INCC
INSTITUTO NACIONAL DE COMBATE AO CRIME CIBERNÉTICO

AS CONTRIBUIÇÕES DA SOCIEDADE CIVIL E DOS SETORES PRODUTIVOS PARA A ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA

JUNTOS POR UM AMBIENTE DIGITAL MAIS SEGURO PARA TODOS


JUNTOS POR UM AMBIENTE DIGITAL
MAIS SEGURO PARA TODOS

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

EQUIPE INCC

Fundador & Chairman

Fábio Diniz

Fundadora e CEO

Luana Tavares

Diretor de Pesquisa e Segurança Pública

Leandro Piquet

Especialista em *Advocacy*

Emília Vasconcelos

Diretor Jurídico

Sérgio Presta

Diretora de Risco Securitário

Marta Schuh

Diretor de Projetos Especiais

Lucas Porto

Diretor de Risco Cibernético

Antônio Brasiliano

Diretor Financeiro

Anderson Santos

Especialista em Atividade Policial

Paulo Cezar Mcgregor

Especialista em Segurança da Informação

Sérgio Estrela Martins

Diretor de Direito Digital

Rony Vainzof

APOIO TÉCNICO:

MacroPlan
Consultoria e Analytics

VLK Direito, Inovação & Tecnologia

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

AGRADECIMENTOS

ESPECIALISTAS E COLABORADORES TÉCNICOS

Andriei Guttierrez

Antonio Brasiliano
Caio Cesar Lima
Carlos Afonso
Fábio Diniz
Glaucio Neves
João Henrique Martins
Leandro Piquet

Lucas Porto

Luciano Tuma

Marcelo Asquino
Marco Gonzalez
Maria Izabel C. Mello
Mariana Ortiz
Ronaldo Andrade
Rony Vainzof

Ygor Cezar

COORDENAÇÃO TÉCNICA

Luana Tavares

INSTITUIÇÕES PARTICIPANTES

FECOMERCIO - Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo
MBC – Movimento Brasil Competitivo
FEBRABAN – Federação Brasileira dos Bancos
ONS – Operador Nacional do Setor Elétrico
CNF – Confederação Nacional do Setor Financeiro
FIESP – Federação das Indústrias do Estado de SP
ABES - Associação Brasileira das Empresas de Software
ABRASCA – Associação Brasileira das Cias de Capital Aberto
ACREFI – Associação Nacional das Instituições de Crédito, Financiamento e Investimento
APIIMF - Associação de Infraestruturas do Mercado Financeiro
DEIC/DCCIBER – Polícia Civil/SP
FBI – Federal Bureau of Investigation

PRINCIPAIS INSTITUIÇÕES CUJOS ESTUDOS SUBSIDIARAM ESTE RELATÓRIO

Fundação Getúlio Vargas/RJ
Instituto Igarapé
ITU – International Telecommunication Union (ONU)
MIT - Massachussets Institute of Technology
Harvard University
Cybersecurity Centre – Oxford University
ANPD – Agência Nacional de Proteção de Dados
ANEEL – Agência Nacional de Energia Elétrica
ANATEL – Agência Nacional de Telecomunicações
TCU – Tribunal de Contas da União
CGU - Controladoria Geral da União
Fórum Brasileiro de Segurança Pública
Ministério Público de São Paulo
BID – Banco Interamericano de Desenvolvimento
GSI – Gabinete de Segurança Institucional
IBGE – Instituto Brasileiro de Geografia e Estatística
IPEA – Instituto de Pesquisa Econômica Aplicada
ENAP – Escola Nacional de Administração Pública
Banco Central do Brasil
SENAC
SEBRAE
NIST.gov
NIC.BR
CERT.BR
Safernet.org

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME

APRESENTAÇÃO

Vivemos em uma era em que a segurança cibernética se tornou uma preocupação global — e o Brasil não está imune a este desafio. Por meio deste trabalho, o Instituto Nacional de Combate ao Cibercrime (INCC) e diversos setores da sociedade, propõem uma reflexão profunda sobre os desafios atuais e futuros do Brasil no cenário da segurança cibernética.

O presente documento é fruto de um esforço conjunto entre o INCC e sua rede de parceiros e colaboradores, e representa um marco significativo na jornada de fortalecimento da segurança digital no Brasil. Ao conectar diferentes atores e indicar caminhos que possam contribuir no aumento da maturidade e resiliência cibernética do Brasil, este projeto encara a segurança cibernética como uma preocupação latente e incontornável em âmbito global atualmente.

Nesse sentido, dada a dimensão dos impactos econômicos e sociais associados a este tema, pode-se afirmar a necessidade de posicioná-lo entre as prioridades do Estado, buscando firmar diretrizes e garantir sua constante evolução. Nossa abordagem, refletida neste documento, não apenas identifica esses desafios a partir de uma perspectiva nacional, mas também aponta caminhos claros para fortalecermos nossas defesas cibernéticas e aumentarmos nossa resiliência diante das ameaças digitais.

Acreditamos firmemente que a solução para esses entraves reside na colaboração estreita entre o estado, setor privado e sociedade civil na construção de uma verdadeira cultura de segurança cibernética. Por isso, o que será exposto a seguir é o resultado de um trabalho que uniu especialistas de diversas áreas a fim de proporcionar uma visão abrangente e integrada, capaz de contribuir para a árdua missão de se revisar a Estratégia Nacional de Cibersegurança do Brasil engajando tomadores de decisão e compartilhando responsabilidades.

Esta é uma contribuição inédita da sociedade para o fortalecimento da segurança no ambiente virtual do Brasil. As informações contidas neste documento não são apenas um conjunto de diretrizes, mas um convite para a união de esforços em torno de soluções que garantam maior preparo do diferentes atores evolvidos na prevenção e resposta aos ataques cibernéticos.

Juntos, podemos construir um ambiente digital mais seguro e próspero para todos.

Atenciosamente,

Fábio Diniz
Fundador e Presidente

Luana Tavares
Fundadora e CEO

AS CONTRIBUIÇÕES DA SOCIEDADE CIVIL E DOS SETORES PRODUTIVOS PARA A ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA

Sumário

1 METODOLOGIA 07

2 INTRODUÇÃO 12

3 CONCEITOS GERAIS DE CIBERSEGURANÇA 17

4 CONTEXTO CIBERSEGURANÇA NO MUNDO 19

5 CONTEXTO CIBERSEGURANÇA NO BRASIL 23

6 CAMINHOS PARA O DESENVOLVIMENTO 28

7 EIXOS ESTRATÉGICOS DE DESENVOLVIMENTO 30

- 1 Conscientização da sociedade 31
- 2 Adequação do capital humano 42
- 3 Engajamento e integração multi-institucional 54
- 4 Informações e conhecimento especializado 60
- 5 Financiamento e incentivos 65
- 6 Arcabouço legal, regulatório e normativo 72

8 PROPOSIÇÕES PRIORIZADAS 86

9 CONCLUSÃO 93

1. Metodologia

No cenário contemporâneo, é inegável o vínculo entre a tecnologia, o cotidiano e a interconexão online. Nesse sentido, como reflexo do panorama de revolução digital no qual o mundo se insere, o Relatório do Fórum Econômico Mundial (WEF) intitulado "The Global Risks Report 2024" destaca a insegurança cibernética como um risco global, cujos impactos se estendem tanto a curto quanto a longo prazo, sendo uma preocupação que demanda atenção imediata e estratégica.

Nesse contexto, frente ao contexto socioeconômico e estrutural do Brasil e à urgência de uma resposta eficaz, o **Instituto Nacional de Combate ao Cibercrime (INCC)** surge como uma organização da sociedade civil voltada para a promoção de pesquisas, diálogos e projetos direcionados à construção de uma agenda robusta de segurança cibernética e combate aos crimes cibernéticos no país.

A partir da promulgação da **Política Nacional de Cibersegurança (PNCiber)** e a criação do **Comitê Nacional de Cibersegurança (CNCiber)**, abrem-se caminhos para contribuir de forma imprescindível quanto a definição dos rumos que essa temática tomará em âmbito nacional. Tal contexto reforça a importância de se engajar a sociedade civil e os setores produtivos na elaboração de uma nova **Estratégia Nacional de Cibersegurança**, de modo não apenas a orientar as políticas públicas, mas também fortalecer uma atuação conjunta para sua efetiva implementação nos próximos anos.

A abordagem deste trabalho parte da percepção de que a cibersegurança – o que inclui toda a complexidade que a envolve - requer uma resposta multifacetada e colaborativa, englobando diversos setores da sociedade. Através da sistematização de temas, influência na agenda nacional, diálogo com os decisores políticos, e mobilização pública, busca-se estabelecer uma base sólida para enfrentar esse desafio, promovendo um ambiente digital mais seguro e resiliente para todos.

Assim sendo, tal iniciativa priorizou a participação ativa de tomadores de decisão com diferentes perspectivas sobre o problema, combinando técnicas qualitativas e quantitativas a fim de explorar as diferentes facetas do cibercrime em território nacional, como será visto a seguir.

RESUMO DAS ETAPAS DE CONSTRUÇÃO

DIAGNÓSTICO DO PROBLEMA
(Nov.23-Fev.24)

- 230 estudos e bases de dados consultadas
- Dezenas de conversas com Lideranças Privadas e Públicas, Especialistas e Profissionais de Tecnologia e Cibersegurança
- Discussões com representantes de cerca de 15 setores da Economia

DEFINIÇÃO DE CRITÉRIOS PARA PROPOSIÇÕES
(Mar.24)

- Critérios Definidos:
  1) Conteúdo Estratégico
  2) Factibilidade de Execução

COLETA DE PROPOSIÇÕES
(Abr.24-Mai.24)

- 12 Entidades Setoriais Consultadas por meio de *Survey*
- 10 Setores da Economia Representados
- 52 Propostas Recebidas (Entidades + Comitê Técnico)
- 20 Propostas Priorizadas

AVALIAÇÃO E SISTEMATIZAÇÃO DAS PROPOSIÇÕES
(Mai.24)

- Comitê Técnico: 13 integrantes de perfil multidisciplinar (Segurança Pública, Risco Cibernético, Cibersegurança, Políticas Públicas, Economia, Cooperação Internacional, Advocacy)

CONSOLIDAÇÃO E ENVIO PARA O GSI – GABINETE DE SEGURANÇA INSTITUCIONAL
(Jun.24)

- Relatório Técnico Preliminar para apoiar Comitê Nacional de Cibersegurança e elaboração da Estratégia Nacional

DIVULGAÇÃO ABERTA E ACOMPANHAMENTO DA AGENDA
(Jul.24 em diante)

- Fóruns de Discussão, Disseminação para a Sociedade
- Acompanhamento e Apoio para Implementação das Medidas Estratégicas

DETALHAMENTO DAS ETAPAS DE CONSTRUÇÃO

Etapa 1 - DIAGNÓSTICO DO PROBLEMA

Através de pesquisa qualitativa e conversas aprofundadas, foi possível a consolidação de um material robusto acerca do cenário de cibersegurança no Brasil. O produto deste esforço foi um profundo **Diagnóstico da Cibersegurança no Brasil**, elaborado com o apoio da VLK Advogados e diversos especialistas. Durante esta primeira etapa, conduziu-se um extenso diagnóstico dos problemas e das medidas atuais acerca da cibersegurança e cibercrimes no Brasil, contando, ainda, com exemplos de países que implementaram estratégias bem-sucedidas nesta temática.

Etapa 2 - DEFINIÇÃO DE CRITÉRIOS PARA INICIATIVAS

O Comitê de Especialistas do INCC, a partir do Diagnóstico realizado, sugeriu dois critérios para a priorização das iniciativas. O primeiro critério se refere ao **conteúdo estratégico**, ou seja, iniciativas que tenham caráter estratégico e alcance multisetorial, capazes de solucionar ou preparar a solução de um gargalo relevante no eixo em que está vinculado, no horizonte de execução da agenda estratégica. Paralelamente, o segundo critério diz respeito à **factibilidade de execução**, portanto, inciativas que sejam factíveis operacionalmente e financeiramente dentro do horizonte de execução da agenda.

Etapa 3 - COLETA DE PROPOSIÇÕES

A etapa de Coleta de Proposições foi conduzida por meio do preenchimento de um formulário pelos membros associados à iniciativa. O objetivo era consolidar sugestões de caminhos e **medidas multissetoriais capazes de enfrentar os desafios apresentados** no Diagnóstico realizado, de forma participativa e colaborativa, unindo os diversos setores da sociedade das diferentes esferas.

As sugestões levaram em consideração os 6 eixos estratégicos, permitindo que cada participante propusesse até cinco iniciativas por eixo estratégico apresentado. Como resultado, foi possível coletar 52 propostas de solução com foco no aumento da resiliência cibernética do Brasil por meio da contribuição de 12 entidades setoriais e organizações sociais, além de 13 especialistas integrantes do Comitê Técnico.

Etapa 4 - AVALIAÇÃO E SISTEMATIZAÇÃO DAS PROPOSIÇÕES

A sistematização das proposições aconteceu por meio da análise qualitativa das propostas e passou pelo crivo do **Comitê Técnico do INCC**. O comitê foi formado por especialistas em diversas áreas do tema, como direito digital; risco cibernético; governança; segurança pública; economia; e políticas públicas. Ademais, esses especialistas representavam diferentes entes da sociedade civil organizada, havendo representantes do setor público; setor privado; terceiro setor, além de atores internacionais. Nele foi estabelecido um processo de **avaliação, validação e priorização das propostas**.

A avaliação se deu através dos dois critérios definidos: conteúdo estratégico e factibilidade de execução. Desta forma, foram estabelecidos as proposições prioritárias consolidadas neste relatório, além de novas proposições para os eixos que demonstraram necessidade de incremento.

Etapa 5 – CONSOLIDAÇÃO E ENVIO PARA O GSI – GABINETE DE SEGURANÇA INSTITUCIONAL

Após a sistematização, consolidou-se um **documento preliminar**, o qual foi enviado oficialmente ao Gabinete de Segurança Institucional da Presidência da República, de modo a contribuir com as discussões do CNCiber – Comitê Nacional de Cibersegurança e servir de insumo para a formulação da Estratégia Nacional de Cibersegurança.

Etapa 6 – DIVULGAÇÃO ABERTA E ACOMPANHAMENTO DA AGENDA

Realizada a primeira entrega, o INCC e sua rede de parceiros organizarão diversos encontros para disseminação pública deste conteúdo, bem como acompanharão e apoiarão a implementação das prioridades oficializadas.

O resultado deste trabalho ficará disponível para toda a sociedade como uma contribuição essencial para tomadores de decisão em todas as áreas, seja do setor público ou privado, acerca da temática de cibersegurança no Brasil.

Tais esforços serão encampados para que a agenda permaneça na agenda pública nacional e gere resultados positivos para o Brasil nos próximos anos, a partir da redução do número de crimes cibernéticos, melhorando a economia e a vida de todos os cidadãos brasileiros.

ATORES E CONTEÚDOS ENVOLVIDOS

1. Introdução

A presente iniciativa apresenta uma abordagem estratégica abrangente para enfrentar os desafios críticos de resiliência cibernética no Brasil. Considerando as principais referências globais e o contexto brasileiro, nossa contribuição com este trabalho é a de estimular a transformação da cultura nacional de segurança no ciberespaço. Dessa forma, a visão central, **"Um Ambiente Digital Mais Seguro para Todos"**, representa o objetivo maior de um trabalho que busca engajar diversos setores da sociedade na construção de um ambiente digital mais seguro.

Para tanto, foi conduzido um extenso diagnóstico sobre os problemas e as medidas atuais relativas à cibersegurança e aos cibercrimes no Brasil, além de analisar exemplos de países com estratégias bem-sucedidas nesta área. Este processo envolveu dezenas de conversas com especialistas, acadêmicos e autoridades, pesquisa secundária e consulta a mais de **230 estudos e bases de dados**, bem como diálogos com cerca de **10 setores econômicos**, compreendendo aproximadamente 70% da produção nacional, buscando um entendimento profundo do cenário brasileiro de cibersegurança.

A partir deste mapeamento, foram identificadas diversas perspectivas relevantes para o futuro da cibersegurança brasileira, agrupadas em **06 Eixos Estratégicos e uma visão central**. Estes elementos fundamentam a construção de propostas capazes de aumentar a resiliência cibernética do Brasil, por meio da união de esforços e da transformação cultural e comportamental na sociedade como um todo.

Nas primeiras sessões deste documento, são apresentados um resumo de dados contextuais sobre cibersegurança, além de informações sobre o cenário internacional e nacional, destacando a posição do Brasil em relação às práticas de outros países que se destacaram na melhoria de suas capacidades de proteção no ambiente cibernético. Em seguida, há uma síntese de dados relevantes relacionados aos seis Eixos Estratégicos propostos, além de sugestões para objetivos, metas e proposições que podem contribuir nos desafios identificados.

Figura 1: Visão geral do documento

Há 50 anos, seria praticamente impossível alguém conseguir imaginar as mudanças que ocorreriam em consequência do desenvolvimento tecnológico. A internet foi, e continua sendo, a grande propulsora da inovação e criação de novos instrumentos tecnológicos[1]. Expressões como IoT, 5G, big data, inteligência artificial, criptoativos, crimes cibernéticos, incidentes de segurança, ransomware, phishing, estão cada vez mais presentes no dia a dia das pessoas[2].

Atualmente, o mundo possui cerca de 8 bilhões de pessoas. Desse número, aproximadamente 5 bilhões de pessoas possuem smartphones e acesso a internet[3]. No Brasil, segundo levantamento feito pela FGV[4] no ano de 2023, existem 464 milhões de dispositivos digitais (computador, notebook, smartphone e tablet) ativos, considerando o uso doméstico e corporativo. Conforme censo do IBGE[5], a população brasileira é de aproximadamente 203 milhões de pessoas. Deste modo, é evidente o engajamento digital da população brasileira, que cada vez mais, está rodeada de novas tecnologias.

Com base nas informações acima, existe uma **tendência de dependência cada vez maior de pessoas e empresas em relação aos instrumentos tecnológicos**, que avançam e se desenvolvem rapidamente, permeando a vida em sociedade por conta das facilidades proporcionadas. Cada vez mais, as pessoas estão:

a) Navegando na internet;

b) Interagindo em redes sociais;

c) Adquirindo dispositivos inteligentes conectados à internet (IoT – Internet of Things)

d) Utilizando a internet como meio de obtenção de informações/notícias;

e) Utilizando a internet para trabalho e aprendizagem;

f) Usando recursos de streaming e jogando online;

g) Adotando novas tecnologias como Realidade Virtual, Realidade Aumentada e assistentes de voz.

Fontes:

1. Ideia trazida por Kevin Kelly, fundador da revista de tecnologia norte americana Wired em sua obra "Inevitável", onde o autor sugere que o desenvolvimento de novas tecnologias está sendo impulsionado pelas mesmas forças que proporcionaram o avanço e desenvolvimento da Internet, e que possivelmente continuarão se expandindo e viabilizando o surgimento de novas tecnologias embrionárias. KELLY, Kevin. Inevitável: as 12 forças tecnológicas que mudarão nosso mundo.

2. Frequentemente é possível visualizar na mídia notícias e reportagens sobre os temas mencionados, demonstrando a sua presença cada vez maior na sociedade, como por exemplo: De acordo com pesquisa feita pela SonicWall (uma das maiores fornecedoras de defesa contra malwares do mundo), o Brasil é o quarto país mais afetado por ataques de ransomware, ficando atrás apenas dos Estados Unidos, do Reino Unido e da Espanha, no ano de 2023. O Relatório e os principais pontos da pesquisa estão disponíveis em: https://www.sonicwall.com/pt-br/news/o-relatorio-de-ameacas-ciberneticas-sonicwall-2023-lanca-uma-nova-luz-sobre-as-linhas-de-frente-em-constante-mudanca-e-o-comportamento-dos-agentes-de-ameacas/ Conforme Relatório da Kaspersky, baseado em dados de junho de 2022 a julho de 2023, o Brasil teve 134 milhões de tentativas de phishing em um ano. Matéria disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/ Sobre criptoativos, o Presidente da República, no dia 22/12/2022, sancionou a Lei 14.478 que trata de aspectos regulatórios dos ativos virtuais, trazendo conceitos, classificações, exceções de aplicabilidade, dentre outros pontos. A Lei está disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14478.htm.

3. Conforme Relatório Digital 2022 – China: The essencial Guide to the Latest Connected Behaviours, pg. 7. Disponível em: https://wearesocial.com/cn/wp-content/uploads/sites/8/2022/01/DataReportal-GDR100-20220208-Digital-2022-China-v01.pdf

4. Artigo "Uso de TI no Brasil: País tem mais de dois dispositivos digitais por habitante, revela pesquisa". Disponível em: https://portal.fgv.br/noticias/uso-ti-brasil-pais-tem-mais-dois-dispositivos-digitais-habitante-revela-pesquisa.

5. Disponível em: https://censo2022.ibge.gov.br/panorama/?utm_source=ibge&utm_medium=home&utm_campaign=portal

6. How People Use The Internet in 2023. Broadband Search. Disponível em: https://www.broadbandsearch.net/blog/how-people-use-the-internet

Entretanto, especificamente no caso da realidade brasileira, houve um fenômeno onde **o avanço da inclusão digital foi consideravelmente maior do que a educação digital**, gerando o problema político social do "analfabetismo digital"[7]. Como país em desenvolvimento, grande parte da população brasileira não tem conhecimento sobre crimes virtuais e ameaças cibernéticas, se tornando presas fáceis e vulneráveis de crackers[8] (hackers maliciosos / blackhats) e organizações cibercriminosas, uma vez que existe um movimento cada vez maior de migração dos crimes patrimoniais para o ambiente virtual[9], tendo em vista as facilidades ofertadas pela sensação de anonimato. Nada disso é ensinado em escolas e somente tratado em cursos de graduação ou pós-graduação que tenham previsão sobre os temas na grade curricular.

Deste modo, fica claro como o avanço tecnológico impacta diretamente as pessoas, sujeitando-as aos mais diversos tipos de prejuízos e ameaças cibernéticas que podem ser ocasionadas por conta do "analfabetismo digital". Em perspectiva semelhante, empresas e órgãos públicos precisam aprimorar seus mecanismos de segurança para enfrentar os desafios de uma sociedade cada vez mais digitalizada, impedindo assim, que dados pessoais e outros tipos de informações confidenciais sejam acessados por ciber criminosos ou terceiros não autorizados.

A falta de conhecimento específico e preparo tecnológico constituem grande problema e são responsáveis por deixar pessoas e entidades (públicas e privadas) em situações de vulnerabilidade[10]. Neste sentido, o desenvolvimento de uma nova **Estratégia Nacional de Cibersegurança** elaborada em parceira com diversas entidades e coordenada pelo Estado, poderá contribuir de forma significativa para o desenvolvimento do ecossistema de segurança cibernética brasileiro, impulsionando medidas e ações para o aumento da maturidade geral de segurança digital e dos mecanismos de persecução de criminosos que cometem ilícitos cibernéticos.

Além dos pontos já mencionados, essa pauta se torna cada vez mais necessária diante do movimento de digitalização do governo, incluindo o desenvolvimento de ferramentas financeiras com tecnologias mais avançadas, como o PIX e o DREX.

Fontes:

7. Tal conceito é utilizado por Patrícia Peck em sua obra "Direito Digital", onde ela menciona que o "analfabetismo digital" é fruto da desigualdade entre países desenvolvidos e em desenvolvimento, sendo um problema político-social que retrata o despreparo das pessoas para aprender a utilizar novas tecnologias. Segundo a autora: "[...] ao mesmo tempo que a Era Digital abre maiores possibilidades de inclusão, a exclusão torna-se mais cruel". PINHEIRO, Patrícia Peck. Direito Digital. 6. ed. São Paulo: Editora Saraiva. 2016. Pg. 70

8. Crackers são Hackers mal-intencionados (black hats) que exploram vulnerabilidades que poderão ser posteriormente utilizadas para fazer chantagens, derrubar sistemas e, inclusive, vendidas para outros indivíduos que podem fazer o que desejarem com essas informações. FIGUEIREDO, Leandro; ZANI, Filipe. A migração dos crimes patrimoniais para a internet, ante a consolidação do mercado paralelo na venda de malwares e vulnerabilidades zero-day na deep web. In: PATURY, Fabrício (Coord). Prospecção sobre a evolução e futuro dos crimes cibernéticos. 1. Ed. Salvador: Faculdade Baiana de Direito, 2019, pg 84.

9. Por conta da utilização massiva de computadores e smartphones pelas pessoas, é crescente o cometimento de ilícitos por meio da internet, uma vez que, está mais fácil para os criminosos induzir as pessoas à erro (por exemplo, se utilizando da técnica fraudulenta do phishing) para atingirem seus objetivos, bem como pela existência de uma sensação de segurança por parte do criminoso, que consegue obter altas vantagens em prejuízo alheio, sem sair da frente de seu dispositivo conectado a internet. DIAS, Daniela; MENESES, Livanilda. O avanço das facções criminosas tradicionais para a internet, objetivando a venda de produtos ilícitos. In: PATURY, Fabrício (Coord). Prospecção sobre a evolução e futuro dos crimes cibernéticos. 1. Ed. Salvador: Faculdade Baiana de Direito, 2019, pg 104.

10. O uso de tecnologias por pessoas sem o preparo adequado pode trazer grandes consequências. De acordo como autor Joseph Steinberg, como o uso, dependência e confiança das pessoas nas tecnologias está crescendo, os efeitos de um incidente de segurança ou vazamento de dados podem ser devastadores, abalando a situação financeira e credibilidade de grandes empresas, bem como a saúde, reputação e até mesmo a vida das pessoas. STEINBERG, Joseph. Cibersegurança para leigos. 1. ed. Rio de Janeiro: Editora Alta Books. 2020. Pg. 01

O PIX foi introduzido para a população brasileira no ano de 2020[11]. Em pouco tempo, este recurso foi massivamente adotado, chegando a ser o meio de pagamento mais utilizado (acima de dinheiro e cartão) em 2023[12], segundo estudo da McKinsey. Na linha do que já foi mencionado, os criminosos seguem as tendências tecnológicas, se aproveitando das facilidades das tecnologias para aplicar golpes e realizar fraudes. Em pesquisa realizada pela empresa Silverguard, quatro em cada dez entrevistados alegaram ter sido vítimas de golpes e fraudes por esse meio de pagamento, sendo constatado um volume de 1,7 milhões de golpes utilizando o PIX[13]. QRs Codes falsos, phishings, comprovantes de transferência falsos, clonagem de aplicações - são apenas alguns exemplos[14] de como essas fraudes são executadas por cibercriminosos, que se aproveitam da **falta de conhecimento da população em se defender dessas ameaças**.

Se o contexto com o PIX se apresenta desta maneira, é possível imaginar que o mesmo poderá ocorrer com a implementação do DREX. Conforme descrito pelo Banco Central, o DREX é o real em formato digital, emitido em plataforma digital operada pelo Banco Central (BC). Trata-se de Moeda Digital de Banco Central, ou CBDC (Central Bank Digital Currency)[15], nome como este formato de moeda é conhecido internacionalmente. Ainda segundo o Banco Central, o DREX proporcionará aos brasileiros[16] acesso a produtos e serviços tradicionais com mais segurança, bem como acesso a contratos inteligentes e protocolos de intermediações para compra e venda de forma otimizada.

Entretanto, toda inovação traz consigo riscos inerentes. Segundo o Fundo Monetário Internacional[17], as vulnerabilidades atreladas ao uso de CBDC podem ser exploradas para comprometer o sistema financeiro de uma nação. Os CBDCs apresentam capacidade de acumular dados confidenciais de pagamentos em escala nunca vista. Nas mãos erradas, tais dados podem ser utilizados para monitorar as transações dos cidadãos, obter detalhes sensíveis de segurança e sobre práticas de indivíduos e organizações e até desviar dinheiro. Se implementado sem protocolos de segurança adequados e sem conscientização correta da população, uma CBDC poderia ampliar consideravelmente as ameaças de segurança e privacidade já existentes em sistemas financeiros de diversos países, incluindo o Brasil, que já está em fase de testes[18] com essa tecnologia.

