44. https://ab.gov.ag/detail_page.php?page=30.

45. https://www.youtube.com/playlist?list=PL9-4wsDIxlCBn_AKzvPD7cBjf_Q7969IA.

46. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.

47. Informações prestadas pelo País.

48. Informações prestadas pelo País.

49. Projeto AR-L1304: https://www.iadb.org/en/project/AR-L1304.

50. https://www.state.gov/joint-statement-on-u-s-argentina-partnership-on-cyber-policy/.

51. Informações prestadas pelo País.

52. https://www.argentina.gob.ar/modernizacion/direccion-nacional-ciberseguridad/normativa.

53. https://www.pwc.com.ar/es/prensa/ciberseguridad-empresas-argentinas-no-protegen-informacion-sensible.html.

54. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

55. Informações prestadas pelo País.

56. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/ARG?p_auth=RS1Kx55S.

57. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

58. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

59. http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105829/norma.htm.

60. https://dpicuantico.com/sitio/wp-content/uploads/2017/02/87-2017.pdf.

61. http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/316036/norma.htm.

62. http://www.thebahamasweekly.com/publish/bis-news-updates/New_Cyber_Security_Strategy_to_strengthen_data_protection_capabilities34602.shtml;
http://caribbean.cepal.org/news/bahamas-embarks-new-national-cyber-security-strategy-strengthen-data-protection-capabilities.

63. https://thenassauguardian.com/2018/05/11/cybercrime-up-80-percent/.

64. https://bit.ly/2QwdUs7.

65. http://www.tribune242.com/news/2017/jul/21/bahamas-must-do-more-to-combat-cyber-crime/.

66. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf.

67. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf.

68. Projeto BH-L1045: https://www.iadb.org/en/project/BH-L1045.

69. https://www.securehost.com/wp-content/uploads/docs/EBusinessPolicy.pdf.

70. http://www.vision2040bahamas.org/media/uploads/Draft National_Development_Plan_01.12.2016_for_public_release.pdf, p. 52.

71. https://www.bahamas.gov.bs/wps/portal/public/gov/government/eServices/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKN3f19A51NLHwtAhxdDTwNQ_z9Ag19DP2djPULsh0VAZl2VXA!/

72. https://www.bibtbahamas.com/copy-of-mp-business.

73. https://www.bifs-edu.com/cyber-security-.

74. http://www.centralbankbahamas.com/news.php?cmd=view&id=16419.

75. http://gisbarbados.gov.bb/blog/cybersecurity-strategy-for-barbados/.

76. Projeto BA-L1046: https://www.iadb.org/en/project/BA-L1046.

77. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

78. http://gisbarbados.gov.bb/blog/stronger-cyber-security-paramount/.

79. Veja provedores de serviços de segurança cibernética como https://www.caribbeancsc.com/ e https://advantagecaribbean.com/cyber-security/.

80. http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf.

81. https://www.barbadosparliament.com/bills/details/396.

82. https://www.barbadosparliament.com/htmlarea/uploaded/File/Resolutions/Resolution_E_Government_Strategy_2006.pdf.

83. https://www.blp.org.bb/wp-content/uploads/2017/07/bb_National_ICT_Strategic_Plan_Final_2010.pdf; https://repositorio.cepal.org/bitstream/handle/11362/39858/S1501269_en.pdf?sequence=1.

84. http://gisbarbados.gov.bb/blog/government-pushing-digital-technology/.

85. http://www.caribbean360.com/business/barbados-moves-to-introduce-digital-payment-network.

86. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

87. http://www.cavehill.uwi.edu/programmes/#FacultyAnchor.

88. https://businessviewcaribbean.com/belize-cyber-crimes-security-symposum-raises-awareness/.

89. https://www.ub.edu.bz/academics/academic-faculties/faculty-of-science-and-technology/.

90. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

91. http://www.siliconcaribe.com/2017/05/05/belize-leads-caribbean-race-to-cyberattack-preparedness/.

92. https://developernetwork.azurewebsites.net/cito.gov.bz/egovpolicy/BelizeNatleGovPolicy2015.pdf.

