Evolução das estratégias de segurança cibernética

Análise do cenário regional e internacional

Autores
Santiago Paz
Martina Bergues
José Callero

BID

Evolução das estratégias de segurança cibernética

Análise do cenário regional e internacional

Autores
Santiago Paz
Martina Bergues
José Callero

Banco Interamericano de Desarrollo

Os projetos de cooperação técnica que cofinanciaram o apoio do BID à EVOLUÇÃO DAS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA: ANÁLISE DO CENÁRIO REGIONAL E INTERNACIONAL foram o *Japan Special Fund*, que é financiado pelo governo do Japão, e o *Korea Fund for Economic Development*, que é financiado pelo governo da Coreia.

Códigos JEL: H11, O38, O33
Palavras-chave: segurança cibernética, estratégias, governança, planos de ação, segurança da informação, segurança cibernética, política pública, economia digital, defesa cibernética, privacidade, segurança por design, resiliência digital

Banco Interamericano de Desenvolvimento
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

O Setor de Instituições para o Desenvolvimento foi o responsável pela produção da publicação.

Coordenação da produção editorial: A&S Information Partners, LLC

Revisão editorial: Giovana Boselli

Diagramação: The Word Express, Inc.

SUMÁRIO

1 Sumário executivo

Por que um estudo sobre as estratégias nacionais de cibersegurança?

- De acordo com o Global Risks Report 2023,[1] do Fórum Econômico Mundial, a segurança cibernética ocupa o oitavo lugar na percepção dos entrevistados. Em 2022, a região da América Latina sofreu pelo menos 360 bilhões de tentativas de ataques, com o Brasil em segundo lugar (depois do México), com 103 bilhões.[2]
- Esses ataques estão se tornando cada vez mais sofisticados, com o tipo *ransomware* (extorsão) representando 17% dos detectados globalmente. Um exemplo desse tipo é o recente ataque à empresa IFX Network,[3] que afetou mais de 50 empresas públicas e privadas na Colômbia e no Chile, deixando-as fora de serviço.
- A prevalência, o aumento e a complexidade dos ataques requerem dos países uma abordagem estratégica que responda às ameaças de forma coordenada. As estratégias nacionais de cibersegurança são uma ferramenta para que os países possam delinear seus planos para proteger e assegurar o ciberespaço.
- Com duas décadas de estratégias nacionais publicadas[4] e países com três versões de suas estratégias publicadas, ainda há pouco conhecimento sistematizado sobre qual é a evolução do seu conteúdo e quais são as principais lições aprendidas.
- Este estudo busca criar uma metodologia para comparar documentos heterogêneos e identificar tendências e padrões que possam auxiliar os países que se encontram no processo de elaboração de novas versões de suas estratégias nacionais de cibersegurança.

Que metodologia foi usada?

- Foram analisadas 43 estratégias nacionais de 19 países, incluindo estratégias de primeira, segunda e terceira geração.
- Para cada estratégia foram analisadas as principiais áreas focais, tomando como referência a adaptação das áreas focais do *Guide to Developing a National Cybersecurity Strategy*, documento liderado pela União Internacional de Telecomunicações (ITU).
- Em primeiro lugar, a análise buscou compreender como cada tema está presente nas estratégias atualmente em vigor, para

[1] Global Risk Report 2023.
[2] https://socradar.io/wp-content/uploads/2023/06/Brazil-Threat-Landscape-Report.pdf.
[3] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-que-informacion-se-pudieron-haber-robado-en-el-ciberataque-805730.
[4] A primeira estratégia analisada neste estudo data de 2003 e corresponde à primeira estratégia dos Estados Unidos.

documentar o estado da arte das estratégias de cibersegurança mais recentes.

- Em seguida, para identificar padrões e diferenças regionais, os mesmos aspectos foram analisados comparando-se as estratégias da América Latina com as de outros países, o que permitiu destacar nuances regionais e pontos de convergência global.
- Por fim, uma abordagem inovadora foi adotada para entender a evolução dos temas ao longo do tempo. As estratégias foram categorizadas tanto em relação ao ano de publicação como em relação à geração (primeira, segunda ou terceira), o que permitiu identificar diferenças nas tendências ligadas à evolução do tempo e naquelas ligadas à maturidade dos países.
- Além disso, traz estudos de caso para oferecer compreensão mais abrangente e detalhada de diversos aspectos das estratégias analisadas. Os casos fornecem *insights* específicos, enriquecendo a análise comparada.

Quais são os principais achados?

- Apesar das heterogeneidades em formatos, alcance, vigência e temas incluídos, é possível identificar diferentes padrões e tendências a partir de uma análise sistemática das estratégias.
- As estratégias de terceira geração são mais operativas e menos teóricas quando comparadas com as das gerações anteriores.
- Entre os achados regionais, em relação ao formato e governança das estratégias, destaca-se que a América Latina costuma associar com mais frequência suas estratégias a normativas, define com menos frequência planos operativos e estabelece mecanismos de coordenação com o setor privado em menor frequência.
- As estratégias mais recentes, em especial no Norte Global, são mais amplas do que a segurança nacional e incluem temas de prosperidade econômica e fomento à indústria, delineando uma tendência a entender o campo da cibersegurança como fértil para o desenvolvimento econômico e social de um país.
- Entre as estratégias atualmente em vigor, virtualmente todas possuem objetivos ou iniciativas ligadas aos temas de prontidão e resiliência, e a grande maioria tem objetivos de fortalecimento das capacidades em cibersegurança.
- Em relação aos temas, objetivos e linhas de ação incluídos, destaca-se que as estratégias analisadas do Norte Global apresentam, com mais frequência, preocupação com ataques à democracia e com ataques extremistas. Também apresentam, em proporção maior, componentes relacionados à prosperidade econômica e ao fomento à indústria, estabelecem medidas para proteger ativos de governos digitais com mais frequência, entre outras tendências que serão exploradas ao longo do estudo.
- Em relação à analise evolutiva, para além da já mencionada tendência ao aumento dos princípios, objetivos e iniciativas ligados à prosperidade econômica e ao fomento à indústria de cibersegurança, destacam-se: (i) aumento dos princípios, objetivos ou iniciativas ligados à transparência e confiança no ciberespaço; (ii) aumento de iniciativas voltadas para promover a diversidade na força de trabalho de cibersegurança; (iii) diminuição de objetivos ligados à infraestrutura crítica nas estratégias de terceira geração; (iv) aumento da presença de mecanismos para

promover o compartilhamento de informações e ampliar a cooperação; (v) aumento da presença do conceito de *security by design*,[5] entre outras tendências que serão exploradas ao longo do estudo.

[5] De acordo com a definição da Agência de Cibersegurança dos Estados Unidos (CISA), *security by design* significa que os produtos de tecnologia são desenvolvidos de forma a proteger contra agentes cibernéticos mal-intencionados que obtêm acesso a dispositivos, dados e software de infraestrutura conectada.

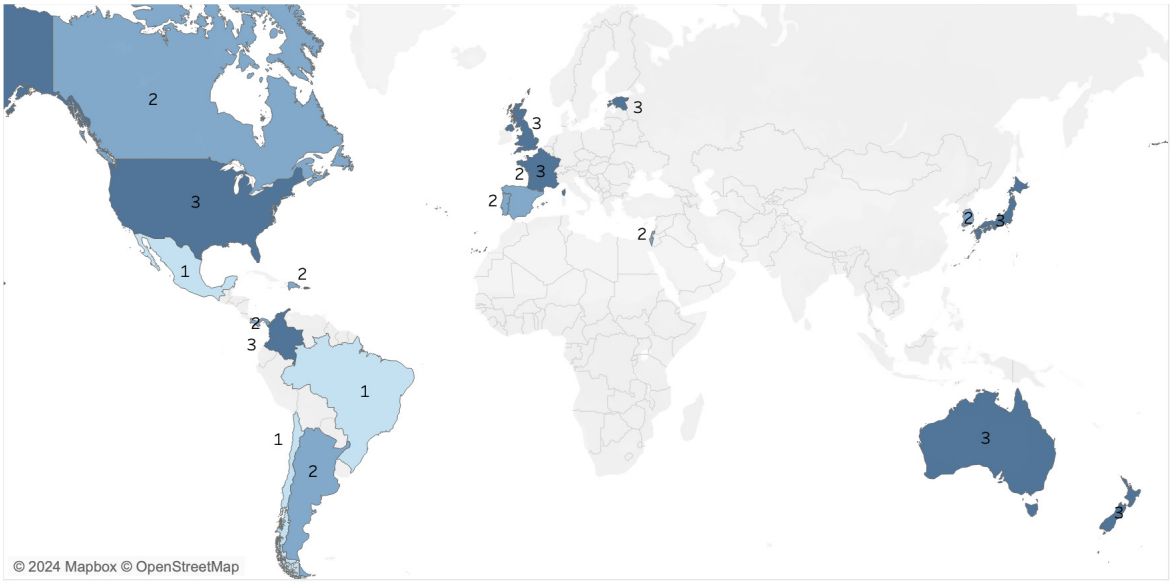
2 Metodologia

2.1. Seleção dos países

O estudo incluiu a análise de 12 países com nível de maturidade avançado fora da região e sete países da América Latina e Caribe (de forma a contemplar a experiência regional na temática), totalizando uma análise de 43 estratégias, das quais 19 estão vigentes. A identificação dos países incluídos no estudo levou em conta o nível de maturidade no ITU Global Cybersecurity Index (GCI)[6] e/ou sua participação no Digital Nations,[7] garantindo que sejam incluídos os países mais avançados no cenário global. Em relação à escolha dos países da América Latina e Caribe, levou-se em conta o extenso trabalho realizado na região, pelo BID, para incluir países com estratégias que poderiam aportar valor ao processo de construção da estratégia de cibersegurança no Brasil. Dessa forma, foram analisados os seguintes países e a evolução de suas estratégias: Argentina, Austrália, Brasil, Canadá, Chile, Colômbia, Coreia, Espanha, Estônia, Estados Unidos da América, França, Israel, Japão, México, Nova Zelândia, Panamá, Portugal, República Dominicana e Reino Unido.

[6] Global Cybersecurity Index.
[7] DN – Digital Nations.

MAPA 1 – NÚMERO DE ESTRATÉGIAS ANALISADAS POR PAÍS



As estratégias analisadas se distribuem no tempo e por geração. O conceito de geração diz respeito à estratégia analisada ser a primeira, segunda ou terceira publicada de cada país. Na amostra analisada, há países com uma, duas ou três estratégias.[8] Sua distribuição por período pode ser verificada na Diagrama 1 a seguir.

DIAGRAMA 1 – NÚMERO DE ESTRATÉGIAS POR PERÍODO E GERAÇÃO

	1ª	2ª	3ª
Antes de 2010	3	0	0
2011-2015	9	3	0
2016-2020	7	9	3
Depois de 2020	0	4	5

2.2. Análise das estratégias

A análise das estratégias foi conduzida a partir de análise documental. Para isso, foram coletados e examinados os documentos das estratégias de segurança cibernética dos países selecionados.

Com o objetivo de realizar uma revisão sistemática que permitisse traçar comparações e identificar tendências, foram criadas categorias de análise pré-definidas, para que todas as estratégias fossem analisadas com o mesmo olhar. Essas categorias foram construídas a partir de uma adaptação do *Guide to Developing a National Cybersecurity Strategy*,[9] documento de referência internacional, elaborado por mais de 12 organizações parceiras e liderado pelo ITU.

[8] A distribuição das estratégias por período e geração ocorre da seguinte forma: 1ª geração, publicadas antes de 2010: EUA (2003), Estônia (2008) e Canadá (2010); 1ª geração, publicadas entre 2011 e 2015: Reino Unido (2011), Nova Zelândia (2011), Coreia (2011), Colômbia (2011), França (2011), Espanha (2013), Panamá (2013); Portugal (2015), Japão (2015); 1ª geração, publicadas entre 2016-2022: Austrália (2016), Chile (2017), Israel (2017), México (2017); República Dominicana (2018), Argentina (2019), Brasil (2020); 2ª geração, publicadas entre 2011-2015: Estônia (2014), Nova Zelândia (2015), França (2015); 2ª geração, publicadas entre 2016-2020: Reino Unido (2016), Colômbia (2016), Canadá (2018), EUA (2018), Japão (2018), Coreia (2019), Espanha (2019), Portugal (2019), Austrália (2020); 2ª geração, publicadas depois de 2020: Israel (2021), Panamá (2021); República Dominicana (2022), Argentina (2023); 3ª geração, publicadas entre 2016-2020: Estônia (2019), Nova Zelândia (2019), Colômbia (2020); 3ª geração, publicadas depois de 2020: Japão (2021), França (2021), Reino Unido (2022), Austrália (2023), EUA (2023). No caso da Colômbia, foram consideradas as CONPES como *proxies* de estratégias.

[9] Guide to developing a National Cybersecurity Strategy.

Para referência, as macrocategorias analisadas incluem componentes transversais: (i) estrutura das estratégias; (ii) ameaças e desafios; (iii) princípios; (iv) objetivos estratégicos (agrupados em 12 categorias); (v) métricas e indicadores. Além disso, as macrocategorias incluem as seguintes áreas focais: (i) governança; (ii) gestão de riscos; (iii) resiliência e prontidão; (iv) infraestrutura crítica e serviços essenciais; (v) capacidades e conscientização; (vi) marco normativo e legislação; (vii) cooperação internacional; (viii) privacidade e dados; (ix) defesa e capacidade militar. As últimas duas foram acrescentadas em complementação às áreas focais sugeridas no documento do ITU. Veja os detalhes na Diagrama 2.

DIAGRAMA 2 – COMPONENTES TRANSVERSAIS

Para cada documento, foi feita uma análise para classificar cada tema da estratégia e poder gerar dados comparáveis. Antes de consolidar os dados, foi feita uma calibragem a partir de três estratégias, entre dois pesquisadores, para garantir que o entendimento das categorias estivesse alinhado e que a metodologia fosse robusta. Vale destacar que o objetivo da categorização é permitir a comparabilidade e identificar as tendências globais e não compreender em profundidade cada uma das estratégias. Pequenas diferenças na categorização podem ser possíveis devido à metodologia, mas não invalidam os achados globais do estudo. Estudos de casos complementares e futuras entrevistas com especialistas podem refinar a categorização e adicionar valor ao estudo.

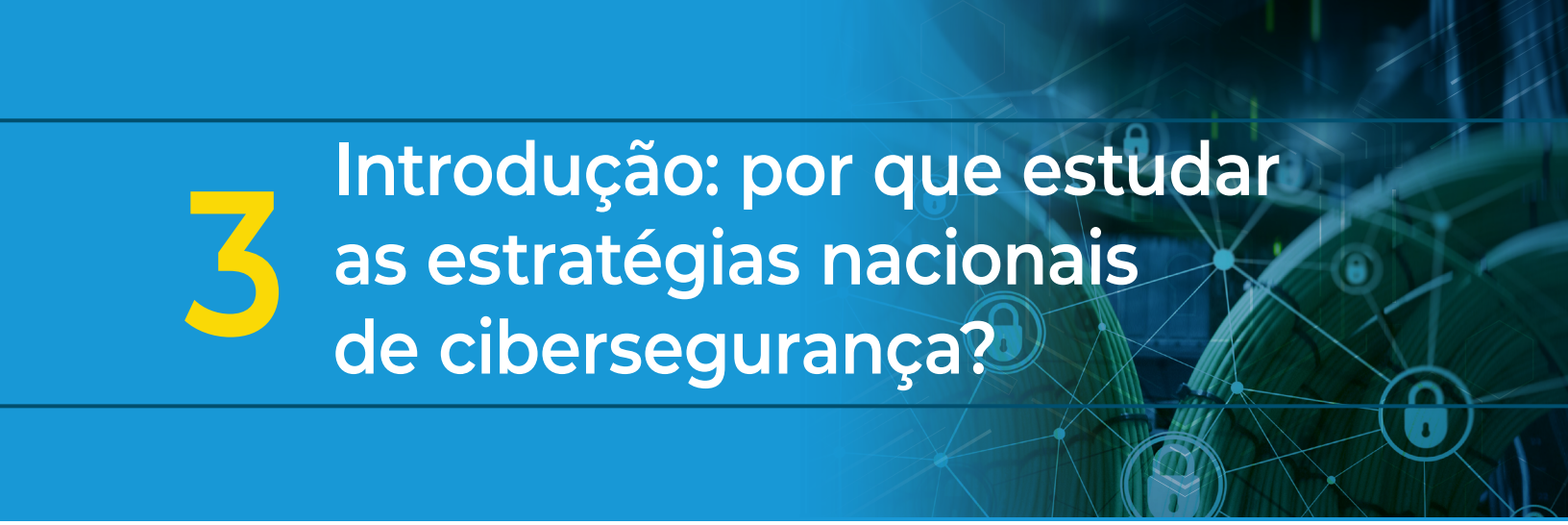
QUADRO 1 – LIMITAÇÕES DO ESTUDO: COMO LER OS GRÁFICOS E DADOS

O estudo segue um padrão de análise para todos os tópicos selecionados. Para cada tema, se apresenta primeiramente uma análise, que inclui somente as estratégias vigentes (sendo que há estratégias da primeira, segunda e terceira geração, a depender do país). Ainda nesse recorte, faz-se uma comparação direta entre as estratégias da América Latina e as dos demais países.

Na sequência, para cada tema, há um gráfico que analisa a evolução das estratégias, sob duas óticas: (i) por geração das estratégias (se é a primeira, a segunda ou a terceira estratégia de determinado país); (ii) por período. A comparação das duas evoluções ajuda a entender se existe algum padrão temporal ou se a variação de determinado tema pode estar relacionada à maturidade dos países, entendendo que uma estratégia de terceira geração inclui lições aprendidas com as versões anteriores.

É importante ter em mente algumas limitações:

i. existe um desafio inerente à classificação comparativa de documentos que possuem estruturas e níveis de profundidade diferentes. Dessa forma, classificar em categorias binárias um documento de cinco páginas e um de 130 é um desafio, uma vez que não é possível capturar a profundidade de cada tema, mas apenas a menção a ele;
ii. o número de estratégias analisadas é pequeno (n=19 para o primeiro conjunto de gráficos e n=43 para o segundo) e não é uniforme entre as gerações, ano e regiões. Isso implica que, para algumas categorias, uma estratégia acaba tendo um peso maior do que para outras. Esse é um desafio inerente ao fenômeno estudado, uma vez que não há o mesmo número de países com estratégias de cada geração publicadas no mesmo ano. A inclusão de novas estratégias no estudo ou de pequenas mudanças de entendimento das categorias pode gerar variações nos resultados. Dessa forma, as estatísticas devem ser usadas apenas como um instrumento para identificar tendências e não como uma forma de determinar um resultado específico;
iii. a análise foi feita a partir da leitura dos documentos. Se fosse um questionário preenchido pelos países, o entendimento de cada estratégia poderia ter nuances que não seriam plenamente identificadas em uma simples análise documental. Apesar de testada para que seja robusta, um certo nível de subjetividade está presente para interpretar documentos com formatos e níveis de detalhamento muito variados;
iv. essas limitações, todavia, não significam que não se possa usar a análise comparada para entender padrões e tendências. Por essa razão, cada seção inclui uma explicação qualitativa das tendências encontradas nos gráficos e constitui um convite para identificar possíveis padrões, embora usando de cautela nas conclusões.



3 Introdução: por que estudar as estratégias nacionais de cibersegurança?

Na era digital, a segurança cibernética tornou-se um imperativo estratégico para governos em todo o mundo. O crescente volume e sofisticação das ameaças cibernéticas destacaram a necessidade de estruturas de proteção robustas e coordenadas. Nesse contexto, as estratégias nacionais de cibersegurança surgem como instrumentos fundamentais para garantir a segurança e a resiliência do ciberespaço.

As estratégias nacionais de cibersegurança podem ser vistas como estruturas estratégicas que os países desenvolvem para proteger suas infraestruturas críticas, redes governamentais, empresas privadas e cidadãos contra ameaças crescentes no mundo digital. Embora não exista uma definição universal do que seja uma estratégia de cibersegurança, e que o próprio ITU no "Guia para o desenvolvimento de uma estratégia nacional de segurança cibernética"[10] aponte que "não existe uma definição consolidada e consensual do que constitui uma estratégia nacional de segurança cibernética", neste estudo, propõe-se considerar que uma estratégia nacional de cibersegurança engloba:

- uma expressão da visão, dos objetivos de alto nível, dos princípios e prioridades que orientam um país na abordagem da segurança cibernética;
- uma concepção das partes interessadas responsáveis por melhorar a segurança cibernética do país e seus respectivos papéis e responsabilidades; e
- uma descrição das medidas, dos programas e das iniciativas que um país tomará para proteger sua infraestrutura cibernética nacional e, no processo, aumentar sua segurança e resiliência.

O objetivo central das estratégias é fornecer orientações claras e atualizadas sobre como os governos, em coordenação com o setor privado e a sociedade civil, podem lidar com ameaças cibernéticas. Além de estabelecer metas e prioridades, essas estratégias também definem os papéis e responsabilidades de diferentes partes interessadas, promovem a cooperação internacional e promovem a inovação em tecnologia de segurança. Em outras palavras, eles servem como uma bússola para orientar os esforços de um país para melhorar sua maturidade em segurança cibernética de maneira abrangente.

Como o ambiente digital evolui rapidamente, os países normalmente atualizam suas estratégias de segurança cibernética a cada quatro ou cinco anos. Esse ciclo de atualização responde à necessidade de adaptação às novas tecnologias, ao surgimento de novas ameaças e à evolução do quadro jurídico internacional. O ciberespaço é dinâmico, e o que pode ter sido eficaz há alguns anos pode não ser eficaz hoje. Portanto, é crucial que os países revisem e renovem proativamente suas estratégias. Esperar até que uma estratégia

[10] Guia para o desenvolvimento de uma estratégia nacional de cibersegurança, 2021

expire para criar uma nova versão pode interromper processos evolutivos, causando estagnação e até retrocessos na evolução da maturidade cibernética do país. É importante ter em mente que as ações orientadas por uma estratégia são comumente a base sobre a qual os objetivos de sua antecessora são construídos.

Uma vez que os países mais avançados em aspectos de segurança cibernética passaram por um processo evolutivo em que as prioridades das diferentes versões de suas estratégias mudaram, à medida que foram sendo executadas, investigar os passos dados nessa jornada por diferentes países pode gerar lições de grande valor.

Dessa forma, um estudo comparativo das estratégias nacionais de segurança cibernética permite identificar tendências globais, avaliar a eficácia das políticas implementadas em diferentes países, aprender com as melhores práticas e fortalecer a cooperação internacional em segurança cibernética. Por meio dessa análise, é possível obter informações valiosas sobre os desafios comuns enfrentados pelos países no domínio cibernético, bem como as soluções mais inovadoras e eficazes.

4 Grandes tendências

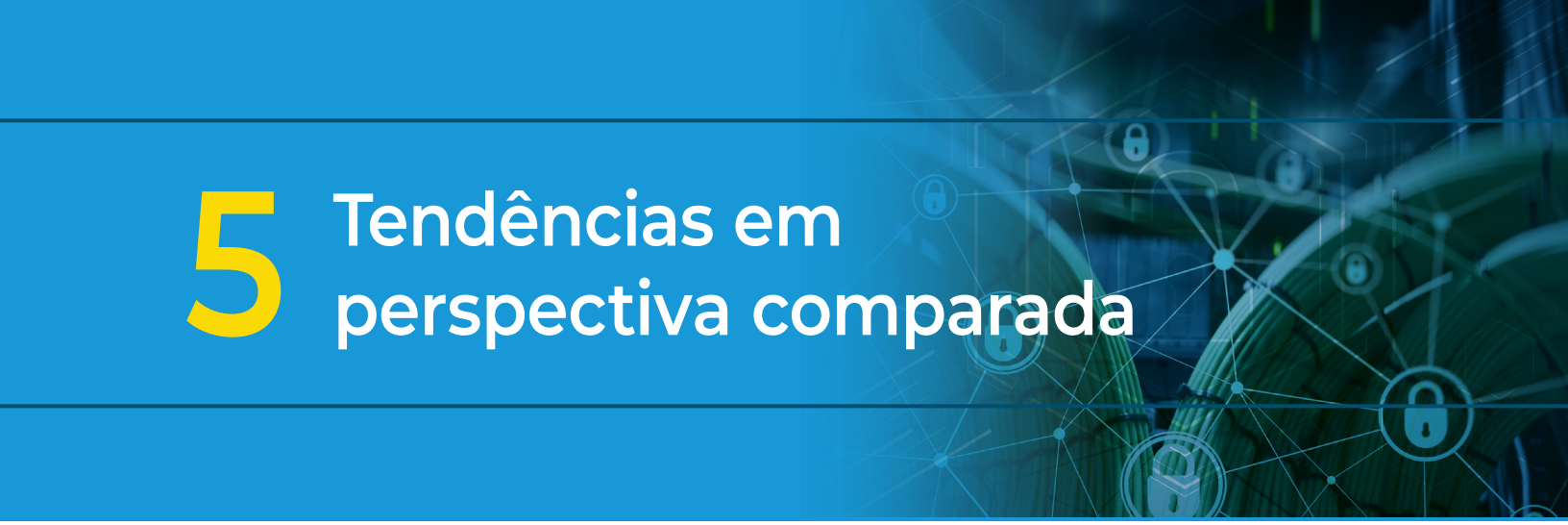
- **As estratégias da terceira geração são mais operativas e menos teóricas quando comparadas com as das gerações anteriores**. As estratégias de terceira geração definem mais claramente os responsáveis pelas ações incluídas (63% comparado com 26% nas de primeira geração), têm mais vinculação explícita com o orçamento[11] para a implementação da estratégia (88% comparado com 21% das de primeira geração), definem com mais frequência um plano operativo[12] (75% comparado com 37% nas de primeira) e, na medida do possível, incluem mais indicadores ou métricas de sucesso (25% comparado com 0% nas de primeira).
- **Recomendações e iniciativas para aprimorar os mecanismos de coordenação intragoverno e com o setor privado são frequentes nas estratégias vigentes.** Embora nem sempre as medidas propostas sejam concretamente identificáveis, nota-se a preocupação constante com a existência e o fortalecimento de mecanismos de coordenação, seja dentro do setor público, seja incluindo o setor privado e a academia.
- **Há uma tendência de que as estratégias mais recentes sejam mais amplas do que a segurança nacional e incluam temas de prosperidade econômica e fomento à indústria**. Em especial nos países do Norte Global, as estratégias de terceira geração tendem a incluir, com mais frequência, princípios (75%), objetivos (71%) ou iniciativas voltadas para o fomento à indústria para oportunidades econômicas (63%), entendendo a área da cibersegurança como um campo fértil para o desenvolvimento econômico e social.
- **A proteção de direitos humanos e direitos fundamentais é uma constante que permeia a grande maioria das estratégias, aparecendo como o princípio mais frequente.** Das estratégias vigentes analisadas que declaram princípios, 83% contêm algum princípio relacionado ao tema.
- **Iniciativas e objetivos vinculados aos temas de prontidão e resiliência, capacidades e sensibilização, e cooperação internacional estão presentes em virtualmente todas as estratégias.** Em alguns casos, os temas aparecem no nível mais alto como objetivos e, em outros, como iniciativas ou linhas de ação, mas sempre há uma preocupação ou uma ação voltada para esses tópicos.
- **Há uma tendência de que as estratégias incluam preocupação crescente com ataques à democracia.** Em termos das ameaças incluídas como preocupação

[11] Foram consideradas tanto as estratégias que já possuem orçamento definido no documento publicado como aquelas que mencionam que a estratégia terá orçamento definido na próxima etapa.

