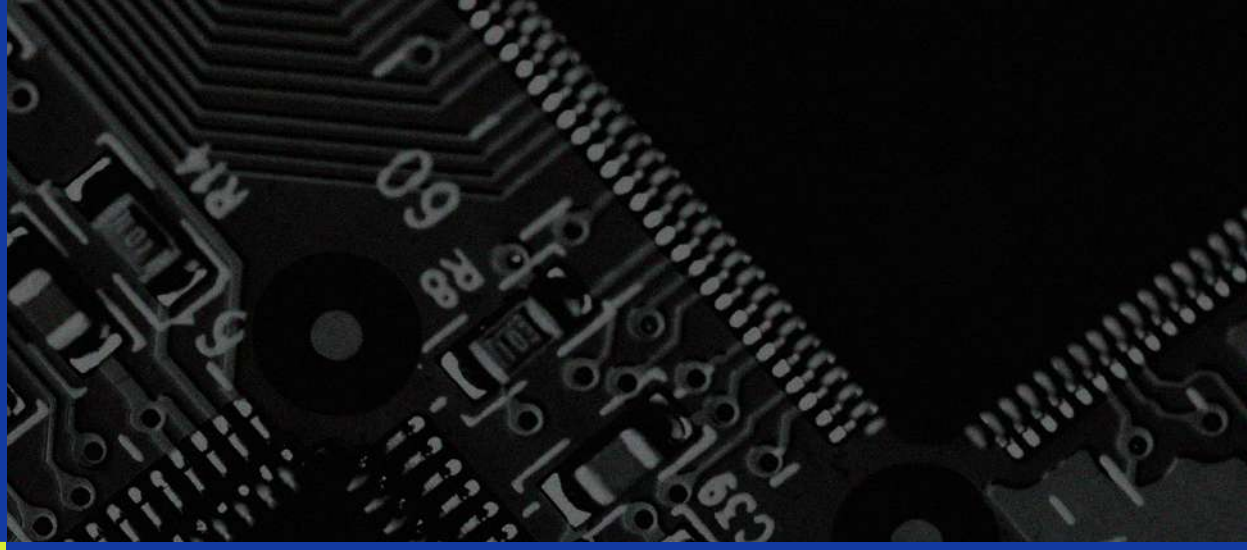


Instituto de Pesquisa em Direito & Tecnologia do Recife

Internet Society Capítulo Brasil

Criptografia e direitos fundamentais no Brasil: um mapeamento das políticas do Poder Executivo

Criptografia e direitos fundamentais no Brasil: um mapeamento das políticas do Poder Executivo

Março de 2026.

Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec

Internet Society Capítulo Brasil – ISOC Brasil

Este estudo faz parte do projeto Criptografia e Direitos Digitais no Brasil: Capacitação, Diálogo e Incidência Política, iniciativa apoiada pela ISOC Foundation por meio do programa Beyond the Net.

Pesquisa e redação

Luana Batista

Raquel Saraiva

Rhaiana Valois

Coordenação e revisão

Raquel Saraiva

Projeto gráfico

Estúdio Puya

Sumário

1. Contexto

2. Metodologia

3. Análise e Resultados

3.1. Panorama Geral

3.2. Análise da Dimensão Jurídico-Normativa

3.3. Análise da Dimensão Técnico-Operacional

4. Conclusões e Recomendações

Anexo - Lista de documentos analisados

1. Contexto

No contexto da Conferência das Partes da Convenção-Quadro das Nações Unidas sobre Mudança do Clima (COP 30), realizada em Belém, no ano passado, diversos países assinaram a Declaração sobre a Integridade da Informação sobre Mudança do Clima, a qual, dentre outras disposições, afirma a necessidade de criação e implementação de políticas públicas alinhadas ao direito internacional dos direitos humanos, capazes de promover a integridade da informação e, simultaneamente, respeitar e proteger direitos como a liberdade de expressão e o acesso à informação. O documento também enfatiza a obrigação de garantir a segurança de jornalistas que cobrem a pauta ambiental, cientistas, pesquisadores, defensores e outras vozes públicas[1].

