CIBERSEGURANÇA NOS ESTADOS BRASILEIROS

Diagnóstico e recomendações

ANIC
AGENCIA NACIONAL DE INTELIGENCIA E CIBERSEGURANCA

SUMÁRIO

1.

BACKGROUND

Background

De acordo com o relatório anual de 2023 da Fortinet, o Brasil foi o segundo país da região com o maior número de tentativas de ataques[1] em 2023 (depois do México). Além disso, cada incidente de violação de dados no Brasil teve custo médio[2] de USD 1,22 milhão. Considerando essa grande ameaça, é essencial conhecer os níveis de preparação do Brasil, tanto no âmbito nacional quanto no estadual.

Nesse sentido, em março de 2024, o Subgrupo de Trabalho de Segurança Cibernética do GTD.GOV[3] conduziu um mapeamento das configurações organizacionais relacionadas à segurança da informação e segurança cibernética nas 27 unidades federativas (UFs) brasileiras.[4] Essa pesquisa pioneira analisou – a partir de dois questionários pré-estruturados – políticas, modelos de governança e capital humano nas UFs, integrando as respostas fornecidas tanto pelos pontos focais do GTD.GOV das Secretarias de Estado da Administração (SEAD), quanto pelas entidades estaduais e públicas de tecnologia da informação e comunicação (TIC), aqui denominadas PRODs.[5] Ao combinar essas perspectivas, o relatório oferece a primeira visão do quebra-cabeça da governança da segurança da informação e cibersegurança nas UFs brasileiras. Este documento apresenta os principais achados desse mapeamento e recomenda ações que as UFs devem adotar para fortalecer a governança, o estabelecimento de normativas e a estruturação das áreas de segurança da informação e cibernética em seus entes, com o objetivo final de aumentar a segurança e confiabilidade nos serviços do governo digital para os cidadãos.

1 60.000 milhões de tentativas de ataque.

2 Data Breach Report 2024, IBM. Inclui danos causados pelo incidente, serviços de resposta e recuperação, perda de clientes e custos de atendimento ao cliente durante a violação.

3 O GTD.GOV é o Grupo de Transformação Digital, formado por uma rede com especialistas dos 26 estados e do Distrito Federal, representando a Associação Brasileira de Entidades Estaduais e Públicas de Tecnologia da Informação e Comunicação – ABEP-TIC (as entidades são conhecidas como PRODs e, embora haja diferenças jurídicas entre os estados, normalmente representam suas empresas públicas de TI) e o Conselho Nacional de Secretários de Estado da Administração – CONSAD. O Subgrupo de Segurança Cibernética foi criado em junho de 2023, no Cyber Day do GTD.GOV, em Manaus, com patrocínio do BID.

4 Neste relatório, usaremos os conceitos de Unidades Federativas (UFs) e estados como intercambiáveis. Dessa forma, o termo estados inclui o Distrito Federal.

5 Entendidas aqui de forma ampla, independentemente da personalidade jurídica que esse organismo assume em cada estado.

2.

CONCEITOS

Neste estudo, foram abordados dois temas distintos, porém complementares: segurança da informação e cibernética. Esses domínios, embora interligados, abordam aspectos específicos da segurança digital, cada um com suas nuances e abordagens.

A segurança da informação concentra-se na proteção da integridade, confidencialidade e disponibilidade das informações. Inclui políticas, procedimentos e tecnologias para garantir que os dados e facilidades sejam acessados e utilizados apenas por pessoas autorizadas e de maneira correta (Whitman e Mattord, 2023).[6]

A cibersegurança ou segurança cibernética refere-se à prática de proteger sistemas, redes e dados contra os ataques cibernéticos. Envolve medidas proativas para prevenir, detectar e responder às ameaças on-line, como *malwares*, ataques de negação de serviço (DDoS) e *hacking*, entre outros (Diogenes e Ozkaya, 2018).[7]

6 M. Whitman e H. Mattord (2023). Meeting the Challenges of Large Online Graduate Cybersecurity Classes in the Age of COVID. *Journal of The Colloquium for Information Systems Security Education*, 10(1): 1-6. https://doi.org/10.53735/cisse.v10i1.165.

7 Y. Diogenes e E. Ozkaya (2018). *Cybersecurity, Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics*. Packt Publishing.

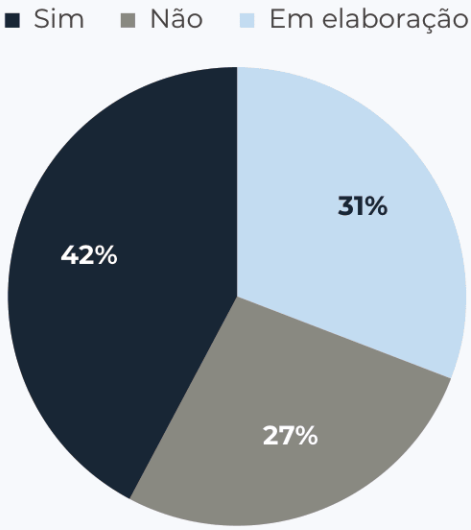
3.

PRINCIPAIS RESULTADOS

Principais resultados[8]

1. Uma em cada quatro UFs brasileiras não possui Política de Segurança da Informação (PSI) em vigor ou em processo de elaboração. Das UFs, 42% indicaram já ter publicado uma Política de Segurança da Informação, enquanto 31% estavam em processo de elaboração, indicando que 58% dos estados ainda não tinham uma PSI vigente. Destaca-se que 27% dos estados não tinham nenhuma iniciativa em andamento para desenvolver ou implementar uma PSI, comprometendo assim a eficácia e abrangência das iniciativas nacionais e estaduais para lidar com riscos em termos de segurança da informação (ver Gráfico 1).

