ANÁLISE DO CENÁRIO REGIONAL E INTERNACIONAL: EVOLUÇÃO DAS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA

Brasil 2023

Autores: Santiago Paz,
Martina Bergues, José Callero.

Os projetos de cooperação técnica que co-financiaram o apoio do BID ao ANÁLISE DO CENÁRIO REGIONAL E INTERNACIONAL: EVOLUÇÃO DAS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA 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.

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].
- Além disso, esses ataques estão se tornando cada vez mais sofisticados, com o tipo de ataque de extorsão ransomware representando 17% dos ataques detectados globalmente. Um exemplo desses ataques 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, aumento e 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 caminhos estratégicos para proteger e assegurar o ciberespaço.
- Com 2 décadas de Estratégias Nacionais publicadas[4], ainda há pouco conhecimento sistematizado sobre qual é a evolução das estratégias e quais são as principais lições aprendidas.
- Este estudo busca criar uma metodologia para comparar documentos heterogêneos e captar tendencias e padrões que possam auxiliar países que se encontram no processo de elaboração de novas versões de suas Estratégias Nacionais de Cibersegurança.

Que metodologia foi usada?

- Neste estudo, foram analisadas 40 Estratégias Nacionais de 17 países, incluindo estratégias de primeira, segunda e terceira geração.
- Para cada estratégia foram analisadas as principiais áreas focais, tomando como referência uma adaptação das áreas focais do *Guide to Developing a National Cybersecurity Strategy*, documento liderado pelo ITU.
- Em primeiro lugar, a análise se focou em compreender como cada tema está presente nas estratégias atualmente em vigor para documentar o estado da arte das Estratégias de Cibersegurança mais recentes.

[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.

- Em seguida, para identificar padrões e diferenças regionais, os mesmos aspectos foram analisados comparando as estratégias da América Latina com as de outros países. Isso 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 (de primeira, segunda ou terceira geração), o que permitiu captar diferenças nas tendencias ligadas à evolução do tempo e tendencias ligadas à maturidade dos países.
- Além disso, o estudo apresenta estudos de caso para oferecer uma compreensão mais completa 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 captar diferentes padrões e tendencias a partir de uma análise sistemática das estratégias.

- As estratégias de terceira geração são mais operativas e menos teóricas quando comparado com as gerações anteriores.

- Dentre 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 segurança nacional e incluem temas de prosperidade econômica e fomento à indústria, delineando uma tendencia a entender o campo da cibersegurança como fértil para o desenvolvimento econômico e social de um país.

- Dentre as estratégias atualmente em vigor, virtualmente todas possuem objetivos ou iniciativas ligadas aos temas de prontidão e resiliência, fortalecimento das capacidades em cibersegurança e cooperação internacional.

- 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 terroristas, apresentam em proporção maior componentes relacionados à prosperidade econômica e fomento à indústria, estabelecem medidas para proteger ativos de governo digital com mais frequência, dentre outras tendencias que serão exploradas ao longo do estudo.

- Em relação à analise evolutiva, para além da já mencionada tendencia ao aumento dos princípios, objetivos e iniciativas ligados à prosperidade econômica e fomento à indústria de cibersegurança, se destacam: (i) aumento dos princípios, objetivos ou iniciativas ligados à transparência e confiança no ciberespaço; (ii) aumento de iniciativas voltadas a promover à diversidade na força de trabalho de cibersegurança; (iii) diminuição de objetivos ligados à infraestrutura crítica nas estratégias de 3ª geração; (iv) aumento da presença de mecanismos para promover o compartilhamento de informações e ampliar a cooperação; (v) aumento do estabelecimento de planos de contingencia; (vi) aumento da presença do conceito de *security by design*, dentre outras tendencias que serão exploradas ao longo do estudo.

2. Metodologia

3.1. Seleção dos países

O estudo incluiu a análise de 12 países com nível de maturidade avançado fora da região e 5 países da América Latina e Caribe (de forma a contemplar a experiência regional na temática), totalizando uma análise de 40 estratégias, das quais 17 estão vigentes atualmente. A identificação dos países incluídos no estudo levou em conta o nível de maturidade no *ITU Global Cybersecurity Index (GCI)*[5] e/ou sua participação no *Digital Nations*[6], garantindo que sejam incluídos os países mais avançados no cenário global. Em relação a escolha dos países da América Latina e Caribe, foi levado 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:

[5] Global Cybersecurity Index
[6] DN - Digital Nations

As estratégias analisadas se distribuem no tempo e por geração. O conceito de geração se refere a se a estratégia analisada é a primeira, segunda ou terceira estratégia publicada de cada país. Na amostra analisada, há países com 1, 2 ou 3 estratégias[7]. A distribuição das estratégias por período pode ser verificada no quadro abaixo.

[7] A distribuição das estratégias por período e geração se distribui da seguinte forma: 1ª Geração publicadas antes de 2010: EUA (2003), Estônia (2008) e Canada (2010); 1ª Geração publicadas entre 2011 e 2015: Reino Unido (2011), Nova Zelandia (2011), Coreia (2011), Colômbia (2011), França (2011), Espanha (2013), Portugal (2015), Japão (2015); 1ª Geração publicadas entre 2016-2022: Austrália (2016), Chile (2017), Israel (2017), República Dominicana (2018), Argentina (2019), Brasil (2020); 2ª Geração publicada entre 2011-2015: Estônia (2014), Nova Zelandia (2015), França (2015); 2ª Geração publicada entre 2016-2020: Reino Unido (2016), Colômbia (2016), Canada (2018), EUA (2018), Japão (2018), Coreia (2019), Espanha (2019), Portugal (2019), Australia (2020); 2ª Geração publicada depois de 2020: Israel (2021), República Dominicana (2022), Argentina (2023); 3ª Geração publicada entre 2016-2020: Estônia (2019), Nova Zelandia (2019), Colômbia (2020); 3ª Geração publicada depois de 2020: Japão (2021), França (2021), Reino Unido (2022), Australia (2023), EUA (2023);

Número de estratégias por período e geração

	1ª	2ª	3ª
antes de 2010	3	0	0
2011-2015	8	3	0
2016-2020	6	9	3
depois de 2020	0	3	5

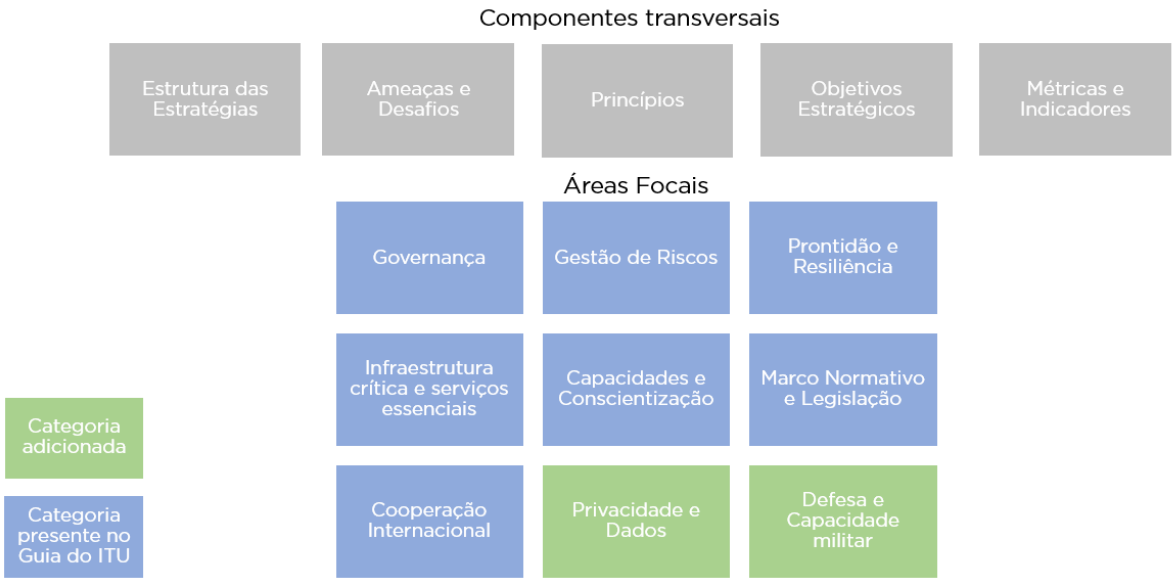
3.2. Análise das Estratégias

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. Estas categorias foram construídas a partir de uma adaptação do *Guide to Developing a National Cybersecurity Strategy*[8], documento de referência internacional, elaborado por mais de 12 organizações parceiras e liderado pelo ITU.

Para referência, as macro categorias 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 macro categorias 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 no diagrama abaixo:

[8] Guide to developing a National Cybersecurity Strategy



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 estava alinhado e que a metodologia era robusta. Vale destacar que o objetivo da categorização é permitir a comparabilidade e captar as tendencias 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.

COMO LER OS GRÁFICOS E DADOS DESTE ESTUDO

O estudo segue um padrão de análise para todos os tópicos selecionados. Para cada tema, se apresenta primeiro uma análise que inclui somente as 17 estratégias vigentes (sendo que há estratégias da primeira, segunda e terceira geração, a depender do país). Ainda na análise desses 17 documentos, se faz 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 1ª, 2ª ou a 3ª estratégia de determinado país); (ii) por período. A comparação das duas evoluções ajuda a entender se existe algum padrão temporal ou se o aumento ou diminuição de determinado tema pode estar mais relacionado à maturidade dos países, entendendo que uma estratégia de 3ª geração pode incluir lições aprendidas das versões anteriores.

Para ler os gráficos, é importante ter em mente algumas limitações:

(i) Os gráficos são um recurso para visualizar a comparação dos países, mas se trata de um estudo qualitativo que classificou os temas presentes nas estratégias para conseguir extrair as principais tendencias a partir de uma análise sistemática.

(ii) O número de estratégias analisadas é pequeno (n=17 para o primeiro conjunto de gráficos e n=40 para o segundo). Dessa forma, vale destacar que se trata somente de estatísticas descritivas. Se sugere cautela especial ao analisar os dados da América Latina, uma vez que somente 5 estratégias vigentes fazem parte da amostra. Isso significa que, se apenas uma estratégia contém ou não um certo tema, há uma variação de 20 pontos percentuais na média daquele indicador. Nesse sentido, é importante não tirar conclusões precipitadas.

(iii) Essa limitação, todavia, não significa que não se possa usar a análise comparada para entender padrões e tendencias. Por essa razão, cada seção inclui uma explicação qualitativa das tendencias encontradas nos gráficos e nos convida a, embora ser cautelosos nas conclusões, capturar possíveis padrões e tendencias que podem auxiliar na elaboração da nova Estratégia de Cibersegurança do Brasil.

(iv) A análise foi feita a partir de uma leitura dos documentos, mas se fosse um auto questionário preenchido pelos países, o entendimento de cada estratégia poderia ter nuances que não são plenamente captadas em uma simples análise documental.

(v) Os gráficos mostram possíveis tendencias agregadas e devem ser complementados com a leitura dos estudos de caso que aprofundam a análise comparada.

3. Grandes tendências

- **As estratégias da terceira geração são mais operativas e menos teóricas quando comparado com as gerações anteriores.** As estratégias de terceira geração definem mais claramente os responsáveis para as ações incluídas (63% comparado com 41% nas de primeira geração), têm maior vinculação explicita com orçamento[9] para implementação da estratégia (63% comparado com 24% das de primeira geração), definem com mais frequência um plano operativo[10] (63% comparado com 29% 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 intra-governo e com o setor privado são frequentes nas estratégias vigentes.** Embora nem sempre as medidas propostas sejam concretamente identificáveis, nota-se uma 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 tendencia a que as estratégias mais recentes sejam mais amplas do que segurança nacional e incluam temas de prosperidade econômica e fomento à indústria.** Em especial nos países do Norte Global, as estratégias de terceira geração tendam a incluir com mais frequência princípios (75%), objetivos (71%) ou iniciativas voltadas para prosperidade econômica (47%), entendendo o campo 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.** 80% das estratégias vigentes analisadas, que declaram princípios, contém 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, aparecem como iniciativas ou linhas de ação, mas sempre há uma preocupação ou uma ação que enderece estes tópicos.

[9] Aqui consideramos tanto as estratégias que já possuem orçamento definido no documento publicado como aquelas que mencionam que a estratégia terá orçamento definido na próxima etapa.
[10] Aqui consideramos 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.

- **Há uma tendencia a que as estratégias incluam preocupação crescente com ataques à democracia.** Em termos das ameaças incluídas como preocupação das estratégias, se nota um aumento crescente da inclusão de ameaças cibernéticas para promover ataques à democracia. Esta tendencia se concentra nos países do Norte Global.

- **Nota-se um aumento do tema da transparência e aumento da confiança no ciberespaço nas estratégias de terceira geração.** Seja como princípio seja como área focal, o tema de transparência e confiança tem aparecido de forma mais consistente nas estratégias mais recentes, ilustrando uma possível tendencia a que o espaço cibernético e sua segurança sejam tratados com maiores preocupações para 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 a Pesquisa & Desenvolvimento, conscientização e estudos formais estão presentes em todas as versões das estratégias. 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 para aumentar a soberania.

- **A colaboração entre entidades e/ou países para detectar e responder a incidentes está desempenhando um 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.

4. Tendências em perspectiva comparada
4.1. 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:
  - 93.3% incluem objetivos estratégicos;
  - 58.8% incluem uma seção de princípios;
  - 58.8% definem uma visão clara para o país.
- **Indicadores:** A maioria das estratégias não possui indicadores ou métricas de sucesso associadas (somente 11.8%) – ver seção sobre indicadores e métricas para 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 5 páginas[11], enquanto a mais longa se estende por 130 páginas[12]. Além disso, as estratégias variam na duração de sua vigência, com algumas cobrindo um período de 4 anos, enquanto outras se estendem por 9 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).

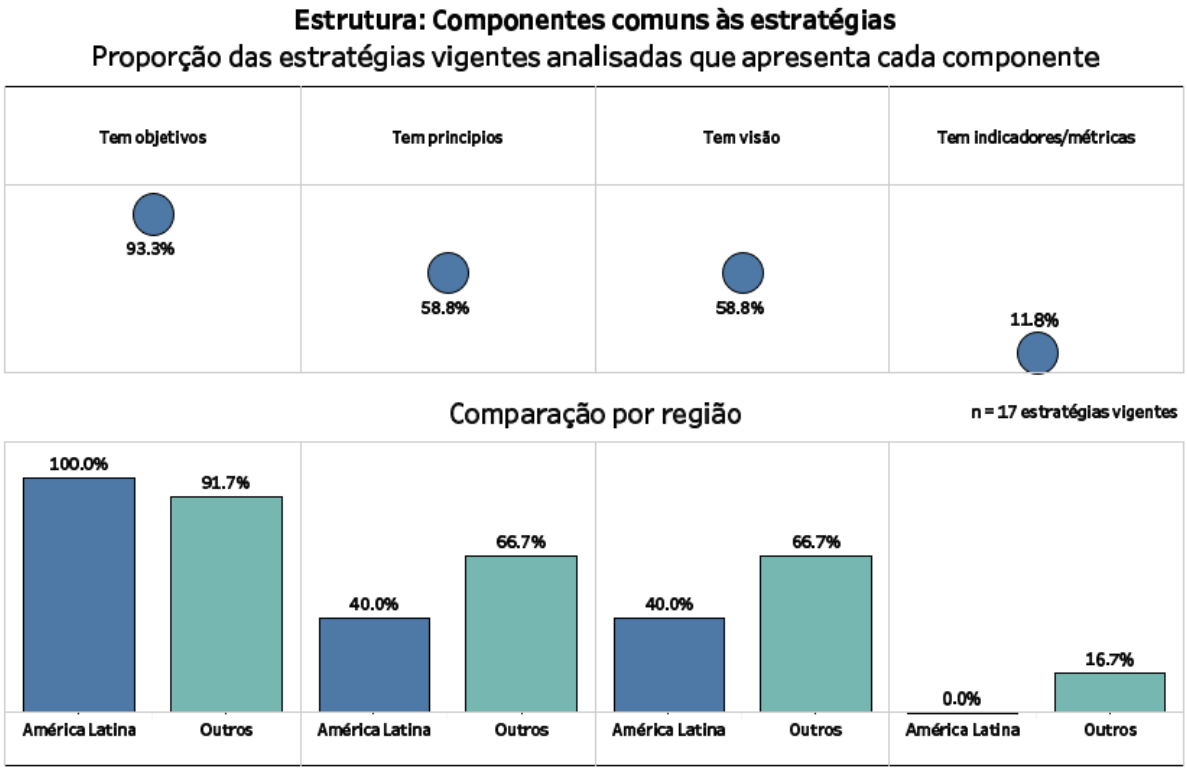
Apesar dessa heterogeneidade, é possível identificar componentes que são relativamente comuns nas diferentes estratégias (e que costumam ser padrão em documentos de estratégias de outros tópicos, não somente de cibersegurança). Dessa forma, para possibilitar a comparação das estruturas da amostra analisada, 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 17 estratégias vigentes analisadas não possui objetivos claramente delineados. Além dos objetivos, cerca de dois terços das estratégias examinadas incorporam princípios (consulte a seção *Princípios* para mais detalhes) e uma

[11] Corresponde à estratégia da Coreia de 2011.
[12] Corresponde à estratégia do Reino Unido de 2022.

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 mais detalhes).

Na análise por região, é possível perceber que as estratégias analisadas do Norte Global se caracterizam por uma maior presença de seções sobre princípios e possuem uma visão estabelecida com maior frequência, além de conter os dois países que possuem algum tipo de indicador.

Gráfico 1



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 em uma forma 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 uma 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 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 abaixo alguns exemplos de como os países têm estruturado suas visões (tradução livre).

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 uma sociedade forte.
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 uma visão para 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.

4.2. Mecanismos de Governança presentes nas Estratégias

PONTOS CHAVE DA SEÇÃO:

- **Autoridade em cibersegurança:** 65% das estratégias vigentes estabelecem (ou reconhecem) uma instituição responsável para os temas de cibersegurança (seja de forma geral, 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**: Somente um terço das estratégias tem orçamento associado, seja na própria estratégia seja previsto para um segundo momento.
- **Plano operativo:** Cerca de metade das estratégias tem ou prevê a criação de um plano operativo para implementação da estratégia.
- **Ênfase na coordenação:** Mais de 80% das estratégias preveem algum mecanismo de coordenação seja intra-governo seja com o setor privado. As estratégias do Norte Global dão maior ênfase à coordenação com o setor privado do que as estratégias da América Latina.

Esta seção analisa categorias relacionadas à governança e institucionalidade das estratégias, procurando compreender que mecanismos para implementação da estratégia existem 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 (88.2%[13] das estratégias vigentes menciona algum tipo de coordenação entre as agências governamentais) seja olhando para a coordenação entre o setor público e o setor privado (76.5%[14] das estratégias vigentes menciona algum tipo de coordenação entre os setores). Além dos mecanismos de coordenação, também se destaca que cerca de 65% estabelecem ou reconhecem (caso já estivesse previamente estabelecida) algum órgão como autoridade para os temas de cibersegurança, de forma geral, e/ou para a liderança da implementação da estratégia, em específico.

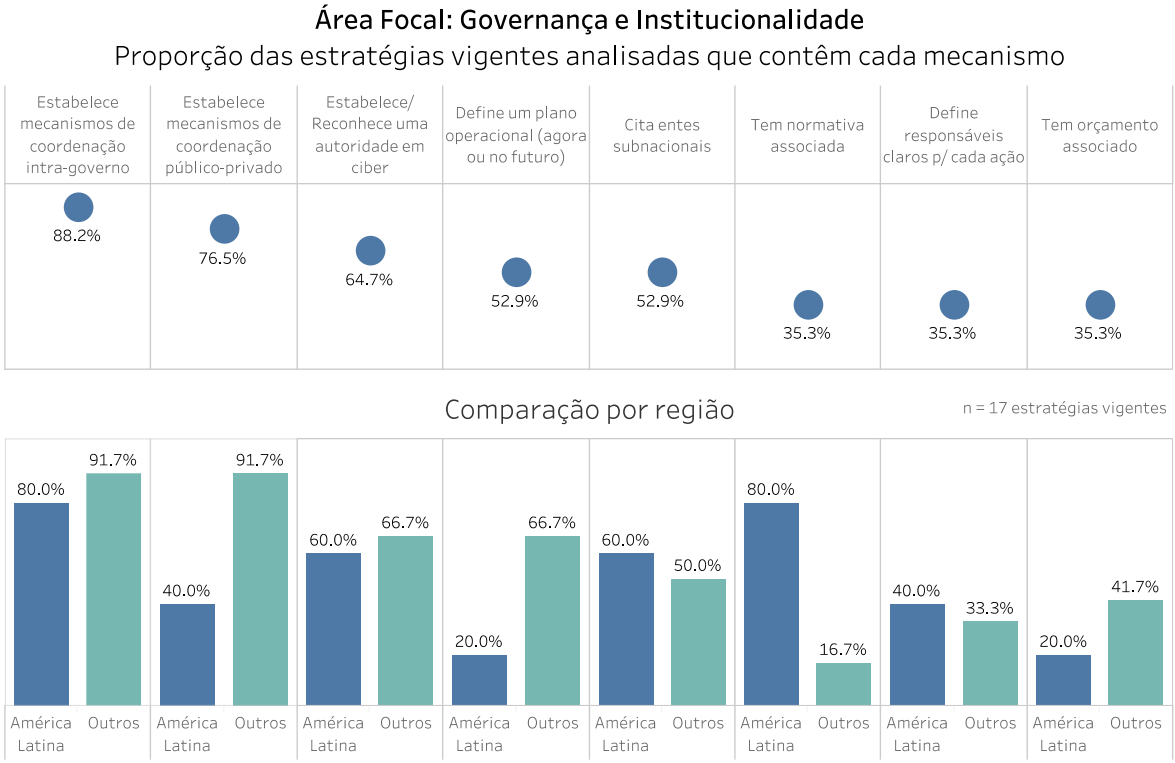
Em termos comparados, a análise das 17 estratégias atualmente vigentes que fizeram parte da amostra selecionada indica que não é muito comum que as estratégias já mencionem a

[13] Aqui foram consideradas menções à mecanismos concretos de coordenação (por exemplo, conselhos, comitês, etc.) e também menções mais genéricas (por exemplo, ações no futuro para aumentar a coordenação)
[14] Idem.

existência de um orçamento vinculado às iniciativas contidas no documento. Embora não queira dizer que as estratégias não estão necessariamente respaldadas por um orçamento (uma vez que nossa análise se limitou à leitura das estratégias sem aprofundar os orçamentos públicos dos países selecionados), essa tendencia indica que este pode ser o caso para muitas 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 então destinar um orçamento especial às iniciativas que fazem parte do documento. Seja qual for o modelo escolhido por um país, o aspecto fundamental é garantir que as iniciativas incluídas na estratégia tenham os recursos necessários para serem executadas adequadamente.

Gráfico 2



A análise por região indica que os países da América Latina apresentam uma tendencia 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 está presente em menor escala do que nos países do Norte Global.