Fontes:
11. Informação disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2020/11/pix-e-lancado-oficialmente-e-esta-disponivel-para-todos-os-clientes-das-734-instituicoes-cadastradas
12. https://www.cnnbrasil.com.br/economia/pix-passa-dinheiro-e-e-mais-usado-para-pagamentos-que-transferencias-diz-pesquisa/#:~:text=Mais%20Pix%20que%20dinheiro&text=Isto%20deixou%20a%20modalidade%20em,fatia%20de%2010%25%20dos%20pagamentos.
13. Informações disponíveis em: https://www.cnnbrasil.com.br/economia/mais-de-17-milhao-de-golpes-com-pix-foram-aplicados-em-2022-mostra-levantamento/#:~:text=Um%20estudo%20divulgado%20na%20terça,usar%20esse%20meio%20de%20pagamento.
14. Informações disponíveis em: https://www.cnnbrasil.com.br/economia/caiu-no-golpe-do-pix-saiba-o-que-fazer-e-como-se-proteger/
15. Informações disponíveis em: https://www.bcb.gov.br/meubc/faqs/p/drex
16. Informações em: https://www.bcb.gov.br/meubc/faqs/p/beneficios-do-drex
17. Mais informações em: https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr
18. Informações em: https://www.bcb.gov.br/meubc/faqs/p/lancamento-do-drex

a. Cibersegurança

Cibersegurança é definido pelo National Institute of Standards and Technology ("NIST")[19], como ***"o processo de proteção da informação por meio da prevenção, detecção e resposta a ataques",*** de modo que, podemos compreender, para os fins deste estudo, cibersegurança como "*conjunto de práticas voltadas para prevenir, detectar, responder e* reprimir cibercrimes".

b. Crimes Cibernéticos

Os crimes cibernéticos são condutas que satisfazem três requisitos:

- **Ser típicas:** isto é, que se enquadram perfeitamente em uma descrição legal prevista como crime, normalmente chamado de "tipo" penal;
- **Ser antijurídicas**: isto é, contrárias ao ordenamento jurídico, inexistindo qualquer causa que exclua a licitude da ação, como a legítima defesa; e
- **Ser culpáveis**: atuação deve se operar com dolo (ou seja, intenção de cometer a conduta e obter o resultado), ou, nas hipóteses em que é admitida, culpa (ou seja, o agente não deseja obter o resultado, mas atua com imperícia, imprudência ou negligência).

Quando nos referimos a "crimes cibernéticos", utilizando-se da tecnicidade jurídica, estamos, em verdade, nos referindo aos crimes de informática, também chamados de crimes virtuais ou digitais, os quais podem ser definidos como aqueles que, para sua prática, utilizam-se de "*meios informáticos como instrumento de alcance e resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos*"[20].

Esses crimes podem ser subdivididos em duas categorias [21]**:**

- **Crimes informáticos próprios:** aqueles voltados para o próprio sistema de informática, seja o hardware, seja o software. É o caso, por exemplo, do crime de invasão de dispositivo informático com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (art. 154-A, do Código Penal).
- **Crimes informáticos impróprios**: são condutas criminosas que são praticadas por meio de sistema informático, mas que poderiam ser praticados de outra forma. É o caso, por exemplo, do crime de estelionato (popularmente conhecido como "golpe"), que, embora a execução possa se operar de forma independente de sistemas informáticos, não raro utilizam-se de meios digitais.

Fontes:
19. Definição de cibersegurança, disponível em: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Acesso em 11.12.2023
20.TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. Ed. Saraivajur. P. 591-592.
21.TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. Ed. Saraivajur. P. 593-594.

Com efeito, é importante ressaltar que vem se identificando um movimento de migração dos crimes patrimoniais, como o roubo, para modalidades como furtos, golpes e estelionatos virtuais, conforme informações promovidas pelo Anuário Brasileiro de Segurança Pública[22], de modo que **parte significativa dos crimes informáticos, senão a sua maioria, ocorrem na modalidade imprópria**, sendo fruto da migração destas condutas para o ambiente virtual e, consequentemente, do alcance massificado que estas práticas passam a ter.

c. Incidentes de Segurança, eventos de segurança e ataques

É necessário compreender, também, o que são eventos de segurança, incidentes de segurança e ataques, os quais não se confundem com o conceito de crimes cibernéticos.

Um evento de segurança pode ser interpretado como uma ocorrência identificada relativa ao estado de um sistema, rede ou serviço que possivelmente se caracterize enquanto violação de uma política de segurança da informação, falha de proteção ou uma situação desconhecida[23]. Assim, evento é qualquer ocorrência que possa, potencialmente, se caracterizar enquanto um incidente de segurança, ou seja: todo incidente de segurança é um evento de segurança, mas o inverso não é verdadeiro.

O Incidente de Segurança, por sua vez, é um (ou mais) evento de segurança indesejado ou inesperado que tenha alta probabilidade de comprometer a segurança da informação e o adequado funcionamento de uma organização[24]. Note-se que, em que pese muitos crimes cibernéticos envolverem incidentes de segurança, essas figuras não se confundem:

- é possível existir um **incidente de segurança sem que haja um crime cibernético** (ex. um colaborador elimina, por acidente, um arquivo)
- é possível, embora mais difícil, que exista um **crime cibernético sem incidente de segurança** (ex. utilizando-se apenas de dados da vítima que foram publicamente disponibilizados pela própria vítima, o criminoso convence a vítima a transferir uma data soma em dinheiro). Essa situação, no entanto, é mais rara, e, em regra, crimes cibernéticos envolvem, no mínimo, a utilização de informações que deveriam ser sigilosas, mas são obtidas de alguma forma pelo criminoso, seja pela própria vítima, seja por meio de um incidente anterior.

Por fim, ataques podem ser descritos como **práticas que objetivam violar a confidencialidade, integridade ou disponibilidade de um ativo** (ex. o destruindo, expondo, alterando, inutilizando, roubando, obtendo acesso não autorizado ou fazendo uso não autorizado[25]). Um ataque sempre gera um evento de segurança, com ataques bem-sucedidos caracterizando-se enquanto incidentes.

Ataques, em regra, caracterizam-se enquanto crimes informáticos, minimamente, enquadrando-se, caso malsucedido, no tipo penal de invasão de dispositivo informático na modalidade tentada.

Fontes:
22. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em 11.12.2023
23. BAARS, Hans *et al*. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Ed. Brasport.p. 12
24. BAARS, Hans *et al*. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Ed. Brasport.p. 14
25. BAARS, Hans et al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Ed. Brasport.p. 11

Conforme Relatório do Fórum Econômico Mundial (WEF) "The Global Risks Report 2024"[26], a insegurança cibernética é um risco de características globais com impacto no curto prazo (2 anos) e longo prazo (10 anos), conforme demonstrado na imagem a seguir:

O relatório traz conclusões relevantes, como:

- Novas ferramentas tecnológicas viabilizarão novas fontes de recursos financeiros para organizações criminosas, com o cibercrime oferecendo um fluxo de receitas com baixo risco e baixo custo para crime organizado;
- Os ataques de phishing estão evoluindo, principalmente por conta da possibilidade de tradução fácil e precisa de voz e vídeos para a maioria dos idiomas, por meio da IA generativa;
- Existe uma crescente preocupação entre os executivos de diversos países sobre o aumento da insegurança cibernética.

a. Países Referência em Cibersegurança

Os países mais avançados em segurança cibernética e considerados mais seguros digitalmente podem ser identificados por meio de índices e estudos. Duas importantes referências são o **National Cyber Power Index (NCPI)** da Harvard University e o **Global Cybersecurity Index (GCI)**.

Segundo o NCPI de 2022[27], considerando os objetivos constantes no documento, os seguintes países são considerados os mais avançados em capacidades cibernéticas:

Fontes:
26. The Global Risks Report 2024 , disponível em https://www.weforum.org/publications/global-risks-report-2024/
27. Disponível em:
https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

Tabela 1. NCPI 2022 - TOP 20 Most Comprehensive Cyber Powers

Rank	2022
1	Estados Unidos
2	China
3	Rússia
4	Reino Unido
5	Australia
6	Holanda
7	ROK
8	Vietnã
9	França
10	Iran

Elaboração própria

Além disso, na última edição do GCI (2020)[28], no ranking desse estudo, constam os seguintes países como os mais avançados em maturidade cibernética:

Tabela 2. GCI results: Global Score and Rank

País	Score	Rank
Estados Unidos	100	1
Reino Unido	99,54	2
Arabia Saudita	99,54	2
Estonia	99,54	3
Coreia	99,48	4
Singapura	98,52	4
Espanha	98,52	4
Rússia	98,06	5
Emirados Árabes Unidos	98,06	5
Malasia	98,06	5
Lituania	97,93	6
Japão	97,82	7
Canada	97,67	8
França	97,6	9
Índia	97,5	10
Turquia	97,49	11
Australia	97,47	12
Luxemburgo	97,41	13
Alemanha	97,41	13
Portugal	97,32	14
Letônia	97,28	15
Holanda	97,05	16
Noruega	96,89	17
Ilhas Maurício	96,89	17
Brasil	**96,6**	**18**

Elaboração própria

Fonte: 28. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Esses indicadores e pontuações do ranking refletem uma combinação de capacidades técnicas, medidas legais e organizacionais, investimentos em infraestrutura de cibersegurança, e uma abordagem proativa e preventiva para o desenvolvimento de políticas e de cooperação internacional em cibersegurança. Os países líderes nos rankings assumiram um compromisso no controle e combate às ameaças cibernéticas e a promoção de um ambiente digital mais seguro e robusto.

Para a classificação dos países no CGI[29], foram considerados os países com os maiores índices de capacidade em:

- Leis e regulamentos sobre crimes cibernéticos e segurança cibernética;
- Implementação de capacidades técnicas por meio de agências nacionais e setoriais;
- Estratégias e organizações nacionais para fortalecimento da segurança cibernética;
- Campanhas de sensibilização, formação, educação e incentivos para o desenvolvimento de capacidades em matéria de cibersegurança;
- Parcerias entre agências, empresas e países.

b. Modelos de Governança em Cibersegurança

Diversos países possuem Agências ou Centros Nacionais focados exclusivamente em cibersegurança. Essas estruturas atuam como ponto de contato para empresas dos mais diversos portes, órgãos públicos, autoridades e a população de forma geral, prestando suporte e auxílio em incidentes de segurança, ações de resiliência, educação, dentre outras formas de atuação para mitigação de riscos cibernéticos.

No Reino Unido, o National Cyber Security Centre[30], traz orientações sobre como gerenciar incidentes de segurança de forma adequada, visando efetivamente detectar, responder e resolver incidentes, bem como ensinando a como criar os próprios processos de resposta. Além disso, no portal eletrônico consta uma série de outras diretrizes e orientações sobre cibersegurança

Fonte:
29. Disponível em: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.
30. National Cyber Security Centre , do Reino Unido, disponível em: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes#im

Nos Estados Unidos, o Cybsersecurity & Infrastructure Security Agency ("CISA") tem a missão de auxiliar a sociedade e o governo estadunidense a compreender, gerenciar e reduzir os riscos relacionados ao ambiente cibernético e infraestruturas físicas. Em seu site, há diversas informações úteis sobre boas práticas, treinamentos e canais de reporte de incidentes cibernéticos.

Já na Australia, o Australian Signals Directorate's Australian Cyber Security Centre é a entidade responsável por promover os esforços do governo em cibersegurança. Assim como as outras agências mencionadas, dispõe de um portal eletrônico com vasta quantidade de boas práticas em segurança da informação, tanto para a sociedade civil quando para órgãos governamentais.

Exemplo recente na América Latina, **em 08 de Abril de 2024 o Governo Chileno aprovou a Lei Número 21.663, que institui o novo Marco da Cibersegurança Nacional.** A iniciativa visa estabelecer um quadro institucional para fortalecer a segurança cibernética; ampliar e fortalecer o trabalho preventivo; formar uma cultura pública em relação à segurança digital; enfrentar contingências nos setores público e privado e proteger a segurança das pessoas no ciberespaço. Além disso, a lei prevê a criação da Agência Nacional de Cibersegurança (ANCI) com poderes regulatórios, de supervisão e sancionatórios, e cria o Conselho Multissectorial de Cibersegurança, bem como cria uma Equipe Nacional de Resposta a Incidentes de Segurança Informática (CSIRT Nacional).

A inexistência de uma Agência ou Centro governamental de cibersegurança no Brasil pode ampliar a vulnerabilidade cibernética do país, principalmente pela ausência de políticas e diretrizes padronizadas e pelo avanço do desenvolvimento tecnológico e da cibercriminalidade. Ainda que existam órgãos e iniciativas governamentais que tratam de aspectos de cibersegurança, a falta de uma estrutura de coordenação, integração e governança dedicada exclusivamente ao tema pode afetar o avanço no nível de maturidade do país em cibersegurança.

Em agosto de 2020, foi publicada a Revisão da Capacidade de Cibersegurança[33] do Brasil baseado em Modelo de Maturidade desenvolvido pela Universidade de Oxford, no Reino Unido.

A título de comparação, a tabela a seguir compara as capacidades de segurança cibernética do Brasil em 2020 e do Reino Unido em 2015:

Tabela 3. Tabela comparativa entre Brasil e Reino Unido

Estágio	BR (2020)	UK (2015)
Formativo	71%	14%
Estabelecido	29%	62%
Estratégico	0%	14%
Dinâmico	0%	10%

Elaboração própria

É possível perceber que o **Reino Unido em 2015 já tinha capacidades cibernéticas mais avançadas do que as apresentadas pelo Brasil em 2020**. Dados do governo britânico mostram que nesses cinco anos foram investidos uma média de 1,35 bilhão de reais anualmente, enquanto a média brasileira no mesmo período foi de apenas 15 milhões de reais.

Assim, fica claro que existe uma necessidade maior de investimento por parte do governo brasileiro nas iniciativas de cibersegurança, de modo a reduzir a discrepância do seu nível de maturidade em relação ao nível dos países mais avançados, como o Reino Unido. Deste modo, com medidas e estratégias de segurança mais adequadas à realidade brasileira, será possível reduzir o impacto e os danos ocasionados por ataques cibernéticos.

Segundo o relatório do **CNM 2023, uma série de intervenções foram feitas desde a última versão, publicada em 2020**. As principais intervenções incluem o desenvolvimento de planos legais para a proteção de infraestruturas críticas (CI), a formalização da coordenação da resposta a incidentes dentro do governo federal e a assinatura da Convenção de Budapeste sobre Crime Cibernético.

Ainda que tenha ocorrido avanços no Brasil nos últimos anos, tais como,

- Avanços na legislação como, por exemplo, o Marco Civil da Internet, LGPD e Lei do "Cyberbullyng"[34];
- Criação de delegacias especializadas em crimes cibernéticos em diversos estados da federação [35];

Fontes:
31. Artigo "Uso de TI no Brasil: País tem mais de dois dispositivos digitais por habitante, revela pesquisa". Disponível em: https://portal.fgv.br/noticias/uso-ti-brasil-pais-tem-mais-dois-dispositivos-digitais-habitante-revela-pesquisa.
32. Disponível em: https://censo2022.ibge.gov.br/panorama/?utm_source=ibge&utm_medium=home&utm_campaign=portal
33. Disponível em: https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf

- Promulgação da Convenção de Budapeste;
- Criação de unidades especializadas de combate à criminalidade cibernética na Polícia Federal
- Desenvolvimento da Política Nacional de Cibersegurança pelo GSI e aprovada por Decreto do Presidente da República;

Estas melhorias ou não foram suficientes ou ainda não refletiram na redução dos números que indicacam que o país está mitigand de forma satisfatória os riscos relacionados a segurança cibernética e garantindo maior resiliência cibernética.

O crime cibernético vem aumentado em complexidade, e os impactos financeiros por conta de incidentes e exploração de vulnerabilidades são cada vez maiores[36]. À medida que a tecnologia aumenta entre os governos e se permeia na sociedade, pessoas e entidades que não estão preparadas para enfrentar esses novos desafios tecnológicos possuem altas chances de se tornarem vítimas de cibercriminosos mal-intencionados. Diante desse cenário, é importante reconhecer que, mesmo entidades com medidas de segurança robustas, elas **nunca estarão completamente imunes e invulneráveis a ataques cibernéticos**, já que estão sempre em evolução.

Ataques sofisticados e execução de diversos tipos de crimes podem ocorrer a partir de um dispositivo eletrônico em qualquer lugar do mundo. Invasão de contas, roubo de identidade e informações financeiras[37], venda de drogas e armas[38], comercialização de pornografia infantil[39], fraudes[40], dentre outros, são apenas alguns exemplos de crimes que podem ocorrer por meios digitais, sem fronteiras físicas. Além disso, as ameaças cibernéticas estão sendo potencializadas[41] pelo uso de Inteligência Artificial.

a) Impactos dos cibercrimes nas empresas e cidadãos

Considerando a realidade das empresas e outros tipos de entidades da sociedade civil, os crimes cibernéticos podem ocasionar danos reputacionais[42], por exemplo, por incidentes de segurança da informação, permitindo acesso indevido aos dados pessoais por terceiros não autorizados, trazendo publicidade negativa que pode prejudicar a organização e esgotar a confiança do titular. Consequências jurídicas podem ser enfrentadas caso seja comprovado que as medidas de segurança aplicadas não eram suficientes para impedir a ocorrência do incidente.

Por conta desse fator, existe um dilema entre as empresas sobre notificar ou não os incidentes. Vale ressaltar, que no cenário da LGPD, não é qualquer incidente de segurança que envolva dados pessoais que deve ser notificado, e sim, os incidentes que possam ocasionar “risco ou dano relevante”, conforme descrito no artigo 48 da Lei.

Fonte:
34. Disponível em: https://www12.senado.leg.br/noticias/audios/2024/01/agora-e-lei-bullying-e-cyberbullying-sao-crimes-previstos-no-codigo-penal
35. Disponível em: São Paulo - https://www.saopaulo.sp.gov.br/spnoticias/governo-do-estado-inaugura-divisao-de-crimes-ciberneticos-2/, Amapá - https://mpap.mp.br/noticias/gerais/mp-ap-participa-de-inauguracao-de-delegacia-de-crimes-ciberneticos e Piauí https://www.pi.gov.br/noticia/secretaria-da-seguranca-publica-inaugura-reforma-da-delegacia-de-repressao-e-combate-aos-crimes-de-informatica-em-teresina.
36. Cyber Crime: Its Impact on Government, Society and the Prosecutor. United States Agency for International Development. Disponível em: https://pdf.usaid.gov/pdf_docs/Pnada641.pdf.
37. Disponível em: https://www.usa.gov/identity-theft.
38. Drug related cybercrime and associated use of the Internet. Overview, analysis and possible actions by the Pompidou Group. Disponível em: https://rm.coe.int/drug-related-cybercrime-and-associated-use-of-the-internet-overview-an/168075ae1c
39. Disponível em: https://www.policechiefmagazine.org/child-pornography-on-the-internet-new-challenges-require-new-ideas/
40. Disponível em: https://www.allowme.cloud/conteudoallowme-2023-02-14-estudo-allowme-olx/
41. Informações em: https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals/#:~:text=AI%20presents%20another%20avenue%20for,potentially%20yield%20greater%20financial%20gains.
42. Disponível em: https://www.compuquip.com/blog/effects-of-cybercrime-for-business-the-hidden-costs#:~:text=Cybersecurity%20breaches%20can%20result%20in,customers%2C%20and%20settling%20legal%20claims.

Empresas de todos os portes também estão sujeitas aos impactos ocasionados pela cibercriminalidade, principalmente as pequenas e médias empresas ("PME"). As PMEs normalmente atribuem menor importância ao tema de cibersegurança e possuem também menos recursos para implementar controles de defesa cibernética, se encontrando em situação de maior vulnerabilidade e sendo um alvo mais fácil para cibercriminosos mal-intencionados. Importante destacar que a exploração de vulnerabilidades cibernéticas gera incidentes de segurança, que possuem diversas implicações legais, como por exemplo, a necessidade de notificação para a Autoridade Nacional de Proteção de Dados ("ANPD") quando o incidente puder ocasionar risco ou dano relevante[48] para os titulares de dados pessoais.

Adicionalmente, é crucial ressaltar que esses incidentes, além dos danos aos titulares e à própria reputação da empresa, também geram altos custos financeiros. Segundo o relatório "Cost of a Data Breach Report", realizado pela IBM, o custo médio de um incidente de segurança envolvendo dados pessoais, no Brasil, pode chegar a aproximadamente 1,2 milhões de dólares[49].

A segunda edição do "Barômetro da Segurança digital", pesquisa encomendada pela Mastercard ao Instituto Datafolha[50], revelou que **64% das empresas brasileiras são alvo de fraudes e ataques digitais com média ou alta frequência**, um **crescimento de 7% se comparado com a primeira edição**, divulgada em 2021.

A mesma pesquisa levantou que cibersegurança **é considerada muito importante para mais de 84% das companhias**, mas não é uma prioridade no orçamento para 23% delas. Apenas **35% das empresas entrevistadas possuem uma área própria de cibersegurança** e somente uma em cada quatro empresas tem planejamento anual para segurança digital. Quando questionados sobre a Lei Geral de Proteção de Dados (LGPD), 81% dos entrevistados responderam que a legislação trouxe benefícios para as organizações.

Em relação a estratégia de segurança**, 79% afirmam ter um plano de resposta a um possível ataque cibernético**, mas apenas um terço fez algum tipo de teste preventivo nos três meses antecedentes à realização da pesquisa. Em relação à composição de times, **cresceu de 44% para 53% o índice de empresas com muita dificuldade para encontrar profissionais para gerir o sistema de segurança digital**.

Além disso, os cidadãos brasileiros não estão imunes à criminalidade cibernética, principalmente os grupos mais vulneráveis. Em 2023, a SaferNet (organização não governamental que defende e promove os direitos humanos na internet) **relatou um aumento de 70% no compartilhamento de imagens de abuso e/ou exploração sexual infantil** reportadas à entidade não governamental e encaminhadas ao Ministério Público[47]. Em sentido semelhante, entre 2022 e 2023, foram registrados no Brasil 134 milhões de tentativas de phishing, representando um aumento de 436% em relação ao ano anterior.

O phishing é uma técnica comumente utilizada pelos criminosos para induzir as pessoas a erro e assim, conseguir obter dados pessoais e informações confidenciais que podem ser utilizadas para fraudar identidade, ganhar acesso e controle indevido a dispositivos eletrônicos dentre outros usos, incluindo composição de banco de dados para usos ilícitos e/ou fraudulentos.

Fontes:
47. Disponível em: https://new.safernet.org.br/content/denuncias-de-imagens-de-abuso-e-exploracao-sexual-infantil-online-compartilhadas-pela
48. LGPD. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
49. Disponível em: https://www.ibm.com/br-pt/reports/data-breach?utm_content=SRCWW&p1=Search&p4=437000788930020 67&p5=p&gad_source=1&gclid=EAIaIQobChMIuMii1N_4gwMVqhCtBh2X7giXEAAYASAAEgL0hvD_BwE&gclsrc=aw.ds.
50. Disponível em: https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/2024/fevereiro/64-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/#:~:text=A%20segunda%20edi%C3%A7%C3%A3o%20do%20%E2%80%9CBar%C3%B4metro,primeira%20edi%C3%A7%C3%A3o%2C%20divulgada%20em%202021.

b) Impactos dos cibercrimes nos entes governamentais

No âmbito governamental, o impacto e os danos dos crimes cibernéticos **podem levar criminosos a lograr êxito em obter segredos nacionais, causar altas turbulência nas operações de um país e influenciar no exercício da atividade política**. À título de exemplo, no ano de 2021, o site do Ministério da Saúde foi alvo de ataque, derrubando o acesso ao site e ocasionando a interrupção das plataformas "ConecteSUS" e "Portal Covid"[43]. Em março de 2022, um ataque cibernético tornou indisponível todos os serviços realizados pelo Tribunal Regional Federal da 3ª Região[44], inclusive a realização de audiências e julgamentos. O Tribunal de Justiça do Rio Grande do Sul[45], em 2021, foi vítima de um ransomware, onde criminosos conseguiram acessar informações sobre processos e julgamentos, além de acessar dados pessoais de colaboradores do Tribunal.

Para se ter uma ideia das fragilidades de entes governamentais, segundo a Lista de Alto Risco (LAR) da Administração Pública Federal, publicada pelo Tribunal de Contas da União (TCU)[46] em 2022, **74,6% das organizações (306 de 410) não possuem política de backup aprovada** formalmente e **66% das organizações que afirmam realizar backups** (254 de 385), apesar de implementarem mecanismos de controle de acesso físico ao local de armazenamento desses arquivos, **não os armazenam criptografados**.

A Lista de Alto Risco (LAR) da Administração Pública Federal, ainda identifica três grandes problemas relacionados à segurança da informação e segurança cibernética que são, a **inadequação da macroestrutura nacional,** responsável pela governança e gestão de Segurança da Informação e de Segurança Cibernética, a **incapacidade da APF** em responder e tratar incidentes de segurança e as **diversas vulnerabilidades** de segurança da informação e de segurança cibernética em grande parte das organizações públicas federais.

- **74,6%** das organizações (306 de 410) não possuem política de backup aprovada formalmente
- **71,2%** das organizações que hospedam seus sistemas em servidores/máquinas próprios (265 de 372) não possuem plano de backup específico para seu principal sistema
- **66%** das organizações que afirmam realizar backup
- **62%** em estágio de capacidade inexpressivo em continuidade institucional
- **60,2%** das organizações (247 de 410) não mantêm suas cópias em ao menos um destino não acessível remotamente
- **Mais de 80%** em estágios iniciais de capacidade em gestão de continuidade institucional e de continuidade de serviços de TI
- **46%** em estágio de capacidade inexpressivo em continuidade de serviços de TI

Fontes:
43. Informações em: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/
44. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2022/03/30/ataque-hacker-deixa-indisponiveis-servicos-do-trf-3.ghtml
45. Disponível em: https://www.correiobraziliense.com.br/politica/2021/04/4921336-grave-ataque-cibernetico-paralisa-sistema-de-justica-do-rio-grande-do-sul.html
46. Disponível em: https://sites.tcu.gov.br/listadealtorisco/index.html

Segundo o JP Morgan[51], há 4 pilares que o setor público deve focar para se prevenir de ataques cibernéticos e aumentar seu nível de maturidade:

1. **Tratar Cibersegurança como uma prioridade:** A gestão de riscos cibernéticos deve ser tratada como prioridade pelo Estado. As consequências de um incidente de segurança no âmbito governamental pode afetar seriamente a segurança nacional por conta, por exemplo, da exposição de informações confidenciais de Estado, que podem ser acessadas por criminosos em caso de exploração de vulnerabilidades.

2. **Realização de Treinamento e Conscientização:** Muitas vezes o colaborador que utiliza um computador ou dispositivo móvel de forma indevida, conectado à determinada rede do governo, pode trazer grandes prejuízos. Por isso é importante a realização regular de exercícios e treinamentos para mantê-los atualizados sobre as ameaças cibernéticas e como devem responder. Quanto mais treinamentos e testes, mais diligentes os colaboradores serão por possuir práticas e conhecimentos adequados e úteis à sua realidade.

3. **Cultura de preparação e prevenção cibernética:** Neste ponto, a recomendação é a utilização de frameworks de segurança cibernética reconhecidos mundialmente. Uma importante referência é o Cybersecurity Framework (CSF)[52], desenvolvido pelo NIST (National Institute of Standards and Technology). O referido framework possui ferramentas para definição de parâmetros de referência, identificação de prioridades, implementação de táticas de gestão de riscos, medição de progresso, dentre outros. Usando esta abordagem, as entidades governamentais podem ajudar a levar a sua preparação a um nível que possa atender ao atual cenário de ameaças. Além do framework do NIST, existe também o framework da ISO 27001[53], desenvolvido pela ISO (International Institute of Standardization) que também pode ser útil para prevenção, detecção e remediação de ameaças cibernéticas e gerenciamento de risco de segurança da informação.

4. **Contar com experiência de terceiros:** As entidades governamentais – especialmente a nível estadual e local – nem sempre podem ter recursos internos ou orçamento necessário para implementar de forma satisfatória os controles de segurança cibernética. Complementar a abordagem de segurança cibernética com terceiros pode ajudar a amadurecer as práticas de cibersegurança.

Fontes:
51. Disponível em: https://www.jpmorgan.com/insights/cybersecurity/business-email-compromise/threat-public-sector
52. Mais informações em: https://www.nist.gov/cyberframework
53. Mais informações em: https://www.iso.org/standard/27001

Complementarmente e de forma alinhada às sugestões acima, o Fórum Econômico Mundial[54] sugere 3 ações específicas para o avanço da maturidade em segurança cibernética de um Estado:

1. **Utilização e desenvolvimento de frameworks:** Os países devem ser mais rápidos na atualização ou desenvolvimento de estratégias nacionais de segurança cibernética, incluindo medidas jurídicas e regulamentares sobre o ciberespaço. Estas iniciativas devem ser compostas por uma abordagem multilateral, incluindo a construção de capacidades sólidas de resposta a incidentes em todos os setores. Os governos não devem agir de forma isolada e a participação da comunidade técnica e do setor privado são essenciais para o aprimoramento das capacidades cibernéticas de um Estado.