Gráfico 1 – UFs com Política de Segurança da Informação (PSI)

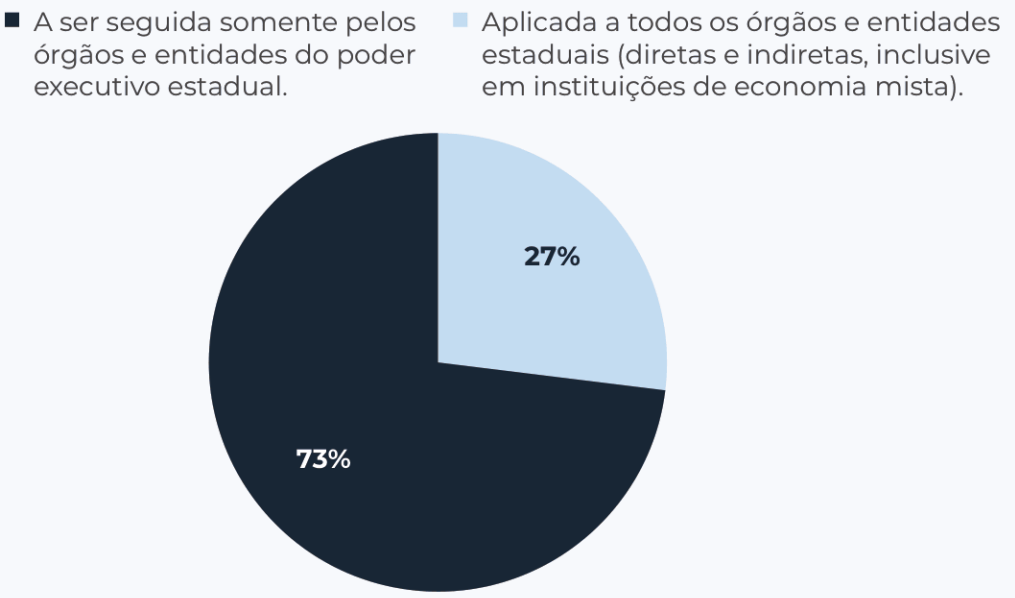


N=26 UFs (questionário do CONSAD)

2. O alcance das PSIs em vigor é limitado, com 73% delas aplicando-se apenas aos órgãos do poder executivo estadual. Do contingente de 42% das UFs que indicaram ter uma PSI em vigor, 73% indicaram que essa política tem caráter transversal no estado, mas que deve ser seguida apenas pelos órgãos do poder executivo estadual, não sendo extensivo às entidades, aos demais poderes ou ao setor privado. Em 27% delas, a política é transversal e aplica-se a todos os órgãos e as entidades estaduais diretas e indiretas (ver Gráfico 2), embora não ao setor privado. O instrumento mais frequente para a publicação dessas políticas, em 75% dos casos, é um decreto estadual.

8 As porcentagens são calculadas com base nas UFs que responderam a cada questão, o que pode acarretar pequenas diferenças no universo de UFs utilizado em cada pergunta. Os dados são de março de 2024.

Gráfico 2 – Alcance da PSI



N=11 UFs com PSI (questionário do CONSAD)

BOAS PRÁTICAS

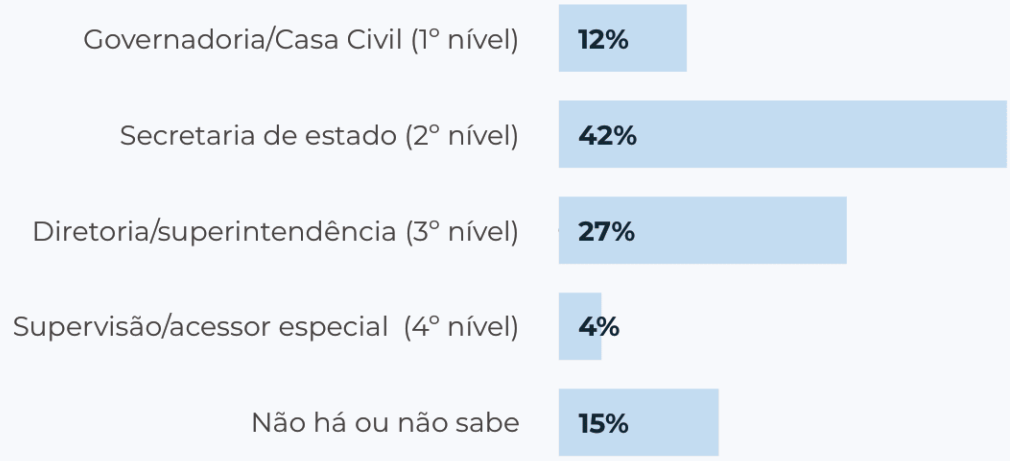
Política

- O Framework de Cibersegurança do NIST, em sua segunda versão, inclui em sua função de "governar", na categoria política (GV.PO), a necessidade de que uma política de cibersegurança seja estabelecida, comunicada e implementada. A política para gerenciar os riscos de cibersegurança deve ser baseada no contexto organizacional, na estratégia de cibersegurança, bem como nas prioridades identificadas.

- A ISO/IEC 27001:2022 define que a alta gestão deve estabelecer uma política de segurança da informação que: (i) seja apropriada ao contexto da organização; (ii) inclua objetivos de segurança da informação; (iii) inclua compromissos para satisfazer aos requisitos de segurança da informação; (iv) inclua compromissos para aprimoramento contínuo do sistema de segurança da informação. Além disso, a política deve ser um documento comunicado e acessível para todas as partes. Vale notar que ambas as práticas se referem ao nível organizacional, enquanto uma política em nível estadual possui escopo mais abrangente, servindo a mais de uma organização.

3. Em 42% das UFs brasileiras, o responsável pela agenda de segurança da informação e privacidade e proteção de dados está localizado em instituição com nível hierárquico de secretaria de estado. Ao mesmo tempo, 12% relataram que esse líder está no primeiro nível hierárquico de governo (Governadoria/Casa Civil) e 27% no terceiro nível hierárquico (em uma diretoria ou superintendência). No entanto, 15% não têm um responsável designado para tratar de assuntos de segurança e privacidade da informação ou indicou não saber de quem se trata, revelando uma lacuna na governança da agenda dos estados no Brasil ver Gráfico 3).[9] Os quadros com os casos dos arranjos institucionais de São Paulo e da Bahia exemplificam a ampla heterogeneidade que existe entre os diferentes estados, seja nos arranjos intrassecretariais, seja nos arranjos das PRODs, seja na relação entre secretarias e PRODs.

Gráfico 3 – Nível hierárquico do líder responsável pela agenda de segurança da informação e privacidade e proteção de dados



N=26 UFs (questionário do CONSAD)

9 Pesquisas adicionais são necessárias para entender com mais profundidade se a localização dos responsáveis pela agenda em níveis hierárquicos mais elevados indica maior relevância do tema na estrutura organizacional ou ausência de uma estrutura específica (de nível mais baixo) para liderar a agenda, o que pode ter gerado dificuldade na identificação das lideranças do tema pelos respondentes da pesquisa (pontos focais do GTD.GOV).