Olhando para a perspectiva evolutiva das estratégias (gráfico 3), alguns padrões são interessantes. Em primeiro lugar, se nota que as estratégias de 2ª e 3ª geração tendem a

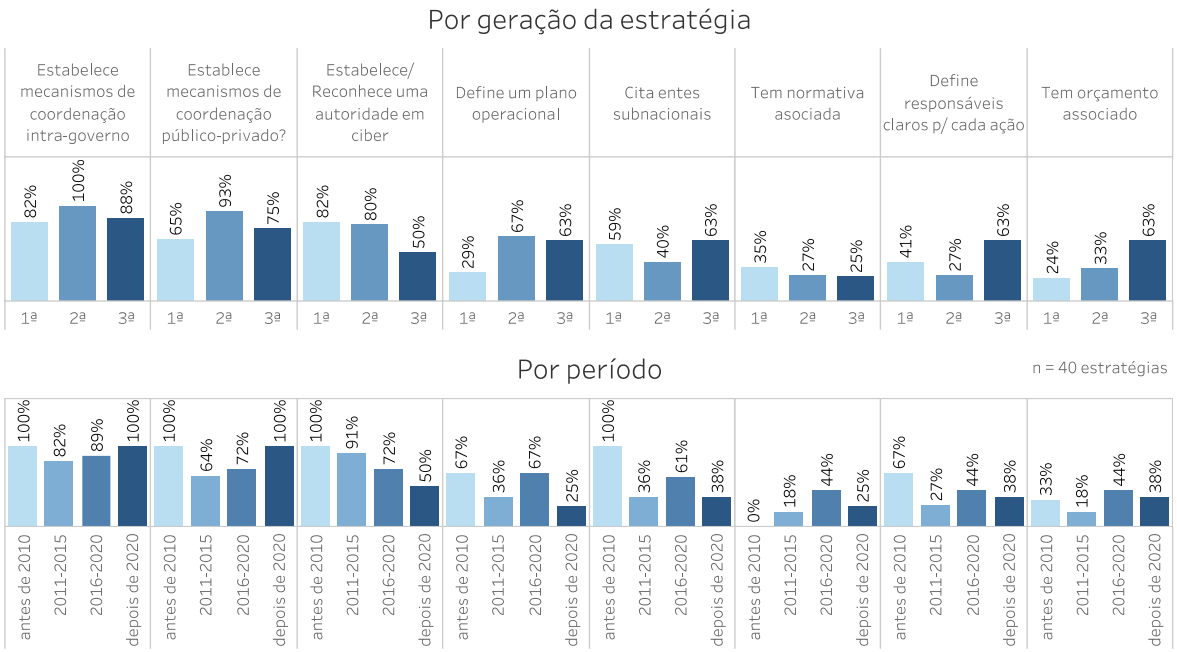
definir um plano operativo (seja na própria estratégia ou seja previsto para a fase da implementação), indicando que as estratégias mais recentes tendem a ser menos teóricas e mais orientadas a ações concretas. Relacionado a este ponto, também se nota um salto grande quando olhamos para a terceira geração de estratégias no que tange à definição clara de responsáveis para cada ação. Com efeito, nas estratégias de 3ª geração, 63% definem mais claramente quem é responsável pelas ações contidas no plano, enquanto nas da segunda geração a frequência era somente 27%.

Na análise evolutiva, nota-se uma tendencia de crescimento a ter orçamento vinculado às estratégias na terceira geração (de 24% na primeira geração para 63% na terceira), também reforçando a percepção indicada na seção de grandes tendencias de que as estratégias estão se tornando cada vez mais operativas e executivas e menos teóricas.

Gráfico 3

Área Focal: Governança e Institucionalidade

Evolução da presença dos mecanismos nas estratégias analisadas



Em relação aos mecanismos de *enforcement* associados, as estratégias não costumam incluir obrigações e/ou punições pelo não seguimento. No geral, a linguagem das estratégias assume um 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 comités que acompanharão a implementação, dentre outros.

BOX de 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 intersecretarial e colaboração com o setor privado e sociedade civil.

É importante destacar que o processo de elaboração da estratégia foi participativo, contando com a participação de órgãos do governo, academia, *think tanks* e do setor privado. Um processo participativo auxilia na fase da implementação, uma vez que os diferentes atores já se encontram apropriados 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, se nomeia em cada ministério/órgão um ponto focal responsável que atua como elo de 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 planeamento de seu departamento. A cooperação e a troca de informações entre os responsáveis é coordenada pelo Ministério dos Assuntos Económicos 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 dentro do governo, a Estratégia também delineia um plano para cooperação com os centros de competência, as universidades, as instituições de investigação e os parceiros do setor privado com conhecimentos e capacidades neste domínio. Aqui se destacam o Centro de Excelência de Ciberdefesa Cooperativa da OTAN (CCD COE) e a E-Governance Academy (EGA), um centro de consulta e de reflexão para a sociedade da informação. A Estratégia também cita outros parceiros para esta troca de conhecimento e expertise.

4.3. Métricas e indicadores

PONTOS CHAVE DA SEÇÃO

- **Incipiência da presença de indicadores.** Dentre as estratégias atualmente vigentes, apenas duas possuem algum tipo de indicador quantitativos e/ou métricas de sucesso. Ampliando a análise para ver a evolução da presença de indicadores, entre as 40 estratégias analisadas, além das estratégias em vigor mencionadas, apenas mais duas possuem algum tipo de métrica de sucesso.

Além dos principais elementos que garantem uma 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 17 estratégias em vigor, apenas uma tem indicadores quantitativos (Estônia, 2019) e uma tem metas qualitativas (França, 2021). Ampliando a análise para incluir as estratégias antigas, também há duas estratégias de segunda geração que tem métricas qualitativas de sucesso (Reino Unido, 2016 e Australia, 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 implementação da estratégia. Estes documentos adicionais não entraram no escopo da análise.

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

Abaixo apresentamos um resumo do tipo de indicadores contido 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 se destacam:

- Percentual de residentes que evita 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 ser expostos a alguma vulnerabilidade online;
- Percentual de empresas que usam uma política de segurança de TIC oficinal;
- Nível de conscientização e competências em cibersegurança entre os funcionários do setor público;
- Déficit da força de trabalho no setor.

O caso da Estratégia da França de 2021 é interessante, pois se trata de uma Estratégia bastante focada no aspecto econômico da cibersegurança, reiterando mais uma vez a tendencia a que as estratégias mais novas do Norte Global incluam os temas de prosperidade econômica com maior frequência. Embora não se trate de indicadores de monitoramento da Estratégia especificamente, destacamos esta estratégia pois ela inclui metas qualitativas que orientam a estratégia. Entre elas, se destacam: triplicar as vendas do setor de cibersegurança, duplicação do número de empregos no setor, aumento de 20% do número de patentes registradas, dentre 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. Neste caso, a estratégia define resultados estratégicos esperados e medidas que indicam o sucesso do atingimento desse resultado. Contudo, entendemos que este formato dificulta um monitoramento mais objetivo do atingimento ou não dos resultados esperados. Veja abaixo alguns exemplos de como essa abordagem é utilizada:

- Resultado esperado: O Reino Unido tem a capacidade de gerenciar e responder com eficácia a incidentes cibernéticos para reduzir os danos que eles causam ao país e combater os adversários cibernéticos.

Indicativos de sucesso:

- Uma proporção maior de incidentes é relatada às autoridades, o que leva a uma 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.

4.4. Desafios e ameaças

PONTOS CHAVE DA SEÇÃO

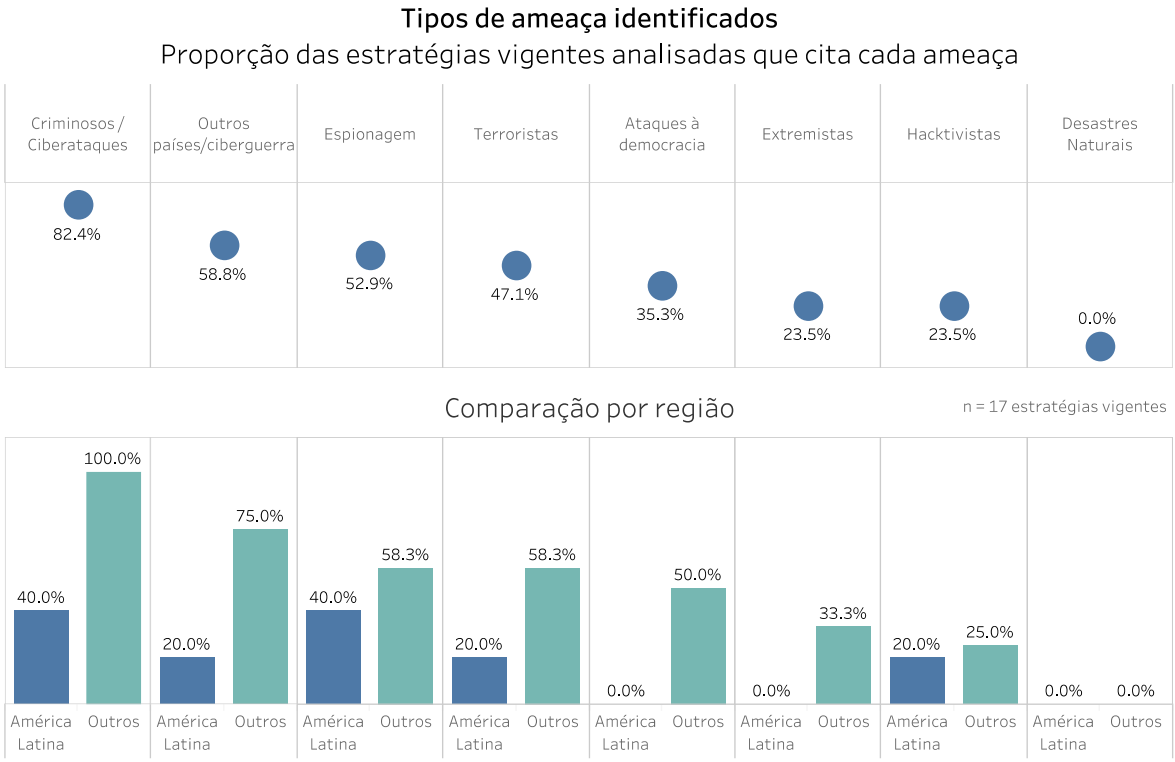
- **Componente de ameaças e desafios:** é comum que as estratégias incluam alguma seção ou capítulo dedicado aos tipos de ameaça e desafios relacionados à cibersegurança em seu contexto.
- **Tipos comuns de ameaça:** entre os tipos mais comum de ameaça mencionados nos documentos, destacam-se: (i) ciberataques criminosos (82,4%); (ii) ciberguerra ou outros países (58,8%); (iii) espionagem (52.9%); e (iv) terrorismo (47,1%).
- **Evolução dos tipos de ameaça:** se percebe uma diminuição do foco em ataques terroristas e um aumento de novas ameaças como ataques à democracia.
- **Ataques à democracia:** a tendencia 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 estes 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, dentre os tipos de ameaça mais frequentes, destaca-se que 82,4% das estratégias analisadas citam ciberataques criminosos e cerca de 60% citam ataques

de outros países (ou ciberguerra) como ameaças recorrentes. Em seguida, temas de espionagem e terrorismo aparecem ocupando a terceira e quarta posição dentre as ameaças mais frequentemente identificadas.

Gráfico 4



Na comparação regional, alguns padrões interessantes são possíveis de captar. Uma primeira conclusão é que as estratégias do Norte Global da nossa amostra costumam incluir um apanhado das ameaças com maior frequência do que as estratégias da América Latina e do Caribe. Um 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 de terrorismo e de ataques à democracia está mais presente em estratégias fora do nosso continente.

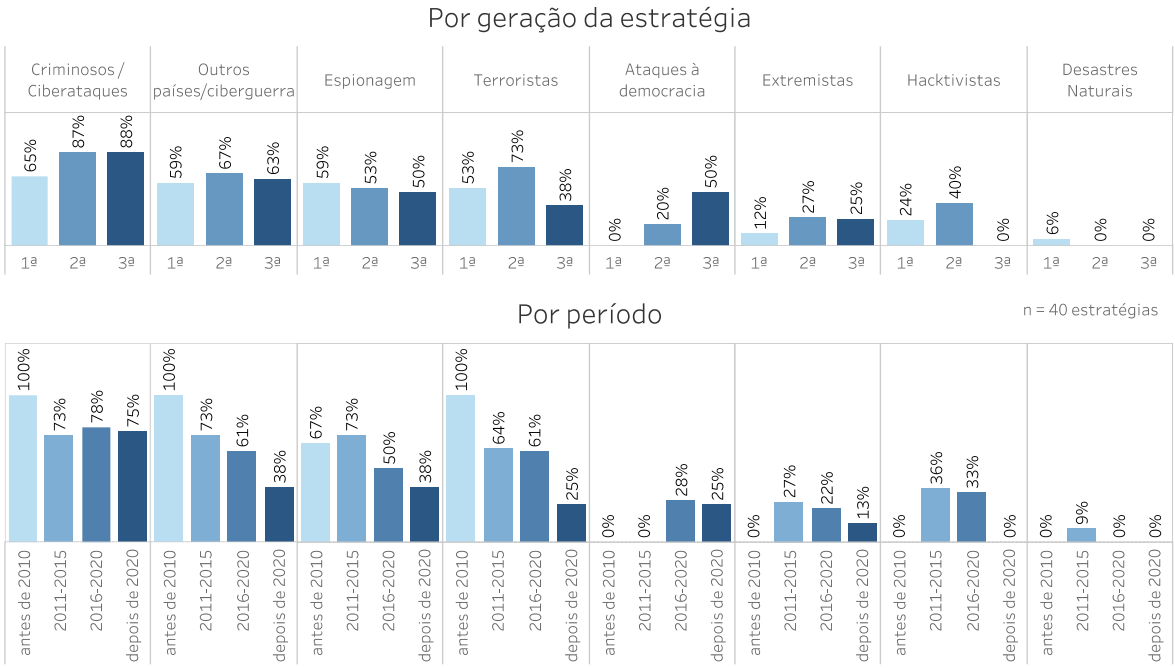
O gráfico 5 mostra a evolução da menção aos tipos de ameaça ao longo do tempo e por geração. Esta série comparativa permite perceber padrões interessantes vinculados a fatos históricos e geopolíticos. Por exemplo, destaca-se a gradual diminuição das estratégias que citam explicitamente a terroristas como as principiais ameaças enfrentadas por seu país em matéria de cibersegurança (o auge deste tipo de ameaça fora antes de 2010). Outro destaque interessante é o forte crescimento de ameaças focadas em ataques à democracia na terceira geração de estratégias, indicando uma possível tendencia para os próximos anos. Casos como

a interferência russa nas eleições americanas e outros episódios podem estar na raiz deste salto recente.

Gráfico 5

Tipos de ameaça identificados

Evolução da presença das ameaças citadas nas estratégias analisadas



Em relação aos desafios da área de cibersegurança, não foi possível realizar uma categorização padrão para realizar uma análise comparada. Isso se deve 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 de nossas sociedades no ciberespaço. Nessa linha, as estratégias mais modernas têm enfatizado como ataques cibernéticos cada vez mais representam ataques à nossa forma de vida e valores. Nesse quesito, muitas das estratégias mencionam os desafios e ameaças relacionados à proteção das infraestruturas críticas e dos serviços essenciais. Também é comum 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 esta situação (as medidas que têm sido priorizadas serão exploradas na seção sobre capacidades).

Por fim, ainda em um âmbito amplo de desafios mencionados, vale lembrar que algumas estratégias, no 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).

BOX 1 – 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 conceitos que são interessantes de discutir: 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 Estado.

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 na área de segurança cibernética. 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 uma relação direta com a melhoria da maturidade da segurança cibernética da Espanha. Não apenas por causa de seu momento oportuno, mas também por causa de sua constante evolução ao longo do tempo.

Fontes: Estratégias de cibersegurança da Espanha

4.5. Princípios

PONTOS CHAVE DA SEÇÃO

- **Princípios:** 58.8% das estratégias analisadas têm uma seção dedicada a compartilhar seus princípios.
- **Direitos Humanos**: o princípio mais comum, citado em 80% das estratégias vigentes, se refere a temas relacionados à direitos humanos ou proteção dos direitos fundamentais.
- **Prosperidade Econômica:** nota-se uma tendencia, principalmente fora da América Latina, ao crescimento da menção de princípios relacionados à prosperidade econômica, indicando uma possível tendencia a 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 um aumento significativo de princípios relacionados à transparência nas estratégias de terceira geração.

Pessoas diferentes têm entendimentos diferentes sobre o que constitui cibersegurança. 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. Escritos em termos gerais, eles fornecem uma referência robusta, mas flexível, para ajudar a orientar as decisões sobre essas questões.

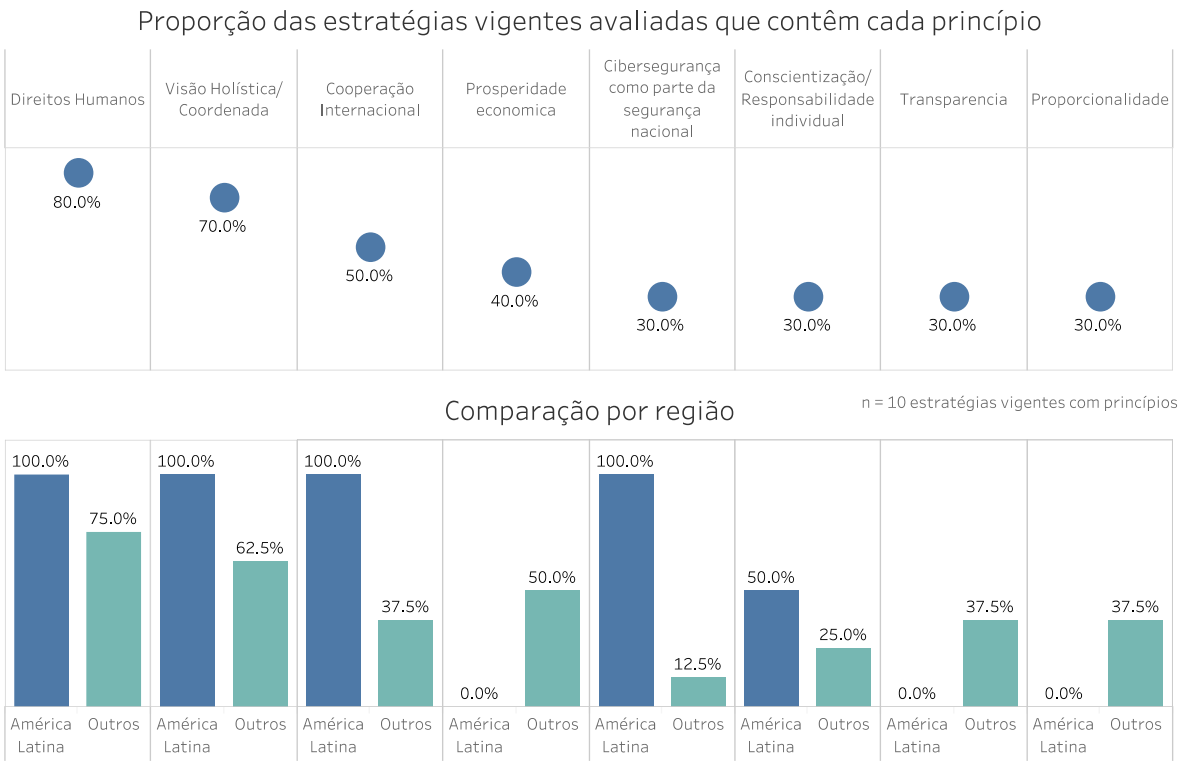
Como evidenciado na seção sobre as estruturas das estratégias, 58.8% incluem uma seção dedicada aos princípios. Em termos de formato, as estratégias usam diferentes graus de detalhes em seus princípios, desde palavras isoladas até frases inteiras que incorporam diretrizes estratégicas. Os gráficos 6 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 podemos 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. Por exemplo, podemos observar uma diminuição nas 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. Este fato pode indicar que nas primeiras estratégias o tema entrava de forma transversal como princípio, mas que agora há uma tendencia a que o tema seja tratado como um objetivo estratégico com iniciativas associadas.

Nossa hipótese é que os temas entram como princípios quando os países consideram o tema importante e transversal, mas quando ainda não há muita clareza sobre como o tema pode ser operacionalizado na prática. Uma vez que há maior clareza, os temas passam a se tornar objetivos com graus de concretude maior.

Gráfico 6



Dentre os princípios mais proeminentes nas estratégias, o tema dos direitos humanos e direitos fundamentais se destaca de maneira significativa. Embora diferentes estratégias possam abordá-lo de formas distintas, notamos que 80% 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 livre) incluem:

- Consideramos a proteção e a promoção dos direitos e liberdades fundamentais tão importantes no espaço cibernético quanto no ambiente físico (Estônia, 2019)
- Protegeremos e promoveremos rigorosamente nossos valores fundamentais. Esses valores incluem a democracia, o estado de direito, a liberdade, governos e instituições

abertos e responsáveis, direitos humanos e liberdade de expressão (Reino Unido, 2016).

- Equilibrar os direitos individuais com a segurança cibernética: Alcançar um 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 parte (Argentina, 2019).

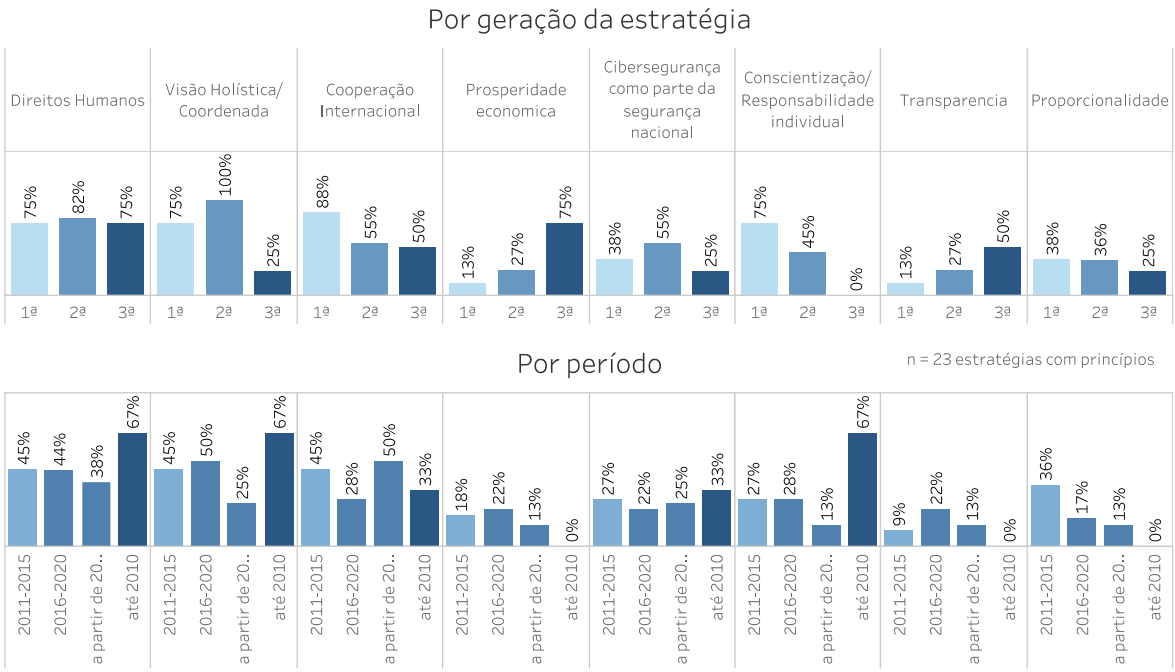
Outro destaque é que 70% das estratégias atualmente vigentes incorporam algum tipo de princípio que enfatiza a necessidade de coordenação ou que considera a cibersegurança como um tema holístico e interconectado. Em determinados casos, essa coordenação é mencionada em relação a diferentes atores, tanto 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 livre) elucidativos incluem:

- Trabalharemos em parceria. Somente trabalhando com as Administrações Devolvidas, todas as partes do setor público, empresas, instituições e o cidadão individual, poderemos proteger com sucesso o Reino Unido no ciberespaço (UK, 2016).
- Garantir a responsabilidade compartilhada entre várias partes interessadas, promovendo o máximo de colaboração e cooperação. Isso, 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 olhamos para os padrões de evolução dos princípios (Gráfico 7), alguns pontos chamam a atenção e podem dar pistas sobre as tendencias recentes de evolução das estratégias.