93. https://web.senado.gob.bo/prensa/noticias/aprueban-pl-que-declara-prioridad-nacional-la-elaboraci%C3%B3n-e-implementaci%C3%B3n-de-la.

94. https://www.cgii.gob.bo/es/normativa.

95. https://www.cgii.gob.bo/es/acerca-del-cgii.

96. https://www.csirtamericas.org/.

97. Pesquisa on-line da OEA

98. Art. 363 do Código Penal.

99. Decreto Supremo n° 28168, Acesso à Informação.
https://www.comunicacion.gob.bo/?q=20130725/decreto-supremo-n%C2%BA-28168-acceso-la-informacion.

100. https://coplutic.gob.bo/IMG/pdf/plan_gobierno_electronico_.pdf.

101. Lei n° 1.080/2018, Lei da Cidadania Digital.

102. http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

103. Proposta de emenda à Constituição n° 17, de 2019. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/135594

104. Código Penal brasileiro (1940), Decreto-Lei n° 2.848, de 7 de dezembro de 1940; disponível em:
http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

105. Código de Defesa do Consumidor (Lei n° 8.078/1990; Disponível em:
https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf.

106. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

107. https://www.csirt.gob.cl/.

108. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

109. Projeto CH-L1142 – https://www.iadb.org/es/project/CH-L1142.

110. Projeto CH-L1142 – https://www.iadb.org/es/project/CH-L1142.

111. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

112. http://www.ciberseguridad.gob.cl/consulta-ciudadana/.

113. https://alianzaciberseguridad.cl/.

114. https://www.latercera.com/pulso/noticia/gobierno-evalua-exigir-inversion-ciberseguridad-algunas-actividades-del-sector-privado/201537/.

115. https://www.leychile.cl/Navegar?idNorma=30590.

116. https://www.leychile.cl/Navegar?idNorma=141599.

117. http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/senado/2018-05-15/181511.html.

118. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

119. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25.

120. https://www.unescap.org/sites/default/files/E-Government%20Survey%202018_FINAL.pdf.

121. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

122. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

123. https://digital.gob.cl/instructivo/acerca-de.

124. https://www.leychile.cl/Navegar?idNorma=1138479.

125. http://www.internetsegura.cl/quienes-somos/.

126. CONPES 3701, 2011 Cybersecurity and Cyberdefense Guidelines, July 2011. Disponível em https://www.mintic.gov.co/portal/604/w3-article-3510.html.

127. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

128. O Comitê de Cibersegurança estuda os seguintes tópicos: Políticas e regulação de segurança cibernética, proteção e defesa da infraestrutura cibernética crítica nacional, gestão dos riscos de cibersegurança, crises e monitoramento de ameaças cibernéticas, proteção de dados pessoais, questões internacionais de cibersegurança e comunicações estratégicas para a cibersegurança.

129. http://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=83433; https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

130. Essa função é desempenhada em colaboração com o Comando Conjunto Cibernético (CCOC) do Comando Geral das Forças Militares e o Centro Cibernético de Polícia (CCP) da Polícia Nacional, o CSIRT do Governo, o CSIRT Financeiro, a Procuradoria-Geral da União, conexões setoriais de cibersegurança e outras iniciativas de CSIRTs setoriais e privados, bem como entidades nacionais ou elos com equipes de resposta de outros países e organizações internacionais que, de acordo com sua declaração de missão, contribuem para dar resposta a incidentes de computador. Da mesma forma, e caso seja detectado um incidente que possa ocasionar uma crise nacional, o ColCERT reporta-se imediatamente ao Coordenador Nacional de Segurança Cibernética para ativar o Comitê de Segurança Cibernética a fim de enfrentar a crise.

131. Da mesma forma, foi publicado o Guia de Administração de Riscos, Corrupção e Cibersegurança, dirigido a todas as entidades do Poder Executivo que fornecem uma metodologia de gestão eficente dos riscos que afetam o cumprimento dos objetivos estratégicos e processuais, inclusive aqueles relacionados à segurança cibernética.
Da mesma forma, a Comissão de Regulação das Comunicações (CRC) emitiu a Resolução n° 5.569, de 2018, "modificando o artigo 5.1.2.3 do Capítulo I do Título V da Resolução CRC 5.050 de 2016 em questões de gestão da segurança em redes de telecomunicações e dando outras providências".