BOAS PRÁTICAS

Papéis e responsabilidades

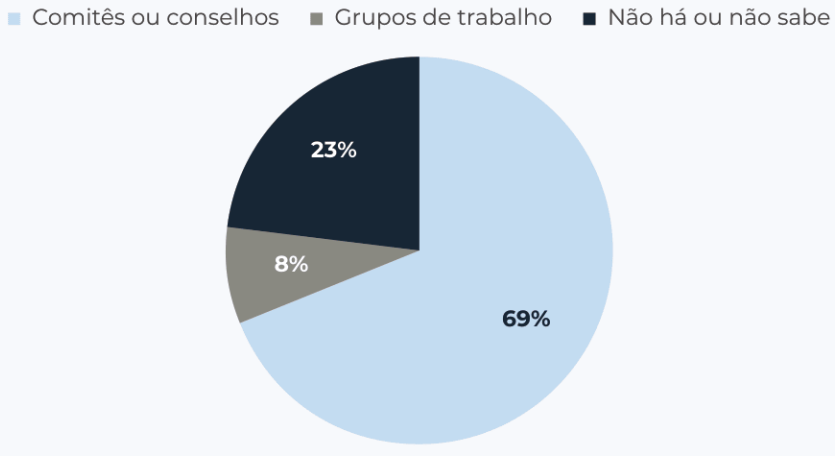
- O Framework de cibersegurança do NIST inclui, na função "governar", a necessidade de que a autoridade, os papéis e as responsabilidades de cibersegurança estejam estabelecidos e comunicados (GV.RR). Em particular, que a liderança seja responsável e responsabilizável pelos riscos de cibersegurança (GV.RR-1), e que os recursos adequados sejam alocados de forma compatível com os riscos de cibersegurança, a estratégia, os papéis e as responsabilidades.

- A ISO/IEC 27001:2022 define que a alta gestão deve assegurar que as responsabilidades e autoridades dos papéis relevantes de segurança da informação sejam atribuídos e comunicados. Em especial, indica que a alta gestão deve designar responsáveis e definir autoridades para reportar o desempenho do sistema de gestão de segurança da informação.

- Recomenda-se que, assim como ocorre no setor privado, onde o CISO (Chief Information Security Officer) é parte integrante dos cargos *C-level*, no setor público também seja garantida a inclusão desse cargo na alta direção. Essa medida reflete a necessidade de considerar a cibersegurança como um elemento estratégico central para as atividades do "negócio" público, uma vez que a cibersegurança desempenha papel fundamental no gerenciamento dos riscos do negócio.

4. Do ponto de vista da coordenação intergovernamental, 69% das UFs indicaram contar com comitês ou conselhos estaduais para lidar com a segurança cibernética. Dessas, 8% indicaram possuir unicamente grupos de trabalho para o tema, e 23% indicaram não ter nenhum mecanismo configurado para lidar com a segurança cibernética de forma coordenada no estado ou não saber se existe (ver Gráfico 4).

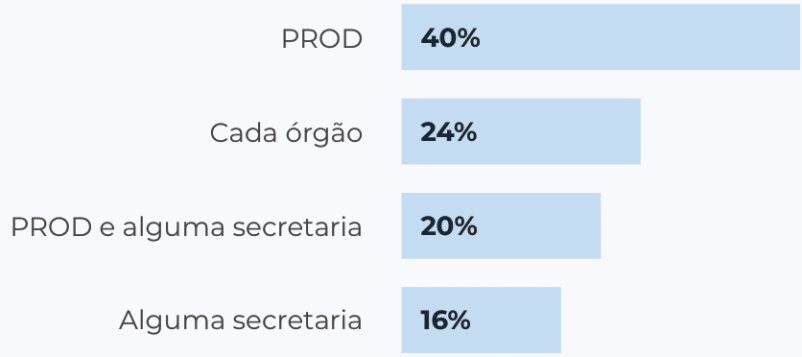
Gráfico 4 – Mecanismos de coordenação intragoverno



N=26 UFs (questionário do CONSAD)

5. Em 60% dos estados, as PRODs ocupam papel central na implementação da política de gestão dos incidentes de cibersegurança. Das UFs respondentes, 40% indicaram unicamente as PRODs como responsáveis pela detecção e tratamento de incidentes de cibersegurança, enquanto 20% indicaram a PROD mais alguma secretaria. Já 24% indicaram que cada órgão é responsável pelo tratamento dos incidentes de cibersegurança. Em 16% dos casos, apenas alguma secretaria tem essa responsabilidade atribuída (ver Gráfico 5).

Gráfico 5 – Responsável pela implementação da política, proteção, detecção e resposta aos incidentes

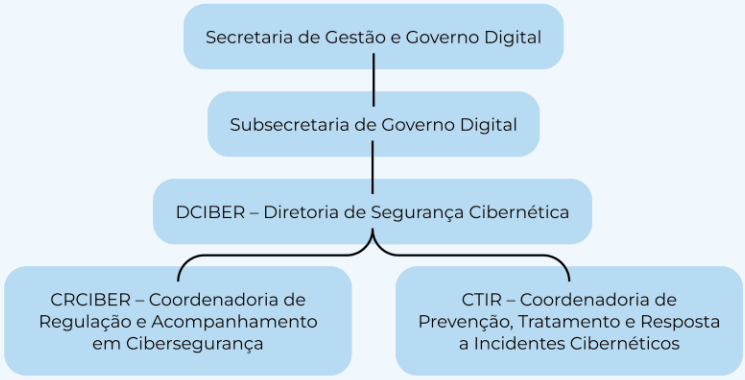


N=25 UFs (questionário do CONSAD)