Gráfico 7

Evolução da presença do princípio nas estratégias analisadas



Um ponto que merece destaque é o princípio da prosperidade econômica. Nota-se que há um padrão claro em relação às gerações de estratégias. Enquanto nas primeiras estratégias era menos comum se falar de prosperidade econômica, 75% das estratégias da terceira geração possui um princípio relacionado ao tema. Esse dado pode indicar uma tendencia a que as estratégias mais recentes não tenham um 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, em relação a esse tema, a América Latina ainda não está dando ênfase a essa dimensão em suas estratégias. Nenhuma das estratégias vigentes analisadas na região destaca claramente a prosperidade econômica como um princípio orientador do documento, indicando uma área potencial de crescimento e desenvolvimento para futuras políticas e estratégias na região. Os exemplos abaixo ilustram como o princípio se manifesta em algumas estratégias:

- Vemos a segurança cibernética como um facilitador e amplificador do rápido desenvolvimento digital da Estônia, que é a base para o crescimento socioeconômico do país. A segurança deve apoiar a inovação e a inovação deve apoiar a segurança. (Estônia, 2019)
- Daremos prioridade à capacidade dos cidadãos e das empresas de operar no ciberespaço de forma segura e protegida para que possam maximizar os benefícios

econômicos e sociais da tecnologia digital e exercer seus direitos legais e democráticos (Reino Unido, 2022)

- Incentivar a 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 veremos na seção sobre capacidades, cerca de 90% das estratégias vigentes analisadas possui pelo menos uma medida relacionada a programas de conscientização. Isso indica uma transferência do tema de um princípio transversal para uma área focal com ações especificas.

Por fim, vale destacar o crescimento do princípio da transparência. Esse princípio indica uma 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.

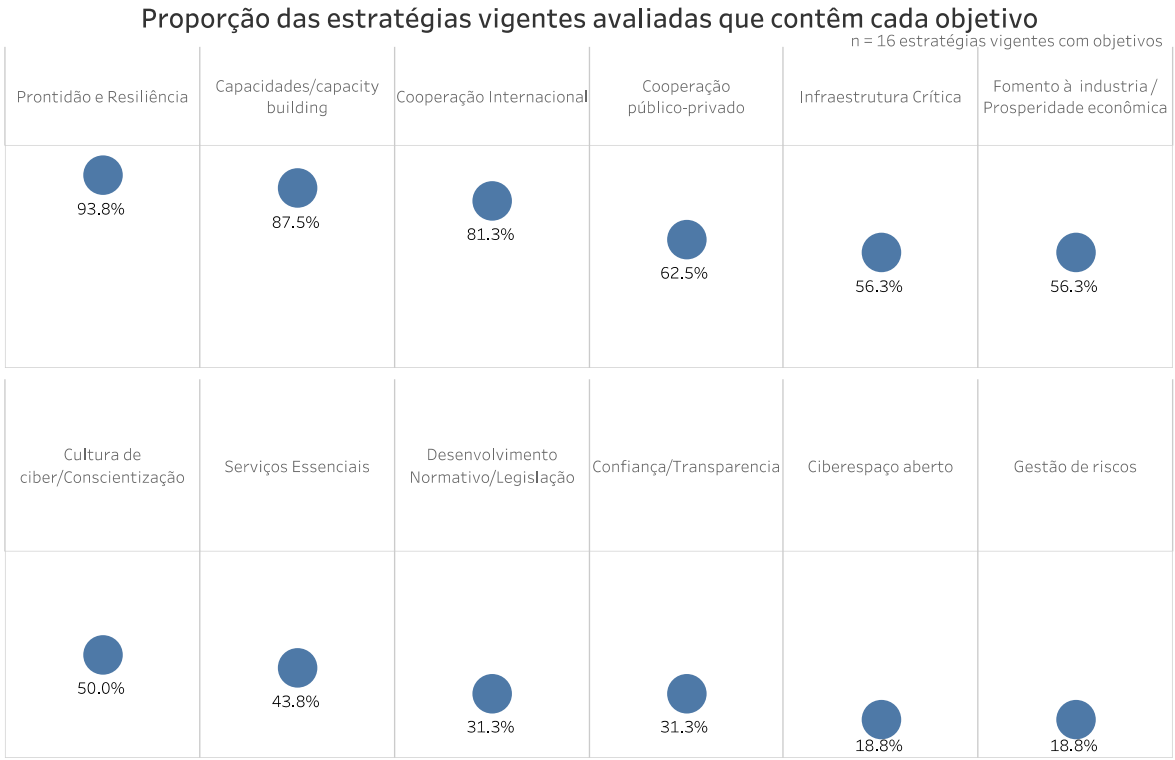
4.6. Objetivos estratégicos

PONTOS CHAVE DA SEÇÃO

- **Objetivos:** 93.3% das estratégias analisadas define objetivos estratégicos.
- **Prontidão e Resiliência:** 93.8% das estratégias analisadas possui pelo menos um objetivo relacionado aos temas de prontidão e resiliência.
- **Capacidades:** 87.5% das estratégias analisadas possui pelo menos um objetivo para fortalecimento das capacidades em cibersegurança do país.
- **Prosperidade Econômica:** assim como nos princípios, nota-se um aumento da presença de objetivos ligados ao fomento da indústria de cibersegurança, principalmente nos países do Norte Global (71% nas estratégias de 3ª geração, comparado com 29% nas de 1ª geração).
- **Cooperação internacional:** O aumento da presença de objetivos estratégicos ligados à cooperação internacional indica uma transferência do tema da categoria de princípios para a categoria de objetivos com ações associadas.
- **Cooperação público-privada**: as estratégias da 3ª geração apresentem com mais frequência objetivos estratégicos ligados à cooperação público-privado (71% comparado com 47% na 2ª geração).
- **Transparência:** as estratégias de 3ª geração apresentam com mais frequência objetivos ligados à transparência (40% comparado com 0% na 2ª geração)

Os objetivos são o coração das estratégias e, como vimos, somente uma das estratégias 40 estratégias analisadas não os definem explicitamente. Assim como analisamos 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, identificamos 8 temas que cobrem a maior parte dos objetivos presentes nas estratégias e, no gráfico 8, destacamos 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, este gráfico captura somente o nível de objetivos estratégicos. Por essa limitação, também é importante ser cautelosos nas conclusões tiradas. Os subobjetivos serão tratados nas áreas focais exploradas nas próximas seções.

Gráfico 8



Pode-se notar que 93,8% das estratégias vigentes analisadas possui pelo menos um objetivo que inclui temas de prontidão e resiliência. Em segundo lugar, os objetivos de fortalecimento das capacidades do país em cibersegurança e algum objetivo relacionado à cooperação internacional aparecem como em 87,5% e 81,3% das estratégias analisadas, respectivamente. Em quarto lugar, encontram-se objetivos que explicitam uma necessidade de maior cooperação público-privado, aparecendo em quase dois terços das estratégias. Objetivos relacionados à Infraestrutura Crítica também são comuns nas estratégias vigentes, com mais da metade delas incluindo o tema explicitamente no nível mais alto dos objetivos. Os demais temas comuns estão evidenciados no gráfico acima.

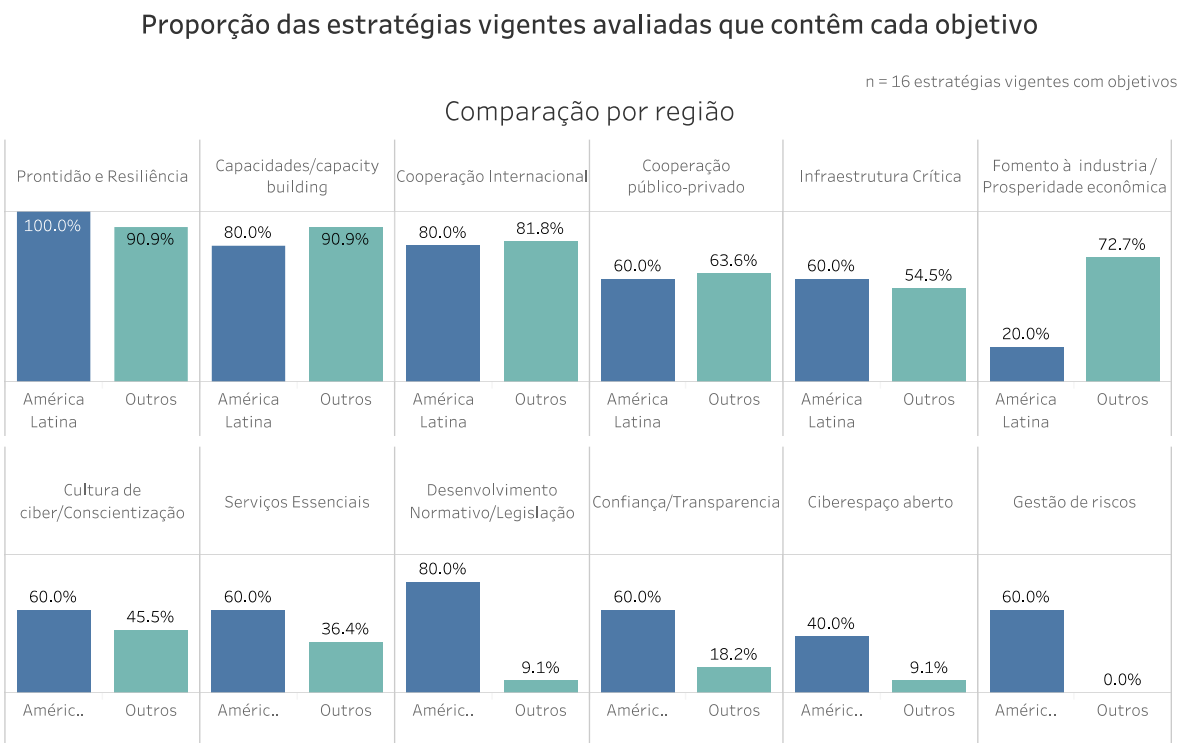
Em relação à análise por região (gráfico 9), nota-se que em muitas categorias não parece haver diferenças tão significativas entre as regiões estudadas. Contudo, alguns temas reforçam tendencias que vimos nas seções anteriores e merecem destaque.

Em primeiro lugar, assim como o princípio da prosperidade econômica não estava muito presente nos princípios nas estratégias da América Latina, nota-se que objetivos estratégicos vinculados ao fomento da indústria de cibersegurança também não estão muito presentes na região. Ao mesmo tempo que o tema não aparece muito 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 comparado com os 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.

Gráfico 9

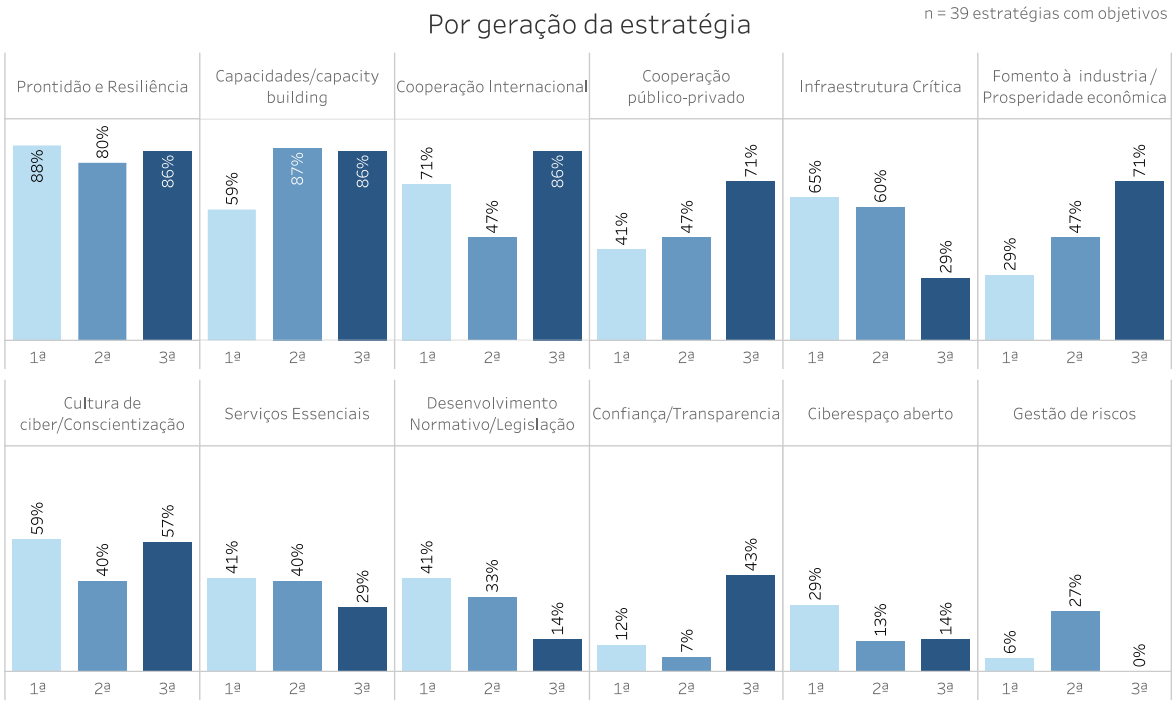


A evolução dos objetivos pela ótica da geração (gráfico 10) também aporta inisghts interessantes sobre possíveis tendencias. Em termos de geração das estratégias, nota-se que os países que estão na terceira geração de suas estratégias, tem uma presença maior dos temas de cooperação internacional (demonstrando o argumento que fizemos na seção dos princípios de que houve uma transferência do tema da cooperação internacional de ser um princípio para ser um objetivo estratégico). Também é possível apurar uma redução na presença de objetivos de primeiro nível explicitamente enfocados na proteção da infraestrutura crítica. Entendemos 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 (tema será explorado na área focal de infraestrutura crítica). Por fim, se nota um aumento de objetivos relacionado ao fomento da indústria, conforme já destacamos anteriormente.

Por fim, o aumento do tema da transparência que destacamos na seção dos princípios também se encontra espelhado em um aumento do tema como objetivo estratégicos, reforçando a tendencia identificada a que as estratégias de cibersegurança levem aspectos de transparência e de aumento da confiança mais a sério.

Gráfico 10

Evolução da presença do objetivo nas estratégias analisadas



Por não encontrar padrões interessantes na análise por ano para este tópico, optamos por não incluir o gráfico que compara os períodos. As tendencias mais interessantes podem ser capturadas avaliando a evolução por geração.

Em relação aos números de macro objetivos, não encontramos um padrão de aumento ou diminuição ao longo dos anos. A grande maioria das estratégias foca em 4 ou 5 pilares, objetivos estratégicos ou grandes áreas de atuação. Nos quadros abaixo, incluímos exemplos qualitativos de como os objetivos estratégicos são apresentados em três estratégias selecionadas:

Exemplos de objetivos
Estônia 2019

OBJETIVO 1 - Uma 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 a Estônia.

OBJETIVO 3 Uma contribuição internacional de destaque

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

OBJETIVO 4 Uma sociedade com alfabetização cibernética

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

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

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 de quaisquer 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

4.7. Áreas focais de ação

Esta seção do estudo analisa as áreas de ação das estratégias, analisando temas incluídos em formatos de iniciativas, subobjetivos, linhas de ação, pilares de ação ou outras categorias similares presentes nos documentos. As áreas focais priorizadas para análise incluem 7 categorias priorizadas no documento mencionado do ITU e 2 categorias adicionais. Dentro de cada área, diferentes temas/ações foram priorizados para avaliação.

4.7.1. Área focal: Gestão de Riscos

PONTOS CHAVE DA SEÇÃO

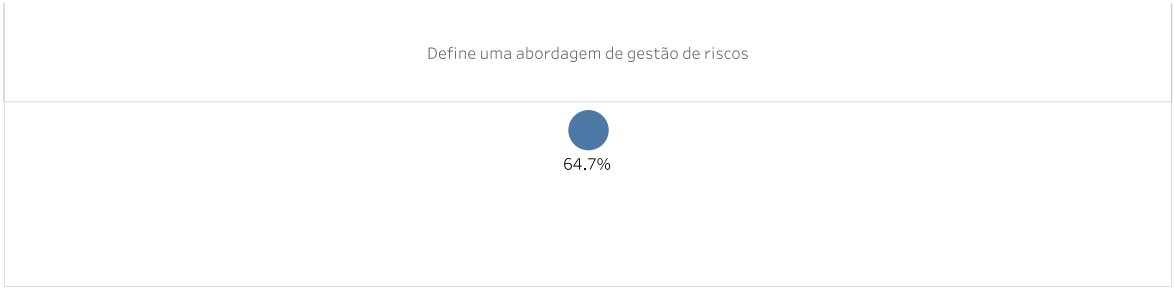
- Abordagem de gestão de riscos: há uma tendência de aumento da inclusão de uma abordagem de gestão de riscos como parte das ações da estratégia, embora não se entre no detalhe operacional de definir uma metodologia propriamente dita.

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 nossa análise tenha identificado que esta definição costuma se dar em documentos complementares e não na própria estratégia.

Das estratégias estudadas, 64,7% das que estão em vigor definem uma abordagem de gestão de riscos. Este valor aumenta para 80% se considerarmos apenas as estratégias latino-americanas. Se observarmos como esse tópico está presente nas estratégias de acordo com a geração ou o período, veremos um 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.

Gráfico 11

Área Focal: Gestão de Riscos
Proporção das estratégias vigentes analisadas que menciona a abordagem



Comparação por região

n = 17 estratégias vigentes

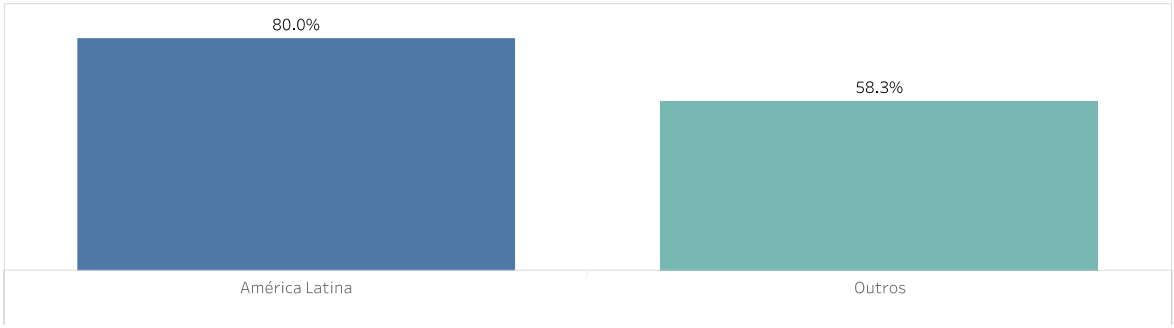
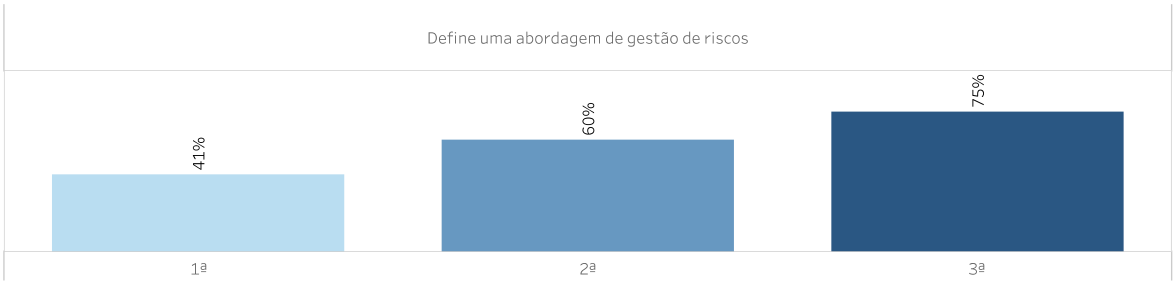


Gráfico 12

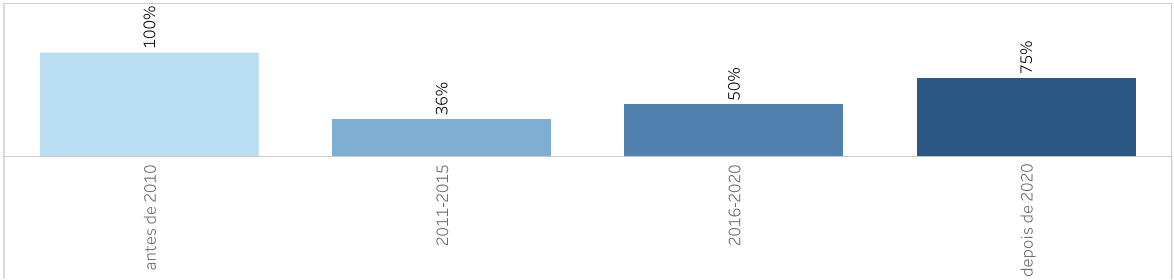
Área Focal: Gestão de Riscos
Evolução da presença da abordagem nas estratégias analisadas

Por geração da estratégia



Por período

n = 40 estratégias



Vale destacar que as estratégias que mencionam a necessidade de uma abordagem de gestão de riscos dificilmente entram em um nível de detalhe técnicos ou operacional a respeito, delegando essa função a outros documentos complementares. Por exemplo, estratégias como a da Espanha que não tem uma metodologia explícita na estratégia, mas tem uma metodologia implementada em nível nacional, podendo indicar uma tendencia de que as estratégias não entrem em um nível de detalhe técnico tão aprofundado.

Embora não o tenhamos incluído no gráfico, também avaliamos a definição de políticas de segurança cibernética, verificando que poucas estratégias em vigor entram em um nível tão detalhado. Um exemplo interessante é o caso do Japão, onde um documento chamado "Guidelines for Information Security Policy for Local Government" (Diretrizes para a política de segurança da informação para o governo local) foi estabelecido como referência para os governos locais na formulação e revisão de políticas de segurança da informação.

BOX 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 e é na iniciativa (e não na estratégia em si) que todos os aspectos necessários para sua implementação são detalhados.

A definição da abordagem, metodologia de gestão e 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 se 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.

4.7.2. Área focal: Resiliência e Prontidão

PONTOS CHAVE DA SEÇÃO

- Capacidades para resposta a incidentes: Praticamente 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 que assumiu um papel de liderança na área de segurança cibernética e é um requisito fundamental para gerar conhecimento, melhorar as capacidades e fortalecer os laços entre os diferentes atores envolvidos na proteção de um país. Esse tópico está presente em 88,2% das estratégias vigentes e tem uma trajetória de crescimento ao longo das gerações.
- Planos de contingência para gestão de crises: embora esse tópico não seja tão presente nas estratégias vigentes (47,1%), podemos ver que há um crescimento do tema nas estratégias de terceira geração (63%).

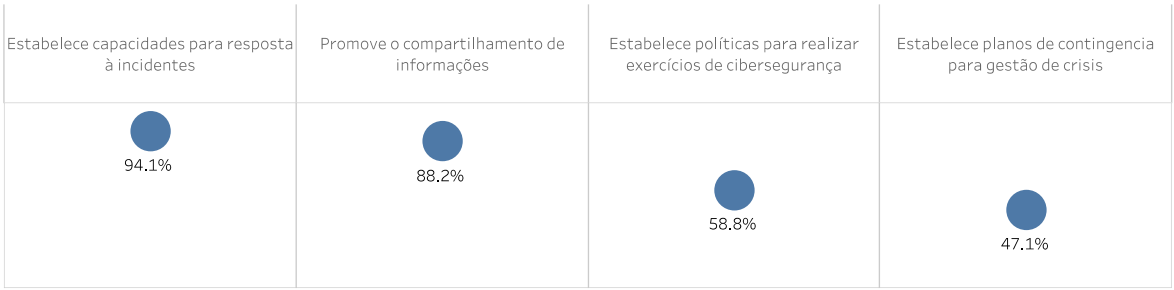
Como será visto em todos os tópicos dessa área focal, a proteção e a resiliência têm grande destaque em todas as estratégias, especialmente nas atuais. Há várias iniciativas que buscam melhorar a proteção e a resiliência de forma transversal. Um exemplo disso é a Lei de Resiliência Cibernética da União Europeia[15], que busca estabelecer requisitos de segurança cibernética para produtos com elementos digitais. Outro exemplo é a Lei de Resiliência Operacional Digital da UE[16], que busca regulamentar e unificar a legislação para a gestão de riscos digitais no setor financeiro.