[12] Foram consideradas tanto as estratégias que já possuem um plano operativo no documento publicado como aquelas que mencionam que um plano de ação ou um plano de implementação será elaborado na próxima etapa.

das estratégias, nota-se o aumento crescente da inclusão de ameaças cibernéticas para promover ataques à democracia. Essa tendência se concentra nos países do Norte Global.

- **Nota-se o aumento dos temas da transparência e da confiança no ciberespaço nas estratégias de terceira geração.** Seja como princípio, seja como área focal, os temas de transparência e confiança têm aparecido de forma mais constante nas estratégias mais recentes, ilustrando a possível tendência de que o espaço cibernético e sua segurança sejam tratados com mais preocupação com os temas de transparência.
- **A necessidade de gerar recursos humanos capazes de enfrentar os desafios impostos pela segurança cibernética está fortemente presente nas estratégias analisadas.** Aspectos relacionados à pesquisa e desenvolvimento, conscientização e estudos formais estão presentes em todas as versões das estratégias. Em paralelo a isso, há uma tendência crescente de incorporar iniciativas relacionadas a medidas, para aumentar a capacidade dos servidores públicos e promover a geração de profissionais no setor privado.
- **A colaboração entre entidades e/ou países para detectar incidentes e responder a eles está desempenhando papel cada vez mais importante.** Isso pode ser observado no aumento da menção de iniciativas ligadas ao compartilhamento de informações relacionadas a incidentes e à cooperação entre os setores público e privado.



5 Tendências em perspectiva comparada

5.1. Estrutura das estratégias

PONTOS-CHAVE DA SEÇÃO

- **Variedade na estrutura:** as estratégias analisadas variam consideravelmente em sua estrutura (documentos de 5 a 130 páginas, com estilos mais teóricos ou operativos, com vigências definidas ou indeterminadas e com alcance e enfoque diferentes).
- **Componentes comuns:** apesar da variedade, as estratégias compartilham alguns componentes comuns para estruturar o documento:
  - 94,7% incluem objetivos estratégicos;
  - 63,2% incluem uma seção de princípios;
  - 63,2% definem uma visão clara para o país.
- **Indicadores:** a maioria das estratégias não possui indicadores ou métricas de sucesso associadas (somente 10,5%) – ver seção sobre indicadores e métricas para saber mais detalhes.

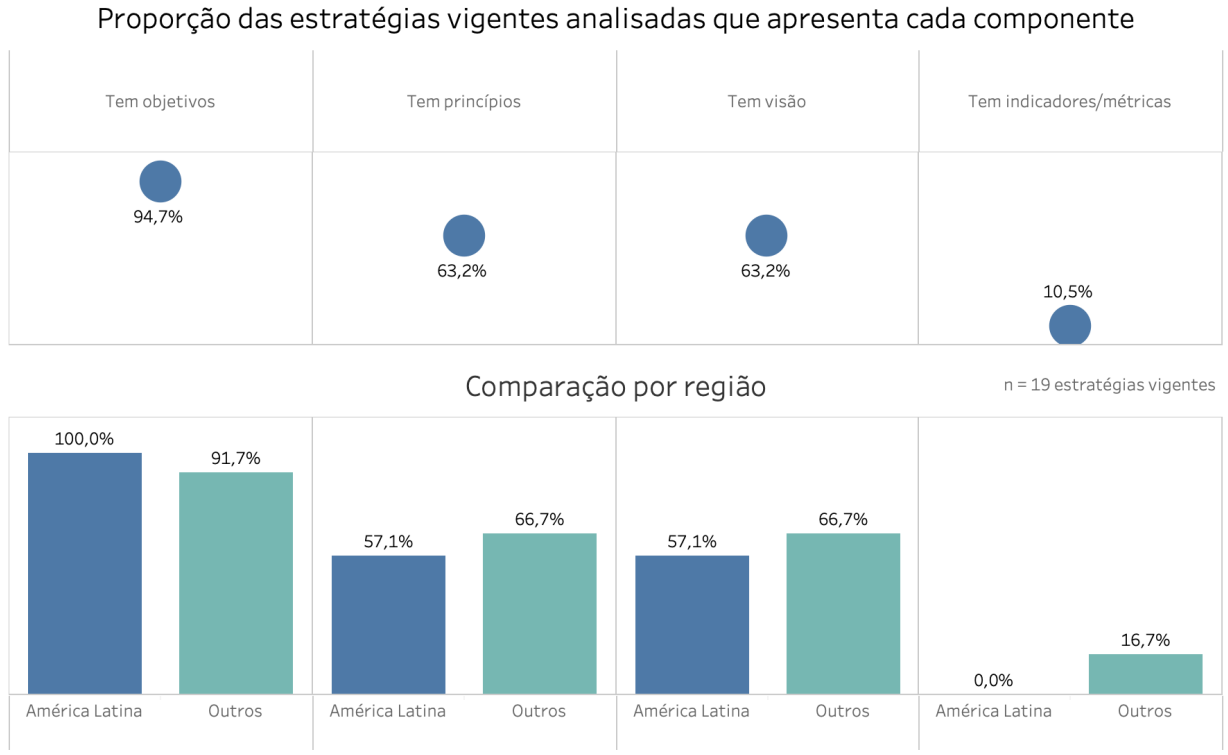
A comparação da estrutura e evolução das estratégias ao longo do tempo é desafiadora, dada a variedade de formatos, extensões e propósitos desses documentos. Para ilustrar a amplitude dessa diversidade, destaca-se que a estratégia mais breve analisada possui apenas cinco páginas,[13] enquanto a mais longa se estende por 130 páginas.[14] Além disso, as estratégias variam na duração de sua vigência, com algumas cobrindo um período de quatro anos, enquanto outras se estendem por dez anos, e muitas não definem um marco temporal específico, permanecendo vigentes até a promulgação de um novo documento.

Ademais, as estratégias também apresentam uma variedade de estilos, algumas adotando uma abordagem mais teórica e acadêmica, enquanto outras optam por uma abordagem mais prática e orientada à ação, delineando atividades concretas (esse aspecto será explorado com mais detalhe na seção sobre governança).

Apesar dessa heterogeneidade, é possível identificar componentes que são relativamente comuns nas diferentes estratégias (e que costumam ser padrão em documentos de estratégias de outros tópicos, não somente de cibersegurança). Dessa forma, para possibilitar a comparação das estruturas da amostra analisada, os documentos foram analisados a partir de quatro categorias: presença de objetivos estratégicos, inclusão de princípios, explicitação de uma visão e uso de indicadores. De forma geral, ficou evidente que a definição de objetivos é quase universal, sendo que apenas uma das 19 estratégias vigentes analisadas não possui objetivos claramente delineados. Além dos objetivos, cerca de dois terços das estratégias examinadas

[13] Corresponde à estratégia da Coreia de 2011.
[14] Corresponde à estratégia do Reino Unido de 2022.

GRÁFICO 1 – ESTRUTURA: COMPONENTES COMUNS ÀS ESTRATÉGIAS



incorporam princípios (consulte a seção *Princípios* para ver mais detalhes) e uma visão claramente definida. Já na categoria de indicadores, a presença é bastante incipiente, com apenas duas das estratégias vigentes incluindo algum tipo de indicador ou métrica de sucesso (consulte a seção *Indicadores e métricas de sucesso* para ver mais detalhes).

Na análise por região, é possível perceber que as estratégias analisadas do Norte Global se caracterizam pela presença um pouco maior de seções sobre princípios e possuem uma visão estabelecida com maior frequência, além de conter os poucos países que têm algum tipo de indicador/métrica para medir o sucesso da estratégia.

QUADRO 2 – CONHEÇA COM MAIS DETALHES COMO AS VISÕES DAS ESTRATÉGIAS ESTÃO ESTRUTURADAS

A visão deve ser uma declaração clara do que o governo pretende alcançar por meio da estratégia, enquadrada no formato aspiracional e com visão de futuro. Ela deve levar a uma expectativa compartilhada dos resultados e de como eles contribuem para objetivos mais amplos. É importante apresentar uma imagem convincente da transformação esperada e promover a compreensão compartilhada com todas as partes interessadas. Uma visão clara pode motivar diferentes atores a trabalhar na mesma direção, permitindo que todos entendam o que a estratégia busca alcançar e como esses objetivos se encaixam

(Continua na próxima página)

QUADRO 2. CONHEÇA COM MAIS DETALHES COMO AS VISÕES DAS ESTRATÉGIAS ESTÃO ESTRUTURADAS *(Continuação)*

em uma narrativa mais ampla. Portanto, a visão deve ser ambiciosa, ousada e inspiradora, mas alcançável em um horizonte de tempo realista. Quanto mais clara for a visão, mais convincente será a estratégia. Veja a seguir alguns exemplos de como os países têm estruturado suas visões (tradução dos autores).

País	Ano	Visão
Estônia	2014	"A Estônia é capaz de garantir a segurança nacional e apoiar o funcionamento de uma sociedade aberta, inclusiva e segura."
Reino Unido	2011	"Nossa visão é que o Reino Unido, em 2015, obtenha um enorme valor econômico e social de um ciberespaço vibrante, resiliente e seguro, no qual nossas ações, guiadas por nossos valores fundamentais de liberdade, justiça, transparência e estado de direito, aumentem a prosperidade, a segurança nacional e foraleçam a sociedade."
Reino Unido	2016	"Nossa visão para 2021 é que o Reino Unido seja seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital."
Reino Unido	2022	"Nossa visão é que, em 2030, o Reino Unido continuará a ser uma potência cibernética líder, responsável e democrática, capaz de proteger e promover nossos interesses no ciberespaço e por meio dele, em apoio aos objetivos nacionais."
Portugal	2019	"Que Portugal seja um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do estado de direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade."
Nova Zelândia	2015	"Nossa visão é que a Nova Zelândia seja segura, resiliente e próspera on-line."
Nova Zelândia	2019	"Esta estratégia tem a visão de que a Nova Zelândia seja confiante e segura no mundo digital — trata-se de permitir que a Nova Zelândia prospere on-line."
Coreia	2019	"Criar um espaço cibernético livre e seguro para apoiar a segurança nacional, promover a prosperidade econômica e contribuir para a paz internacional."
República Dominicana	2022	"Até o ano de 2030, a República Dominicana terá um espaço cibernético mais seguro, no qual as medidas necessárias estarão em vigor para o desenvolvimento confiável de atividades produtivas e recreativas para toda a população, dentro da estrutura de respeito aos direitos fundamentais."
Israel	2017	"O governo de Israel definiu uma visão para que Israel seja uma nação líder no aproveitamento do ciberespaço como um mecanismo de crescimento econômico, bem-estar social e segurança nacional."

As visões são abordadas de forma diferente nos exemplos acima. A maioria dos países, como o Reino Unido, Portugal e a Nova Zelândia, destaca a importância da segurança nacional e resiliência no ciberespaço e a busca por um ambiente digital seguro e resistente contra ameaças. Alguns países, incluindo o Reino Unido, a Estônia e Israel, reconhecem o ciberespaço como um motor para a prosperidade econômica. Eles compartilham a visão de usar o ciberespaço para impulsionar o crescimento econômico e o bem-estar social.

Ainda em termos comparativos, alguns países enfatizam valores fundamentais como liberdade, justiça, transparência e estado de direito como orientadores de suas ações no ciberespaço. Já outros países aproveitam a visão para destacar sua aspiração de ser uma nação líder no aproveitamento do ciberespaço. Isso demonstra a ambição de não apenas garantir a segurança e prosperidade internas, mas também de exercer influência global na arena cibernética.

5.2. Mecanismos de governança presentes nas estratégias

PONTOS-CHAVE DA SEÇÃO:

- **Autoridade em cibersegurança:** 78,9% das estratégias vigentes reconhece uma instituição responsável para os temas de cibersegurança (seja de forma geral para o tema, seja como guardião da estratégia).
- **Responsáveis claros:** embora se defina uma autoridade, as ações presentes na estratégia não têm claros responsáveis em cerca de dois terços das estratégias vigentes analisadas.
- **Orçamento:** 47,4% têm orçamento associado, seja na própria estratégia, seja previsto para um segundo momento.
- **Plano operativo:** 63,2% das estratégias têm ou preveem a criação de um plano operativo para sua implementação.
- **Ênfase na coordenação:** mais de 80% das estratégias preveem algum mecanismo de coordenação, seja intragoverno, seja com o setor privado. As estratégias do Norte global dão maior ênfase à coordenação com o setor privado do que às estratégias da América Latina.

Esta seção analisa categorias relacionadas à governança e institucionalidade das estratégias, procurando compreender que mecanismos existem para a implementação da estratégia e como se estrutura a coordenação para tal.

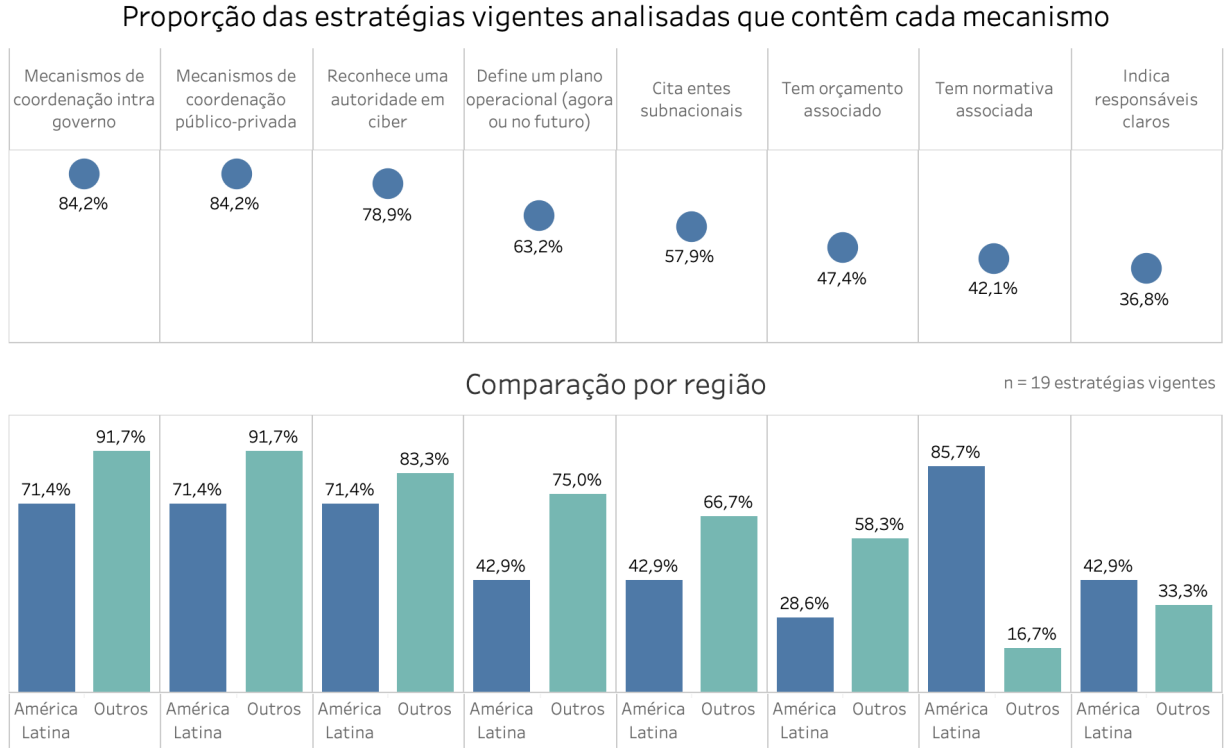
Alguns aspectos interessantes são a ênfase que a maior parte das estratégias dá ao tema da coordenação, seja olhando para dentro do governo (84,2%[15] das estratégias vigentes mencionam algum tipo de coordenação entre as agências governamentais), seja olhando para a coordenação entre o setor público e o setor privado (84,2%[16] das estratégias vigentes mencionam algum tipo de coordenação entre os setores). Além dos mecanismos de coordenação, também se destaca que cerca de 78,9% reconhecem algum órgão como autoridade para os temas de cibersegurança, de forma geral, e/ou especificamente para a liderança da implementação da estratégia.

Em termos comparados, a análise das 19 estratégias atualmente vigentes que fizeram parte da amostra selecionada indica que não é muito comum que as estratégias já mencionem o valor do orçamento destinado diretamente à estratégia. Contudo, cerca de metade das estratégias indica o orçamento destinado explicitamente ou menciona que o orçamento será buscado no futuro, o que indica uma preocupação com o financiamento e em conseguir executar as iniciativas contidas no documento. Embora não queira dizer que metade das estratégias não estão necessariamente respaldadas por um orçamento (uma vez que esta análise se limitou à leitura das estratégias sem aprofundar os orçamentos públicos dos países selecionados), essa tendência indica que este pode ser o caso para aproximadamente a metade delas.

Considerando que nenhuma estratégia se sustenta por si só, para garantir a execução das iniciativas incluídas no documento, é essencial definir os recursos que serão alocados para a estratégia e como esse processo será conduzido. Por exemplo, podem-se incluir apenas iniciativas que são financiadas pelo orçamento de cada instituição governamental ou destinar um orçamento especial às iniciativas que fazem parte do documento. Seja qual for o modelo escolhido por um país, o aspecto fundamental

[15] Aqui foram consideradas menções a mecanismos concretos de coordenação (por exemplo, conselhos, comitês etc.) e também menções mais genéricas (por exemplo, ações no futuro para aumentar a coordenação ou o reconhecimento explícito da necessidade da coordenação).
[16] Idem.

GRÁFICO 2 – ÁREA FOCAL: GOVERNANÇA E INSTITUCIONALIDADE



é garantir que as iniciativas incluídas na estratégia tenham os recursos necessários para serem executadas adequadamente.

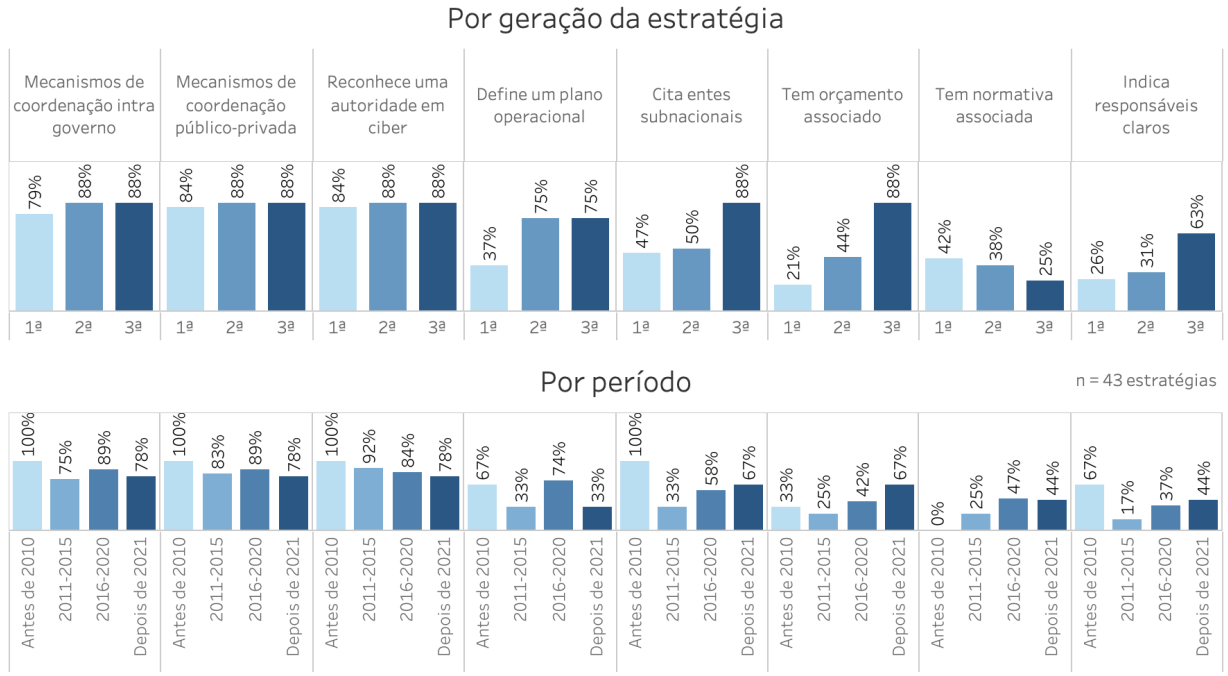
A análise por região indica que os países da América Latina apresentam uma tendência maior a vincular as suas estratégias a alguma normativa (decreto, portaria, resolução ou similar) e indicam que a preocupação com a coordenação com o setor privado e intragoverno está presente em menor escala do que nos países do Norte Global. Também é possível verificar que as estratégias da América Latina vinculam um orçamento em menor medida do que as estratégias do Norte Global, indicando uma possível oportunidade para fortalecer os documentos da região.

Olhando para a perspectiva evolutiva das estratégias (Gráfico 3), alguns padrões são interessantes. Em primeiro lugar, nota-se que as estratégias de terceira geração tendem a definir um plano operativo (seja na própria estratégia, seja previsto para a fase da implementação), indicando que as estratégias mais recentes tendem a ser menos teóricas e mais orientadas a ações concretas. Relacionado a esse ponto, também é possível notar um salto grande quando se observa a terceira geração de estratégias no que tange à definição clara de responsáveis para cada ação. Com efeito, nas estratégias de terceira geração, 63% definem mais claramente quem é responsável pelas ações contidas no plano, enquanto nas da segunda geração a frequência é somente 31%.

Na análise evolutiva, nota-se uma tendência de crescimento a ter orçamento vinculado às estratégias na terceira geração (de 21% na primeira geração para 88% na terceira), também reforçando a percepção indicada na seção de grandes tendências de que as estratégias estão

GRÁFICO 3 – EVOLUÇÃO DA ÁREA FOCAL: GOVERNANÇA E INSTITUCIONALIDADE

Evolução da presença dos mecanismos nas estratégias analisadas



se tornando cada vez mais operativas e executivas e menos teóricas.

Em relação aos mecanismos de aplicação da lei associados, as estratégias não costumam incluir obrigações e/ou punições pelo não seguimento. No geral, a linguagem das estratégias assume caráter mais orientador, definindo grandes linhas de atuação, prioridades, objetivos e recomendações. Ao mesmo tempo, muitas indicam que serão criados mecanismos para implementação das estratégias, como, por exemplo, a definição de pontos focais em cada departamento, a criação de obrigações de monitoramento anual, a criação de comitês que acompanharão a implementação, entre outros.

QUADRO 3 – APROFUNDAMENTO DA ÁREA FOCAL

Governança da estratégia da Estônia (2019)

A terceira estratégia da Estônia, atualmente em vigor, apresenta um modelo interessante de governança, incorporando mecanismos de coordenação interssecretarial e colaboração com o setor privado e a sociedade civil.

É importante destacar que o processo de elaboração da estratégia foi participativo, contando com a participação de órgãos do governo, da academia, de *think tanks* e do setor privado. Um processo

(Continua na próxima página)

QUADRO 3 – APROFUNDAMENTO DA ÁREA FOCAL *(Continuação)*

desse tipo auxilia na fase da implementação, uma vez que os diferentes atores já se apropriaram dos conteúdos e objetivos do documento.

O planejamento da política de segurança cibernética e a implementação da estratégia são coordenados pelo Ministério de Assuntos Econômicos e Comunicações, o mesmo responsável pelos temas de governo digital e transformação digital do setor público. Em nível estratégico, a coordenação ocorre por meio do Conselho de Segurança Cibernética do Comitê de Segurança do Governo da República, que garante a implementação dos objetivos da estratégia por meio de documentos de planejamento, programas e planos de trabalho elaborados com as instituições governamentais responsáveis. A principal responsabilidade pela implementação da estratégia cabe, então, às instituições governamentais que fazem parte do Conselho.

Para a execução coordenada dos objetivos acordados na estratégia, nomeia-se, em cada ministério/órgão, um ponto focal responsável que atua como ligação para as questões relacionadas com a garantia da cibersegurança nacional na sua área e assegura que as prioridades acordadas na estratégia sejam executadas e respaldadas nos documentos de planejamento de seu departamento. A cooperação e a troca de informações entre os responsáveis é coordenada pelo Ministério dos Assuntos Econômicos e das Comunicações.

Uma vez por ano, o Comitê de Segurança do Governo da República aprova o relatório consolidado sobre as atividades de cada organismo no domínio da cibersegurança para compartilhar com a sociedade e com o governo uma visão panorâmica das atividades realizadas no escopo da estratégia.

Para além da governança no âmbito do governo, a estratégia também delineia um plano para a cooperação com os centros de competência, as universidades, as instituições de pesquisa e os parceiros do setor privado com conhecimentos e capacidades nesse domínio. Aqui, destacam-se o Centro de Excelência de Ciberdefesa Cooperativa da OTAN (CCD COE) e a e-Governance Academy (EGA), um centro de consulta e reflexão para a sociedade da informação. A estratégia também cita outros parceiros para a troca de conhecimento e expertise.