A integridade da informação constitui, nesse sentido, um pressuposto essencial para o funcionamento da democracia contemporânea. Não se trata apenas da veracidade de conteúdos, mas da existência de condições institucionais e técnicas que permitam a produção, circulação e preservação de informações livres de manipulação, intimidação ou interferência indevida, além da proteção de ativistas e defensores dos direitos humanos.

Nesse contexto, a criptografia assume papel central. Não apenas como ferramenta técnica, responsável por confidencialidade, integridade e autenticidade nas comunicações digitais, mas também para permitir as condições materiais para o exercício de direitos, como o de liberdade de expressão, de associação e de reunião, especialmente em ambientes marcados por vigilância estatal ou privada. Em contextos autoritários ou de erosão democrática, a ausência de proteção criptográfica robusta expõe defensores de direitos humanos e ativistas a riscos concretos de perseguição, intimidação e silenciamento.

No contexto brasileiro, a relevância dessa infraestrutura técnica se torna ainda mais evidente diante de dados que mostram que o país figura entre o quarto

[1] Brasil. Secretaria de Comunicação Social da Presidência da República. *Declaração sobre a Integridade da Informação sobre Mudança do Clima*. Assinado em 12 de novembro de 2025. https://www.gov.br/secom/pt-br/assuntos/iniciativa-global/declaracao-sobre-a-integridade-da-informacao-sobre-mudanca-do-clima.

que mais mata ativistas de direitos humanos no mundo[2]. Além disso, de acordo com a Revisão da Capacidade de Segurança Cibernética - Brasil (2023), o grau de maturidade de cibersegurança do país ainda é desigual e carece de padronização sistêmica[3], o que pode acarretar sérios riscos não só para a privacidade e a proteção dos dados dos cidadãos brasileiros, bem como a soberania nacional, sobretudo em áreas críticas e estratégicas para o Brasil.

O levantamento demonstrou que setores regulados têm apresentado maior nível de implementação de controles técnicos e criptográficos, em conformidade com padrões internacionais[4]. Já nos setores não regulados, a adoção desses controles é variável e, muitas vezes, insuficiente. Além disso, observou-se que pequenas e médias empresas enfrentam limitações financeiras e técnicas que dificultam a implementação de mecanismos adequados de segurança, especialmente na configuração segura de serviços em nuvem.

O relatório também identifica a inexistência de um catálogo nacional de software seguro e a ausência de diretrizes uniformes para desenvolvimento e manutenção de sistemas seguros em todos os setores[5]. Embora haja avanços impulsionados pela Lei Geral de Proteção de Dados Pessoais, com a criação de centros de operações de segurança e maior uso de inteligência contra ameaças cibernéticas na esfera federal, essa maturidade não se reproduz de maneira homogênea nos níveis estadual e municipal[6]. O resultado é uma arquitetura de proteção fragmentada, que compromete tanto a segurança econômica quanto a proteção de direitos fundamentais no ambiente digital.

Em um cenário marcado ainda pela intensificação da crise climática global, da desinformação, do aumento das tensões entre as grandes potências globais e da crescente fragmentação tecnológica, a dependência de fornecedores estrangeiros

---

[2] Albuquerque, Beatriz. "Brasil é o 4º país que mais mata ativistas de direitos humanos". Radioagência Nacional, 2023. https://agenciabrasil.ebc.com.br/radioagencia-nacional/direitos-humanos/audio/2023-03/brasil-e-o-4o-pais-que-mais-mata-ativistas-de-direitos-humanos.

[3] Centro Global de Capacidade de Segurança Cibernética (GCSCC). *Revisão da Capacidade de Segurança Cibernética*. 2023. https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/eventos-anteriores/CMMreportBrazil2023_final_PT.pdf.

[4] Ibid.

[5] Ibid.

[6] Ibid.

pode gerar vulnerabilidades estruturais, comprometer a resiliência sistêmica e restringir a autonomia decisória do país no que concerne à proteção de dados e à segurança da informação. A assimetria tecnológica, nesse contexto, converte-se em fator de risco regulatório e estratégico. Nessa perspectiva, o investimento em infraestrutura criptográfica e o fortalecimento da cadeia nacional de segurança da informação configuram medidas estruturantes para a consolidação da soberania digital brasileira.