132. Projeto CO-L1233: https://www.iadb.org/en/project/CO-L1233.

133. https://www.mintic.gov.co/portal/604/w3-article-15119.html.

134. https://www.mintic.gov.co/portal/604/w3-article-11319.html.

135. http://www.oas.org/es/sap/dgpe/escuelagob/novedades_OEA-capacita-estudiantes-seguridad-digital.asp.

136. https://www.enticconfio.gov.co/quienes-somos.

137. http://www.oas.org/juridico/spanish/cyb_col_ley1273.pdf.

138. https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Proteccion-de-datos-personales.aspx.

139. http://www.sic.gov.co/sites/default/files/files/Superintendente_Proteccion_Datos_Personales.pdf.

140. https://www.interpol.int/en/Who-we-are/Member-countries/Americas/COLOMBIA; https://www.europol.europa.eu/agreements/colombia

141. Por exemplo, a Comissão das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, Grupos de Peritos e Membros Abertos; o Grupo de Trabalho sobre Medidas de Fortalecimento da Confiança da Organização dos Estados Americanos (OEA), em que a Colômbia atuou como Presidente do Grupo em 2018; a Aliança do Pacífico; a Convenção de Budapeste do Conselho da Europa; o Centro Europeu de Crime Cibernético (EC3); a Organização do Tratado do Atlântico Norte (OTAN); a EUROPOL e a INTERPOL.

142. http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf.

143. http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf; http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

144. https://www.micit.go.cr/files/estrategia-nacional-ciberseguridad.

145. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC.

146. Pesquisa on-line da OEA

147. https://www.tec.ac.cr/fundatec/especialista-gestion-ciberseguridad-empresarial.

148. https://presidencia.go.cr/comunicados/2018/02/expertos-espanoles-estan-en-costa-rica-para-capacitar-a-funcionarios-publicos-sobre-ciberseguridad/;
https://micit.go.cr/index.php?option=com_content&view=article&id=10337:estudiantes-costarricenses-reciben-capacitacion-en-seguridad-digital-de-la-oea&catid=40&Itemid=630.

149. https://www.imprentanacional.go.cr/pub/2012/11/06/ALCA172_06_11_2012.pdf.

150. https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/.

151. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

152. http://www.firma-digital.cr/plan_maestro_gob_digital.pdf.

153. https://dominicastatecollege.com/?page_id=2818.

154. https://www.dominicavibes.dm/education-175314/.

155. http://www.dominica.gov.dm/laws/2010/Electronic%20Evidence%20no.%2013.pdf.

156. http://www.dominica.gov.dm/laws/2013/Electronic%20Filing,%202013%20ACT%2020%20of%202013.pdf.

157. http://www.dominica.gov.dm/laws/2013/Electronic%20Funds%20Transfer%20Act,%202013%20ACT%2017%20of%202013.pdf.

158. http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf.

159. https://indotel.gob.do/media/10605/decreto-230-18.pdf.

160. http://optic.gob.do/wp-content/uploads/2019/02/Decreto-258-16.pdf.

161. http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

162. https://indotel.gob.do/media/6200/ley_172_13.pdf.

163. Artigo 44, parágrafo 2 e Artigo 70 da Constituição.

164. https://indotel.gob.do/media/6200/ley_172_13.pdf.
http://dominicana.gob.do/index.php/politicas/2014-12-16-20-56-34/politicas-para-el-buen-gobierno/politica-de-privacidad.

165. https://www.ecucert.gob.ec/nosotros.html.

166. http://www.oas.org/juridico/pdfs/mesicic4_ecu_estat.pdf.

167. https://www2.deloitte.com/ec/es/pages/risk/articles/cyber-risk-2018.html.

168. https://indotel.gob.do/media/6200/ley_172_13.pdf.

169. http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf.

170. https://vlex.ec/vid/codigo-organico-integral-penal-631464447?_ga=2.104058179.2107735450.1529940398-1975001013.1529940398#section_35.

