INSTITUTO IGARAPÉ
a think and do tank

MAPEAMENTO DE RISCOS DIGITAIS:

UMA AGENDA MULTISSETORIAL PARA A SEGURANÇA DIGITAL NO BRASIL

ABRIL 2021

Índice

MAPEAMENTO DE RISCOS DIGITAIS:

UMA AGENDA MULTISSETORIAL PARA A SEGURANÇA DIGITAL NO BRASIL

INTRODUÇÃO[1]

Ao longo das últimas duas décadas, o Brasil se tornou cada vez mais digitalmente conectado. Embora haja um longo caminho para democratizar o acesso à Internet, atualmente cerca de 70% da população brasileira está conectada. A Covid-19 acelerou o processo de digitalização no país, que deixou de ser uma tendência para se tornar uma necessidade. As medidas adotadas para reduzir o contágio, como o distanciamento social, o lockdown e o isolamento, evidenciaram ainda mais a importância e centralidade da Internet para a sociedade e economia. Diversas organizações, por exemplo, transferiram suas operações para o ambiente on-line, adotando regimes de home office. Além disso, mais pessoas utilizaram a Internet para se distrair, comprar, acessar serviços e manter contato com familiares e amigos.

Nesse contexto de expansão do acesso e de dependência cada vez maior da Internet, o desafio da segurança digital se tornou urgente. Cidades dependem mais do que nunca de redes estáveis para manterem suas atividades rotineiras. Conforme indivíduos e instituições transferem novas partes de suas vidas para o ambiente digital, terminam mais expostos e vulneráveis às ameaças digitais. Tanto o setor público quanto o privado e organizações da sociedade civil precisam se preparar para identificar e desenhar estratégias para o fortalecimento da segurança e resiliência do ecossistema digital.

Apesar de todos os setores enfrentarem os riscos associados à digitalização, a agenda de segurança digital nacional é extremamente fragmentada. Cada setor experimenta as ameaças de uma maneira e possui diferentes entendimentos sobre riscos prioritários e compartilhados, assim como sobre terminologias (“segurança da informação”, “segurança digital”, “cibersegurança” e “segurança de dados”, por exemplo). Embora todos os setores venham desenvolvendo esforços para melhorar o ambiente digital, a evidente interdependência da sociedade e de setores nesse espaço aumenta o potencial do impacto transversal desses riscos.

1 A equipe do Programa de Segurança Digital do Instituto Igarapé gostaria de agradecer e reconhecer a colaboração de: Gustavo Kruel, Vanessa Copetti Cravo, Marcelo Lintomen, Nathalia Sautchuk, Sabrina Medeiros, Vinícius Mariano, Virgilio Almeida e Fabio Assolini, assim como dos respondentes do nosso questionário de riscos digitais (realizado em fevereiro e março de 2021), entre outros especialistas que tornaram o desenvolvimento deste documento possível.

Em consequência disso, é impossível pensar a garantia e a manutenção da segurança digital sem a atuação conjunta e coordenada de todos os atores relevantes: governos, empresas, sociedade civil, academia e comunidade técnica. Essa cooperação permite a criação de processos sistêmicos com impactos coordenados e transversais, envolvendo o amplo espectro de atividades sociais e econômicas que hoje dependem do ambiente digital.

Este documento é resultado desse diagnóstico: interdependência dos setores, responsabilidade compartilhada e a necessidade de se pensar uma agenda comum para a segurança digital no Brasil. Compreendemos que, para avançarmos no desenvolvimento dessa agenda com ações mais efetivas, sustentáveis e duradouras para a segurança digital, é necessário criar um espaço de integração de conhecimentos, visões e práticas sobre riscos. É por isso que, ao longo de 2020, trabalhamos continuamente com especialistas de diferentes setores para compreender a ampla gama de ativos que precisam ser protegidos, bem como elaborar um mapa de riscos digitais e estratégias de mitigação que pudesse auxiliar no processo de construção de uma visão ampliada sobre segurança digital no Brasil.

Embora ainda haja um longo caminho para promover mudanças estruturais, conciliando agendas e entendimentos sobre segurança digital, este documento é o primeiro passo para uma ação coletiva. Esperamos que ele possa inspirar novas iniciativas que desdobrem e aprofundem o enquadramento aqui proposto.

CONSTRUINDO UMA VISÃO INTEGRAL PARA A SEGURANÇA DIGITAL

O aumento de notícias relacionadas a vazamentos de dados, ataques ou campanhas de desinformação, apesar de importantes para deixar desafios da segurança digital mais evidentes para a população, refletem de forma fragmentada e pontual as múltiplas dimensões de riscos digitais que continuamente impactam a economia, a sociedade e a política no Brasil.[2] Neste documento, riscos digitais são uma categoria de risco relacionada ao uso, desenvolvimento e/ou gestão do ambiente digital na condução de quaisquer atividades.[3]

Por mais que determinadas entidades sejam capazes de identificar seus próprios riscos, elas desconhecem aqueles compartilhados com outros setores. As demandas e pressões imediatas para se reagir a riscos dentro de organizações resultam em respostas e experiências estritamente setoriais para desafios que transcendem a esfera organizacional. Outros atores carecem de recursos e/ou capacidades para identificar e responder às ameaças, como, por exemplo, organizações da sociedade civil e entes do setor privado que tiveram que se digitalizar rapidamente para atender a um contexto de serviços virtuais por causa da pandemia.

É fundamental aliar respostas intra-

2 Exemplos de notícias recentes disponíveis em: TECNOBLOG. Antivírus e Segurança. Vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acesso em: mar. 2021. G1. Política. STJ diz que sistema de informática do tribunal foi alvo de ataque hacker e pede investigação da PF. Disponível em: https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml. Acesso em: mar. 2021. CORREIO BRASILIENSE. Hackers. Investigação aponta que ataque cibernético ao TSE vazou dados recentes. Disponível em: https://www.correiobraziliense.com.br/politica/2020/11/4890026-investigacao-aponta-que-ataque-cibernetico-ao-tse-vazou-dados-recentes.html. Acesso em: mar. 2021.

3 Baseado no relatório “Digital Security Risk Management for Economic and Social Prosperity” (2015), da OCDE. Disponível em: https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf.

organizacionais às estratégias de combate e identificação de riscos que sejam interorganizacionais. E, ainda, considerar um panorama mais amplo de experiências e expertise multissetorial para construir ações coordenadas, estabelecer canais (formais e informais) de cooperação e compartilhamento de informações e construir confiança entre setores.

Buscando endereçar o problema da fragmentação da agenda nacional de segurança digital, construímos colaborativamente, por meio de reuniões multissetoriais e aplicação de um questionário com especialistas em segurança digital, (1) um mapa com os ativos a serem protegidos e os riscos que mais afetam cada um deles; (2) uma tipologia para analisar os principais riscos digitais; e (3) as estratégias para a mitigação desses riscos. O processo envolveu a harmonização do vocabulário e alinhamento de conceitos para abordar os diferentes desafios associados à segurança digital, levando em conta as especificidades de cada setor, bem como a transversalidade dos riscos.

Este documento apresenta a consolidação desse trabalho culminando com uma agenda de mitigação de riscos digitais com foco nos cinco maiores riscos comuns a todos os setores. As estratégias apontadas aqui sugerem a atuação de diferentes setores, reforçando a necessidade de ações coletivas.

O QUE PROTEGER?

Para a elaboração desta agenda, iniciamos com a identificação de **seis eixos prioritários para a proteção digital**. Os eixos refletem, para além das infraestruturas e sistemas de comunicação e informação (ativos diretamente relacionados a tecnologias), a centralidade de ativos como direitos, processos e pessoas para a compreensão e mapeamento de ameaças, vulnerabilidades e riscos digitais. Tal integração é fundamental para uma visão de segurança digital nacional que inclua o indivíduo como parte central do desenho e implementação de estratégias de mitigação. Essa visão expande o escopo de definições nacionais de "segurança cibernética" e introduz novas dimensões sobre "o que" e "como" algo deve ser protegido em um contexto de alta digitalização, interconectividade e crescentes vulnerabilidades.

Figura 1: Ativos da Segurança Digital no Brasil

Tabela 1: Definições dos Ativos

	DADOS	SISTEMAS	INFRAESTRUTURA
Definição dos Ativos	Grupo de ativos que se refere às unidades nas quais informações e conhecimentos são criados. Dados possibilitam a representação do mundo por meio de unidades como números, caracteres, símbolos, imagens, bits, entre outros.[4] Neste caso, incluem categorias como dados pessoais, sensíveis e, sigilosos,[5] bem como dados relacionados ao pleno funcionamento de qualquer organização.	A coleção de componentes computacionais e/ou comunicacionais que apoiam mais de um objetivo de uma organização, grupo ou Estado.[6]	Categoria mais geral que engloba tanto infraestruturas críticas, quanto infraestruturas críticas da informação.[7] Inclui áreas prioritárias como: Energia, Águas, Telecomunicações, Transporte, Biossegurança e Bioproteção.