Com base nesse cenário, o presente mapeamento se propõe a examinar de que modo as políticas públicas editadas pelo Poder Executivo, no campo da criptografia, contribuem para a conformação de um ambiente normativo e tecnológico apto a assegurar a integridade informacional e a proteção de direitos fundamentais no Brasil, tanto no nível individual quanto coletivo, ou se, diversamente, perpetuam lacunas regulatórias e dependências estruturais capazes de fragilizar defensores de direitos, ativistas e, em última instância, a própria ordem democrática.

2. Metodologia

A elaboração deste relatório baseou-se em uma pesquisa documental qualitativa voltada ao mapeamento e análise do cenário normativo e institucional relacionado à criptografia no Brasil. A metodologia adotada combinou levantamento sistemático de documentos oficiais, organização estruturada das informações coletadas e análise substantiva à luz de parâmetros de direitos humanos.

A primeira etapa consistiu na identificação e coleta de documentos oficiais produzidos por órgãos do Poder Executivo federal que possam ter incidência direta ou indireta sobre o tema da criptografia, especialmente no contexto das comunicações digitais, da segurança pública e da proteção de dados. Foram considerados diferentes tipos de instrumentos normativos e de orientação institucional, incluindo leis, decretos, políticas públicas, marcos regulatórios, diretrizes estratégicas e documentos produzidos por agências reguladoras ou órgãos governamentais.

Para localizar documentos potencialmente relevantes, foram utilizadas combinações de palavras-chave relacionadas ao tema da criptografia e suas interfaces com políticas públicas de segurança, comunicações e privacidade. Entre os principais termos empregados na busca, destacam-se:

- criptografia + comunicações
- criptografia + plataformas digitais
- segurança + comunicações
- segurança + plataformas digitais
- privacidade + comunicações
- privacidade + plataformas digitais
- criptografia + segurança
- criptografia + privacidade

A utilização dessas combinações permitiu identificar documentos que tratam diretamente da criptografia, bem como políticas e diretrizes que abordam indiretamente o tema no contexto mais amplo da segurança da informação, cibersegurança e governança digital.

Após a organização e sistematização dos documentos coletados, foi realizada a análise qualitativa dos documentos selecionados. Para isso, os materiais foram examinados a partir de categorias temáticas que permitissem compreender como a criptografia aparece no contexto das políticas públicas brasileiras.

Por fim, os documentos foram avaliados sob a perspectiva dos direitos humanos, com atenção especial aos possíveis impactos das políticas e diretrizes identificadas sobre direitos fundamentais no ambiente digital. A análise considerou, entre outros aspectos, as implicações para a liberdade de expressão, o direito à privacidade e à proteção de dados pessoais, a segurança digital de indivíduos e comunidades e o acesso seguro a comunicações privadas. Os resultados dessa

análise fundamentam as recomendações de políticas públicas e estratégias de defesa de direitos apresentadas nas seções finais deste relatório.