CASO 1

ARRANJO DA CIBERSEGURANÇA NO ESTADO DE SÃO PAULO

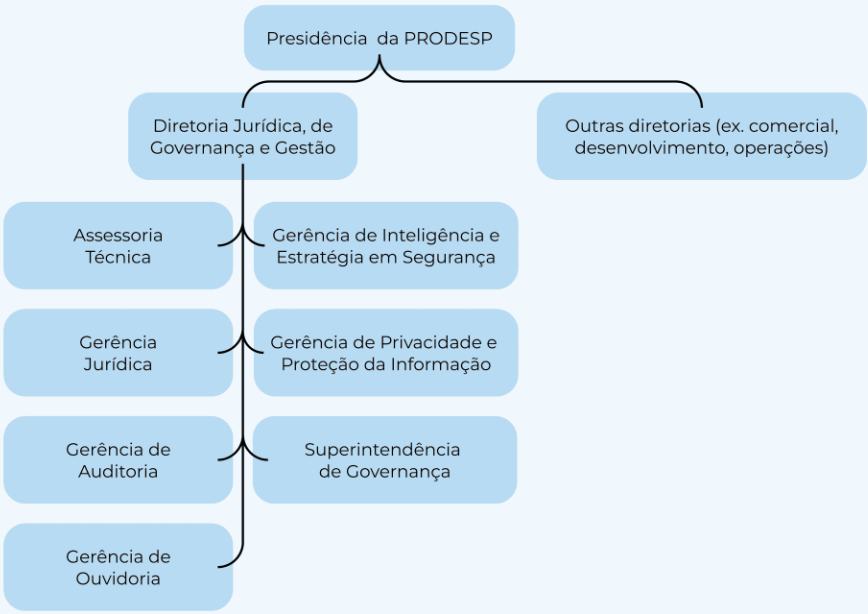
O Decreto Estadual nº69.052, de 14 de novembro de 2024, aprovou a estrutura organizacional da Secretaria de Gestão e Governo Digital e criou uma estrutura dedicada à segurança cibernética.



A Diretoria de Segurança Cibernética (DCIBER) é o departamento estratégico da Subsecretaria de Governo Digital (SGD), pertencente à Secretaria de Gestão e Governo Digital (SGGD) do estado de São Paulo, fundamental para garantir a proteção digital e a segurança das informações na administração pública estadual, sendo sua atuação crucial no cenário de crescentes ameaças cibernéticas. A DCIBER conta com duas coordenadorias especializadas: a Coordenadoria de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CTIR), responsável por monitorar, prevenir, comunicar e responder a ameaças e ataques cibernéticos, atuando de forma ágil na proteção dos sistemas e dados; e a Coordenadoria de Regulação e Acompanhamento em Cibersegurança (CRCIBER), encarregada de estabelecer normas, políticas e diretrizes de segurança cibernética, além de acompanhar sua implementação nos órgãos estaduais, desempenhando assim papel essencial na transformação digital segura e garantindo a continuidade e confiabilidade dos serviços públicos digitais

A DCBIER é responsável por propor padrões, modelos e tecnologias para a aplicação da Política de Segurança da Informação do estado, coordenar atividades, incluir medidas de comunicação, apoiar o desenvolvimento de tecnologias e atuar em iniciativas.

O estado também conta com a PRODESP, a companhia de processamento de dados do estado de São Paulo, empresa pública estadual vinculada à SGGD e parte integrante da administração indireta do estado. A vinculação da PRODESP à SGGD facilita o alinhamento da política de segurança e a implementação das iniciativas associadas. A SGGD define a política, e a PRODESP atua como o principal braço implementador. Na PROD, a área de segurança da informação está vinculada à Diretoria Jurídica, de Governança e Gestão, conforme o organograma abaixo.

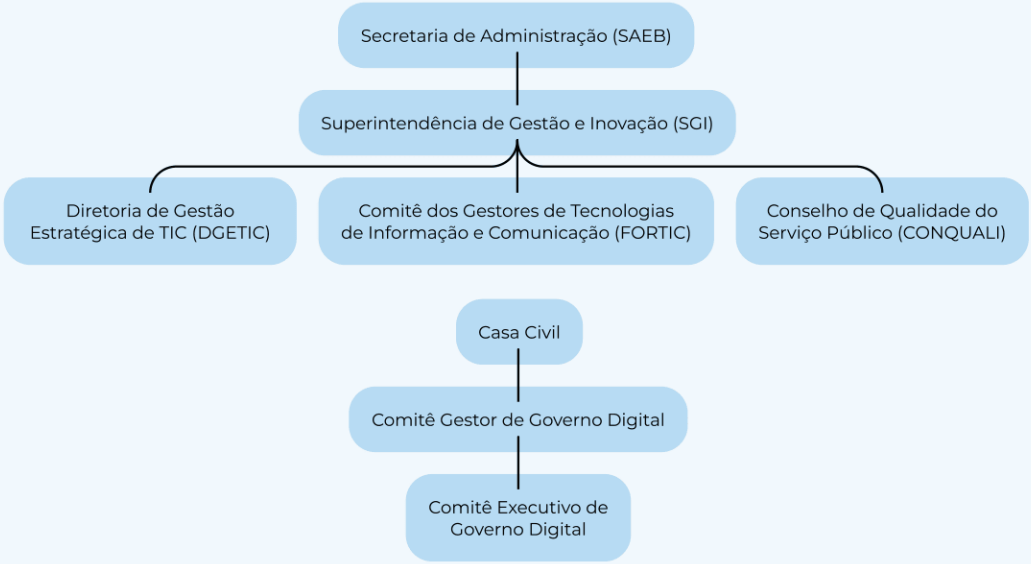


Fonte: Decreto Estadual nº 69.052 e organograma no website da PRODESP.

CASO 2

ARRANJO DA CIBERSEGURANÇA NO ESTADO DA BAHIA

O Decreto Estadual nº 13.473, de 28 de novembro de 2011, homologou a resolução nº 02/2011, a fim de instituir a Política da Informação do Estado. Os Decretos Estaduais nº 21.451, de 9 de junho de 2022, e nº 22.269, de 6 de setembro de 2023, definem a estrutura organizacional voltada à segurança da informação no estado:



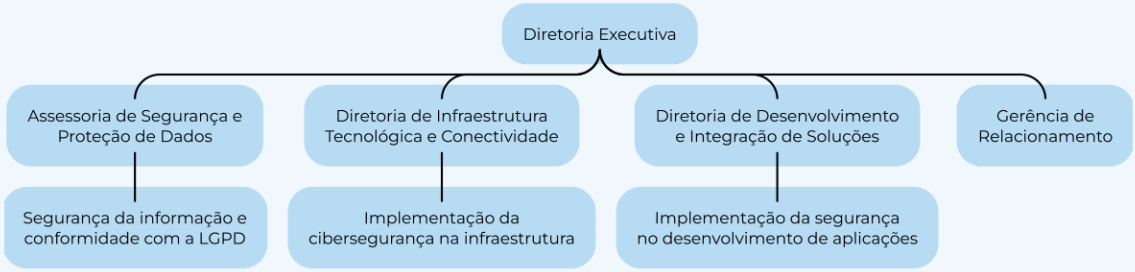
Do ponto de vista da coordenação intergovernamental, o Comitê Gestor de Governo Digital, chefiado pela Casa Civil e composto por titulares das secretarias, delibera sobre os temas relacionados à segurança da informação, sendo assessorado diretamente pelo Comitê Executivo de Governo Digital.