171. Artigo 66, parágrafo 19 da Constituição.

172. A Lei Orgânica das Comunicações, a Lei Orgânica das Telecomunicações e o Regulamento da Lei Orgânica das Telecomunicações contêm artigos relacionados à proteção dos dados pessoais.

173. https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/250%20protec-intimidad-grivadeneira-12-07-2016/PP-protec-intimidad-grivadeneira-12-07-2016.pdf.

174. Fonte: Estado-Membro.

175. https://ec.okfn.org/files/2014/12/PlanGobiernoElectronicoV1.pdf.

176. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf.

177. Artigo 10 (5 e 11), Lei Orgânica do Sistema Nacional de Compras Públicas. Disponível em https://www.epn.edu.ec/wp-content/uploads/2018/08/Ley-Org%C3%A1nica-de-Contrataci%C3%B3n-P%C3%BAblica.pdf.

178. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

179. https://www.dinero.com.sv/es/economia/el-salvador-busca-la-transformacion-digital-desde-el-gobierno.html; http://secretariatecnica.egob.sv/transformacion-del-estado/dgte-gobelectronico/.

180. Informações prestadas pelo País.

181. https://universidades.sv/carreras/administracion-de-las-tecnologias-de-la-informacion.

182. https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf.

183. https://www.asamblea.gob.sv/decretos/details/166.

184. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

185. http://www.secretariatecnica.gob.sv/gobierno-lanza-politica-de-datos-abiertos-y-presenta-portal-datos-gob-sv/; http://www.secretariatecnica.gob.sv/lanzan-el-sistema-integrado-de-gestion-administrativa-siga/.

186. http://tenoli.gobiernoelectronico.gob.sv/.

187. https://www.gobiernoelectronico.gob.sv/?p=483.

188. http://www.nowgrenada.com/2014/02/cyber-security-strategy-needed-fight-cyber-crimes/.

189. Pesquisa on-line da OEA

190. https://www.gov.gd/hop/acts.

191. https://www.oecs.org/en/procurement/e-gov/data-protection-act.

192. https://www.gov.gd/short-medium-term-ict-plan-government-ict-functions-be-ready-approval-within-months.

193. http://www.gov.gd/egov/docs/ict_egov/draft_2010_2014_CARICOM_egovernment_strategy.pdf.

194. Pesquisa on-line da OEA

195. http://mingob.gob.gt/wp-content/uploads/2018/06/version-digital.pdf.

196. https://www.cert.gt/

197. https://www2.deloitte.com/gt/es/pages/risk/articles/cyber-risk.html; https://www.widefense.com/contacto/; https://www.cyberseg.com/.

198. https://www.linkedin.com/company/soluciones-seguras?originalSubdomain=gt ; https://www.facebook.com/events/ministerio-de-gobernaci%C3%B3n-guatemala/guatemala-mes-de-la-ciberseguridad/389628648376004/ ; https://www.solucionesseguras.com/noticias/soluciones-seguras-cybersecurity-magazine#edicion8 .

199. https://www.isoc.org.gt/ciberseguridad/grupo-de-trabajo-de-ciberseguridad/.

200. http://mingob.gob.gt/viceministerio-de-tecnologia-realiza-capacitacion-sobre-ciberamenazas/.

201. https://mingob.gob.gt/iniciativa-de-ciberdelincuencia-espera-aprobacion-del-congreso-de-la-republica/; http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf.

202. https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/Registro5254.pdf.

203. Artigo 1° da Iniciativa n° 5.254, de 2017.

204. http://www.oas.org/es/sla/ddi/docs/G7%20Iniciativa%204090-2009.pdf.

205. http://www.transparencia.gob.gt/ejes-de-accion/gobierno-electronico/.

206. https://cirt.gy/about.

207. https://cirt.gy/.

208. Pesquisa on-line da OEA

209. https://www.kaieteurnewsonline.com/2019/04/06/guyana-gets-uk-help-to-fight-cyber-crime/.

210. http://dpi.gov.gy/gpf-launches-zara-cyber-security-centre-lauded-as-exemplary-publicprivate-partnership/; https://guyanachronicle.com/2017/03/22/first-cyber-security-centre-to-be-launched-in-georgetown-thousands-benefit-from-ict-training.