5.3. Métricas e indicadores

PONTOS-CHAVE DA SEÇÃO

- **Incipiência da presença de indicadores:** entre as estratégias atualmente vigentes, apenas duas possuem algum tipo de indicador quantitativo e/ou métricas de sucesso. Ampliando a análise para ver a evolução da presença de indicadores, entre as 43 estratégias analisadas, além daquelas em vigor mencionadas, apenas mais duas possuem algum tipo de métrica de sucesso.

Além dos principais elementos que garantem a efetiva governança, a literatura enfatiza a importância dos mecanismos de monitoramento das estratégias. Seu estabelecimento, juntamente com o de indicadores-chave de desempenho ou outras medidas para uma avaliação, é importante para a implementação bem-sucedida das estratégias. No entanto, apesar da importância de as estratégias possuírem indicadores e formas de monitoramento, a análise realizada permitiu apurar que a presença de indicadores ou métricas de sucesso nas estratégias é muito incipiente. Entre as 19 estratégias em vigor, apenas duas têm indicadores (Estônia, 2019, e França, 2021). Ampliando a análise para

incluir as estratégias antigas, também há duas estratégias de segunda geração que têm métricas qualitativas de sucesso (Reino Unido, 2016, e Austrália, 2020).

Vale destacar que algumas estratégias mencionam que os indicadores e os ritos de monitoramento serão definidos em etapa posterior, prevendo, por exemplo, a elaboração de um plano de ação para a implementação da estratégia. Esses documentos adicionais não entraram no escopo da análise.

Nesta seção, serão explorados com mais detalhe os indicadores presentes na terceira estratégia da Estônia (2019), na terceira estratégia da França (2021) e na segunda estratégia do Reino Unido (2016). Uma vez que a Estônia é referência no tema e pioneira na publicação das estratégias, entende-se que, embora ainda não se reflita nos dados, o fato dessa estratégia explicitar os indicadores pode indicar uma tendência que outros países passarão a seguir na publicação de seus documentos futuros.

A seguir, um resumo dos tipos de indicadores contidos na estratégia mencionada. Os tipos incluem indicadores de impacto, ligados transversalmente à estratégia, e indicadores de performance, ligados a cada objetivo.

Entre os indicadores de impacto monitorados na estratégia, destacam-se:

- percentual de residentes que evitam a comunicação eletrônica com o setor público ou com provedores de serviço para evitar riscos de segurança;
- percentual de usuários com identidade digital segura.

Sobre os indicadores de performance, alguns podem servir de inspiração para a elaboração de novas estratégias:

- número total de serviços abertos na rede do Estado;
- volume de exportações das empresas do setor;
- número de novas startups no setor de cibersegurança;
- número de doutorados defendidos em temas de cibersegurança;
- percentual de usuários que tiveram perdas por serem expostos a alguma vulnerabilidade on-line;
- percentual de empresas que usam uma política de segurança de Tecnologia da Informação e Comunicações (TIC) oficial;
- nível de conscientização e competências em cibersegurança entre os funcionários do setor público;
- déficit da força de trabalho no setor.

O caso da estratégia de 2021 da França é interessante, por se tratar de uma estratégia bastante focada no aspecto econômico da cibersegurança, reiterando mais uma vez a tendência de que as estratégias mais novas do Norte Global incluam os temas de prosperidade econômica com mais frequência. Embora não se trate de indicadores de monitoramento da estratégia especificamente, seu destaque se deve ao fato de incluir metas que orientam a estratégia. Entre elas, destacam-se: triplicar as vendas do setor de cibersegurança, duplicar o número de empregos no setor, aumentar em 20% o número de patentes registradas, entre outras.

A abordagem qualitativa de métricas de sucesso adotada na estratégia do Reino Unido também é interessante, pois materializa o que se entende como sucesso da implementação da estratégia. Nesse caso, a estratégia define resultados estratégicos esperados e medidas que indicam o atingimento desse resultado. Contudo, entende-se que esse formato dificulta o monitoramento mais objetivo do atingimento dos resultados esperados. Veja a seguir alguns exemplos de como essa abordagem é utilizada:

- Resultado esperado: o Reino Unido tem capacidade de gerenciar e responder com eficácia a incidentes cibernéticos para reduzir os danos causados ao país e combater os adversários cibernéticos.
- Indicativos de sucesso:
  - uma proporção maior de incidentes é relatada às autoridades, o que leva à melhor compreensão do tamanho e da escala da ameaça;
  - os incidentes cibernéticos são gerenciados de forma mais eficaz, eficiente e abrangente, como resultado da criação do Centro Nacional de Segurança Cibernética como um mecanismo centralizado de notificação e resposta a incidentes;
  - há uma redução da ocorrência de exploração repetida em vítimas e setores.

5.4. Desafios e ameaças

PONTOS-CHAVE DA SEÇÃO

- **Componente de ameaças e desafios:** é comum que as estratégias incluam alguma seção ou capítulo dedicado aos tipos de ameaça e desafios relacionados à cibersegurança em seu contexto.
- **Tipos comuns de ameaça:** entre os tipos mais comuns de ameaça mencionados nos documentos, destacam-se: (i) ciberataques criminosos (84,2%); (ii) ciberguerra ou outros países (57,9%); (iii) terrorismo (57.9%); e (iv) espionagem (42,1%).
- **Evolução dos tipos de ameaça:** percebe-se a diminuição do foco em ataques terroristas e o aumento de novas ameaças como ataques à democracia.
- **Ataques à democracia:** a tendência a incluir ataques à democracia como ameaça no ciberespaço cresce nas estratégias de terceira geração dos países do Norte global.

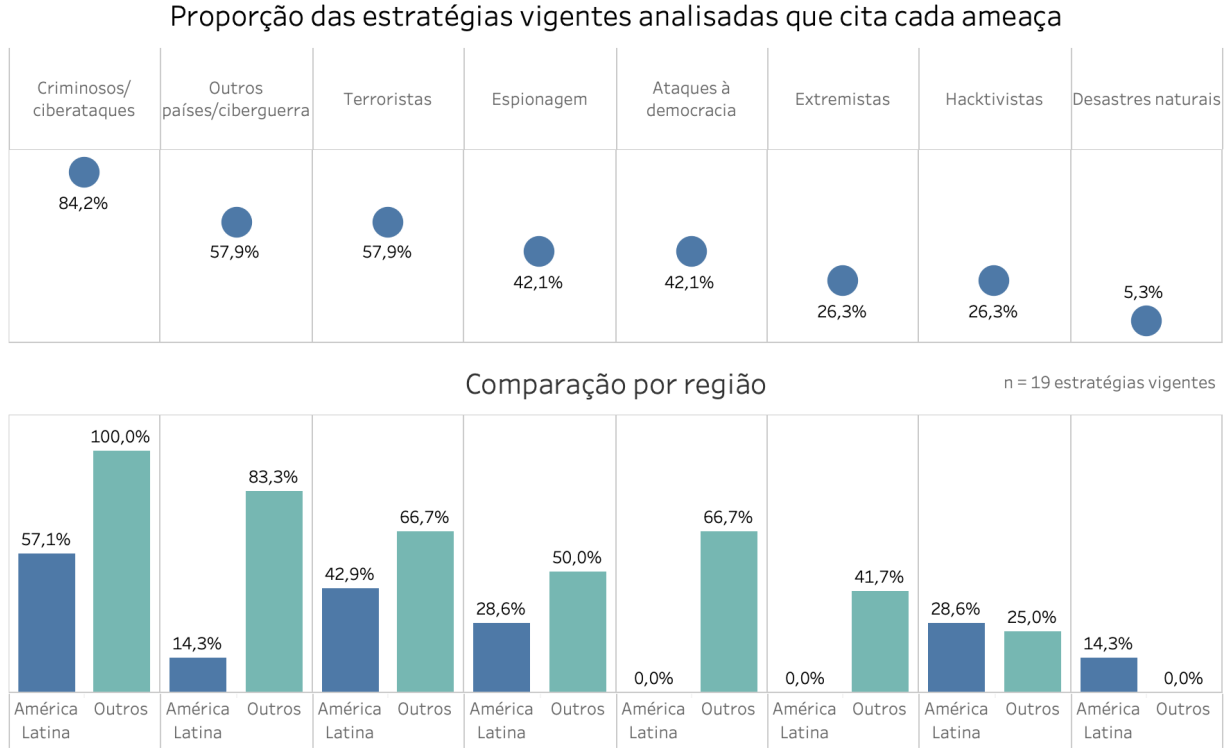
É muito comum que as estratégias de cibersegurança incluam alguma seção ou capítulo dedicado a discorrer sobre quais são os tipos de ameaça e desafios que o país enfrenta na área. A estratégia, de alguma forma, vem justamente como uma resposta a esses tipos de ameaça. Em alguns casos, como é o exemplo da primeira estratégia da Estônia (2008), os tipos de ameaças assumem um contorno bem real, exemplificado pelo grande ataque que o país sofrera no ano anterior. Em outros casos, trata-se de mapear as principais categorias de riscos associados, de forma a garantir que as iniciativas incluídas na estratégia possam dar conta de tais ameaças.

Conforme ilustrado no Gráfico 4, entre os tipos de ameaça mais frequentes, destaca-se que 84,2% das estratégias analisadas citam ciberataques criminosos, e cerca de 60% citam ataques de outros países (ou ciberguerra) como ameaças recorrentes. Em seguida, temas de terrorismo e espionagem aparecem ocupando a terceira e quarta posições entre as ameaças mais frequentemente identificadas.

Na comparação regional, pode-se inferir alguns padrões interessantes. A primeira reflexão é que as estratégias do Norte Global da amostra costumam incluir um apanhado das ameaças com maior frequência do que as estratégias da América Latina e do Caribe. O segundo ponto é que, mesmo entre as estratégias que incluem ameaças, alguns tipos parecem ser mais frequentes nas estratégias fora da região da América Latina, o que pode ser explicado por fatores geopolíticos, entre outros. Nesse sentido, destaca-se como a ameaça criada por outros países, o terrorismo e os ataques à democracia estão mais presentes em estratégias fora do continente americano.

O Gráfico 5 mostra a evolução da menção aos tipos de ameaça ao longo do tempo e por geração. Essa série comparativa permite identificar padrões interessantes vinculados a fatos históricos e geopolíticos. Por exemplo,

GRÁFICO 4 – TIPOS DE AMEAÇA IDENTIFICADOS



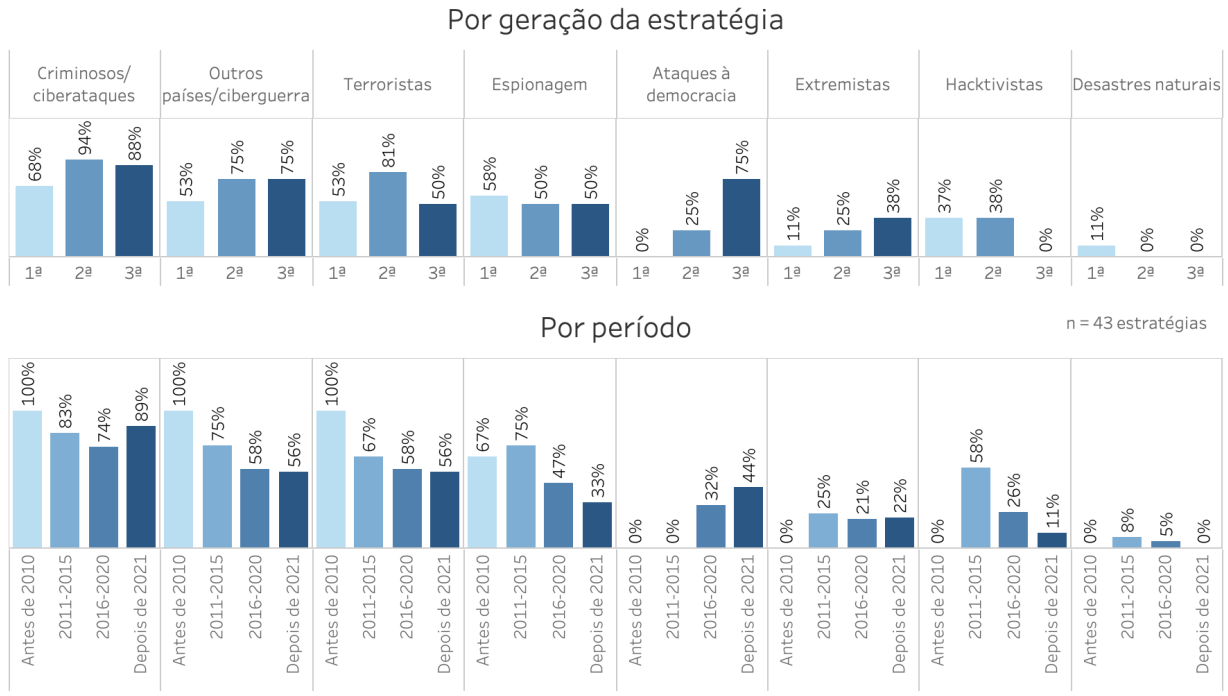
destaca-se a gradual diminuição das estratégias que citam explicitamente os terroristas como as principiais ameaças enfrentadas por seu país em matéria de cibersegurança (o auge desse tipo de ameaça foi antes de 2015). Outro destaque interessante é o forte crescimento de ameaças centradas em ataques à democracia, na terceira geração de estratégias, indicando uma possível tendência para os próximos anos. Casos como a interferência russa nas eleições americanas e outros episódios podem estar na raiz desse salto recente.

Em relação aos desafios da área de cibersegurança, não foi possível realizar uma categorização padrão para fazer uma análise comparada. Isso se deveu ao fato de que, muitas vezes, os desafios mencionados estavam vinculados a contextos específicos ou eram abordados de forma fragmentada ao longo das estratégias, sem uma seção dedicada que permitisse extrair dados de maneira uniforme em todas as estratégias da amostra selecionada.

Apesar dessa heterogeneidade, é importante destacar que alguns desafios são recorrentes em várias das estratégias analisadas. Entre eles, o crescimento exponencial da tecnologia e o aumento da conectividade, com sua consequente expansão do ciberespaço, emergem como desafios compartilhados por praticamente todos os países. Para além do tamanho do ciberespaço, muitas estratégias mencionam como principal desafio a dependência crescente das sociedades no ciberespaço. Nessa linha, as estratégias mais modernas têm enfatizado como os ataques cibernéticos, cada vez mais, representam ataques à forma de vida e valores sociais. Nesse quesito, muitas das estratégias mencionam os desafios e ameaças relacionados à proteção das infraestruturas críticas e dos serviços essenciais. Também é comum

GRÁFICO 5 – TIPOS DE AMEAÇA IDENTIFICADOS

Evolução da presença das ameaças citadas nas estratégias analisadas



citar desafios e riscos associados à maior digitalização dos serviços públicos.

Ademais, algumas estratégias abordam desafios mais específicos com maior detalhe. Um que merece destaque é a falta de oferta de profissionais de cibersegurança qualificados nos países, indicando um déficit desse tipo de profissional e a urgência de que as estratégias também incluam iniciativas para superar essa situação (as medidas que têm sido priorizadas serão exploradas na seção sobre capacidades).

Por fim, ainda no âmbito amplo dos desafios mencionados, vale lembrar que algumas estratégias, em geral do Norte Global, indicam as mudanças geopolíticas como um grande desafio para os temas de cibersegurança. Também é muito presente o desafio da natureza transnacional do ciberespaço, indicando que é impossível que as estratégias não levem em conta iniciativas para fortalecer o ciberespaço para além de suas fronteiras nacionais. O tema da cooperação internacional será explorado na seção correspondente.

QUADRO 4 – ESTUDO DE CASO

ESTRATÉGIAS DE CIBERSEGURANÇA NA ESPANHA E O ESQUEMA DE SEGURANÇA NACIONAL

Apesar de não ter sido um dos primeiros países a ter uma estratégia de segurança cibernética, a Espanha desenvolveu sua primeira estratégia antes da maioria dos países estudados (2013), lançando sua segunda versão em 2019. Embora ambas as estratégias tenham muitos pontos notáveis, há dois

(Continua na próxima página)

QUADRO 4 – ESTUDO DE CASO *(Continuação)*

conceitos que permitem interessantes discussões: a geração de uma estrutura comum para a gestão da segurança cibernética em todo o Estado e a definição, desde o início, de uma estrutura organizacional para apoiar os objetivos das estratégias.

O Esquema de Segurança Nacional é um marco comum de princípios básicos, requisitos e medidas de segurança para a proteção adequada das informações processadas e dos serviços prestados pela administração pública e seus fornecedores. Sua definição começou antes do lançamento da primeira estratégia de segurança nacional, mas foi na estratégia que ela foi estabelecida como uma linha de ação específica. O marco também manteve seu papel importante na segunda versão da estratégia. Sua constante evolução, a definição de regulamentações e o desenvolvimento de um ecossistema público-privado proporcionaram à Espanha uma ferramenta capaz de estabelecer requisitos mínimos de segurança mensuráveis e auditáveis, capazes de melhorar a segurança cibernética em todo o país.

Em sua primeira estratégia, a Espanha dedica um capítulo inteiro à definição de uma estrutura organizacional para a segurança cibernética, a fim de apoiar os objetivos definidos. Em busca de uma visão abrangente da segurança cibernética e de acordo com os princípios do Sistema de Segurança Nacional, ela define dois comitês no âmbito do Conselho de Segurança Nacional, um especializado em segurança cibernética e outro especializado em consciência situacional. O primeiro apoiará a coordenação da Política de Segurança Nacional na área de segurança cibernética, enquanto o segundo será convocado para gerenciar situações de crise nessa área. Na segunda versão da estratégia, essa estrutura é ampliada, substituindo o comitê de segurança cibernética por uma nova estrutura liderada pelo Conselho Nacional de Segurança Cibernética. Esse conselho tem três entidades: o Fórum Nacional de Segurança Cibernética, a Comissão Permanente de Segurança Cibernética e uma terceira, formada pelas autoridades públicas competentes na área de segurança de redes, sistemas de informação e os CSIRTs de referência nacional.

Tanto o Esquema de Segurança Nacional quanto a definição antecipada de uma estrutura organizacional são exemplos de ações que tiveram relação direta com a melhoria da maturidade da segurança cibernética da Espanha. Não apenas por causa de seu momento oportuno, mas também devido à sua constante evolução ao longo do tempo.

Fontes: estratégias de cibersegurança da Espanha.

5.5. Princípios

PONTOS-CHAVE DA SEÇÃO

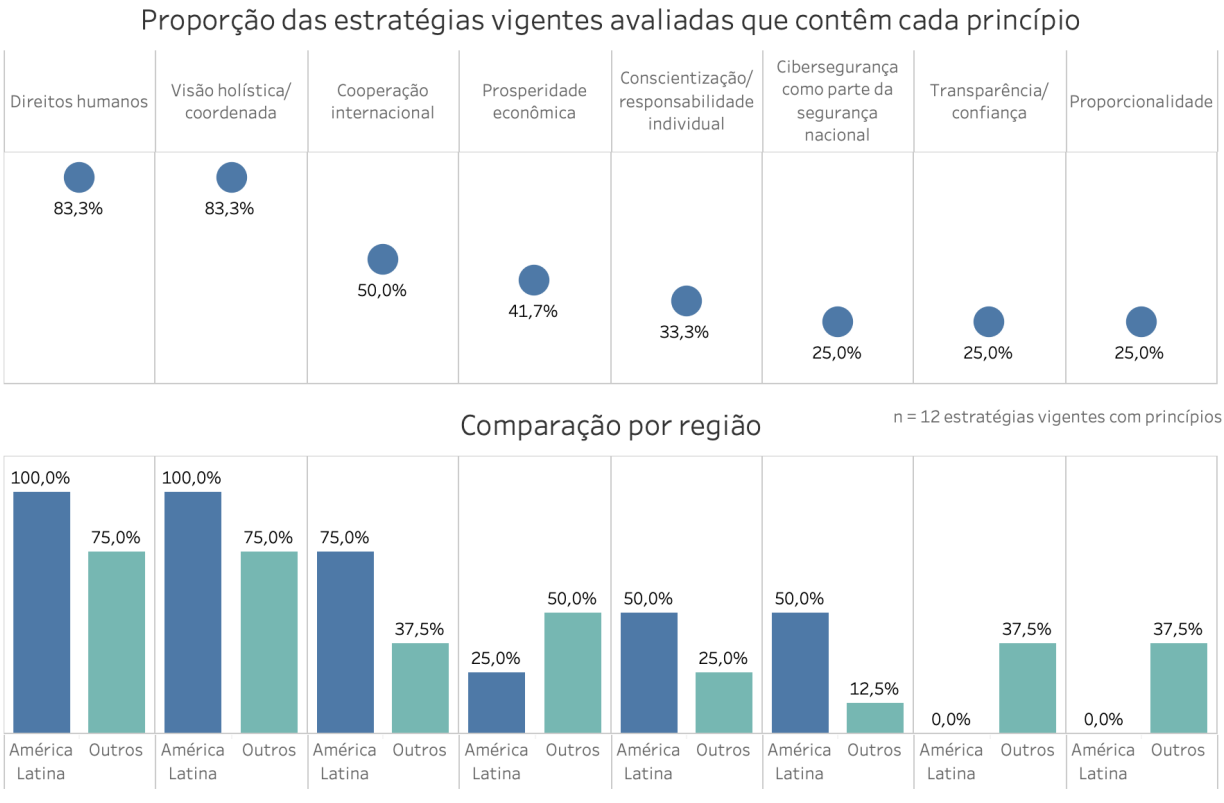
- **Princípios:** cerca de dois terços das estratégias analisadas têm uma seção dedicada a compartilhar seus princípios.
- **Direitos humanos:** o princípio mais comum, citado em 83,3% das estratégias vigentes, se refere a temas relacionados aos direitos humanos ou à proteção dos direitos fundamentais.
- **Prosperidade econômica:** nota-se uma tendência, principalmente fora da América Latina, ao aumento da menção de princípios relacionados à prosperidade econômica, indicando uma possível tendência de que as estratégias enfatizem temas de economia e fomento à indústria, para além dos temas mais clássicos de segurança nacional.
- **Transparência e confiança:** também se destaca o aumento significativo de princípios relacionados à transparência nas estratégias de terceira geração.

O entendimento sobre o que oconceito de cibersegurança engloba não é necessariamente consensuado entre todos os atores. Como resultado, as estratégias costumam incluir princípios fundamentais para orientar os formuladores de políticas e garantir que todas as partes interessadas tenham um entendimento comum do que é esperado. Os princípios são um conjunto de diretrizes que informam e apoiam a forma como a cibersegurança deve ser abordada de forma transversal. Em termos gerais, eles fornecem uma referência robusta, mas flexível, para ajudar a orientar as decisões sobre essas questões.

Como evidenciado na seção sobre as estruturas das estratégias, cerca de dois terços incluem uma seção dedicada aos princípios. Em termos de formato, as estratégias usam diferentes níveis de detalhes em seus princípios, desde palavras isoladas até frases inteiras que incorporam diretrizes estratégicas. Os Gráficos 6 e 7 destacam os temas dos princípios mais comuns encontrados nas estratégias analisadas, bem como sua evolução ao longo do tempo.

É crucial ressaltar que não se pode tirar conclusões precipitadas com base nesses padrões. O fato de um princípio específico ganhar ou perder destaque ao longo do tempo não implica, necessariamente, que o tema associado tenha ganhado ou perdido importância na estratégia do país. Por exemplo, pode-se observar a diminuição das referências a princípios de cooperação internacional em estratégias mais recentes ou nas estratégias de terceira geração. No entanto, é importante notar que a cooperação internacional ainda é um tema recorrente em todas as estratégias. Esse fato pode indicar que, nas primeiras estratégias, o tema entrava de forma transversal como princípio, mas que

GRÁFICO 6 – TIPOS DE PRINCÍPIOS



agora há uma tendência de que o tema seja tratado como um objetivo estratégico com iniciativas associadas.

A hipótese aqui levantada é a de que os temas entram como princípios quando os países ainda não têm clareza sobre como operacionalizá-los na prática (e traduzi-los em objetivos ou ações concretas), mas já querem demonstrar que os consideram importantes e transversais. Já quando há maior clareza sobre as formas de operacionalização, os temas presentes nos princípios passam a se tornar objetivos com graus de concretude maior.

Entre os princípios mais proeminentes nas estratégias, o tema dos direitos humanos e dos direitos fundamentais se destaca de maneira significativa. Embora diferentes estratégias possam abordá-lo de formas distintas, nota-se que 83,3% das estratégias vigentes incorporam algum princípio relacionado a esse tema. É relevante observar que todas as estratégias na América Latina incluem tal princípio. Alguns exemplos ilustrativos (tradução dos autores) incluem:

- A proteção e a promoção dos direitos e liberdades fundamentais são consideradas tão importantes no espaço cibernético quanto no ambiente físico (Estônia, 2019).
- Os valores fundamentais do Reino Unido serão protegidos e promovidos rigorosamente. Esses valores incluem a democracia, o estado de direito, a liberdade, os governos e as instituições abertos e responsáveis, os direitos humanos e a liberdade de expressão (Reino Unido, 2016).
- Equilíbrio dos direitos individuais com a segurança cibernética: alcançar equilíbrio entre a proteção do espaço cibernético e a salvaguarda dos direitos fundamentais das pessoas, por exemplo, a privacidade (Coreia, 2019).
- Respeito aos direitos e liberdades individuais: a proteção dos indivíduos na área de segurança cibernética deve contemplar o respeito aos direitos e liberdades individuais consagrados na constituição nacional e nos Tratados Internacionais dos quais a República Argentina é signatária (Argentina, 2019).