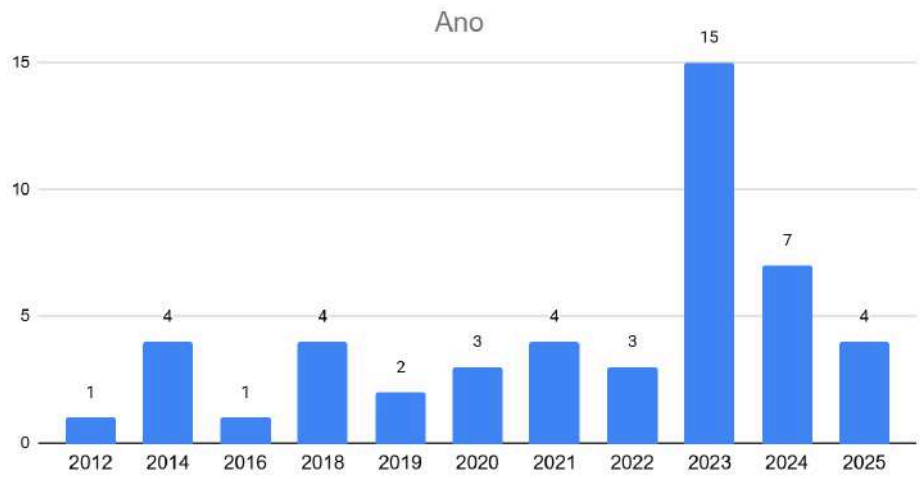
3. Análise e Resultados

3.1. Panorama Geral

A consolidação de uma política pública sobre criptografia não se revela apenas no conteúdo isolado dos atos normativos, mas no conjunto de instrumentos que, ao longo do tempo, estruturam a atuação estatal no campo da segurança da informação e da proteção de direitos no ambiente digital. Compreender esse arranjo exige olhar para além das declarações formais de princípios e examinar como diferentes órgãos do Poder Executivo têm incorporado o tema em decretos, resoluções, estratégias, guias técnicos e demais documentos.

Nesse contexto, o mapeamento realizado identificou um conjunto heterogêneo de documentos expedidos no âmbito do Poder Executivo que abordam a criptografia sob distintas perspectivas. A partir de uma abordagem quantitativa e qualitativa, foi possível examinar variações no padrão temporal, na linguagem empregada, diferenças quanto à força normativa dos atos, o modo como a criptografia e os direitos fundamentais foram mencionados e articulados, bem como o grau de abertura institucional para participação social.

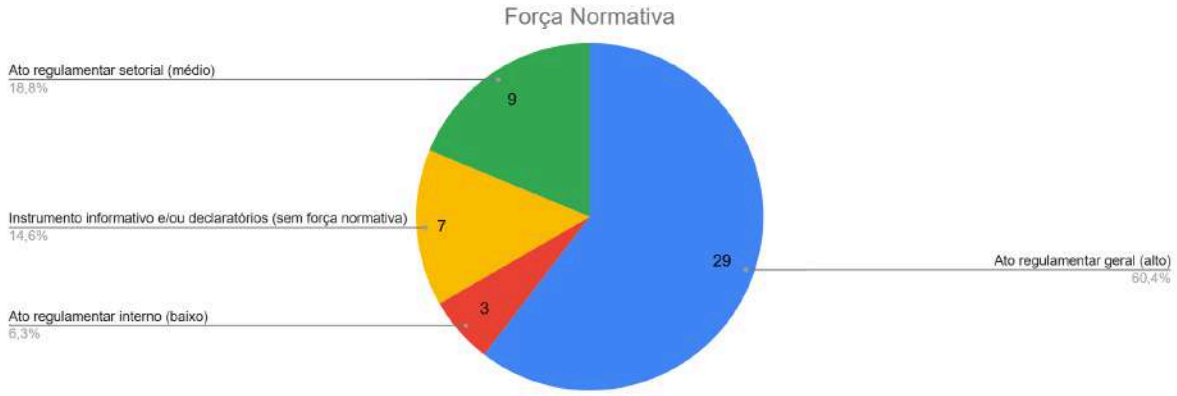
Dessa forma, foram analisados documentos produzidos entre 2012 e o primeiro semestre de 2025, abrangendo diferentes momentos da agenda governamental relacionada à segurança da informação e proteção de dados. A distribuição temporal revela presença pontual e pouco sistemática do tema nos anos iniciais da série, seguida de um pico (15 documentos identificados) em 2023, ano de início de um novo mandato presidencial, o que sugere que mudanças na agenda governamental e na reformulação de políticas públicas podem ter impulsionado uma maior produção normativa e institucional.



Também se examinou a natureza dos instrumentos incluídos no mapeamento. Considerando que todos os instrumentos analisados foram editados pelo Poder Executivo, concluiu-se que possuem natureza predominantemente regulamentar e, portanto, infralegal. A partir dessa constatação, os instrumentos foram organizados conforme o nível de força normativa que exercem no ordenamento administrativo, distinguindo-se: (i) atos regulamentares gerais, de alto grau de força normativa dentro do universo considerado; (ii) atos regulamentares setoriais, de força normativa intermediária, voltados à disciplina de áreas ou setores específicos; (iii) atos regulamentares internos, de baixo grau de força normativa, destinados principalmente à organização administrativa; e (iv) instrumentos informativos e declaratórios, desprovidos de força vinculante, utilizados sobretudo para fins de registro, análise ou orientação técnica.