211. https://www.kaieteurnewsonline.com/2018/08/20/president-assents-to-cybercrime-bill/.

212. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

213. http://parliament.gov.gy/documents/bills/6033-cybercrime_bill_2016_-_no._17_of_2016.doc.

214. https://dpi.gov.gy/tag/cyber-crime-bill/.

215. https://doe.gov.gy/gsds.

216. http://conatel.gouv.ht/node/188.

217. http://www.haitilibre.com/article-24457-haiti-technologie-vers-un-centre-d-alerte-en-matiere-de-cybersecurite.html.

218. https://lenouvelliste.com/article/189514/haiti-laudit-informatique-une-necessite-pour-nos-entreprises-aujourdhui.

219. https://www.lenouvelliste.com/article/171291/cyberattaque-sommes-nous-proteges-ou-en-sommes-nous-en-haiti.

220. https://www.lamjol.info/index.php/INNOVARE/article/view/5571/5274.

221. Relatório de País do Haití, atividades cibernéticas por ano.

222. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

223. https://www.haititechnews.com/haitila-cyberlegislation-une-necessite-pour-renforcer-le-commerce-electronique/; https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_F.pdf.

224. http://primature.gouv.ht/?page_id=36.

225. Pesquisa on-line da OEA

226. http://congresonacional.hn/index.php/2018/02/08/dictamen/.

227. http://www.sre.gob.hn/portada/2016/Diciembre/08-12-16/Honduras%20da%20%E2%80%9Cun%20gran%20salto%E2%80%9D%20en%20esta%20alianza%20con%20Israel.pdf

228. Projeto HO-L1202: https://www.iadb.org/en/project/HO-L1202

229. Com base nas respostas recebidas à Pesquisa On-line da OEA

230. http://www.latribuna.hn/2018/02/09/mexico-apoyara-honduras-materia-ciberseguridad/.

231. https://ceabad.com/honduras-taller-local-ciberseguridad-como-estrategia-nacional/.

232. http://www.elheraldo.hn/pais/1168270-466/congreso-nacional-honduras-continua-aprobacion-ley-de-proteccion-datos.

233. https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf.

234. http://agendadigital.hn/wp-content/uploads/2013/10/AgendadigitalCOR.pdf.

235. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

236. https://jis.gov.jm/cyber-incident-response-team-fully-equipped-and-operational/.

237. https://mof.gov.jm/documents/documents-publications/document-centre/file/1643-estimates-of-expenditure-2018-2019.html.

238. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

239. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

240. https://www.pwc.com/jm/en/press-room/boards-and-cyber-attacks.html.

241. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf.

242. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf; https://jis.gov.jm/government-employees-trained-cybersecurity/.

243. https://moj.gov.jm/sites/default/files/laws/Cybercrimes%20Act.pdf.

244. https://moj.gov.jm/laws/cybercrimes-act.

245. http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf.

246. https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf.

247. https://planipolis.iiep.unesco.org/en/2009/vision-2030-jamaica-information-and-communications-technology-ict-sector-plan-2009-2030-final.

248. https://www.mset.gov.jm/documents/the-goj-ict-governance-handbook/.

249. https://japarliament.gov.jm/attachments/article/339/The%20National%20Identification%20and%20Registration%20Act,%202017--.pdf.

250. https://www.nidsfacts.com/.

251. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

252. https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es; http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059

253. https://www.pwc.com/mx/es/archivo/2019/20190402-digital-trust-pt1.pdf?utm_source=Website&utm_medium=SiteDTrust&utm_content=DescargaPDF1

254. https://www.gob.mx/cms/uploads/attachment/file/274782/Resumen-Ciberseguridad.pdf.

255. https://www.gob.mx/policiafederal/es/articulos/manual-basico-de-ciberseguridad-para-la-micro-pequena-y-mediana-empresa?idiom=es.

256. http://www.informatica-juridica.com/codigo/articulo-211-codigo-penal-federal-mexicano/.

257. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

258. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

259. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

260. https://www.gob.mx/.