A Superintendência de Gestão e Inovação (SGI) da Secretaria de Administração (SAEB), através da Diretoria de Gestão Estratégica de TIC (DGETIC), gerencia atividades e projetos de segurança da informação para o poder executivo estadual, além de propor normas e padrões sobre o tema. A DGETIC analisa tecnicamente todas as contratações de TIC do poder executivo estadual, inclusive a revisão dos aspectos de segurança da informação, e acompanha a implementação das ações de segurança, garantindo a transformação digital segura e a continuidade dos serviços públicos digitais.

A SGI também atua através do Comitê dos Gestores de Tecnologias de Informação e Comunicação do estado da Bahia (FORTIC), composto por servidores de diversos órgãos estaduais e pela PRODEB. Trata-se de um fórum para discutir temas de TIC que conta com um grupo de trabalho específico para temas de segurança da informação. As proposições elaboradas pelo FORTIC são validadas pela SGI/DGETIC e resultam em atos normativos e publicações sobre segurança da informação.

A SGI, através do Conselho de Qualidade do Serviço Público (CONQUALI), aprovou e publicou a Resolução CONQUALI nº 001/2018, contendo a Política de Tecnologia da Informação e Comunicação – TIC, constituída por um conjunto de objetivos, princípios e diretrizes que visam alinhar as ações e a utilização dos recursos de TIC às estratégias da administração pública. Uma das diretrizes é a definição e implementação de normas e padrões de segurança da informação para os serviços e aplicações de TIC.

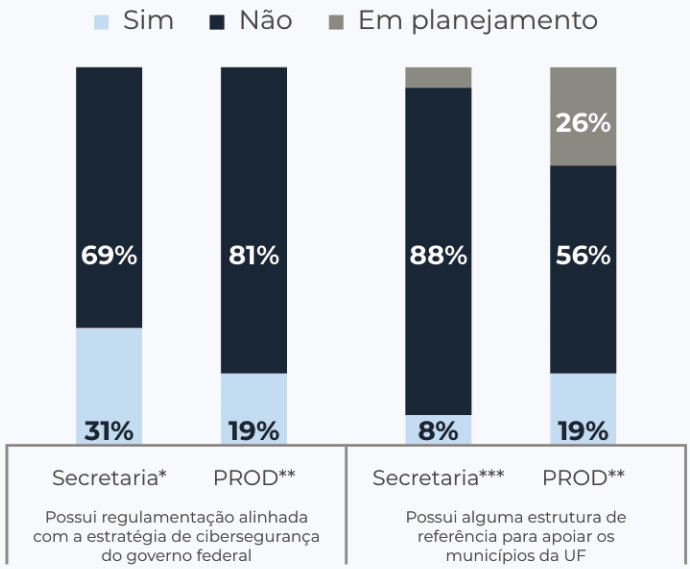
O estado também conta com a PRODEB, a companhia de processamento de dados do estado da Bahia, empresa pública estadual, parte integrante da administração indireta do estado. Na PROD, a área de segurança da informação e conformidade com a LGPD está vinculada à Diretoria Executiva, conforme o organograma abaixo:



Fonte: Decretos nº 21.451, de 9/6/2022 e nº 22.269, de 6/9/2023, nº 13.473, de 28/11/2011, e resolução CONQUALI nº 001/2018.

6. A coordenação federativa e o intercâmbio de informações em temas de cibersegurança entre a União, as UFs e os municípios continuam enfrentando desafios para se concretizar. Constatou-se que 69% das secretarias dos estados e 81% das PRODs afirmaram que não existe em sua UF uma regulamentação formalmente alinhada ou em conformidade com os princípios, diretrizes, normas, procedimentos, controle ou ações da estratégia nacional de cibersegurança do governo federal e política nacional de cibersegurança (Decreto nº 11.856/2023). Além disso, 88% das Secretarias de Estado da Administração e 56% das PRODs informaram que não existe nenhuma estrutura de referência estadual para apoiar os municípios do seu estado no tratamento e troca de informações de incidentes cibernéticos (ver Gráfico 6).

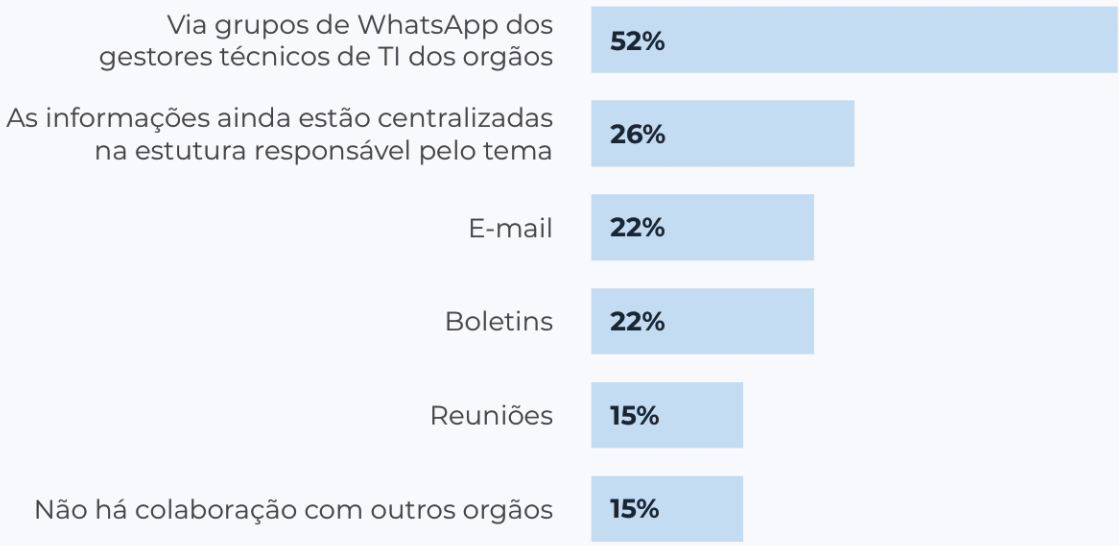
Gráfico 6 – Coordenação federativa



*N=26 UFs (questionário do CONSAD)
**N=27 UFs (questionário da ABEP)
***N=24 UFs (questionário do CONSAD)