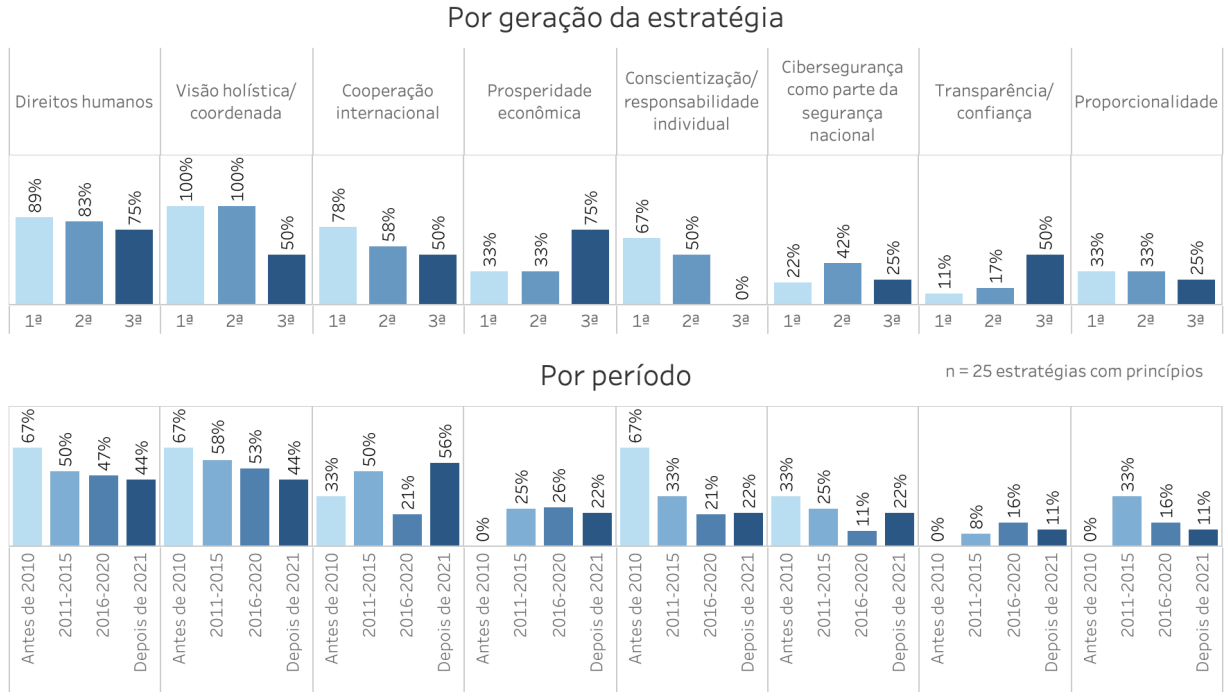
Outro destaque é que 83,3% das estratégias atualmente vigentes incorporam algum tipo de princípio que enfatiza a necessidade de coordenação ou que considera a cibersegurança como um tema holístico e interconectado. Em determinados casos, essa coordenação é mencionada em relação a diferentes atores, tanto do setor privado quanto do público. Em outros casos, ressalta-se a importância de não segmentar a cibersegurança em uma categoria isolada, separada dos demais temas de segurança e/ou transformação digital. Alguns exemplos (tradução dos autores) elucidativos:

- O trabalho será em parceria. Somente trabalhando com as Administrações Devolvidas, todas as partes do setor público, empresas, instituições e o cidadão individual, é possível proteger com sucesso o Reino Unido no ciberespaço (Reino Unido, 2016).
- Garantia de responsabilidade compartilhada entre várias partes interessadas, promovendo o máximo de colaboração e cooperação, levando em conta a função e o grau de responsabilidade de cada parte para gerenciar os riscos de segurança digital e proteger o ambiente digital (Colômbia, 2016).

Quando se observam os padrões de evolução dos princípios (Gráfico 7), alguns pontos chamam a atenção e podem dar pistas sobre as tendências recentes de evolução das estratégias.

Um ponto que merece destaque é o princípio da prosperidade econômica. Nota-se que há um padrão claro em relação às gerações de

GRÁFICO 7 – EVOLUÇÃO DOS TIPOS DE PRINCÍPIO NAS ESTRATÉGIAS ANALISADAS



estratégias. Enquanto nas primeiras estratégias era menos comum se falar de prosperidade econômica, 75% das estratégias da terceira geração têm um princípio relacionado ao tema. Esse dado pode indicar a tendência de que as estratégias mais recentes não tenham foco puramente em segurança nacional ou proteção, mas ampliem o alcance e escopo para incorporar temas relacionados ao fomento da indústria e outros.

Além disso, é interessante observar que a América Latina ainda não está dando ênfase a essa dimensão em suas estratégias. Apenas uma em cada quatro estratégias da amostra do continente destaca claramente a prosperidade econômica como princípio orientador do documento, indicando uma área potencial de crescimento e desenvolvimento para futuras políticas e estratégias na região. Os exemplos a seguir ilustram como o princípio se manifesta em algumas estratégias:

- A segurança cibernética é vista como uma facilitadora e amplificadora do rápido desenvolvimento digital da Estônia, que é a base para o crescimento socioeconômico do país. A segurança deve apoiar a inovação, e esta deve apoiar a segurança (Estônia, 2019).
- A capacidade dos cidadãos e das empresas de operar no ciberespaço de forma segura e protegida será prioridade, para que possam maximizar os benefícios econômicos e sociais da tecnologia digital e exercer seus direitos legais e democráticos (Reino Unido, 2022).
- Incentivo da segurança cibernética para os negócios, o crescimento econômico e a prosperidade (Canadá, 2018).

Outro padrão interessante que se destaca é a diminuição, ao longo do tempo e ao longo das gerações das estratégias, do princípio

relacionado à conscientização geral da população e/ou ao foco na responsabilidade individual em relação ao tema da cibersegurança. Assim como mencionado com o tema da cooperação internacional, essa diminuição não indica que o tema tenha saído do foco das estratégias. Conforme os dados da seção sobre capacidades, quase todas as estratégias vigentes da amostra têm pelo menos uma medida relacionada a programas de conscientização. Isso indica a transferência do tema do princípio transversal para a área focal com ações específicas.

Por fim, vale destacar o crescimento do princípio da transparência nas estratégias de terceira geração. Esse princípio indica a crescente atenção para a necessidade de as políticas de cibersegurança incorporarem transparência e se concentrarem em aumentar a confiança no ciberespaço. Esse aumento na importância atribuída à transparência sugere uma mudança nas abordagens anteriores, indicando uma tendência geral em direção a políticas mais abertas em relação à cibersegurança.

5.6. Objetivos estratégicos

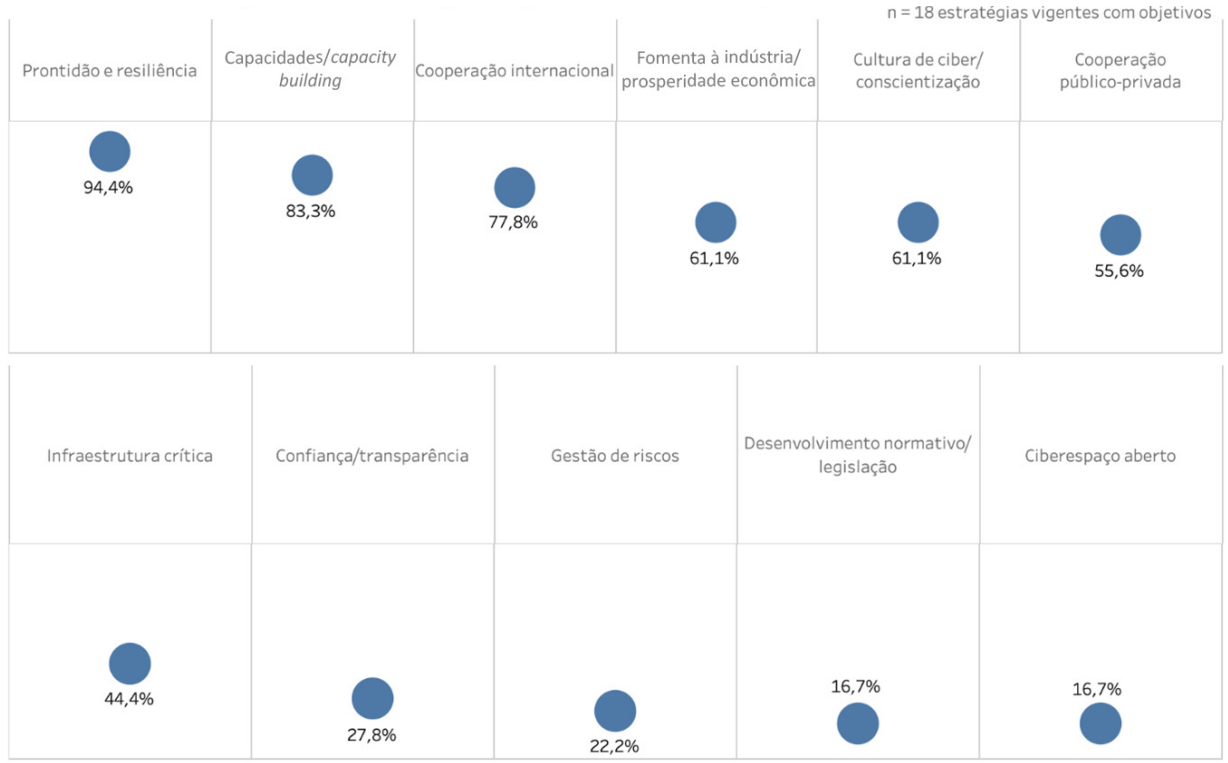
PONTOS-CHAVE DA SEÇÃO

- **Objetivos:** 94,7% das estratégias analisadas definem objetivos estratégicos.
- **Prontidão e resiliência:** 94,4% das estratégias analisadas possui pelo menos um objetivo relacionado aos temas de prontidão e resiliência.
- **Capacidades:** 83,3% das estratégias analisadas possui pelo menos um objetivo para o fortalecimento das capacidades em cibersegurança do país.
- **Prosperidade econômica:** assim como nos princípios, nota-se o aumento da presença de objetivos ligados ao fomento da indústria de cibersegurança, principalmente nos países do Norte Global (71% nas estratégias de terceira geração, comparado com 39% nas de primeira geração).
- **Cooperação público-privada:** as estratégias da terceira geração apresentam com mais frequência objetivos estratégicos ligados à cooperação público-privada (71% comparado com 44% na primeira geração).
- **Transparência:** as estratégias de 3ª geração apresentam com mais frequência objetivos ligados à transparência (43% comparado com 17% na primeira geração)

Os objetivos são o coração das estratégias e, como visto, somente uma das 43 estratégias analisadas não os define explicitamente. Assim como se analisou a evolução dos princípios ao longo do tempo, esta seção analisa os destaques do conteúdo dos objetivos, bem como sua evolução ao longo da geração das estratégias e ao longo do tempo. Para fazer uma análise exaustiva, foram identificados sete temas que abrangem a maior parte dos objetivos presentes nas estratégias e, no Gráfico 8, destacou-se a frequência de aparição. Vale destacar que esta análise inclui somente o nível mais alto dos objetivos, isto é, se uma estratégia, por exemplo, possuía objetivos estratégicos e subobjetivos, esse gráfico identifica somente o nível de objetivos estratégicos. Por essa limitação, também é importante ter cautela nas conclusões. O fato de que um país não tenha colocado no seu nível mais alto um determinado tema não implica que não possua frentes de ações concretas sobre esse tema. Os subobjetivos serão tratados nas áreas focais exploradas nas próximas seções.

Pode-se notar que 94,4% das estratégias vigentes analisadas possuem pelo menos um objetivo que inclui temas de prontidão e resiliência. Em segundo lugar, os objetivos de fortalecimento das capacidades do país em

GRÁFICO 8 – TIPOS DE OBJETIVOS



cibersegurança e algum objetivo relacionado à cooperação internacional aparecem em 83,3% e 77,8% das estratégias analisadas, respectivamente. Os demais temas comuns estão evidenciados no gráfico acima.

Em relação à análise por região (Gráfico 9), nota-se que, em muitas categorias, não parece haver diferenças tão significativas entre as regiões estudadas. Contudo, alguns temas reforçam as tendências vistas nas seções anteriores e merecem destaque.

Em primeiro lugar, assim como o princípio da prosperidade econômica não estava muito presente nos princípios das estratégias da América Latina, nota-se que objetivos estratégicos vinculados ao fomento da indústria de cibersegurança também estão menos presentes na região. Ao mesmo tempo que o tema aparece em 42,9% das estratégias analisadas na América Latina, 72,7% das estratégias do Norte Global possuem algum tipo de objetivo estratégico focado na indústria nacional ou na prosperidade econômica.

Outro destaque que vale a menção é que as estratégias da América Latina possuem uma frequência maior de objetivos relacionados ao desenvolvimento normativo ou melhora legislativa nos temas de cibersegurança, quando comparadas com as dos países da amostra fora da região. As estratégias da América Latina atualmente vigentes também possuem maior frequência de objetivos estratégicos relacionados à gestão de riscos.

A evolução dos objetivos pela ótica da geração (Gráfico 10) também aporta *insights* interessantes sobre possíveis tendências. Em termos de geração das estratégias, nota-se que os países que estão na terceira geração têm presença

GRÁFICO 9 – TIPOS DE OBJETIVO, POR REGIÃO

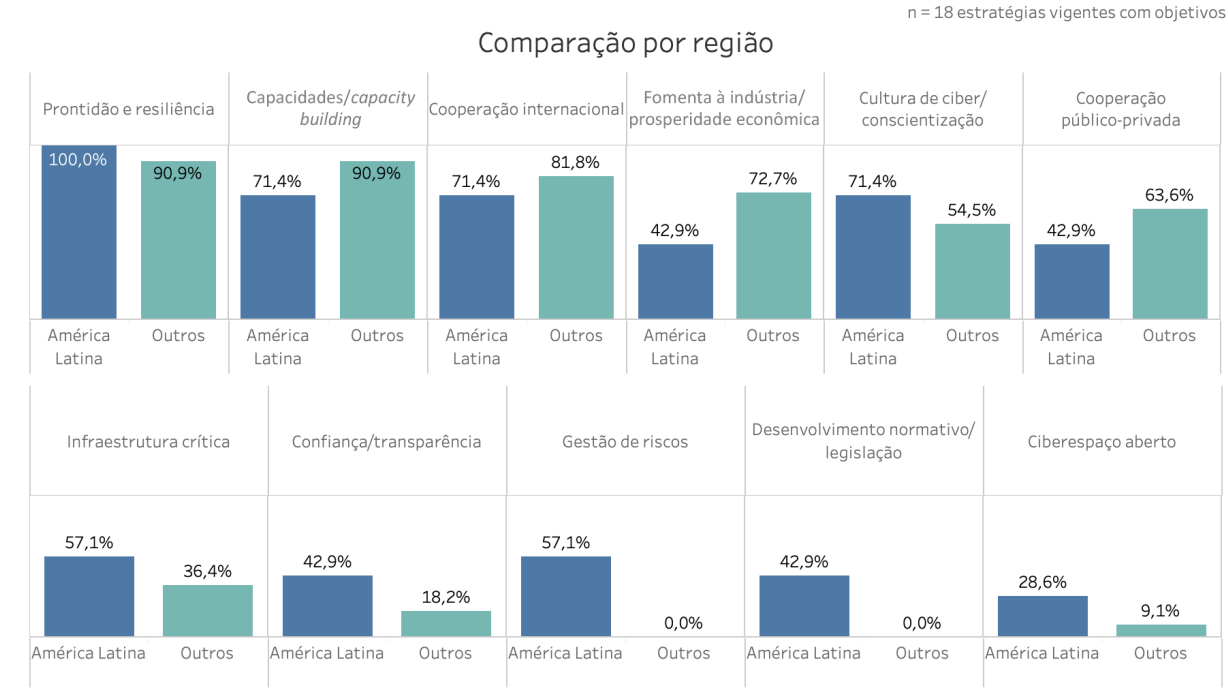
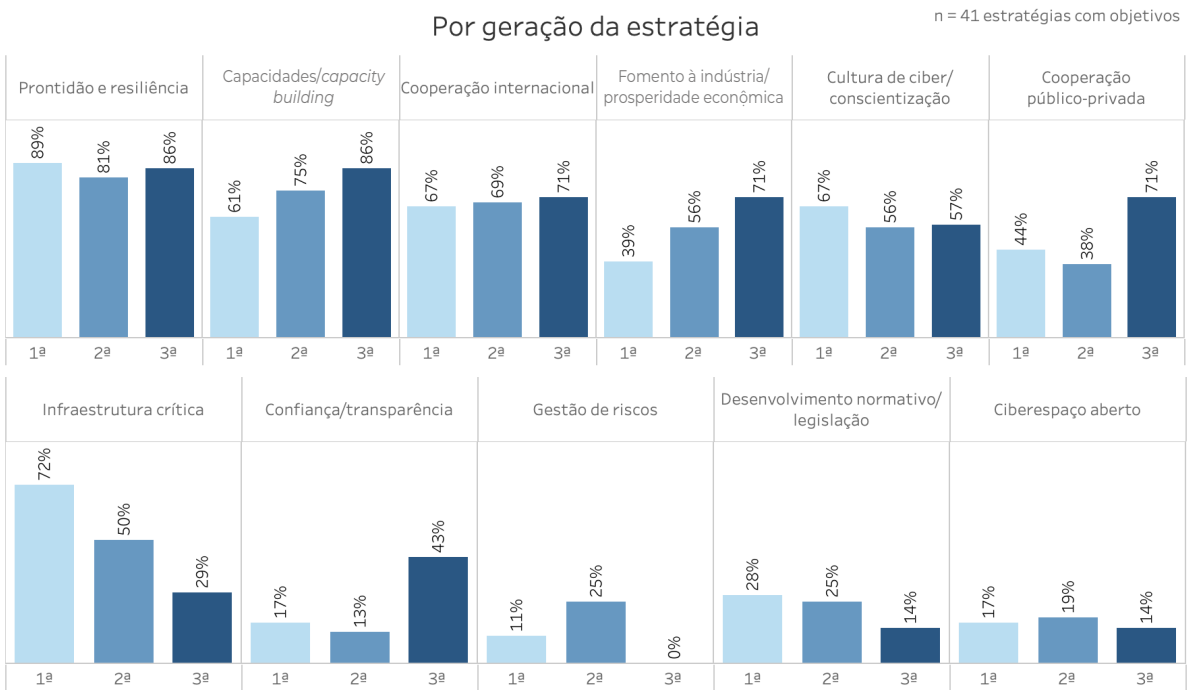


GRÁFICO 10 – EVOLUÇÃO DOS TIPOS DE OBJETIVOS



maior dos temas de prosperidade econômica, conforme já mencionado. Ademais, nota-se o crescimento do tema da cooperação público-privada, à medida que os países evoluem em suas estratégias. Também é possível apurar a redução na presença de objetivos de primeiro nível explicitamente centrados na proteção da infraestrutura crítica. Entende-se que essa diminuição pode ser explicada pelo fato de o tema da proteção da infraestrutura crítica passar a ser tratado de forma mais transversal e incluído em conceitos mais amplos como resiliência ou, inclusive, cooperação com o setor privado (esse tema será explorado na área focal de infraestrutura crítica).

Por fim, o aumento do tema da transparência, destacado na seção dos princípios, também está espelhado no aumento do tema como objetivos estratégicos, reforçando a tendência identificada de que as estratégias de cibersegurança levem aspectos de transparência e de aumento da confiança mais a sério.

Por não encontrar padrões interessantes na análise por ano para esse tópico, optou-se por não incluir o gráfico que compara os períodos. As tendências mais interessantes podem ser identificadas avaliando a evolução por geração.

Em relação aos números de macro objetivos, não foi identificado um padrão de aumento ou diminuição ao longo dos anos. A grande maioria das estratégias se concentra em quatro ou cinco pilares, objetivos estratégicos ou grandes áreas de atuação. Nos quadros a seguir, foram incluídos exemplos qualitativos de como os objetivos estratégicos são apresentados em três estratégias selecionadas:

QUADRO 5 – EXEMPLOS DE OBJETIVOS – ESTÔNIA 2019

OBJETIVO 1 – Sociedade digital sustentável

A Estônia é uma sociedade digital sustentável que conta com forte resiliência tecnológica e preparo para emergências.

OBJETIVO 2 – Setor de segurança cibernética, pesquisa e desenvolvimento

O setor de segurança cibernética da Estônia é forte, inovador, orientado para a pesquisa e competitivo globalmente, abrangendo todas as competências essenciais para o país.

OBJETIVO 3 – Contribuição internacional de destaque

A Estônia é um parceiro confiável e capaz na arena internacional.

OBJETIVO 4 – Sociedade com alfabetização cibernética

A Estônia é uma sociedade cibernética e garante a oferta de talentos suficiente e voltada para o futuro.

QUADRO 6 – EXEMPLO DE OBJETIVOS – ESTADOS UNIDOS 2023

I. Defender a infraestrutura crítica
II. Interromper e desmantelar os agentes de ameaças
III. Moldar as forças de mercado para impulsionar a segurança e a resiliência
IV. Investir em um futuro resiliente
V. Forjar parcerias internacionais para buscar objetivos compartilhados

QUADRO 7 – EXEMPLO DE OBJETIVOS – COREIA 2019

Garantir operações estáveis do estado: fortalecer a segurança e a resiliência da infraestrutura principal do país para permitir a operação contínua, apesar das ameaças cibernéticas.

Responder a ataques cibernéticos: fortalecer as capacidades de segurança para impedir ameaças cibernéticas, detectá-las e bloqueá-las rapidamente e responder a qualquer incidente prontamente.

Construir uma forte base de segurança cibernética: cultivar um ecossistema justo e autônomo, em que a tecnologia de segurança cibernética, os recursos humanos e os setores sejam competitivos.

5.7. Áreas focais de ação

Esta seção do estudo analisa as áreas de ação das estratégias, por meio dos temas incluídos em formatos de iniciativas, subobjetivos, linhas de ação, pilares de ação ou outras categorias similares presentes nos documentos. As áreas focais incluem sete categorias priorizadas no documento do ITU mencionado anteriormente e duas categorias adicionais. Dentro de cada área, diferentes temas e ações foram priorizados para avaliação.

5.7.1. *Área focal: gestão de riscos*

PONTOS-CHAVE DA SEÇÃO

- **Abordagem de gestão de riscos:** há uma tendência de aumento da inclusão de uma abordagem de gestão de riscos como parte das ações da estratégia, embora o detalhamento não inclua a definição de uma metodologia propriamente dita.

GRÁFICO 11 – ÁREA FOCAL: GESTÃO DE RISCOS

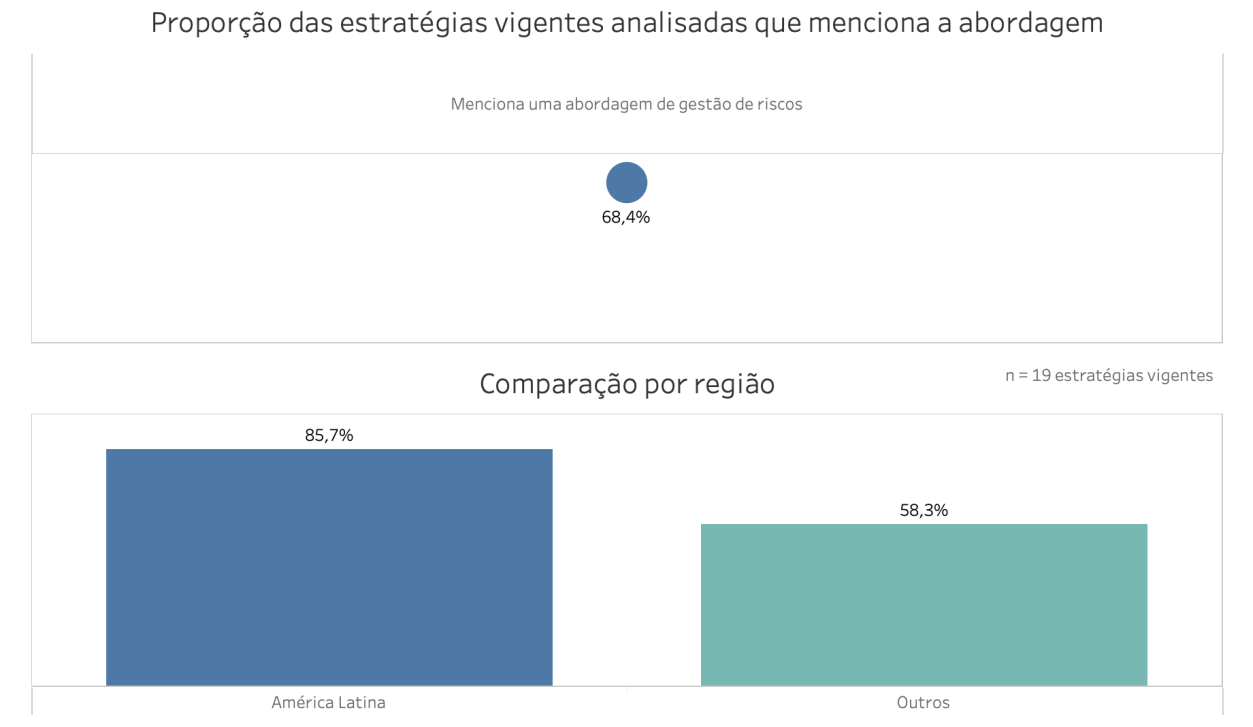
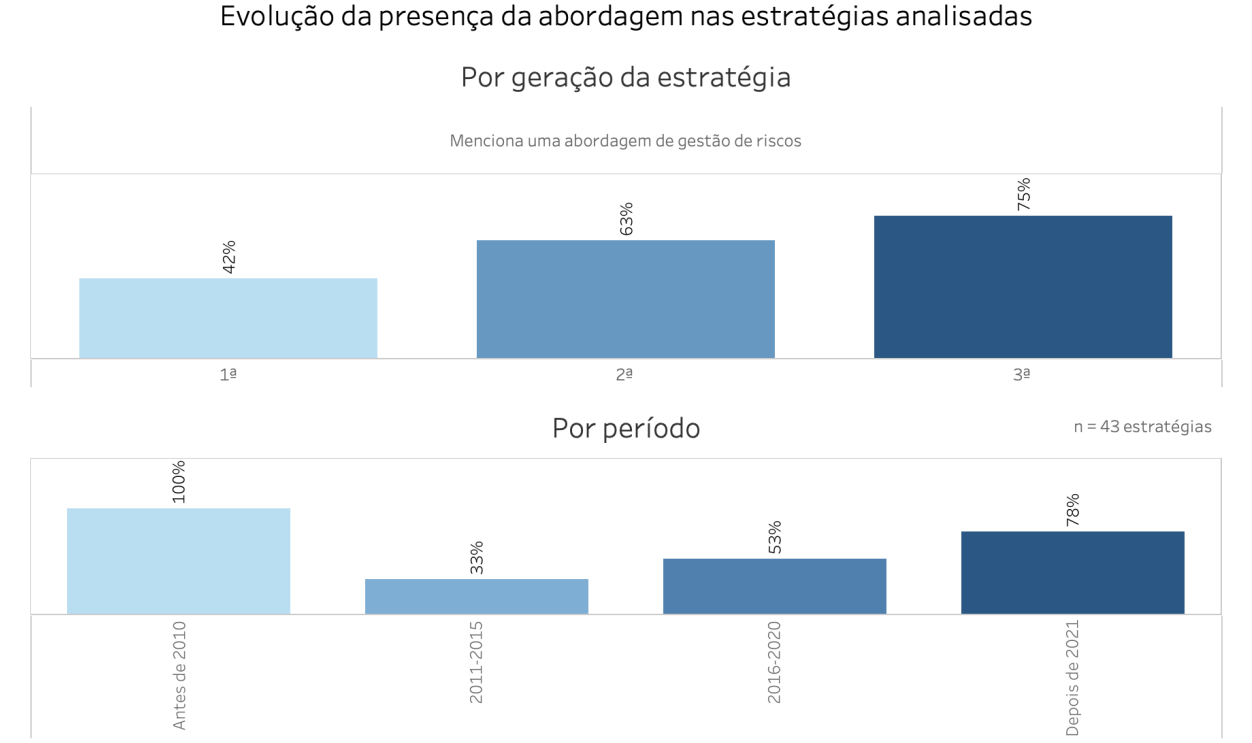


GRÁFICO 12 – EVOLUÇÃO DA ÁREA FOCAL: GESTÃO DE RISCOS



QUADRO 8 – QUADRO DE APROFUNDAMENTO DA ÁREA FOCAL

Gestão de riscos na Espanha

A Espanha é um exemplo em que há uma definição de gestão de riscos, uma metodologia de gestão e um conjunto de políticas e regulamentações que apoiam essa abordagem. Entretanto, a estratégia apenas detalha a iniciativa a ser promovida, sendo nesta (e não na estratégia em si) que todos os aspectos necessários para sua implementação são detalhados.