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

Gráfico 13

Área Focal: Prontidão e Resiliência

Proporção das estratégias vigentes analisadas que menciona cada mecanismo



Comparação por região

n = 17 estratégias vigentes

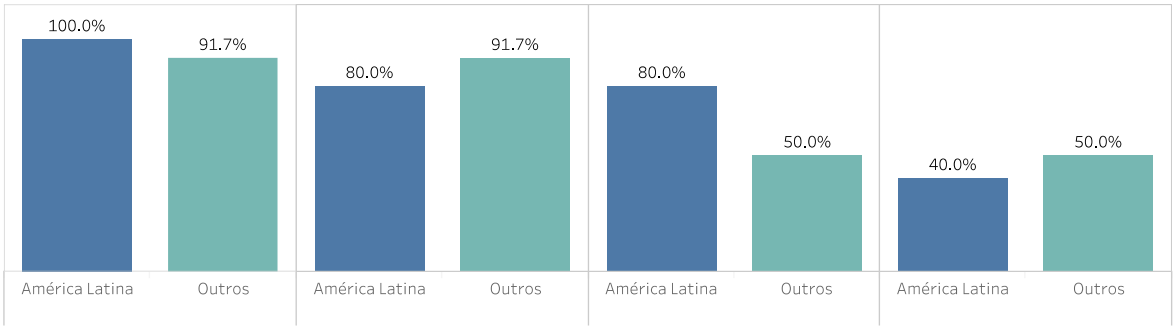
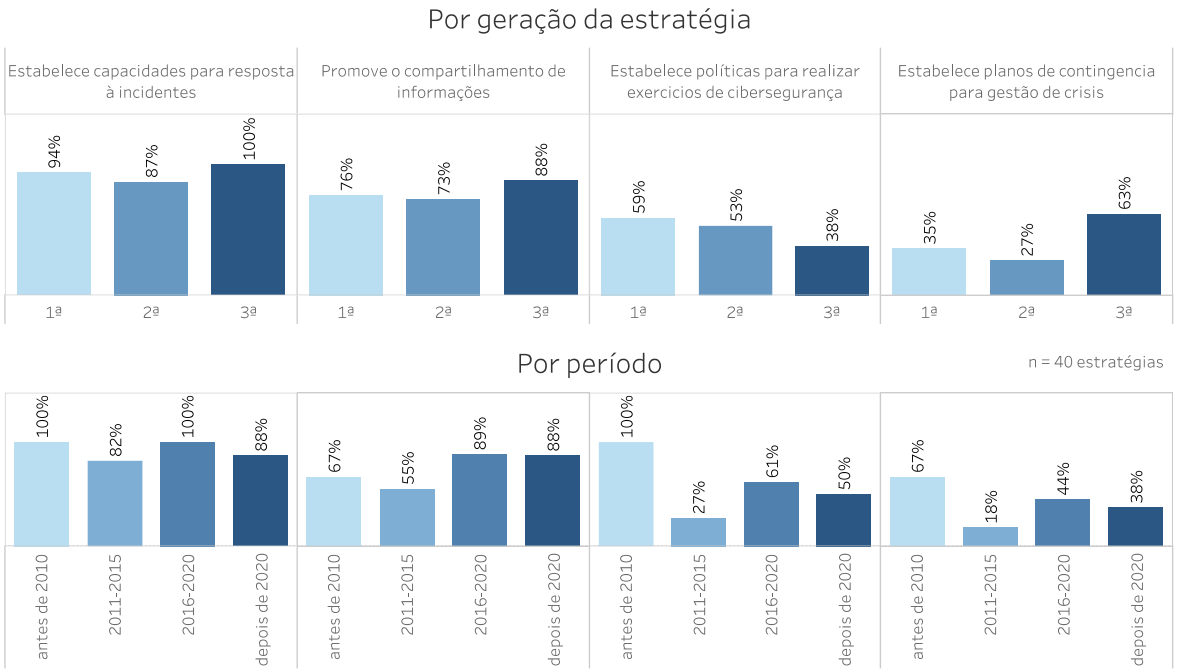


Gráfico 14

Área Focal: Prontidão e Resiliência
Evolução da presença do mecanismo nas estratégias analisadas



A capacidade de resposta a incidentes é um tópico de interesse para todos os países, e podemos ver como ela aparece explicitamente em 93,3% de todas as estratégias atuais, atingindo 100% na América Latina. Diferentemente de outros tópicos, o tema de capacidades 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. Se tomarmos 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 CSIRTs 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.

Como se sabe, as ameaças que existem 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 e responder a incidentes 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. Se observarmos os dados deste estudo em relação a essa questão, 88,2% das estratégias atuais promovem o compartilhamento de informações, uma tendência que vem aumentando constantemente ao longo dos anos. 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[17], 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[18] (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 de segurança cibernética, 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 que são orientados para diferentes públicos, como exemplo podemos ver dois:

- Exercícios orientados às equipes técnicas: a infraestrutura de uma organização é simulada (da forma mais realista possível) e cenários em que as equipes técnicas enfrentam diferentes tipos de incidentes são simulados de forma controlada. 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 tomadores de decisão, os Table Top Exercises são usados com frequência. Se trata de cenários falados que simulam incidentes nos quais todos os envolvidos devem tomar decisões que afetam a situação e o resultado final do incidente. Esses exercícios podem ser realizados dentro de uma organização, em nível nacional ou internacional.

Embora apenas 58,8% das estratégias atuais levem em conta esse tipo de exercício, isso não quer dizer que o tema não seja considerado.

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. Se observarmos as estratégias atuais, apenas 53,3% delas fazem menção direta ao tópico; no entanto, podemos ver que, para as terceiras gerações, esse valor sobe acentuadamente para 63%. De acordo 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."

[17] Cyber Threat Intelligence Integration Center - https://www.dni.gov/index.php/ctiic-home
[18] ISC2 Cybersecurity Workkforce Study - https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196

BOX 2 – ESTUDO DE CASO

ESTRATÉGIAS DE CIBERSEGURANÇA NA COLOMBIA

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 que não é 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 considera que os principais desafios são os pontos fracos na capacidade do Estado de lidar com as ameaças na época (muitos permanecem até hoje), a falta de coordenação nas 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 a: (i) 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) oferecer treinamento especializado em segurança e defesa cibernéticas, e (iii) Fortalecer aspectos da legislação e da adesão a instrumentos internacionais.

Para sua segunda edição (lançada em 2016), a Colômbia analisou as ações promovidas por sua primeira estratégia e a situação da segurança cibernética naquele momento e concluiu que havia aspectos a serem considerados que não haviam sido abordados na primeira versão da estratégia. 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.

Em sua 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 da 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 um insumo fundamental para o desenvolvimento da estratégia seguinte, seguindo assim um processo evolutivo que leva em conta tanto os aspectos que ficaram pendentes quanto aqueles que estão se tornando mais importantes.

4.7.3. Área focal: Infraestrutura Crítica (IC) e Serviços Essenciais

PONTOS CHAVE DA SEÇÃO

- Medidas para proteger as IC: esse é um tópico que está presente na maioria das estratégias (82,4% 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. Podemos ver que, ao longo dos anos, as estratégias mencionaram esse aspecto com mais frequência.
- Ativos de governo digital: observamos um 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 identificaçãoem maior frequência.

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 é surpreendente, pois esses ataques são vistos há décadas, desde 2010, quando um malware afetou uma fábrica iraniana[19], até mais recentemente (2021), quando a infraestrutura de suporte a gasodutos nos Estados Unidos foi comprometida por ransomware[20].

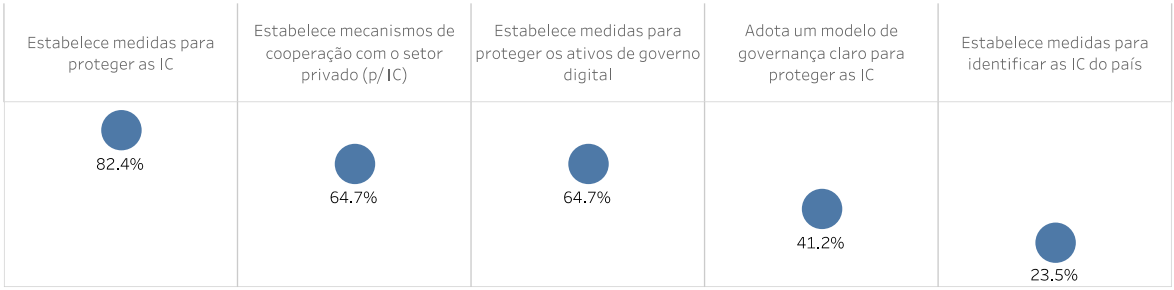
De acordo com a Diretiva Europeia 2008/114/EC de 8 de dezembro de 2008[21], a infraestrutura crítica é definida como "um elemento, sistema ou parte dele localizado nos Estados-Membros que é essencial para a manutenção de funções vitais da sociedade, saúde, segurança, proteção, bem-estar social e econômico 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".

[19] Stuxnet case - https://www.bbc.com/news/world-middle-east-11414483
[20] 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
[21] 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 = 17 estratégias vigentes

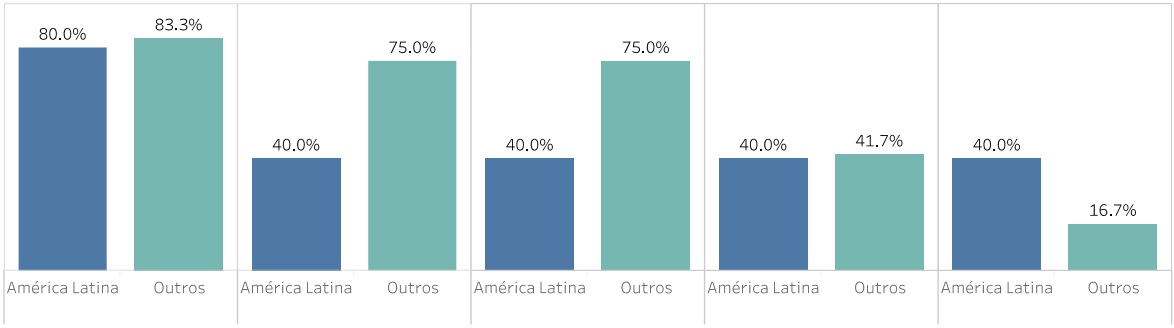
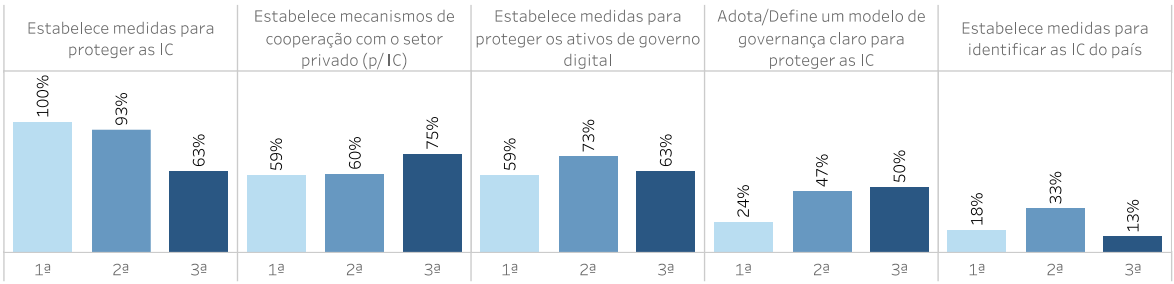


Gráfico 16

Área Focal: Infraestrutura crítica (IC) e Serviços Essenciais

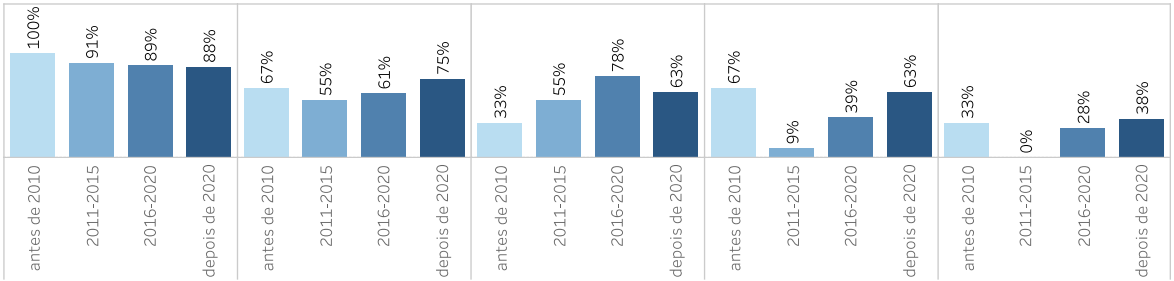
Evolução da presença do mecanismo nas estratégias analisadas

Por geração da estratégia



Por período

n = 40 estratégias



Entre os tópicos dessa área focal, o estabelecimento de medidas para proteger a IC tem uma presença de 82,4% nas estratégias atuais. Da mesma forma, podemos observar que, à medida que os países publicam novas edições de suas estratégias, esse tópico tem presença cada vez menor, sendo 93% na média das segundas estratégias e 63% na 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 uma mudança de nomenclatura para “serviços essenciais”.

A cooperação com o setor privado está presente em várias áreas focais da maioria das 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 "Estabelecimento de mecanismos de cooperação com o setor privado" esteja cada vez mais 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", vemos uma presença moderada nas estratégias latino-americanas, com 40%, e maior nas outras, com 75%. Observamos que parece haver havido um pico do tema na segunda geração, possivelmente coincidindo com a rápida evolução da digitalização de 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.

Com relação à adoção de um modelo de governança claro para a proteção de IC, o estudo não apresenta um padrão claro com relação aos anos de publicação e/ou edições das estratégias. Também é desafiador apreender o que é um modelo claro. De qualquer forma, deve-se observar que há uma heterogeneidade em como o tema é tratado. Em algumas estratégias a questão não é abordada claramente. Em outras, o tema está incluído na própria estratégia, como no caso do Chile, que busca alinhar a governança aos padrões internacionais. Por fim, em outros países o tema não se menciona detalhadamente na estratégia de segurança cibernética, mas existem estratégias específicas para a infraestrutura crítica, como no caso dos Estados Unidos.

O último tópico "Medidas para identificar a infraestrutura crítica do país" está claramente mais presente na América Latina, com 40%, 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 em sua terceira edição, o aborde.

4.7.4. 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 cinco tópicos sobre capacidades mais mencionados nas estratégias, destacam-se: Inovação e Pesquisa & Desenvolvimento (94,1%); Programas de conscientização (94,1%); Medidas na educação superior (88,2%); Medidas para formação de profissionais (88,2%) e Medidas na educação primária/secundária (76,5%).
- **Diversidade:** nota-se uma tendencia crescente a que as estratégias incluam 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.

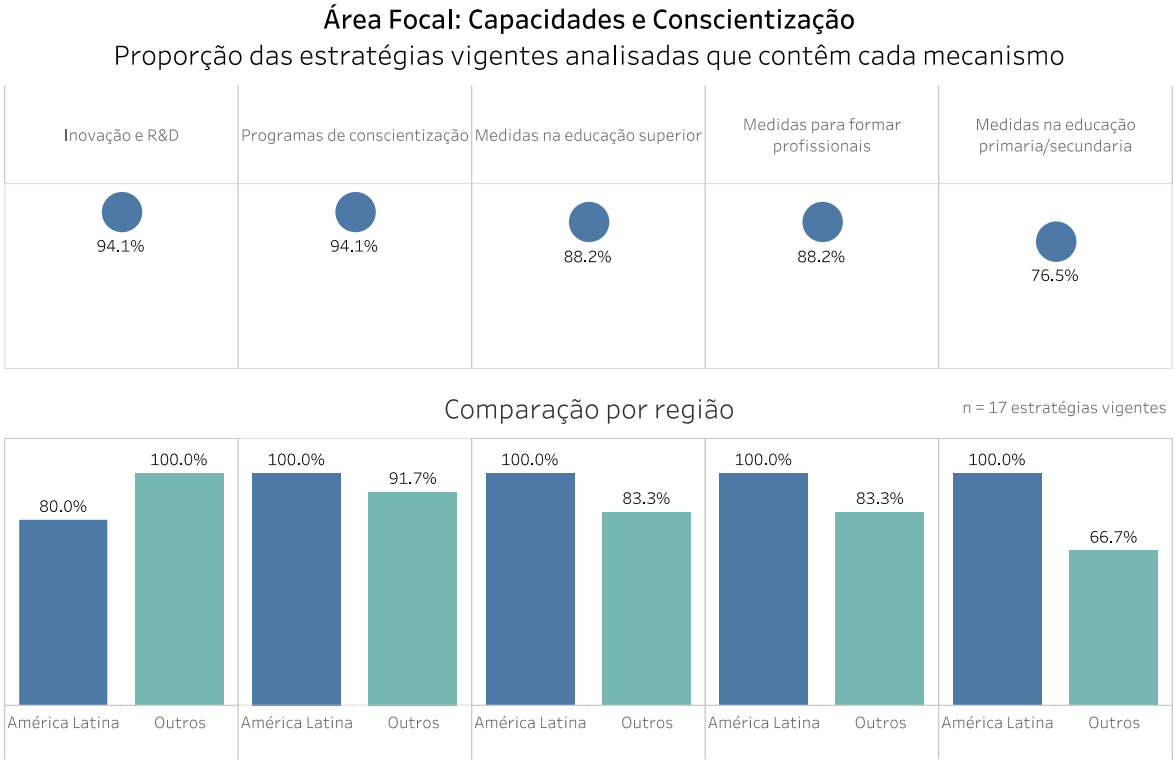
Entre os cinco tópicos mais mencionados nas estratégias relacionados a esse assunto, destacam-se: Inovação e Pesquisa & Desenvolvimento, programas de conscientização, medidas na educação superior, medidas para formação de profissionais e medidas na educação primária/secundária.

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 uma melhor compreensão dos desafios e das 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 94,1% 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 incluem:

- Preparação de um plano nacional de Pesquisa & Desenvolvimento em segurança cibernética que defina áreas de foco prioritário 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 neste domínio (Portugal, 2019).

Gráfico 17



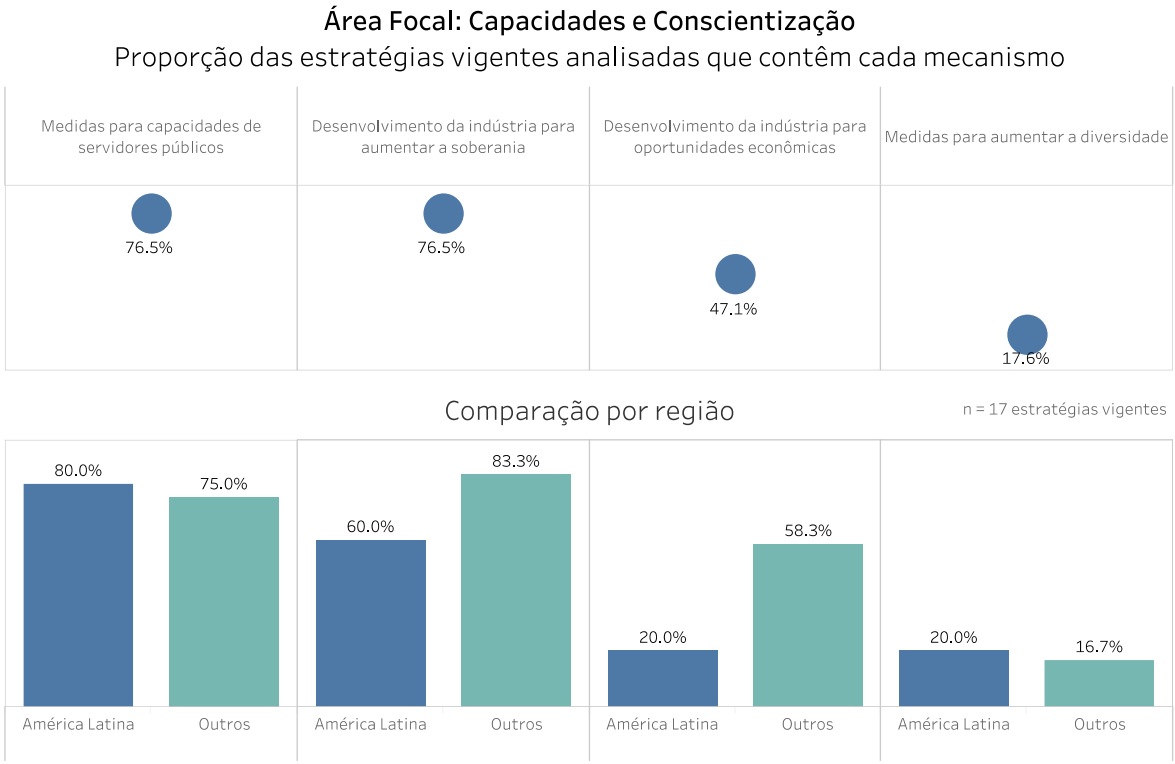
Em relação às medidas de conscientização, também com presença em 94,1% das estratégias vigentes, se apresentam alguns exemplos ilustrativos para materializar o tema:

- Criar um programa nacional de conscientização sobre segurança no espaço cibernético, abrangendo a sociedade como um todo. (Argentina, 2019).
- Serão realizadas 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 5 temas recorrentes nas ações relacionadas aos temas de capacidades, incluindo medidas para estudos técnicos, medidas para aumentar as capacidades e competências de servidores públicos, medidas ligadas ao desenvolvimento da indústria e medidas para aumentar a diversidade da força de trabalho.

Gráfico 18



Em relação à análise evolutiva no tempo (gráficos 19 e 20), uma das tendencias encontrada é o crescimento nas medidas destinadas à educação primária/secundária, refletindo um esforço para aumentar a conscientização das novas gerações sobre práticas seguras no ambiente virtual. Em paralelo, observa-se, a partir de 2016, um aumento nas iniciativas de formação de profissionais, 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 R & D, bem como de educação superior permaneceu sempre presente, oscilando entre 76% e 94%.