2. **Aperfeiçoamento da Cooperação Internacional:** Um exemplo próximo de cooperação internacional é a rede CSIRTAmericas, uma comunidade de Equipes de Resposta a Incidentes de Segurança Informática (CSIRTs) no Hemisfério Ocidental, em que o Brasil figura como membro. Em situações de crise, como o caso do ransomware Wannacry e da pandemia da COVID-19, este grupo fazia reuniões virtuais para compartilhar informações e dados em tempo real e trocar conhecimentos para contornar os desafios regionais próprios de cada país.

3. **Reforçar e unificar campanhas de conscientização, principalmente para crianças:** Ninguém está imune a um incidente cibernético. Organizações e pessoas a qualquer momento podem ser vítimas de cibercrimes. É necessário assim aumentar a conscientização em todas as idades e níveis, independentemente do setor. É de suma importância educar crianças sobre segurança cibernética, já que cada vez mais, as tecnologias se encontram presentes entre essa categoria de titulares. Considerando o rápido avanço tecnológico, as crianças precisam ser educadas cedo para aprender as habilidades e conhecimentos sobre cibersegurança que serão uteis ao longo da vida. Também é importante a união entre os governos e o setor privado, realizando campanhas de conscientização de forma unificada para evidenciar e comunicar o tema.

Tais ações podem auxiliar o Brasil no amadurecimento de suas políticas, práticas e ações de cibersegurança, se tornando um país digitalmente seguro e dificultando as ações de cibercriminosos. Apesar dos esforços, o Brasil tem um longo caminho para atingir um nível sofisticado em segurança cibernética e figurar ao lado dos países com os melhores indicadores em cibersegurança. Nos próximos tópicos, serão listados os principais entraves e desafios aos quais o Brasil está sujeito, incluindo ainda possíveis soluções que podem ser implementadas, consideradas a partir de uma ótica multisetorial.

Fonte:
54. https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/

6. Eixos Estratégicos

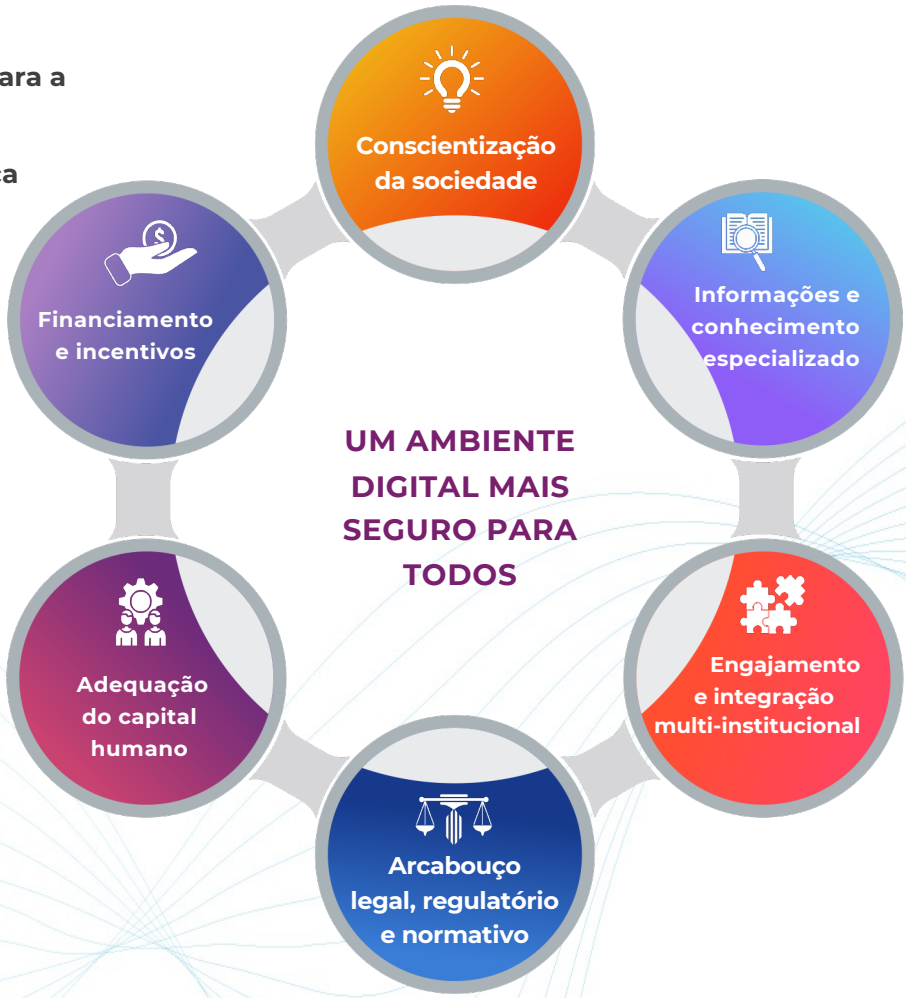
A partir do mapeamento de contexto e cenário realizado, foram constatadas diversas perspectivas relevantes para o futuro da cibersegurança brasileira. Estas perspectivas **foram agrupadas em 6 Eixos Estratégicos e uma Visão Central**, com o objetivo de possibilitar o aprofundamento de dados que facilitarão a construção de **contribuições para a Estratégia Nacional de Cibersegurança**.

Os seis Eixos Estratégicos levam em consideração as principais **referências do mundo e o contexto brasileiro**, se tratando de uma **contribuição inédita e efetiva** para que o país possa fazer frente aos **entraves mais críticos para o aumento da resiliência cibernética do Brasil.**

A Visão Central representa o objetivo maior que um país pode almejar ao desenvolver um **trabalho que transforme a cultura nacional e fortaleça o ecossistema de segurança no ciberespaço**, garantindo o engajamento dos mais diversos setores da sociedade na construção de um ambiente digital mais seguro para todos.

Nas páginas a seguir haverá um detalhamento e **apresentação em profundidade de cada um dos eixos estratégicos**, seguindo a lógica de expor o contexto atual, os desafios prioritários e referências nacionais e internacionais. Além disso, serão apresentadas sugestões de **objetivos, metas e proposições** que possam impulsionar o Brasil no alcance desta visão e enfrentar os entraves apontados no levantamento.

Figura 2. Eixos Estratégicos para a Resiliência da Cibersegurança Brasileira



1 Conscientização da Sociedade

O primeiro eixo, Conscientização da Sociedade, tem como intuito o aumento do nível de conhecimento da sociedade, o engajamento social e autonomia na prevenção e proteção cibernética.

I. Contexto do Eixo

Este eixo tem como objetivo **aumentar o nível de consciência e conhecimento da sociedade em relação aos riscos e proteção no ambiente digital,** além de seu engajamento com a importância da segurança cibernética no Brasil.

Tal perspectiva contempla o **desafio de se criar uma verdadeira cultura de segurança cibernética na sociedade por meio de ações de educação e comunicação ampla e ativa**, envolvendo segmentos específicos (idosos, jovens, pais e educadores, empresários, entre outros) e ações junto a canais de mídias tradicionais e digitais.

A figura humana enquanto elo mais fraco da cadeia de segurança cibernética é uma máxima já conhecida, encontrando-se presente em grande parte da literatura sobre o tema.

Atualmente existem ações mais robustas e direcionadas a agentes de segurança pública e persecução penal por parte do poder público, mas sem muitas medidas efetivas e concretas de projetos educacionais para reforçar a conscientização da sociedade civil sobre o tema.

É possível visualizar, por exemplo, cartilhas de algumas instituições, tais como a da Autoridade Nacional de Proteção de Dados (ANPD)[58] e do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) [59] sobre os temas. Bem como iniciativas com foco mais abrangente, como o caso do programa “Hackers do Bem” citado anteriormente neste documento.

A **Estratégia Nacional de Segurança Cibernética** prevê direcionamentos e orientações para a conscientização da sociedade civil sobre os riscos e impactos dos crimes cibernéticos.

Na **Política Nacional de Cibersegurança**, consta como uma das atribuições da possível Agência Nacional de Cibersegurança, propor medidas para o desenvolvimento da educação em segurança cibernética, contribuindo assim para o desenvolvimento de uma cultura nacional sobre o tema.

Fontes:
58. Disponíveis em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes
59. Disponíveis em: https://cartilha.cert.br/

No entanto, é evidente a necessidade de o governo, em todas as suas esferas, direcionar esforços para a conscientização da sociedade civil sobre criminalidade cibernética, principalmente diante do aumento massivo do uso de tecnologias, do crescimento de ataques cibernéticos e do fenômeno político social do Analfabetismo Digital, que torna a população brasileira especialmente vulnerável.

II. Desafios prioritários

Dentre os desafios prioritários da conscientização social, se destacam quatro frentes:

a. Conscientização contra a prática de engenharia social

A engenharia social traduz-se na prática de obter "acesso a determinadas informações privilegiadas, por meio de técnica de persuasão[60]". São muitas as facetas que o engenheiro social pode utilizar-se, desde o contato telefônico com a potencial vítima ("vishing"), passando para o envio de mensagens, sejam em massa ("phishing"), sejam direcionadas (spear phishing"), seja oferecendo (ou fingindo oferecer) algo em troca para a vítima ("quid pro quo"), dentre outras inúmeras abordagens, que se renovam e aprimoram com o avanço da tecnologia.

No dia a dia, essas práticas são popularmente conhecidas pelos termos guarda-chuva de "golpe" ou mesmo "fraude". Essas condutas usualmente enquadram-se no tipo penal de "estelionato", positivada no art. 171, do Código Penal ("estelionato"):

> *Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.*
> *(...)*
> *§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo*
> *§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional*

Fontes:
60. ZANIOLO, Pedro Augusto Fernando. **Crimes Modernos**: o impacto da tecnologia no Direito. Ed. Juspodivm. p. 248.

Desta forma, embora se reconheça que, a depender das consequências práticas e circunstâncias concretas, outros tipos penais podem se fazer mais adequados para a prática da engenharia social, utilizaremos os termos "fraude", "golpe" e "estelionato" de forma intercambiável.

Conforme dados do Fórum de Segurança Pública[61], "**entre 2018 e 2022 os crimes de estelionato registrados pelas Polícias Civil cresceram 326,3%**, passando de 426.799 casos em 2018 para 1.819.409 em 2022". Em relação especificamente aos estelionatos cometidos por meio eletrônico, a citada entidade[62] informa que entre 2021, quando a conduta foi tipificada no Código Penal, e 2022 houve um aumento de 65,2%, o qual tende a ser, na realidade, ainda mais gravoso, considerando que os "dados disponíveis excluem cinco das mais populosas Unidades da Federação do país (BA, CE, RJ, RS e SP) e o Rio Grande do Norte, que não informaram a quantidade desagregada de registros".

Esses dados evidenciam o sensível e célere crescimento dos chamados "golpes virtuais". Ocorre que muitas dessas práticas envolvem ações razoavelmente conhecidas e que poderiam ser evitadas mediante pequenos cuidados dos usuários, por exemplo[63] :

- **Golpe do Whatsapp**, como ficou conhecida a prática em que o golpista assume "a identidade de outra pessoa para ludibriar seus amigos e familiares", copiando a foto de seu perfil no aplicativo de mensageria e abordando a vítima, informando que alterou o número de celular, para, então, pedir algum valor financeiro, a título de ajuda[64]; e

- **Golpes envolvendo promessas de retornos rápidos e demasiadamente altos**, habitualmente envolvendo a transferência de uma determinada quantia ao fraudador. São exemplos dessas práticas o chamado Golpe do "Robô do Pix", em que a vítima é levada a transferir ao golpista um determinado valor, sob a promessa de lhe ser devolvido um montante muito superior, não raro, o dobro do valor depositado[65].

Note-se que em ambos os casos, o crime cibernético poderia ter sido evitado com práticas razoáveis ao alcance da vítima: na primeira situação, bastaria que a vítima contactasse o familiar ou amigo que teve a sua identidade roubada, ou alguém próximo ao mesmo, para averiguar a situação. Igualmente, na segunda situação bastaria que a vítima mantivesse a própria ambição sob controle, armada com o entendimento de que rendimentos irreais ou "dinheiro falso" tipicamente são golpes.

Assim, temos uma realidade em que os crimes virtuais seriam substancialmente reduzidos se entidades públicas e privadas se empenhassem em **conscientizar a população sobre traços comuns de práticas golpistas** e de ações de engenharia social, difundido socialmente alguns cuidados básicos ao se receber mensagens ou observar ofertas – como, não responder mensagens de números ou perfis desconhecidos, sempre buscar entrar em contato com a pessoa com quem aparenta se conversar por meio de canais de comunicação confiáveis e conhecidos, ignorar ofertas de investimento com rendas muito superiores à média de mercado ou que venham por meios não confiáveis (como redes sociais).

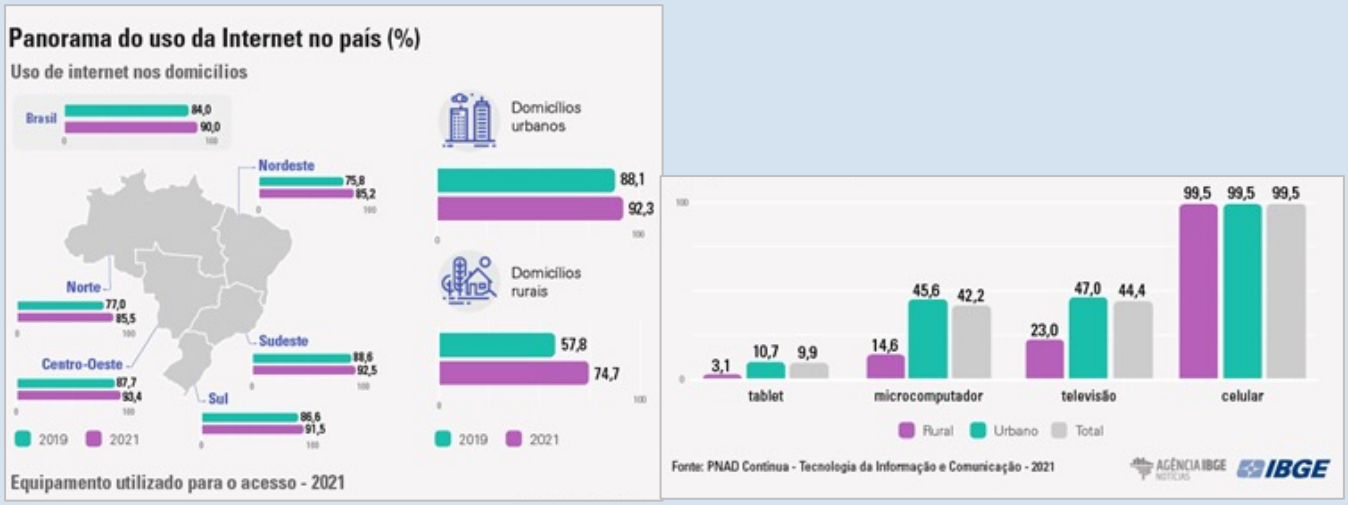
Com isso, destacamos, não se busca afirmar que toda e qualquer situação, o conhecimento dos mencionados cuidados básicos se fará suficiente para prevenir golpes (de certo, existem golpes mais sofisticados, que podem passar despercebidos ao usuário médio, como ataques com nome de domínio semelhantes).

Fontes:
61. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-05-as-novas-configuracoes-dos-crimes-patrimoniais-no-brasil.pdf. Acesso em 21.11.2023
62. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-05-as-novas-configuracoes-dos-crimes-patrimoniais-no-brasil.pdf. Acesso em 21.11.2023
63. Disponível em: https://veja.abril.com.br/coluna/maquiavel/os-golpes-mais-comuns-no-mundo-virtual-e-como-escapar-deles. Acesso em 21.11.2023
64. Disponível em: https://veja.abril.com.br/coluna/maquiavel/os-golpes-mais-comuns-no-mundo-virtual-e-como-escapar-deles. Acesso em 21.11.2023
65. Disponível em: https://olhardigital.com.br/2022/12/28/tira-duvidas/o-que-e-e-como-funciona-o-golpe-do-pix/. Acesso em 21.11.2023

b. Conscientização sobre práticas de segurança mobile

Conforme pesquisa promovida pelo IBGE[66] em 2021, o dispositivo celular lidera, com larga dianteira, os meios pelo qual o brasileiro acessa a rede mundial de computadores, com efeito, enquanto **99,5% dos domicílios brasileiros que têm acesso a internet utilizam-se de aparelhos celulares, apenas 42,2% fazem uso de computador.**

Figura 3. Panorama do uso de internet no país (%)



Grande entrave é que essa massiva adesão ao uso de smartphones não se reflete na adoção de cuidados básicos de segurança relacionados com esse dispositivo. Em estudo elaborado pelo *Real Time Big Data*[67], **71% dos brasileiros não sabem utilizar ferramentas de segurança em caso de roubo e 91% sequer sabem o que é o número IMEI, com 98% dos brasileiros não possuindo o número anotado.**

Igualmente, em pesquisa promovida em 2019 pela ESET[68], 60% dos usuários brasileiros não possuíam antivírus no celular e utilizavam redes de Wifi públicas, 47% utilizaram algum mecanismo, como JailBreak[69] e Root[70], para burlar controles de segurança dos dispositivos, instalando aplicativos não-autorizados, ainda, 60% dos usuários não se atentam às permissões requiridas por um aplicativo.

Considerado o cenário acima, uma extensa campanha de conscientização a respeito de práticas adequadas de segurança na utilização de aparelhos celulares, notadamente smartphones, é de sensível relevância para o combate do cibercrime.

Fontes:
66. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/21581-informacoes-atualizadas-sobre-tecnologias-da-informacao-e-comunicacao.html.
67. Disponível em: https://recordtv.r7.com/fala-brasil/fala-brasileiro/celular-nove-em-cada-dez-brasileiros-nao-sabem-o-que-e-imei-17082023. Acesso em 27.11.2023
68.Disponível em: https://www.tecmundo.com.br/seguranca/139281-60-pessoas-nao-usa-antivirus-celular.htm. Acesso em 27.11.2023
69.Uso de exploit de escalação de privilégios para remover restrições de software imposta pelo fabricante.
70.Adição, modificação ou deleção de arquivos do sistema.

c. Prevenção e Preparo para Resposta a Incidentes de Segurança

Após a ocorrência de um incidente de segurança, é necessário que esse incidente seja respondido de forma hábil e adequada. Para que isso seja feito, é importante a existência prévia de ações documentadas para resposta à incidentes de segurança, principalmente aqueles que envolvem dados pessoais.

Importante destacar o conceito de incidente de segurança. De acordo com o NIST[71], um incidente de segurança computacional pode ser definido como "uma ocorrência que resulta em risco real ou potencial à confidencialidade, integridade ou disponibilidade de um sistema de informação ou às informações que esse sistema processa, armazena ou transmite, ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis".

Confidencialidade, integridade e disponibilidade são conhecidas como a "Tríade" da Segurança da Informação. Abaixo, os conceitos objetivos de cada termo segundo a Washington University in St. Louis[72] :

- Confidencialidade: Refere-se à proteção de informações contra acesso de terceiros não autorizados;
- Integridade: Significa que os dados são confiáveis, completos, atualizados e não foram alterados ou modificados acidentalmente por um usuário não autorizado.
- Disponibilidade: Significa que os dados estão acessíveis quando necessário.

Assim, ocorre um incidente de segurança da informação (incluindo quando há o envolvimento de dados pessoais), quando há o comprometimento da confidencialidade, integridade e/ou disponibilidade das informações.

Fontes:
71. Disponível em: https://csrc.nist.gov/glossary/term/computer_security_incident
72. Disponível em: https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/

d. Incentivos para o Mercado de Cibersegurança Nacional

A maioria das empresas que prestam serviços de segurança cibernética no Brasil não estão sediadas no território nacional. Dentre as 15 maiores operando no país, não há nenhuma empresa brasileira. Incentivar o mercado brasileiro contribui diretamente no aumento da complexidade econômica e autonomia na capacidade local brasileira em cibersegurança.

A Segurança Cibernética é atividade basilar para a utilização de todas as funcionalidades relacionadas à internet. Países como Estados Unidos restringem a atuação de empresas estrangeiras no setor de cibersegurança, por ser considerado estratégico[73]. A proteção de informações e dados por empresas estrangeiras pode resultar em controle sobre os dados e informações estratégicas nacionais por outros países, conforme os casos Snowden e Schrems I e II[74].

No Brasil, por exemplo, a Res. CMN 4.893/21[75] traz requisitos especiais para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem no exterior, para o setor financeiro.

Nesse contexto, é imperativo o desenvolvimento de empresas e tecnologias brasileiras de segurança cibernética para a proteção das informações confidenciais armazenadas no Brasil. A própria PNCiber prevê como um de seus primeiros objetivos, a promoção do desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética.

Fontes:
73. Section 1.50002 of the Commission's rules directs the Public Safety and Homeland Security Bureau to publish a list of communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, based exclusively on any of four sources for such a determination and that such equipment or services possess certain capabilities as enumerated in section 2(a) of the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609). Pursuant to the Commission's rules, the Public Safety and Homeland Security Bureau will maintain this list on the Commission's website, and will monitor the status of any determinations in order to update the Covered List. More information on how the Covered List is compiled and updated can be found in the Commission's rules at 47 C.F.R. § 1.50000 et seq.
Disponível em: https://www.fcc.gov/supplychain/coveredlist
74. Snowden e Schrems I e II. Em 2013, Edward Snowden divulgou que o governo dos EUA usou empresas de "big tech" e programas como " PRISM " ou " Upstream " sob FISA 702 e EO 12.333 para "espionar" sem fundamental legal. NA UE, desde 1995, dados pessoais geralmente não podem ser enviados para fora da UE, a menos que haja uma proteção "essencialmente equivalente" no país de destino. A indústria dos EUA dependeu fortemente de uma decisão da Comissão Europeia chamada "Safe Harbor" que declarou os EUA "essencialmente equivalentes" em 2000.C-362/14 ("Schrems I") em 2015, dadas as leis de vigilância invasivas dos EUA. Em 2016, a Comissão Europeia aprovou em grande parte a mesma decisão sobre transferências de dados UE-EUA novamente, sob o novo nome "Privacy Shield", que foi invalidado pelo TJEU no C-311/18 ("Schrems II") em 2020 em grande parte em os mesmos fundamentos. Disponível em: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.
75. Disponível em:
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893&ref=blog.ecotrust.io

Como exemplos de ações de incentivo ao mercado nacional de cibersegurança, é possível mencionar:

a) **Investimento em pesquisa e desenvolvimento**, alocando recursos para o fomento da inovação e criação de soluções brasileiras para o mercado de segurança cibernética;

b) **Parcerias com universidades e centros de pesquisa**, promovendo a formação de profissionais especializados e o desenvolvimento de soluções avançadas de segurança cibernética;

c) **Incentivos para contratação de empresas de segurança** da informação brasileiras para entidades públicas nos processos de licitação;

d) **Apoio ao empreendedorismo na área de segurança da informação**, dando suporte a pequenas empresas e startups com palestras, recursos e espaços;

e) **Incentivo para participação de empresas nacionais de segurança cibernética em grandes eventos,** ampliando a visibilidade e o alcance dos serviços; dentre outras possibilidades.

III. Referências nacionais e internacionais

Em relação a Prevenção e Preparo para Resposta à Incidentes de Segurança, Regulações como a LGPD[76] e o GDPR[77] (General Data Protection Regulation) trazem direcionamentos para comunicar a respectiva Autoridade e/ou os titulares de dados pessoais na ocorrência de um incidente de segurança, cada uma dentro de seu respectivo escopo.

Já a ENISA[78] (European Network and Information Security Agency), traz orientações para a **prevenção e preparo para resposta a incidentes de segurança,** se baseando em direcionamentos do CERT (Computer Emergency Response Team), o manejo de incidentes de segurança (conhecido também como "Incident Handling") é composto de 4 etapas, conforme descrição e imagem abaixo:

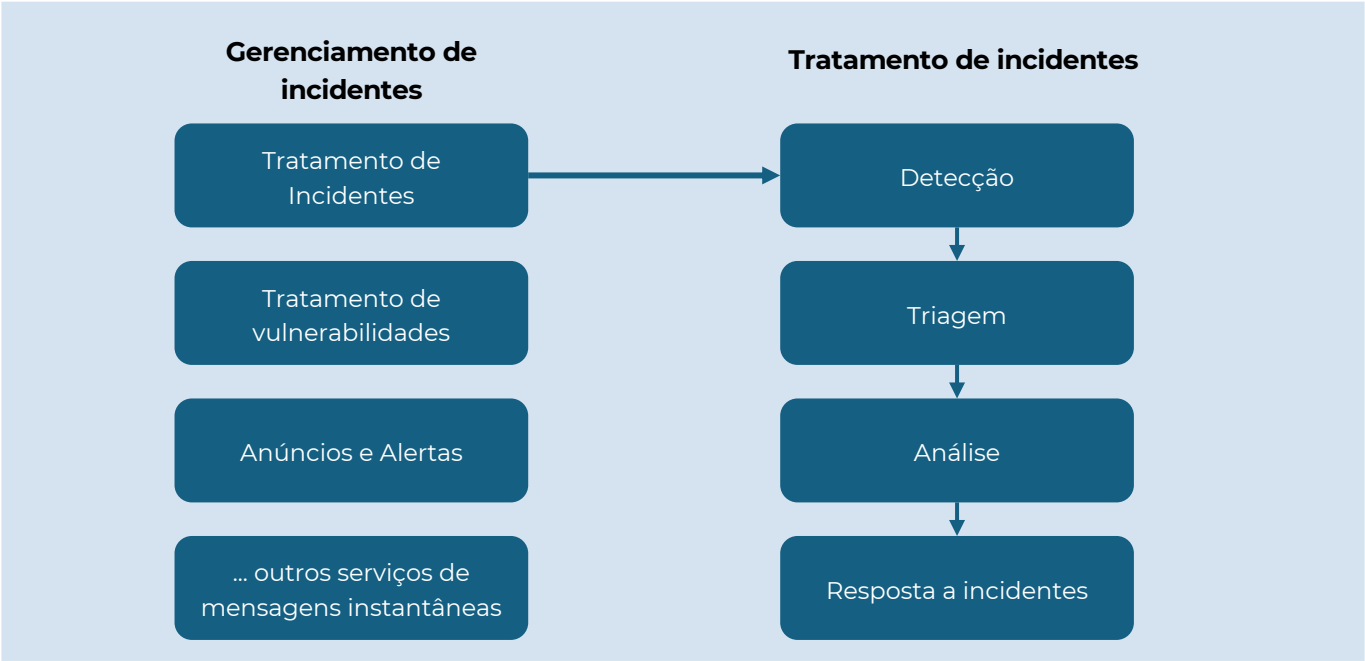
a. **Detecção:** Momento específico em que o incidente é identificado;

b. **Triagem:** Momento em que o incidente é avaliado, categorizado e priorizado para tomada das ações cabíveis;

c. **Análise:** Identificar como o incidente ocorreu, quem foi afetado, a causa raiz, dentre outras informações pertinentes para a compreensão do incidente;

d. **Resposta ao incidente:** a partir das informações coletadas nas etapas anteriores, o incidente deverá ser respondido para a sua correta contenção e remediação.

Figura 4. Gerenciamento de incidentes e tratamento de incidentes esclarecidos



Fontes:
76. Obrigação se encontra no artigo 48, incluindo os requisitos que devem conter na notificação, o que também inclui informações técnicas sobre o incidente. A notificação é necessária quando o incidente puder acarretar "risco ou dano relevante" aos titulares de dados pessoais". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
77. Previstos nos artigos 33 e 34. Diferentemente da LGPD, o GDPR prevê que a respectiva Autoridade deve ser notificada quando o incidente envolver "risco", e os titulares devem ser comunicados quando envolver um "alto risco". Disponível em: https://gdpr-info.eu
78. ENISA. Good Practice Guide for Incident Management.

Como referências de padrões e boas práticas internacionais para auxiliar organizações dos mais diversos segmentos, é possível citar o "Computer Security Incident Handling Guide"[79], elaborado pelo NIST, e a "ISO/IEC 27035-2:2023" elaborada pela ISO, que prevê diretrizes para planejar e preparar respostas a incidentes.

Em relação a segurança mobile, no setor de telecomunicações, a ANATEL[80] é a entidade responsável por garantir o desenvolvimento do setor e monitorar o seu exercício pelas empresas que prestam o serviço. Suas atribuições são definidas na Lei 9.472/1997[81] (Lei Geral de Telecomunicações).