7. O compartilhamento de informações sobre ameaças cibernéticas e incidentes entre as PRODs e os órgãos estaduais permanece concentrado em canais informais, como o WhatsApp. O aplicativo foi citado por 52% dos respondentes como um dos canais utilizados para o compartilhamento de informações sobre ameaças cibernéticas. Com relação a canais mais formais, as taxas de uso são menores. Apenas 15% indicam reuniões periódicas para esse tipo de compartilhamento, e 22% indicam o uso de boletins com fonte de troca de informações. Também vale notar que 26% informaram que centralizam as informações de ameaças e incidentes, e 15% não fornecem nenhum tipo de informação a outros órgãos (ver Gráfico 7).

Gráfico 7 – Compartilhamento de informações sobre ameaças cibernéticas ou incidentes de SI entre a PROD e os órgãos estaduais



N=27 PRODs (questionário da ABEP)
Resposta múltipla

BOAS PRÁTICAS

Comunicação e intercâmbio de informações

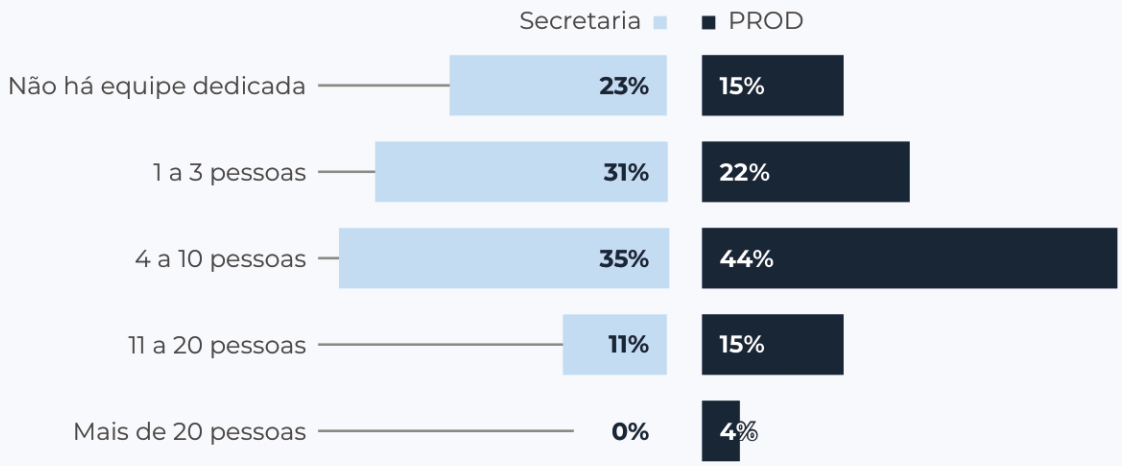
- Embora o uso de WhatsApp e canais extraoficiais possa ter benefícios para facilitar a comunicação entre diferentes partes, uma boa prática é o uso de plataformas automatizadas, como a MISP – *Malware Information Sharing Platform*. Um *benchmarking* reconhecido internacionalmente é o caso do CCN-CERT na Espanha, que desenvolveu o REYES, um núcleo de informações baseado na tecnologia da MISP. O REYES é uma solução desenvolvida para acelerar o trabalho de análise de ciberincidentes e o compartilhamento de informações, incluindo também comunidades autônomas e municípios. Através de um portal centralizado de informações, a solução é alimentada por diferentes fontes de informação, especialmente analisadas e escolhidas. Ademais, também se criam relações de inteligência entre diferentes indicadores e eventos que permitem ao analista estabelecer uma visão mais clara dos criminosos cibernéticos. O REYES também processa e analisa as informações, mostrando ao analista as mais relevantes. Vale destacar que, para além da instalação de uma ferramenta, o que agrega valor ao processo é a criação de uma comunidade de prática e colaboração ativa entre os participantes.

- A ISO/IEC 27001:2022 inclui controle sobre o relato de informações sobre eventos de segurança da informação, indicando que devem ser informados por meio de canais de gestão apropriados.

8. Nos últimos cinco anos, os estados avançaram na composição de suas equipes de cibersegurança, embora permaneçam alguns desafios em relação ao capital humano nos órgãos dos executivos estaduais. Entre as secretarias pesquisadas, 23%[10] informaram que não têm equipe dedicada, e 31% têm equipes de até três pessoas (ver Gráfico 8).

9. As PRODs ajudam a preencher as lacunas de capital humano dos órgãos executivos estaduais, mas também enfrentam desafios de subdimensionamento em suas equipes. Dos seis executivos estaduais que relataram não ter uma equipe de cibersegurança dedicada, quatro possuem essas equipes nas PRODs estaduais. Já dois estados não têm equipes dedicadas nas secretarias nem nas PRODs. Além disso, ao considerar apenas as PRODs, 14,8% não têm uma equipe de cibersegurança dedicada, e 66% têm equipes com menos de dez pessoas, evidenciando a necessidade de mais recursos humanos especializados (ver Gráfico 8).[11] Embora com metodologia ligeiramente diferente, pesquisa feita pelo BID em 2020, também em parceria com GTD.GOV, havia revelado que 19,2% dos estados contavam com equipes exclusivamente dedicadas ao tema, 26,9% com equipes parcialmente dedicadas e 53,8% não contavam com equipes dedicadas. Os dados desta pesquisa, em comparação com os dados de 2020, revelam avanços importantes na composição das equipes estaduais de cibersegurança nos últimos cinco anos.[12]

Gráfico 8 – Tamanho das equipes de cibersegurança nas secretarias e PRODs



N=26 UFs (questionário do CONSAD) e 27 PRODs (questionário da ABEP)

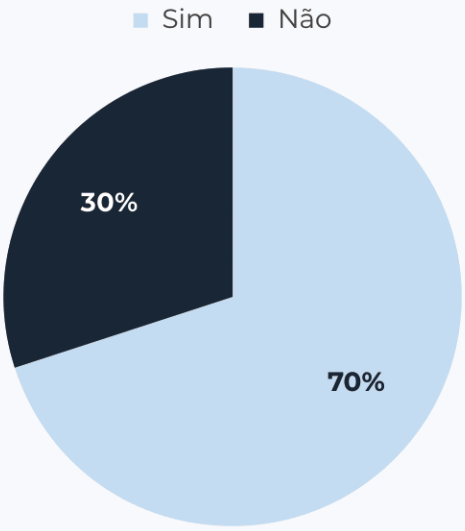
10 Um estado não respondeu e não foi considerado para essa questão (N=26).