A definição da abordagem, da metodologia de gestão e das políticas de gestão de riscos são práticas excelentes a serem consideradas em uma estratégia em termos gerais, mas nem todas precisam ser incluídas no documento principal. Trata-se de um tópico amplo que requer um grande conjunto de definições e afeta vários atores. Além disso, também requer uma estrutura normativa para dar solidez e aplicabilidade. Dessa forma, a estratégia serve como uma ferramenta para impulsionar a sua promoção, mas não necessariamente para definir os detalhes técnicos.

Identificar, medir e avaliar os riscos dá ao governo a capacidade de gerenciá-los de forma eficaz. Em nível nacional, também é necessário definir uma metodologia comum e transversal que permita a avaliação e a comparação de cada um dos órgãos estatais, embora esta análise tenha identificado que essa definição costuma se dar em documentos complementares e não na própria estratégia.

Das estratégias estudadas, 68,4% das que estão em vigor definem uma abordagem de gestão de riscos. Esse valor aumenta para

85,7%, quando se consideram apenas as estratégias latino-americanas. Ao observar como esse tópico está presente nas estratégias de acordo com a geração ou o período, vê-se claro aumento, mostrando que esse é um aspecto que está sendo cada vez mais contemplado. Um exemplo é a estratégia da Colômbia, onde a gestão de riscos é incluída a partir da segunda edição de sua estratégia, mantendo sua importância na terceira edição.

Vale destacar que as estratégias que mencionam a necessidade de uma abordagem de gestão de riscos dificilmente entram no nível de detalhes técnicos ou operacionais, delegando essa função a outros documentos complementares. Por exemplo, estratégias como a da Espanha, não explicitam uma metodologia no documento da estratégia, mas contam com um método implementado em nível nacional, podendo indicar a tendência de que as estratégias não entrem no detalhe técnico tão aprofundado.

5.7.2. *Área focal: resiliência e prontidão*

PONTOS-CHAVE DA SEÇÃO

- **Capacidades de resposta a incidentes:** todas as estratégias abordam esse tópico, mesmo em diferentes gerações do mesmo país, abrangendo diferentes questões.
- **Compartilhamento de informações:** o compartilhamento de informações é uma capacidade essencial na área de segurança cibernética, sendo um requisito fundamental para gerar conhecimento, melhorar as capacidades em cibersegurança e fortalecer os laços entre os diferentes atores envolvidos na proteção de um país. Esse tópico está presente em 84,2% das estratégias vigentes e tem uma trajetória de crescimento ao longo das gerações.

Como será visto em todos os tópicos dessa área focal, a proteção e a resiliência têm grande destaque em todas as estratégias, especialmente nas atuais. Há várias iniciativas que buscam melhorar a proteção e a resiliência de forma transversal. Um exemplo disso é a Lei de Resiliência Cibernética da União Europeia,[17] que busca estabelecer requisitos de segurança cibernética para produtos com elementos digitais. Outro exemplo é a Lei de Resiliência Operacional Digital da UE,[18] que busca regulamentar e unificar a legislação para a gestão de riscos digitais no setor financeiro.

A capacidade de resposta a incidentes é um tópico de interesse para todos os países, sendo possível ver como ela aparece explicitamente em todas as estratégias vigentes. Diferentemente de outros tópicos, o tema da capacidade de resposta está presente em todas as gerações de estratégias em uma grande porcentagem porque, à medida que os países melhoram suas capacidades em alguns aspectos, devido ao dinamismo das ameaças, são gerados novos desafios que devem ser abordados por meio de novos objetivos. Tomando a República Dominicana como exemplo, em sua primeira estratégia, as principais linhas de ação para melhorar a capacidade de resposta a incidentes estavam relacionadas à promoção das melhores práticas, à criação de um centro nacional de resposta a incidentes e ao desenvolvimento de Grupos de Resposta a Incidentes de Segurança (CSIRT) setoriais. Na segunda geração de sua estratégia, o objetivo continua o mesmo, mas as linhas de ação estão mais relacionadas ao desenvolvimento de planos de resposta, ao fortalecimento das estruturas organizacionais já existentes e à coordenação e troca de informações.

[17] Cyber Resilience Act – https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
[18] Digital Operational Resilience Act - https://www.digital-operational-resilience-act.com/.

GRÁFICO 13 – ÁREA FOCAL: PRONTIDÃO E RESILIÊNCIA

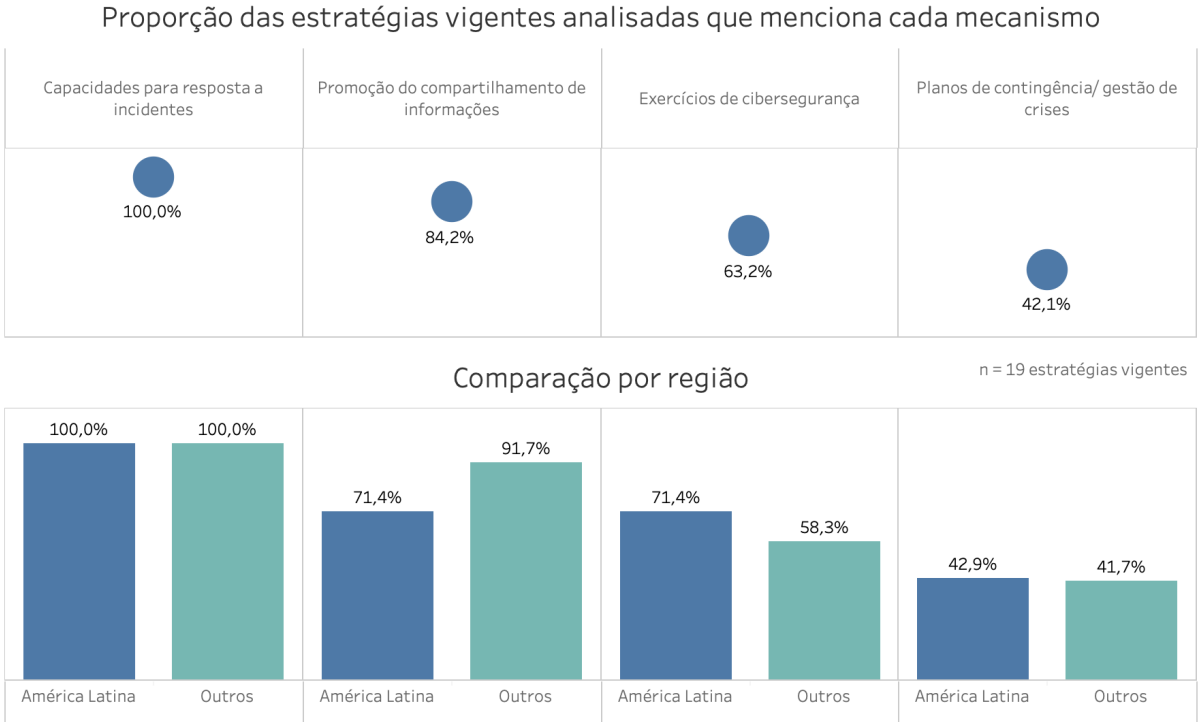
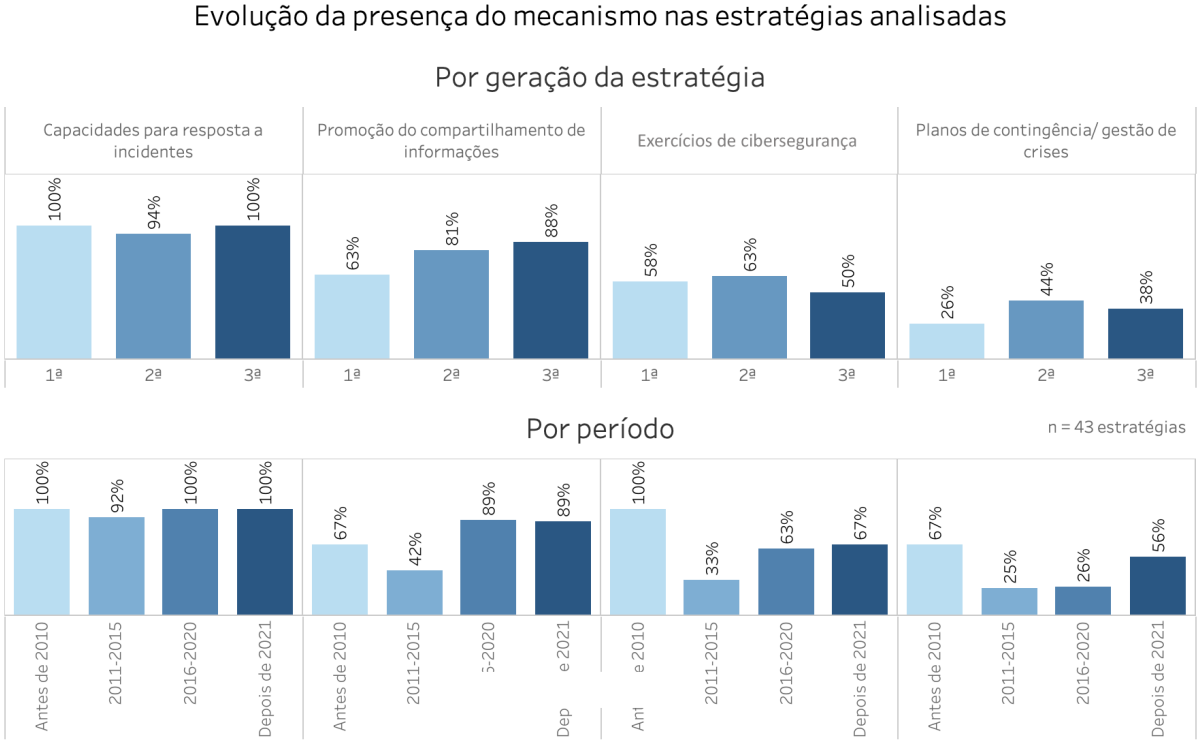


GRÁFICO 14 – EVOLUÇÃO DA ÁREA FOCAL: PRONTIDÃO E RESILIÊNCIA



Como se sabe, as ameaças existentes no espaço cibernético não têm fronteiras, assim como os grupos criminosos organizados que operam nele. Um insumo fundamental na preparação para as ameaças atuais e emergentes é o conhecimento. Saber quais são as ameaças ativas, quais são as tendências e quais dados técnicos podem enriquecer e fortalecer a capacidade de detectar incidentes e responder a eles são aspectos que devem estar presentes nas estratégias de segurança cibernética. Esse conhecimento deve ser gerado e compartilhado em nível nacional e internacional, buscando estabelecer vínculos bidirecionais capazes de nutrir todas as partes. A observação dos dados deste estudo em relação a essa questão mostra que 84,2% das estratégias atuais promovem o compartilhamento de informações, uma tendência que vem aumentando constantemente ao longo das gerações. Os Estados Unidos, em sua estratégia mais recente, estabelecem como objetivo estratégico "Aumentar a velocidade e a escala do compartilhamento de informações e da notificação de vítimas", o que é apoiado pelo Centro de Integração de Inteligência contra Ameaças Cibernéticas,[19] entre outras entidades.

Conforme declarado na área focal capacidades e conscientização, a capacitação em segurança cibernética é uma constante em praticamente todas as estratégias. Não é de surpreender que, de acordo com o ISC2, em seu relatório Cybersecurity Workforce Study[20] (Estudo da força de trabalho de segurança cibernética), haja uma estimativa de 3,4 milhões de empregos de segurança cibernética não preenchidos. Uma maneira de desenvolver habilidades de segurança cibernética é por meio de exercícios, que buscam expor os envolvidos em cenários de crise. O principal objetivo é adquirir experiência e estar preparado para gerenciar crises da melhor maneira possível. Existem vários tipos de exercícios, orientados para diferentes públicos, conforme os exemplos a seguir:

- exercícios orientados às equipes técnicas: simulam-se a infraestrutura de uma organização (da forma mais realista possível) e também os cenários, de forma controlada, em que as equipes técnicas enfrentam diferentes tipos de incidentes. Nessa simulação, as equipes devem detectar, conter e atenuar as ameaças da mesma forma que fariam em um cenário real;
- exercícios orientados aos tomadores de decisão: para simular incidentes que envolvam os tomadores de decisão de uma organização, em nível nacional ou internacional, os *Table Top Exercises* são usados com frequência. Trata-se de cenários falados que simulam incidentes, nos quais todos os envolvidos devem tomar decisões que afetem a situação e o resultado final do incidente.

Das estratégias atuais, 63,2% levam em conta esse tipo de exercício, em maior ou menor grau.

Na área focal de proteção e resiliência, o tópico menos presente nas estratégias é o estabelecimento de um plano de contingência para o gerenciamento de crises. Ao se observar as estratégias atuais, apenas 42,1% delas fazem menção direta ao tópico; no entanto, pode-se ver que esse valor aumenta nas estratégias publicadas mais recentemente. De acordo

[19] Cyber Threat Intelligence Integration Center – https://www.dni.gov/index.php/ctiic-home.

[20] ISC2 Cybersecurity Workforce Study – https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196.

com a ITU, "A estratégia deve exigir o desenvolvimento de um plano nacional de contingência para emergências e crises de segurança cibernética. O plano deve fazer parte do plano de contingência nacional geral ou estar alinhado a ele".

QUADRO 9 – ESTUDO DE CASO

ESTRATÉGIAS DE CIBERSEGURANÇA NA COLÔMBIA

A Colômbia é o primeiro país da região a ter uma estratégia de segurança cibernética (a primeira foi publicada em 2011) e o único país da América Latina a ter publicado três versões. Todas as suas estratégias abordam questões de segurança cibernética e estão fortemente relacionadas à defesa cibernética, uma característica não muito comum nas estratégias analisadas neste estudo. Um aspecto muito interessante é a inclusão, tanto na segunda quanto na terceira edição, das lições aprendidas e como elas influenciam os objetivos.

Em sua primeira edição da estratégia, a Colômbia considerava que os principais desafios eram os pontos fracos na capacidade do Estado de lidar com as ameaças, na época (muitos permanecem até hoje), a falta de coordenação das iniciativas e operações de segurança e defesa cibernéticas, bem como as deficiências nos aspectos legais e regulatórios. Para resolver esses problemas, os principais objetivos estavam relacionados: (i) à implementação de órgãos para prevenir, coordenar e controlar possíveis ameaças contra o Estado, destacando a criação de uma estrutura organizacional para coordenar e responder a incidentes; (ii) a oferecer treinamento especializado em segurança e defesa cibernéticas; e (iii) a fortalecer aspectos da legislação e da adesão a instrumentos internacionais.

Para sua segunda edição (lançada em 2016), a Colômbia analisou as ações promovidas pela primeira estratégia e a situação da segurança cibernética naquele momento, concluindo que havia aspectos a serem considerados que não haviam sido abordados na primeira versão. Um desses aspectos era a gestão de riscos, que assume um papel de destaque nos novos objetivos. Assim, a segunda estratégia se concentrou em quatro princípios: salvaguardar os direitos humanos e os valores fundamentais dos cidadãos, adotar uma abordagem inclusiva e colaborativa, garantir a responsabilidade compartilhada entre todas as partes e adotar uma abordagem de gestão de riscos.

Na terceira (lançada em 2020) e última edição, assim como na segunda edição, a Colômbia analisa os aspectos que foram deixados de fora das estratégias anteriores. A partir dessa análise, a confiança e a segurança digital como ferramenta para fortalecer a inclusão da sociedade e aumentar a competitividade da Colômbia em aspectos digitais surge como um conceito novo e fundamental. Com isso em mente, o primeiro objetivo é fortalecer as capacidades de segurança digital dos cidadãos, do setor público e do setor privado. Em segundo lugar, atualizar a estrutura de governança para a segurança digital.

A Colômbia é um excelente exemplo de como as lições aprendidas com uma estratégia são insumo fundamental para o desenvolvimento da próxima estratégia, seguindo assim um processo evolutivo que leva em conta tanto os aspectos que ficaram pendentes quanto aqueles que estão se tornando mais importantes.

5.7.3. *Área focal: infraestrutura crítica (IC) e serviços essenciais*

PONTOS-CHAVE DA SEÇÃO

- **Medidas para proteger as ICs:** este é um tópico que está presente na maioria das estratégias (89,5% das que estão em vigor).
- **Setor privado:** o setor privado geralmente está muito envolvido no gerenciamento de infraestruturas críticas, e é importante abordar a cooperação com o setor privado na estratégia. Pode-se ver que, ao longo dos anos, as estratégias mencionaram esse aspecto com mais frequência.
- **Ativos de governo digital:** observa-se o aumento desse tópico nas estratégias por ano, possivelmente devido à preocupação em proteger os ativos de governo digital para continuar a digitalização dos serviços.
- **Identificação de infraestruturas críticas:** a identificação das infraestruturas críticas é fundamental para estabelecer um plano de proteção. A análise mostra que as estratégias dos países em estágios mais iniciais costumam se preocupar com a identificação em maior frequência.
- **Serviços essenciais:** especialmente nas estratégias mais recentes do Norte global, nota-se o aumento do conceito de serviços essenciais (seja em substituição, seja em complementaridade ao conceito de infraestruturas críticas).

A proteção de infraestruturas críticas é uma preocupação compartilhada por todos os países. Com efeito, 100% das estratégias analisadas, em sua primeira edição, têm o objetivo de estabelecer medidas para sua proteção. Isso não surpreende, pois esses ataques são vistos há décadas, desde 2010, quando um *malware* afetou uma fábrica iraniana,[21] até mais recentemente (2021), quando a infraestrutura de suporte a gasodutos nos Estados Unidos foi comprometida por um *ransomware*.[22]

De acordo com a Diretiva Europeia 2008/114/EC, de 8 de dezembro de 2008,[23] a infraestrutura crítica é definida como "um elemento, sistema ou parte dele localizado nos estados-membros, que é essencial para a manutenção de funções vitais da sociedade, saúde, segurança, proteção, bem-estar social e econômico da população, cuja interrupção ou destruição afetaria seriamente a capacidade de um estado-membro de manter essas funções". Quanto aos serviços essenciais, a ITU os define como "serviços que são essenciais para atividades socioeconômicas indispensáveis".

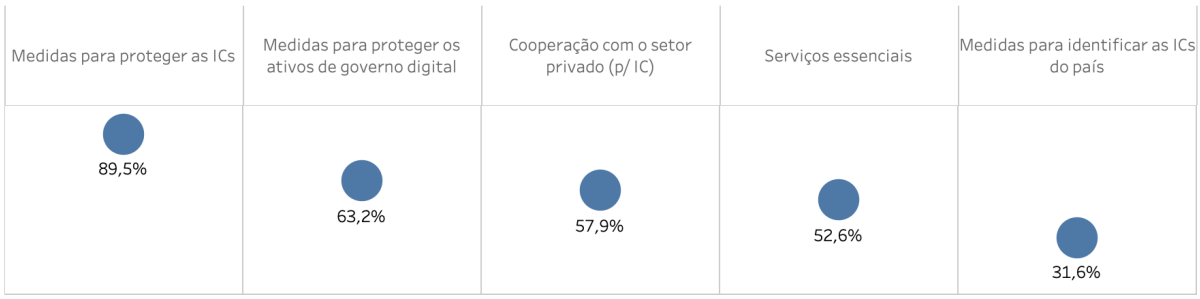
Entre os tópicos dessa área focal, o estabelecimento de medidas para proteger a IC está presente em 89,5% das estratégias vigentes. Da mesma forma, pode-se observar que, à medida que os países publicam novas edições de suas estratégias, esse tópico tem presença cada vez menor, partindo de 100%, nas de primeira geração, e chegando a 75% nas de terceira. Isso pode ser devido ao fato de que, embora ainda seja um aspecto importante, os países conseguiram aumentar suficientemente a proteção de suas infraestruturas críticas e preferiram se concentrar em outros aspectos. Também se nota a mudança de nomenclatura para "serviços essenciais". Na primeira geração, apenas 32% mencionavam o termo comparado com 50% nas de terceira geração.

A cooperação com o setor privado está presente em várias áreas focais da maioria das

[21] Stuxnet case – https://www.bbc.com/news/world-middle-east-11414483.
[22] CISA – The Attack on Colonial Pipeline - https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
[23] DIRECTIVA 2008/114/CE – https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf.

GRÁFICO 15 – ÁREA FOCAL: INFRAESTRUTURA CRÍTICA (IC) E SERVIÇOS ESSENCIAIS

Proporção das estratégias vigentes analisadas que menciona cada mecanismo



Comparação por região

n = 19 estratégias vigentes

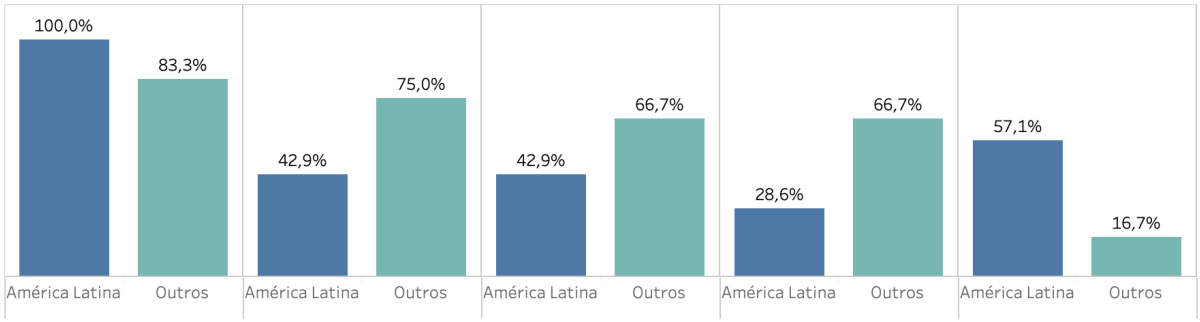
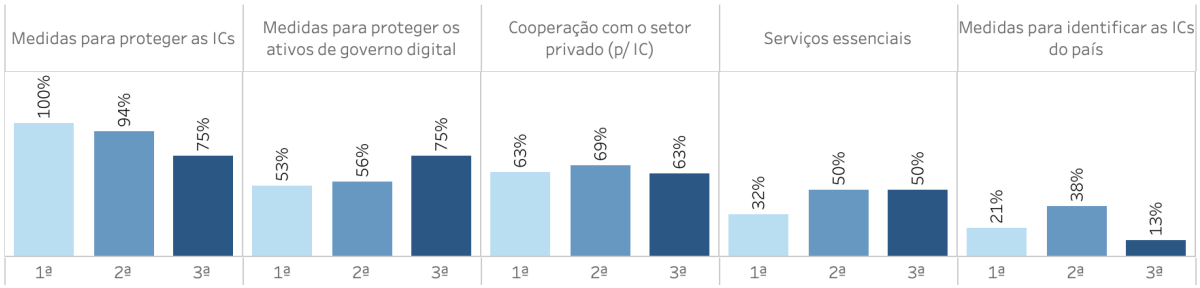


GRÁFICO 16 – EVOLUÇÃO DA ÁREA FOCAL: INFRAESTRUTURA CRÍTICA (IC) E SERVIÇOS ESSENCIAIS

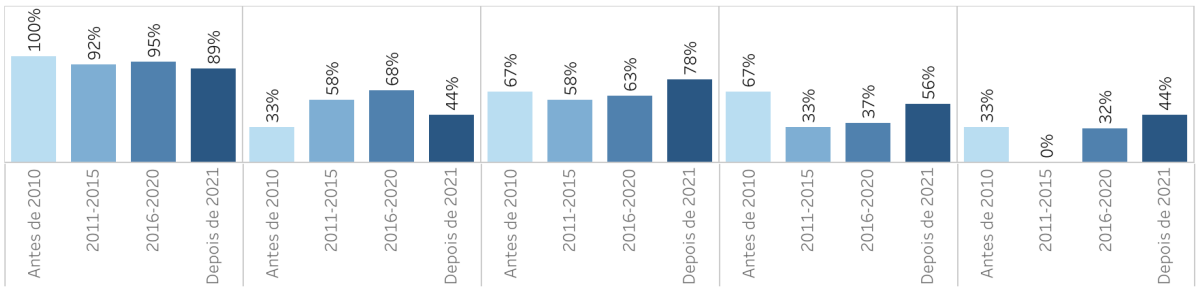
Evolução da presença do mecanismo nas estratégias analisadas

Por geração da estratégia



Por período

n = 43 estratégias



estratégias modernas, e essa não é uma exceção. Considerando que, na maioria dos países, as infraestruturas críticas são gerenciadas por empresas privadas, é natural que o tópico cooperação com o setor privado para infraestruturas críticas esteja constantemente presente. Por exemplo, em sua terceira estratégia, o Japão declara como atividade "Avançar na proteção de infraestruturas críticas com base em parcerias público-privadas", na qual detalha: "Para o fornecimento seguro e contínuo de serviços de infraestruturas críticas, que formam a base da vida das pessoas e das atividades socioeconômicas, os setores público e privado compartilharão uma política comum entre o governo nacional, que assume a responsabilidade pela proteção de infraestruturas críticas, e os operadores de infraestruturas críticas, que realizam a proteção de infraestruturas críticas de forma independente".