Considerando a existência de diretrizes já mencionadas no decorrer deste documento como Política Nacional de Segurança da Informação e a Estratégia Nacional de Segurança Cibernética, bem como as funções institucionais da ANATEL, a Agência editou o **Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações** aprovado por meio da Resolução nº 740/2020[82].

O objetivo desse Regulamento pode ser identificado no artigo 1º, que dispõe: "Este Regulamento tem por objetivo estabelecer condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo a **Segurança Cibernética** e a proteção das **Infraestruturas Críticas de Telecomunicações**". Essa norma é aplicável a todas as prestadoras de serviço de telecomunicações.

Após a aprovação do mencionado Regulamento, a Agência também aprovou, por meio do Ato nº 77[83] da Superintendência de Outorga e Recursos à Prestação (SOR), os **Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações**[84], cujo principal objetivo é definir requisitos de segurança cibernética para os equipamentos utilizados no setor de telecomunicações de modo a mitigar riscos e vulnerabilidades inerentes ao uso de tecnologias, propondo diversas medidas para atualização de softwares/firmwares e recomendações de configuração específicas para equipamentos.

Mais recentemente, em outubro de 2023, foram aprovados por meio do Despacho Decisório Nº 18/2023/COQL/SCO[85], o **Guia Orientativo de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações**[86] e o **Guia Orientativo DevSecOps**[87]. O primeiro tem o objetivo de orientar as prestadoras de serviço de telecomunicações a proteger suas informações, redes e dados, enquanto o segundo, propor boas práticas para desenvolvimento e operação de softwares utilizados no setor de telecomunicação.

Fontes:
79. Disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
80. Disponível em: https://www.gov.br/anatel/pt-br/acesso-a-informacao/institucional#:~:text=É%20administrativamente%20independente%20e%20financeiramente,%2C%20legalidade%2C%20impessoalidade%20e%20publicidade.
81. Disponível em: https://informacoes.anatel.gov.br/legislacao/leis/2-lei-9472
82. Disponível em: https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1497
83. Disponível em: https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302
84. Disponível em: https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505
85. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89flQ7RjX8EYU46IzCFD26Q9Xx5QNDbqaDQxaILcmj8Kq8tPNX0VAcGL0ND9-vgbfuXNhoKvCYOVbUIsA7xqRAUZkQcjPHKHieSAeg87-6Zt2V-ITnnpW2
86. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89flQ7RjX8EYU46IzCFD26Q9Xx5QNDbqZ2HzV7pQor_uuxREh18J3Uudb6CTERhXP0S4cd3uwKgaVaCTjFK3en6G5rF19eRcBOqoN2PCw94zGOYWsdmvHZ.
87. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89flQ7RjX8EYU46IzCFD26Q9Xx5QNDbqYAHRbPZD4lyjHVrVE1lGFpJ0XBdoGuy3lvgTwNBzOeSHWwkbm0RTQYCZ3cNJiD3fF951IYCChNOxMQu5Ei2Gj2

Diante dessa promoção da cultura e do fomento da importância das medidas de cibersegurança, algumas operadoras oferecem produtos específicos focados em segurança cibernética para os seus clientes, como o caso da **VIVO[88], CLARO[89] e da TIM[90], contribuindo para a difusão de controles de segurança cibernética** em um ambiente digital cada vez mais vulnerável diante do avanço tecnológico e da ausência de conhecimento em segurança da informação por parte da população.

Em dezembro de 2023, **o Governo Federal lançou o aplicativo "Celular Seguro"[91]**. A medida proposta pelo Ministério da Justiça e Segurança Pública (MJSP) com apoio da ANATEL e visa aumentar o combate contra roubos e furtos de celulares no Brasil. Com esse aplicativo, a vítima poderá bloquear o aparelho, a linha telefônica e os aplicativos bancários, minimizando a probabilidade de os danos se materializarem.

No âmbito da pesquisa e desenvolvimento em cibersegurança, um exemplo é o projeto do Centro de Estudos e Sistemas Avançados do Recife (Cesar), que venceu a concorrência entre outros seis institutos de pesquisa e investimentos (ICTs) para ser credenciado como **Centro de Competência em Segurança Cibernética pela Embrapii (Empresa Brasileira de Pesquisa e Inovação Industrial)**. O instituto receberá um aporte de R$ 60 milhões, tendo o projeto um período de execução de 42 meses.

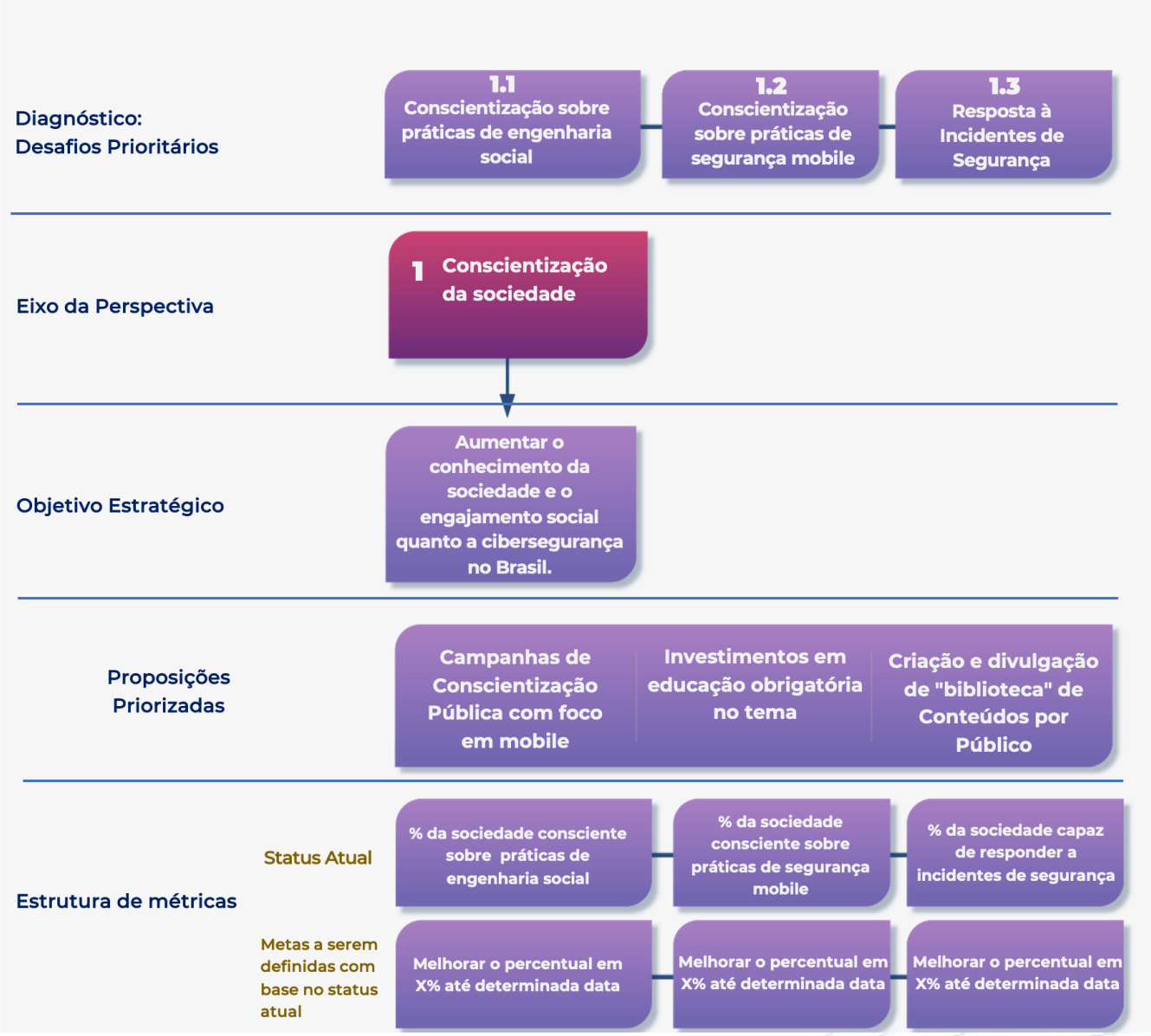
O projeto do Cesar irá atuar em quatro linhas temáticas de pesquisa: (1) gestão de identidade e acesso, (2) proteção e privacidade de dados, (3) inteligência para ameaças cibernéticas, (4) aspectos legais, éticos e comportamentais.

Fontes:
88. Disponível em: https://protecao.vivo.com.br/vivo-seguranca-online
89. Serviços disponíveis em: https://www.claro.com.br/internet/banda-larga/servicos-adicionais/antivirus.
90. Serviços disponíveis em: https://www.timsegurancadigital.com.br/
91. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/dezembro/celular-seguro-ja-esta-disponivel-no-gov.br

IV. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 5. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 1



a. Recomendações para Construção das Metas:

Incluir questionário relativo aos indicadores de população em pesquisas amostrais nacionais de frequência trimestral, semestral ou anual, de forma a estabelecer série histórica. Buscar fontes já existentes, como a PNAD Contínua, as pesquisas do Cetic.br e a PINTEC (IBGE).

2 Adequação do capital humano

O segundo eixo é a adequação do capital humano, que possui como objetivo a necessidade de fomentar e estimular a formação adequada de capital humano na área de segurança cibernética.

I. Contexto do Eixo

O eixo se relaciona com a urgente necessidade de aumento na formação de mão de obra qualificada em cibersegurança como base para a construção de maior resiliência nacional nesta temática. Incluindo criação de cursos superiores, certificados de proficiência profissional, além do melhor aproveitamento das estruturas de formação do Estado.

A ausência de profissionais qualificados em segurança cibernética é uma problemática global, sensível mesmo em países desenvolvidos e que, historicamente, figuram como atrativos para a mão-de-obra estrangeira especializada.

Essa problemática, no entanto, é particularmente sensível em países do sul global, com a Ásia e o Pacífico possuindo um déficit de profissionais quase três vezes maior que a Europa e a América do Norte combinados[92].

Em relação ao gap global de profissionais de segurança cibernética, pesquisa feita pela ISACA, publicada em sede do "State of Cybersecurity 2022"[93], dispõe que:

Cerca de **62% dos respondentes informaram que os seus times de segurança cibernética se encontram sem o volume adequado de profissionais**;

Cerca de **63% dos respondentes informaram que suas organizações se encontram com vagas abertas em segurança cibernética**;

Cerca de **59% dos profissionais da área de cibersegurança pedem demissão em razão do recrutamento por outras empresas**, demonstrando a concorrência entre empresas por profissionais do setor.

Fontes:
92. Disponível em: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e. Acesso em 11.12.2023
93. Disponível em: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf?mod=djemCybersecruityPro&tpl=cy. Acesso em 21.11.2022

Particularmente em relação ao Brasil, em 2021, segundo pesquisa elaborada pela (ISC)[94], o país figurava com um **déficit de 441 mil profissionais de cibersegurança**, ocupando a primeira posição de países deficitários. Embora, em 2023, este número tenha se reduzido significativamente, o país ainda lidera o número de vagas em aberto na América Latina, com quase 232 mil vagas.

A situação, no entanto, tende a ser mais gravosa do que os números atuais revelam, considerando que o Brasil, igualmente, **lidera as demissões mundiais na área de Segurança Cibernética**, com 38% dos respondentes da pesquisa da (ISC)[95] informando que as suas empresas realizaram demissões em segurança cibernética.

Deste modo, é possível que parte significativa da redução de vagas em aberto possa ter transcorrido não em razão do aumento de profissionais qualificados, mas pela significativa redução de vagas, em um ano marcado por um **aumento de 52% no número de pedidos de recuperação judicial[96].** Pelo que, em caso de retorno da aceleração da economia, podemos nos deparar com um crescimento acelerado do déficit de profissionais, que já é considerável.

Particularmente, as empresas brasileiras reportaram algumas dificuldades na contratação de profissionais de cibersegurança, em pesquisa realizada pela ManpowerGroup, que parecem refletir a problemática global[97] :

Gráfico 1. Motivos pelos quais as empresas brasileiras não conseguem contratar profissionais de cibersegurança [109]

Abordando especialmente aspectos formativos na área, notadamente os cursos superiores direcionados a profissionais da área (Segurança da Informação, Cibersegurança, Gestão da Segurança e Defesa Cibernética), vemos, conforme os micro dados do Censo da Educação Superior 2022[98], que:

- O total de vagas ofertadas no país encontra-se muito aquém das vagas abertas no setor anualmente. Com o número total de vagas sendo de 101.848 (cento e um mil oitocentos e quarenta e oito)
- Não obstante, a quantidade de inscritos se mostra extremamente pequena, com cerca de 17.347 (dezessete mil trezentos e quarenta e sete inscritos).

Fontes:
94. Disponível em: https://valorinveste.globo.com/objetivo/empreenda-se/noticia/2021/11/06/brasil-tem-maior-dficit-de-profissionais-de-cibersegurana.ghtml. Acesso em 11.12.2023
95. Disponível em: https://www.isc2.org/Insights/2023/12/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-State-of-the-Workforce
96. https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/pedidos-de-recuperacao-judicial-cresceram-quase-70-em-2023-revela-serasa-experian/#:~:text=Em%20dezembro%20de%202023%2C%20foram,queda%20de%2041%2C7%25.&text=Mais%20informa%C3%A7%C3%B5es%20dispon%C3%ADveis%20no%20site%20oficial%20da%20Serasa%20Experian.
97. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em 24.11.2023
98. Disponível em: https://www.gov.br/inep/pt-br/areas-de-atuacao/pesquisas-estatisticas-e-indicadores/censo-da-educacao-superior/resultados. Acesso em 12.12.2023.

Assim, temos um ambiente formativo em que o número de inscritos encontra-se significativamente aquém ao número de vagas que, por sua vez, já se encontra aquém da demanda de mercado. Revelando a necessidade de políticas públicas que não apenas forneçam opções formativas, mas que, também, **incentivem a perseguição de carreira e conhecimento na área pelas pessoas,** demonstrando e divulgando como elas e a própria sociedade podem dela beneficiar-se.

Dentre os cursos oferecidos hoje voltados para cibersegurança, a maioria se concentra em cursos livres ou especializações, como o curso de Gestão de Riscos Cibernéticos oferecido pela FGV[99] ou até os mais de 10 cursos oferecidos pelo Instituo Brasileiro de Cibersegurança (IBSEC)[100], que já certificou mais de 35.000 profissionais. Além disso o SENAC disponibiliza cursos de graduação e especialização na área de segurança e defesa cibernética.

Outro instituto voltado para certificações na área de cibersegurança é o Instituto Daryus de Ensino Superior Paulista (IDESP)[101], em 2021 o instituto registrou um aumento de 85% em novas matrículas para os cursos de Desenvolvimento Seguro, Continuidade de Negócios, Gestão de Riscos, Gestão de Segurança da Informação, Cibersegurança e Inteligência Cibernética.

II. Desafios Prioritários

Dentre os desafios prioritários, se destacam:

a. Ausência de profissionais de segurança cibernética

A pandemia do Covid-19 foi uma grande impulsionadora da adoção de recursos tecnológicos para a continuação das atividades de diversas organizações[102]. Na mesma linha, a importância do profissional de segurança cibernética se fez cada vez mais necessária por conta do aumento crescente de ameaças digitais e outras vulnerabilidades relacionadas ao uso de dispositivos eletrônicos.

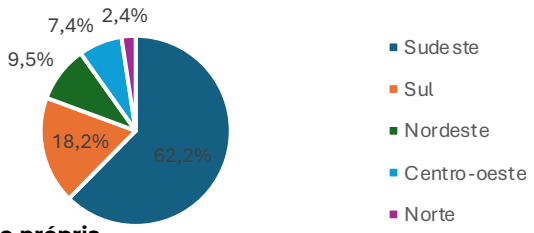
Mesmo com o mercado aquecido e com ofertas de salários acima da média brasileira, a quantidade de profissionais disponíveis não é suficiente para suprir a demanda.

Em pesquisa realizada pelo SENAC[103], 57,3% das empresas entrevistadas relataram ter enfrentado dificuldade para contratar profissionais da área de tecnologia. Das dificuldades citadas, 35,8% estão relacionadas à dificuldade de **encontrar profissionais capacitados para executar as atividades, enquanto 30,6% mencionaram que o problema era o mercado estar aquecido, faltando profissionais disponíveis para contratação.**

Fontes:
99. Disponível em: https://certs.ibsec.com.br/?_gl=1*128e4xn*_ga*MTE4NjQwNDc5Ny4xNzE1MDA2MTA1*_ga_GPETBBW5MR*MTcxNTAwNjEwNC4xLjEuMTcxNTAwNjMwMS4wLjAuNjA2MjQyNjI5*_fplc*c2xma01EMDhoRVJKNWdCcmNGZUN3MDYlMkJuVHJjcGIlMkJucyUyQk42Y21VNEtEWmVlVnM0cEJIQjM2U09LV29kUlBzOWtlRjFMRm1LRGJLYmV2bEVNMkxTNUxuOFNOTmZCTEZleG8lMkIzaEIlMkZ3QUpzQkFqeXJsZ2YwR3VDeVc0WXZkQSUzRCUzRA.
100. Disponível em: https://www.cisoadvisor.com.br/sobe-40-busca-pelos-cursos-de-cibersegurança/
101. Mais informações em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais
102.Informações em: https://g1.globo.com/tecnologia/noticia/2023/08/17/seguranca-da-informacao-tem-salario-de-r-38-mil-mas-nao-encontra-profissionais-veja-como-entrar.ghtml#setor
103. SENAC. Pesquisa de Demanda por Educação Profissional - Setor de TI. Disponível em: <https://www.dn.senac.br/wp-content/uploads/2017/03/pesq_dem_atual.pdf>

Outra importante estatística é sobre a distribuição geográfica da população de empresas respondentes: 2,4% no Norte, 9,5% no Nordeste, 62,2% no Sudeste, 18,2% no Sul e 7,4%. Tais números evidenciam um quantitativo maior de empresas respondentes na região sudeste, sendo os números das outras regiões consideravelmente inferiores.

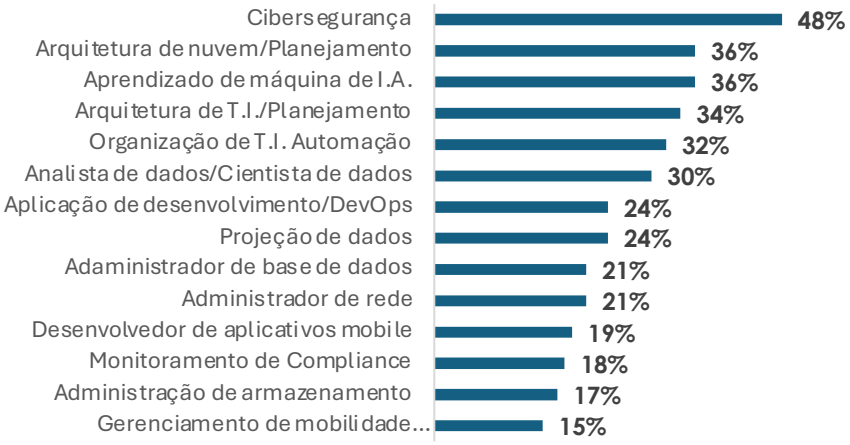
Gráfico 2. Distribuição geográficas das empresas respondentes da pesquisa do SENAC



Elaboração própria

Segundo o relatório "Panorama de talentos em tecnologia"[104], realizado pelo Google for Startups, das áreas relacionadas a Tecnologia da Informação, a área de segurança cibernética é a que apresenta uma maior lacuna de profissionais: a área de cibersegurança é a área que apresenta o maior gap de talentos globais (48%), seguindo pela área de aprendizado de máquinas e IA (36%).

Gráfico 3. Áreas que apresentam os maiores gaps de talentos globais



Essa problemática, no entanto, é particularmente sensível em países do sul global, com a Ásia e o Pacífico possuindo um déficit de profissionais quase três vezes maior que a Europa e a América do Norte combinados. No cenário Brasil, existe uma ausência sistêmica de profissionais de tecnologia da informação ocasionado pela ausência de capacidade do país em formar profissionais capacitados conforme o crescimento da demanda do mercado.

Conforme relatado pelo Google, entre 2021 e 2025, 53 mil profissionais se graduarão anualmente, enquanto a demanda estimada é de aproximadamente 800 mil novos talentos. O resultado é um déficit potencial de 530 mil profissionais nesse período de quatro anos.

Em linha com indicadores da pesquisa do SENAC, o Google menciona que um dos maiores desafios é a homogeneidade do mercado de talentos no Brasil, que é pouco diverso e concentrado na região sudeste, sendo 43% apenas em São Paulo. Além da questão regional mencionada, há ainda barreiras maiores para mulheres e pessoas negras, que por conta das dificuldades de permanência, acabam deixando o mercado de tecnologia de lado.

Fontes:
104. Panorama de Talentos em Tecnologia. Disponível em: https://campus.co/sao-paulo/gap-de-talentos/

A fuga de talentos é um outro ponto trazido no relatório. Os profissionais mais gabaritados em segurança da informação buscam melhores oportunidades e recebem diversas propostas, boa parte delas de organizações de fora do Brasil. Assim, a falta de estrutura apresentada no Brasil, bem como a ausência de referências, aumentam **o sentimento de descrença no mercado brasileiro** entre os profissionais mais experientes e os recém-formados. Dos entrevistados para o relatório, 73% concordam que as condições são mais atrativas no exterior, e 63% informaram que a remuneração local não é competitiva em relação ao ofertado fora do Brasil.

Atualmente no Brasil, existem cursos ofertados na área de cibersegurança por diferentes instituições. O próprio SENAC, cumprindo com sua missão institucional[105], oferece uma série de cursos relacionados à segurança cibernética. Tais cursos **podem ser promovidos e incentivados pelo poder público para a sua expansão**, visando ampliar a formação de novos profissionais para auxiliar na redução do déficit existente, bem como contribuir para a manutenção dos profissionais no Brasil a partir de oferecimento de melhores condições, aperfeiçoamento da estrutura de segurança cibernética e valorização da remuneração desses profissionais.

Fontes:
105. Considerando o Senac São Paulo: "A missão do Senac São Paulo é proporcionar o desenvolvimento de pessoas, por meio de ações educacionais que estimulem o exercício da cidadania e a atuação profissional transformadora e empreendedora, de forma a contribuir para o bem-estar da sociedade". Disponível em: https://www.sp.senac.br/pdf/58192.pdf
106 Disponível em: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf?mod=djemCybersecruityPro&tpl=cy. Acesso em 21.11.2022

b. Necessidade de empresas formadoras

Além da ausência de profissionais qualificados em segurança cibernética, outro desafios é a necessidade de empresas formadoras. Grande parte das organizações, naturalmente, não disporão dos recursos necessários para competir pelos profissionais disponíveis com multinacionais. Daí a necessidade de disponibilizar vagas para profissionais iniciantes ("juniores") que são, de fato, vagas de entrada no mercado – ou seja, destinadas para que pessoas com interesse pela área possam aprender suas funções, ainda que não possuam experiência ou conhecimento prévio, inclusive pessoas fora da área da tecnologia.

Com isso, as empresas precisam se tornar verdadeiros centros de formação em que profissionais interessados por segurança da informação possam aprender a desenvolver as suas competências.

É necessário que as empresas incentivem seus colaboradores a desenvolverem interesse pela área, divulgando eventuais benefícios que podem ser alcançados.

É consenso a relevância da criação de programas voltados a recolocação de profissionais de maior senioridade na área de Segurança Cibernética, sobretudo considerando que o Brasil passa por um processo de envelhecimento populacional, com redução de cerca de 5%, entre 2012 e 2021, da população abaixo de 30 anos[111]. Desta forma, é importante pensar em programas de formação de profissionais que incluam, também, profissionais mais seniores, que tendem a se tornar maioria com o passar do tempo.

c. Necessidade de programas governamentais de formação de profissionais

Mesmo com a adoção de programas formativos e de abertura de vagas, o desbalanceamento entre a oferta e demanda por profissionais do setor não seria solucionado. São necessárias, portanto, discussões sobre a necessidade de adoção de **políticas públicas para a formação e educação em segurança cibernética**, mesmo entre os demais cursos na área de TI, o que, além de auxiliar na redução do gap de profissionais disponíveis, tende a aumentar a conscientização da população em geral sobre a temática.

Na apresentação do projeto da Política Nacional de Cibersegurança[112], foi dedicado um capítulo específico (Capítulo VI) para tratar sobre medidas de **fomento e incentivo para obtenção de conhecimento sobre cibersegurança**, e impulsionar estudos, pesquisas e inovação sobre o tema, incluindo a difusão desse tipo de conhecimento na grade curricular do ensino fundamental e médio, das escolas públicas e privadas. Além disso, iniciativas relacionadas à criação de programas educacionais para a disseminação da cultura de cibersegurança e projetos para a ativação de ecossistemas sobre segurança cibernética devem ser consideradas de interesse nacional e prioritárias para a alocação de recursos públicos.

Fontes:
111.Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf
112. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34438-populacao-cresce-mas-numero-de-pessoas-com-menos-de-30-anos-cai-5-4-de-2012-a-2021. Acesso em 11.12.2023

III. Referências nacionais e internacionais

É de extrema relevância a criação de programas voltados à recolocação de profissionais de maior senioridade na área de Segurança Cibernética, sobretudo, considerando que o Brasil passa por um processo de envelhecimento populacional, com redução de cerca de 5%, da população abaixo de 30 anos, entre 2012 e 2021[113]. Desta forma, é importante pensar em programas de formação de profissionais que incluam, também, profissionais mais seniores, que tendem a se tornar maioria com o passar do tempo.

Como exemplo, é possível citar o programa "Hackers do Bem", do Governo Federal, que será coordenado pela Softex e executado pela Rede Nacional de Ensino e Pesquisa (RNP) em conjunto com o Senai-SP. A meta é preparar mais de 30 mil profissionais até 2025 em diferentes níveis: básico, avançado, especializado e residência tecnológica em laboratórios de cibersegurança ao redor do Brasil [118].

Um outro exemplo de política pública que pode ser estudada para a construção de uma iniciativa nacional é a estadunidense "National Cyber Workforce and Education Strategy" [114], instituída pela administração Biden.

O primeiro ponto de destaque da estratégia estadunidense é a atribuição da "National Cyber Workforce Coordination Group" ("NCWCG") enquanto órgão responsável pela implementação e coordenação da estratégia, coordenando as atividades entre entes públicos e privados. O "National Cyber Workforce Coordination Group" ("NCWCG") é dividido em quatro pilares.

O primeiro pilar da estratégia é garantir que todos os estadunidenses tenham competências cibernéticas fundacionais, as quais dividem-se em três macrocategorias: literacia digital [115], literacia computacional [116], e a resiliência digital [117]. Dentro da macrocategoria de "literacia computacional", encontra-se a habilidade de utilizar a informação de forma ética e segura, que nos interessa para fins deste relatório. Para tanto, busca-se garantir que:

- Todos as pessoas interessadas em aprender competências cibernéticas possam acessar esse conhecimento com pouco ou nenhum custo. Para tanto, buscar-se-á (i) aumentar as oportunidades de aprendizado através de investimentos federais; (ii) produção e disponibilização pública de conteúdo por especialistas da área; (iii) encorajamento de uma rede de conhecimento aberto em competências cibernéticas fundacionais;

Fontes:
113. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/05/programa-hackers-do-bem-vai-fortalecer-a-ciberseguranca-no-pais.
114. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf. Acesso em 21.11.2023
115. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34438-populacao-cresce-mas-numero-de-pessoas-com-menos-de-30-anos-cai-5-4-de-2012-a-2021. Acesso em 11.12.2023
116. Descrita como: "As habilidades cognitivas e técnicas necessárias para usar informações e tecnologias para encontrar, avaliar, criar e comunicar informações".
117. Descrita como: "capacidade de consumir informações e usar aplicativos e sistemas para: analisar dados, tirar conclusões e resolver problemas; com segurança, ética e segurança interagir em ambientes de rede; e entender como a computação, os dados e a conectividade afeta a sociedade".
118.Descrita como: "a consciência, as habilidades, a agilidade e a confiança para serem usuários capacitados de novas tecnologias e adaptar-se às novas exigências em matéria de competências digitais".