A distribuição dos instrumentos identificados mostra a predominância de atos regulamentares gerais, que representam 60,4% do conjunto analisado (29 documentos). Esses instrumentos indicam que a maior parte das diretrizes relacionadas ao tema é estabelecida por normas de alcance mais amplo no âmbito do Poder Executivo. Em seguida, aparecem os atos regulamentares setoriais, que correspondem a 18,8% (9 documentos). Os atos regulamentares internos, por sua vez, são voltados à organização administrativa e com menor alcance normativo, correspondem a 6,3% (3 documentos).

Por fim, os instrumentos informativos e declaratórios representam 14,6% (7 documentos) do total e desempenham função predominantemente analítica ou orientativa. Esse panorama sugere que o tratamento institucional do tema ocorre predominantemente por meio de instrumentos regulamentares de caráter geral, complementados por normas setoriais e, em menor medida, por instrumentos de gestão interna e documentos técnicos.



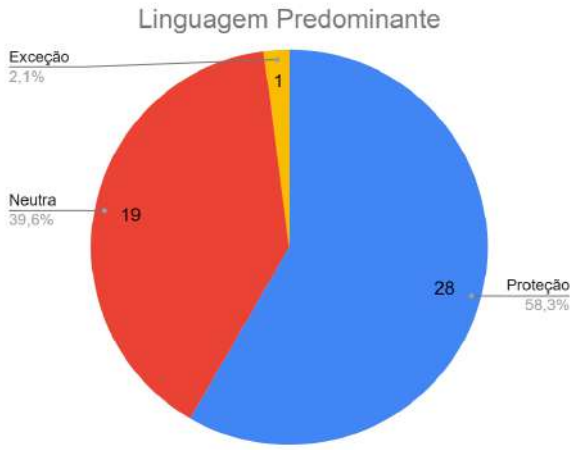
No plano discursivo, a análise concentrou-se na forma como a segurança digital é abordada nos documentos examinados em três categorias principais.

A primeira corresponde à linguagem neutra, na qual a segurança é tratada como requisito técnico ou operacional, sem juízo valorativo explícito quanto à sua função de proteção de direitos. A segunda refere-se à linguagem de proteção, que reconhece a segurança digital como mecanismo de garantia da confidencialidade, integridade e autenticidade das comunicações, associando-a à proteção de dados pessoais e a direitos fundamentais. A terceira consiste na linguagem de exceção, por fim, caracterizada por menções à necessidade de acesso estatal, flexibilização ou adoção de mecanismos que permitam, em determinadas circunstâncias, a mitigação de salvaguardas técnicas, inclusive com potencial superação da proteção criptográfica.

A distribuição dos documentos evidencia a predominância de linguagem orientada à proteção, presente em 58,3% dos casos (28 documentos). Em seguida, observa-se a ocorrência de linguagem neutra, identificada em 39,6% dos documentos (19 casos). A linguagem de exceção aparece de forma residual,

correspondendo a 2,1% do conjunto analisado (1 documento), de natureza meramente declaratória.

Esses resultados indicam a predominância de formulações discursivas vinculadas à proteção de direitos e garantias fundamentais, ainda que, em muitos casos, não explicitem de forma clara as ferramentas técnicas responsáveis por viabilizar a efetiva proteção desses direitos.