Gráfico 19

Área Focal: Capacidades e Conscientização
Evolução da presença dos mecanismos nas estratégias analisadas

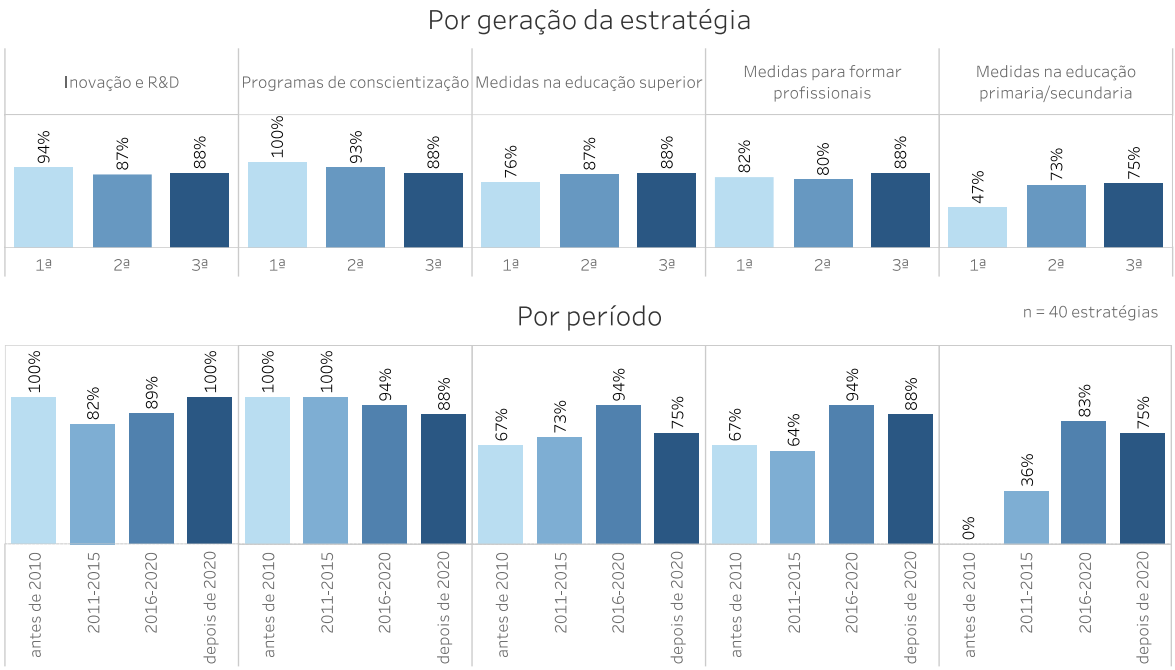
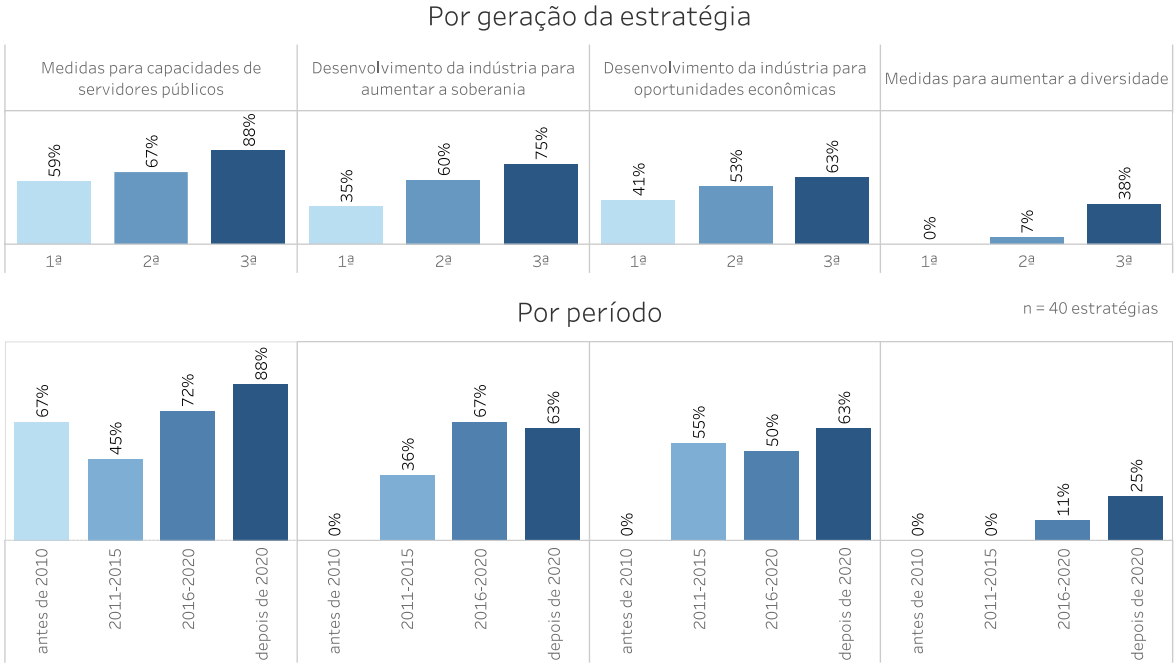


Gráfico 20

Área Focal: Capacidades e Conscientização
Evolução da presença dos mecanismos nas estratégias analisadas



A análise comparada também permite aferir uma tendencia a incluir com mais frequência medidas para desenvolvimento da indústria, especialmente com foco em aumentar a soberania (se passa de 35% na primeira geração das estratégias para 75% na última).

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 de estratégias, nas estratégias de terceira geração, medidas do tipo foram mencionadas em 38% das estratégias analisadas na amostra. Isso sugere uma mudança de mentalidade, com um reconhecimento crescente da importância de promover a inclusão e diversidade no setor de cibersegurança. Aqui dois exemplos (tradução livre) de como essas medidas são incluídas:

- Daremos 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 nossa segurança nacional, garantindo que aproveitemos 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 nosso país. Mulheres, pessoas de cor, profissionais e imigrantes de primeira geração, pessoas com deficiências e indivíduos LGBTQI+ estão entre as comunidades que estão subrepresentadas no campo (Estados Unidos, 2023)

4.7.5. Área focal: cooperação Internacional

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.

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 para o país na esfera internacional, em alguns casos se limitando a garantir a participação nos fóruns internacionais enquanto em outros aspirando a ocupar uma posição de influência nestes 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, se citam fóruns ou organizações internacionais especificas e, em outros, se priorizam as relações bilaterais. No caso dos países da Europa, existe um forte alinhamento com a atuação da Uniao Europeia no tema.

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

(i) Cooperação com outros países – nota-se que 100% das estratégias do Norte Global incluem medidas relacionadas a esta frente de trabalho

(ii) Alinhamento com iniciativas regionais/globais – 70,6% das estratégias vigentes analisadas citam a necessidade de atuar em blocos regionais ou globais.

Gráfico 21

Área Focal: Cooperação Internacional
Proporção das estratégias vigentes analisadas que contêm cada mecanismo

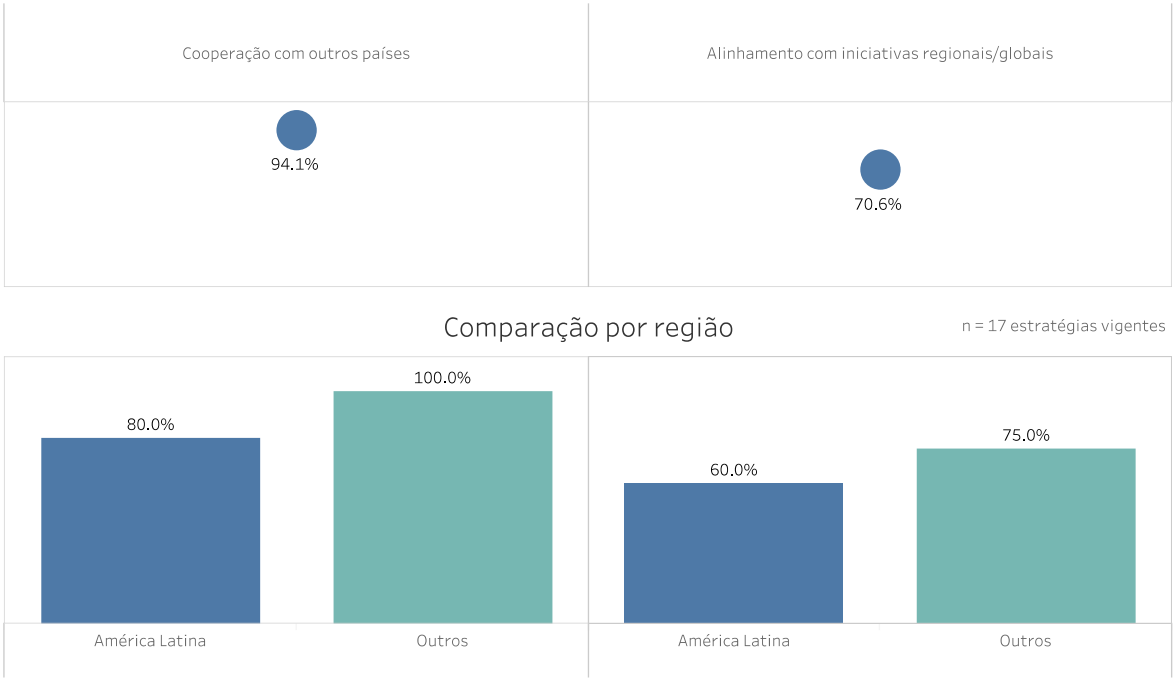
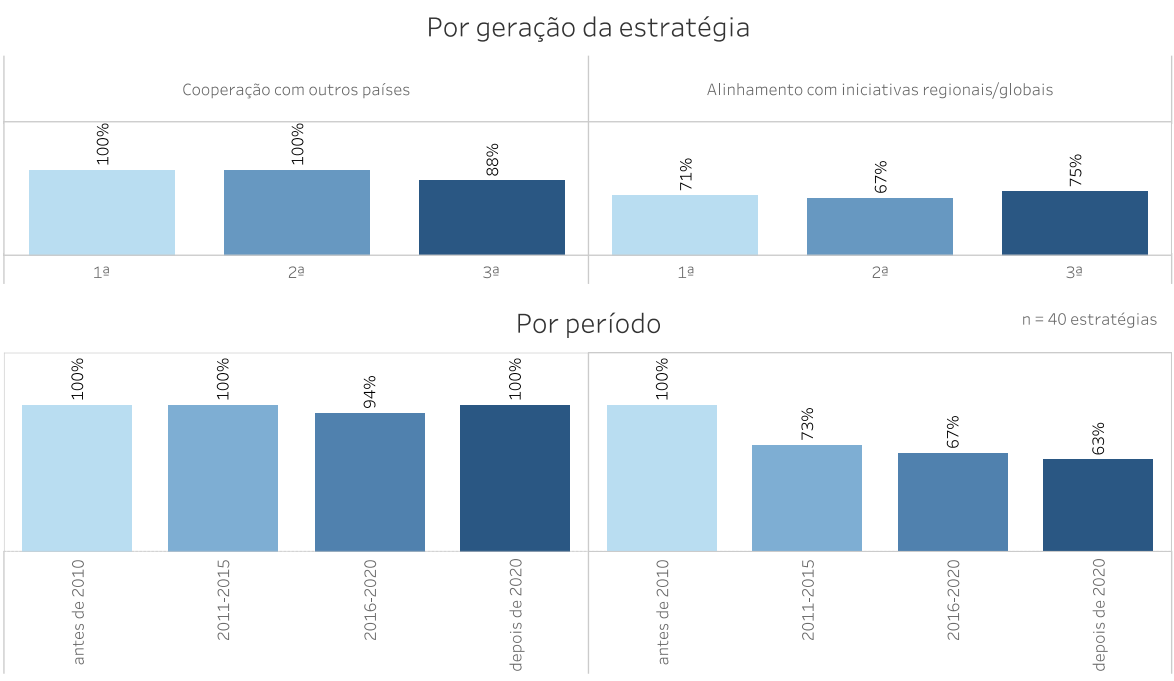


Gráfico 22

Área Focal: Cooperação Internacional
Evolução da presença dos mecanismos nas estratégias analisadas



4.7.6. Área focal: Legislação e Marco Normativo

PONTOS CHAVE DA SEÇÃO

- **Aprimoramento do marco normativo atual:** A grande maioria das estratégias vigentes analisadas têm alguma medida para aprimorar a estrutura normativa atual, pois é impossível obter melhorias substanciais se não tivermos uma estrutura regulatória que apoie as mudanças e lhes dê sustentabilidade ao longo do tempo.
- **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 a Convenção. Especificamente, cerca da metade menciona 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

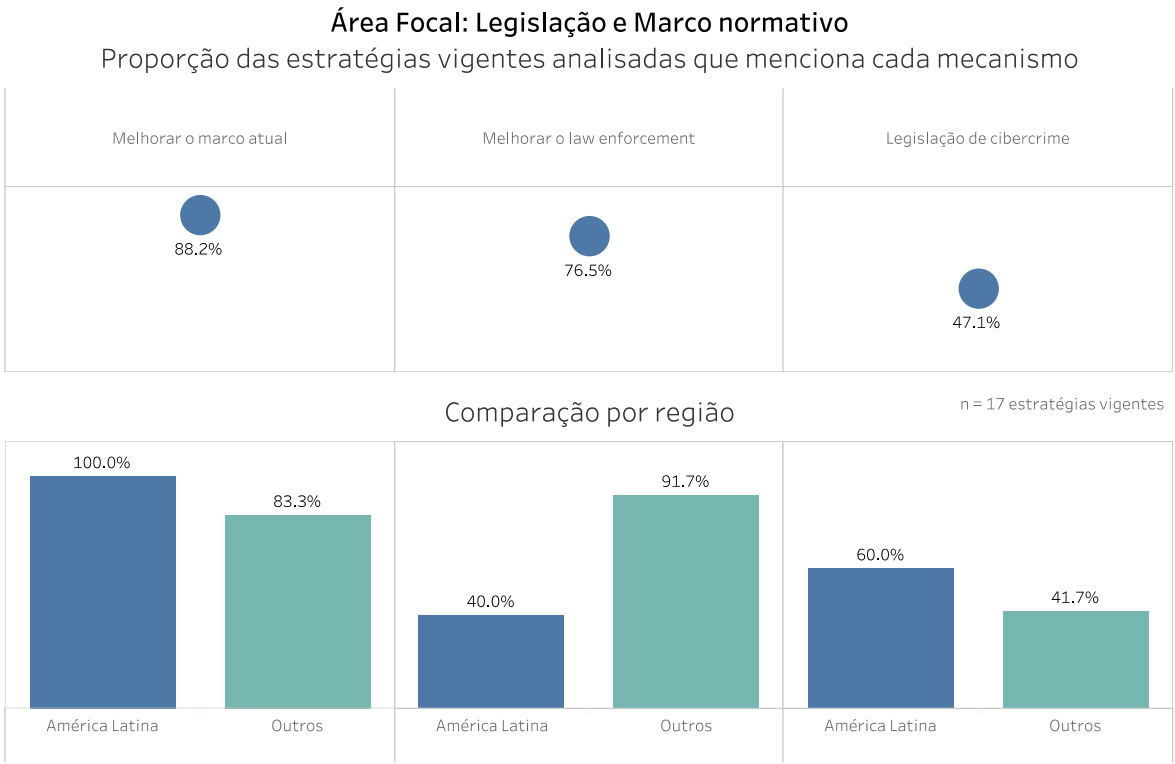
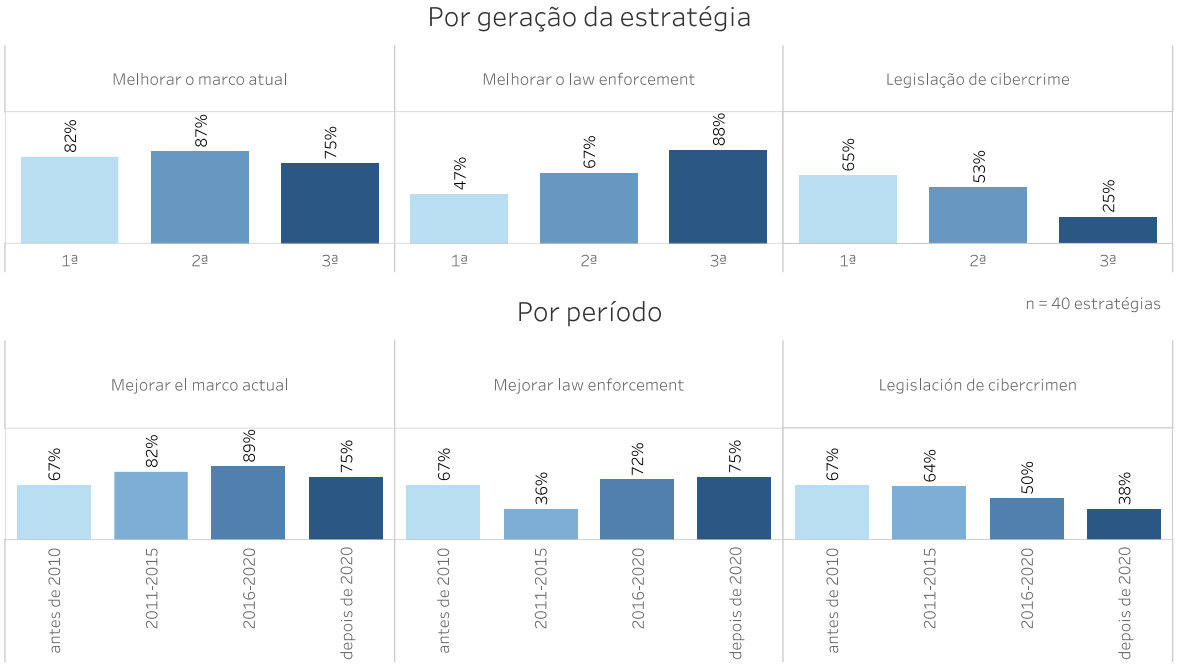


Gráfico 24

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 88,2% das estratégias em vigor mencionam esse tópico. Algo semelhante acontece quando observamos sua presença nas estratégias por geração, em que seu aparecimento é, em sua maioria, alto e tende a aumentar. 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 que tem uma presença em 76,5% das estratégias atuais. É impressionante a pouca participação proporcional desse tema nas estratégias latino-americanas, com apenas 40% delas mencionando-o. A estratégia dos EUA se refere a esse tópico em várias ocasiões e o mostra como um esforço transversal, pois está presente em vários dos objetivos, seja por meio de capacitação, agências nacionais ou acordos internacionais.

Quanto ao tópico da legislação sobre crimes cibernéticos, é notável a baixa presença desse tópico nas estratégias em vigor, com apenas 47,1% delas mencionando-o. Também observamos uma menção decrescente tanto por ano quanto por geração. Deve-se observar que praticamente todos os países deste estudo são partes 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.

4.7.7. 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 dois terços das estratégias vigentes analisadas.
- Security by design: com uma clara tendencia crescente, o conceito tem assumido um papel protagonista rapidamente, estando presente em 63% 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[22], 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 da UE e do Espaço Econômico Europeu. O principal objetivo é melhorar o controle e os direitos dos indivíduos sobre seus dados pessoais e simplificar o ambiente regulatório para negócios internacionais.

Em relação à presente área focal, a OEA, em sua publicação Princípios Atualizados sobre privacidade e proteção de dados pessoais)[23], estabelece 13 princípios que refletem as diferentes abordagens predominantes nos Estados Membros sobre as questões centrais da proteção de dados pessoais, a saber

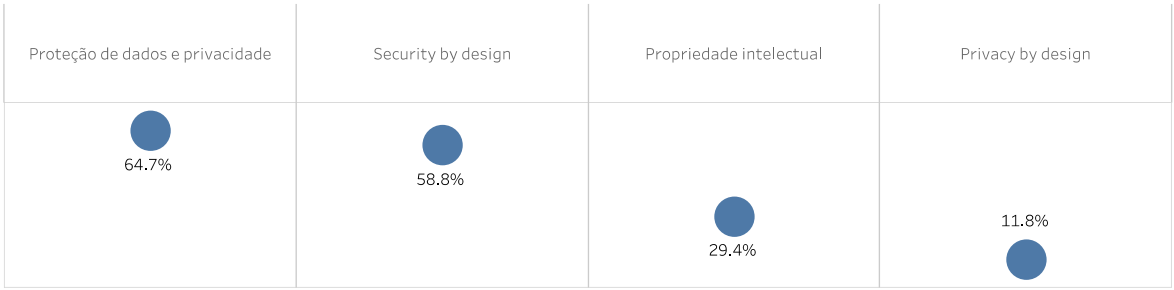
- Objetivos legítimos e justiça
- Transparência e consentimento
- Relevância e necessidade
- Processamento e retenção limitados
- Confidencialidade
- Segurança dos dados
- Precisão dos dados
- Acesso, retificação, exclusão, cancelamento, objeção e portabilidade
- Dados pessoais sensíveis
- Responsabilidade e obrigação
- Fluxo de dados transfronteiriços e responsabilidade
- Exceções
- Autoridade de proteção de dados

[22] General Data Protection Regulation - https://gdpr.eu/tag/gdpr/
[23] 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 = 17 estratégias vigentes

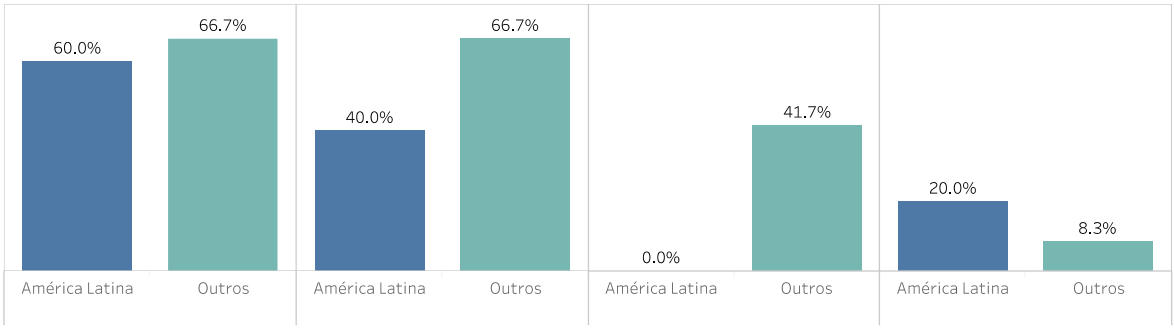
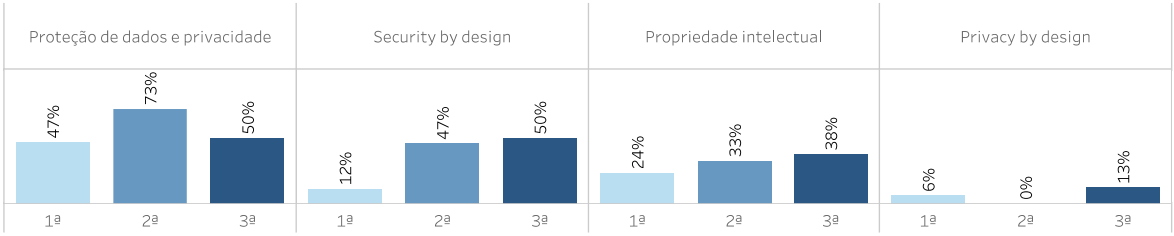


Gráfico 26

Área Focal: Privacidade e Dados

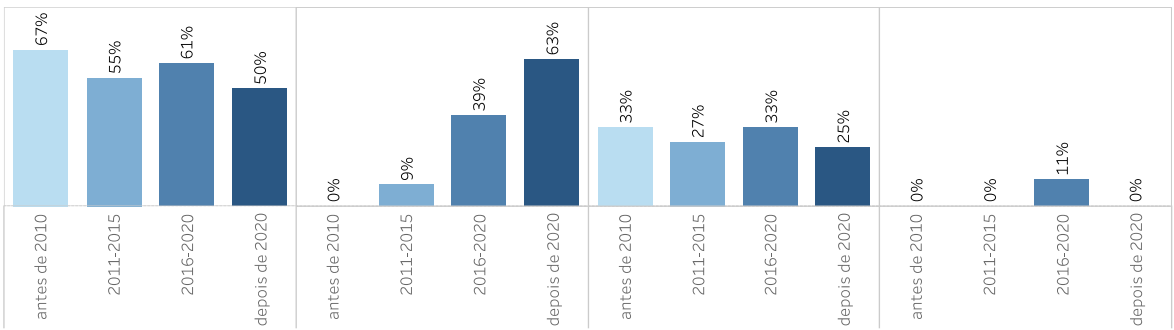
Evolução da presença do mecanismo nas estratégias analisadas

Por geração da estratégia



Por período

n = 40 estratégias



O tópico de proteção de dados e privacidade é abordado por 64,7% das estratégias em vigor, quase igualmente na América Latina (60%) e no resto do mundo (66,7%). Esse é um tópico que está presente há algum tempo e continuou a crescer ligeiramente 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, para gerar confiança nos processos das entidades públicas e garantir a proteção dos dados pessoais e a inclusão e atualização permanente das políticas de segurança e confiança digital".