- As pessoas são conscientizadas sobre como o aprendizado de competências cibernéticas fundacionais podem beneficiá-las e à sociedade como um todo. Para tanto, buscar-se-á: (i) promover os benefícios econômicos e sociais de competências cibernéticas; (ii) encorajar entidades privadas a incluir a promoção de competências cibernéticas fundacionais nos portfólios de responsabilidade corporativa social; (iii) encorajar integrantes do ecossistema a expandir e promover campanhas que encorajam o desenvolvimento de competências cibernéticas fundacionais, como mês da consciência em cibersegurança; (iv) criar um prêmio presidencial para competências cibernéticas fundacionais;

- Impulsionar progresso global em competências cibernéticas fundacionais. Para tanto buscar-se-á: (i) trocar boas práticas no aprimoramento de competências cibernéticas fundacionais com parceiros estratégicos; (ii) incluir o desenvolvimento de competências cibernéticas fundacionais nos programas internacionais de desenvolvimento de capacidades; promover o desenvolvimento de padrões e frameworks internacionais em competências cibernéticas fundacionais.

O segundo pilar da estratégia é transformar a educação cibernética. O objetivo desse pilar é, a um só tempo, atender as demandas atuais por profissionais de cibersegurança e preparar a força de trabalho para a dinamicidade do ambiente tecnológico. Para tanto busca-se:

- Construir e se aproveitar de ecossistemas que aprimorem a educação cibernética. Para tanto, buscar-se-á: (i) expandir e apoiar financeiramente ecossistemas de educação cibernética, identificando e destacando ecossistemas bem-sucedidos; (ii) encorajar a participação de empresas, associações laborais e empresariais e câmeras de comércio nos ecossistemas de educação cibernética; (iii) integrar cibersegurança, sobretudo práticas de segurança no design, em programas financiados pelo governo federal; (iv) proteger estudantes do ecossistema com protocolos adequados de segurança e privacidade;

- Expandir educação cibernética baseada em competências. Para tanto buscar-se-á: (i) concentrar os investimentos federais em educação cibernética no desenvolvimento de recursos de aprendizagem alinhados com estágios de desenvolvimento cognitivo; (ii) aumentar e aprimorar o conteúdo cibernético aplicado a programas educacionais multidisciplinares; (iii) aumentar a disponibilidade de componentes curriculares de educação cibernética, com diversas agências governamentais devendo colaborar no desenvolvimento de recursos educacionais e na redução de custos; (iv) encorajar que estudantes do ensino médio obtenham créditos universitários por meio da realização de cursos de segurança cibernética; (v) permitir que os estudantes ganhem créditos acadêmicos por experiências em questões cibernéticas fora da escola;

- Investir em educadores e aprimorar os sistemas de educação cibernética, buscando garantir que estes sejam resilientes, responsivos e suficientemente sustentáveis para acomodar as rápidas mudanças tecnológicas. Para tanto buscar-se-á (i) aprimorar o ensino escolar ("K-12") e pós-secundário, incentivado universidades e faculdades a formar profissionais capacitados a ensinar competências cibernéticas naqueles ambientes; (ii) estabelecer programas de bolsas de estudo para educadores cibernéticos; (iii) adotar ações para aumentar o número de integrantes em programas avançados de graduação, para fortalecer a pesquisa cibernética por exemplo, explorar mecanismos, incluindo programas de subsídios e bolsas de estudo, para aumentar o número de alunos cibernéticos em programas de graduação avançados que impulsionarão a inovação cibernética e apoiar a implementação de princípios de segurança desde o design; (iv) aumentar a participação em programas de graduação avançada para expandir a linha de produção do corpo docente cibernético; (v) encorajar abordagens interdisciplinares para o ensinamento de competências cibernéticas; (vi) incorporar educação cibernéticas em iniciativas de plano de carreira, inclusive, buscando estabelecer conceitos comuns entre partes interessadas; (vii) expandir as oportunidades de obtenção de créditos em aprendizado cibernético experimental; (ix) Estabelecer e suportar programas de premiações nacionais de cibernética para escolas e professores.

- Fazer com que a educação cibernética seja menos dispendiosa e mais inclusiva. Para tanto, buscar-se-á: (i) aumentar a produção de força de trabalho na área em populações pouco representadas, por intermédio de um programa coordenado pela Federação; (ii) aumentar o acesso para oportunidades de aprendizado e conteúdos que sejam culturalmente adaptados; (iii) aumentar a participação de estudantes e professores em cibernética em bolsas escolares; (iv) incorporar instrução cibernética em programas que atendem a comunidades locais.

O terceiro pilar da estratégia é expandir e aprimorar a força de trabalho cibernética estadunidense, buscando-se atuar de forma conjunta com as partes interessadas do ecossistema. Para tanto, busca-se:

- Aumentar a força de trabalha fortalecendo o ecossistema, buscando garantir uma melhor colaboração, melhor acesso a dados e acesso, com baixo ou nenhum custo, a ferramentas para a formação de profissionais. Para tanto, buscar-se-á: (i) encorajar o envolvimento mais robusto das partes interessadas no ecossistema, permitindo que estas atuem enquanto lideranças ativas; (ii) aprimorar a interoperabilidade de dados sobre a força de trabalho cibernética; (iii) expandir a disponibilidade de ferramentas para a formação de profissionais de baixo custo;

- Promover a contratação baseada em competências e o desenvolvimento da força de trabalho, após contratação, pelos empregadores, para tanto buscar-se-á: (i) fazer uso de colégios comunitários para aprimorar a diversidade da força de trabalho cibernética e sua capacidade de atender às necessidades locais; (ii) construir e aprimorar parcerias industriais em ecossistemas de educação cibernética e desenvolvimento de força de trabalho para aumentar a diversidade e melhorar os programas; (iii) encorajar o uso de práticas de contratação baseadas em competências por empregadores; (iv) Expandir o uso de práticas de desenvolvimento da força de trabalho baseadas em competências; (v) aumentar as oportunidades de acesso às carreiras cibernéticas através de oportunidades de aprendizagem no trabalho; (vi) Incentivar a adoção de modelos de emprego flexíveis, como o emprego fracionário, permitindo que profissionais de cibernética possam ser contratados por múltiplos empregadores; (vii) envolver-se com setores de recursos humanos para identificar informações sobre necessidades em competências cibernéticas e incentivar empregados a apoiarem que os gerentes busquem profissionais com competências cibernéticas.

- Fortalecer a força de trabalho cibernética com uso da diversidade estadunidense. Para tanto buscar-se-á: (i) explorar incentivos em concessões e contratos cibernéticos federais voltados para comunidades pouco representadas e carentes; (ii) expandir a disponibilidade de credenciais baseadas em competências de baixo ou nenhum custo; (iii) aumentar a colaboração com organizações que servem ou operam em comunidades pouco representadas; (iv) facilitar a integração de veteranos na força de trabalho cibernética; (v) desenvolver políticas migratórias que atraiam e retenham imigrantes que trabalhem no setor cibernético.

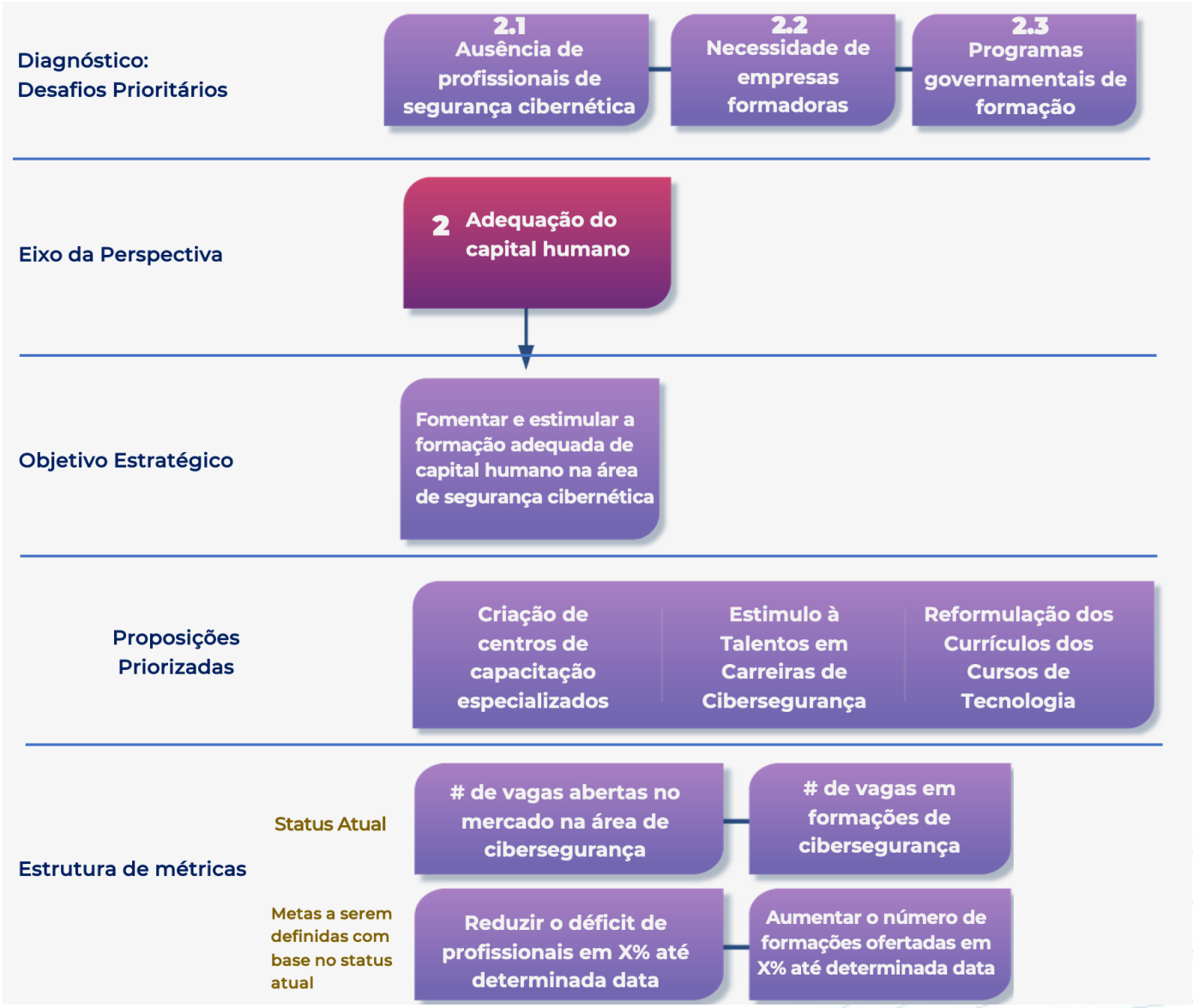
- Aprimorar interações internacionais, por meio de (i) colaboração com parceiros e aliados internacionais no desenvolvimento de melhores práticas de formação de força de trabalho cibernética; e (ii) incluir o desenvolvimento de força de trabalho cibernética nos esforços internacionais dos Estados Unidos.

O quarto e último pilar é a aprimoração da força de trabalho cibernética federal. O qual, uma vez que se enfoca especificamente em estratégias para aprimorar a força de trabalho cibernética em um contexto mais estrito, isto é, em sede do governo federal dos Estados Unidos, não será objeto de análise mais aprofundada neste momento.

IV. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 6. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 2



a. Recomendações para Construção das Metas:

Incluir questionário relativo aos indicadores de população em pesquisas amostrais nacionais de frequência trimestral, semestral ou anual, de forma a estabelecer série histórica. Buscar fontes já existentes, como a PNAD Contínua, as pesquisas do Cetic.br e a PINTEC (IBGE).

3 Engajamento e Integração Multi-institucional

O terceiro eixo foca no engajamento e integração multi-institucional, tendo como objetivo a construção de arcabouço institucional capaz de gerir, monitorar e avaliar os esforços da estratégia nacional.

I. Contexto do Eixo

O eixo busca iniciativas com objetivo de fomentar o engajamento e integração multi-institucional, através de acordos bilaterais ou multilaterais e de cooperação técnica, além de acordos formais de cooperação entre as forças de segurança e justiça.

Tal eixo está diretamente ligado ao desafio de integração, capacitação e infraestrutura necessários para que o **sistema de segurança pública atue efetivamente no combate aos cibercrimes, além do fortalecimento da cooperação internacional e a coordenação nacional de segurança cibernética com foco na gestão, monitoramento e integração dos esforços nacionais.**

II. Desafios Prioritários

a. Ausência de Dados e Integração

Em 2021, na sede do fórum "A evolução tecnológica na segurança pública", o então secretário de segurança pública de Goiás, o senhor Rodney Miranda[119], pontuou que, desde o começo do século, se discute, sem sucesso, a necessidade de se integrar as bases de dados de segurança pública.

Na mesma linha, o TCU[120] elaborou estudo no qual divulgou que mais da metade, **cerca de 67% das SSP, não compartilhavam seus dados sequer com as SSP dos Estados limítrofes**, o que dificulta o combate à criminalidade, na medida em que permite que criminosos migrem pelas fronteiras interestaduais.

Isso é especialmente verdade para os crimes cibernéticos, em que, pela sua própria natureza, podem ser cometidos de forma independente da localização física de seu executor, de modo que a ausência de integração entre as SSP pode se consubstanciar em verdadeira impunidade ao mesmo, que muda a sua localização física para outro Estado, sem interromper a prática dos atos criminosos.

Fontes:
119. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Vinte-anos-depois%2C-seguranca-publica-no-Brasil-padece-com-a-falta-de-integracao-de-dados-57081.html?UserActiveTemplate=mobile%2Csite. Acesso em 24.11.2023
120. Disponível em: https://www12.senado.leg.br/noticias/materias/2014/10/17/falta-de-integracao-entre-estados-facilita-criminalidade-revela-estudo-do-tcu. Acesso em 23.11.2023
121. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/12/19/governo-de-sp-inaugura-divisao-policial-com-delegacias-especializadas-no-combate-a-crimes-ciberneticos.ghtml. Acesso em 23.11.2023

b. Ausência de infraestrutura e capacitação

A ausência de infraestrutura e capacitação é um desafio também, mesmo que em alguns Estados da federação estejam desenvolvendo estruturas sólidas de combate ao cibercrime - com o **Estado de São Paulo** [122]**, destacando-se pela inauguração de uma Divisão de Crimes Cibernéticos**, formada por quatro delegacias especializadas - muitos Estados sequer possuem delegacias especializadas no combate ao crime cibernético [123].

Mesmo nos Estados que possuem delegacias especializadas, muitos apenas passaram a possuir há pouquíssimo tempo. **Por exemplo, na Bahia** [124]**, a primeira delegacia especializada foi fundada no último semestre de 2022**, o que é um forte indicativo de que muitas dessas delegacias ainda encontram-se em processo de estruturação.

Atualmente, é possível visualizar algumas iniciativas de capacitação das forças policiais e entidades de persecução criminal para o aperfeiçoamento do conhecimento sobre criminalidade cibernética.

A criação de **delegacias e outros órgãos de segurança pública especializados**, no entanto, não será uma solução eficaz, caso não seja acompanhado de capacitação e atualização de policiais, do Ministério Público e do próprio Judiciário, inclusive para que esses **profissionais se encontrem conscientes das novas práticas cometidas por cibercriminosos e como combatê-las** de forma apropriada.

Em 2022, o Ministério da Justiça e Segurança Pública lançou o **Plano Tático de Combate aos Crimes Cibernéticos**[125], com o principal objetivo de aprimorar as medidas de prevenção e repressão relacionadas a esse tipo de crime. Algumas medidas importantes fazem parte desse Plano, como por exemplo:

- Acordo de Cooperação entre a Polícia Federal e a FEBRABAN para o compartilhamento de informações visando o aprimoramento de medidas preventivas e educativas para a melhoria da segurança do ambiente cibernético.
- Criação de banco de dados de ocorrências, tendo acesso garantido às polícias judiciárias da União e dos estados, tornando o processo de investigação e solução de crimes mais eficientes.
- Criação de estrutura integrada com forças de segurança federais e estaduais, entidades privadas e públicas nacionais e internacionais com expertise sobre o tema.

Fontes:
122. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em 23.11.2023
123 Disponível em: https://www.bahianoticias.com.br/noticia/271273-policia-civil-cria-delegacia-especializada-em-investigacoes-de-crimes-virtuais. Acesso em 23.11.2023
124. Disponível em: https://revistaft.com.br/crimes-ciberneticos-analise-do-processo-investigatorio-e-os-desafios-para-combate-los/. Acesso em 24.11.2023
125. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-lanca-plano-tatico-de-combate-a-crimes-ciberneticos

c. Fortalecimento da Cooperação Internacional

O Crime Cibernético é, por sua própria natureza, um crime com componente transnacional. Com efeito, pela própria natureza da internet, fronteiras nacionais tornam-se cada vez mais tênues. Um ataque lançado em um determinado país pode afetar pessoas em diversos outros países. Somado a isso, ainda que direcionado para vítimas localizadas no mesmo país que o atacante, as evidências necessárias para se investigar o ataque podem encontrar-se localizadas em outros países, na medida em que servidores e outros ativos computacionais envolvidos na prática encontram-se dispersos no território de diversos Estados, o que é especialmente verdade com o avançar da computação em nuvem.

O Estado brasileiro já tem conhecimento da importância da cooperação internacional e, em especial, as forças de Segurança Pública, com a atuação preponderante da Polícia Federal. Com efeito, a Estratégia Nacional de Segurança Cibernética[126] previu enquanto uma de suas ações estratégicas, a necessidade de **ampliar a cooperação internacional brasileira** em matéria de segurança cibernética. Nesse sentido, o documento aponta enquanto diretrizes para guiar o aprofundamento da cooperação internacional:

- Estimular a cooperação internacional em segurança cibernética;
- Incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro;
- Ampliar o relacionamento internacional com os países da América Latina;
- Promover eventos e exercícios internacionais sobre segurança cibernética;
- Participar de eventos internacionais de interesse para o País;
- Ampliar os acordos de cooperação em segurança cibernética;
- Ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos;
- Estimular a participação do País em iniciativas futuras de estruturação normativa, como as relativas à criação de padrões de segurança em tecnologias emergentes, e
- Identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética.

Fontes:
126. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em 27.11.2023.

d. Gestão, Monitoramento e Integração dos Esforços Nacionais

Mesmo diante da realidade de possíveis ataques, identifica-se a ausência de políticas públicas robustas e estruturas permanentes capazes de resguardar o Brasil, as organizações e cidadãos aqui sediadas, de ameaças cibernéticas. Segundo mostra o GCI – Global Cybersecurity Index, realizado pelo Telecommunication Union, das Nações Unidas, um dos pilares centrais para que um país melhore suas capacidades de cibersegurança é a "Capacidade Organizacional". Neste pilar, se avalia a criação de Estratégias Nacionais, Agências Nacionais e Estratégias específicas ligadas a Proteção de Crianças no Ambiente Digital.

No Brasil, o GSI é o órgão responsável por planejar, coordenar e supervisionar as atividades de segurança da informação na administração pública federal, incluindo segurança cibernética, gestão de incidentes e proteção de dados[127]. Com o suporte do GSI, o Presidente da República promulgou em 26 de dezembro de 2023, o Decreto 11.856 instituindo a Política Nacional de Cibersegurança e criando o Comitê Nacional de Cibersegurança, representando um **grande passo rumo ao avanço da melhoria da cibersegurança no ambiente digital brasileiro e na construção de estruturas capazes de garantir a integração de entes competentes, realização de acordos bilaterais ou multilaterais e de cooperação técnica, além de acordos formais de cooperação entre as forças de segurança e justiça.**

Como apresentado no Contexto Internacional presente neste relatório e reforçado em diversos outros pontos, a implementação de um **estrutura que integre e coordene ações públicas e privadas, compreendendo seus diferentes níveis e segmentos,** relacionadas à segurança cibernética, se torna imperativo para que haja avanços consistentes nesta temática no cenário brasileiro.

Fontes:
127. Disponível em: https://www.calameo.com/read/0075181919588c4864ea6.
128. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

III. Referências nacionais e internacionais

Em relação a cooperação internacional, o Brasil aderiu e, por intermédio do Decreto nº 11.491/2023 promulgou a **Convenção de Budapeste**, um dos principais acordos internacionais em matéria de combate ao crime cibernético. A Convenção fornece importantes mecanismos de cooperação internacional, sinteticamente:

- Assistência mútua na conservação, busca, acesso, apreensão, interceptação ou guarda, ou revelação dos dados.
- Acessar, sem necessidade de autorização de outra Parte do Acordo: (i) dados de computador publicamente disponíveis; (ii) acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados no território de outra Parte, desde que obtenha o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para revelar os dados;
- Dever de indicar um órgão de contato 24x7 para assegurar assistência imediata relacionada a crimes cibernéticos.

No entanto, em que pese a adesão a Convenção de Budapeste possa ser vista enquanto medida de atendimento da diretriz de ampliação de acordos de cooperação internacional, a falta de Planos de Nação, impediram o avançar dos demais componentes da Estratégia de Segurança Cibernética. Deste modo, é recomendado que a Agenda envolva debates, propostas e promoções de um Plano Nacional que auxilie a concretizar as demais diretrizes da Estratégia Nacional de Segurança Cibernética e da Política Nacional de Cibersegurança, inclusive, como conscientizar as autoridades nacionais sobre as ferramentas que lhe foram disponibilizadas com a aderência a Convenção de Budapeste.

No âmbito da ausência de infraestrutura e capacitação, na esfera do Poder Legislativo, no ano de 2022, foi aprovado pela Comissão de Segurança Pública da Câmara dos Deputados o Projeto de Lei 4556/2020, de origem da ex Deputada Federal Policial Katia Sastre [129]. O objetivo deste Projeto de Lei é alterar a Lei 13.756/2018 para promover treinamento e conscientização dos servidores dos órgãos de segurança pública sobre criminalidade cibernética, utilizando recursos do Fundo Nacional de Segurança Pública. Neste momento o PL aguarda Designação de Relator na Comissão de Constituição e Justiça e de Cidadania (CCJC)[130].

Em novembro de 2023, a Secretaria de Segurança Pública (SSP) de Santa Catarina se reuniu com o CyberGAECO para o aperfeiçoamento das capacitações dos agentes e realização de novas parcerias para o combate aos crimes cibernéticos.

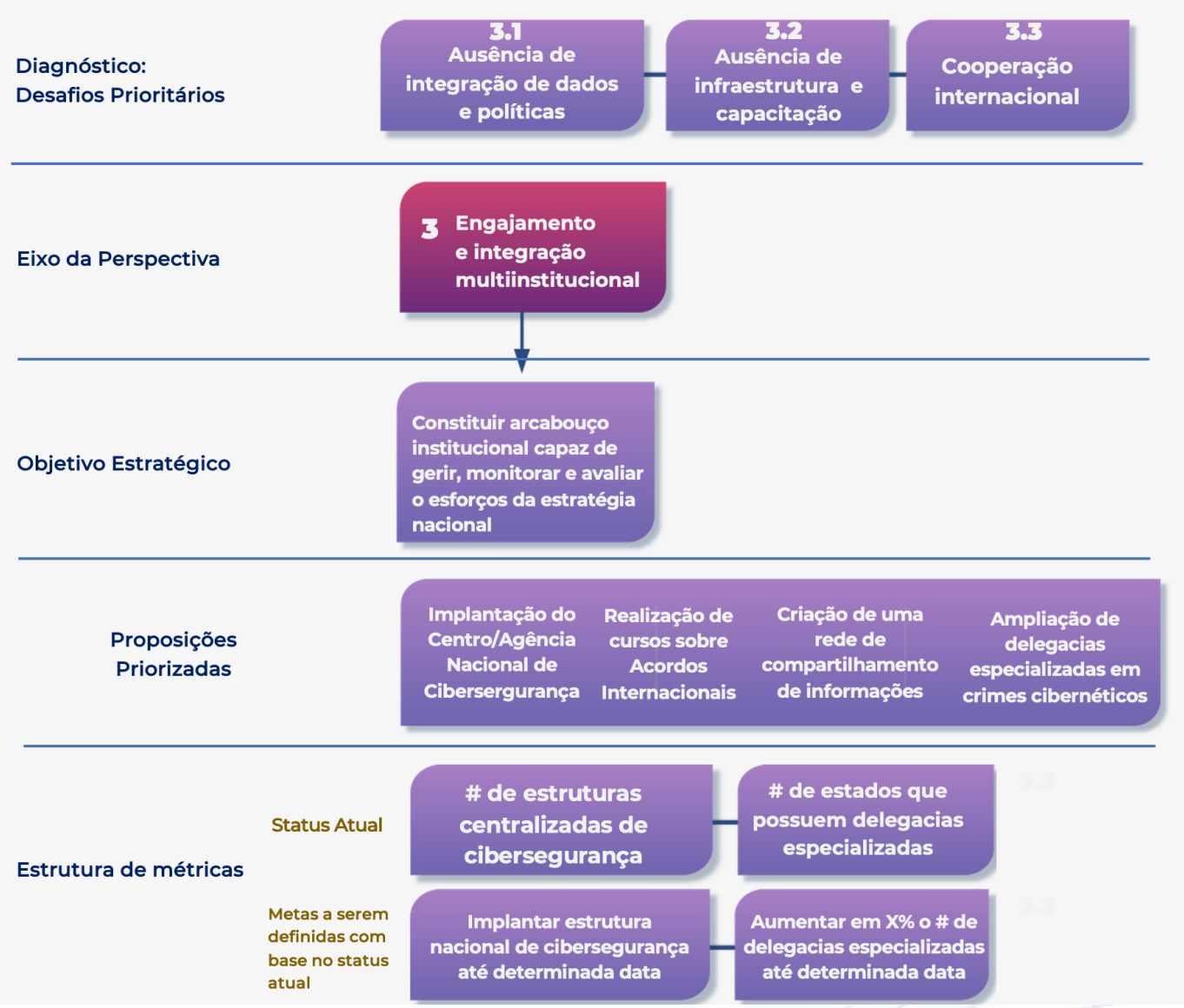
Assim, apesar da crescente necessidade de aprimorar e ampliar a capacitação dos profissionais de Segurança Pública em todo Brasil, este trabalho vem sendo feito por diversas entidades, que cada vez mais, buscam treinar e conscientizar os profissionais sobre as técnicas e melhores formas de combater a criminalidade cibernética.

Fontes:
129. Informações disponíveis em: https://www.camara.leg.br/noticias/871062-comissao-aprova-financiamento-de-cursos-contra-crimes-ciberneticos-para-servidores/
130. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2262834.
131. Disponível em: https://estado.sc.gov.br/noticias/em-visita-ao-cybergaeco-secretaria-de-seguranca-publica-discute-fortalecimento-de-novas-parcerias-e-capacitacoes-2/

IV. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 7. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 3



a. Recomendações para Construção das Metas:

Envolver o Ministério da Justiça e Segurança Pública na articulação interfederativa, visando à construção e integração de bases de dados de cibersegurança.

4. Informações e Conhecimento Especializado

O quarto eixo foca na disseminação de informações e conhecimento especializado, tendo como objetivo a criação de bases de dados qualificados e confiáveis, integrando os sistemas de segurança pública e demais atores pertinentes.

I. Contexto do Eixo

O eixo contempla o grande desafio que é a inexistência de base de dados qualificados, pesquisa e desenvolvimento em cibersegurança, de modo a apoiar o planejamento de iniciativas sobre a temática, planos de ação e políticas públicas eficientes.

A necessidade da integração dos dados das Secretárias de Segurança Pública (SSPs) é discutido desde 2003, no entanto um grande desafio para esta integração é a **ausência de dados para a criação de uma base compartilhada**, conforme mencionado também no Eixo 3 deste Relatório.

As políticas públicas baseadas em evidências requerem a disponibilidade de dados de alta qualidade e profissionais com capacidade em analisar os dados e avaliar as políticas. De acordo com o estudo da ENAP, "Políticas públicas baseadas em evidências: Mapeamento e direções" [133], analisou a produção sobre o uso de evidências em políticas públicas no Brasil, analisando o período de 1990 a 2020, foram encontrados 293 registros, após a limpeza e seleção, tais registros foram então classificados de acordo com o foco, se o trabalho explora a formulação de políticas ou a prática/implementação.

Entre 1990 e 2000 constam somente 11 estudos sobre o tema no Brasil, após a quantidade foi crescendo, no entanto o tema se tornou mais presente a partir de 2010, quando são observados o mínimo de 8 estudos em 2011 e o máximo de 36 estudos em 2018 sobre o tema. Quando considerado o foco das análises, 83% (243) dos estudos explora a prática na área de políticas públicas, isto é, como evidências são usadas ou podem ser usadas para a tomada de decisão na prática ou na implementação de políticas.

O estudo ainda levantou que os ministérios com maior esforço institucional de produção e disponibilização de dados são os ministérios da Saúde, Educação e Fazendo (dados consolidados de 2020), já os ministérios com menor desempenho no indicador de esforço de produção e disponibilização de dados são Minas e Energia, Integração Nacional e Cidades.