261. http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d.

262. https://www.poderjudicial.gob.ni/pjupload/noticia_reciente/CP_641.pdf.

263. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

264. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

265. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

266. https://www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf.

267. https://cert.pa/sobre-nosotros/.

268. Projeto PN-L1114: https://www.iadb.org/en/project/PN-L1114

269. https://yabt.net/news.php?n=cyberseguirdad-panama-2017.

270. https://cert.pa/cursos/.

271. http://www.organojudicial.gob.pa/wp-content/uploads/2016/11/Texto-%C3%9Anico-del-C%C3%B3digo-Penal-2010.pdf.

272. http://www.asamblea.gob.pa/proyley/2017_P_558.pdf.

273. https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2013/2013_606_1726.pdf.

274. https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf.

275. http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf.

276. https://www.mitic.gov.py/materiales/publicaciones/plan-nacional-de-ciberseguridad-paraguay; https://www.presidencia.gov.py/archivos/documentos/DECRETO7052_5cq17n8g.pdf.

277. https://www.cert.gov.py/index.php; https://www.presidencia.gov.py/archivos/documentos/DECRETO2274_30nobos1.PDF; https://www.cert.gov.py/application/files/4115/6642/8626/MITIC_Iniciativas_Ciberseguridad_PY.pdf.

278. Projeto PR-L1153; https://www.iadb.org/en/project/PR-L1153; https://www.mitic.gov.py/agenda-digital/documentos.

279. Plano Nacional de Segurança Cibernética, p. 26

280. Plano Nacional de Segurança Cibernética, p. 26

281. http://www.paraguay.com/nacionales/lanzan-campana-de-ciberseguridad-conectate-seguro-py-105453; https://www.conectateseguro.gov.py/.

282. http://fiadi.org/wp-content/uploads/2017/10/LEY-4439-DELITOS-INFORMATICOS.pdf.

283. http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado.

284. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

285. http://gestordocumental.senatics.gov.py/share/s/kSvUFg7rSdmez7fA8OTaOA.

286. https://www.senatics.gov.py/application/files/2414/5200/6345/ley_4989_senatics.pdf.

287. https://www.cert.gov.py/index.php/controles-criticos-seguridad.

288. https://www.cert.gov.py/index.php/criterios-minimos-de-seguridad-de-software.

289. https://www.cert.gov.py/index.php/directivas-de-ciberseguridad-para-canales-de-comunicacion-oficiales-del-estado.

290. http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf.

291. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

292. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

293. https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1/.

294. https://www.pecert.gob.pe/index.php/acerca-de-nosotros/que-es-el-pe-cert.

295. https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/301898.

296. Projeto PE-L1222; https://www.iadb.org/en/project/PE-L1222

297. https://elperuano.pe/noticia-expertos-analizan-desafios-y-gestion-seguridad-digital-66976.aspx.

298. Decreto Legislativo n° 1.412. Disponível em https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/.

299. https://busquedas.elperuano.pe/normaslegales/declaran-de-interes-nacional-el-desarrollo-del-gobierno-digi-decreto-supremo-n-118-2018-pcm-1718338-2/.

300. Decreto Supremo n° 118-2018. Disponível em http://www.gobiernodigital.gob.pe/banco/segdi_BUSQ_NORMAS.asp.

301. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412.

302. http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf.

303. http://www.oas.org/juridico/spanish/cyb_per_ley_27309.pdf.

304. http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

305. https://www.sknvibes.com/news/newsdetails.cfm/100223.

306. https://buzz-caribbean.com/article/st-kitts-government-wants-digital-transformation-of-local-economy/.

307. http://www.mof.gov.kn/wp-content/uploads/2017/12/Estimates-2018-Volume-II-Final-Website.pdf.

308. Informação recebida do país.

309. https://www.unodc.org/res/cld/document/kna/Electronic_Crimes_Act._No._27_of_2009_pmd_-_Electronic_Crimes_Act_No._27_of_2009.pdf.

310. https://www.thestkittsnevisobserver.com/local-news/st-kitts-and-nevis-legislators-pass-data-protection-bill-2018/.