Israel faz referência em sua estratégia à proteção de dados em relação à inteligência artificial, onde 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 micros alvos 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 Segurança por design, podemos ver como sua presença tem aumentado acentuadamente ao longo dos anos, começando com nenhuma presença nas estratégias anteriores a 2010 e chegando a 63% nas mais atuais. Conforme mencionado acima, 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, podemos ver que ele tem pouca presença nas estratégias atuais, onde está presente em 29,4% delas, sem presença nas da América Latina, fato que se corrobora pela tendencia dos países do Norte Global serem mais fortemente produtores de novas tecnologias. Embora seja uma questão que se mantém ao longo do tempo, vemos um aumento em sua abordagem nas estratégias se olharmos do ponto de vista geracional dessas estratégias. 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 segurança por design, apoiando especificamente aqueles que apoiam as necessidades de interesse nacional para fortalecer a autonomia digital e a propriedade intelectual e industrial".

A privacidade por design é um tópico relativamente novo que tem baixa presença nas estratégias atuais, estando presente em apenas 11,8% dos estatutos 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. Abandonaremos plataformas obsoletas (princípio "no legacy"). Para isso, desenvolveremos um recurso de consultoria de arquitetura de segurança central."

4.7.8. Área focal: Defesa e Militar

PONTOS CHAVE DA SEÇÃO

- **Capacidades militares:** embora 41,2% 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. Primeiro, como ocorre com outros tópicos, é possível que a questão seja abordada em outra estratégia, como a estratégia de segurança nacional ou a estratégia 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 claramente igualmente importantes para todos os países, sua importância pode estar aberta à discussão.

Gráfico 27

Área Focal: Defesa e Capacidade militar
Proporção das estratégias vigentes analisadas que menciona cada mecanismo

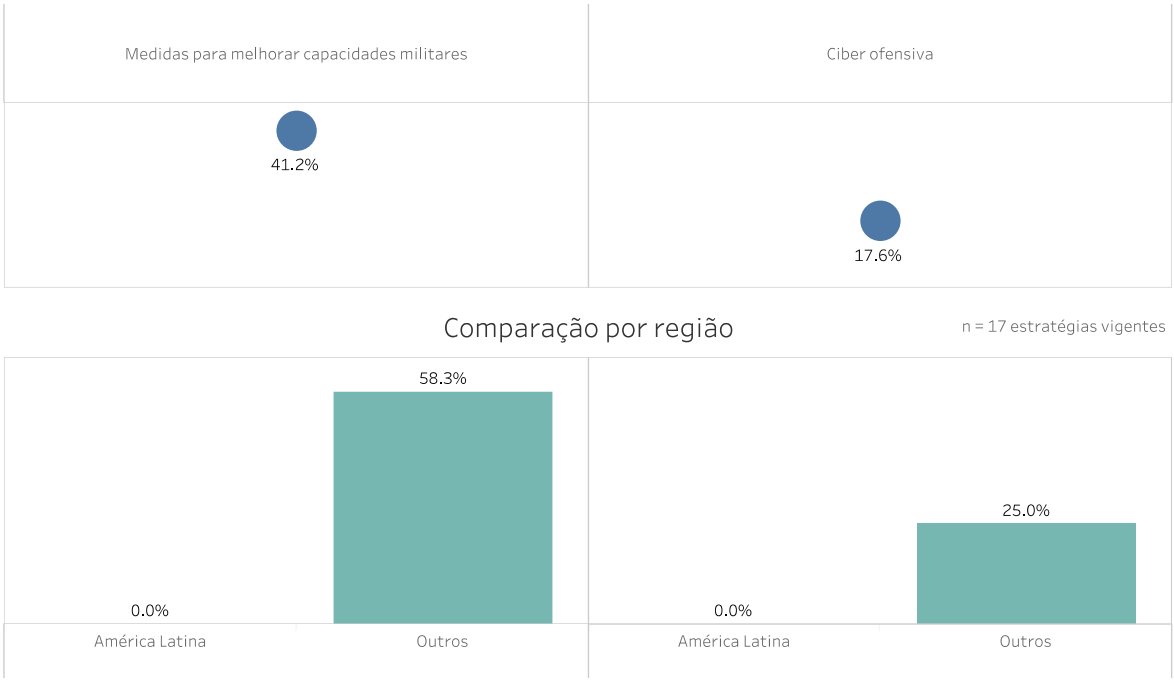
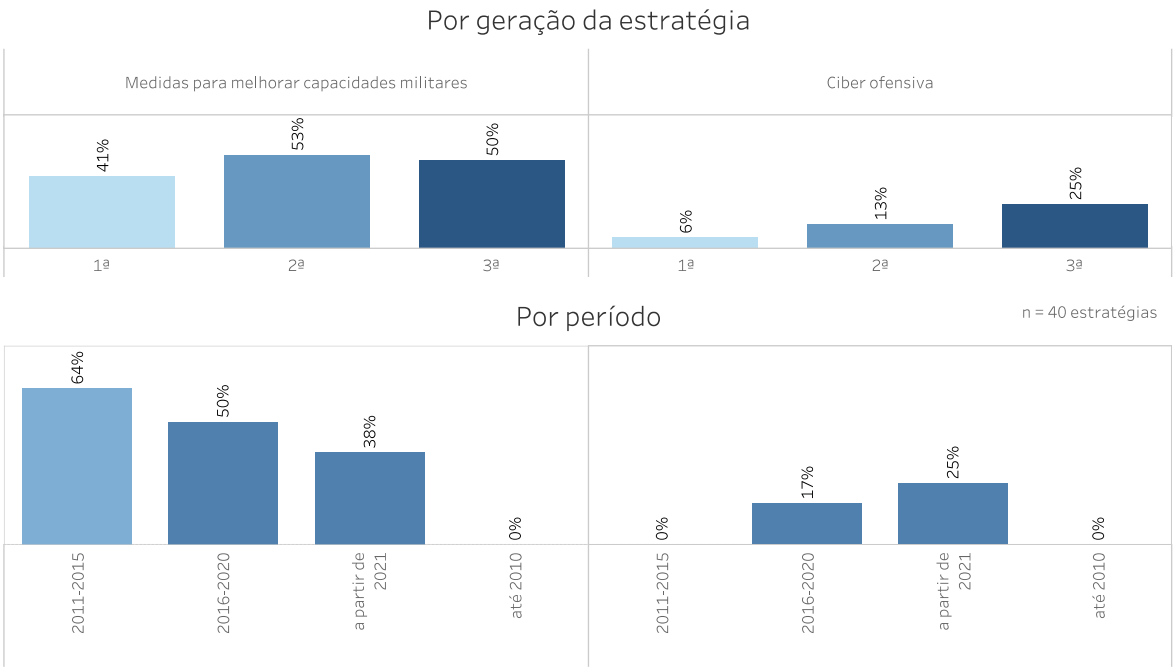


Gráfico 28

Área Focal: Defesa e Capacidade militar
Evolução da presença do mecanismo nas estratégias analisadas



Especificamente sobre o tópico de aprimoramento das capacidades militares, vemos uma menção de 41,2% nas estratégias atuais. Embora seja geralmente tratado em proporção

semelhante para estratégias em diferentes períodos, vemos um aumento em seu aparecimento do ponto de vista geracional, onde começa com 41% para a primeira geração e termina com 50% na terceira geração. Alguns exemplos ilustrativos incluem:

- "Incluiremos continuamente a segurança cibernética na abordagem geral de defesa nacional. Para isso, integraremos ainda mais a segurança cibernética nos documentos de planejamento de segurança nacional (o plano de desenvolvimento da defesa nacional e o plano de atividades de defesa nacional) e realizaremos 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).

O tema da segurança cibernética ofensiva no contexto militar tem uma presença reduzida, atingindo apenas 17,6% das estratégias em vigor. Embora haja um aumento em sua participação nas estratégias, se olharmos do ponto de vista geracional, ainda poucas o englobam. Um exemplo desse tópico nas estratégias estudadas é:

- "Os Estados que não compartilham dos desafios impostos por uma Internet livre e aberta estão explorando os desafios impostos por uma Internet livre e aberta para promover suas visões autoritárias do ciberespaço, sob o pretexto de segurança. O Reino Unido adotará uma abordagem mais proativa, trabalhando com nossos aliados e parceiros para garantir regras e estruturas internacionais alinhadas com nossos valores democráticos. Nosso 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. Alcançaremos os seguintes resultados até 2025" (Parágrafo 160, Objetivo 2, Reino Unido, 2022)

BOX 3 – ESTUDO DE CASO
EVOLUÇÃO DAS ESTRATÉGIAS DE CIBERSEGURANÇA NO REINO UNIDO.

O Reino Unido se encontra 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 estratégia, 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 "para "poder cibernético" (ou *cyber power*, no original). Veja abaixo um breve relato da evolução das estratégias:

1ª 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 online, aumentar a resiliência contra os ataques, fomentar um ciberespaço aberto e estável e garantir que a nação possuísse o conhecimento e as habilidades necessárias para alcançar essas metas. Pioneiramente, a estratégia estabeleceu um orçamento específico para um 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

2ª Estratégia (2016):
Construindo sobre a estratégia de 2011 e sobre 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 recursos para enfrentar as ameaças cibernéticas". O próprio estabelecimento do Centro de Segurança Cibernética Nacional (NCSC) indica a busca por um papel mais proativo do governo. Para além de orientações como na primeira estratégia, agora há uma ênfase maior em incentivos e regulação.

3ª Estratégia (2021):
A estratégia mais recente, lançada em 2021, muda a ênfase de cibersegurança para "poder cibernético" (ou *cyber power*, no original). Nesta terceira geração, com uma linguagem mais assertiva, o Reino Unido entende o ciberespaço como uma arena central na competição entre países democráticos e autocráticos. Nessa visão, também a uma mudança do alcance, uma vez que a segunda estratégia mencionava uma abordagem "Whole-of-government" e agora se passa a uma visão "Whole-of-society". Esta abordagem se concretiza na criação de um National Cyber Advisory Board que vai apoiar o governo na implementação da estratégia. Nesse sentido, para além do foco em segurança, a estratégia foca muito em como usar o ciberespaço para vantagens econômicas e sociais
A evolução das estratégias nacionais de cibersegurança do Reino Unido demonstra uma mudança de abordagens orientadas pelo mercado para um papel mais proativo do governo, culminando em um foco no "poder cibernético" como um ativo nacional vital. Esta evolução representa o reconhecimento mais amplo da importância do ciberespaço, não apenas em termos de segurança, mas também como um domínio para competição e 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

5. Considerações Finais

Este estudo, a partir de uma análise documental de 40 estratégias, conseguiu identificar grandes tendencias na evolução das estratégias de cibersegurança no mundo. Como vimos, 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. Ao longo do estudo, se identificaram os padrões de mudança e as tendencias em diferentes áreas focais, ilustrando a direção na qual os países mais maduros estão se dirigindo.

Embora se verifiquem tendencias importantes, cada país deve conduzir uma análise específica considerando sua situação, 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 os diversos stakeholders.

Assim, adotar um processo colaborativo que incorpore os avanços e 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.

6. Anexo I – Dicionário/Glossário de Dados

Neste anexo, detalhamos as categorias de análise utilizadas para definição de como se considerou se as estratégias cobriam determinado aspecto ou não. O glossário está estruturado a partir da ordem de aparição nos gráficos apresentados:

Gráfico I - Estrutura

"Tem objetivos" – Se considerou que "sim" se o documento possui explicitamente objetivos estratégicos, objetivos gerais, subobjetivos ou categoria similar.

"Tem princípios" – Se considerou que "sim" se o documento explicitamente anuncia o uso de princípios.

"Tem visão" – Se considerou que "sim" se o documento explicitamente declara a visão ou se a visão se encontra englobada em outra sessão do documento. Em algumas estratégias se considerou o "propósito", desde que tivesse uma redação que olhasse para um direcionamento futuro na área.

"Tem indicadores/métricas" – Se considerou que "sim" se o documento explicitamente apresenta uso de indicadores quantitativos ou métricas qualitativas para medir o sucesso e verificar o atingimento das propostas da Estratégia. Não se contabilizaram os casos em que a estratégia menciona que os indicadores serão elaborados em etapa posterior.

Gráfico 2 – Área Focal: Governança e Institucionalidade

Estabelece mecanismos de coordenação intra-governo – Se considerou que "sim" sempre que a estratégia menciona linhas de ação, objetivos ou intervenções para aumentar a coordenação entre as diferentes agencias e departamentos do governo. 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.

Estabelece mecanismos de coordenação público-privado - Se considerou que "sim" sempre que a estratégia menciona linhas de ação, objetivos ou intervenções para aumentar a coordenação entre o setor 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.

Estabelece/Reconhece uma autoridade em ciber – se considerou que "sim" sempre que a estratégia menciona explicitamente o nome da agência ou departamento responsável pela cibersegurança (caso já criado anteriormente) ou utiliza o documento da estratégia para definir este responsável. Foi considerado que "sim" se autoridade é para os temas de ciber de forma ampla, bem como especificamente para implementação da estratégia.

Define um plano operacional (agora ou no futuro) – Se considerou que "sim" sempre que a estratégia possui um plano concreto de implementação já no corpo do documento principal ou sempre que se mencionou explicitamente que a criação de um plano de ação será uma decorrência da publicação da estratégia.

Cita entes subnacionais – Se considerou "sim" sempre que a estratégia menciona pelo menos uma ação que inclua governos subnacionais (províncias, regiões, estados, municipalidades, governos locais, comarcas, ou definições similares a depender do país)

Tem normativa associada – Se considerou que "sim" sempre que o próprio documento da Estratégia menciona o instrumento pelo qual foi publicada e vincula o número correspondente (decreto, resolução ou similar). Não se fez pesquisa adicional externa ao documento para verificar se existe normativa associada.

Define responsáveis claros para cada ação – Se considerou que "sim" sempre que o corpo principal da estratégia deixa explicito quem é responsável pela implementação das ações contidas. Também se considerou positivamente o caso em que há uma seção da estratégia que descreve detalhadamente os arranjos de sua implementação.

Tem orçamento associado – Se considerou que "sim" sempre que a estratégia explicitamente atribui um orçamento ou quantifica o custo da sua implementação. Não se analisaram os orçamentos propriamente ditos.

Gráficos 4 – Tipos de ameaça

Criminosos/Ciberataques – Se considerou que "sim" se a estratégia explicitamente menciona criminosos ou ciberataques como uma ameaça no espaço cibernético.

Outros países/ciberguerra – Se considerou que "sim" se a estratégia explicitamente menciona ameaças vindo de outros Estados ou fala explicitamente de guerra no espaço cibernético.

Espionagem – Se considerou que "sim" se a estratégia explicitamente menciona espionagem como ameaça. Muitas vezes este conceito estava correlacionado com a categoria anterior.

Terroristas – Se considerou que "sim" se a estratégia explicitamente menciona terrorismo ou terroristas como ameaça.

Ataques à democracia – Se considerou que "sim" se a estratégia menciona ameaças ligadas a manipulação das eleições, crenças democráticas, desinformação orientada a minar a democracia, ou categorias similares.

Extremistas – Se considerou "sim" se a estratégia menciona explicitamente extremistas ou polarização política ou religiosa no ciberespaço.

Hacktivistas – Se considerou "sim" se a estratégia menciona explicitamente o termo hacktivistas ou hackers.

Desastres naturais – Se considerou "sim" se a estratégia menciona explicitamente riscos naturais (terremotos, desabamentos, alagamentos) como tipos de ameaça ao espaço cibernético no país.

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

Direitos Humanos – Se considerou que "sim" unicamente se, na sessão de princípios, se mencionam direitos humanos, valores democráticos, direitos fundamentais ou algum conceito ligado a liberdades civis.

Visão holística/coordenada – Se considerou que "sim" unicamente se, na sessão de princípios, se menciona a necessidade de ter uma abordagem integrada ou holística ou se existe algum princípio com foco em aumentar a coordenação entre os diferentes atores envolvidos na temática.

Cooperação internacional – Se considerou que "sim" unicamente se, na sessão de princípios, há algum princípio orientador com foco em cooperação internacional ou atuação global.

Cibersegurança como parte da segurança nacional – Se considerou que "sim" unicamente se, na sessão dos princípios, há alguma menção mais ampla relacionada à segurança nacional.

Prosperidade econômica – Se considerou que "sim" unicamente se, na sessão de princípios, existe algum princípio orientado à prosperidade econômica ou se, ao menos, se usam palavras como "prosperidade", "oportunidade econômica", "fomento à indústria", "desenvolvimento econômico" ou similar.

Conscientização/responsabilidade individual – Se considerou "sim" unicamente se, na sessão de princípios, existe algum princípio orientado ao cidadão ou usuário final e/ou se menciona um foco em sensibilização ou conscientização dos riscos do ciberespaço.

Transparência – Se considerou "sim" unicamente se, na sessão de princípios, existe algum princípio orientado ao aumento da transparência ou confiança no ciberespaço e/ou nas políticas de cibersegurança.

Proporcionalidade – Se considerou "sim" unicamente se, na sessão de princípios, existe algum princípio que menciona a palavra proporcionalidade ou o seu 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 – Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe alguma menção explicita a melhorias na resiliência, prontidão ou preparação para resposta a ataques.

Capacidades/Capacity Building – Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe algum objetivo orientado a melhorar as capacidades (do país ou do

governo), ampliar conhecimento no país, ampliar a capacidade de resposta ou ações relacionadas a profissionais e educação.

Cooperação Internacional - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se menciona algum objetivo direcionado à cooperação internacional ou atuação global.

Cooperação público-privado - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se menciona algum objetivo para ampliar a cooperação com o setor privado.

Infraestrutura crítica - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se utiliza explicitamente o conceito de infraestrutura crítica.

Fomento à indústria - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe algum objetivo orientado ao setor econômico de cibersegurança no país ou a ampliar a prosperidade econômica de forma mais ampla.

Cultura de ciber/Conscientização - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se menciona algum objetivo orientado à cultura de forma ampla e/ou à necessidade de aumentar a conscientização das diferentes partes, em especial dos usuários individuais.

Serviços Essenciais – Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se utiliza explicitamente o conceito de serviços essenciais ou vitais.

Desenvolvimento normativo - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe alguma menção a melhorias no marco legal, normativo ou regulatório.

Confiança/Transparência - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe alguma menção a aumento da confiança ou transparência no ciberespaço ou nas políticas de cibersegurança.

Ciberespaço aberto - Se considerou que "sim", unicamente se no nível mais alto dos objetivos, se menciona a necessidade de um ciberespaço aberto ou livre (ou alguma menção explicita a uma internet aberta ou livre).

Gestão de riscos – Se considerou que "sim", unicamente se no nível mais alto dos objetivos, existe algum objetivo sobre gestão de riscos em cibersegurança.

Gráfico 11 – Gestão de Riscos

Define uma abordagem de gestão de riscos - se considerou que "sim" sempre que a estratégia menciona a necessidade de uma abordagem de gestão de riscos na temática de cibersegurança. Nesta categoria não se exigiu uma definição de qual abordagem, mas tão somente um reconhecimento da importância de abordar a gestão de riscos.

Gráfico 13 – Prontidão e Resiliência

Estabelece capacidades para resposta à incidentes - se considerou que "sim" sempre que a estratégia menciona a capacidade operacional de responder aos incidentes, incluindo menções à CERTs, CIRTs, CSIRTs, dentre outros.

Promove o compartilhamento de informações – se considerou "sim" sempre que a estratégia menciona medidas (ou intenções) para aumentar o compartilhamento de informações (seja intra-governo seja entre setores).

Estabelece políticas para realizar exercícios de cibersegurança – se considerou "sim" sempre que a estratégia menciona o fomento à realização de exercícios de cibersegurança, incluindo simulações ou exercícios em tempo real.

Estabelece planos de contingência para gestão de crises – se considerou "sim" sempre que a estratégia menciona medidas (ou intenções) para criar planos de contingência para gestão de crises.

Gráfico 15 – Infraestrutura Crítica (IC) e Serviços Essenciais

Estabelece medidas para proteger as IC – se considerou que "sim" se a estratégia estabelece medidas ou intenções de estabelecer medidas para proteção das ICs.

Estabelece mecanismos de cooperação com o setor privado (p/ IC) – se considerou que "sim" se a estratégia encoraja a colaboração público-privado para proteção de ICs.

Estabelece medidas para proteger os ativos de governo digital – se considerou que "sim" se a estratégia menciona a digitalização de serviços ou a expansão do governo digital e a importância de sua proteção (como o GOV.BR).

Adota um modelo de governança claro para proteger as ICs – se considerou que "sim" se a estratégia deixa claros os papéis e responsabilidades de cada ator e identifica um modelo de governança para a proteção das ICs.

Estabelece medidas para identificar as IC do país – se considerou que "sim" se a estratégia explicitamente tem uma medida ou ação orientada a identificar e nomear as ICs do país.

Gráfico 17 – Capacidades e Conscientização

Inovação e R & D – Se considerou que "sim" se a estratégia cita ações ou medidas para aumentar a pesquisa e desenvolvimento na área de cibersegurança ou menciona políticas de inovação na área.

Programas de conscientização – Se considerou que "sim" se a estratégia cita 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 – Se considerou que "sim" sempre que a estratégia menciona medidas relacionadas à universidades, tal como mudanças no currículo, aumento de PhDs, dentre outras.

Medidas na educação primária/secundária – Se considerou que "sim" sempre que a estratégia menciona medidas para estimular o desenvolvimento de competências em crianças e/ou na educação primaria/secundária.

Medidas para formação profissional – Se considerou que "sim" sempre que a estratégia menciona medidas parta estimular o desenvolvimento de profissionais e mão de obra em cibersegurança, excluindo investimentos em educação superior.

Medidas para capacidades de servidores públicos – Se considerou que "sim" sempre que a estratégia menciona medidas para estimular o desenvolvimento de competências em servidores públicos ou, de forma mais ampla, nos órgãos públicos (inclui treinamentos ou capacidades de forma mais ampla).

Desenvolvimento da indústria para aumentar a soberania – Se considerou que "sim" sempre que a estratégia menciona o fomento da indústria de ciber atrelado a uma preocupação de reduzir a dependência de soluções estrangeiras.

Desenvolvimento da indústria para oportunidades econômicas – Se considerou que "sim" sempre que a estratégia menciona o fomento da indústria de ciber ligado a objetivos de oportunidades econômicas.

Medidas para aumentar a diversidade – Se considerou que "sim" sempre que a estratégia menciona medidas para aumentar o número de mulheres, pessoas LGBTQ+ e/ou outros grupos vulneráveis ou tradicionalmente subrepresentados nas áreas de cibersegurança.

Gráfico 21 – Cooperação internacional

Cooperação com outros países – Se considerou que "sim" sempre que a estratégia inclui medidas para aumentar a cooperação bilateral ou ampla entre países nos temas de cibersegurança.

Alinhamento com iniciativas regionais/globais – Se considerou que "sim" sempre que a estratégia menciona nomes específicos de blocos ou iniciativas regionais ou globais (por exemplo, NATO, União Europeia etc.)

Gráfico 24 – Legislação e Marco Normativo

Melhorar o marco atual – Se considerou que "sim" quando a estratégia menciona de forma ampla a necessidade de melhorias no marco normativo atual

Legislação sobre cibercrime – Se considerou que "sim" quando a estratégia menciona medidas explicitamente voltadas à legislação de cibercrime

Melhorar o law enforcement – Se considerou que "sim" quando a estratégia menciona melhorias para processar, punir, investigar o cibercrime e/ou usa explicitamente a expressão law enforcement (especialmente nas estratégias em inglês).