	DIREITOS	PROCESSOS	PESSOAS
Definição dos Ativos	Categoria de ativos que inclui direitos fundamentais e humanos como a liberdade de expressão, reputação e imagem. Introduz a perspectiva intangível dos ativos da governança da segurança digital.	As práticas associadas com a garantia da confidencialidade, integridade e disponibilidade das atividades de uma organização, grupo ou ente público.	Ativo associado ao comprometimento físico e à ameaça à integridade da vida de indivíduos a partir dos riscos associados a ferramentas tecnológicas e/ou digitais, como o comprometimento de um elevador ou hospital.

O crescimento da digitalização não só proporciona o desenvolvimento de novos horizontes para o fornecimento de serviços, informações e oportunidades, como também consolida a presença dessas tecnologias como uma camada cada vez mais fundamental para a sociedade,

4 Kitchin, R. The Data Revolution. SAGE Publications, 2014, p.3.

5 Ver definições para “dados pessoais” e “dados pessoais sensíveis” na Lei Geral de Proteção de Dados (Lei 13.709 de 2018), em seu art. 5º, incisos I e II; para “informação sigilosa” na Lei de Acesso à Informação (Lei 12.527 de 2011), em seu art. 4º, inciso III. Disponíveis em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

6 Tradução adaptada da NIST SP 800-16/1998.

7 Vale notar que não existe um consenso global sobre o entendimento de infraestruturas. Contudo, dentro do contexto brasileiro, o Glossário da Segurança da Informação, por exemplo, inclui três componentes associados ao ativo: infraestruturas cibernética, infraestrutura crítica e infraestrutura crítica de informação, conforme descrito abaixo: INFRAESTRUTURA CIBERNÉTICA - “Sistemas e serviços de informação e comunicações compostos por todo o hardware e software necessários para processar, armazenar e transmitir a informação, ou qualquer combinação desses elementos. O processamento inclui a criação, acesso, modificação e destruição da informação. O armazenamento engloba qualquer tipo de mídia na qual a informação esteja armazenada. A transmissão é composta tanto pela distribuição como pelo compartilhamento da informação, por qualquer meio”; INFRAESTRUTURA CRÍTICA - “Instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança”; INFRAESTRUTURA CRÍTICA DE INFORMAÇÃO – “Sistemas de TIC que suportam ativos e serviços chaves da Infraestrutura Nacional Crítica.”

a economia e a política. Porém, metodologias de análise de risco, em especial aquelas que estão associadas a aos riscos digitais e à cibersegurança, permanecem focadas no ambiente intraorganizacional.[8]

Faz-se necessário expandir as metodologias e as abordagens de risco para que incorporem e reflitam a centralidade das pessoas, processos e direitos como elementos fundamentais de uma ação de mitigação, identificação e planejamento coletivo e duradouro para proteger esses riscos. Esse trabalho passa pelo estabelecimento de processos conjuntos de mapeamento de riscos, expansão das fontes de metodologias, desenvolvimento de espaços de colaboração e diálogo para mitigação de riscos específicos.

Em conjunto, esses e outros esforços calcados na proteção dos ativos acima (Figura 1) podem contribuir para maior resiliência na sociedade, na medida em que permitem a construção de uma visão holística sobre a segurança digital. E, assim, favorecem a compreensão sobre transversalidade do tema, incentivando a tomada de ações coletivas.

O PANORAMA DE RISCOS

A partir dos grupos de ativos apresentados, identificamos os 10 principais riscos para a segurança digital no Brasil,[9] descritos na Tabela 2. Esses riscos foram incorporados em um questionário enviado a profissionais de segurança digital de diferentes setores, pedindo para que indicassem quais dos riscos tinham maior impacto em seus setores.

Tabela 2: Definições dos Riscos à Proteção e Segurança Digital

	Ausência/ Inadequação de Marcos Regulatórios	Ausência de Protocolos	Cibercrimes	Desinformação e Manipulação	Ameaça à Infraestrutura Crítica
Descrição do Risco	Ausência de marco legal (ambiente legal) adequado para proteção de dados, sistemas, infraestruturas e indivíduos e/ ou a existência de uma lei que possa prejudicar a proteção de direitos.	Ausência de protocolos de compartilhamento de informações, de responsabilização integral sobre processos de integração (muitas vezes, os protocolos de responsabilização se concentram apenas em componentes individuais dos processos ou em serviços independentes); ausência de planos de resposta à incidentes que levem em consideração os danos diretos e indiretos que podem afetar a integridade física, psicológica e patrimonial de indivíduos; má configuração de sistemas.	Atos criminosos, praticados com o uso de um ou mais computadores, que podem violar direitos de personalidade - como crimes contra a honra e discriminação - representar a prática de pedofilia e exploração infantil e realizar roubo de credenciais, assim como o acesso indevido a outros tipos de dados.	Disseminação de informação falsa, ou a manipulação de pessoas por meio do uso de informação, que podem vir a afetar a integridade física, psicológica e patrimonial de indivíduos, tais como a manipulação de "sentimentos" por meio de ferramentas de inteligência artificial e a desinformação sobre questões relacionadas à saúde, ou de outras tecnologias de informação e comunicação e seus algoritmos.	Quedas de fornecimento de energia e outros serviços essenciais; Falha no controle de temperatura; Falha no controle de umidade; Manutenção inadequada; Falta de pessoal; Falhas no controle de descarte de material; Ataques cibernéticos.

8 Baseado no artigo "Cyber risk measurement and the holistic cybersecurity approach" (BOEHM; MERRATH, POPPENSIEKER; RIEMENSCHNITTER; STÄHLE, 2018). Disponível em: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cyber%20risk%20measurement%20and%20the%20holistic%20cybersecurity%20approach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf.

9 Ver Anexo 1 para acessar a lista extensa de vulnerabilidades e ameaças que informaram os 10 riscos incluídos no questionário amplamente compartilhado com profissionais do campo.

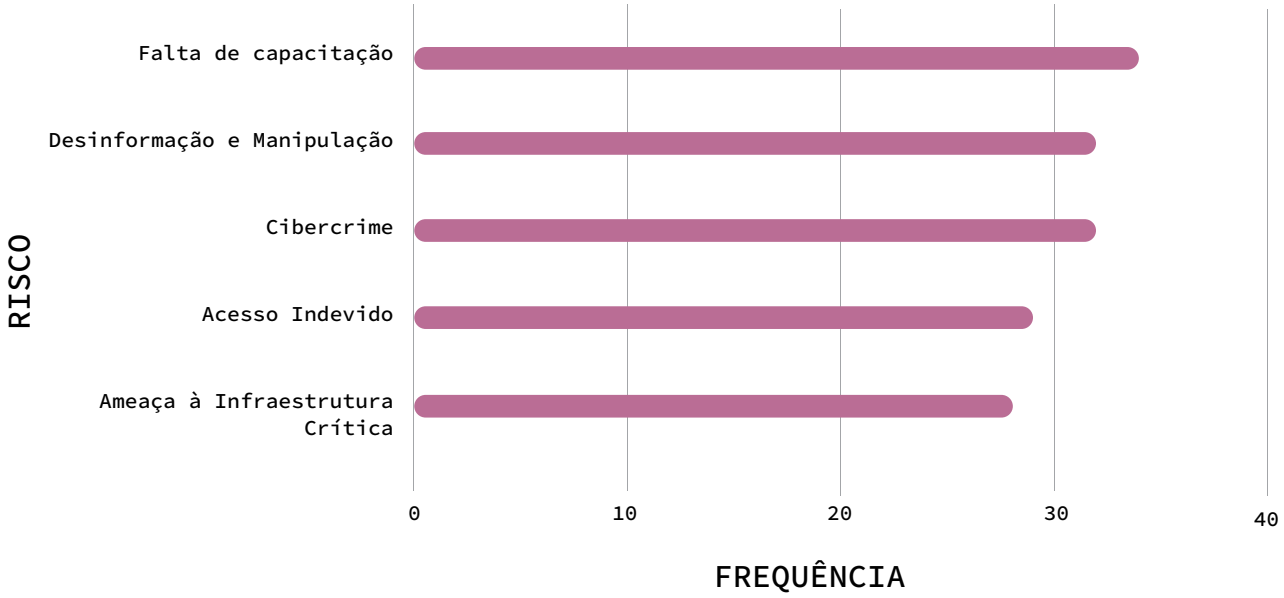
continuação Tabela 2

	Acesso Indevido	Ameaças Ambientais	Ameaças ao Direito de Propriedade Imaterial	Ameaças a Direitos Humanos	Falta de Capacitação
Descrição do Risco	Acesso indevido a sistemas de informação, obtidos por meio de engenharia social ou roubo de credenciais, que pode prejudicar os processos de interação entre os diferentes componentes de um determinado sistema ou organização.	Fenômenos naturais, que afetam o ambiente e podem afetar a disponibilidade e integridade dos sistemas, tais como: condições climáticas desfavoráveis, alagamentos, enchentes, tempestades e raios e interferências eletromagnéticas.	Ações perpetradas por grupos, indivíduos ou organizações com o intuito de prejudicar a imagem e/ou a reputação de uma organização, ou violar algum bem imaterial como segredo industrial ou patente.	Ações que podem prejudicar o exercício de direitos humanos e fundamentais (como liberdade de expressão e de imprensa, privacidade e proteção de dados), através de meios tecnológicos (de vigilantismo, por exemplo) por agentes de Estado, governos não democráticos e/ou autocráticos, ou devido a práticas do setor privado (desde desafios relacionado à adequação com legislações até práticas de coleta massiva de dados de forma indevida).	Ausência de conhecimento de práticas básicas de proteção de dados em sistemas de informática na sociedade como um todo, ausência de capacitação técnica de pessoal encarregado de determinada infraestrutura; falta de clareza sobre responsabilidades e competências para garantir a proteção do sistema/infraestrutura/banco de dados, processos não planejados ou mal planejados (desenhados de forma muito simplificada ou excessivamente complexa); processos não implementados (apesar de planejados) ou mal implementados; ausência de políticas e protocolos para o tratamento de dados e proteção de sistemas; falta de integração institucional; falta de capacitação sobre novas tecnologias de informação e comunicação.