Fontes:

133. ENAP Cadernos, nº106, Políticas públicas baseadas em evidências: Mapeamento e direções. 2019. Disponível em: https://repositorio.enap.gov.br/jspui/bitstream/1/7201/2/Caderno_106_Politicas_publicas_20220916.pdf

II. Desafios Prioritários

a. Ausência de Dados Qualificados

Nem todos os crimes cibernéticos possuem sua tipificação precisa, a Lei 12.737/12, conhecida também como Lei Carolina Dieckmann, foi a primeira norma brasileira a tipificar crimes informáticos, instituindo por exemplo, o crime de "invasão de dispositivo informático", previsto no artigo 154-A.

Para os crimes cibernéticos impróprios, normalmente **o enquadramento é feito por analogia ao tipo previsto no Código Penal**. Por exemplo, não há uma tipificação própria para o phishing, entretanto, por analogia, se aplica o tipo previsto no artigo 171 do Código Penal, com a qualificante prevista no § 2º-A ("Fraude Eletrônica") do mesmo artigo, aumentando a pena quando a vítima é induzida a erro por meio de redes sociais, contato telefônico ou correio eletrônico fraudulento.

Ainda considerando o artigo 171, a Lei 14.478/22, que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais, alterou o Código Penal para prever o artigo 171-A ("Estelionato contra idoso ou vulnerável"), que dispõe:

> *"Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento"*

Deste modo, considerando que nem sempre há a distinção do crime previsto no artigo com sua modalidade cibernética e/ou respectiva qualificadora, não é possível visualizar com precisão dados sobre os ilícitos cibernéticos para a formação da base de dados.

A ausência de bases de dados integradas ou informações qualificadas é um óbice significativo ao desenvolvimento de políticas públicas eficientes no combate ao crime cibernético, uma vez que, no escopo das políticas públicas, dados se traduzem em "um recurso imprescindível e valioso", considerando a sua capacidade de apoiar na "identificação da demanda do público, de forma mais rápida e constante", e no cenário nacional, se torna um desafio devido à falta de tipificação dos dados.

Fontes:
134. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

Adicionada à esta finalidade, a construção de uma ampla base de dados públicos relacionados aos crimes cibernéticos. Conforme informações prestadas pelo então secretário de segurança pública de Goiás, em 2021, em sede do fórum "A evolução tecnológica na segurança pública" [135], o senhor Rodney Miranda, pontuou que, desde 2003, no lançamento do Colégio Nacional de Secretários de Segurança, discute-se a necessidade de se integrar os dados das Secretarias de Segurança Pública ("SSPs").

Se isso é um problema a nível dos crimes, em geral, a problemática se mostra ainda maior para os crimes cibernéticos, uma vez que, não raro, os dados divulgados pelas SSP não distinguem essa modalidade de crime de suas contrapartes intentadas por outros meios. Por exemplo, em relação ao estelionato, cinco dos Estados mais populosos da federação (Bahia, Ceará, Rio de Janeiro, Rio Grande do Sul e São Paulo) e o Rio Grande do Norte não informam a quantidade desagregada de registros de crimes de fraude eletrônica, das demais modalidades de estelionato [136].

A ausência de dados qualificados no âmbito do combate ao crime cibernético, impossibilita uma visão clara das necessidades da sociedade no combate ao cibercrime, como por exemplo, quais ações criminosas encontram-se em ascensão, impossibilitando a criação de políticas públicas efetivas para combater essas práticas, nomeadamente planos nacionais.

Fontes:
135. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Vinte-anos-depois%2C-seguranca-publica-no-Brasil-padece-com-a-falta-de-integracao-de-dados-57081.html?UserActiveTemplate=mobile%2Csite. Acesso em 24.11.2023
136. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-05-as-novas-configuracoes-dos-crimes-patrimoniais-no-brasil.pdf. Acesso em 21.11.2023
137. Disponível em: https://publications.iadb.org/pt/politicas-publicas-orientadas-por-dados-os-caminhos-possiveis-para-governos-locais. Acesso em 24.11.2023

III. Referências nacionais e internacionais

Em relação as políticas baseadas em dados, o surgimento das PPBEs (Políticas Públicas Baseadas em Evidências) nos Estados Unidos e em países da Comunidade Britânica pode ser visto como parte de uma agenda modernizante, aplicada simultaneamente às práticas profissionais médicas e ao setor público, emergindo a partir dos anos 1980 e finalmente ganhando grande impulso com a reforma do Estado britânico promovida por Tony Blair [138].

À título de referência, nos Estados Unidos, existe o Internet Complaint Center ("IC3") que consiste em um hub centralizado de informações para o reporte de crimes cibernéticos e posterior investigação. O IC3 é mantido e gerenciado pelo Federal Bureau of Investigation ("FBI"), e por conta disso, é possível a extração de métricas relevantes como: i) Estados mais afetados; ii) Tipos de crimes cibernéticos ocorridos com maior frequência, iii) Variação da ocorrência dos crimes, dentre outros. Anualmente, o resultado das análises das ocorrências são publicadas em relatório denominado "Internet Crime Report" [139], elaborado pelo FBI.

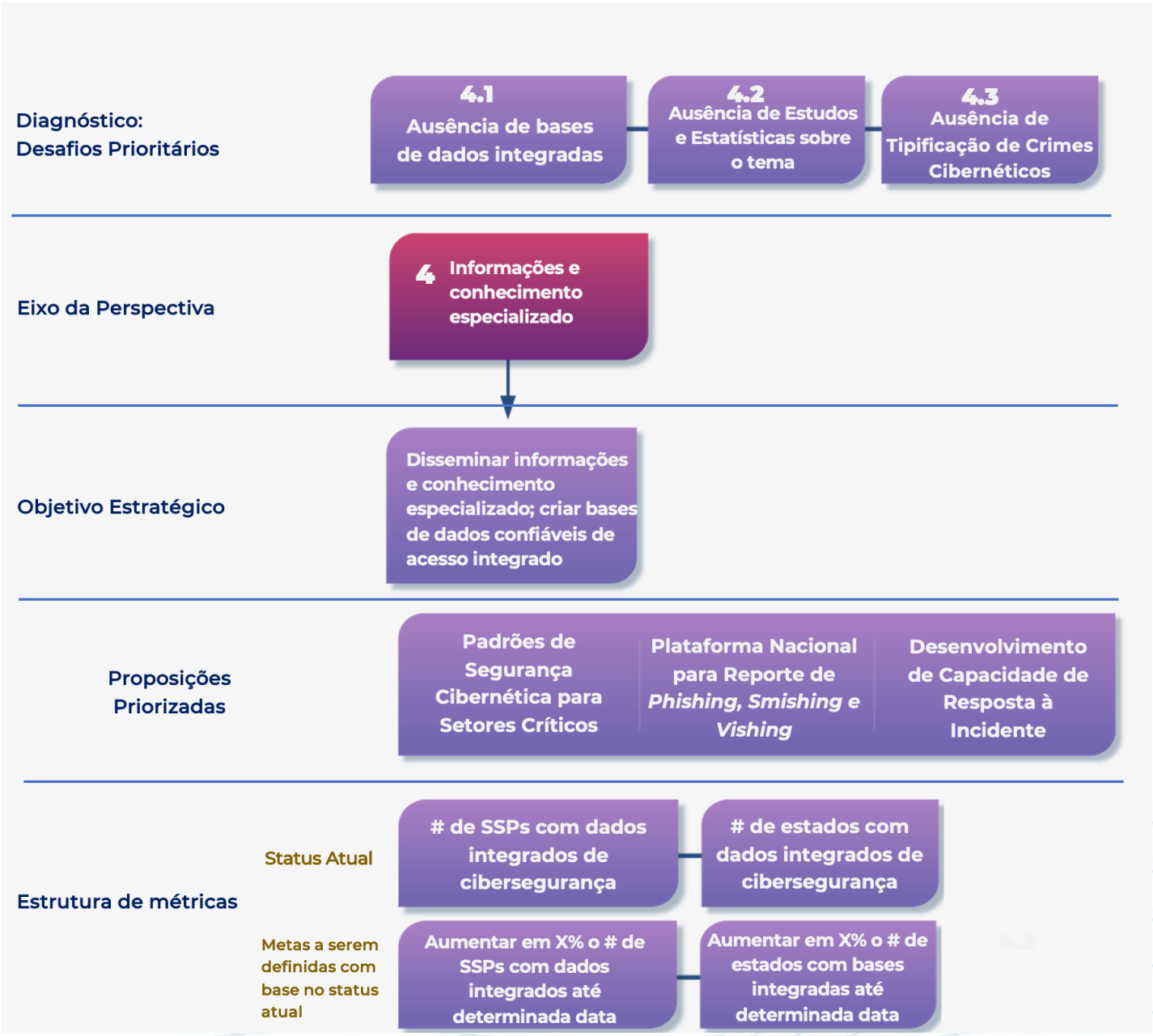
No Brasil, organizações como a SaferNe.org prestam um importante serviço ao país com os dados divulgados através do **Help Line, um canal online gratuito direcionado aos cidadãos** que oferece orientação de forma pontual e informativa para esclarecer dúvidas sobre segurança na Internet e como prevenir riscos e violações, a exemplo de intimidação, humilhações (ciberbullying), troca e divulgação de mensagens íntimas não-autorizadas (sexting ou nudes), entre outros crimes digitais.

Fontes:
138. Disponível no relatório "Políticas Públicas Baseadas em Evidências (PPBEs): delimitando o problema conceitual, disponível em: https://repositorio.ipea.gov.br/bitstream/11058/9915/1/td_2554.pdf
139. O Relatório do ano de 2022 é o mais recente. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Acessado em: 28.11.2023.

IV. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 8. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 4



a. Recomendações para Construção das Metas:

Envolver o Ministério da Justiça e Segurança Pública na articulação interfederativa, visando à construção e integração de bases de dados de cibersegurança.

5 Financiamento e Incentivos

O quinto eixo foca no financiamento e incentivos a cibersegurança brasileira, tendo como objetivo estimular a priorização real deste tema no planejamento nacional, garantindo as bases para o aumento significativo da maturidade do Brasil neste desafio.

I. Contexto do Eixo

O financiamento é um ponto chave para se debater a propositura de um programa nacional de cibersegurança eficaz. Um programa sem financiamento adequado tende a resultar em insucesso. Nesse sentido, o financiamento não se limita necessariamente a recursos financeiros, mas também a viabilização de recursos humanos, administrativos e tecnológicos.

Outro fator fundamental ao se debater a propositura de um programa nacional de segurança cibernética diz respeito ao seu financiamento – com efeito, um programa sem adequado financiamento tende a resultar em insucesso. Financiamento, para que não restem dúvidas, não se limita necessariamente a recursos financeiros, mas também a disponibilização de recursos humanos, administrativos e tecnológicos.

Um dos pilares apresentados pelo Índice de Defesa Cibernética do MIT, por meio dos quais os países são avaliados, é, justamente, os **recursos empregados para fins de cibersegurança** – o qual abrange tanto ativos legais, quanto tecnológicos empregados com este fim.

Em seu relatório do Indice de Defesa Cibernética do ano 2022/2023 [140], o MIT aponta que, em linhas gerais, **países com práticas robustas de proteção de dados tendem a obter melhores pontuações** – com a França obtendo a melhor pontuação do ranking, em parte devido a atuação de sua Autoridade de Dados.

Enquanto isso o Brasil, em que pese a existência da Lei Geral de Proteção de Dados e da própria ANPD, figurou apenas na 16ª posição. A má classificação nacional parece resultar da ausência de disponibilização de recursos adequados ao regulador, que, conforme reportado pelo próprio Diretor-Presidente, sofre com a ausência de autonomia financeira e forte limitação de pessoal [141]. Com efeito, foi reportado, inclusive, a ocorrência de significativo corte de orçamento do Regulador em 2024, bem como a ausência de adequado apoio político [142].

Assim, ao se abordar o financiamento de iniciativas nacionais de segurança cibernética, indubitavelmente, se fará necessário avaliar e defender o adequado financiamento dos agentes reguladores sobre o tema, incluindo, mas não se limitando, a própria ANPD.

Fontes:
140. Disponível em: https://mittrinsights.s3.amazonaws.com/CDIreport.pdf.
141. Disponível em: https://teletime.com.br/08/11/2023/presidente-da-anpd-cobra-concurso-publico-e-autonomia-financeira-do-orgao/.
142. Disponível em: https://capitaldigital.com.br/o-caos-administrativo-da-anpd/.

II. Desafios prioritários

a. Financiamento dos Órgãos Reguladores

Quando comparado, enquanto a ANPD, principal regulador federal sobre o tema no **Brasil, obteve um orçamento de cerca de R$: 24 milhões para o ano de 2024,** no ano antecedente a Cybersecurity and Infrastructure Security Agency, principal regulador federal sobre o tema nos Estados Unidos, obteve um orçamento de US$: 2.9 bilhões (cerca de R$: 14 bilhões, em câmbio atual) [143].

Mesmo considerando-se as diferenças proporcionais de PIB entre os países, com o Estados Unidos possuindo um PIB cerca de 12 (doze) vezes maior que o nacional em 2023 [144], a diferença em investimentos em segurança cibernética segue chamativa, com **o investimento estadunidense em seu principal regulador federal no tema superando proporcionalmente o investimento brasileiro em quase 49** (quarenta e nove) vezes.

Tabela 4. Orçamentos em Cibersegurança

País	Ano	Orçamento
Brasil	**2024**	**R$ 24 milhões**
Estados Unidos	2023	US$ 2.9 bilhões (cerca de R$: 14 bilhões, em câmbio atual)
França	2023	€26 milhões (cerca de R$: 144 milhões, em câmbio atual) [145]
Reino Unido	2023	£85.3 milhões (ou cerca de R$: 543,31 milhões, em câmbio atual) [146]
Itália	2021	€30 milhões (aproximadamente, R$: 163,3 milhões, em câmbio atual) [147]

Elaboração própria

Essas discrepâncias revelam um desinteresse público no fortalecimento da Autoridade de Dados Nacional o que, naturalmente, gera significativos impactos em matéria de Segurança Cibernética, sobretudo, tendo em vista que, na maioria dos casos, a cibersegurança se encontrará intrinsicamente ligada à proteção de dados. O adequado financiamento da ANPD deverá, por conseguinte, ser tema de proposituras relacionadas a programas nacionais de segurança cibernética.

Em se tratando especificamente de Segurança Cibernética, foi **proposta a criação de uma Agência Nacional de Segurança Cibernética, cujo orçamento seria de aproximadamente R$: 600 milhões a partir do quinto ano de sua implementação**. No entanto, mencionada entidade não foi criada na última versão aprovada da Política de Segurança Cibernética, em 26 de dezembro de 2023 – a qual limitou-se o Comitê Nacional de Cibersegurança, um órgão com função preponderantemente consultiva, sem poder decisório de fato, e que não inclui, dentre os órgãos com representação em sua composição, a ANPD.

Fontes:
143. Disponível em: https://securityintelligence.com/articles/how-much-is-us-investing-in-cyber/
144. Disponível em: https://oglobo.globo.com/economia/noticia/2024/03/01/com-crescimento-de-29percent-brasil-ocupa-a-14a-posicao-em-ranking-global-das-economias-e-perde-duas-posicoes.ghtml.
145. Disponível em: https://www.data.gouv.fr/en/datasets/budget-de-la-cnil-1/#/resources.
146. Disponível em: https://ico.org.uk/media/about-the-ico/minutes-and-papers/4024826/budget-20230320.pdf
147. Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9755883#:~:text=In%20Italia%2C%20come%20%C3%A8%20noto,di%2030%20milioni%20di%20euro.

Tabela 5. Orçamentos das Agências de Cibersegurança

País	Período	Orçamento
Brasil	**5 anos**	**R$: 600 milhões (proposta)** [148]
Itália	2021-2027	€529 milhões (cerca de R$ 2,87 bilhões, em câmbio atual)
França	2022	€22,8 milhões (cerca de R$ 124,05 milhões, em câmbio atual) [149]
Reino Unido	2016-2021	£1,9 bilhão (cerca de R$: 12,13 bilhões, em câmbio atual) [150]

Elaboração própria

b. Financiamento das Forças de Segurança

Segundo o Relatório do Fórum Brasileiro de Segurança Pública de 2023, **apesar de crescimento das despesas, a proporção de gastos com segurança pública caiu na maioria dos estados e na União em 2022**. Houve um gasto com a função segurança pública de R$124,8 bilhões, sendo que, destes, R$ 101 bilhões foram financiados pelos Estados e Distrito Federal. O gasto total em segurança teve crescimento de 11,6% em relação ao ano anterior justamente pelo maior volume de despesas estaduais, essas 12,9% em relação a 2021.

Ainda nesta frente, em 2024 o Governo Federal realizou redução de aproximadamente R$ 400 milhões nas verbas destinadas ao Ministério da Defesa, Polícia Federal e Abin – Agência Nacional de Inteligência.

Além do financiamento de estruturas centralizadas de combate ao crime cibernético, é importante garantir que haja recursos também para as forças de segurança pública nacional, de modo que sejam capazes de adequar sua infraestrutura e realizar a contínua capacitação de seu corpo efetivo em relação às práticas cada vez mais sofisticadas de crimes cibernéticos.

Fontes:
148. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Orcamento-de-R%24-600-milhoes-e-maior-desafio-para-Agencia-Nacional-de-Ciberseguranca-63455.html?UserActiveTemplate=mobile.
149 Disponível em: https://cyber.gouv.fr/sites/default/files/document/Rapport%20annuel%202022.pdf
150. Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf. Acesso em 11.03.2024

c. Linhas de Financiamento Especiais – Suporte às PMEs

De acordo com pesquisa realizada pela IBM [151], 62% dos ataques cibernéticos foram direcionados a pequenas e médias empresas. Em estudo realizado pela Mastercard [152], este conjunto de empresas dá menor importância à cibersegurança em comparação com as grandes empresas.

No entanto, o Brasil possui cerca de 9 milhões de pequenas e microempresas cadastradas, representando aproximadamente 27% do PIB (Sebrae) e 99% dos negócios no país. Deste modo, a exemplo de outros países como Portugal e Reino Unido, é premente considerar investimentos, linhas de crédito especiais e políticas de educação voltadas a este público como prioridade nas ações nacionais.

De acordo com uma pesquisa realizada pelo Datafolha, solicitada pela Mastercard [153], feita com 351 tomadores de decisão da área de tecnologia de empresas dos setores de educação, financeiro e seguros, tecnologia e telecom, saúde e varejo, apontou que 80,6% das empresas afirmam dar muita importância à cibersegurança, mas apenas 31% delas priorizam a área no plano de investimento. O resultado desse descompasso entre discurso e realidade é que a maioria dessas mesmas empresas (57%) **já foi alvo de fraudes e ataques digitais com alta ou média frequência**.

Investimentos empresariais em segurança

78% das empresas têm profissional de TI para segurança digital

53% creem que investimento na área traz alto nível de confiança

48% têm política de cibersegurança para os funcionários

31% priorizam a área no plano de investimentos

25% têm planejamento anual para a área

32% têm departamento próprio para a área

Como as empresas se protegem

98% fazem backups regularmente

78% afirmam ter plano de resposta a ataque

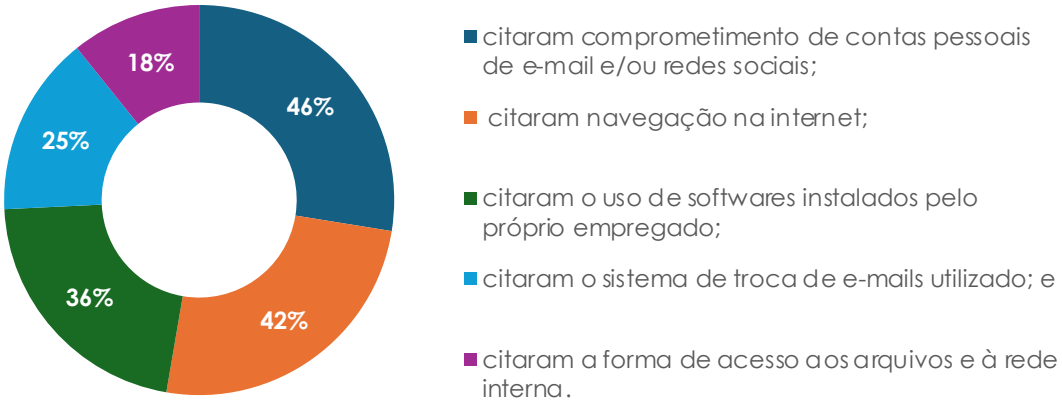
58% costumam realizar testes de segurança

32% fizeram simulação de ataques de vazamento nos últimos 3 meses

Fontes:
151. Informações em: https://tiinside.com.br/04/10/2023/pmes-sao-alvos-em-62-dos-casos-de-ataques-ciberneticos-diz-estudo/
152. Disponível em: https://sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD
Informações disponíveis em: https://mercadoeconsumo.com.br/28/07/2023/artigos/medias-empresas-por-que-ninguem-fala-delas/
153. Dados disponíveis em: https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/mais-que-cartao/ciberseguranca/investimento-em-ciberseguranca-ainda-nao-e-prioridade-para-empresas-aponta-datafolha/

A mesma pesquisa da Mastercard, levantou as principais ameaças e riscos das MPEs.

Gráfico 4. Relação ameaças e principais riscos das PMEs [154]



Em relação as linhas de financiamento voltadas para as PMEs, se destacam o **Programa Nacional de Apoio às Microempresas e Empresas de Pequeno Porte (PRONAMPE)** da Caixa, que tem como objetivo auxiliar no desenvolvimento e fortalecimento do seu negócio.

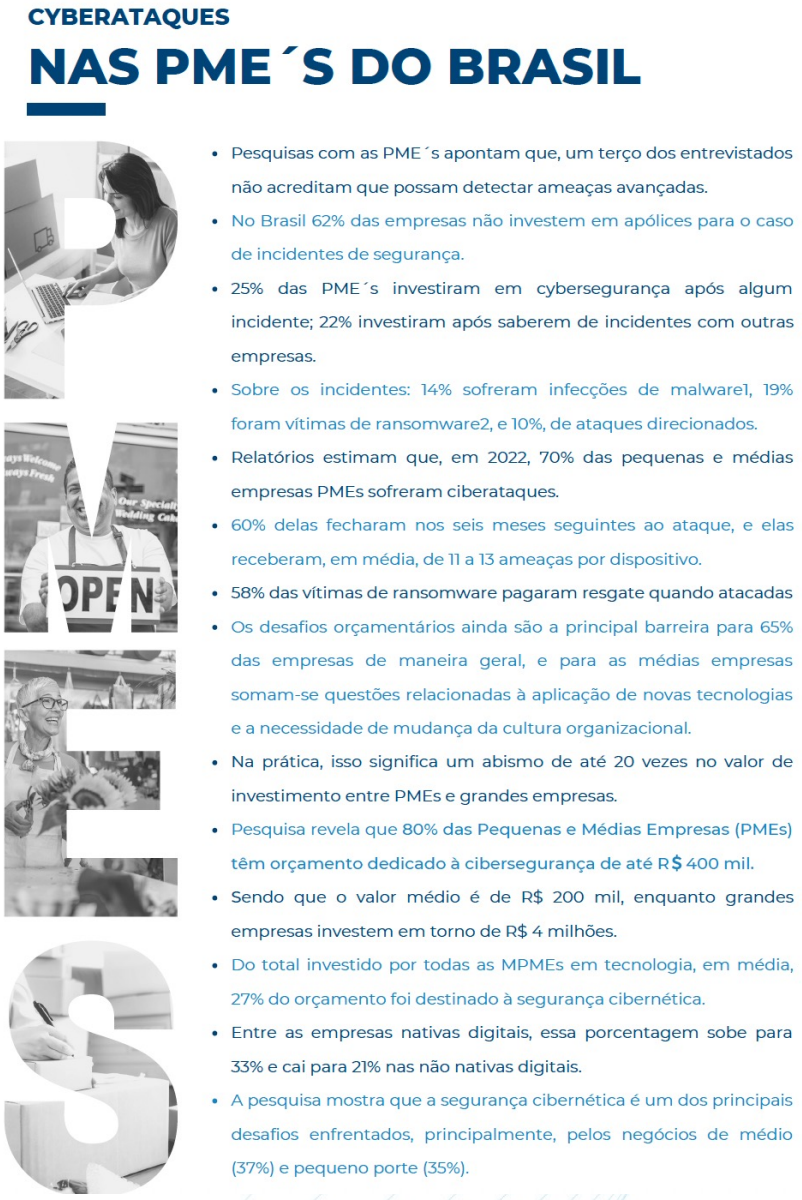
Além da falta de linhas de financiamento voltadas para PMEs, identifica-se uma ausência de políticas públicas direcionadas para as médias e pequenas empresas, tais empresas ocupam um papel de protagonismo na economia, representando quase a totalidade das empresas existentes no Brasil. Seguindo as tendencias já relatadas neste documento, as micro e pequenas empresas também se aliam a tecnologia para aprimorar seus negócios [155]. Entretanto, muitas empresas, por se acharem "pequenas", entendem que não serão alvos de cibercriminosos mal-intencionados, acabando por não investir os recursos necessários para garantir a proteção das informações de seu negócio, incluindo dados de clientes e colaboradores [156], se encontrando em situação de alta vulnerabilidade cibernética. Importante ressaltar que, de acordo com pesquisa realizada pela IBM, 62%[3] dos ataques cibernéticos foram direcionados a pequenas e médias empresas. Em estudo realizado pela Mastercard [157], as pequenas e médias empresas dão menor importância à cibersegurança em comparação as grandes empresas.

Por conta de todos os impactos que podem ocorrer em uma empresa pela ocorrência de um incidente de segurança ocasionado por uma exploração de vulnerabilidade cibernética (danos reputacionais, prejuízo financeiros e geração de danos aos titulares de dados pessoais), é imperativo que micro, pequenas e médias empresas passem a desenvolver maior consciência dos riscos Cibernéticos a que estão sujeitas e apliquem medidas de segurança adequada aos riscos.

Fontes:
154. Mais informações em: https://febrabantech.febraban.org.br/temas/meios-de-pagamento/micro-e-pequenas-empresas-brasileiras-aceleram-adocao-de-pagamento-digital
155. Informações em: https://www.nvseguros.com.br/investimento-em-ciberseguranca
156. Informações em: https://tiinside.com.br/04/10/2023/pmes-sao-alvos-em-62-dos-casos-de-ataques-ciberneticos-diz-estudo/
157. Dados disponíveis em: https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/mais-que-cartao/ciberseguranca/investimento-em-ciberseguranca-ainda-nao-e-prioridade-para-empresas-aponta-datafolha/

É imperativo a adoção de controles de segurança adequados aos riscos por parte das empresas, principalmente as pequenas e médias, que ainda possuem uma estrutura defasada em cibersegurança. Conforme estudo do INCC (Instituto Nacional de Combate ao Crime Cibernético) [158], **ataques a micro e pequenas empresas no Brasil crescem até 41% ao ano**, sendo que em 27% das empresas analisadas, os responsáveis não tratam cibersegurança como uma prioridade.