Gráfico 25 – Privacidade e Dados

Proteção de Dados e privacidade – se considerou que "sim" quando a estratégia inclui preocupações e intenções de avançar na área de proteção de dados e privacidade. Caso seja somente um princípio, foi considerado que não.

Security By Design – se considerou que "sim" unicamente quando a estratégia usa explicitamente o conceito.

Propiedade Intelectual – se considerou que "sim" quando existem iniciativas específicas para proteção da propriedade intelectual ou quando se percebe uma preocupação existente específica para este tipo de proteção.

Privacy by Design – se considerou que "sim" unicamente quando a estratégia usa explicitamente o conceito.

Gráfico 27 – Defesa e capacidade militar

Medidas para melhorar capacidades militares – se considerou que "sim" quando a estratégia menciona medidas ligadas às capacidades militares ou à defesa.

Ciber ofensiva – se considerou que "sim" unicamente quando a estratégia menciona o conceito explicitamente.

7. Anexo II – Fichas técnicas de cada País analisado

(as fichas contêm traduções livres dos idiomas originais das estratégias)

País: Estônia
Nome: Estratégia de Cibersegurança
Ano de publicação: 2008
Vigência: 2008-2013
Instituição a cargo da elaboração: Ministério da Defesa, por meio de um comitê da Estratégia de Cibersegurança.
Instituições participantes: Cooperação com o Ministério da Educação e Pesquisa, Ministério da Justiça, Ministério de Assuntos Econômicos e Comunicações, Ministério de Assuntos Internos e o Ministério de Relações Exteriores. O comitê interministerial encarregado de desenvolver a estratégia também incluiu especialistas em segurança da informação do setor privado da Estônia**.**
Estrutura: 5 macro objetivos com medidas associadas, além de princípios e uma revisão das principais ameaças.

Definição de Cibersegurança: Segurança cibernética nacional é um termo amplo que abrange muitos aspectos de informações eletrônicas, dados e serviços de mídia que afetam os interesses e o bem-estar de um país.
Alcance: "Nação como um todo" (não limitado ao governo)
Visão: (não explícita) A estratégia de segurança cibernética da Estônia busca principalmente reduzir as vulnerabilidades inerentes ao espaço cibernético da nação como um todo.
Princípios:

- Os planos de ação de segurança cibernética devem ser integrados aos processos de rotina do planejamento de segurança nacional;
- A segurança cibernética deve ser buscada por meio de esforços coordenados de todas as partes interessadas, dos setores público e privado, bem como da sociedade civil;
- A cooperação efetiva entre os setores público e privado deve ser promovida para a proteção da infraestrutura crítica de informações;
- A segurança cibernética deve se basear na segurança eficiente da informação, o que significa que todo usuário de um sistema de informação deve estar ciente de suas responsabilidades no uso prudente dos sistemas de informação e deve tomar as medidas de segurança necessárias para gerenciar os riscos identificados;
- Deve-se promover uma conscientização social geral sobre as ameaças no ciberespaço e o estado de prontidão para enfrentá-las; esses são pré-requisitos importantes, já que cada membro da sociedade da informação é responsável pela segurança dos instrumentos ou sistemas baseados em rede que possui;
- A Estônia deve cooperar estreitamente com organizações internacionais e outros países para aumentar a segurança cibernética globalmente;
- Deve-se dar a devida atenção à proteção dos direitos humanos, dos dados pessoais e da identidade;
- O desenvolvimento e a administração de soluções de TI para a prestação de serviços públicos devem estar em conformidade com a arquitetura de TI e a estrutura de interoperabilidade da Estônia, incluindo a estrutura de segurança da informação. Além disso, deve-se levar em consideração a segurança interna.

Objetivos/áreas de política:

- 1) aplicação de um sistema graduado de medidas de segurança na Estônia (desenvolvimento e implementação em larga escala de um sistema de medidas de segurança);
- 2) desenvolvimento da expertise e da alta conscientização da Estônia em relação à segurança da informação, atingindo o mais alto padrão de excelência;
- 3) desenvolvimento de uma estrutura regulatória e jurídica adequada para apoiar a segurança e a operacionalidade contínua dos sistemas de informação;
- 4) promoção da cooperação internacional com o objetivo de fortalecer a segurança cibernética global.
- 5) Aumentar a conscientização sobre a segurança cibernética.

Indicadores: Não há
Governança:
- Criação de um Conselho de Segurança Cibernética do Comitê de Segurança do Governo da República com a responsabilidade de implementar as metas da Estratégia de Segurança Cibernética;

- Determinação dos deveres da unidade estrutural dentro do Ministério de Assuntos Econômicos e Comunicações responsável pela segurança dos sistemas de informação do estado e execução desses deveres para fornecer análises de risco em diferentes níveis;
- Criação de um grupo de trabalho de especialistas com a responsabilidade de identificar deficiências na segurança das informações, avaliar os recursos necessários para atualizar as medidas de segurança e trocar informações operacionais. O grupo de trabalho de especialistas fornecerá consultoria profissional sobre segurança da informação ao Conselho de Segurança Cibernética do Comitê de Segurança do Governo da República;
- Coordenar campanhas de conscientização sobre a segurança cibernética e designar uma agência específica com essa responsabilidade.

Alinhamento Estratégico: Information Security Interoperability Framework (2007), Estonian Information Society Strategy 2013, Knowledge-based Estonia: Estonian Research and Development Strategy
Marcos: Estonian IT Architecture and Interoperability

País: Estônia
Nome: Estratégia de Cibersegurança
Ano de publicação: 2014
Vigência: 2014-2017

Instituição a cargo da elaboração: Ministério de Assuntos Econômicos e Comunicações
Instituições participantes: Não se menciona
Estrutura: 1 objetivo geral e 5 subobjetivos, além de uma análise da situação atual, princípios e uma seção sobre a governança.
Definição de cibersegurança: Não tem
Alcance: Público-privado
Visão: A Estônia é capaz de garantir a segurança nacional e apoiar o funcionamento de uma sociedade aberta, inclusiva e segura.

Princípios:

- A segurança cibernética é parte integrante da segurança nacional e apoia o funcionamento do Estado e da sociedade, a competitividade da economia e a inovação.
- A segurança cibernética é garantida pelo respeito aos direitos e liberdades fundamentais, bem como pela proteção das liberdades individuais, das informações pessoais e da identidade.
- A segurança cibernética é garantida com base no princípio da proporcionalidade, levando em conta os riscos e recursos existentes e potenciais.
- A segurança cibernética é garantida de forma coordenada por meio da cooperação entre os setores público, privado e terceiro setor, levando em conta a interconexão e a interdependência da infraestrutura e dos serviços existentes no ciberespaço.
- A segurança cibernética começa com a responsabilidade individual pelo uso seguro das ferramentas de TIC.

- Uma das principais prioridades para garantir a segurança cibernética é a antecipação, bem como a prevenção de possíveis ameaças e a resposta eficaz às ameaças que se materializam.
- A segurança cibernética é apoiada por pesquisa e desenvolvimento intensivos e internacionalmente competitivos.
- A segurança cibernética é garantida por meio da cooperação internacional com aliados e parceiros. Por meio da cooperação, a Estônia promove a segurança cibernética global e aprimora sua própria competência.

Objetivos/áreas de política:

- GERAL: a meta de quatro anos da estratégia de segurança cibernética é aumentar as capacidades de segurança cibernética e aumentar a conscientização da população sobre as ameaças cibernéticas, garantindo assim a confiança contínua no espaço cibernético.
- Subobjetivo 1: Garantir a proteção dos sistemas de informação subjacentes a serviços importantes
- Subobjetivo 2: Aprimorar o combate ao crime cibernético
- Subobjetivo 3: Desenvolvimento de capacidades nacionais de defesa cibernética
- Subobjetivo 4: Gerenciar a evolução das ameaças à segurança cibernética
- Subobjetivo 5: Desenvolver atividades intersetoriais

Indicadores: não há
Governança:
- O Ministério de Assuntos Econômicos e Comunicações dirige a política de segurança cibernética e coordena a implementação da estratégia.
- A estratégia será implementada com a participação de todos os ministérios e agências governamentais, especialmente o Ministério da Defesa, a Autoridade do Sistema de Informações, o Ministério da Justiça, o Conselho da Polícia e da Guarda de Fronteiras, o Gabinete do Governo, o Ministério das Relações Exteriores, o Ministério do Interior e o Ministério da Educação e Pesquisa.
- ONGs, organizações empresariais, governos e instituições educacionais cooperarão na implementação e avaliação da estratégia.
- A pedido do Ministério de Assuntos Econômicos e Comunicações, as agências envolvidas na execução da estratégia apresentarão uma visão geral por escrito da implementação das medidas e atividades a cada. Com base nas análises, o Ministério de Assuntos Econômicos e Comunicações avaliará a eficácia das medidas e atividades e compilará um relatório sobre a implementação da estratégia.

Alinhamento Estratégico: Não está explicito como uma seção da estratégia, mas tem claro alinhamento com a Agenda Digital e é elaborada pelo mesmo ministério.
Marcos: Não há.

País: Estônia
Nome: Estratégia de Cibersegurança

Ano de publicação: 2019
Vigência: 2019-2022
Instituição a cargo da elaboração: Ministério de Assuntos Econômicos e Comunicações
Instituições participantes: A Estratégia de segurança cibernética é um documento horizontal referente a acordos e coordenação no campo da segurança cibernética, que todas as partes interessadas mais importantes da Estônia mais importantes da Estônia ajudaram a redigir: instituições governamentais, universidades e *think tanks* e o setor privado.
Estrutura: Visão, com 4 objetivos estratégicos, ações associadas e indicadores para cada objetivo.

Definição de cibersegurança: Cibersegurança não significa proteger as soluções tecnológicas. Significa proteger a sociedade digital e o modo de vida como um todo.
Alcance: Envolve todos os stakeholders – setor público (civil e militar), provedores de serviços essenciais, empreendedores e academia.
Visão: A Estônia é a sociedade digital mais resiliente. A Estônia pode lidar com as ameaças cibernéticas como uma sociedade digital segura e sem interrupções, contando com a indivisibilidade das capacidades nacionais, um setor privado bem-informado e engajado e uma excelente competência em pesquisa e desenvolvimento. A Estônia é um líder reconhecido internacionalmente em segurança cibernética, uma posição que apoia a segurança nacional e contribui para o crescimento da competitividade global das empresas que operam nesse domínio. A sociedade estoniana percebe a segurança cibernética como uma responsabilidade compartilhada, na qual todos têm um papel a desempenhar.
Princípios:

- Consideramos a proteção e a promoção dos direitos e liberdades fundamentais tão importantes no espaço cibernético quanto no ambiente físico.
- Vemos a segurança cibernética como um facilitador e amplificador do rápido desenvolvimento digital da Estônia, que é a base para o crescimento socioeconômico do país. A segurança deve apoiar a inovação e a inovação deve apoiar a segurança.
- Reconhecemos que a garantia de segurança das soluções criptográficas é de importância singular para a Estônia, pois é a base do nosso ecossistema digital.
- Consideramos que a transparência e a confiança pública são fundamentais para a sociedade digital. Portanto, nos comprometemos a aderir ao princípio da comunicação aberta.

Objetivos/áreas de política:

- OBJETIVO 1 - Uma sociedade digital sustentável
  A Estônia é uma sociedade digital sustentável que conta com forte resiliência tecnológica e preparação 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 a Estônia.
- OBJETIVO 3 Uma contribuição internacional de destaque
  A Estônia é um parceiro confiável e capaz na arena internacional.
- OBJETIVO 4 Uma sociedade com alfabetização cibernética
  A Estônia é uma sociedade cibernética e garante uma oferta de talentos suficiente e voltada para o futuro.

Indicadores: Possui indicadores. Alguns exemplos:

- Porcentagem de residentes que evitam os canais digitais com o setor público ou prestadores de serviços para evitar riscos de segurança;
- Porcentagem de usuários de identidade digital segura entre todos os portadores de identidade digital;
- Volume de exportação das empresas do setor;
- Número de novas startups no setor;
- Número de doutorados defendidos no setor;
- Nível de conscientização e habilidades cibernéticas entre os funcionários de instituições governamentais e governos locais, medido com base em um teste prático de habilidades;
- Uso de uma política de segurança de TIC oficialmente confirmada entre as empresas (%);
- Déficit estimado da força de trabalho;

Governança:

- O planejamento da política de segurança cibernética e a implementação da estratégia são coordenados pelo Ministério de Assuntos Econômicos e Comunicações. 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 de Segurança Cibernética.
- A principal responsabilidade pela implementação da política nacional do setor cibernético acordada na Estratégia de segurança cibernética cabe às instituições governamentais que contribuem para o trabalho do conselho de segurança cibernética. Para a implementação coordenada dos objetivos acordados na Estratégia de Segurança Cibernética, os ministérios que contribuem diretamente para a implementação da estratégia e o Gabinete do Governo nomeiam um ponto focal que é o responsável por questões relacionadas à garantia da segurança cibernética nacional em sua jurisdição e garante que as prioridades acordadas na Estratégia sejam executadas, preparando com base nisso, um relatório anual para o conselho de segurança cibernética.
- A cooperação e a troca de informações entre os funcionários responsáveis são organizadas pelo Ministério de Assuntos Econômicos e Comunicações.
- Uma vez por ano, o comitê de segurança do Governo da República aprova o relatório consolidado sobre as atividades no campo da segurança cibernética e, dentro do relatório sobre a implementação da estratégia da sociedade da informação. Com isso, uma visão geral das atividades realizadas é fornecida ao Governo da República.

Alinhamento Estratégico: Agenda Digital da Estônia

Marcos: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)

País: Espanha

Nome: Estratégia de Cibersegurança Nacional

Ano de publicação: 2013

Vigência: Não definido

Instituição a cargo da elaboração: Departamento de Segurança Nacional - Presidência do Governo

Instituições participantes: Não mencionado.
Estrutura: 1 objetivo general e 6 objetivos específicos, com ações e princípios.
Definição de cibersegurança: Não definido
Alcance: Nação como um todo
Visão: (propósito) O objetivo da Estratégia Nacional de Segurança Cibernética, promovida pela Estratégia, promovida pelo Conselho de Segurança Nacional Conselho de Segurança Nacional é estabelecer diretrizes gerais para o uso seguro do diretrizes para o uso seguro do espaço cibernético, promovendo uma visão inclusiva cuja implementação ajuda a garantir a segurança e o progresso de nossa nação e o progresso de nossa nação, por meio da coordenação e cooperação adequadas de todas as administrações públicas e cooperação entre si, com o setor privado e com os cidadãos setor privado e com os cidadãos.
Princípios:

- Liderança nacional e coordenação de esforços;
- Responsabilidade compartilhada (atores públicos e privados, inclusive cidadãos)
- Proporcionalidade, racionalidade e eficácia (gerenciamento dinâmico dos riscos, equilíbrio entre oportunidades e ameaças, garantia da proporcionalidade das medidas)
- Cooperação internacional
- E todos os itens acima, respeitando os direitos fundamentais

Objetivos/áreas de política:

- Objetivo global: Garantir que a Espanha faça uso seguro dos sistemas de informação e telecomunicações, fortalecendo as capacidades de prevenção, defesa, detecção e resposta a ataques cibernéticos.
- Objetivo 1 - Garantir que os sistemas de informação e telecomunicações utilizados pelas administrações públicas tenham um nível adequado de segurança cibernética e resiliência.
- Objetivo 2 - Aumentar a segurança e a resiliência dos sistemas de informação e de telecomunicações usados pelo setor empresarial em geral e pelos operadores de infraestruturas críticas em particular.
- Objetivo 3 - Aprimorar as capacidades de prevenção, detecção, reação, análise, recuperação, resposta, investigação e coordenação contra atividades de terrorismo e crimes cibernéticos.
- Objetivo 4 - Conscientizar os cidadãos, os profissionais, as empresas e as administrações públicas espanholas sobre os riscos decorrentes do ciberespaço.
- Objetivo 5 - Obter e manter o conhecimento, as habilidades, a experiência e as capacidades tecnológicas de que a Espanha precisa para sustentar todos os objetivos de segurança cibernética.
- Objetivo 6 - Contribuir para a melhoria da segurança cibernética no âmbito internacional.

Indicadores: não há
Governança:
Composto pelos seguintes componentes sob a direção do Presidente do Governo:
A. O Conselho de Segurança Nacional – assiste ao presidente na direção da política de Segurança Nacional

B. o Comitê Especializado em Segurança Cibernética – com órgãos da administração pública que tenham competência em cyber e participação do setor privado
C. o Comitê de Situação Especializado, o único para todo o Sistema de Segurança Nacional – para situações de crise

Alinhamento Estratégico: Estratégia Nacional de Segurança (2013) na qual cibersegurança é uma das 12 áreas de atuação. Também está alinhado com norma reguladora de infraestrutura crítica.
Marcos: Esquema Nacional de Segurança.

País: Espanha
Nome: Estratégia Nacional de Cibersegurança
Ano de publicação: 2019
Vigência: Não definido
Instituição a cargo da elaboração: Departamento de Segurança Nacional - Presidência do Governo

Instituições participantes: Os seguintes ministérios participaram do processo de elaboração: Relações Exteriores, Justiça, Defesa, Finanças, Interior, Educação, Obras Públicas, Indústria e muitos outros ministérios. Um Comitê de Especialistas de associações profissionais, empresas e universidades também participou.
Estrutura: Um objetivo geral, 5 objetivos, linhas de ação.
Definição de Cibersegurança: A nova segurança cibernética vai além da mera proteção dos ativos tecnológicos, abrangendo as esferas política, econômica e social.
Alcance: Geral
Visão: Fazer com que esse momento de mudança não seja uma fonte de mal-estar cultural e de regressão econômica e de emprego, mas uma oportunidade de aumentar a competitividade da Espanha e o bem-estar dos espanhóis, juntamente com os parceiros europeus.

Proposito - A Espanha precisa garantir o uso seguro e responsável das redes e sistemas de informação e comunicação, fortalecendo a capacidade de prevenir, detectar e responder a ataques cibernéticos, aprimorando e adotando medidas específicas que contribuam para a promoção de um espaço cibernético seguro e confiável.

Princípios:

- Unidade de ação: qualquer resposta a um incidente de segurança cibernética que possa envolver diferentes agentes estatais será fortalecida se for coerente, coordenada e resolvida de forma rápida e eficiente.
- Antecipação: as ações preventivas têm precedência sobre as reativas.
- Eficiência
- Resiliência

Objetivos/áreas de política:

- Objetivo geral - De acordo com a Estratégia de Segurança Nacional (2017) e ampliando o objetivo de segurança cibernética previsto nela, a Espanha garantirá o uso seguro e confiável do ciberespaço, protegendo os direitos e liberdades dos cidadãos e promovendo o progresso socioeconômico.
- Segurança e resiliência das redes e sistemas de informação e comunicação do setor público e serviços essenciais.
- Uso seguro e confiável do espaço cibernético contra o uso ilícito ou mal-intencionado.
- Proteção do ecossistema comercial e social e dos cidadãos (o ciberespaço é uma responsabilidade compartilhada entre os atores estatais e privados).
- Cultura e compromisso com a segurança cibernética e capacitação de recursos humanos e tecnológicos
- Segurança do espaço cibernético em nível internacional

Indicadores: não há
Governança:
Se define uma governança que conta com:
- Conselho de Segurança Nacional para assessoramento do presidente na direção da política nacional de segurança;
- Comite de situação para gestão de crises;
- Conselho Nacional de Cibersegurança para assessoramento do presidente nos temas de cibersegurança e coordenação com os órgãos públicos;
- Comissão Permanente de Cibersegurança para coordenação interministerial operativa;
- Fórum Nacional de Cibersegurança para coordenar a relação público-privado;
- CSIRTs.

Alinhamento Estratégico: Estratégia Nacional de Segurança (2017)
Marcos: Esquema Nacional de Segurança
Modelo de Proteção da Infra Crítica: Normativa sobre proteção de infraestruturas críticas

País: Reino Unido
Nome: A Estratégia de Segurança Cibernética do Reino Unido - Protegendo e promovendo o Reino Unido em um mundo digital
Ano de publicação: 2011
Vigência: 2011-2015
Instituição a cargo da elaboração: Escritório de Segurança Cibernética e Proteção de Informações do Gabinete do Governo

Instituições participantes: não mencionado.
Estrutura: 4 objetivos, abordagem e ações para cada objetivo
Definição de cibersegurança: não definido
Alcance: Geral
Visão: 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 uma sociedade forte.

Princípios:

- Abordagem baseada em riscos
- Trabalho em parceria (privada e internacional)
- Equilíbrio entre segurança, liberdade e privacidade

Objetivos/áreas de política:

- O Reino Unido deve combater o crime cibernético e ser um dos locais mais seguros do mundo para fazer negócios no espaço cibernético
- O Reino Unido deve ser mais resistente a ataques cibernéticos e ter mais condições de proteger nossos interesses no espaço cibernético
- O Reino Unido deve ajudar a moldar um espaço cibernético aberto, estável e vibrante que o público britânico possa usar com segurança e que apoie sociedades abertas.
- O Reino Unido deve ter o conhecimento, as habilidades e a capacidade transversais de que precisa para sustentar todos os nossos objetivos de segurança cibernética.

Indicadores: Não há
Governança: Não definido
Alinhamento Estratégico: Government ICT Strategy, National Security Strategy
Marcos: Não há.

***

País: Reino Unido
Nome: Estratégia de cibersegurança nacional
Ano de publicação: 2016
Vigência: 2016-2021
Instituição a cargo da elaboração: Escritório de Segurança Cibernética e Proteção de Informações do Gabinete do Governo

Instituições participantes: Não mencionado.

Estrutura: 3 grandes áreas de objetivos (defender, deter, desenvolver) com ações associadas.

Definição de cibersegurança: "Segurança cibernética" refere-se à proteção dos sistemas de informação (hardware, software e infraestrutura associada), dos dados neles contidos e dos serviços que eles fornecem, contra acesso não autorizado, danos ou uso indevido. Isso inclui danos causados intencionalmente pelo operador do sistema ou acidentalmente, como resultado do não cumprimento dos procedimentos de segurança.
Alcance: Foca mais nas ações do governo, embora diga que também dá uma visão clara ao setor privado e sociedade civil.
Visão: Nossa visão para 2021 é que o Reino Unido seja seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital.
Princípios:

- Nossas ações e políticas serão orientadas pela necessidade de proteger nosso povo e aumentar nossa prosperidade;
- Trataremos um ataque cibernético ao Reino Unido com a mesma seriedade com que trataríamos um ataque convencional equivalente e nos defenderemos conforme necessário;

- Agiremos de acordo com as leis nacionais e internacionais e esperaremos que outros façam o mesmo;
- Protegeremos e promoveremos rigorosamente nossos valores fundamentais. Esses valores incluem a democracia, o estado de direito, a liberdade, governos e instituições abertos e responsáveis, direitos humanos e liberdade de expressão;
- Preservaremos e protegeremos a privacidade dos cidadãos do Reino Unido;
- Trabalharemos em parceria. Somente trabalhando com as Administrações Devolvidas, todas as partes do setor público, empresas, instituições e o cidadão individual, poderemos proteger com sucesso o Reino Unido no ciberespaço;
- O governo cumprirá suas responsabilidades e liderará a resposta nacional, mas as empresas, as organizações e os cidadãos individuais têm a responsabilidade de tomar medidas razoáveis para se proteger on-line e garantir que sejam resilientes e capazes de continuar operando no caso de um incidente;
- A responsabilidade pela segurança das organizações do setor público, incluindo a segurança cibernética e a proteção de dados e serviços on-line, é dos respectivos ministros, secretários permanentes e conselhos de administração;
- Não aceitaremos riscos significativos para o público e para o país como um todo como resultado de empresas e organizações que não tomarem as medidas necessárias para gerenciar as ameaças cibernéticas;
- Trabalharemos em estreita colaboração com os países que compartilham nossos pontos de vista e com os quais nossa segurança se sobrepõe, reconhecendo que as ameaças cibernéticas não conhecem fronteiras. Também trabalharemos de forma ampla com todos os parceiros internacionais para influenciar a comunidade em geral, reconhecendo o valor de coalizões amplas; e
- Para garantir que as intervenções do governo tenham um impacto substancial na segurança cibernética nacional geral e na resiliência, procuraremos definir, analisar e apresentar dados que meçam o estado da nossa segurança cibernética coletiva e o nosso sucesso no cumprimento das nossas metas estratégicas.