Usando o critério de **frequência**,[10] definimos os cinco maiores riscos digitais no Brasil (Gráfico 1): a falta de capacitação, com o maior número de respondentes (34), seguida de desinformação e manipulação (32 respondentes) e cibercrime (32), acesso indevido (29) e, por fim, ameaça à infraestrutura crítica (28).

10 O "Questionário sobre Riscos Digitais no Brasil " foi dividido em quatro grande etapas: na primeira, os respondentes informaram seu setor de atuação, gênero e cargo. Na segunda parte, eles indicaram quais dos dez riscos apresentados por nossa equipe seriam os cinco de maior impacto em seu setor. Em uma terceira etapa, os respondentes informaram sobre o horizonte temporal de ocorrência para cada risco, sendo pedido para que eles os categorizassem entre curto (0 a 2 anos), médio (3 a 5 anos) e longo prazo (5 a 10 anos). Por fim, os participantes indicaram quais estratégias de mitigação seus setores adotam para cada risco apresentado. O gráfico "Cinco maiores riscos digitais no Brasil" foi gerado a partir das respostas da segunda parte do questionário, em que cada respondente indicou os cinco riscos mais graves em sua perspectiva. Uma vez que o questionário obteve 45 respostas válidas, logo se alcançou um universo de 225 respostas sobre riscos entendidos como prioritários. Desse universo, os cinco mais frequentes deram origem ao gráfico, uma vez entendidos como os riscos digitais de maior proporção, comum a todos os setores/participantes da pesquisa. O critério de frequência se refere, dessa forma, à quantidade de vezes que o termo apareceu nas respostas dos participantes.

Gráfico 1: Cinco Maiores Riscos Digitais no Brasil

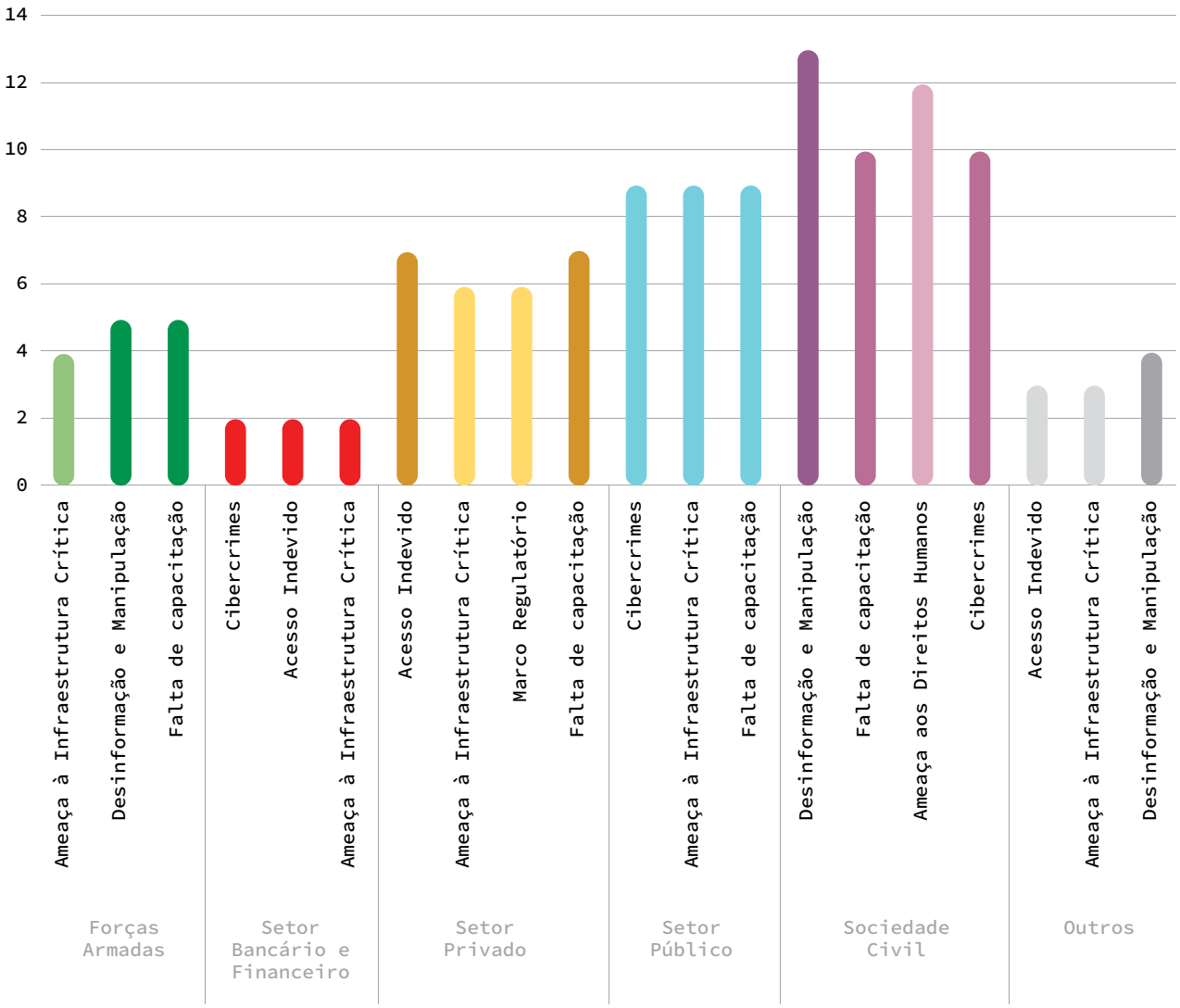


Os riscos geram diferentes impactos, a depender do que cada setor compreende como prioridade em cibersegurança. No gráfico abaixo é possível perceber quais são os três principais riscos para cada setor participante da pesquisa.[11] Falta de capacitação e ameaça à infraestrutura crítica permeiam quase todas as respostas, sendo assim uma preocupação compartilhada. Para a sociedade civil, a maior ameaça está relacionada a processos de desinformação e manipulação. O setor público entende que cibercrimes, ameaça à infraestrutura crítica e falta de capacitação são riscos de igual relevância, sendo que o mesmo cenário se espelha para setor financeiro e bancário em relação a cibercrimes, acesso indevido e ameaça à infraestrutura crítica. Diferente de outros setores, a ausência e/ou inadequação de marco regulatório desponta como uma das preocupações para o setor privado.[12]

11 O gráfico "Três Maiores Riscos Digitais no Brasil por Setor" foi gerado a partir das respostas da segunda parte do questionário, em que os respondentes informaram quais eram os cinco maiores riscos digitais a partir da sua perspectiva de atuação. Os três riscos mais frequentes entre essas respostas foram entendidos como de maior impacto nos respectivos setores, uma vez que foram consideradas todas as cinco possibilidades indicadas por cada respondente. A distribuição setorial das respostas do questionário como um todo está presente na seção "Resumo das Respostas".

12 Para setor privado e sociedade civil, o ranking dos terceiros maiores riscos ficam empatados entre duas diferentes categorias, entendendo que esses setores as consideram de igual relevância. Para o setor privado, "acesso indevido" e "falta de capacitação" estão presentes em sete das respostas, e "marco regulatório" e "ameaça à infraestrutura crítica" estão igualmente representadas em seis. Já para a sociedade civil o ranking foi: "desinformação e manipulação", com 13 respostas, "ameaça aos direitos humanos", com 12, "falta de capacitação" e "cibercrimes", igualmente com dez respostas computadas.

Gráfico 2: Três Maiores Riscos Digitais no Brasil



A PRÓXIMA DÉCADA DE RISCOS DIGITAIS

Gráfico 3: Percepção dos Respondentes sobre Horizonte Temporal de Riscos Digitais no Brasil

Em outra parte do questionário, foi perguntado aos respondentes qual a percepção deles sobre o horizonte temporal para a ocorrência dos riscos apresentados.[13] **Curto prazo** seriam aqueles riscos passíveis de ocorrer de **0 a 2 anos, médio prazo,** de **3 a 5 anos,** e **longo prazo,** de **5 a 10 anos**. Todos os cinco **principais riscos: falta de capacitação, desinformação e manipulação, cibercrime, acesso indevido e ameaça à infraestrutura crítica foram entendidos como riscos passíveis de ocorrer no curto prazo**, indicando a urgência para se implementar estratégias de mitigação eficiente no seu combate. No **médio prazo**, destacam-se tanto desafios relacionados à adequação, insuficiência ou ao surgimento de **marcos regulatórios**, bem como preocupações com **ausência de protocolos**. Um dos únicos riscos enquadrados no espectro de **longo prazo são os de ameaça ambientais**.