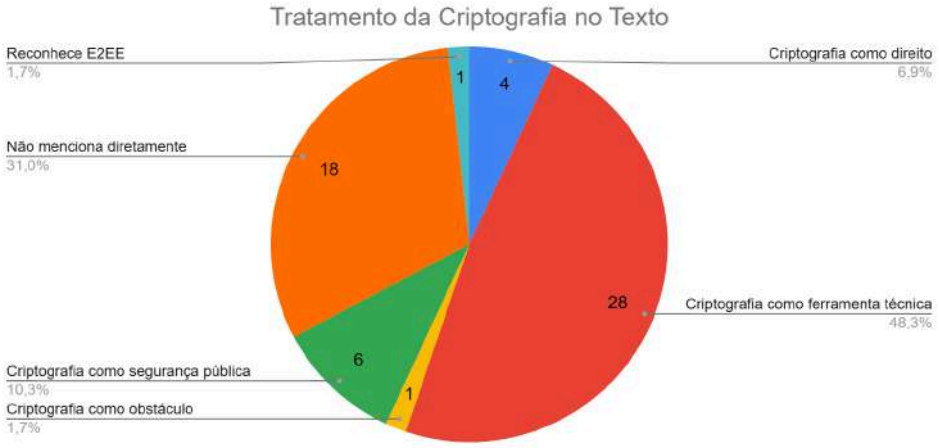


No que se refere ao tratamento da criptografia no texto, a análise indica predominância de sua abordagem como ferramenta técnica. No caso, foram identificados 28 documentos (48,3%) que tratam a criptografia dessa forma, posicionando-a sobretudo como recurso instrumental da gestão da segurança da informação. Nesse conjunto, a criptografia é apresentada como mecanismo operacional voltado à implementação de controles de segurança, conformidade normativa e gestão de riscos, sem associação direta a garantias de direitos.

Em proporção menor, a criptografia é tratada como expressão de direito ou garantia, sendo vinculada à proteção da confidencialidade das comunicações e à tutela de liberdades individuais. Essa abordagem aparece em 4 documentos (6,9%). Também se observa sua associação à segurança pública, presente em 6 documentos (10,3%), especialmente em textos que a inserem no contexto de proteção institucional e de infraestrutura crítica. Há ainda 18 documentos (31%) que não mencionam diretamente a criptografia, aspecto que merece atenção, pois indica

uma dissociação entre o discurso de proteção e a explicitação dos mecanismos técnicos que a viabilizam.

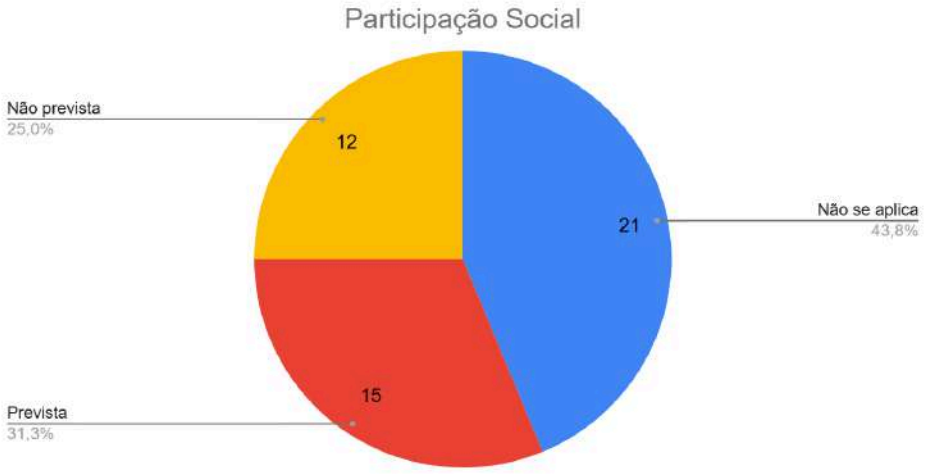
Em casos residuais, 1 documento (1,7%) apresenta a criptografia como obstáculo, sugerindo tensão entre proteção da informação e atividades de investigação ou controle, enquanto 1 documento (1,7%) reconhece explicitamente a criptografia de ponta a ponta (E2EE) como mecanismo relevante de proteção das comunicações.



Quanto aos direitos fundamentais mencionados, a análise revela uma distribuição heterogênea dos direitos mencionados. As menções mais frequentes dizem respeito à segurança nacional, que corresponde a 32,5% do total (40 ocorrências), indicando a relevância dessa dimensão no enquadramento institucional das políticas relacionadas à segurança da informação. Em seguida aparecem as referências à proteção de dados, com 28,5% (35 ocorrências), e à privacidade, com 22,0% (27 ocorrências), categorias que refletem necessidade de salvaguarda de direitos individuais no ambiente informacional.