Com relação às "medidas para a proteger os ativos de governo digitais", nota-se a presença moderada nas estratégias latino-americanas, com 42,9%, e maior nas outras, com 75%. Observa-se uma tendência de aumento do tema, à medida que aumentam as gerações, com pico entre os anos 2016 a 2020, possivelmente coincidindo com a rápida evolução da digitalização dos serviços públicos. Isso pode indicar que a preocupação com a proteção dos ativos digitais do governo aumenta, à medida que os Estados aumentam sua digitalização, pois mais serviços são expostos e se tornam cada vez mais importantes.

O último tópico "medidas para identificar as infraestruturas críticas do país" está claramente mais presente na América Latina, com 57,1%, em comparação com outros países, com apenas 16,7%. Esse ponto é fundamental no início da abordagem da proteção da infraestrutura crítica. É evidente que, depois de identificá-las, esse não é mais um objetivo prioritário. Talvez seja por isso que apenas 13% das estratégias o abordem em sua terceira edição.

5.7.4. *Área focal: capacidades e conscientização*

PONTOS-CHAVE DA SEÇÃO

- **Capacidades e conscientização:** a necessidade de fortalecer as capacidades em cibersegurança no país é uma constante em praticamente todas as estratégias.
- **Medidas mais frequentes:** entre os três tópicos sobre capacidades mais mencionados nas estratégias, destacam-se: inovação e pesquisa e desenvolvimento (94,7%); programas de conscientização (94,7%); e medidas para formar profissionais (89,5%).
- **Diversidade:** nota-se a tendência crescente a incluir nas estratégias medidas para aumentar a diversidade da força de trabalho no campo da cibersegurança (gênero, entre outras brechas).

A necessidade de fortalecer as capacidades de cibersegurança é uma constante em praticamente todas as estratégias, sendo um elemento presente no cerne dos documentos. O que varia entre as estratégias analisadas é o enfoque e a ênfase atribuídos às diferentes dimensões do tema.

Entre os cinco tópicos mais mencionados nas estratégias relacionados a esse assunto, destacam-se: inovação e pesquisa e desenvolvimento, programas de conscientização, medidas na educação superior, medidas para a formação de profissionais e medidas para aumentar as capacidades em cibersegurança dos servidores públicos.

É notável que esses tipos de medidas têm objetivos distintos. Algumas concentram-se na escassez de profissionais e mão de obra especializada em cibersegurança, procurando estimular a oferta de especialistas qualificados na área. Outras se voltam para o usuário final, com

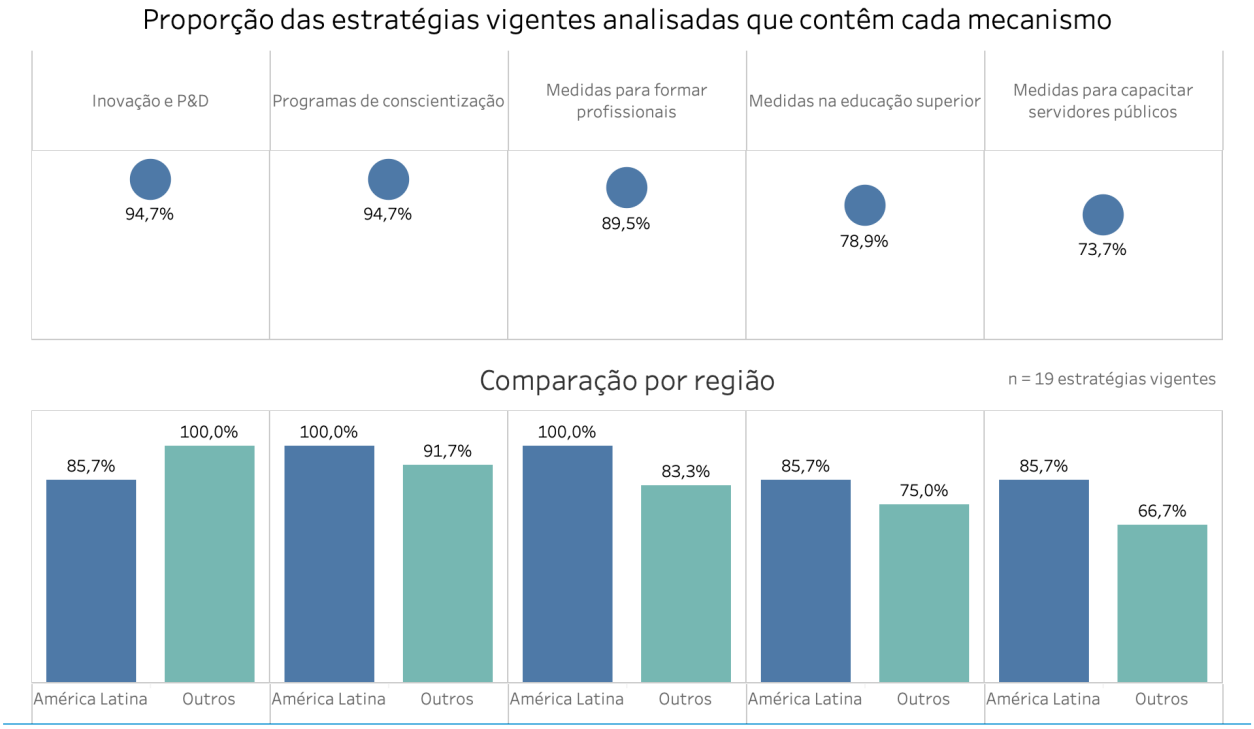
o intuito de aumentar a conscientização sobre questões de cibersegurança entre a população em geral. Na prática, a maioria das estratégias adota uma abordagem híbrida, que reconhece a importância tanto de contar com especialistas altamente qualificados quanto de educar o público em geral para melhor compreender os desafios e as práticas seguras no ambiente digital. Esse equilíbrio reflete uma visão holística para fortalecer as capacidades de cibersegurança em um contexto nacional.

O Gráfico 17 ilustra que 94,7% das estratégias analisadas possui iniciativas ou subobjetivos relacionados ao fomento da inovação e da pesquisa e desenvolvimento no tema de cibersegurança. Alguns exemplos de como essas iniciativas aparecem são:

- preparar um plano nacional de pesquisa e desenvolvimento em segurança cibernética que defina áreas prioritárias para o Estado (Estônia, 2019);
- promover e aprimorar as capacidades tecnológicas necessárias para ter soluções confiáveis que possam proteger adequadamente os sistemas contra diferentes ameaças, incentivando as atividades de pesquisa, desenvolvimento e inovação (P&D&I) nos níveis público e privado (Argentina, 2019);
- promover a produção científica, o desenvolvimento e a inovação nos vários domínios da segurança do ciberespaço, tendo como objetivo manter e afirmar a independência nacional nesse domínio (Portugal, 2019).

Em relação às medidas de conscientização, também com presença em 94,7% das estratégias vigentes, se apresentam alguns exemplos ilustrativos para materializar o tema:

GRÁFICO 17 – ÁREA FOCAL: CAPACIDADES E CONSCIENTIZAÇÃO



- criar um programa nacional de conscientização sobre segurança no espaço cibernético, abrangendo a sociedade como um todo (Argentina, 2019);
- realizar atividades de conscientização voltadas para o público em geral (Estônia, 2019);
- estabelecer uma política para o desenvolvimento de competências digitais na população, com ênfase na segurança cibernética, incluindo programas de educação, treinamento técnico, programas de sensibilização e conscientização para obter um espaço cibernético mais seguro (República Dominicana, 2022).

O Gráfico 18 apresenta mais cinco temas recorrentes nas ações relacionadas aos temas de capacidades, em especial nas medidas ligadas ao desenvolvimento da indústria e medidas para aumentar a diversidade da força de trabalho.

Em relação à análise evolutiva no tempo (Gráficos 19 e 20), uma das tendências encontradas é o crescimento das medidas destinadas à educação primária/secundária a partir de 2016, refletindo o esforço para aumentar a conscientização das novas gerações sobre práticas seguras no ambiente virtual. Em paralelo, observa-se, também, a partir de 2016, o aumento das iniciativas de formação profissional, em resposta ao desafio da escassez de profissionais qualificados no mercado de cibersegurança. Além disso, ao longo dos anos, a proporção de estratégias com iniciativas de inovação e pesquisa e desenvolvimento, próximo dos 88–89%.

A análise comparada também permite aferir a tendência a incluir com mais frequência medidas para o desenvolvimento da indústria, especialmente com o objetivo de aumentar a soberania (passa de 42%, na primeira geração das estratégias, para 75% na última).

GRÁFICO 18 – ÁREA FOCAL: CAPACIDADES E CONSCIENTIZAÇÃO (CONT.)

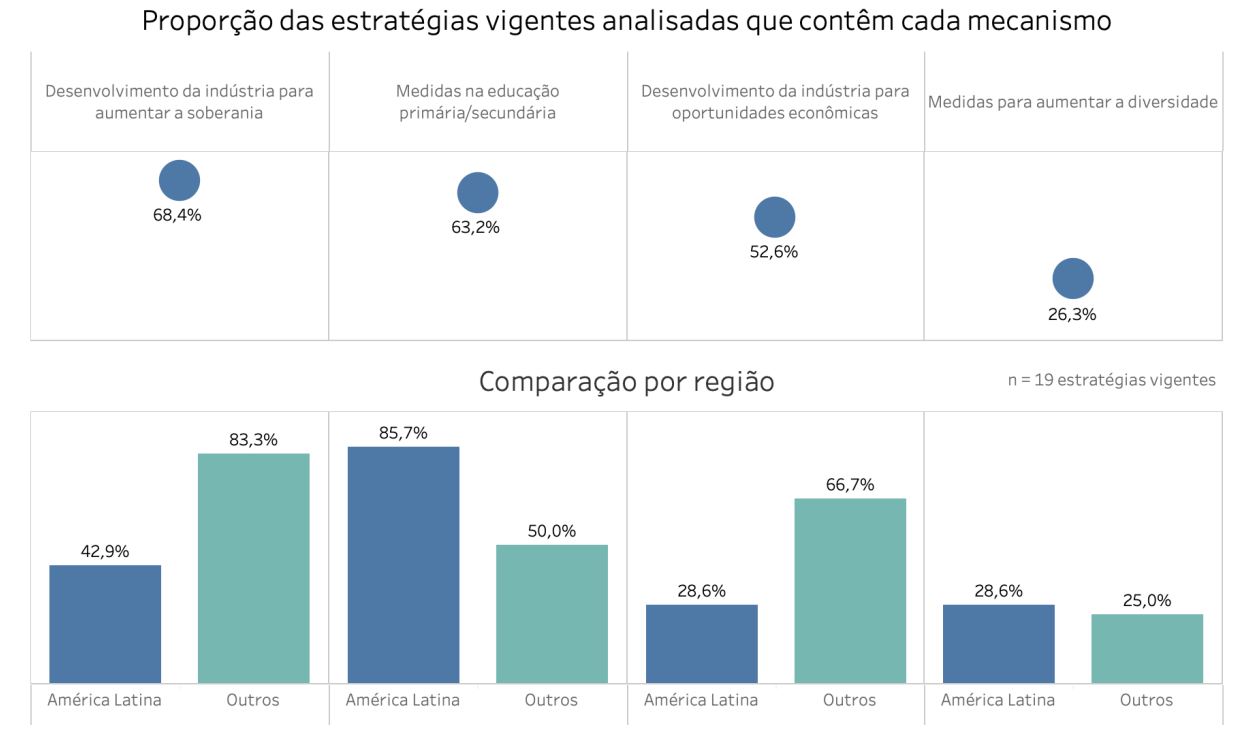


GRÁFICO 19 – EVOLUÇÃO DA ÁREA FOCAL: CAPACIDADES E CONSCIENTIZAÇÃO

Evolução da presença dos mecanismos nas estratégias analisadas

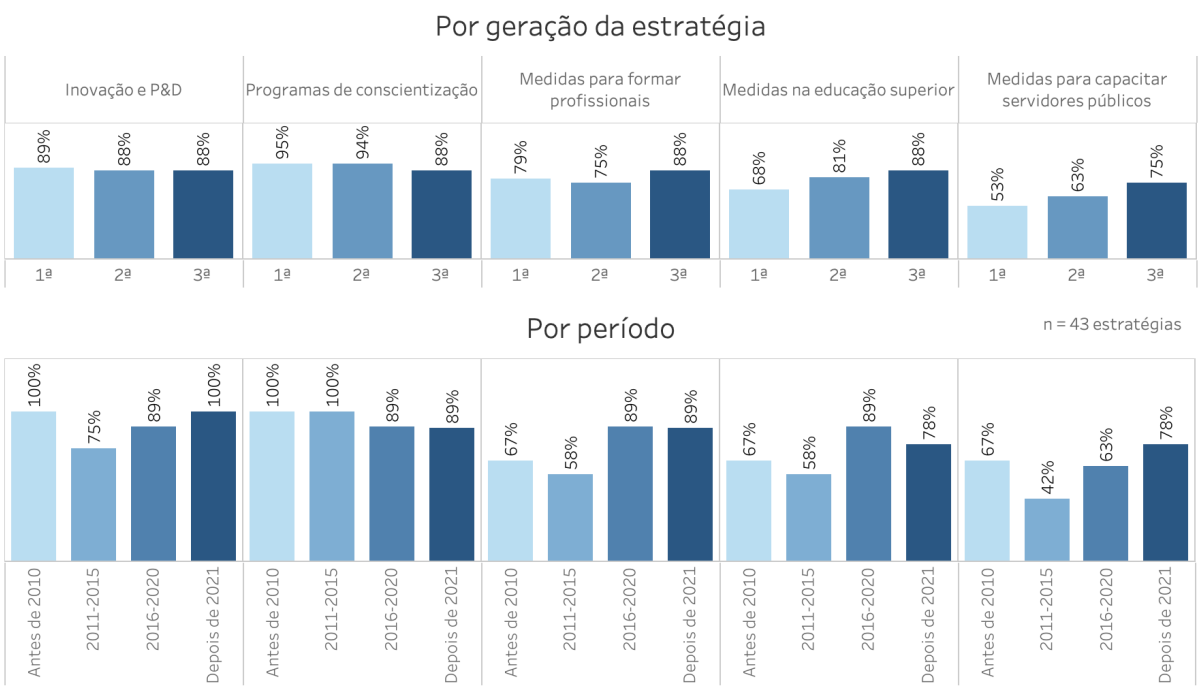
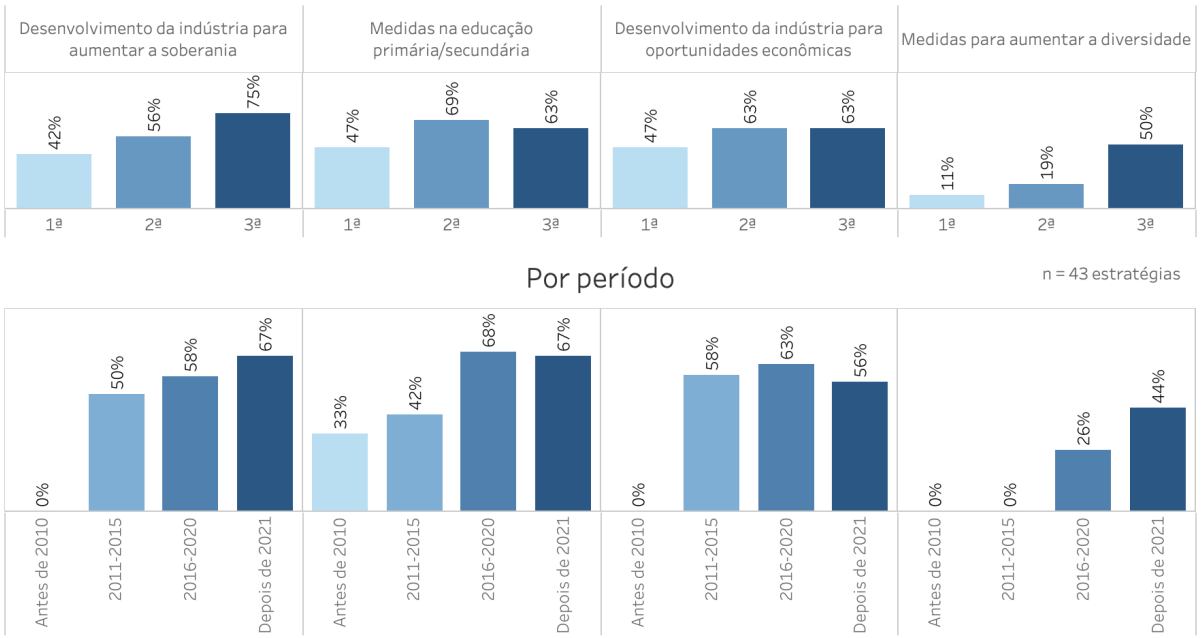


GRÁFICO 20 – EVOLUÇÃO DA ÁREA FOCAL: CAPACIDADES E CONSCIENTIZAÇÃO (CONT.)

Evolução da presença dos mecanismos nas estratégias analisadas



Por fim, embora ainda incipiente nas estratégias, uma tendência notável é a crescente preocupação com a diversidade no campo de cibersegurança. Embora esse tema fosse praticamente inexistente em gerações anteriores, nas estratégias de terceira geração, medidas desse tipo foram mencionadas em 50% das estratégias analisadas na amostra. Isso sugere mudança de mentalidade, com o reconhecimento crescente da importância de promover a inclusão e a diversidade no setor de cibersegurança. Dois exemplos (tradução dos autores) de como essas medidas são incluídas:

- será dada prioridade a uma série de ações concretas para aumentar a diversidade da força de trabalho cibernética. Não se trata apenas de garantir que esses empregos e carreiras sejam disponibilizados para todos, mas também de missão crítica para a segurança nacional, garantindo que sejam aproveitados o talento e as habilidades de toda a população (Reino Unido, 2022);
- essa estratégia abordará de frente a falta de diversidade na força de trabalho de cibersegurança. Os empregadores estão contratando a partir de um grupo muito pequeno de talentos e de redes profissionais que não são capazes de aproveitar toda a diversidade do país. Mulheres, pessoas pretas, profissionais e imigrantes de primeira geração, pessoas com deficiência e indivíduos LGBTQI+ estão entre as comunidades que estão sub-representadas no campo (Estados Unidos, 2023).

5.7.5. *Área focal: cooperação internacional*

Todas as estratégias, de alguma forma, mencionam o caráter global da cibersegurança e a necessidade de cooperação com outros países para atingir os resultados esperados. As estratégias, dependendo da maturidade e da geração, variam no escopo de qual papel é esperado do país na esfera internacional, em alguns casos, se limitando a garantir a participação nos fóruns internacionais enquanto, em outros, aspira ocupar uma posição de influência nesses fóruns.

Para além do eixo sobre a intensidade da participação, as estratégias também variam no enfoque dado ao tipo de atuação internacional. Em alguns casos, citam fóruns ou organizações internacionais específicas e, em outros, priorizam as relações bilaterais. No caso dos países da Europa, existe forte alinhamento com a atuação da União Europeia no tema.

Partindo das categorias do guia da ITU, nesta seção, analisa-se a frequência de duas categorias associadas à área focal da cooperação internacional:

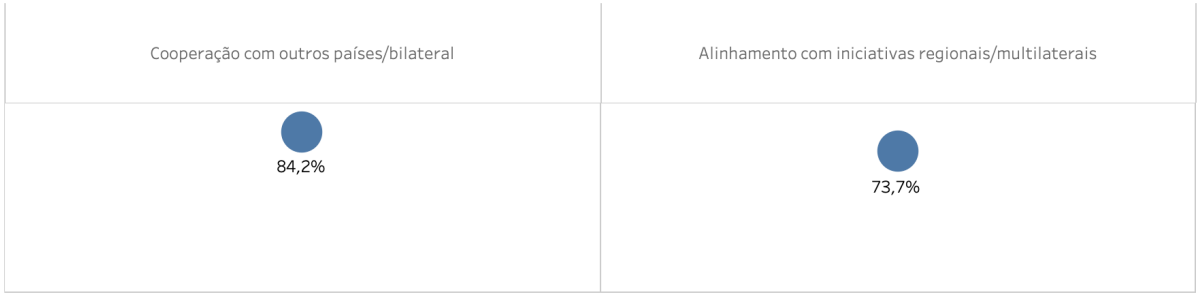
i. cooperação com outros países – nota-se que 91,7% das estratégias do Norte Global incluem medidas relacionadas a essa frente de trabalho;
ii. alinhamento com iniciativas regionais/multilaterais – 73,7% das estratégias vigentes analisadas citam a necessidade de atuar em blocos regionais ou multilaterais.

PONTOS-CHAVE DA SEÇÃO

- **Presença forte da cooperação internacional:** a cooperação com outros países na arena de cibersegurança é uma constante em todas as estratégias e se manteve presente ao longo do tempo e das gerações. A ênfase, às vezes, se encontra na atuação bilateral e, às vezes, multilateral.

GRÁFICO 21 – ÁREA FOCAL: COOPERAÇÃO INTERNACIONAL

Proporção das estratégias vigentes analisadas que contêm cada mecanismo



Comparação por região

n = 19 estratégias vigentes

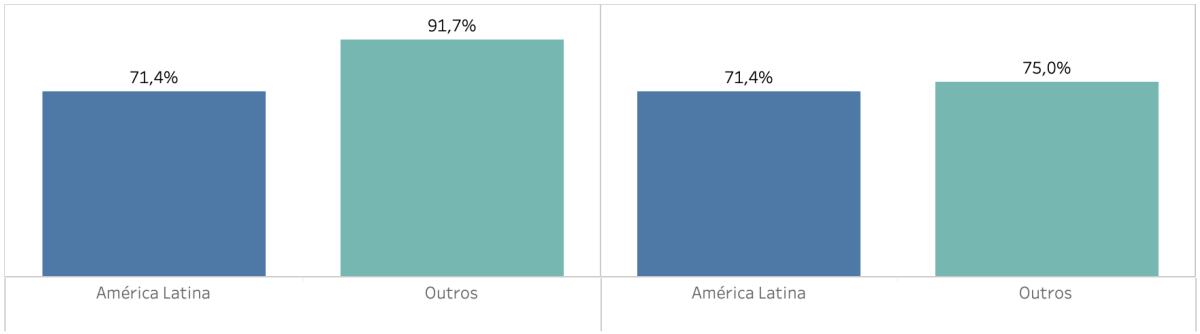
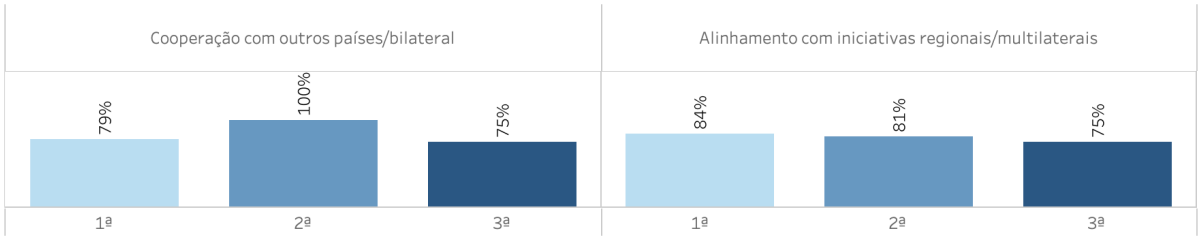


GRÁFICO 22 – EVOLUÇÃO DA ÁREA FOCAL: COOPERAÇÃO INTERNACIONAL

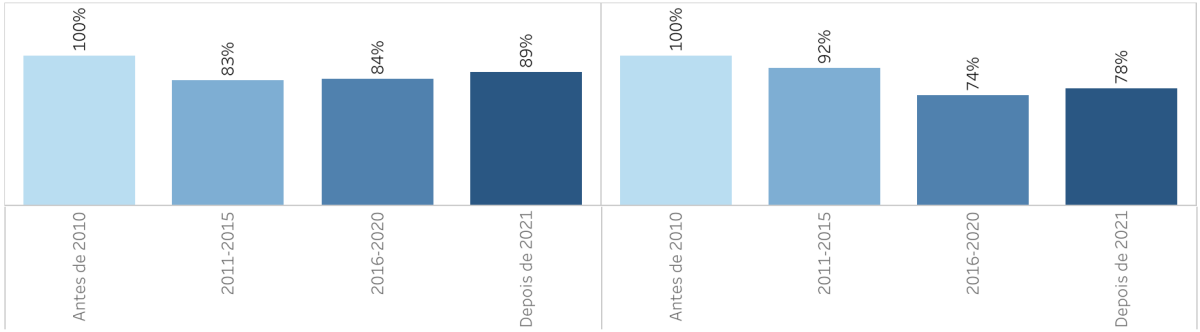
Evolução da presença dos mecanismos nas estratégias analisadas

Por geração da estratégia



Por período

n = 43 estratégias



5.7.6. *Área focal: legislação e marco normativo*

PONTOS-CHAVE DA SEÇÃO

- **Aprimoramento do marco normativo atual:** a grande maioria das estratégias vigentes analisadas (84,2%) têm alguma medida para aprimorar a estrutura normativa atual, pois é impossível obter melhorias substanciais sem uma estrutura regulatória que apoie as mudanças e lhes dê sustentabilidade ao longo do tempo.
- **Aplicação da lei:** a grande maioria das estratégias vigentes analisadas (84,2%) têm alguma medida para melhorar a a aplicação da lei nos temas de cibersegurança.
- **Legislação sobre crimes cibernéticos:** praticamente todos os países deste estudo assinaram a Convenção de Budapeste, o que torna necessário promover iniciativas relacionadas a crimes cibernéticos que estejam de acordo com ela. Especificamente, cerca de 42,1% mencionam, na sua estratégia, medidas relacionadas à legislação sobre cibercrime.