Compreendemos que este é um esforço inicial de mapeamento de riscos que precisa ser reiterado, expandido e levado adiante em novos esforços de colaboração para a concretização de uma visão integrada do panorama de riscos. De qualquer forma, o esforço nos permite não só visualizar as percepções de riscos de forma multissetorial, mas também as convergências de perspectivas e as prioridades que podem informar o desenho de um horizonte de respostas.

13 Para esses dados sobre o horizonte temporal o universo de análise foi de 35 respostas válidas, pois nem todos os participantes do questionário responderam a essa seção.

DESAFIOS E ESTRATÉGIAS DE MITIGAÇÃO

Diante dos múltiplos ativos e riscos digitais, é preciso estabelecer critérios de priorização que possam **apoiar tanto uma agenda nacional de segurança digital quanto ações estratégicas mais imediatas para o fortalecimento da cooperação multissetorial no combate dos principais riscos**. A partir do mapeamento realizado com especialistas dos diversos setores (questionário e reuniões), selecionamos os que foram mencionados com maior frequência:

1 - Falta de capacitação;
2 - Desinformação e manipulação;
3 - Crimes cibernéticos;
4 - Acesso indevido;
5 - Ameaças à infraestrutura crítica.

Tratam-se de riscos que atravessam todos os setores e que, por consequência disso, são compreendidos aqui como os maiores desafios para a segurança digital no Brasil. O enfrentamento desses desafios não trará apenas um ambiente digital mais seguro no aspecto intrassetorial, mas também **vai potencializar a colaboração entre os setores, de modo a consolidar uma agenda de segurança compartilhada, mitigando o problema da fragmentação de iniciativas**.

Nesse sentido, as estratégias de mitigação apresentadas para cada um dos cinco desafios necessitam, antes de tudo, **da ação coletiva entre diversos setores**. Em suma, tratam-se de ações para mitigar os maiores riscos que, ao mesmo tempo, irão fortalecer as capacidades de resposta e a resiliência da segurança digital nacional.

Desafio 1 Amplo esforço para capacitação multissetorial

Há um consenso entre os diversos setores da segurança cibernética de que a ausência de conhecimentos e práticas básicas de proteção de dados, de capacitação técnica para a proteção de infraestruturas e de capacidades para planejamento e implementação de processos são ameaças para a segurança digital. Embora esforços de capacitação venham sendo realizados setorialmente, é preciso incentivar o surgimento de iniciativas multissetoriais de conscientização e capacitação para enfrentamento dos riscos digitais.

Diante do cenário de fragmentação da agenda de segurança digital, a capacitação multissetorial incentivará o compartilhamento de conceitos, percepções e experiências. Assim, ela trará uma compreensão sobre a transversalidade dos riscos e sobre a construção de uma cultura de segurança no país, elemento essencial para o fortalecimento da resiliência do ambiente digital brasileiro.

Estratégias de mitigação:

- **Incentivos à criação de trilhas de capacitação para servidores públicos e funcionários de empresas**, com medição e mensuração de eficiência e eficácia de resultados, bem como premiações para estimular a participação. As trilhas de capacitação devem ser realizadas periodicamente — tendo em vista a evolução dos sistemas utilizados por órgãos públicos e privados, as tecnologias e os métodos de ataques cibernéticos, bem como a rotatividade de servidores e profissionais.

- **Desenvolvimento de um repositório de pontos de contato de especialistas em segurança digital alocados em órgãos públicos.** Apesar de atores como CTIR.gov e outros já serem reconhecidos como atores centrais em processos de cooperação técnica dentro da Administração Pública Federal (APF), a alta rotatividade dos servidores públicos em diferentes órgãos traz desafios de continuidade de comunicação e coordenação de atividades. A adoção de práticas como a inserção e adoção de protocolos para a constante atualização da lista de profissionais atuantes no tema fortalecerá a sustentabilidade dos esforços no setor público em pelo menos duas formas. Facilitará o acompanhamento de mudanças em pontos de contato e, com base nisso, poderá, inclusive, melhor direcionar as iniciativas dedicadas ao treinamento, capacitação e inclusão de analistas e servidores em posições associadas à segurança da informação.

- **Desenvolvimento de ações de conscientização e sensibilização da sociedade**, com participação de todos os setores. As ações devem ser periódicas, de modo a manter o público atualizado e o tema da segurança digital sempre em pauta. Ações de conscientização e sensibilização também permitem atingir um público que não está incluído em sistemas tradicionais de ensino. Atualmente, o Dia da Internet Segura e o Fórum da Internet no Brasil (FIB) têm congregado esforços similares.14 Futuras atividades devem buscar não só trazer mais visibilidade sobre iniciativas existentes, mas também criar espaços, fóruns e campanhas para abordar dimensões de riscos e comunidades afetadas de forma mais direcionada. Esses e outros esforços contribuirão também para a capacitação para além do sistema de educação formal, tornando o tema e o conhecimento mais acessível a um público maior.[15]

- **Ensino de noções básicas de segurança digital em todos os níveis de ensino**, com inserção do tema na Base Nacional Curricular.

- **Priorização de temas de segurança digital nos cursos técnicos, nível superior e pós-graduação**. A inclusão desses temas não deve se restringir a aspectos técnicos nos cursos de Ciências Exatas, mas também deve ser levada à formação em Ciências Humanas e Sociais.

- **Inclusão da formação sobre direitos em todos os esforços de capacitação**, para que os incidentes sejam compreendidos também em sua gravidade jurídica. Nesse sentido, os diversos órgãos reguladores têm um importante papel em processos de capacitação.

- **Realização de simulações e cenários de ataques tanto como instrumentos de capacitação para estudantes e profissionais, bem como para a integração de setores.** Exercícios como esses têm se tornado um elemento prioritário para muitos países como Reino Unido,[16] EUA, Alemanha, Suíça e outros que organizam os chamados Cyber 9/12 Challenge com estudantes de diferentes universidades a nível nacional. Já a Organização dos Estados Americanos

14 SAFERNET. Sid2021. Programação. Disponível em: https://www.safernet.org.br/site/sid2021/programacao. Acesso em: mar. 2021.

15 Um exemplo a ser destacado é o Cybersecurity Symposium da OEA, o qual é especificamente dedicado ao tema da cibersegurança, mas proporciona trilhas temáticas (workshops) que abordam dimensões específicas de segurança como estratégias nacionais, direitos humanos e treinamento de CSIRTs, entre outras. Ver: OEA. OEA Cyber Simposio 2019. Disponível em: https://oeacybersimposio19.gob.cl/eng/wp-content/uploads/2019/09/AgendaSimposioOEA19ENG.pdf. Acesso em: mar. 2021.

16 A exemplo do “Cyber Strategy Challenge” (Fevereiro de 2021). Disponível em: https://www.cyber912uk.org/en/.

(OEA) em parceria com a Trend Micro, têm organizado CyberWomen Challenge, exercícios específicos para mulheres no campo.[17] No Brasil, o Exercício do Guardião Cibernético[18] buscou realizar um esforço similar. No entanto, faz-se necessário expandir esforços para incluir organizações da sociedade civil, uma vez que isso possibilitará maior sensibilização sobre como os riscos impactam diferentes setores e como eles trabalham em conjunto para responder a crises.

Desafio 2
Engajamento de todos os setores no enfrentamento à desinformação e à manipulação

O uso da Internet, em especial das redes sociais, como meio para a propagação de campanhas de desinformação e manipulação da opinião pública pode ser considerado como um dos principais novos riscos digitais. Esse risco se destaca como o segundo maior, de acordo com especialistas de diferentes setores no Brasil. A disseminação de informação falsa, ou a manipulação de pessoas por meio do uso de informação, pode afetar a integridade física, psicológica e patrimonial de indivíduos, através da coordenação da sua difusão e do uso de ferramentas de inteligência artificial.

Conforme campanhas coordenadas ganham força e volume, a tendência é que a própria confiabilidade das informações que circulam na rede venha a ser amplamente afetada, o que pode contribuir para o enfraquecimento das instituições públicas e privadas. Assim, é preciso compreender que o problema da desinformação e da manipulação afeta todos os setores, tornando-se uma responsabilidade compartilhada.

Novamente, estratégias de mitigação fragmentadas não serão suficientes para o enfrentamento desse risco. As Forças Armadas têm um papel central na mitigação de influências externas, mas é preciso criar esforços de colaboração entre o setor público, a academia, a sociedade civil e o setor privado. Esses esforços devem incluir o compartilhamento de informações e o desenvolvimento de conhecimentos e ferramentas que permitam a compreensão do fenômeno da desinformação e da manipulação, bem como incentivar a conscientização a respeito dos seus danos e a capacitação da população como um todo.