11 Esta pesquisa não perguntou explicitamente sobre os serviços de cibersegurança prestados por meio de contratos com o setor privado, o que poderia indicar a ampliação da capacidade de cibersegurança de um estado por meio de equipes terceirizadas. Futuras pesquisas poderiam aprofundar o papel do setor privado nos arranjos dos estados, bem como a relação com os serviços prestados pelas PRODs.

12 M. Lafuente, R. Leite, M. Porrúa e P. Valenti. (2021). *Transformação digital dos governos brasileiros: Tendências na transformação digital em governos estaduais e no Distrito Federal do Brasil.* https://doi.org/10.18235/0003009

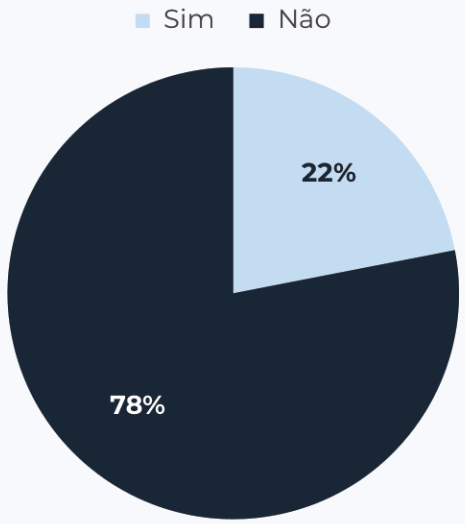
10. Enquanto 70% das UFs contam com ao menos um analista de cibersegurança, apenas 22% possuem um Chief Information Security Officer (CISO). Ao observar o tipo de perfil profissional, independentemente da quantidade, nota-se que há uma presença maior de analistas de cibersegurança, em comparação com perfis mais especializados ou de hierarquia mais alta, o que ilustra a falta de liderança institucional nessa área (ver Gráficos 9 e 10).

Gráfico 9 – UFs com analistas de cibersegurança



N=26 UFs (questionário do CONSAD)
N=27 UFs (questionário da ABEP)
Considerou-se que sim quando pelo menos um dos dois respondeu que sim.

Gráfico 10 – UFs com CISO (na PROD ou nas secretarias)



N=26 UFs (questionário do CONSAD)
N=27 UFs (questionário da ABEP)

BOAS PRÁTICAS

Equipes e perfis profissionais

- É fundamental contar com equipes dimensionadas corretamente, além de perfis profissionais adequados para ter as habilidades e competências necessárias para fazer frente às ameaças cibernéticas, inclusive perfis mais operacionais, gerenciais e de liderança. Entre os exemplos de abordagens que podem ser seguidas estão o Modelo de estrutura da força de trabalho para a cibersegurança (NICE Framework), do NIST, e o Modelo de estrutura europeia de habilidades em cibersegurança (ECSF), da ENISA. O GTD.GOV está trabalhando em uma proposta adaptada para a realidade dos governos estaduais brasileiros.

- Os tamanhos das equipes variam nas diferentes organizações. Como referência internacional, foram destacadas abaixo algumas agências nacionais e seus respectivos tamanhos, além de um exemplo subnacional:

PAÍS	ORGANIZAÇÃO	CAPITAL HUMANO APROXIMADO	POPULAÇÃO APROXIMADA
Itália	Agência para a Cibersegurança Nacional (ACN)	165	59 milhões
Coreia	Agência da Internet e Segurança da Coreia (KISA)	+800	51 milhões
	Centro Nacional de Segurança Cibernética (NCSC)	+400	
Espanha	Instituto Nacional de Segurança Cibernética da Espanha (INCIBE)	160	48 milhões
	Centro Criptológico Nacional – Equipe de Resposta a Emergências de Computadores (CCN-CERT)	+200	
	Ayuntamiento de Madrid	23	3,5 milhões
Israel	Diretoria Nacional de Cibersegurança (INCD)	~300	10 milhões

4.

RECOMENDAÇÕES

Considerando o diagnóstico analisado, apresentam-se as seguintes recomendações para fortalecer os níveis de cibersegurança nos estados brasileiros:

1. **Definir o arranjo institucional e os mecanismos de governança da segurança da informação e cibernética em nível estadual.** Devido à necessidade de promover uma visão conjunta e coordenar múltiplos atores a partir de dentro e fora do governo estadual, é imprescindível contar com três elementos principais para fortalecer a institucionalidade de cada estado na agenda de segurança da informação e cibernética: (i) política; (ii) autoridade; e (iii) modelo de governança, conforme segue:

   i. **Publicação de uma política de segurança da informação e cibernética.** Uma política estadual com alcance transversal é fundamental para guiar as ações de cada estado, comunicando claramente a todos os envolvidos as metas, as diretrizes e os princípios que nortearão os esforços. Além disso, recomenda-se que, aproveitando o movimento de atualização da estratégia nacional de cibersegurança, os estados editem suas políticas em alinhamento com as diretrizes federais, de forma a fortalecer a agenda e obter ganhos de escala.

   ii. **Definição de uma autoridade estadual de segurança da informação e cibernética.** A definição de uma autoridade estadual com mandato, poderes, equipe dedicada e orçamento definido é essencial para fortalecer a cibersegurança do estado. Essa estrutura deve ter a implementação da estratégia como parte do seu mandato, além do estabelecimento de políticas, diretrizes e mecanismos para estruturar um programa estadual efetivo de cibersegurança. Pode ser criada de forma vinculada à estrutura da governança da TI, da transformação digital ou da gestão de riscos do estado, por exemplo.

   iii. **Estabelecimento de um modelo de governança adequado com mecanismos claros de coordenação.** Além da definição da autoridade responsável, é essencial estabelecer mecanismos de coordenação interssecretarial, além de mecanismos de coordenação adequados entre o poder executivo estadual e a PROD do estado. A criação de instâncias formais para tomar decisões vinculadas – por exemplo, os comitês interssecretariais e com participação das PRODs – pode ser um caminho para estruturar mecanismos colegiados de coordenação em um tema que exige colaboração entre os diferentes atores. Os comitês podem ser estruturados em diferentes níveis e ter diferentes composições, a depender das realidades de cada estado, incluindo a coordenação em nível executivo e operacional, além de grupos de trabalho técnico. No nível operacional, especialmente no gerenciamento de incidentes, os Centros de Operações de Segurança Cibernética (SOCs) são essenciais para melhorar as capacidades de detecção e resposta a incidentes, bem como é fundamental fortalecer o compartilhamento de informações e a cooperação no tratamento de incidentes de segurança da informação e cibernética. Nesse aspecto, é necessário estabelecer estruturas de SOC nos estados e contar com canais de comunicação seguros entre as entidades, incluindo o uso de plataformas como a MISP, que vêm se expandindo nos estados brasileiros.