Essa área focal avalia os aspectos relacionados ao desenvolvimento de uma estrutura jurídica e regulatória, não apenas para proteger a sociedade contra o crime cibernético e promover um ambiente cibernético seguro, mas também como base para a realização dos objetivos almejados pela estratégia. Melhorias substanciais não podem ser alcançadas sem uma estrutura regulatória que apoie as mudanças e as torne sustentáveis ao longo do tempo.

GRÁFICO 23 – ÁREA FOCAL: LEGISLAÇÃO E MARCO NORMATIVO

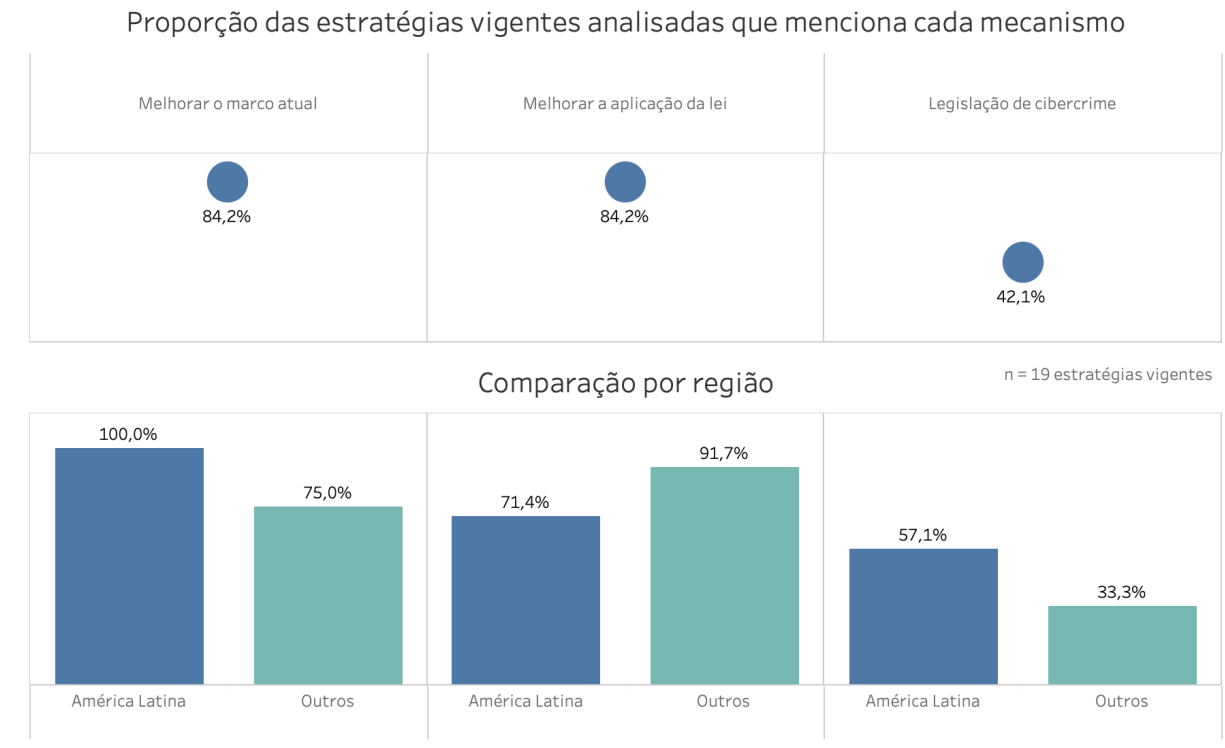
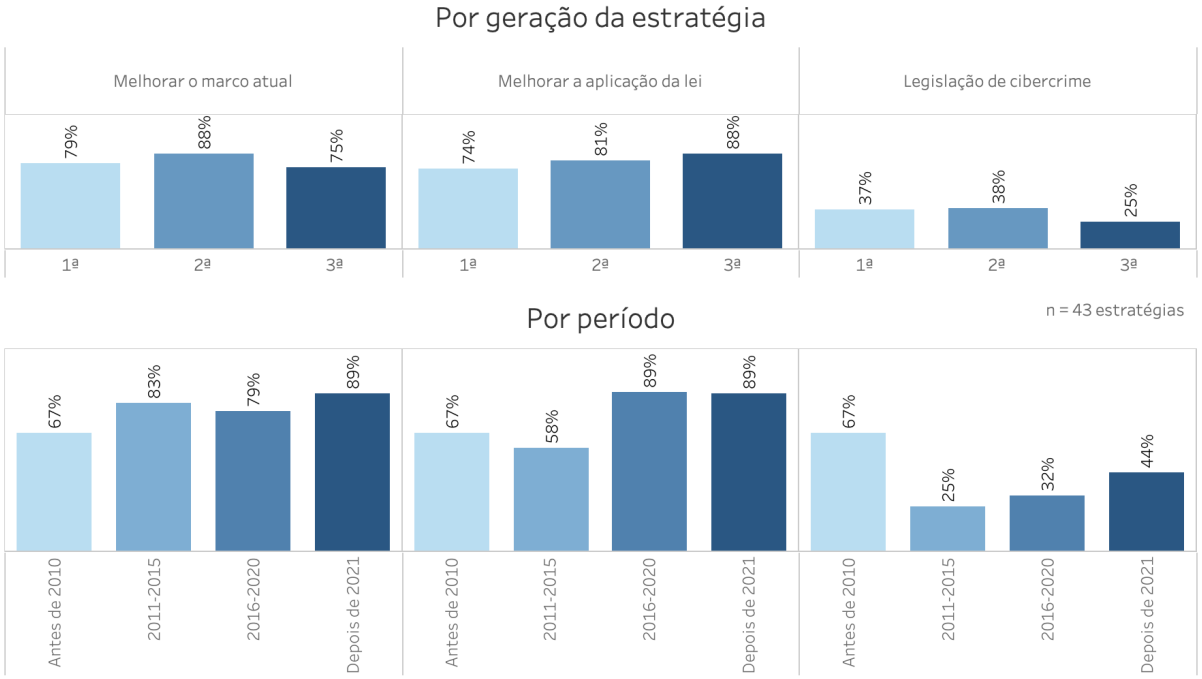


GRÁFICO 24 – EVOLUÇÃO DA ÁREA FOCAL: LEGISLAÇÃO E MARCO NORMATIVO

Evolução da presença do mecanismo nas estratégias analisadas



A importância de melhorar a estrutura regulatória é clara, tanto que 84,2% das estratégias em vigor mencionam esse tópico. Algo semelhante acontece quando se observa sua presença nas estratégias por geração, em que seu aparecimento é, em sua maioria, alto. É interessante ver como as estratégias abordam a melhoria da estrutura atual de diferentes maneiras e com diferentes escopos. Por exemplo, em sua terceira estratégia, o plano de ação da Colômbia, sob a atividade "Fortalecer as capacidades de segurança digital dos cidadãos, do setor público e do setor privado para aumentar a confiança digital no país", declara, no ponto dez, que "O Ministério da Justiça e do Direito, com o apoio do Ministério de Tecnologias da Informação e Comunicações, da Procuradoria Geral da República, do Ministério da Defesa Nacional, com o apoio das entidades públicas e privadas que considerem relevantes, diagnosticará e fará recomendações de soluções para os possíveis problemas existentes no marco regulatório atual que possam afetar (i) o exercício livre e pacífico da cidadania digital; (ii) a defesa e a segurança nacionais; e (iii) a persecução, investigação e punição do cometimento de condutas puníveis por meio do uso de Tecnologias da Informação e Comunicação (TICs)". Já a Argentina estabelece um objetivo (número 6) exclusivamente para o desenvolvimento de um marco regulatório, no qual busca "Gerar, adaptar, atualizar e adotar marcos regulatórios, normas e protocolos para enfrentar os desafios apresentados pelos riscos do espaço cibernético, garantindo o respeito aos direitos fundamentais".

A melhoria da aplicação da lei é um tópico presente em 84,2% das estratégias atuais. É interessante notar o aumento do tópico, no tempo e nas gerações, quando comparado com a diminuição no tempo e nas gerações no tópico da legislação de cibercrime, o que pode

mostrar que, no início, os países se concentram em fortalecer a legislação e, ao atingir esse objetivo, aumentam a aplicação da lei e fortalecem as forças de investigação e perseguição. A estratégia dos EUA se refere a esse tópico em várias ocasiões e o mostra como um esforço transversal, presente em vários dos objetivos, seja por meio de capacitação, das agências nacionais ou de acordos internacionais.

Quanto ao tópico da legislação sobre crimes cibernéticos, é notável sua baixa presença nas estratégias em vigor, sendo mencionado em apenas 42,1% delas. Também se observa a menção decrescente tanto por ano quanto por geração. Deve-se notar que praticamente todos os países deste estudo fazem parte da Convenção de Budapeste. Apenas a Nova Zelândia e a Coreia não são partes plenas, mas são convidadas a aderir, pois atualmente estão ausentes como observadores. Para aderir à Convenção de Budapeste, é necessário atender a uma série de requisitos, inclusive a necessidade de gerar uma legislação em conformidade com a convenção sobre crimes cibernéticos. É por isso que, embora o valor de presença desse tópico seja baixo, ele deve ser abordado em outro contexto, ou seja, na legislação sobre crimes cibernéticos.

5.7.7. *Área focal: privacidade e dados*

PONTOS-CHAVE DA SEÇÃO

- **Proteção de dados e privacidade:** embora não costume ser o cerne das estratégias, menções à proteção de dados e privacidade estão presentes em quase 80% das estratégias vigentes analisadas.
- ***Security by design*:** com clara tendência crescente, o conceito vem assumindo um papel protagonista rapidamente, estando presente em 67% das estratégias publicadas após 2020.

Na área focal da privacidade de dados, são abordados vários tópicos que, embora estejam relacionados entre si, apresentam grandes diferenças em sua abordagem, entre outras coisas porque alguns deles existem há muito tempo, como a propriedade intelectual, e outros foram criados na última década, como a privacidade por design. Em termos gerais, a proteção de dados teve um grande avanço nos últimos anos, muitos países legislaram sobre o assunto e foram definidas iniciativas que mudaram o paradigma de como os dados devem ser protegidos. O principal exemplo é a Regulamentação Geral de Proteção de Dados da UE,[24] que diz respeito à proteção de indivíduos com relação ao processamento de seus dados pessoais e à livre circulação desses dados dentro da UE e do Espaço Econômico Europeu, bem como à transferência de dados pessoais fora desses espaços. O principal objetivo é melhorar o controle e os direitos dos indivíduos sobre seus dados pessoais e simplificar o ambiente regulatório para os negócios internacionais.

Em relação à presente área focal, a Organização dos Estados Americanos, em sua publicação "Princípios atualizados sobre privacidade e proteção de dados pessoais",[25] estabelece 13 princípios que refletem as diferentes abordagens predominantes nos estados-membros sobre as questões centrais da proteção de dados pessoais, a saber:

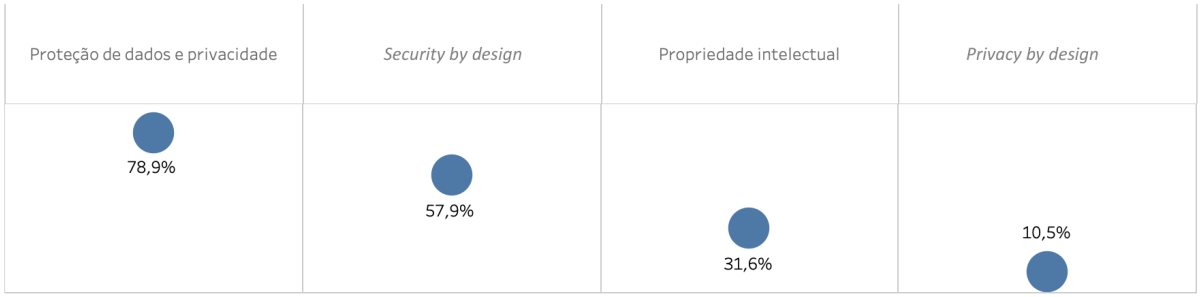
- objetivos legítimos e justiça;
- transparência e consentimento;
- relevância e necessidade;
- processamento e retenção limitados;
- confidencialidade;
- segurança dos dados;

[24] General Data Protection Regulation – https://gdpr.eu/tag/gdpr/.

[25] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, OEA – https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.

GRÁFICO 25 – ÁREA FOCAL: PRIVACIDADE E DADOS

Proporção das estratégias vigentes analisadas que menciona cada mecanismo



Comparação por região

n = 19 estratégias vigentes

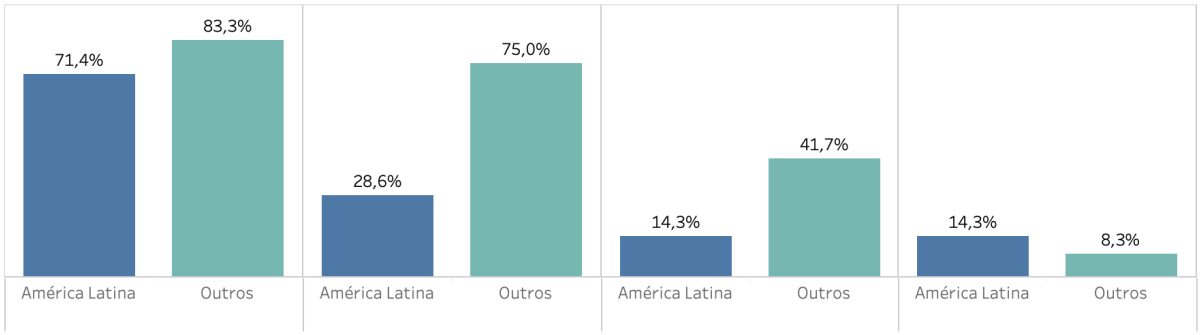
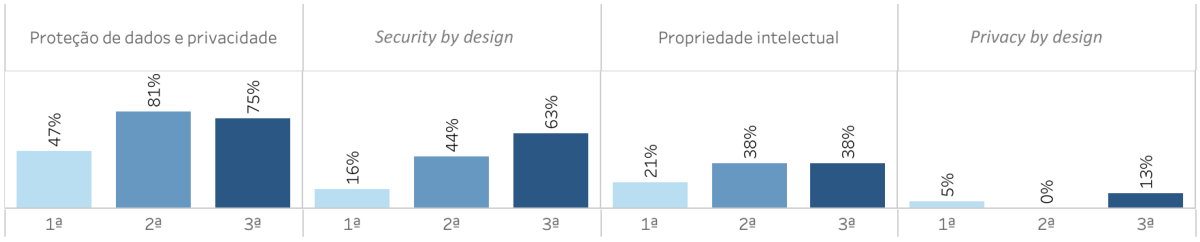


GRÁFICO 26 – EVOLUÇÃO DA ÁREA FOCAL: PRIVACIDADE E DADOS

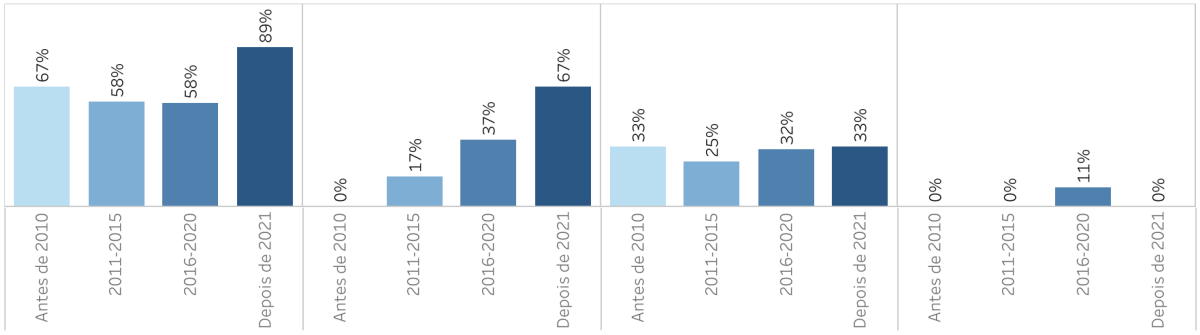
Evolução da presença do mecanismo nas estratégias analisadas

Por geração da estratégia



Por período

n = 43 estratégias



- precisão dos dados;
- acesso, retificação, exclusão, cancelamento, objeção e portabilidade;
- dados pessoais sensíveis;
- responsabilidade e obrigação;
- fluxo de dados transfronteiriços e responsabilidade;
- exceções;
- autoridade de proteção de dados.

O tópico de proteção de dados e privacidade é abordado, mesmo que superficialmente, por 78,9% das estratégias em vigor, com margem levemente menor na América Latina (71,4%) do que no Norte Global (83,3%). Esse é um tópico que está presente há algum tempo e continuou a crescer a partir da segunda geração. A Colômbia, em seu plano de ação da estratégia, no ponto 5.3.3, define: "Analisar a adoção de modelos, padrões e estruturas de segurança digital, com ênfase em novas tecnologias para preparar o país para os desafios da 4RI" e estabelece o seguinte em relação à proteção de dados: "Em primeiro lugar, a Secretaria Administrativa da Presidência da República, por meio do coordenador nacional de segurança digital, formulará o decreto regulamentar para a aplicação e o uso de padrões, modelos, normas e ferramentas que permitam a gestão adequada dos riscos de segurança digital e a resposta a incidentes no setor. O acima exposto tem o objetivo de gerar confiança nos processos das entidades públicas, garantir a proteção dos dados pessoais e a inclusão, bem como atualizar permanentemente as políticas de segurança e confiança digital".

Israel faz referência aos temas de proteção de dados quando menciona os desafios de segurança ligados à inteligência artificial. Na seção "Preparação para tecnologias emergentes", afirma o seguinte: "Frequentemente, os dados de treinamento foram criados antes que o aprendizado de máquina fosse compreendido e, às vezes, são obtidos de fontes desavisadas. Isso representa um desafio de segurança, como o potencial de selecionar pessoas como microalvos de maneiras sem precedentes. Os dados biométricos são particularmente sensíveis, e os bancos de dados biométricos de Israel para identificação segura são altamente protegidos e regulamentados por lei. O trabalho está em andamento na coleta segura de dados e no treinamento de IA. Os ataques à privacidade estão sendo investigados. Soluções técnicas de anonimização estão sendo estudadas".

Com relação ao tópico *security by design*, pode-se ver como sua presença tem aumentado acentuadamente, ao longo dos anos, começando com nenhuma presença nas estratégias anteriores a 2010 e chegando a 67% nas mais atuais. Conforme supramencionado, esse é um exemplo de tópico que, embora tenha sido desenvolvido na década de 1970, tornou-se particularmente relevante em nível de estratégia nacional nos últimos anos. Um exemplo de normas que mencionam esse princípio são as normas ISO/IEC 27000. A Argentina, em sua segunda estratégia, no objetivo 3 "Proteção e recuperação dos sistemas de informação do setor público", estabelece "Promover a segurança desde a concepção e em todas as fases da implementação e adoção de projetos tecnológicos do Setor Público Nacional, garantindo padrões adequados para a proteção de dados pessoais e segurança da informação".

Em relação ao tema da propriedade intelectual, nota-se que tem pouca presença nas estratégias atuais (31,6% delas), com baixa presença nas da América Latina, fato que se corrobora pela tendência de os países do Norte Global serem mais fortemente produtores de novas tecnologias. Embora seja uma questão que se mantém ao longo do tempo, é visível o aumento de sua abordagem nas estratégias, se observadas do ponto de vista geracional. A Espanha estabelece

uma medida clara para a linha de ação 5 de sua segunda estratégia, na qual define "Aumentar as atividades nacionais para o desenvolvimento de produtos, serviços e sistemas de segurança cibernética e *security by design*, apoiando especificamente aqueles que apoiam as necessidades de interesse nacional para fortalecer a autonomia digital e a propriedade intelectual e industrial".

Privacy by design é um tópico relativamente novo, com baixa presença nas estratégias atuais, estando presente em apenas 13% das que estão em vigor. A Estônia, em sua terceira estratégia, define uma de suas atividades prioritárias da seguinte forma: "O desenvolvimento de novos serviços e bancos de dados seguirá os princípios de segurança e privacidade desde a concepção. Serão abandonadas as plataformas obsoletas (princípio "*no legacy*"). Para isso, será desenvolvido um recurso de consultoria de arquitetura de segurança central".

5.7.8. *Área focal: defesa e capacidade militar*

PONTOS-CHAVE DA SEÇÃO

- **Capacidades militares:** embora 42,1% das estratégias atuais mencionem o aprimoramento das capacidades militares, deve-se ter em mente que isso nem sempre é abordado pela estratégia de segurança cibernética, mas sim pelas estratégias de defesa ou segurança nacional.

Os tópicos de aprimoramento das capacidades militares e defesa cibernética ofensiva não são os mais populares entre as estratégias analisadas. Dois aspectos principais devem ser levados em consideração ao analisá-los. Primeiramente, como ocorre com outros tópicos, é possível que

GRÁFICO 27 – ÁREA FOCAL: DEFESA E CAPACIDADE MILITAR

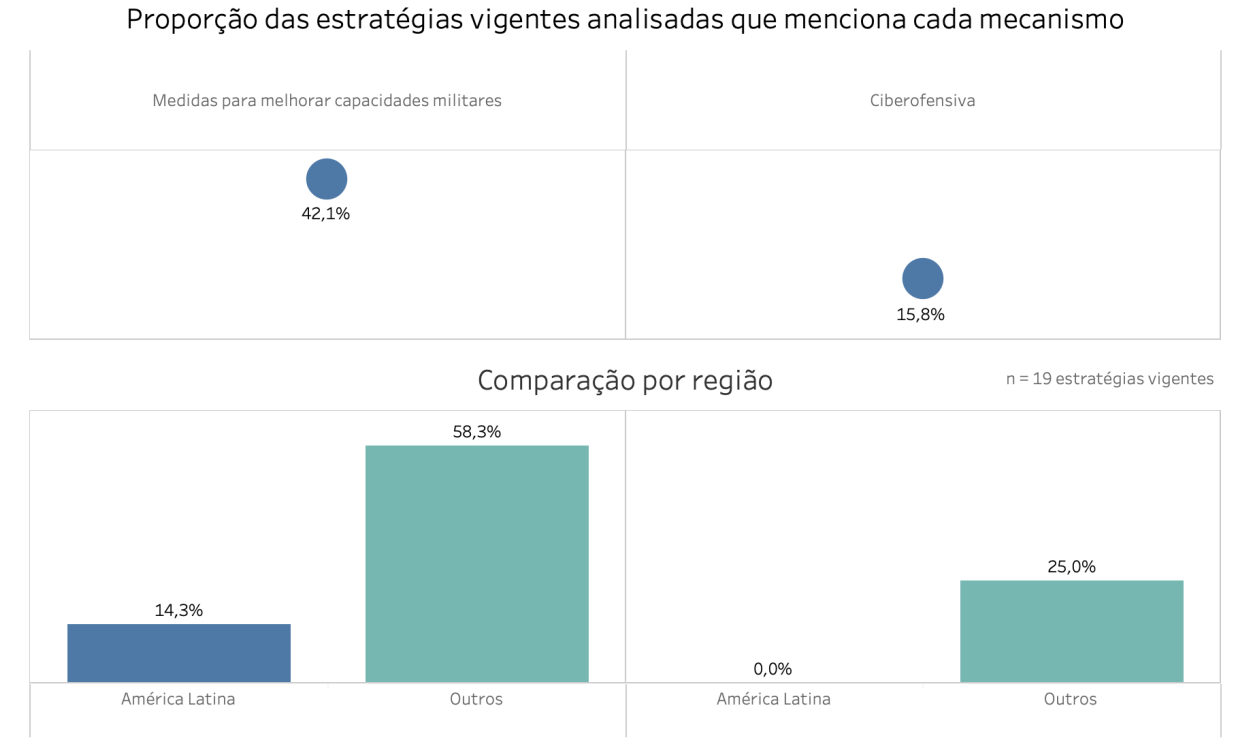
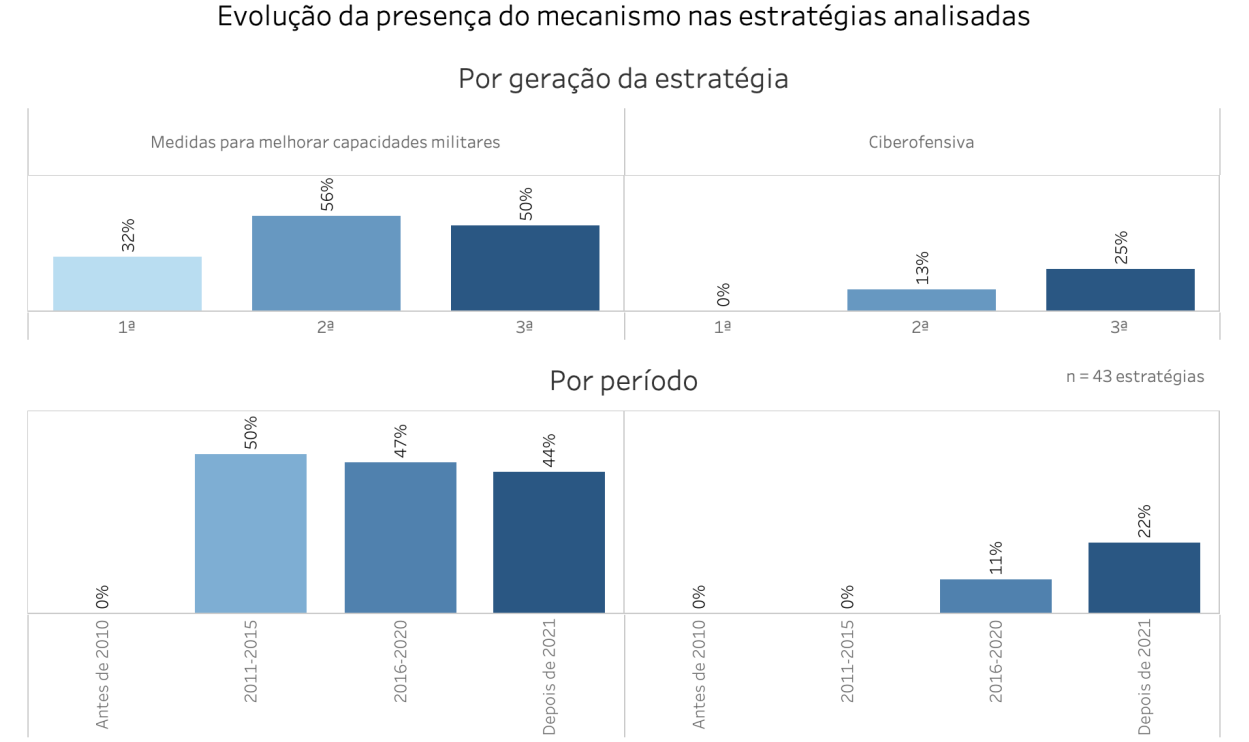


GRÁFICO 28 – EVOLUÇÃO DA ÁREA FOCAL: DEFESA E CAPACIDADE MILITAR



a questão seja abordada em outra estratégia, como a de segurança nacional ou a de defesa nacional; portanto, o fato de não estar presente na estratégia não significa que não seja uma preocupação do país. Em segundo lugar, embora esses sejam tópicos comuns a todos os países, a prioridade e a urgência de abordar essa questão dependem muito do contexto. Ao contrário de outros tópicos, como capacitação ou resiliência, que são clara e igualmente importantes para todos os países, sua importância pode estar aberta à discussão.