Estratégias de mitigação:

- **Desenvolvimento de estratégias de comunicação e planos de comunicação em períodos de crise**. Conforme visto no caso dos vazamentos de dados do Tribunal Superior Eleitoral (TSE) durante as eleições de 2020, uma estratégia de comunicação bem articulada poderia ter evitado os danos e ruídos provocados pelo incidente.

- **Criação de Forças Tarefas Multissetoriais ou Independentes para auxiliar o processo democrático.** Um exemplo internacional é a "Election Integrity Partnership",[19] dos EUA, formada por instituições acadêmicas e think

17 TRENDMICRO. Cyber Women Challenge. 2018. Disponível em: https://resources.trendmicro.com/2018-LAR-CyberWomen-Challenge-ES-About.html. Acesso em: mar. 2021.

18 EXÉRCITO BRASILEIRO. Exercício Guardião Cibernética 2.0. Jul. 2019. Disponível em: https://www.eb.mil.br/web/imprensa/aviso-de-pauta/-/asset_publisher/0004ie79MBVM/content/exercicio-guardiao-cibernetico-2-0. Acesso em: mar. 2021.

19 ELECTION INTEGRITY PARTNERSHIP. The Long Fuse: Misinformation and the 2020 Election. Relatório. 2021, 282p. Disponível em: https://www.eipartnership.net/. Acesso em: mar. 2021.

tanks, voltada para a colaboração entre governo e sociedade civil, auxiliando no fortalecimento dos padrões de combate à desinformação nas plataformas digitais e no compartilhamento de informações sobre o tema com o público em geral. Durante as eleições de 2020, o TSE brasileiro criou o Programa de Enfrentamento à Desinformação com Foco nas Eleições 2020.[20] No entanto, é preciso que esses esforços multissetoriais tenham maior perenidade, para que produzam conhecimento e desenvolvam ações de médio e longo prazo.

- **Alocação de recursos específicos para esforços de capacitação em literacia digital, em todos os níveis de ensino**. Trilhas de capacitação podem ser construídas em parcerias com jornalistas e profissionais de checagem de fatos. A capacitação deve envolver não apenas a conscientização a respeito das técnicas de desinformação, mas também o esclarecimento a respeito de direitos fundamentais que podem ser potencialmente violados em campanhas desse tipo.

- **Fomento de pesquisa e campanhas de conscientização a respeito das modalidades e técnicas usadas em campanhas de desinformação e operações de influência.[21]** Diversos grupos da academia e da sociedade civil já desenvolvem pesquisas sobre o tema. Comissões multissetoriais e grupos de trabalho podem ser formados para a produção de material para ampla circulação.

Desafio 3
Aprimoramento da prevenção e combate aos crimes cibernéticos

A categoria de crime cibernético engloba uma ampla variedade de atos criminosos, praticados com o uso de um ou mais computadores. Tais atos vão desde a violação aos direitos de personalidade — como crimes contra a honra e descriminação no ambiente digital — até a prática de pedofilia e de exploração infantil por meio da Internet.

Outras modalidades de crimes cibernéticos dizem respeito a práticas relacionadas a outros desafios listados aqui, como o acesso indevido a sistemas e dados. Podemos citar como exemplo o notório vazamentos de dados do TSE[22] durante as eleições de 2020, e o recente vazamento de dados pessoais de 220 milhões de brasileiros.[23] De acordo com uma pesquisa do MIT, publicada no Journal of Data and Information Quality, o Brasil teve um aumento de 493% de dados entre os anos de 2018 e 2019.[24]

20 TSE. Programa de Enfrentamento à Desinformação com foco nas Eleições 2020 mobiliza instituições. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020-mobiliza-instituicoes. Acesso em: mar. 2021.

21 As operações de influência têm como alvo a formação de opinião através do uso de meios, ferramentas e técnicas ilegítimas, ainda que não necessariamente ilegais. Tradicionalmente, a literatura da área argumenta que operações de influência são realizadas por atores estrangeiros ou atores internos que atuam em nome destes (WANLESS; PAMMENT, 2019). Disponível em: https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf.

22 UOL. Segurança. Bugs do TSE colocam eleição em risco. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/16/bugs-do-tse-nao-colocam-eleicao-em-risco-entenda-4-pontos-do-vazamento.htm. Acesso em: mar. 2021.

23 TSE. Segurança. Vazamento expõe dados de 2020 milhões de pessoas. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/01/28/vazamento-expoe-dados-de-220-mi-de-brasileiros-origem-pode-ser-cruzada.htm. Acesso em: mar. 2021.

24 NETO, N.; MADNICK, S.; DE PAULA, A.; BORGES, N. Desenvolvendo um banco de dados global de violação de dados e os desafios encontrados. Journal of Data Information Quality, Jan. 2021, Art. 3. Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. Acesso em: mar. 2021.

O aprimoramento da prevenção e combate aos crimes cibernéticos deve passar por iniciativas que reúnam esforços de todos os setores. Por um lado, é preciso fortalecer as capacidades de investigação dos órgãos competentes. Por outro, deve-se também incentivar o compartilhamento de conhecimento entre os diversos setores e empreender esforços de sensibilização da população sobre suas vulnerabilidades, junto com o desenvolvimento e disponibilização de tecnologias seguras e acessíveis.

Estratégias de mitigação:

- **Criação de rotinas de fiscalização e manutenção dos sistemas utilizados por entes públicos e privados.** Alguns órgãos e empresas já possuem essa prática consolidada, de modo que é possível criar guias de boas práticas para serem compartilhados entre diferentes instituições.

- **Investimento para fortalecer e capacitar tecnologicamente a Polícia Federal e as Delegacias de Polícia Civil especializadas em crimes cibernéticos**. Atualmente existem 18 delegacias desse tipo no país, mas é preciso aprimorá-las para que tenham plenas capacidades de investigação.

- **Ênfase na importância e incentivo da cooperação internacional no combate aos crimes cibernéticos**, principalmente no âmbito da Interpol, Ameripol e o Escritório das Nações Unidas sobre Drogas e Crime (UNODC). O Brasil já é signatário de acordos que tratam sobre o tema com os BRICS e vem trabalhando para assinar a Convenção de Budapeste. Novos acordos bilaterais podem ser um importante instrumento para o fortalecimento institucional no combate a essas modalidades criminosas.

- **Desenvolvimento de ferramentas públicas e abertas para detecção, filtragem e prevenção de ataques.** Tal medida pode facilitar o acesso a recursos básicos de prevenção de crimes para todos os tipos de usuários, sejam eles instituições ou indivíduos. Ferramentas abertas também permitem o aprimoramento constante e o escrutínio da comunidade técnica.

- **Compartilhamento com o público mais amplo de informações sobre os sistemas de detecção, filtragem e prevenção de ataque.** Existem ferramentas de compartilhamento de informações sobre incidentes que já são utilizadas por instituições do setor bancário e financeiro que podem ser adotadas por outros setores. É preciso incentivar esse compartilhamento de informações e boas práticas no âmbito intrassetorial, multissetorial e com o público geral.

- **Incentivo ao desenvolvimento e ao uso de sistemas que sejam seguros por design.** Na medida em que usuários comecem a adotar sistemas seguros, há uma tendência de que sistemas concorrentes busquem investir na segurança como forma de atrair e manter seus consumidores, aumentando, assim, a segurança do ambiente digital como um todo.

Desafio 4
Garantia da segurança no acesso a sistemas

Os acessos indevidos a sistemas de informação, obtidos por meio de engenharia social, falhas de segurança digital ou física, ou através do roubo de credenciais, podem ser considerados como um dos maiores riscos à segurança, pois prejudicam os processos de interação entre diferentes componentes de um sistema.

O risco dos acessos indevidos afeta desde usuários individuais, até os sistemas de infraestrutura. Assim, a garantia da segurança digital no acesso a sistemas deve ser transversal, tendo em vista a interdependência dos setores e o modo como a presença de uma vulnerabilidade pode afetar toda uma cadeia de atores e organizações. Novamente, trata-se de mais um desafio que deve ser enfrentado com capacitação multissetorial, conscientização e disponibilização de ferramentas acessíveis para todos.

Estratégias de mitigação:

- **Maior conscientização a respeito de ferramentas e mecanismos básicos de proteção, disponíveis a todos**, como o uso de dispositivos e plataformas com criptografia de ponta a ponta, VPNs, múltiplos fatores de autenticação e criação de senhas fortes.

- **Incentivo ao desenvolvimento e uso de sistemas que sejam seguros por design**. Tal como mencionado nas estratégias de mitigação no desafio de enfrentamento aos crimes cibernéticos, o uso de ferramentas que consideram a segurança digital como prioridade desde o momento do seu desenvolvimento contribui para a criação de um ambiente digital mais seguro e menos propenso à exploração de vulnerabilidades.

- **Criação de ferramentas abertas e públicas para o usuário individual**. Ferramentas públicas e abertas tendem a ser mais seguras, uma vez que seu código pode ser examinado pela comunidade técnica. Além disso, quando públicas, permitem o fácil acesso por parte da população.