311. https://unstats.un.org/unsd/dnss/docViewer.aspx?docID=2297.

312. http://timescaribbeanonline.com/st-kitts-nevis-government-launches-e-government-portal-that-promises-cost-effectiveness-and-time- efficiency/.

313. Informação recebida do país.

314. http://www.govt.lc.

315. Lei de Transações Eletrônicas nº 16, de 2011.

316. http://www.govt.lc/news/senate-votes-on-data-protection-amendment.

317. https://stluciatimes.com/saint-lucia-to-strengthen-laws-to-protect-cyber-shoppers/.

318. Evento apoiado pelo Grupo Caribenho de Operadores de Redes (CaribNOG) e pelo Capítulo da Internet Society do país. Ver http://www.isoc.vc/news-release/st-vincent-to-host-cyber-security-forum/.

319. https://www.caribjournal.com/2017/12/19/st-vincent-moves-strengthen-cybersecurity/.

320. http://finance.gov.vc/finance/images/PDF/the_role_of_education_in_cyber_security.pdf.

321. http://www.isoc.vc/about/.

322. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Electronic_Transactions_Act_2015.pdf.

323. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Cybercrime_Act_2016.pdf.

324. http://www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf.

325. http://www.gov.vc/images/pdf_documents/svg_egov_development_strategy_report.pdf.

326. http://www.gov.vc/images/PoliciesActsAndBills/SVGICTStrategyAndActionPlanFinal.pdf.

327. http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14.

328. https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2017/20287.aspx; http://www.tas.sr/.

329. https://www.oas.org/es/sap/dgpe/gemgpe/suriname/suriname.pdf.

330. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

331. https://ttcsirt.gov.tt/index.php/background/.

332. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

333. Pesquisa on-line da OEA

334. https://www.samtt.com/index.php/programmes/anglia-ruskin-university/msc-network-sec.

335. http://www.ttparliament.org/legislations/b2017h15g.pdf; http://www.ttparliament.org/legislations/a2011-13.pdf.

336. http://www.ttconnect.gov.tt.

337. https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf.

338. https://www.cert.uy/inicio/institucional/que_es_el_cert/; https://www.agesic.gub.uy/innovaportal/v/33/1/agesic/que-es-agesic.html?idPadre=19.

339. Projeto UR-L1152: https://www.iadb.org/en/project/UR-L1152.

340. https://www.impo.com.uy/bases/decretos/36-2015.

341. https://www.agesic.gub.uy/innovaportal/file/94/1/prespuesto_2018.pdf.

342. https://tramites.gub.uy/ampliados?id=3847.

343. https://www.cert.uy/seguroteconectas/recomendaciones.

344. https://parlamento.gub.uy/camarasycomisiones/representantes/documentos/repartido/48/433/0/pdf.

345. https://www.impo.com.uy/bases/leyes/18331-2008.

346. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-de- gobierno-digital-uruguay-2020.

347. https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf.

348. https://www.gub.uy/.

349. http://www.suscerte.gob.ve/?p=2074.

350. https://www.mppeuct.gob.ve/actualidad/noticias/plan-nacional-de-ciberseguridad-y-ciberdefensa.

351. http://www.suscerte.gob.ve/?page_id=1736.

352. http://www.suscerte.gob.ve/?page_id=1736.

353. http://www.presidencia.gob.ve/Site/Web/Principal/paginas/classMostrarEvento3.php?id_evento=4397.

354. http://www.redipd.es/legislacion/common/legislacion/venezuela/13-leydelitosinformaticos.pdf.

355. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

356. https://web.oas.org/mla/en/Countries_Intro/Ven_intro_fundtxt_esp_1.pdf.

* https://data.worldbank.org/indicator/SP.POP.TOTL.

** https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

www.cybersecurityobservatory.org

CIBERSEGURANÇA

RISCOS, AVANÇOS E O CAMINHO A SEGUIR NA AMÉRICA LATINA E CARIBE

Relatório de Cibersegurança 2020

Relatório de Cibersegurança

2020

BID
Melhorando vidas

OEA
Mais direitos
para mais pessoas

www.cybersecurityobservatory.org