Ainda no plano qualitativo, a análise considerou a presença de participação social como indicador de transparência e legitimidade democrática. Entre os documentos analisados, 21 (43,8%) foram classificados como “não se aplica”, por se tratarem de instrumentos técnicos ou administrativos que não prevêem mecanismos participativos; 15 (31,3%) apresentam previsão de participação social, ainda que frequentemente de modo genérico e 12 (25%) não preveem qualquer forma de participação.

Nesse ponto, observou-se que a previsão de espaços formais de consulta ou manifestação externa aparece de forma variável, indicando que a abertura à contribuição social não constitui prática uniforme na formulação dos atos examinados ou quando prevista, limita-se muitas vezes a dispositivos vagos, sem o detalhamento como a participação social será efetivada na prática, o que pode indicar uma reprodução meramente formal.



3.2. Análise da Dimensão Jurídico-Normativa

A partir dessa análise, tornou-se também possível avaliar como o conjunto de instrumentos normativos identificados (decretos, resoluções e portarias) contribui para um ambiente apto a assegurar a integridade da informação e a proteção de direitos fundamentais. O mapeamento revelou, nesse sentido, uma densidade regulatória relevante nos mecanismos de segurança das comunicações e de consolidação da confiança digital. Nesse cenário, princípios e diretrizes convergem para a criptografia como um pressuposto técnico central, ainda que sua menção nem sempre ocorra de forma explícita e com o detalhamento técnico necessário para operacionalizar essa tecnologia na defesa de direitos.

No âmbito da Política Nacional de Segurança da Informação, originalmente instituída pelo Decreto nº 9.637/2018[7] e posteriormente alterada pelo Decreto nº 10.641/2021[8], estabeleceu-se uma estrutura normativa voltada à proteção, integridade, confidencialidade e disponibilidade das informações na administração pública federal. A política adotava uma linguagem predominantemente protetiva, centrada na governança da segurança da informação, na gestão de riscos e na salvaguarda de direitos fundamentais, como privacidade, proteção de dados pessoais, liberdade de expressão e acesso à informação.

Nesse contexto, a criptografia era reconhecida expressamente como instrumento técnico relevante, na medida em que o art. 17, §1º, I, do Decreto nº 9.637/2018 previa a utilização de recursos criptográficos adequados aos graus de sigilo exigidos no tratamento das informações. A previsão conferia densidade normativa à proteção da informação, ao vincular diretamente a efetivação dos direitos e princípios da política à adoção de mecanismos técnicos capazes de garantir confidencialidade, integridade e autenticidade das comunicações e dados.

---

[7] BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), dispõe sobre a governança da segurança da informação e altera o Decreto nº 2.295, de 4 de agosto de 1997. 2018.https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm

[8] BRASIL. Decreto nº 10.641, de 2 de março de 2021. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997. 2021.https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10641.htm

A atualização da política por meio do Decreto nº 12.572/2025 manteve a centralidade da governança da segurança da informação, da gestão de riscos e da proteção de dados pessoais, reafirmando a necessidade de assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações e ativos informacionais da União[9]. Todavia, a nova redação não preservou a menção explícita à utilização de recursos criptográficos. Essa omissão representa um ponto crítico do ponto de vista normativo, pois a criptografia constitui um dos principais mecanismos técnicos para concretizar os objetivos declarados da política.

Ao retirar essa referência, o decreto reduz o grau de precisão técnica do instrumento normativo e pode enfraquecer a clareza quanto às ferramentas necessárias para operacionalizar a proteção da informação. Observa-se também uma alteração na dimensão participativa da política, uma vez que o modelo de 2018 previa abertura para contribuições da sociedade civil na formulação da estratégia nacional de segurança da informação, enquanto o decreto de 2025 concentra a implementação da política em estruturas internas da administração pública.

Uma dinâmica semelhante pode ser observada na Política Nacional de Cibersegurança, instituída pelo Decreto nº 11.856/2023[10]. O instrumento estabelece diretrizes voltadas à proteção, integridade, confidencialidade, disponibilidade e autenticidade das informações no ambiente digital, adotando uma abordagem predominantemente preventiva e protetiva. Embora seus princípios e objetivos pressuponham a adoção de mecanismos técnicos voltados à mitigação de riscos cibernéticos e à proteção das comunicações, o decreto também não menciona expressamente a criptografia. No Relatório da Audiência Pública GSI 01/2023 sobre o anteprojeto da Política Nacional de Cibersegurança, contudo, em grande parte das contribuições, destacou-se a necessidade de garantir a aplicação da criptografia como instrumento de proteção de direitos digitais, com gestão de chaves local para

[9] BRASIL. Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. 2025. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm

[10] BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023, que institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. 2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

assegurar a soberania dos dados e evitar mecanismos que comprometam sua eficácia[11].