- **Incentivo à publicação e à divulgação de relatórios ou outras medidas de transparência por parte de entes públicos e privados, relatando os acessos indevidos aos seus sistemas**. Uma vez que se identifique um acesso indevido, ele poderá ser reportado para o público em geral, incluindo pessoas que não estão entre as vítimas. Tais medidas de transparência são interessantes para a sociedade civil, pois permitem o monitoramento social de possíveis impactos aos direitos humanos.[25]

Desafio 5
Aprimoramento da proteção de infraestruturas críticas

As infraestruturas críticas são os ativos e serviços essenciais para o pleno funcionamento da sociedade. No Brasil, são consideradas infraestruturas críticas os sistemas de energia, água, transporte, telecomunicações e finanças. Tratam-se de serviços que dependem cada vez mais da conectividade, além do fato de que, no caso dos sistemas de energia e dos sistemas de telecomunicações, garantem o próprio funcionamento da Internet. É importante ressaltar que a proteção das infraestruturas críticas depende não somente da prevenção e resposta às ameaças digitais, mas também às ameaças físicas, que comprometem o pleno funcionamento da rede.

Dada à interdependência que todos os setores possuem com a infraestrutura crítica do país, as estratégias de mitigação dos seus riscos

25 Pesquisas como o artigo do Maschmeyer et al (2020) apontam que relatórios de inteligência de ameaças em grande parte não reportam os impactos ou incidentes associados a grupos da sociedade civil. Alguns exemplos incluem a APT28, apelido dado ao grupo de hackers russo associado à agência de inteligência russa GRU, que também ficou conhecido pelos ataques ao Partido Democrata dos EUA em 2016 (MASCHMEYER; DEIBERT; LINDSAY). Disponível em: https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658.

devem ser de responsabilidade compartilhada. As Forças Armadas já vêm empreendendo esforços de capacitação do setor de infraestrutura por meio do exercício Guardião Cibernético, mas é preciso ampliar o volume de iniciativas e as redes de cooperação entre os órgãos públicos e o setor privado. A troca de conhecimento e o desenvolvimento de iniciativas em conjunto permitirá a criação de uma cultura de segurança e a compreensão das vulnerabilidades existentes.

Estratégias de mitigação:

- **Estabelecimento de políticas rigorosas de acesso aos sistemas ligados à infraestrutura crítica, com perfis de segurança, controle e registro de usuários.** Muitas organizações já possuem políticas de acesso a sistemas, mas é preciso criar e incentivar o uso de um padrão próprio para o setor de infraestrutura crítica, baseado em boas práticas do setor privado e de órgãos públicos.

- **Incentivo às políticas de manutenção mensal de hardwares essenciais.** Os hardwares costumam ser menos monitorados para a identificação de vulnerabilidades do que softwares. Assim, uma política de manutenção e fiscalização regular dos hardwares utilizados na infraestrutura crítica torna-se fundamental para a prevenção de incidentes.

- **Criação de uma cultura de realização de auditorias externas regulares.** Auditorias independentes, voltadas para a avaliação dos padrões de segurança nos sistemas empregados na infraestrutura crítica, podem ser uma boa prática capaz de identificar vulnerabilidades que passaram despercebidas pelo monitoramento das instituições responsáveis. Essas auditorias também podem cumprir a função de prestação de contas para os demais setores que dependem do pleno funcionamento da infraestrutura crítica.

- **Criação de uma rede de cooperação contínua entre as instituições de infraestrutura crítica e a Polícia Federal**, para monitoramento de crimes cibernéticos que possam comprometer o funcionamento pleno dos serviços.

- **Realização e manutenção contínua de mapeamentos detalhados das vulnerabilidades e dos riscos específicos do setor de infraestrutura**. É possível estabelecer parcerias com a academia para o desenvolvimento de metodologias e acompanhamento da evolução tecnológica, permitindo a continuidade e a atualização constante de mapeamentos.

CONCLUSÃO

No decorrer das conversas multissetoriais realizadas nos últimos 6 meses e durante a análise das múltiplas estratégias de mitigação mencionadas nos questionários, foi possível identificar que os desafios compartilhados pelos diversos setores refletem um aspecto central: a ausência de uma cultura de segurança digital mais inclusiva, sustentável e transparente. Assim, se esse documento tem início no diagnóstico que aponta o problema transversal da fragmentação da agenda de segurança digital, sua conclusão se dá com a percepção de que é preciso trabalhar para o estabelecimento de uma cultura que consolide a importância desse tema.

Entende-se por cultura de segurança digital um conjunto de conceitos, paradigmas e práticas que podem moldar diversas percepções e ações sobre segurança. A criação de uma cultura de segurança digital passa pela realização de esforços de conscientização sobre o tema, mas também pela criação de normas, políticas, padrões e práticas institucionais.

A Estratégia Nacional de Segurança Cibernética (E-Ciber) menciona a necessidade do estabelecimento de uma cultura de segurança digital, mas é necessário aprofundar e transformar esse imperativo em ações concretas. Todos os setores envolvidos na governança da segurança digital demonstram ter consciência da importância da aculturação em práticas de segurança. Ela passa pela popularização de ferramentas, protocolos e técnicas de proteção e prevenção, bem como por esforços maiores de capacitação. No entanto, observamos que ainda não existem parâmetros para a atribuição de responsabilidades no estabelecimento de uma cultura de segurança digital.

Para que uma cultura de segurança digital seja criada, cada setor deve ir além da gestão dos riscos que afetam suas próprias atividades. Governos e empresas precisam capacitar os usuários dos seus serviços para que eles tenham o conhecimento e as ferramentas necessárias para garantir sua segurança, de modo a não só protegê-los, mas também educá-los. Em outras palavras, é preciso investir no desenvolvimento de ferramentas e ambientes seguros, ao mesmo tempo em que os motivos que levaram à escolha dessas ferramentas sejam deixados claros.

A academia e a comunidade técnica podem colaborar no fortalecimento dessa cultura fornecendo o conhecimento necessário para o desenvolvimento dessas capacidades técnicas. Contudo, ambas precisam, por sua vez, de investimento público na área de pesquisa e desenvolvimento, para a criação de tecnologias de ponta. Organizações da sociedade civil também vão se beneficiar desses investimentos e dos esforços de capacitação, ao mesmo tempo em que fornecem a expertise necessária para que esses esforços atinjam e beneficiem toda a população, incluindo grupos particularmente vulneráveis.

Esperamos que este trabalho, e suas futuras iterações, possam auxiliar a construção de uma cultura de segurança digital. E, assim, permitam que todos os setores se tornem plenamente conscientes do panorama geral de ameaças e dos ativos que devem ser protegidos; informem processos como a atualização da Estratégia de Transformação Digital Brasileira (E-Digital); auxiliem o desenho de planos de implementação concretos para o fortalecimento da Confiança no Ambiente Digital de forma multissetorial e multidimensional; e reconciliem defesa e segurança no ambiente digital em um panorama mais amplo de fortalecimento da proteção de dados e da privacidade na sociedade brasileira.

ANEXO 1: GLOSSÁRIO DE RISCOS PARA A SEGURANÇA DIGITAL

Abaixo segue uma lista completa das ameaças e vulnerabilidades destacadas no processo de mapeamento de riscos para a segurança digital. Conforme previamente apontado, essa lista não é exaustiva, mas apresenta uma visão mais detalhada dos desafios presentes no panorama nacional atual. Vale ressaltar que algumas ameaças e vulnerabilidades se repetem, pois foram desenhadas de forma a evidenciar elementos específicos de cada ativo.

ATIVOS	AMEAÇAS & VULNERABILIDADES	
Dados	Vazamento de Dados	A transmissão não autorizada de dados de uma organização para destino ou recipiente externo, realizado de modo eletrônico ou físico, acidental ou intencional.
	Roubo de Credenciais	A obtenção não autorizada de credenciais de segurança que concedem acesso a dados, incluindo identificação, autenticação, senhas, e perfis de acesso.
	Marco Regulatório	Ausência de marco legal (ambiente legal) adequado para proteção de dados, sistemas, infraestruturas e indivíduos e/ou a existência de uma lei que possa prejudicar a proteção de direitos.
	Ausência de Protocolos de Compartilhamento de Informações	A ausência de parâmetros internos e externos que definam como dados podem ser compartilhados e/ou transferidos entre diferentes departamentos de uma organização e/ou entre diferentes organizações.
	Ransomware	Indisponibilização de acesso de dados por meio de implementação de código malicioso até que um valor seja pago pelo resgate.
	Falta de Capacitação no Uso de Recursos e Sistemas de Informática em Nível Social	A ausência de conhecimento de práticas básicas de proteção de dados em sistemas de informática, na sociedade.