Além desses indicadores, o Instituto traz outras importantes estatísticas que revelam a fragilidade da segurança cibernética de pequenas e médias empresas no Brasil, conforme imagem abaixo



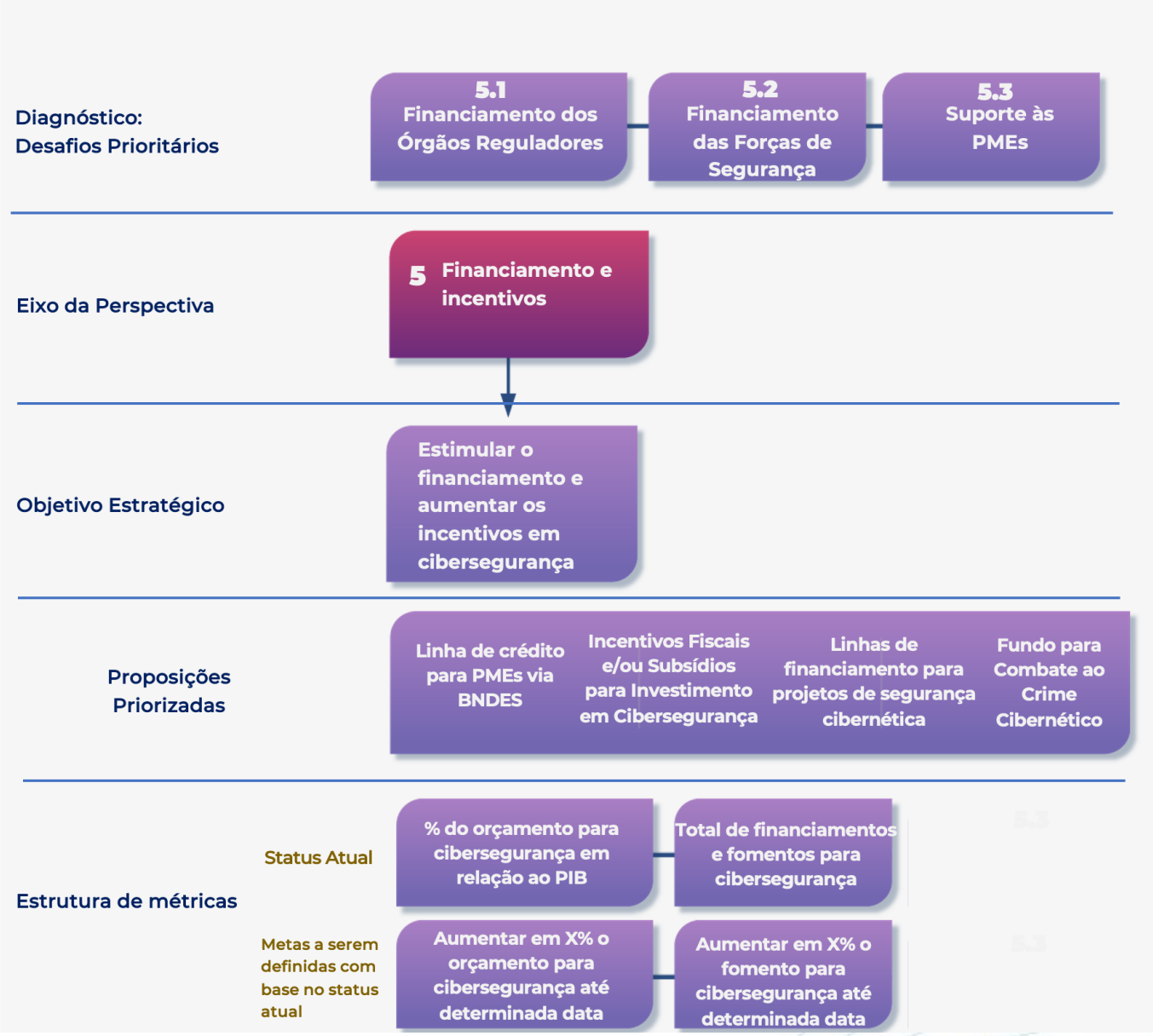
Assim, dentro desse cenário, é importante a realização de ações de conscientização por parte do governo para esse grupo de empresas, de modo a mitigar potenciais danos que podem ser causados pela exploração de vulnerabilidades cibernéticas. Além disso, parcerias com entidades privadas são essenciais, já que as grandes empresas de cibersegurança e tecnologia possuem recursos e conhecimentos úteis para sustentar a difusão do conhecimento e promover o aculturamento sobre segurança digital.

Fontes:
158. INCC. Visão Global – Panorama sobre Crimes Cibernéticos no Brasil 2023-2024.

III. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 9. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 5



a. Recomendações para Construção das Metas:

Criar codificação na estrutura do orçamento federal de foma a identificar os gastos em custeio e investimento relacionados ao tema da cibersegurança.

6 Arcabouço Legal, Regulatório e Normativo

O sexto eixo concentra-se na análise do arcabouço legal, regulatório e normativo, visando à formulação de políticas públicas direcionadas às vulnerabilidades nacionais.

I. Contexto do Eixo

O eixo ressalta a importância das políticas públicas voltadas para as fragilidades que demandam desenvolvimento no Brasil, com foco na aprimoração da regulamentação e do arcabouço legal, além do estabelecimento de colaborações internacionais. Isso engloba a implementação da política nacional de cibersegurança, o estabelecimento de uma estrutura operacional dedicada à cibersegurança, a promulgação de leis de combate ao crime cibernético e a elaboração de instrumentos regulatórios específicos.

É evidente que o Brasil possui um extenso conjunto de normas relacionadas ao ambiente digital e à criminalidade cibernética. No entanto, os cibercriminosos se adaptam rapidamente, aproveitando as tecnologias mais recentes em seu favor e deixando um histórico de vítimas antes que medidas defensivas adequadas possam ser implementadas. Nesse sentido, é crucial destacar a importância da **integração de ações entre os diferentes níveis de governo - federal, estadual e municipal - para lidar eficazmente com essas ameaças**. Embora não tenham sido identificados dados sobre iniciativas coordenadas de integração em atividade no Brasil, é imperativo reconhecer que **tais esforços são essenciais para fortalecer a segurança cibernética e minimizar as vulnerabilidades existentes**.

Em tempos de Inteligência Artificial, o Brasil começa a demonstrar preocupação com o uso desse tipo de tecnologia nas eleições [159], diante do aumento recente do uso de Deep Fake no contexto político. Assim, o Direito deve seguir a sua tendência natural de regular cenários fáticos para combater ações que possam violar direitos fundamentais.

Exemplos de normas relacionadas à proteção de dados, segurança cibernética e crimes digitais:

- **Marco Civil da Internet (Lei nº 12.965/2014)** [160] **:** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Inclui disposições sobre neutralidade da rede, privacidade, segurança e retenção de dados.

Fontes:
159. Disponível em: https://exame.com/brasil/justica-eleitoral-intensifica-guerra-contra-as-deepfakes-que-poderao-gerar-ate-cassacao/
160. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

- **Decreto 8.771/2016** [161] **:** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

- **Lei Geral de Proteção de Dados (LGPD)(Lei nº 13.709/2018)** [162] **:** Regulamenta o tratamento de dados pessoais por parte de organizações públicas e privadas.

- **Código Penal Brasileiro (Decreto-Lei nº 2.848/1940)** [163]**:** Contém disposições relativas a crimes cibernéticos. Já foi alterado pelas seguintes normas:

    - **Lei 12.737/2012 (Lei Carolina Dieckmann)** [164]**:** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências

    - **Lei 14.478/2022** [165]**:** Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.

    - **Lei 14.811/2024 (Lei do Bullyng e do Cyberbullyng)** [166]**:** Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).

- **Decreto Nº 10.222/2020**[167]**:** Aprova a Estratégia Nacional de Segurança Cibernética.

Fontes:
161. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm
162. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
163. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm
164. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
165. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=14478&ano=2022&ato=c12ITVE9kMZpWTf4c
166. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm
167. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

II. Desafios prioritários

São perceptíveis obstáculos significativos no contexto brasileiro em relação ao avanço efetivo em cibersegurança, como visto a seguir:

a. Legislação criminal e tipificação de crimes cibernéticos

- A legislação brasileira precisa **continuamente tipificar novas modalidades de crimes cibernéticos**, como fraudes sofisticadas e ataques a infraestruturas críticas. Grande parte das alterações no Código Penal até agora foram **reativas,** respondendo a casos específicos que demonstraram a precariedade das leis existentes. **Para enfrentar esse cenário, é essencial que a legislação aborde o uso de tecnologias emergentes, como inteligência artificial e blockchain, no contexto de crimes cibernéticos.** Por exemplo, as fraudes financeiras online, especialmente com o uso de Pix e carteiras digitais, estão em ascensão e exigem legislação específica para combater esses novos métodos de crime. Além disso, **os ataques ransomware** estão se tornando mais frequentes e mais prejudiciais, exigindo uma legislação mais rigorosa e específica para lidar com eles, bem como os crimes cometidos por meio de **redes sociais e outros agravados por estes meios tais como o abuso sexual infantil pela internet**.

b. Gargalos no Decreto n° 8.771/2016

- Quando se analisam os padrões nacionais de cibersegurança, destaca-se o marco inicial estabelecido em 2016 pelo **Decreto n° 8.771/2016**, o qual **regulamentou o Marco Civil da Internet**. Este decreto definiu nos artigos 13° ao 16° os Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, constituindo-se como um padrão multisetorial, uma vez que abrange todos os provedores de aplicações de internet, assim como os provedores de conexão com a internet. **No entanto, apesar de sua abrangência, o Decreto não previu a necessidade de adoção de controles técnicos básicos, como soluções de proteção contra malware, além de não mencionar quaisquer medidas de segurança administrativas.** Essas lacunas podem representar um desafio significativo para a eficácia dos padrões de cibersegurança no país, demandando revisões e atualizações que contemplem um espectro mais abrangente de medidas de proteção e prevenção.

c. Abrangência da Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709/2018

- Embora a **Lei Geral de Proteção de Dados brasileira** se inspire amplamente na legislação europeia, apresenta uma diferença substancial em relação ao Regulamento Geral de Proteção de Dados da União Europeia: **enquanto o *General Data Protection Regulation* (GDPR) estabelece diretrizes mais específicas sobre as medidas de segurança mínimas a serem implementadas, a norma nacional determina que tais medidas serão definidas por meio de regulamentação a ser emitida pela Autoridade Nacional de Proteção de Dados (ANPD). Essa distinção pode gerar impactos na interpretação e aplicação das medidas de segurança**, demandando uma atenção especial às futuras regulamentações emitidas pela ANPD para garantir a conformidade efetiva com os requisitos de proteção de dados.

Fontes:
173. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf
174. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm
175. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf

d. Implementação e limitação das Diretrizes da ANPD

- Até o momento, a atuação da ANPD **tem sido marcada pela apresentação de um único framework multisetorial, conforme descrito em seu Guia Orientativo Sobre Segurança da Informação para Agentes de Pequeno Porte**. Esse guia tem como objetivo estabelecer um padrão para ser seguido por agentes de pequeno porte, como microempresas, empresas de pequeno porte e startups, visando fornecer diretrizes específicas para a implementação de medidas de segurança da informação adequadas às suas necessidades e recursos.

- Apesar de sua importância, há lacunas a serem destacadas nessa iniciativa. Uma delas é a **falta de abordagem específica para certas áreas de risco que podem ser particularmente relevantes para agentes de pequeno porte, como a segurança de dados em ambientes de trabalho remoto ou o gerenciamento de terceirizados que têm acesso aos dados da empresa**. Outro ponto a ser considerado é a necessidade de **atualização periódica do guia** para acompanhar as mudanças no cenário de ameaças cibernéticas e as evoluções na tecnologia e nas práticas de segurança da informação. Isso garantiria que o guia permaneça relevante e eficaz ao longo do tempo, adaptando-se às novas demandas e desafios enfrentados pelos agentes de pequeno porte no contexto da proteção de dados.

Na próxima página é apresentada uma tabela resumo com as principais legislações internacionais sobre o tema de cibersegurança.

Fonte:
176. Decreto n°11.856, disponível em https://www.calameo.com/read/0075181919588c4864ea6.
177. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf

Tabela 6. Principais legislações internacionais sobre cibersegurança

Aspecto	Brasil	EUA	União Europeia	China
Lei Principal	Lei Geral de Proteção de Dados (LGPD)	Cybersecurity Information Sharing Act (CISA)	General Data Protection Regulation (GDPR)	Cybersecurity Law of the People's Republic of China
Ano de Implementação	2020	2015	2018	2017
Objetivo Principal	Proteção de dados pessoais	Compartilhamento de informações de cibersegurança	Proteção de dados pessoais e privacidade	Proteção da segurança nacional e dos cidadãos
Autoridade Responsável	ANPD (Autoridade Nacional de Proteção de Dados)	CISA (Cybersecurity and Infrastructure Security Agency)	European Data Protection Board (EDPB)	CAC (Cyberspace Administration of China)
Multas e Penalidades	Multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração	Multas e ações civis	Multas de até 4% do faturamento global anual da empresa	Multas e penalidades criminais severas
Proteção de Dados Pessoais	Sim	Sim	Sim	Sim
Notificação de Violações	Obrigatória	Obrigatória	Obrigatória	Obrigatória
Cooperação Internacional	Sim	Sim	Sim	Limitada
Regulação de Infraestruturas Críticas	Sim	Sim	Sim	Sim
Responsabilidade das Empresas	Elevada	Elevada	Elevada	Elevada
Tecnologias Específicas Regulamentadas	Inclui Pix e carteiras digitais	Inclui redes sociais e plataformas online	Inclui qualquer processamento de dados pessoais	Inclui qualquer atividade online e dados pessoais

Elaboração própria

III. Referências nacionais e internacionais

O Modelo de Maturidade desenvolvido pela Universidade de Oxford, estabelece como uma de suas dimensões de avaliação os Frameworks Legais e Regulatórios – dimensão esta compreendida como a capacidade governamental de desenhar e promulgar frameworks legislativos com relevante afetação para a área da segurança cibernética [180].

A dimensão avaliativa dos frameworks legais e regulatórios é dividida em quatro grupos, os quais serão abordados nas linhas que seguem:

a) Provisões regulatórias e legais: o objetivo deste grupo é avaliar os dispositivos legais que afetem diretamente a segurança cibernética [181].

b) Frameworks legislativos relacionados: o objetivo deste item é avaliar os frameworks regulatórios existentes relacionados com segurança cibernética, incluindo frameworks de Proteção de Dados[3] [182]

O primeiro destes padrões foi estabelecido em 2016, como o Decreto n° 8.771/2016, que regulamentou o Marco Civil da Internet, estabelecendo em seu art. 13° ao 16° os Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas. Tratou-se de um padrão multisetorial, vez que abrange todas os provedores de aplicações de internet (ou seja, qualquer provedor de funcionalidades acessíveis através da internet), bem como provedores de conexão com a internet.

Ele incluiu o dever de (i) controle de acesso estrito aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários (ii) mecanismos de autenticação de acesso aos registros; (iii) criação de inventário detalhado dos acessos aos registros de conexão [183] e de acesso a aplicações [184], contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado; (iv) o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes; e (v) dever de minimizar os dados; (vi) o dever de manter os dados cadastrais em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal; (vii) o dever de divulgar de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, informações sobre as medidas de segurança adotadas.

Fontes:
180. Disponível em: https://gcscc.ox.ac.uk/cmm-dimensions-and-factors
181. Disponível em: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
182 Disponível em: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
183. O conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
184. O conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Note-se, no entanto, que o Decreto, além de deixar de prever a necessidade de adoção de controles técnicos básicos, como soluções de proteção contra malware, também deixou de citar quaisquer medidas de segurança administrativas.

A nossa Lei Geral de Proteção de Dados, embora em muito se inspire na legislação europeia, apresenta uma diferença significativa em relação ao Regulamento Geral de Proteção de Dados da União Europeia: enquanto este apresenta diretrizes mais claras sobre as medidas de segurança mínimas a serem adotadas, a norma nacional fixa que essas medidas de segurança serão definidas por intermédio de regulamento a ser expedido pela ANPD.

Nessa esteira, até o presente momento, a ANPD limitou-se a apresentar um único framework multisetorial em sede de seu **Guia Orientativo Sobre Segurança da Informação para Agentes de Pequeno Porte** [185], voltado, como o nome sugere, a definir um padrão a ser seguido pelos agentes de pequeno porte (microempresas, empresas de pequeno porte e startups).

Citado framework apresenta um razoável conjunto de controles administrativos (ex. Política de Segurança da Informação; dever de gerenciar contratos; elaborar acordos de nível de serviço para serviços em nuvem; e adotar medidas de conscientização e treinamento) e técnicos (ex. controle de acesso; pseudonimização e criptografia; cópias de segurança; criptografia de dados em trânsito; deleção remota de dados de dispositivos móveis, dentre outros).

O framework é razoavelmente robusto para o público ao qual ele se dirige, sobretudo considerando que os agentes regulados não serão considerados de pequeno porte se realizarem operações de tratamento de risco crítico, não poderão ser beneficiários do regime dos agentes de pequeno porte (art. 3°, I, da Resolução CD/ANPD n° 2/2022 [186]).

Em se tratando de frameworks setoriais, o principal em vigor nacionalmente é a Resolução CMN n° 4.893/2021 [187], o qual demanda às Instituições Financeiras a implementação de uma Política de Segurança Cibernética, a qual deve incluir controles técnicos de administrativos.

Enquanto controles administrativos, a Resolução demanda uma série de medidas, desde a própria elaboração da Política, seguida pela disseminação da cultura de segurança cibernética, incluindo avaliação periódica de pessoal, perpassando pelo compromisso da alta gestão, procedimentos para o tratamento de incidentes, o dever de divulgar publicamente uma síntese da Política, gestão de riscos, dentre outros.

Fontes:
185. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf
186. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019
187. Disponível em: https://www.ancord.org.br/wp-content/uploads/2021/03/Resolucao-CMN-n-4.893-de-26_2_2021.pdf

Por sua vez, em aspectos técnicos, requer que as organizações implementem uma série de controles, tais como "a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações" [188].

Ainda, caso a organização faça uso de serviços relevantes de computação em nuvem, a regulação apresenta uma série de requisitos a serem cumpridos, desde a implementação de procedimentos de diligência prévia, perpassando por cláusulas contratuais específicas mandatórias e até mesmo uma obrigação de comunicação das contratações ao Banco Central. De fato, as obrigações presentes na Resolução do Banco Central muitas vezes se aproximam de sua contraparte europeia, o Digital Operational Resilience Act [189].

No entanto, enquanto o *framework* do Banco Central busca fixar controles mínimos específicos que devem ser adotados pelos agentes regulados, o modelo europeu opta por adotar um modelo predominantemente baseado em risco, orientando as fases em que o programa de segurança cibernética da organização deve atuar, mas, com algumas exceções, não quais controles concretamente a organização deve implementar.

A maior vantagem da abordagem nacional em relação à europeia é sua concretude: os agentes regulados sabem os controles mínimos que se encontram obrigados a adotar, recaindo sobre si apenas o processo decisório de estabelecer "como" implementar os controles mínimos e, sendo o caso, apenas quais controles complementares (não mandatórios) implementar. A maior desvantagem, entretanto é sua tendência à rápida obsolescência, precisando ser constantemente revisado, considerando a célere evolução das ameaças cibernéticas.

Em linhas gerais, apesar das diferenças em abordagem, o regulamento nacional é razoavelmente maduro, apresentando controles consideravelmente robustos. Podendo, o framework europeu ser observado como fonte para aprimoramento daquela previsto no Banco Central. Nessa esteira, existem alguns controles previstos no Digital Operational Resilience Act, que não se encontram no framework nacional e cuja adoção nos parece razoável, por exemplo: (i) gestão de mudanças; e (ii) mapeamento de ativos de tecnologia da informação.

Fontes:
188. Disponível em: https://www.ancord.org.br/wp-content/uploads/2021/03/Resolucao-CMN-n-4.893-de-26_2_2021.pdf
189. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

Por sua vez, o padrão proposto pela ANATEL, em sua Resolução n° 740/2020 [190], embora, tal como o framework do Banco Central, seja pautado na necessidade de construção de uma Política de Segurança Cibernética, aparenta adotar uma abordagem baseada em riscos, não apresentando uma listagem de controles mínimos a serem adotados, com algumas exceções (ex. Plano de Resposta a Incidentes), antes requerendo que as organizações (i) adotem "procedimentos e controles adotados para a identificação e a análise das vulnerabilidades, das ameaças e dos riscos associados à Segurança Cibernética, às Infraestruturas Críticas de Telecomunicações e à continuidade dos serviços de telecomunicações"; (ii) mapeiem "possíveis riscos de incidentes e de eventos que possam afetar a segurança do armazenamento dos dados dos usuários"; e (iii) realização de ciclos de avaliação de vulnerabilidades por entidade aferidora ou empresa capacitada independente, cujo resultado deve ser comunicado à ANATEL.

De semelhante natureza é a Resolução Nº 964/2021, da ANEEL [191], que, embora preveja alguns requisitos mínimos a serem atendidos pela Política de Segurança Cibernética das empresas de energia, em última análise confere aos agentes regulados o papel de fixar os controles a serem adotados, em atenção aos seus deveres de (i) "identificar, avaliar, classificar e tratar os riscos cibernéticos na estrutura estabelecida pelo agente"; e (ii) compatibilizar a Política com (a) relevância da instalação no contesto do sistema de produção e transmissão de energia elétrica do Brasil; e (b) com a sensibilidade dos dados e das informações sob sua responsabilidade.

Essa abordagem, para serviços essenciais, baseada em risco, parece encontrar-se em linha com as tendências internacionais: a Diretiva EU 2016/1148 [192], que requer que os Estados Membros que "os operadores de serviços essenciais tomem as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações" e adotem "medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços", não fixando controles de segurança específicos a serem adotados.

Isso posto, é razoável concluir que, muito embora os frameworks regulatórios setoriais aparentam maturidade adequada em segurança cibernética, a ausência de regulação dos aspectos mínimos de segurança da informação pela ANPD, resulta em um sensível gap regulatório em matéria de segurança cibernética, dado que a regulação atualmente aplicável a todos os agentes regulados, mormente o Decreto n° 8.771/2016, é sensivelmente limitado, falhando em apresentar a necessidade de adoção de controles de segurança básicos, notadamente controles administrativos. No entanto, considerando a mencionada qualidade das regulações setoriais, é importante que eventual regulação abrangente de aspectos de segurança cibernética, considere as regulações setoriais e como integrá-las de forma orgânica.

Fontes:
190. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776
191. Disponível em: https://www2.aneel.gov.br/cedoc/ren2021964.html
192. Disponível em: https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=pt

c) **Capacidade e capabilidade legal e regulatória:** trata-se da capacidade dos órgãos regulatórios, policiais, do Ministério Público e dos tribunais promoverem a aplicação dos padrões legais e regulatórios [193].

Em relação aos órgãos regulatórios, em que pese a existência e reconhecida capacidade de atuação de reguladores setoriais, como o próprio Banco Central, no momento, a principal reguladora em matéria atinente à segurança cibernética é a Autoridade Nacional de Proteção de Dados.

A ANPD não detém orçamento ou volume de profissionais suficiente para a adequada execução de suas atividades institucionais – possuindo um orçamento significativamente inferior àqueles das Autoridades de Dados de países com PIB bastante próximo ao brasileiro.

Em relação às forças policiais, embora a situação tenha melhorado significativamente no último ano, com a criação de delegacias especializadas no combate ao cibercrime em muitas das unidades federativas, subsistem dificuldades relevantes a serem enfrentadas.

Dentre essas dificuldades, destaca-se a necessidade de adequada estruturação dessas delegacias, considerada sua relativa juventude e a crescente demanda pela atuação destes profissionais especializados. Com efeito, no Distrito Federal, o volume de Peritos na Polícia Civil é deficitário para a demanda crescente pela análise de vestígios em aparelhos eletrônicos, que quase dobrou entre 2021 e 2022 [194]. Essa situação tende a ser refletida no Ministério Público ou, minimamente, em sua atuação, vez que intrinsicamente ligada a atuação das delegacias de política.

Igualmente, o Judiciário não aparenta encontrar-se adequadamente preparado ao combate a cibercriminalidade, com o Ministro Sebastião Reis Júnior, do Superior Tribunal de Justiça, tendo se manifestado pela necessidade de adaptação das cortes no país – com seu necessário aparelhamento técnico e material.

Tudo exposto, é clara a necessidade de melhor instrumentalizar os entes públicos responsáveis pela aplicação das leis e frameworks relacionados com segurança cibernética no país, destacando-se a atual situação precária da ANPD.

Fontes:
193. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2023/03/5077781-falta-de-pericia-em-aparelhos-eletronicos-atrasa-investigacoes-criminais-no-df.html
194. Disponível em: https://www.conjur.com.br/2022-jun-30/judiciario-nao-preparado-crimes-virtuais-opina-ministro/

d) Frameworks formais e informais de cooperação para o combate do cibercrime: refere-se a existência e funcionamento de mecanismos formais e informais de cooperação, nacional ou internacional [195].

Internacionalmente, conforme mencionado acima, o Brasil é membro da CSIRTAmericas e promulgou, em 2023, a Convenção de Budapeste, um dos maiores e mais abrangentes mecanismos existentes de cooperação internacional em matéria de crimes cibernéticos. No entanto, considerando a recente promulgação da convenção não é possível avaliar seu eficiente uso pelos tribunais nacionais, sobretudo tendo em vista que, em regra, processos penais tramitam em segredo de justiça, minimamente, em sua fase investigatória.

Internamente, podem ser visualizados alguns acordos de cooperação entre diferentes entes relevantes. A título de exemplo, em 2022 o Governo Federal lançou o primeiro **Plano Tático de Combate a Crimes Cibernéticos**, tendo enquanto enfoque o combate às fraudes bancárias. Este plano foi fruto de uma parceria entre a Polícia Federal e a Federação Brasileira de Bancos (Febraban), objetivando o compartilhamento de informações para o fomento de ações preventivas, incluindo a ideação da criação de um banco de dados de ocorrências, o qual poderá ser acessado pelas polícias judiciárias da União e dos estados, com o fim de permitir a replicação dos modelos de investigação e soluções adotados [196].

A ANPD, igualmente, realizou acordos de cooperação técnica com diversas entidades da administração pública, dentre os quais a Controladoria-Geral da União ("CGU") [197], o Tribunal Superior Eleitoral ("TSE") [198], o Núcleo de Informação e Coordenação do Ponto BR ("NIC.BR") [199], o Conselho Administrativo de Defesa Econômica ("CADE") [200] e a Secretária Nacional do Consumidor ("SENACON") [201]. Destas parcerias da ANPD, importantes materiais preventivos e educativos foram originados:

- Guias para Pessoas Físicas sobre como resguardar seus dados na *internet* [202] cuidados quando do vazamento de dados [203], ambos frutos da parceria com o NIC.BR
- Guia aos consumidores sobre as regras para o tratamento de dados pessoais, fruto da parceria com a SENACON [204].
- Guia orientativo sobre a aplicação da LGPD no contexto eleitoral [205], fruto da parceria com o TSE

Fontes:
195. Disponível em: https://acscc.ox.ac.uk/files/cmm2021editiondocpdf
196. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos
197. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-acordo-de-cooperacao-tecnica-com-a-cgu#:~:text=O%20acordo%20formaliza%20a%20converg%C3%AAncia,a%20LGPD%20s%C3%A3o%20leis%20complementares.
198. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-tse-assinam-acordo-de-cooperacao-tecnica
199. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-nic-br-assinam-acordo-de-cooperacao
200. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-na-proxima-quarta-feira-02-06
201. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica
202. Disponível em: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf
203. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf
204. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-como-proteger-seus-dados-pessoais.pdf
205. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

Existem, ainda que de forma pontual, outras ocorrências de parcerias internas relacionadas à segurança cibernética, por exemplo:

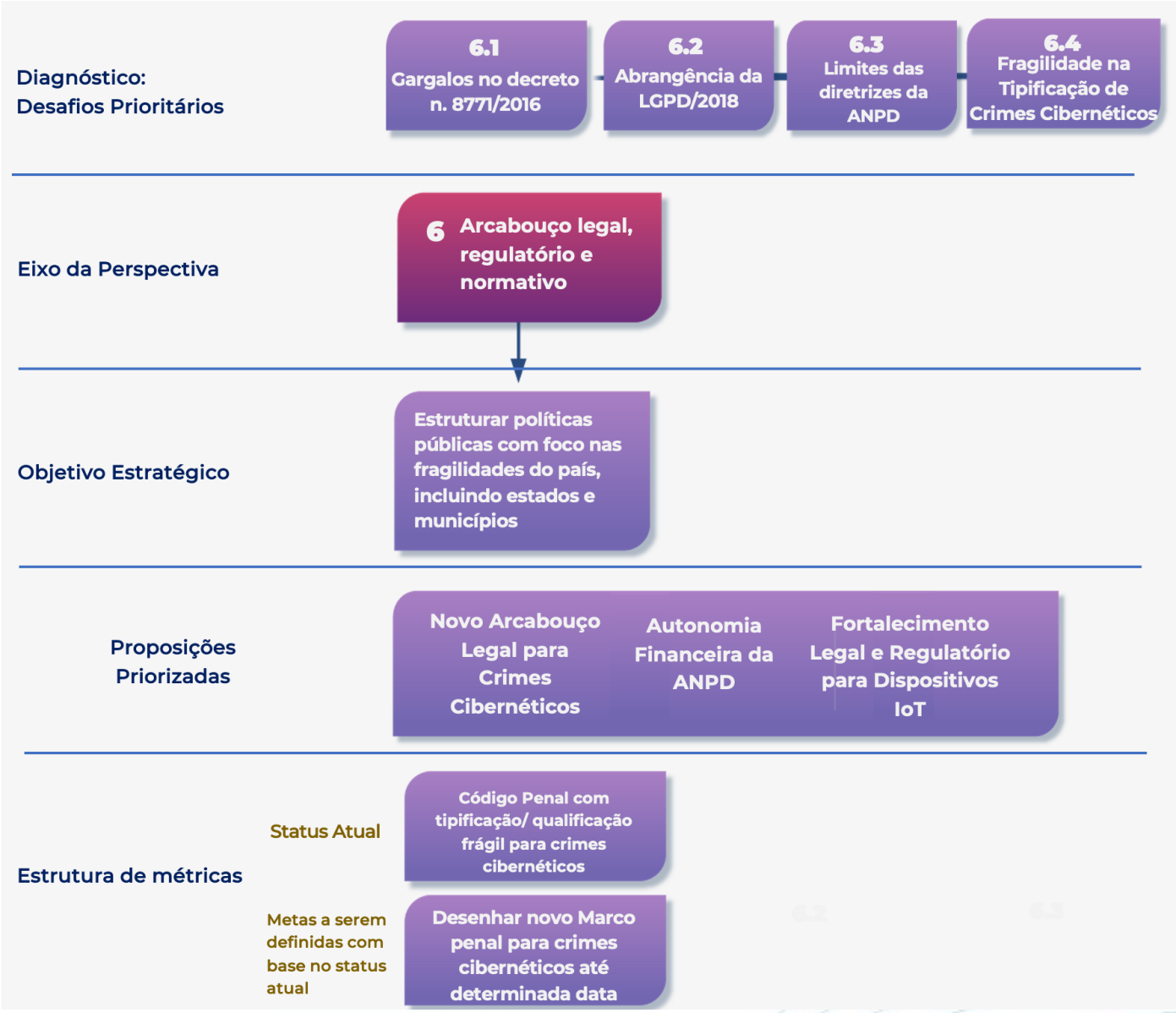
- Em 2019 o Ministério Público de São Paulo firmou acordo de cooperação com a Polícia Militar de São Paulo, com o objetivo de utilizar do serviço de inteligência policial para combate a cibercrime [206];
- Em 2014, o Governo Federal e a Universidade Federal do Espírito Santo firmaram parceria para mapear crimes virtuais, com enfoque em violações aos Direitos Humanos e das minorias [207];
- Em 2019, o Governo do Paraná firmou parceria com a Safernet com o objetivo de "fortalecer as ações da Força-Tarefa Infância Segura na prevenção e combate aos crimes cibernéticos"[3] [208]

Fontes:
206. Disponível em: https://www.terra.com.br/noticias/tecnologia/ministerio-publico-e-pm-fecham-parceria-para-combate-a-cibercrime,3e8afdb5a229f7fc74e92539a7ef9e5d0s3ffeq9.html
207. Disponível em: https://www.ufes.br/conteudo/governo-federal-e-ufes-firmam-parceria-para-mapear-crimes-virtuais
208. Disponível em: https://www.aen.pr.gov.br/Noticia/Governo-firma-parceria-para-prevencao-e-combate-cibercrimes

IV. Sugestões de Metas, Objetivo e Proposições Priorizadas

A seguir, a partir do contexto e desafios apresentados, tem-se a agregação das principais sugestões de caminhos estratégicos para evolução do Brasil neste Eixo:

Figura 10. Resumo dos desafios, objetivos e proposições priorizadas do Eixo estratégico 6



a. Recomendações para Construção das Metas:

Propor projeto de lei de revisão do código penal para permitir registro específico de crimes relacionados à cibersegurança, contribuindo para a construção de série de dados de interesse para o monitoramento.