Especificamente sobre o tópico de aprimoramento das capacidades militares, 42,1% das estratégias atuais o mencionam. Embora seja geralmente tratado em proporção semelhante nas estratégias, em diferentes períodos, nota-se o aumento em seu aparecimento do ponto de vista geracional, que começa com 32%, na primeira geração, e termina com 50% na terceira geração. Alguns exemplos ilustrativos:

- "A segurança cibernética será continuamente incluída na abordagem geral de defesa nacional. Para isso, será ainda mais integrada nos documentos de planejamento de segurança nacional (o plano de desenvolvimento e o de atividades de defesa nacional) e serão realizados regularmente exercícios conjuntos com prestadores de serviços vitais, formuladores de políticas seniores e organizações de defesa nacional" (atividade prioritária, Estônia, 2022).
- "Melhorar a defesa cibernética e as capacidades de inteligência cibernética", "Implementar medidas ativas de defesa cibernética no setor público com o objetivo de melhorar as capacidades de resposta" (linha de ação 1, medidas 6 e 12, Espanha, 2019).

Existe uma diferença significativa entre as regiões, com presença elevada do tópico fora da América Latina (58,3%) e baixa na região (14,3%).

O tema da segurança cibernética ofensiva no contexto militar tem presença reduzida, atingindo apenas 15,8% das estratégias em vigor. Embora haja o aumento de sua participação nas estratégias, quando se observa do ponto de vista geracional, ainda poucas o incluem e sempre no Norte Global. Um exemplo desse tópico nas estratégias estudadas é:

- "Os Estados que não compartilham dos desafios impostos pela internet livre e aberta os estão explorando para promover suas visões autoritárias do ciberespaço, sob o pretexto de segurança. O Reino Unido adotará uma abordagem mais proativa, trabalhando com aliados e parceiros para garantir regras e estruturas internacionais alinhadas com seus valores democráticos. O objetivo é apoiar o crescimento econômico nacional e global e a segurança coletiva, incentivar o uso responsável de ferramentas cibernéticas ofensivas e consequências reais para as ferramentas maliciosas e irresponsáveis. Os seguintes resultados serão alcançados até 2025" (parágrafo 160, objetivo 2, Reino Unido, 2022).

QUADRO 10 – ESTUDO DE CASO
EVOLUÇÃO DAS ESTRATÉGIAS DE CIBERSEGURANÇA NO REINO UNIDO

O Reino Unido está na terceira estratégia de cibersegurança publicada e é uma ilustração interessante da evolução de alguns aspectos-chave na abordagem de cada estratégia. Na comparação da primeira para a segunda, percebem-se algumas mudanças significativas, em especial em relação ao papel do setor privado. Já em relação à passagem da segunda para a terceira estratégia, nota-se um papel mais assertivo do Reino Unido e uma mudança do enfoque de cibersegurança para "poder cibernético" (ou *cyber power*, no original). Veja a seguir um breve relato da evolução das estratégias:

Primeira estratégia (2011):

A estratégia inaugural de cibersegurança, em 2011, estabeleceu as bases para a abordagem do Reino Unido ao ciberespaço. Em seu cerne, priorizou o valor econômico do ciberespaço, estruturando objetivos em torno de cidadãos, empresas e governo. Os principais objetivos incluíam combater o cibercrime para tornar o país um local seguro para negócios on-line, aumentar a resiliência contra os ataques, fomentar um ciberespaço aberto e estável e garantir que a nação tivesse o conhecimento e as habilidades necessárias para alcançar essas metas. Pioneiramente, a estratégia estabeleceu um orçamento específico para o Programa Nacional de Cibersegurança, enfatizando a cooperação entre o mercado privado e o setor público. De forma geral, a estratégia tinha uma abordagem mais de incentivos e orientações, esperando que o setor privado fortalecesse sua postura de segurança.

Segunda estratégia (2016):

Elaborada considerando a estratégia de 2011 e o lançamento do Centro de Cibersegurança Nacional, a estratégia de 2016 reconheceu o progresso feito, mas percebeu a necessidade de um papel mais proativo por parte do governo. A estratégia cita que "uma abordagem baseada no mercado para a promoção da cibersegurança não produziu o ritmo e a escala de mudança necessários; portanto, o governo precisa liderar o caminho e intervir mais diretamente, exercendo sua influência e seus

(Continua na próxima página)

QUADRO 10 – ESTUDO DE CASO *(Continuação)*

recursos para enfrentar as ameaças cibernéticas". O próprio estabelecimento do Centro de Cibersegurança Nacional indica a busca por um papel mais proativo do governo. Para além de orientações como na primeira estratégia, agora há ênfase maior em incentivos e regulação.

Terceira estratégia (2021):

A estratégia mais recente, lançada em 2021, muda a ênfase de cibersegurança para "poder cibernético" (ou *cyber power*, no original). Nessa terceira geração, com linguagem mais assertiva, o Reino Unido entende o ciberespaço como uma arena central na competição entre países democráticos e autocráticos. Nessa visão, também há uma mudança do alcance, uma vez que a segunda estratégia mencionava uma abordagem de todo o governo (*whole-of-government*) e agora passa a visão de toda a sociedade (*whole-of-society*). Essa abordagem se concretiza na criação de um National Cyber Advisory Board, que apoia o governo na implementação da estratégia. Nesse sentido, para além do foco em segurança, a estratégia se concentra muito em como usar o ciberespaço para vantagens econômicas e sociais.

A evolução das estratégias nacionais de cibersegurança do Reino Unido demonstra a mudança de abordagens orientadas pelo mercado para um papel mais proativo do governo, culminando na priorização do "poder cibernético" como um ativo nacional vital. Essa evolução representa o reconhecimento mais amplo da importância do ciberespaço, não apenas em termos de segurança, mas também como domínio para a competição e a cooperação econômica, social e geopolítica.

Fontes:

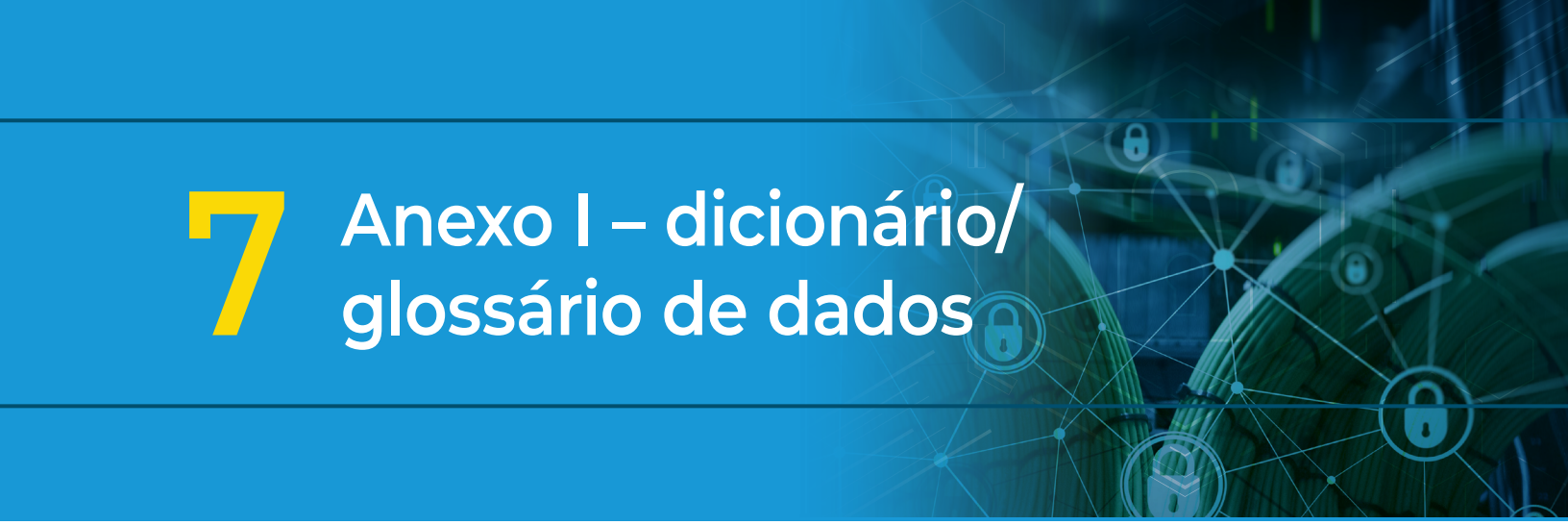
- Análise das três estratégias
- https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security--pub-86037
- https://www.holyrood.com/news/view,the-uks-national-cyber-strategy-2022-an-evolution

6 Considerações finais

Este estudo, a partir de uma análise documental de 43 estratégias, conseguiu identificar grandes tendências na evolução das estratégias de cibersegurança no mundo. Como visto, as novas estratégias são mais executivas e orientadas à ação e costumam apontar para um universo mais amplo da cibersegurança, entendida para além das questões de segurança nacional, englobando temas de prosperidade e desenvolvimento socioeconômico. Ao longo do estudo, identificaram-se os padrões de mudança e as tendências em diferentes áreas focais, ilustrando a direção dos países mais maduros.

Embora se verifiquem tendências importantes, cada país deve conduzir uma análise específica considerando sua situação, suas prioridades e capacidades individuais. Nesse processo, a consulta e a inclusão de diversas partes interessadas, como o governo, a sociedade civil, a academia e o setor privado, tornam-se passos essenciais para garantir a legitimidade da estratégia de cibersegurança no país, transformando-a em um documento de referência para essas partes .

Assim, adotar um processo colaborativo que incorpore os avanços e as lições aprendidas com a implementação das primeiras estratégias emerge como uma abordagem crucial para os países que estão elaborando suas segundas ou terceiras estratégias. Esse caminho não apenas fortalece o engajamento e a cooperação, mas também contribui para a evolução contínua e adaptabilidade das estratégias de cibersegurança em um cenário dinâmico e em constante transformação.



7 Anexo I – dicionário/ glossário de dados

Neste anexo, estão detalhadas as categorias de análise utilizadas para definir os critérios para identificar se as estratégias cobriam determinado aspecto ou não. O glossário está estruturado a partir da ordem de aparição nos gráficos apresentados.

Gráfico 1 – Estrutura

- **"Tem objetivos" –** considerou-se que "sim" se o documento tivesse objetivos estratégicos, objetivos gerais, pilares estratégicos, subobjetivos ou categoria similar explícitos.
- **"Tem princípios" –** considerou-se que "sim" se o documento explicitamente anunciasse o uso de princípios.
- **"Tem visão" –** considerou-se que "sim" se o documento explicitamente declarasse a visão ou se a visão estivesse englobada em outra sessão do documento. Em algumas estratégias, considerou-se o "propósito", desde que tivesse uma redação que olhasse para o direcionamento futuro na área.
- **"Tem indicadores/métricas" –** considerou-se que "sim" se o documento explicitamente usasse indicadores quantitativos ou métricas qualitativas para medir o sucesso e verificar o atingimento das propostas da estratégia. Não foram contabilizados os casos em que a estratégia mencionasse que os indicadores seriam elaborados em etapa posterior.

Gráfico 2 – Área focal: governança e institucionalidade

- **Mecanismos de coordenação intragoverno –** considerou-se que "sim" sempre que a estratégia mencionasse linhas de ação, objetivos ou intervenções para aumentar a coordenação entre as diferentes agências e departamentos do governo. Vale destacar que, em algumas estratégias, os mecanismos estão mais concretos (por exemplo, conselhos, comitês ou grupos de trabalho), enquanto em outras estão mais genéricos.
- **Mecanismos de coordenação público-privados –** considerou-se que "sim" sempre que a estratégia mencionasse linhas de ação, objetivos ou intervenções para aumentar a coordenação entre os setores público e privado. Vale destacar que, em algumas estratégias, os mecanismos são mais concretos (por exemplo, conselhos, comitês ou grupos de trabalho), enquanto em outras estão mais genéricos.
- **Reconhecimento de uma autoridade em ciber –** considerou-se que "sim" sempre que a estratégia mencionasse explicitamente o nome da agência ou do departamento responsável pela cibersegurança (caso já tivesse sido criado anteriormente) ou utilizasse o documento da estratégia para definir esse responsável. Considerou-se que "sim" quando a autoridade abrangia os

temas de ciber de forma ampla, bem como especificamente para a implementação da estratégia.

- **Definição de um plano operacional (agora ou no futuro) –** considerou-se que "sim" sempre que a estratégia tivesse um plano concreto de implementação já no corpo do documento principal ou sempre que mencionasse explicitamente que a criação de um plano de ação seria um resultado da publicação da estratégia.
- **Citação de entes subnacionais –** considerou-se que "sim" sempre que a estratégia mencionasse pelo menos uma ação que incluísse governos subnacionais (províncias, regiões, estados, municipalidades, governos locais, comarcas, ou definições similares, a depender do país).
- **Normativa associada –** considerou-se que "sim" sempre que o próprio documento da estratégia mencionasse o instrumento pelo qual foi publicada e vinculasse o número correspondente (decreto, resolução ou similar). Não foi feita pesquisa adicional externa ao documento para verificar se existia normativa associada.
- **Indicação clara de responsáveis –** considerou-se que "sim" sempre que o corpo principal da estratégia deixasse explícito quem era o responsável pela implementação das ações nela contidas. Também se considerou positivamente o caso em que houvesse uma seção da estratégia que descrevesse detalhadamente os arranjos de sua implementação, identificando os atores.
- **Orçamento associado –** considerou-se que "sim" sempre que a estratégia explicitamente atribuísse um orçamento, quantificasse o custo da sua implementação ou considerasse que seria feito logo na sequência. Não foram analisados os orçamentos propriamente ditos.

Gráfico 4 – Tipos de ameaça

- **Criminosos/ciberataques –** considerou-se que "sim" se a estratégia explicitamente mencionasse criminosos ou ciberataques como ameaças no espaço cibernético.
- **Outros países/ciberguerra –** considerou-se que "sim" se a estratégia explicitamente mencionasse ameaças vindas de outros Estados ou abordasse explicitamente as guerras no espaço cibernético.
- **Espionagem –** considerou-se que "sim" se a estratégia explicitamente mencionasse espionagem como ameaça. Muitas vezes, esse conceito estava correlacionado com a categoria anterior.
- **Terroristas –** considerou-se que "sim" se a estratégia explicitamente mencionasse terrorismo ou terroristas como ameaça.
- **Ataques à democracia –** considerou-se que "sim" se a estratégia mencionasse ameaças ligadas à manipulação de eleições, crenças democráticas, desinformação orientada a minar a democracia, ou categorias similares.
- **Extremistas –** considerou-se que "sim" se a estratégia mencionasse explicitamente extremistas ou a polarização política ou religiosa no ciberespaço.
- **Hacktivistas –** considerou-se que "sim" se a estratégia mencionasse explicitamente o termo hacktivistas ou hackers.
- **Desastres naturais –** considerou-se que "sim" se a estratégia mencionasse explicitamente riscos naturais (terremotos, desabamentos, alagamentos) como tipos de ameaça ao espaço cibernético no país.

Gráfico 6 – Proporção das estratégias vigentes avaliadas que contém cada princípio

- **Direitos humanos –** considerou-se que "sim" unicamente se, na sessão de princípios,

fossem mencionados os direitos humanos, valores democráticos, direitos fundamentais ou algum conceito ligado a liberdades civis. Caso o tema fosse mencionado fora da sessão, não seria contabilizado.

- **Visão holística/coordenada –** considerou-se que "sim" unicamente se, na sessão de princípios, fosse mencionada a necessidade de ter uma abordagem integrada ou holística ou se existisse algum princípio com foco em aumentar a coordenação entre os diferentes atores envolvidos na temática.
- **Cooperação internacional –** considerou-se que "sim" unicamente se, na sessão de princípios, houvesse algum princípio orientador com foco em cooperação internacional ou atuação global.
- **Cibersegurança como parte da segurança nacional –** considerou-se que "sim" unicamente se, na sessão dos princípios, houvesse alguma menção mais ampla relacionada à segurança nacional.
- **Prosperidade econômica –** considerou-se que "sim" unicamente se, na sessão de princípios, existisse algum princípio orientado à prosperidade econômica ou se, ao menos, fossem usados termos como "prosperidade econômica", "oportunidade econômica", "fomento à indústria", "desenvolvimento econômico" ou similares.
- **Conscientização/responsabilidade individual –** considerou-se que "sim" unicamente se, na sessão de princípios, houvesse algum princípio orientado ao cidadão ou usuário final e/ou se fosse mencionado um foco em sensibilização ou conscientização dos riscos do ciberespaço.
- **Transparência/confiança –** considerou-se que "sim" unicamente se, na sessão de princípios, houvesse algum princípio orientado ao aumento da transparência ou confiança no ciberespaço e/ou nas políticas de cibersegurança.
- **Proporcionalidade –** considerou-se que "sim" unicamente se, na sessão de princípios, houvesse algum princípio que mencionasse o termo proporcionalidade ou o sentido de calibrar as ações de cibersegurança pela magnitude do risco.

Gráfico 8 – Proporção das estratégias vigentes avaliadas que contém cada objetivo

- **Prontidão e resiliência –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse alguma menção explícita a melhorias na resiliência, prontidão ou preparação para resposta a ataques.
- **Capacidades/*capacity building* –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse algum objetivo orientado a melhorar as capacidades (do país ou do governo), ampliar o conhecimento no país, ampliar a capacidade de resposta ou ações relacionadas a profissionais e educação.
- **Cooperação internacional –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, fosse mencionado algum objetivo direcionado à cooperação internacional ou atuação global.
- **Cooperação público-privada –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, fosse mencionado algum objetivo para ampliar a cooperação com o setor privado.
- **Infraestrutura crítica –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, fosse utilizado explicitamente o conceito de infraestrutura crítica.
- **Fomento à indústria –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse algum objetivo orientado ao setor econômico de cibersegurança

no país ou a ampliar a prosperidade econômica de forma mais abrangente.

- **Cultura de ciber/conscientização –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, fosse mencionado algum objetivo orientado à cultura de forma ampla e/ou à necessidade de aumentar a conscientização das diferentes partes, em especial dos usuários individuais.
- **Desenvolvimento normativo –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse alguma menção a melhorias no marco legal, normativo ou regulatório.
- **Confiança/transparência –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse alguma menção ao aumento da confiança ou transparência no ciberespaço ou nas políticas de cibersegurança.
- **Ciberespaço aberto –** considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, fosse mencionada a necessidade de um ciberespaço aberto ou livre (ou alguma menção explícita à internet aberta ou livre).
- **Gestão de riscos** – considerou-se que "sim", unicamente se, no nível mais alto dos objetivos, houvesse algum objetivo sobre gestão de riscos em cibersegurança.

Gráfico 11 – Gestão de riscos

- **Define uma abordagem de gestão de riscos –** considerou-se que "sim" sempre que a estratégia mencionasse a necessidade de uma abordagem de gestão de riscos na temática de cibersegurança. Nessa categoria, não se exigiu a definição da abordagem, mas tão somente o reconhecimento da importância de abordar a gestão de riscos.

Gráfico 13 – Prontidão e resiliência

- **Capacidades para resposta a incidentes –** considerou-se que "sim" sempre que a estratégia mencionasse a capacidade operacional de responder aos incidentes, incluindo menções a times de resposta a incidentes, times de emergência ou similares(CERTs, CIRTs, CSIRTs), entre outros.
- **Promoção do compartilhamento de informações –** considerou-se que "sim" sempre que a estratégia mencionasse medidas (ou intenções) para aumentar o compartilhamento de informações (fosse intragoverno ou entre setores).
- **Exercícios de cibersegurança –** considerou-se que "sim" sempre que a estratégia mencionasse o fomento à realização de exercícios de cibersegurança, incluindo simulações ou exercícios em tempo real.
- **Planos de contingência/gestão de crises –** considerou-se que "sim" sempre que a estratégia mencionasse medidas (ou intenções) para criar planos de contingência para a gestão de crises.

Gráfico 15 – Infraestrutura crítica (IC) e serviços essenciais

- **Medidas para proteger as ICs –** considerou-se que "sim" se a estratégia estabelecesse medidas ou intenções de estabelecer medidas para proteção das ICs.
- **Cooperação com o setor privado (p/IC) –** considerou-se que "sim" se a estratégia encorajasse a colaboração público-privada para a proteção de ICs.
- **Medidas para proteger os ativos de governo digital –** considerou-se que "sim" se a estratégia mencionasse a digitalização de serviços ou a expansão do governo digital e a importância de sua proteção.

- **Medidas para identificar as ICs do país –** considerou-se que "sim" se a estratégia explicitamente tivesse uma medida ou ação orientada a identificar e nomear as ICs do país.

Gráfico 17 – Capacidades e conscientização

- **Inovação e P&D –** considerou-se que "sim" se a estratégia citasse ações ou medidas para aumentar a pesquisa e o desenvolvimento na área de cibersegurança ou mencionasse políticas de inovação na área.
- **Programas de conscientização –** considerou-se que "sim" se a estratégia citasse medidas para aumentar a conscientização dos usuários nos temas de cibersegurança, incluindo campanhas, cursos, programas de sensibilização e conscientização na área.
- **Medidas na educação superior –** considerou-se que "sim" sempre que a estratégia mencionasse medidas relacionadas a universidades, como mudanças no currículo, aumento de PhDs, entre outras.
- **Medidas na educação primária/secundária –** considerou-se que "sim" sempre que a estratégia mencionasse medidas para estimular o desenvolvimento de competências em crianças e/ou na educação primária/secundária.
- **Medidas para formar profissionais –** considerou-se que "sim" sempre que a estratégia mencionasse medidas para estimular o desenvolvimento de profissionais e mão de obra em cibersegurança, excluindo investimentos em educação superior.
- **Medidas para capacidades de servidores públicos –** considerou-se que "sim" sempre que a estratégia mencionasse medidas para estimular o desenvolvimento de competências em servidores públicos ou, de forma mais ampla, nos órgãos públicos (incluiu treinamentos ou capacidades de forma mais ampla).
- **Desenvolvimento da indústria para aumentar a soberania –** considerou-se que "sim" sempre que a estratégia mencionasse o fomento da indústria de ciber atrelado à preocupação de reduzir a dependência de soluções estrangeiras.
- **Desenvolvimento da indústria para oportunidades econômicas –** considerou-se que "sim" sempre que a estratégia mencionasse o fomento da indústria de ciber ligado a objetivos de oportunidades econômicas.
- **Medidas para aumentar a diversidade –** considerou-se que "sim" sempre que a estratégia mencionasse medidas para aumentar o número de mulheres, pessoas LGBTQ+ e/ou outros grupos vulneráveis ou tradicionalmente sub-representados nas áreas de cibersegurança.

Gráfico 21 – Cooperação internacional

- **Cooperação com outros países/bilateral –** considerou-se que "sim" sempre que a estratégia incluísse medidas para aumentar a cooperação bilateral ou ampla entre países nos temas de cibersegurança.
- **Alinhamento com iniciativas regionais/multilaterais –** considerou-se que "sim" sempre que a estratégia mencionasse nomes específicos de blocos ou iniciativas regionais ou globais (por exemplo, OTAN, União Europeia etc.)

Gráfico 24 – Legislação e marco normativo

- **Melhorar o marco atual –** considerou-se que "sim" quando a estratégia mencionasse

de forma ampla a necessidade de melhorias no marco normativo atual.

- **Legislação sobre cibercrime –** considerou-se que "sim" quando a estratégia mencionasse medidas explicitamente voltadas à legislação de cibercrime
- **Melhorar a aplicação da lei –** considerou-se que "sim" quando a estratégia mencionasse melhorias para processar, punir, investigar o cibercrime e/ou usasse explicitamente a expressão *law enforcement* (especialmente nas estratégias em inglês).

Gráfico 25 – Privacidade e dados

- **Proteção de dados e privacidade –** considerou-se que "sim" quando a estratégia incluísse preocupações e intenções de avançar na área de proteção de dados e privacidade. Caso fosse somente um princípio, foi considerado que não.
- ***Security by design* –** considerou-se que "sim" unicamente quando a estratégia usasse explicitamente o conceito.
- **Propriedade intelectual** – considerou-se que "sim" quando existissem iniciativas específicas para a proteção da propriedade intelectual ou quando se percebesse a preocupação existente específica para esse tipo de proteção.
- ***Privacy by design* –** considerou-se que "sim" unicamente quando a estratégia usasse explicitamente o conceito.

Gráfico 27 – Defesa e capacidade militar

- **Medidas para melhorar capacidades militares –** considerou-se que "sim" quando a estratégia mencionasse medidas ligadas às capacidades militares ou à defesa.
- **Ciberofensiva –** considerou-se que "sim" unicamente quando a estratégia mencionasse o conceito explicitamente.


BID
Melhorando vidas