Sistemas	Ameaças Ambientais	Fenômenos naturais, que afetam o ambiente e podem afetar a disponibilidade e integridade dos sistemas, tais como: condições climáticas desfavoráveis, alagamentos, enchentes, tempestades e raios e interferências eletromagnéticas.
	Ameaças Físicas	Roubo; Vandalismo; Sabotagem; Terrorismo; Transporte inadequado.
Infraes-truturas	Acesso Indevido	Acesso indevido a sistemas de informação, obtidos por meio de engenharia social ou roubo de credenciais, que pode prejudicar os processos de interação entre os diferentes componentes de um determinado sistema ou organização.
	Ameaças à Infraestrutura Crítica	Quedas de fornecimento de energia e outros serviços essenciais; Falha no controle de temperatura; Falha no controle de umidade; Manutenção inadequada; Falta de pessoal; Falhas no controle de descarte de material; Ataques cibernéticos.
	Ameaças Ambientais	Desastres naturais que comprometem a integridade e a disponibilidade de determinada infraestrutura.
	Espionagem	Ataque cibernético dirigido contra a confidencialidade de informações sobre determinada infraestrutura.
	Falhas de Energia	Falhas no abastecimento de energia que possam comprometer a integridade e a disponibilidade de determinada infraestrutura.
	Falta de Capacitação Técnica de Pessoal Encarregado	A ausência de conhecimento técnico do pessoal responsável pela manutenção, administração e operação de determinada infraestrutura.
	Incêndios	Incêndios, acidentais ou intencionais, que possam comprometer a integridade e a disponibilidade de determinada infraestrutura.
	Invasões Físicas	Incidente de segurança no qual o ataque foi bem sucedido, resultando no acesso, manipulação e/ou destruição de informações e/ou sistema que comprometa a integridade ou a disponibilidade determinada infraestrutura. Invasões físicas podem ser acompanhadas de estratégias de ataques cibernéticos maliciosos.
	Má Configuração de Sistemas	Sistemas configurados de modo inadequado e que possam vir a comprometer a integridade e a disponibilidade de determinada infraestrutura.

Direitos	Ameaças ao Direito de Propriedade Imaterial	Ações perpetradas por grupos, indivíduos ou organizações com o intuito de prejudicar a imagem e/ou a reputação de uma organização, ou violar algum bem imaterial como segredo industrial ou patente.
	Controle e censura	Ações que podem prejudicar o exercício da liberdade de expressão, da liberdade de imprensa, do direito à privacidade e à proteção de dados, através do uso de meios tecnológicos e não tecnológicos por agentes de Estado, governos não democráticos e/ou autocráticos.
	Cibercrimes	Atos criminosos, praticados com o uso de um ou mais computadores, que podem violar direitos de personalidade - como crimes contra a honra e discriminação - representar a prática de pedofilia e exploração infantil e realizar roubo de credenciais, assim como o acesso indevido a outros tipos de dados.
	Desinformação e Manipulação	Disseminação de informação falsa, ou a manipulação de pessoas por meio do uso de informação, que podem vir a afetar a integridade física, psicológica e patrimonial de indivíduos, tais como a manipulação de “sentimentos” por meio de ferramentas de inteligência artificial e a desinformação sobre questões relacionadas à saúde, ou de outras tecnologias de informação e comunicação e seus algoritmos.
	Ataques a Infraestruturas Críticas	Ataques cibernéticos a infraestruturas críticas que, ao afetarem sua disponibilidade e integridade, podem prejudicar o exercício de direitos.
	Uso Desproporcional ou Inadequado de TICs	A utilização de novas tecnologias que, por desconhecimento dos seus operadores, falta de regulação ou por características intrínsecas ao seu funcionamento, podem prejudicar ou violar direitos, tais como: tecnologias de vigilantismo e predições/ alterações de comportamento em função dos algoritmos de plataformas.

Processos	Acesso Indevido	Acesso indevido a sistemas de informação, obtidos por meio de engenharia social ou roubo de credenciais, que pode prejudicar os processos de interação entre os diferentes componentes de um determinado sistema ou organização.
	Falta de Atribuição de Responsabilidade dos Processos	A ausência de protocolos de responsabilização integral sobre processos de integração de tecnologias. Falta de clareza sobre responsabilidades e competências para garantir a proteção do sistema/infraestrutura/banco de dados.
	Indisponibilidade	Falhas de comunicação entre os diferentes componentes do processo, interrupção de serviços (man-in-the-middle/DDoS); perda de conectividade e interferência nos processos de comunicação entre sistemas.
Pessoas	Negligência de Pessoas em Planos de Resposta a Incidentes	Planos de resposta a incidentes, sejam eles públicos ou corporativos, que não levam em consideração os danos diretos e indiretos que podem afetar a integridade física, psicológica e patrimonial de indivíduos.
	Desinformação e Manipulação	Disseminação de informação falsa, ou a manipulação de pessoas por meio do uso de informação, que podem vir a afetar a integridade física, psicológica e patrimonial de indivíduos, tais como a manipulação de “sentimentos” por meio de ferramentas de inteligência artificial e a desinformação sobre questões relacionadas à saúde.
	Ameaças à Integridade Física e à Vida das Pessoas	Falhas, ataques ou mau uso de sistemas que afetam controles de vida (a exemplo de ransomware em hospitais), ataques que causem interrupção de serviços essenciais, exploração de vulnerabilidades em tecnologias vitais para a saúde de um indivíduo (por exemplo, marcapassos) e take-over de sistemas de vigilância (em segurança pública, aviação, entre outros).

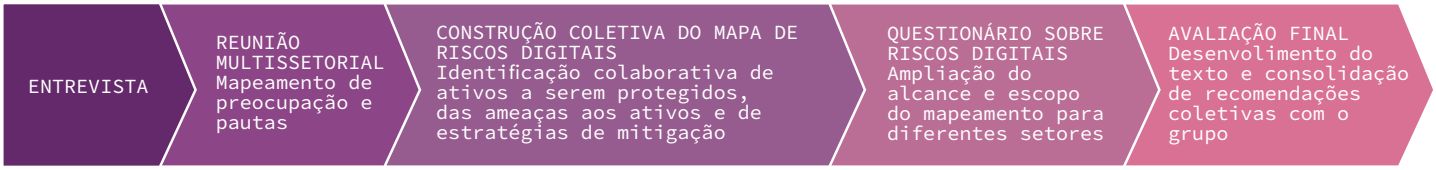
ANEXO 2: METODOLOGIA

Este documento é o resultado de um ano de diálogos com representantes de diferentes setores no Brasil. Iniciamos uma conversa em abril de 2020, com o intuito de compreender os impactos da pandemia na reconfiguração de riscos e prioridades para a segurança digital no país. Como resultado dessa conversa, identificamos que diferentes setores possuem visões distintas sobre o conceito de segurança, sobre o que precisa ser protegido, como proteger e quais as lacunas para atingir esses objetivos de proteção e mitigação. Isso, por si só, não é um ponto negativo. Pelo contrário, reflete a diversidade de riscos, experiências e prioridades que compõem a segurança digital do Brasil. Contudo, ao passo que a boa compreensão dos riscos setoriais tem ajudado atores específicos a estarem preparados para proteger dados, sistemas, infraestruturas, informações e direitos, a falta de diálogo entre setores talvez seja um dos principais desafios para o avanço de uma visão mais estratégica para a segurança digital no país.

Com base nesse diagnóstico, compreendemos que, mais do que trazer esses setores para um diálogo, fazia-se necessário integrar os diferentes conhecimentos sobre riscos digitais, buscando trabalhar conjuntamente em um vocabulário capaz de refletir tanto os impactos específicos como a transversalidade desses riscos.

O PROCESSO DE PESQUISA

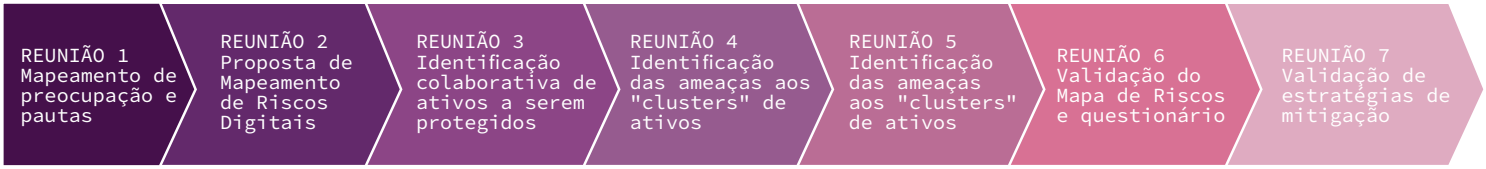
Ao longo de um ano (2020-2021), desenvolvemos um mapeamento colaborativo de riscos com representantes de diferentes setores. O documento respalda-se em uma robusta metodologia que incluiu entrevistas (semiestruturadas e não estruturadas), reuniões multissetoriais com a aplicação de técnicas de design thinking e um questionário.



AS REUNIÕES MULTISSETORIAIS

Ao todo, o processo de construção coletiva contou com sete reuniões multissetoriais virtuais. Iniciamos com uma reunião de prospecção de cenário para compreender as principais pautas e preocupações de segurança digital e as transformações e os impactos advindos da pandemia. Identificou-se uma falta de vocabulário e de entendimento comum capaz de abordar desafios associados à segurança no contexto de crescente interconectividade. Por mais que uso intercambiável de conceitos como segurança da informação, segurança cibernética e segurança digital também apontasse para uma preocupação compartilhada com riscos digitais, por outro lado, ela também vinha acompanhada de uma necessidade de demarcação sobre inquietações específicas de riscos associados a cada setor.