Objetivos/áreas de política:

- DEFENDER Temos os meios para defender o Reino Unido contra as ameaças cibernéticas em evolução, para responder com eficácia a incidentes e para garantir que as redes, os dados e os sistemas do Reino Unido sejam protegidos e resilientes. Os cidadãos, as empresas e o setor público têm o conhecimento e a capacidade de se defender.
- DETER O Reino Unido será um alvo difícil para todas as formas de agressão no espaço cibernético. Detectamos, entendemos, investigamos e interrompemos as ações hostis tomadas contra nós, perseguindo e processando os infratores. Temos os meios para tomar medidas ofensivas no espaço cibernético, se assim o desejarmos.
- DESENVOLVER Temos um setor de segurança cibernética inovador e crescente, sustentado por pesquisa e desenvolvimento científicos líderes mundiais. Temos um canal de talentos autossustentável que fornece as habilidades necessárias para atender às nossas necessidades nacionais nos setores público e privado. Nossa análise e especialização de ponta permitirão que o Reino Unido enfrente e supere ameaças e desafios futuros.

- Com base nesses objetivos, buscaremos a AÇÃO INTERNACIONAL e exerceremos nossa influência investindo em parcerias que moldem a evolução global do ciberespaço de forma a promover nossos interesses econômicos e de segurança mais amplos.

Indicadores: Possui métricas qualitativas de sucesso (por exemplo “nossas empresas mais importantes entendem o nível de ameaça” / “o número de empresas de cibersegurança aumentou”) - mas não tem metas ou indicadores claros
Governança:
Centro Nacional de Segurança Cibernética (NCSC) como autoridade de segurança cibernética do Reino Unido, compartilhando conhecimento, abordando vulnerabilidades sistêmicas e oferecendo liderança em principais questões nacionais de segurança cibernética.
Pela primeira vez, os principais setores poderão se envolver diretamente com a equipe do NCSC para obter a melhor aconselhamento e suporte para proteger redes e sistemas e sistemas contra ameaças cibernéticas.

Alinhamento Estratégico: Estratégia Nacional de Segurança
Marcos: Não há

País: Reino Unido
Nome: Estratégia Nacional de Cibersegurança 2022 - Pioneirismo em um futuro cibernético com todo o Reino Unido
Ano de publicação: 2022
Vigência: 2022-2030
Instituição a cargo da elaboração: Escritório de Segurança Cibernética e Proteção de Informações do Gabinete do Governo

Instituições participantes: Não definido
Estrutura: 5 pilares estratégicos com objetivos e ações associadas, além de uma seção com a governança.
Definição de cibersegurança: A proteção de sistemas conectados à Internet (incluindo hardware, software e infraestrutura associada), os dados neles contidos e os serviços que eles fornecem, contra acesso não autorizado, danos ou uso indevido. Isso inclui danos causados intencionalmente pelo operador do sistema ou acidentalmente, como resultado de não seguir os procedimentos de segurança ou de ser manipulado para fazê-lo.
Alcance: Toda a sociedade, com o governo liderando.
Visão: 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.
Princípios:

- Priorizaremos a capacidade dos cidadãos e das empresas de operar no ciberespaço de forma segura e protegida para que possam maximizar os benefícios econômicos e sociais da tecnologia digital e exercer seus direitos legais e democráticos;
- Trabalharemos para defender uma Internet aberta e interoperável como o melhor modelo para apoiar a prosperidade e o bem-estar globais, resistindo à pressão de

Estados autoritários em direção à fragmentação e à sua ideia de soberania na Internet;
- Faremos uso legal, proporcional e responsável de nossas capacidades cibernéticas, com o apoio de uma supervisão clara e do envolvimento do público e de nossos aliados, e responsabilizaremos os outros por comportamentos imprudentes ou indiscriminados no ciberespaço;
- Tomaremos medidas contra o uso criminoso do ciberespaço por todos os meios disponíveis, denunciando aqueles que usam representantes criminosos ou abrigam grupos criminosos em seus territórios e trabalhando para evitar a proliferação de capacidades cibernéticas de ponta para criminosos;
- Defenderemos uma abordagem inclusiva e de múltiplas partes interessadas nos debates sobre o futuro do ciberespaço e da tecnologia digital, defendendo os direitos humanos no ciberespaço e combatendo os movimentos em direção ao autoritarismo digital e ao controle estatal.

Objetivos/áreas de política:
- Pilar 1: Fortalecer o ecossistema cibernético do Reino Unido, investir em nosso pessoal e em nossas habilidades e aprofundar a parceria entre o governo, a academia e o setor
- Pilar 2: Construir um Reino Unido digital resiliente e próspero, reduzindo os riscos cibernéticos para que as empresas possam maximizar os benefícios econômicos da tecnologia digital e para que os cidadãos estejam mais seguros on-line e confiantes de que seus dados estão protegidos.
- Pilar 3: Assumir a liderança em tecnologias vitais para o poder cibernético, desenvolver nossa capacidade industrial e desenvolver estruturas para garantir tecnologias futuras
- Pilar 4: Promover a liderança e a influência global do Reino Unido para uma ordem internacional mais segura, próspera e aberta, trabalhando com parceiros do governo e do setor e compartilhando a experiência que sustenta o poder cibernético do Reino Unido
- Pilar 5: Detectar, interromper e dissuadir nossos adversários para aumentar a segurança do Reino Unido no e pelo ciberespaço, fazendo uso mais integrado, criativo e rotineiro de todo o espectro de alavancas do Reino Unido.

Indicadores: Não há

Governança:

(i) estabelecer um novo Conselho Consultivo Cibernético Nacional, convidando líderes seniores do setor privado e do terceiro setor para desafiar, apoiar e informar nossa abordagem;
(ii) expansão dos recursos de pesquisa do National Cyber Security Centre (NCSC), incluindo o novo centro de pesquisa aplicada em Manchester, com foco em tecnologias emergentes em áreas como locais conectados e transporte.
(iii) National Cyber Force – braço operativo da cibersegurança.

(iv) O Conselho de Segurança Nacional exercita supervisão ministerial da estratégia.

Alinhamento Estratégico: Estratégia de Segurança Nacional e normas de Infraestrutura Crítica.
Marcos: NCSC`s Cyber Assessment Framework

País: Portugal
Nome: Estratégia de Segurança do Ciberespaço Nacional
Ano de publicação: 2015
Vigência: não definido
Instituição a cargo da elaboração: Conselho de Ministros

Instituições participantes: não mencionado.
Estrutura: 4 objetivos organizados em 6 eixos de ação
Definição de cibersegurança: Não definido
Alcance: Geral
Visão: Não tem
Princípios:

- A estratégia é baseada nos princípios gerais de soberania do Estado, regras da UE, direitos fundamentais da UE, dados pessoais e privacidade.
- 5 pilares
    - 1- Subsidiariedade
    - 2 - Complementaridade
    - 3 - Cooperação
    - 4 - Proporcionalidade
    - 5 - Conscientização

Objetivos/áreas de política:

- Promover a conscientização, o uso livre, seguro e eficiente do ciberespaço;
- Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
- Fortalecer e garantir a segurança do espaço cibernético, das infraestruturas críticas e dos serviços vitais;
- Afirmar o ciberespaço como um local para o crescimento econômico e a inovação

Indicadores: Não tem
Governança: Se fala da necessidade, mas não tem muitas medidas concretas além de nomear o Centro Nacional de Cibersegurança.
Alinhamento Estratégico: Não definido
Marcos: Menciona Planos de Proteção de Infra Critica

País: Portugal

Nome: Estratégia Nacional de Segurança do Ciberespaço 2019-2023
Ano de publicação: 2019
Vigência: 2019-2023
Instituição a cargo da elaboração: Centro Nacional de Cibersegurança

Instituições participantes: Foi constituído um grupo de projeto, denominado Conselho Superior de Segurança do Ciberespaço, que teve como um dos seus objetivos propor a revisão e elaborar a nova Estratégia Nacional de Segurança do Ciberespaço.
Estrutura: Três objetivos estratégicos e eixos de intervenção

Definição de cibersegurança: Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Alcance: Geral
Visão: 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.
Princípios:

- Princípio da subsidiariedade
- Princípio da complementaridade
- Princípio da proporcionalidade

Objetivos/áreas de política:

- Objetivo estratégico 1 - Maximizar a resiliência:
  Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede de forma a salvaguardar a segurança do ciberespaço de interesse nacional face às ameaças que possam comprometer ou provocar a disrupção das redes e sistemas de informação essenciais à sociedade.
- Objetivo estratégico 2 - Promover a inovação:
  Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económico, social, cultural e de prosperidade.
- Objetivo estratégico 3 - Gerar e garantir recursos:
  Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço.

Indicadores: Não tem
Governança:

- Conselho Superior de Segurança do Ciberespaço como órgão específico de consulta do Primeiro-ministro que assegure a coordenação político-estratégica para a segurança do ciberespaço, com representantes de todas as partes interessadas, que garanta uma abordagem transversal e inclusiva relativamente às políticas e iniciativas desenvolvidas pelas diversas entidades com responsabilidades neste âmbito;

- Centro Nacional de Cibersegurança como Autoridade Nacional de Cibersegurança e, por inerência, como ponto de contacto único nacional para efeitos de cooperação internacional em matéria de cibersegurança, sem prejuízo das atribuições legais cometidas a outras entidades, nomeadamente, ao Ministério Público e à Polícia Judiciária, relativas a cooperação internacional em matéria penal, às Forças Armadas em matéria de ciberdefesa, ao Secretário-Geral do Sistema de Informações da República Portuguesa relativamente à produção de informações de segurança nacional, nas suas vertentes externa e interna e ao Secretário Geral do Sistema de Segurança Interna relativamente ao Ponto Único de Contacto em matéria de cooperação policial internacional e às situações de alerta e resposta rápidas às ameaças à segurança interna;

Alinhamento Estratégico: Estratégia Nacional de Combate ao Terrorismo, Estratégia TIC 2020 - Estratégia para a Transformação Digital na Administração Pública e a Estratégia de Inovação Tecnológica e Empresarial para Portugal 2018-2030.

Marcos: Não há

País: Canadá

Nome: Estratégia de segurança cibernética do Canadá

Para um Canadá mais forte e mais próspero

Ano de publicação: 2010

Vigência: Não definido

Instituição a cargo da elaboração: Ministério de Segurança Publica

Instituições participantes: Não explicito

Estrutura: 3 pilares

Definição de cibersegurança: Não definido

Alcance: Geral e inclui entidades subnacionais

Visão: A estratégia é o nosso plano para enfrentar a ameaça cibernética

Princípios: Não tem

Objetivos/áreas de política:

- A estratégia é construída sobre três pilares:
    1. Proteger os sistemas do governo
    2. Parceria para proteger sistemas cibernéticos vitais fora do governo federal
    3. Ajudar os canadenses a estarem seguros on-line

Indicadores: Não tem

Governança:

O Ministério da Segurança Pública do Canadá coordenará a implementação da Estratégia. No âmbito da Segurança Pública do Canadá, o Centro Canadense de Resposta a Incidentes Cibernéticos continuará a ser o ponto focal para monitorar e aconselhar sobre a atenuação das ameaças cibernéticas e direcionar a resposta nacional a qualquer incidente de segurança cibernética.

Alinhamento Estratégico: Policy on Government Security, relacionada aos serviços digitais, e Estratégia Nacional e Plano para Infraestrutura Crítica

Marcos: Não há

País: Canada
Nome: Estratégia Nacional de Cibersegurança - Visão do Canadá para a segurança e a Prosperidade na Era Digital
Ano de publicação: 2018
Vigência: Não definido
Instituição a cargo da elaboração: Ministro da Segurança Pública e Preparação para Emergências do Canadá
Instituições participantes: Em parceria com os Ministros da Defesa, Inovação, Infraestrutura, Serviços Públicos e o Conselho do Tesouro, foi realizada consulta pública.
Estrutura: 3 temas transversais
Definição de cibersegurança: A segurança cibernética é a proteção das informações digitais e da infraestrutura em que elas residem.
Alcance: Foco maior no governo.
Visão: Uma forte segurança cibernética é um elemento essencial da inovação e da prosperidade dos canadenses. Indivíduos, governos e empresas querem ter confiança nos sistemas cibernéticos que sustentam suas vidas diárias. O Governo do Canadá prevê um futuro em que todos os canadenses desempenhem um papel ativo na formação e manutenção da resiliência cibernética de nossa nação.
Princípios:

- Proteger a segurança e a proteção dos canadenses e da nossa infraestrutura crítica
- Promover e proteger os direitos e as liberdades on-line
- Incentivar a segurança cibernética para os negócios, o crescimento econômico e a prosperidade
- Colaborar e apoiar a coordenação entre jurisdições e setores para fortalecer a resiliência cibernética do Canadá
- Adaptar-se proativamente às mudanças no cenário da segurança cibernética e ao surgimento de novas tecnologias

Objetivos/áreas de política:

- Segurança e resiliência: Por meio de ações colaborativas com parceiros e capacidades aprimoradas de segurança cibernética, protegeremos melhor os canadenses contra cibercrime, responder às ameaças em evolução e defender os sistemas críticos do governo e do setor privado.
- Inovação cibernética: Ao apoiar a pesquisa avançada, promover a inovação digital e desenvolvimento de habilidades e conhecimentos cibernéticos, o governo federal posicionará o Canadá como líder global em segurança cibernética.
- Liderança e colaboração: O governo federal, em estreita colaboração com as províncias, territórios e o setor privado, assumirá um papel de liderança para promover a segurança cibernética no Canadá e, em coordenação com aliados, trabalhará para moldar o ambiente internacional de segurança cibernética a favor do Canadá.

Indicadores: Não tem
Governança: Se prevê a elaboração de planos de ação de segurança cibernética para complementar a estratégia. Esses planos detalharão as iniciativas específicas que o governo federal empreenderá ao longo do tempo, com métricas de desempenho claras e o

compromisso de informar sobre os resultados alcançados. Eles também descreverão o plano do governo para trabalhar com parceiros internos e externos para alcançar sua visão.
Alinhamento Estratégico: A implementação dessa estratégia será alinhada com outras iniciativas relacionadas ao governo do Canadá. Entre elas estão: o mandato do Ministro das Instituições Democráticas para defender o processo eleitoral de ameaças cibernéticas; a política externa cibernética na agenda internacional do Canadá; o uso da cibernética pelos militares canadenses; e o Plano de Inovação e Habilidades.
Marcos: Não há.

País: Estados Unidos
Nome: A Estratégia Nacional Para um Ciberespaço Seguro
Ano de publicação: 2003
Vigência: Não definido
Instituição a cargo da elaboração: Casa Branca por meio de um grupo e depois o DHS foi criado

Instituições participantes: O processo de desenvolvimento da Estratégia incluiu a solicitação de opiniões dos setores público e privado. Para isso, a Casa Branca patrocinou reuniões em prefeituras sobre segurança do ciberespaço em dez áreas metropolitanas. Consequentemente, setores individuais (por exemplo, educação superior, governo estadual e local, bancário e financeiro) formaram grupos de trabalho para criar estratégias iniciais de segurança do ciberespaço. A Casa Branca criou um painel consultivo presidencial, o Conselho Consultivo de Infraestrutura Nacional, composto por líderes dos principais setores da econômicos, governamentais e acadêmicos.
Estrutura: 3 macrobjetivos e 5 prioridades nacionais (ações para o governo federal e recomendações para os outros atores)
Definição de cibersegurança: Não definido
Alcance: Geral
Visão: Não tem
Princípios:
1. Um esforço nacional
2. Proteger a privacidade e as liberdades civis
3. Regulamentação e força de mercado - o governo não regulamentará
4. Prestação de contas
5. Flexibilidade
6. Planejamento plurianual

Objetivos/áreas de política:

Os objetivos estratégicos são:

- Prevenir ataques cibernéticos contra as infraestruturas críticas dos EUA;
- Reduzir a vulnerabilidade nacional a ataques cibernéticos; e
- Minimizar os danos e o tempo de recuperação de ataques cibernéticos que ocorram.

As prioridades:

- Prioridade I: um sistema nacional de resposta à segurança do espaço cibernético.
- Prioridade II: um programa nacional de redução de ameaças e vulnerabilidades à segurança do espaço cibernético
- Prioridade III: Um Programa Nacional de Conscientização e Treinamento em Segurança do Espaço Cibernético.
- Prioridade IV: Proteger o espaço cibernético dos governos
- Prioridade V: Segurança nacional e cooperação internacional em segurança do ciberespaço

Indicadores: Não tem
Governança: Cada departamento vai elaborar um plano e um programa para executar as iniciativas contidas na estratégia. O Departamento de Segurança Interna (DHS) vai ser o ator central na implementação e coordenação seja dentro do governo seja as ações recomendadas para academia e setor privado.
A estratégia menciona que cada departamento vai ser responsável pela sua performance, medidas através de medidas de performance que serão sugeridas
Alinhamento Estratégico: É um componente de implementação da
Estratégia Nacional de Segurança Interna e é complementada por uma Estratégia Nacional para a Proteção Física de Infraestruturas Críticas e dos principais ativos.
Marcos: Não tem

País: EUA
Nome: Estratégia Nacional de Ciber
Ano de publicação: 2018
Vigência: Não definido
Instituição a cargo da elaboração: Casa Branca

Instituições participantes: Não definido
Estrutura: 4 pilares
Definição de cibersegurança: Não definido
Alcance: Geral
Visão: Não tem
Princípios: Não tem
Objetivos/áreas de política:

- Pilar I - Proteger o povo americano, a pátria e o modo de vida americano
  OBJETIVO: Gerenciar os riscos de segurança cibernética para aumentar a segurança e a resiliência das informações e dos sistemas de informação do país.
- Pilar II - Promover a prosperidade americana
  OBJETIVO: Reservar a influência dos Estados Unidos no ecossistema tecnológico e o desenvolvimento do ciberespaço como um mecanismo aberto de crescimento econômico, inovação e eficiência.
- Pilar III - Preservar a paz pela força
  OBJETIVO: Identificar, combater, interromper, degradar e deter o comportamento no espaço cibernético que seja desestabilizador e contrário aos interesses nacionais,

enquanto preservando a superioridade dos Estados Unidos no e através do ciberespaço.

- Pilar IV - Avançar a influência americana
  OBJETIVO: Preservar a abertura de longo prazo, interoperabilidade, segurança e confiabilidade a longo prazo da Internet, que apoia e é reforçada pelos interesses dos interesses dos Estados Unidos.

Indicadores: Não tem
Governança: O Conselho de segurança Nacional vai coordenar com a área do orçamento para ter recursos. Os Departamentos e Ministérios executarão suas missões informados pela Estratégia.

Alinhamento Estratégico: Usa os pilares da Estratégia de Segurança Nacional e as ordens executivas de Infraestrutura Crítica
Marcos: Não há.

País: EUA
Nome: Estratégia Nacional de Cibersegurança
Ano de publicação: 2023
Vigência: Não definido
Instituição a cargo da elaboração: Casa Branca
Instituições participantes: Processo interministerial seguido de processo de consulta com o setor privado e a sociedade civil
Estrutura: 5 pilares
Definição de cibersegurança: Não definido
Alcance: Geral (governo federal, estados e setor privado)
Visão: Não tem
Princípios: Não tem
Objetivos/áreas de política:
5 pilares
I - Defesa de infraestruturas críticas
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

Indicadores: Não tem
Governança:
O NSC vai trabalhar com todas as agencias para desenvolver um plano de ação e assegurar o orçamento. Dizem que o plano vai ter dados e medir efetividade e métricas.
Alinhamento Estratégico: Estratégia de Segurança Nacional e Estratégia de Defesa
Marcos: NIST
Modelo de Proteção da Infra Crítica: Executive Order13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Presidential Directive 21, Presidential Directive 41.

País: Nova Zelandia
Nome: Estratégia Nacional de Cibersegurança
Ano de publicação: 2015
Vigência: Não definido
Instituição a cargo da elaboração: Ministério das Comunicações

Instituições participantes: Não mencionado
Estrutura: 4 objetivos
Definição de cibersegurança: Não definido
Alcance: Geral
Visão: Nossa visão é que a nova Zelândia seja segura, resiliente e próspera on-line
Princípios:

- As parcerias são essenciais
- O crescimento econômico é viabilizado
- A segurança nacional é mantida
- Os direitos humanos são protegidos

Objetivos/áreas de política:

- Resiliência
- Capacidade
- Endereçando cibercrime
- Cooperação Internacional

Indicadores: Não tem
Governança: Não definida
Alinhamento Estratégico: National Plan to Address Cybercrime
Marcos: Não tem

País: Nova Zelandia
Nome: Estratégia Nacional de Cibersegurança – Fazendo a NZ prosperar online
Ano de publicação: 2019
Vigência 2019 -2023
Instituição a cargo da elaboração: Ministro da Radiodifusão, Comunicações e Mídia Digital

Instituições participantes: não mencionado

Estrutura: 5 áreas prioritárias
Definição de cibersegurança: Proteger as pessoas e seus computadores, redes, programas e dados contra acesso não autorizado, exploração ou modificação não autorizadas.
Alcance: A estratégia destaca iniciativas para indivíduos, empresas e governo
Visão: Essa estratégia tem a visão de que a Nova Zelândia está confiante e segura no mundo digital - trata-se de permitir que a Nova Zelândia prospere on-line. Queremos que os

neozelandeses aproveitem ao máximo as oportunidades oferecidas por um mundo cada vez mais conectado, sem sofrer danos ou perdas. A visão reconhece que, embora a conectividade traga riscos, podemos tomar medidas para minimizá-los, e que a conectividade se tornou vital para a sociedade e a economia da Nova Zelândia.
É uma oportunidade para o governo da Nova Zelândia assumir a liderança na resposta aos riscos cibernéticos, mas também para alcançarmos essa visão como nação.

Princípios:
- criar e manter a confiança;
- centrar nas pessoas, de forma respeitosa e inclusiva;
- equilibrar o risco com agilidade e adaptabilidade;
- usar nossos pontos fortes coletivos para obter melhores resultados e resultados
- ser aberto e responsável.

Nossos valores:
- As parcerias são fundamentais
- As pessoas estão seguras e os direitos humanos são respeitados
- O crescimento econômico é aprimorado
- A segurança nacional é protegida

Objetivos/áreas de política:

- Cidadãos ativos e conscientes dos riscos de segurança
- Ecossistema e força de trabalho de cibersegurança fortes e capazes
- País Internacionalmente ativo
- País resiliente e responsivo
- Proativamente combater o cibercrime

Indicadores: Não tem
Governança: Um programa de trabalho anual acompanhará a estratégia. O programa de trabalho descreverá uma série de ações de ações para avançar em cada uma dessas áreas prioritárias.
O ministro responsável divulgará um relatório anual público sobre o progresso de cada uma das áreas prioritárias.
Alinhamento Estratégico: Não tem
Marcos: Não tem


BID