I. Comitê Técnico e Processo de Priorização

No dia 27 de maio de 2024 foram reunidas no Comitê Técnico de modo presencial e simultaneamente online 13 integrantes com perfil multidisciplinar (Segurança Pública, Risco Cibernético, Cibersegurança, Políticas Públicas, Economia, Cooperação Internacional, *Advocacy*), para a realização da atividade de avaliação e priorização de propostas recebidas das entidades participantes para os seis Eixos Estratégicos, segundo os critérios **conteúdo estratégico** e **factibilidade de execução**.

A priorização foi realizada segundo a atribuição de notas 1 a 3 para cada proposta, em cada critério, por cada membro do Comitê Técnico. Vale pontuar que o Comitê Técnico realizou a discussão sobre cada proposição, com a prerrogativa de condensar ou sugerir novas, submetidas a nova votação posterior.

Figura 11. **Instituições consultadas para a formulação das propostas**

Imagem 1. **Reunião do Comitê Técnico para avaliação e priorização de propostas**

O resultado da priorização de propostas - com a atribuição de notas 1 a 3 para cada proposta, em cada critério, por cada membro do Comitê Técnico – pode ser observado nas matrizes a seguir:

Figura 12. Priorização do Eixo 1 – Conscientização da Sociedade

Figura 13. Priorização do Eixo 2 – Adequação do Capital Humano

Elaboração própria

Figura 14. **Priorização do Eixo 3 – Engajamento e Integração Multi-institucional**

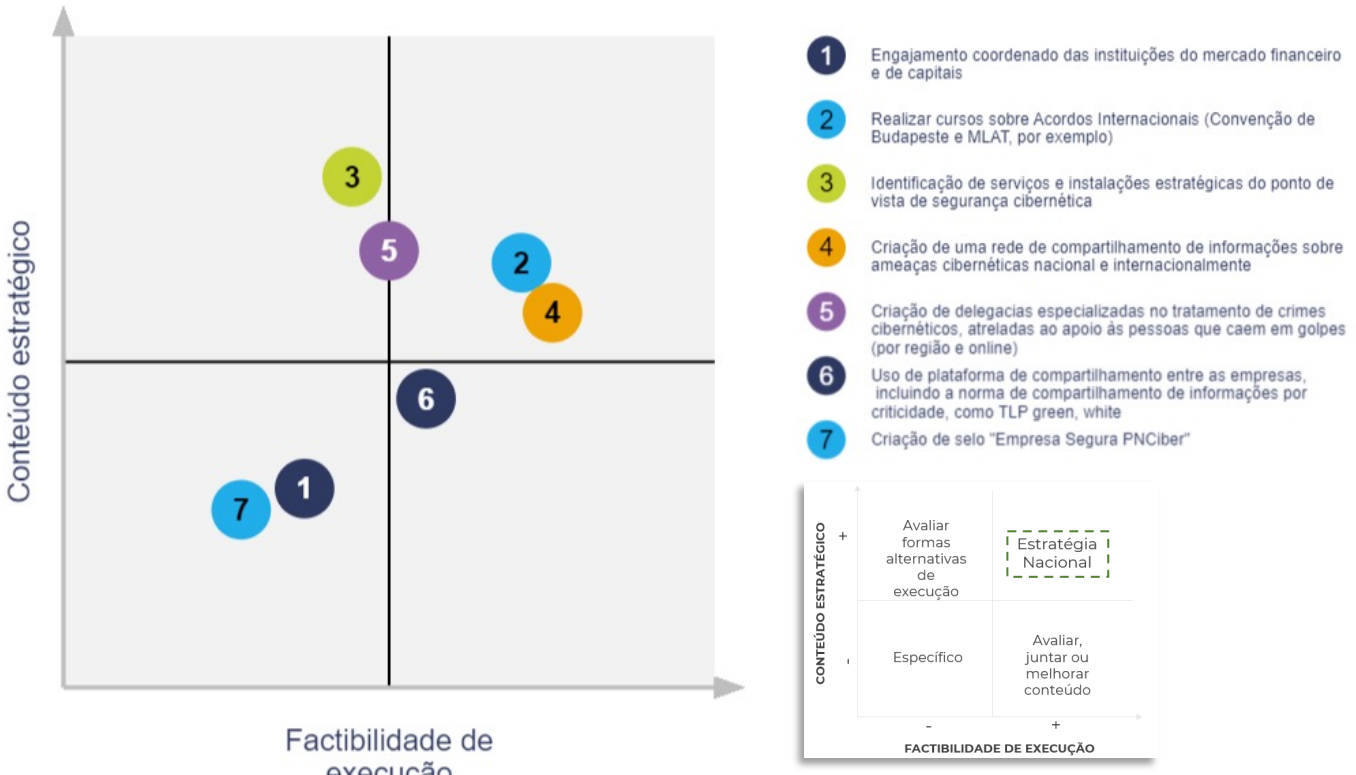


Figura 15. **Priorização do Eixo 4 – Informações e Conhecimento Especializado**

Elaboração própria

Figura 16. **Priorização do Eixo 5 – Financiamento e Incentivos**

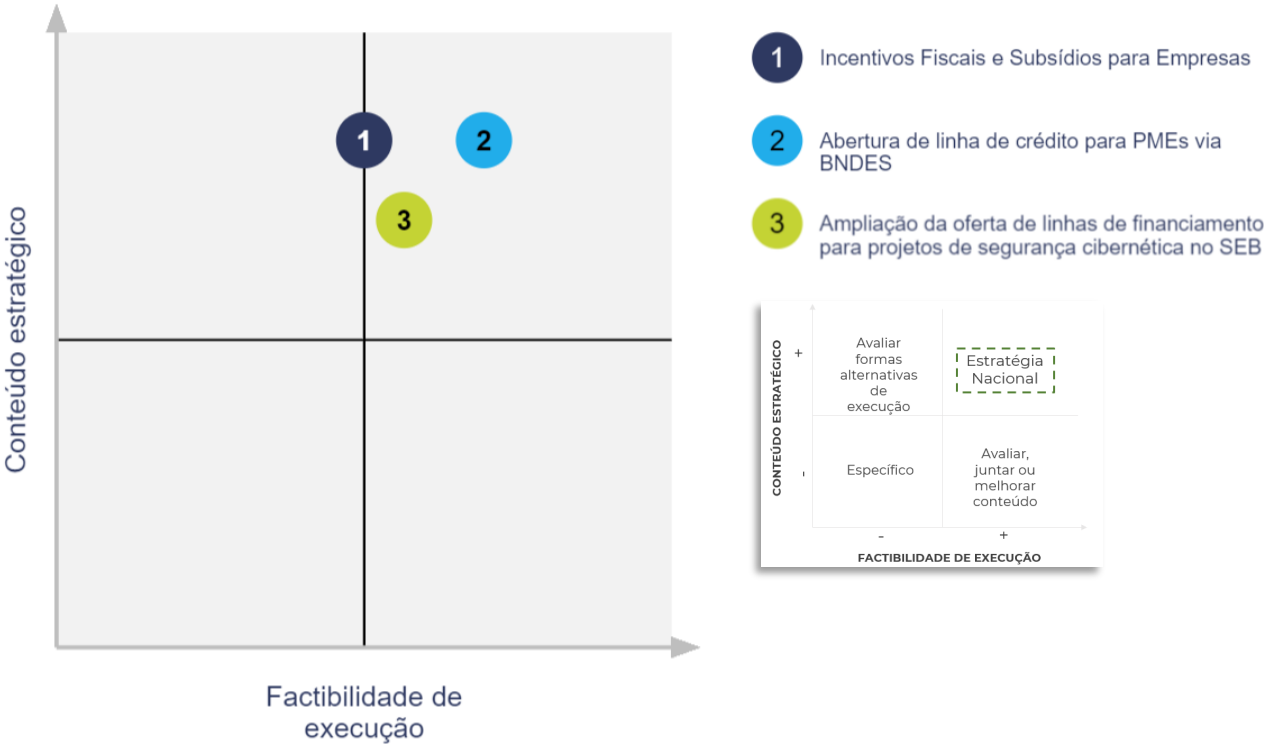
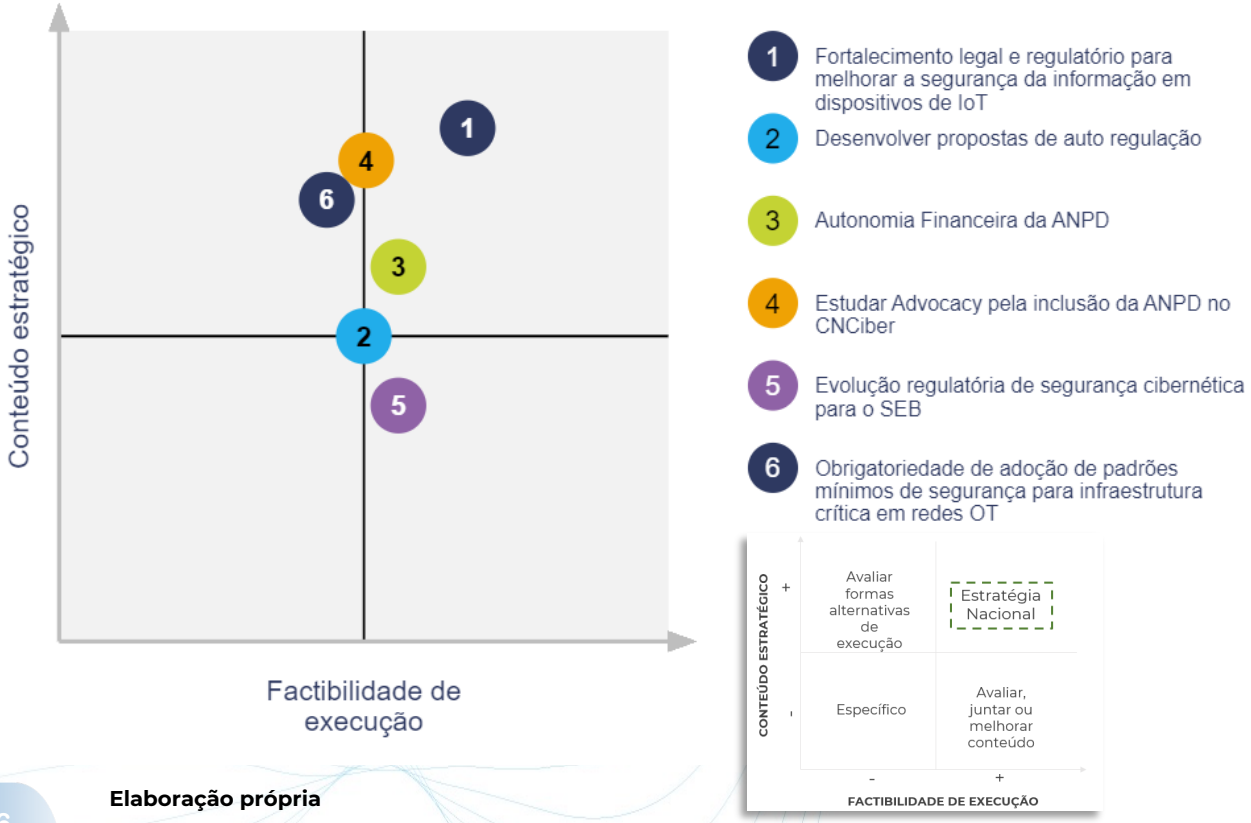
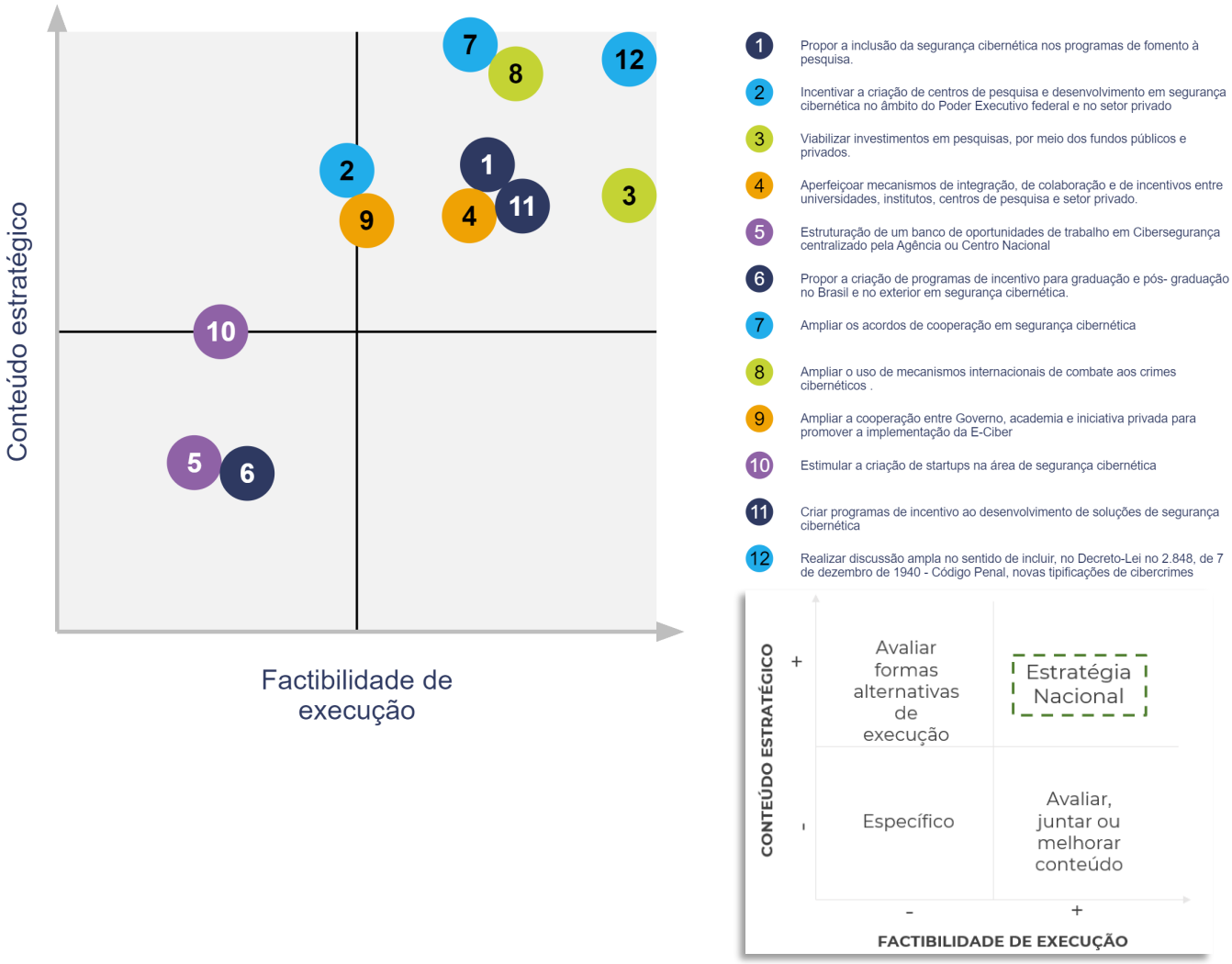


Figura 17. **Priorização do Eixo 6 – Arcabouço Legal, Regulatório e Normativo**



Elaboração própria

Figura 18. **Priorização de propostas adicionais**



PROPOSIÇÕES ADICIONAIS (Não Votadas pelo Comitê – recebidas em 04.06):

1. Inclusão de Discplinas de Segurança Cibernética nos cursos de formação técnica;
2. Construir indicadores Nacionais de Maturidade em Segurança Cibernética;
3. Criação de estatísticas nacionais de crimes cibernéticos;
4. Política Nacional de Compartilhamento de Incidentes;
5. Capacitação de Gestores Públicos em Segurança Cibernética;
6. Capacitação de Professores e Formadores em Segurança Cibernética.

7. Proposições Priorizadas

Durante reunião em conjunto com o comitê técnico, foi realizado o exercício de priorização das proposições, e os participantes tiveram a oportunidade de sugerir proposições adicionais.

Na tabela 4 a seguir foram identificadas até quatro proposições mais bem colocadas de cada um dos eixos para a seleção durante a reunião do comitê, além de quatro proposições adicionais, que passaram por uma nova votação e também são consideradas como prioritárias [209].

Tabela 7. Proposições Priorizadas pelo Comitê Técnico

EIXO	PROPOSIÇÃO
Eixo 1 Conscientização da sociedade	**Campanhas de Conscientização Pública com Foco em Mobile e Redes Sociais:** lançar recorrentemente campanhas de conscientização pública nacionais para educar os cidadãos sobre ameaças cibernéticas comuns (como *phishing* e *malware*), e promover boas práticas de segurança com foco em *mobile* e redes sociais.
	Investimento em Educação Obrigatória no Tema: inserir o tema no currículo básico e universitário, além de técnico e multissetorial (por exemplo, dentro das estruturas do mercado de capitais e certificações).
	Criação e Divulgação de "Biblioteca" de Conteúdos: divulgar conteúdos educativos com orientações aos cidadãos, empresas e governos (políticas, diretrizes e procedimentos voltados para cyber - aproveitar conteúdos NIC.br, e outras instituições que já possuem conteúdo sobre o tema).
Eixo 2 Adequação do capital humano	**Criação de Centros de Capacitação Especializados:** desenvolver centros de segurança cibernética específicos para áreas relacionadas à infraestrutura crítica, dada a sua criticidade social e econômica para o país.
	Estimulo à Talentos em Carreiras de Cibersegurança: estimular setor privado no investimento em permanência e crescimento de profissionais em carreiras de Cibersegurança.
	Reformulação dos Currículos dos Cursos de Tecnologia: garantir que Cibersegurança se torne uma matéria obrigatória nas formações da área de Tecnologia devido ao seu carácter social e econômico e ligação direta com a defesa e segurança nacional.
Eixo 3 Engajamento e integração multi-institucional	**Centro Nacional de Segurança Cibernética**: criar um centro ou agência que sirva como ponto central de conscientização, diretrizes, integração de atores e iniciativas de Cibersegurança.
	Realização de Cursos sobre Acordos Internacionais (Convenção de Budapeste e MLAT, por exemplo): buscar, em conjunto com o Conselho Federal da OAB, CNJ e CNMP, elaborar e implementar cursos para advogados, juízes, delegados e promotores sobre os mecanismos jurídicos internacionais de cooperação existentes.
	Criação Rede de Compartilhamento de Ameaças: coletar e divulgar de forma centralizada e segura informações sobre ameaças cibernéticas nacional e internacionalmente (os TTPs: Técnica, Táticas e Procedimentos, e os IoCs: *Indicators of Compromise*), apoiando na prevenção, solução e proteção do mercado contra ameaças.
	Ampliação das Delegacias Especializadas em Crimes Cibernéticos: ampliar as DCCibers com atuação integrada por região e atendimento virtual, além disso, garantir que haja um representante por estado e município ligado ao Centro Nacional de Cibersegurança e Ministério da Defesa/PF para integração de dados e desdobramento das políticas e ações nacionais.

209. Vale destacar que após a reunião, houve uma realocação das proposições priorizadas a fim de melhor abarcar os eixos correspondentes.

Tabela 7. (Continuação) Proposições Priorizadas pelo Comitê Técnico

EIXO	PROPOSIÇÃO
Eixo 4 Informações e conhecimento especializado	**Padrões de Segurança Cibernética**: desenvolver e implementar de padrões de segurança cibernética obrigatórios para setores críticos, como energia, saúde, finanças e transporte, de modo a garantir maior resiliência em níveis padronizados no mercado.
	Plataforma Nacional para Reporte *de Phishing* (E-mail/ WhatsApp), *Smishing* (SMS) e *Vishing* (voice): criar uma plataforma única (aplicativo mobile) em colaboração com órgãos reguladores (por exemplo: ANPD, ANATEL, BCB e iniciativa privada) a fim de que o usuário possa reportar e-mails, números de celulares; telefones "ofensores" e garantir agilidade nos bloqueios.
	Desenvolvimento da Capacidade de Resposta a Incidente: investir na criação e no fortalecimento de equipes de resposta a incidentes cibernéticos em todo o país, com treinamento adequado, protocolos de resposta claros e exercícios regulares de simulação para testar a prontidão e eficácia da resposta.
Eixo 5 Financiamento e incentivos	**Linha de Crédito para PMEs via BNDES:** estimular a abertura de linhas de crédito especiais voltadas ao investimento por PMEs em Segurança Cibernética, de modo a garantir amplo acesso à ferramentas e redução da vulnerabilidade cibernética deste grupo de empresas.
	Incentivos Fiscais e/ou Subsídios para Empresas: oferecer incentivos fiscais e/ou subsídios para empresas que investem em medidas de segurança cibernética, como a aquisição de tecnologias de segurança, treinamento de funcionários e implementação de melhores práticas de segurança.
	Linhas de Financiamento para Projetos de Segurança Cibernética no SEB (Sistema Educacional Brasileiro): ampliar as linhas de financiamento (BNDES, FINEP, Banco Mundial, P&D ANEEL, entre outros) para desenvolvimento de projetos de P&D e de implantação de soluções de cibersegurança, garantindo a possibilidade de uso tanto pela iniciativa privada quanto por instituições estatais e paraestatais.
	Fundo para Combate ao Crime Cibernético: estruturar um fundo Estadual, alinhado com a legislação Federal, para destinação de percentual de valores recuperados de lavagem de dinheiro e demais proventos do crime para o fomento ao combate do crime (especialmente, organizado e cibercrime).
Eixo 6 Arcabouço legal, regulatório e normativo	**Novo Arcabouço Legal para Cibercrimes:** realizar discussão ampla no sentido de incluir, no Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, novas tipificações de cibercrimes que compreendam as práticas atuais e aumentem o custo dos crimes digitais para os criminosos.
	Fortalecimento Legal e Regulatório para Dispositivos IoT: os padrões inadequados de proteção aos dispositivos torna-os passíveis de abusos por um ator de conhecimento maior na área de tecnologia. É importante ter regras e padrões que sejam seguidos antes desses dispositivos serem consumidos pelo público e melhorar a segurança da informação.
	Autonomia Financeira da ANPD: a ANPD é um das autoridades com maior relevância neste ecossistema no país e garantir sua autonomia financeira é prerrogativa para institucionalidade e segurança jurídica nacional e internacionalmente (nos termos do PL nº 615/2024).

A **tabela completa das proposições sugeridas e priorizadas** foi disponibilizada ao GSI como parte integrante deste relatório, bem como o conjunto de **sugestões realizadas pela Divisão de Crimes Cibernéticos (DCCiber) do Departamento Estadual de Investigações Criminais - Polícia Civil do Estado de São Paulo.**

209. Vale destacar que após a reunião, houve uma realocação das proposições priorizadas a fim de melhor abarcar os eixos correspondentes.

7. Conclusão

Por todo o exposto no decorrer deste levantamento, não restam dúvidas sobre as inúmeras **oportunidades e necessidades de adequação das estruturas das diversas entidades que compõem o Estado brasileiro** para a efetiva prevenção, combate à criminalidade cibernética e construção de um ecossistema ativo na formação da cultura nacional de proteção no espaço digital.

Apesar do relativo preparo dos agentes públicos e ações privadas em torno do tema, é evidente que a população brasileira carece de **medidas mais efetivas de conscientização e capacitação sobre os riscos e ações de prevenção**. Isso é reforçado também pelo fato de as **micro, pequenas e médias empresas serem diretamente e frequentemente afetadas por incidentes de segurança**, ao mesmo tempo que possuem estruturas de tecnologia deficitárias perante os riscos existentes e necessitam de incentivos para elevar suas capacidades.

Além disso, para que haja um **aumento no custo do crime cibernético e redução dos incentivos existentes a esta modalidade de ação criminosa**, é imperativo que haja um debate profundo no âmbito do Código Penal brasileiro, criando tipificações e qualificações com penas compatíveis aos tipos de crime e sua respectiva gravidade para a sociedade brasileira.

Um dos pontos centrais para o avanço dos pontos destacados nesta iniciativa, **é a prioridade de investimentos por parte do Estado e um coordenação institucional centralizada** por meio da aprovação de uma nova Estratégia Nacional que consolide prioridades, garanta eficácia às ações de segurança cibernética e principalmente, **impulsione a criação de políticas de estado** capazes de conscientizar, conduzir e integrar diferentes atores e iniciativas.

A eficácia desta construção dependerá **do engajamento de todas as partes da sociedade interessadas**, incluindo o governo, o setor privado e a sociedade civil. Esperamos que o **movimento ocasionado pela presente iniciativa sirva como mola propulsora** para o atingimento destes objetivos e que os dados e sugestões contidas neste documento contribuíam profundamente para o aumento da resiliência cibernética brasileira nos próximos anos.

Seguimos unidos por um ambiente digital mais seguro para todos!

INSTITUTO NACIONAL DE
COMBATE AO CIBERCRIME

JUNTOS POR UM AMBIENTE DIGITAL MAIS SEGURO PARA TODOS

FEBRABAN Federação Brasileira de Bancos

FIESP

Acrefi

MBC Movimento Brasil Competitivo

abrasca

CNF

FECOMERCIOSP

ONS Operador Nacional do Sistema Elétrico

ABES

Federal Bureau of Investigation

Polícia Civil SP — Departamento Estadual de Investigações Criminais DEIC — Divisão de Crimes Cibernéticos

APOIO TÉCNICO:

MacroPlan Consultoria e Analytics

VLK Direito, Inovação & Tecnologia

incc.org.br

INCC
INSTITUTO NACIONAL DE COMBATE
AO CRIME CIBERNÉTICO

JUNTOS POR UM AMBIENTE DIGITAL MAIS SEGURO PARA TODOS