Na segunda fase, reunimos um grupo maior de especialistas de diferentes setores para iniciar um processo de mapeamento colaborativo de riscos para a segurança digital. O processo, que durou seis meses, passou pela identificação dos principais ativos a serem protegidos, mapeamento das principais ameaças a esses ativos e, por fim, a identificação de estratégias de mitigação e respostas.



Nesse último momento, combinamos o trabalho colaborativo com o grupo de especialistas com entrevistas mais pontuais e um questionário direcionado a profissionais que trabalham em temas relacionados à segurança digital.

O QUESTIONÁRIO

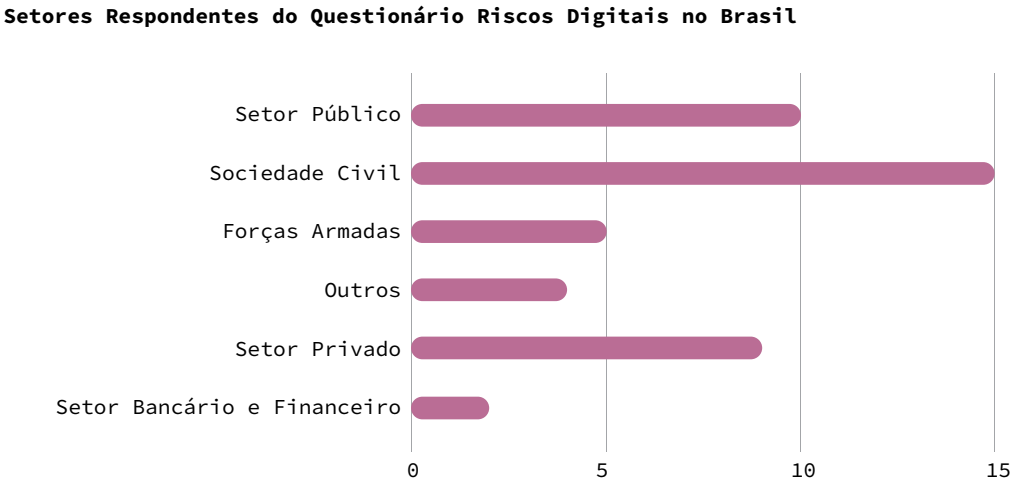
Compartilhamos o questionário com especialistas e profissionais de diferentes setores trabalhando com temas relacionados a direitos digitais, tecnologia e, mais especificamente, segurança. No total, obtivemos 45 respostas válidas. O questionário foi dividido em duas partes: a primeira seção apresentou perguntas de múltipla escolha para auxiliar no processo de mapeamento dos principais riscos de acordo com o setor. A segunda seção apresentou perguntas sobre as estratégias de mitigação aplicadas ou sugeridas pelos respondentes.

Os resultados do questionário foram codificados e classificados de acordo com o emprego da metodologia de Análise Hierárquica (Analytic Hierarchy Process) para a realização de uma análise temática. Após a análise, desenvolvemos uma lista inicial de principais recomendações para o fortalecimento de estratégias de mitigação no país. Uma vez elencadas, trabalhamos com o grupo multissetorial de especialistas para consolidá-las e validá-las em conjunto.

O RESUMO DAS RESPOSTAS

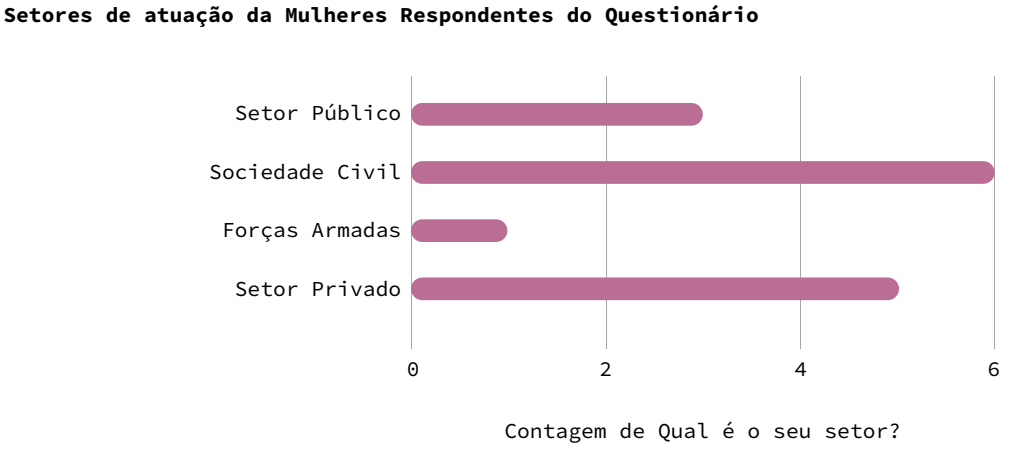
Distribuição setorial

O questionário foi enviado para 69 instituições representantes dos seguintes setores: (I) setor público, (II) privado, (III) Forças Armadas, (IV) organizações da sociedade civil, (V) entidades do setor financeiro e bancário e (VI) outros. O questionário contou com a contribuição de 89 respostas, sendo 45 computadas como finalizadas e completas, a partir da seguinte divisão setorial:

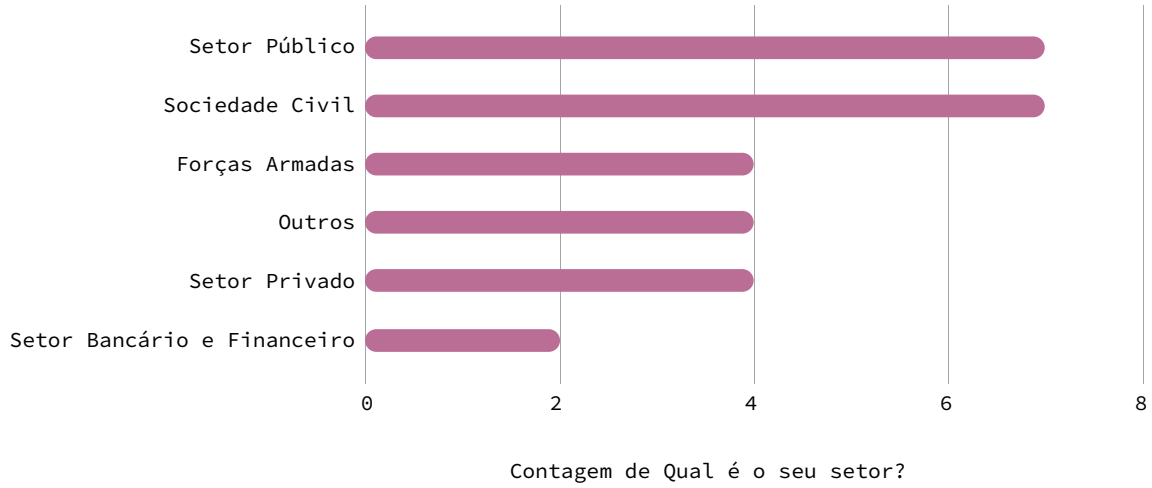


Distribuição de Gênero

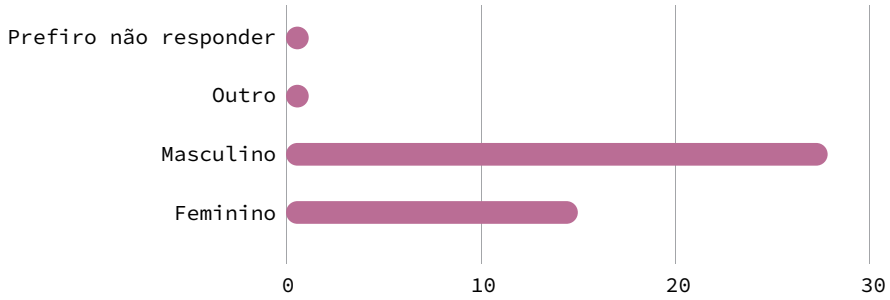
Mesmo não se tratando de uma pesquisa, cujo critério de gênero seja definidora de seus resultados, das 45 respostas válidas, 28 foram respondidas por homens e 15 por mulheres. Os/as demais participantes preferiram não informar seu gênero. Esses respondentes encontram-se distribuídos nos seguintes campos de atuação:



Setores de Atuação dos Homens Respondentes do Questionário



Distribuição dos Respondentes por Gênero



INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado à integração das agendas de segurança, clima e desenvolvimento. Nosso objetivo é propor soluções e parcerias a desafios globais por meio de pesquisas, novas tecnologias, influência em políticas públicas e comunicação. Somos uma instituição sem fins lucrativos, independente e apartidária, com sede no Rio de Janeiro, mas cuja atuação transcende fronteiras locais, nacionais e regionais. Premiada como a melhor ONG de Direitos Humanos no ano de 2018, o melhor think tank em política social pela Prospect Magazine em 2019 e considerada pelo Instituto Doar, pelo segundo ano consecutivo, como uma das 100 melhores organizações brasileiras do terceiro setor.

Apoio:

Embaixada Britânica
Brasília

Instituto Igarapé

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Direção criativa e layout
Raphael Durão - STORMdesign.com.br

ISSN 2359-0998

www.igarape.org.br

INSTITUTO IGARAPÉ
a think and do tank