2. **Fortalecer o capital humano na área de segurança da informação e cibernética nas secretarias e nas PRODs.** Uma autoridade estadual de cibersegurança sem uma equipe com os perfis profissionais adequados e dimensionada às necessidades estaduais não é suficiente para fortalecer os níveis de cibersegurança. Dessa forma, de maneira vinculada à primeira recomendação, é fundamental estruturar processos de recrutamento, formação e manutenção de capital humano especializado, tanto no nível da gestão como no operacional. A definição dos perfis necessários, inclusive perfis de liderança e responsabilidade, é essencial. No quesito formação, a criação de trilhas de segurança da informação e cibernética, nas escolas de governo, é um bom caminho inicial para reaproveitar a estrutura existente.

3. **Adotar um Framework de maturidade em SI e privacidade estadual.** Para que haja avanços de forma consistente na agenda de segurança da informação e cibernética, é imprescindível que cada estado atualize periodicamente os dados da sua situação. Para isso, recomenda-se a adoção de frameworks ou boas práticas estabelecidas no mercado, como os ISO da família 27k, o NIST ou CIS, ou outros frameworks coerentes, como o de segurança da informação e privacidade, desenvolvida pela Secretaria de Governo Digital (SGD). De forma a fortalecer a coordenação federativa, é benéfico que os frameworks adotados sejam padronizados entre os estados, de forma a permitir comparações e medir o progresso de forma consistente.

4. **Fortalecer a coordenação federativa em cibersegurança.** A coordenação federativa e o intercâmbio de informações na área de cibersegurança entre a União, as UFs e os municípios devem ser fortalecidos para gerar ganhos de escala e aumentar a resiliência do Brasil. Tanto no nível estratégico (por exemplo alinhando as estratégias de cibersegurança), como no operacional (por exemplo, compartilhando informações sobre incidentes), a cooperação entre os diferentes níveis da federação é essencial para o país. Para as entidades que já contam com equipes de tratamento de incidentes de SI formalizadas, a Rede de Tratamento de Incidentes do Governo Federal (ReGIC) pode ser uma estratégia de integração da entidade ou do estado. Para aquelas que já têm a área de segurança da informação, mas não formalizaram ainda sua ETIRs, recomenda-se formalizá-las.

5. ANEXO METODOLÓGICO

Para mapear as configurações organizacionais nas 27 UFs brasileiras, esta pesquisa foi estruturada em três dimensões: (1) regulamentos, políticas e estratégias; (2) institucional, organizacional e governança; e (3) capital humano.

O processo de coleta de dados se deu em duas fases: na primeira fase, foi realizada uma pesquisa documental prévia, a qual, além de servir para estruturar as perguntas do questionário, também funcionou como fonte de referência para a arcabouço legal das UFs – esse processo ocorreu durante o mês de fevereiro de 2024. A segunda fase da coleta de dados, a mais robusta, se deu por meio de questionário aplicado às 27 UFs brasileiras, durante o período de 05 a 20 de março de 2024, utilizando a plataforma *JotForm*. Para validar o instrumento de coleta de dados, foi realizado um teste com três UFs: os estados do Amapá, Mato Grosso do Sul e Paraná.

Para coletar as características inerentes à tecnologia e à gestão, foram estruturados dois questionários distintos, um para as entidades estaduais e públicas de tecnologia da informação e comunicação (as PRODs), com 15 perguntas, e outro, direcionado às Secretarias de Estado da Administração das 26 UFs e do Distrito Federal, com 22 perguntas. Os questionários foram enviados pela ABEP-TIC e pelo CONSAD aos seus respectivos pontos focais nas 27 UFs.

Para a fase de coleta de dados, a dimensão “regulamentos, políticas e estratégias” teve como escopo a identificação das atuais normativas, políticas e estratégias de segurança da informação e cibernética existentes nos 26 estados e no Distrito Federal. Para abranger os mecanismos de regulação, fiscalização e controle, revisão e atualização das políticas no cenário de segurança cibernética, essa dimensão foi estruturada com seis perguntas direcionadas às PRODs e onze para as Secretarias Estaduais de Administração.

A dimensão “institucional, organizacional e governança” teve como escopo identificar as atuais estruturas organizacionais que apoiam a segurança da informação e a segurança cibernética dos estados e do Distrito Federal. As perguntas abordaram a configuração das estruturas organizacionais e a presença de equipes dedicadas ao tema. Para abranger os mecanismos de regulação, fiscalização e controle, revisão e atualização das políticas no cenário de segurança cibernética, essa dimensão foi estruturada com seis perguntas direcionadas às PRODs e oito para as Secretarias Estaduais de Administração.

Igualmente, para a dimensão “capital humano”, que teve como escopo levantar o contingente de recursos humanos responsável pelo tema de segurança cibernética nos estados e no Distrito Federal, essa dimensão foi estruturada com três perguntas direcionadas tanto às PRODs quanto às Secretarias Estaduais de Administração.

Todas as 27 UFs brasileiras responderam ao questionário, tanto pela ABEP-TIC como pelo CONSAD, exceto o estado do Pará, que não respondeu pelo CONSAD, totalizando 53 respostas, das 27 PRODs e das 26 secretarias de estado.

Após a consolidação dos dados, foram extraídas as respostas duplicadas de algumas UFs. Para analisar os dados, foi utilizada a técnica da análise de conteúdo. Algumas UFs foram contactadas durante a fase de análise dos dados, por telefone, para complementar e/ou sanar dúvidas pontuais sobre alguns dados discrepantes.

ANIC

AGENCIA NACIONAL DE INTELIGENCIA
E CIBERSEGURANCA