Nesse caso, a ausência de referência direta à criptografia não implica necessariamente sua exclusão do campo de aplicação da política, mas reforça uma tendência de formulação normativa mais abstrata e menos detalhada quanto aos instrumentos tecnológicos envolvidos. Ainda assim, o decreto apresenta um elemento relevante ao instituir o Comitê Nacional de Cibersegurança e prever a participação de representantes da sociedade civil em sua composição, criando um espaço institucional de acompanhamento e contribuição para a formulação das políticas de segurança digital.

A Política Nacional de Inteligência, fixada pelo Decreto nº 8.793/2016, por sua vez, aborda a proteção da informação sob uma perspectiva distinta, vinculada à segurança do Estado e à prevenção de ameaças como espionagem e ataques cibernéticos. Embora o decreto não mencione expressamente a criptografia, trata da necessidade de resguardar a integridade e a confiabilidade de sistemas e dados estratégicos[12]. O texto estabelece que a atividade de inteligência deve observar os direitos e garantias fundamentais, mas não detalha mecanismos específicos para a proteção das comunicações ou dos dados. Ademais, o decreto não prevê mecanismos de participação da sociedade civil, concentrando a governança da política no âmbito das instituições estatais.

No campo da defesa, a Política Cibernética de Defesa introduz uma perspectiva estratégica e militar sobre o uso do espaço cibernético[13]. Diferentemente de diversos outros instrumentos analisados, o documento menciona expressamente a criptografia ao estabelecer a diretriz de criação de padrões interoperáveis para a defesa nacional. Contudo, a abordagem adotada é marcadamente operacional e estratégica, priorizando conceitos como guerra cibernética e capacidade ofensiva.

---

[11] *Relatório da Audiência Pública do GSI N° 01/2023 sobre a Política Nacional de Cibersegurança (PNCiber)*. 2023. https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/audiencia-publica/01-2023.

[12] BRASIL. Decreto nº 8.793, de 25 de julho de 2016. Fixa a Política Nacional de Inteligência. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

[13] BRASIL. Portaria Normativa do Ministério da Defesa nº 3.389, de 21 de dezembro de 2012. Política Cibernética de Defesa. 2012. https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/doutrina_militar/MD31P02PoliticaCiberneticadeDefesa1Ed2012.pdf/@@download/file

Nesse contexto, a segurança da informação é tratada como instrumento para garantir a liberdade de ação do Estado no domínio cibernético, enquanto a proteção de direitos fundamentais individuais não constitui eixo central da política. Além disso, o documento abre margem para o desenvolvimento de ferramentas de reconhecimento de artefatos digitais e para a condução de ações ofensivas no espaço cibernético, em conformidade com planejamentos militares. Essa orientação revela uma tensão estrutural entre a lógica da defesa nacional e a lógica de proteção de direitos que orienta outras políticas públicas analisadas, indicando que a governança da criptografia no país também é influenciada por perspectivas estratégicas que priorizam o êxito operacional e a capacidade de atuação estatal no domínio digital.

A Estratégia Nacional de Transformação Digital evidencia outra dimensão relevante da governança da criptografia no país. Na versão referente ao ciclo de 2018-2022[14], a estratégia buscava estabelecer as bases institucionais e regulatórias para a digitalização da economia e da administração pública, identificando lacunas normativas e destacando a necessidade de criação de um marco legal de proteção de dados. Nesse contexto, a criptografia já era tratada como tecnologia estratégica associada à certificação digital da ICP-Brasil e à garantia de autenticidade, integridade e validade jurídica de transações eletrônicas.

A revisão da estratégia para o ciclo 2022-2026 demonstra o amadurecimento institucional do país, incorporando avanços como a vigência da legislação de proteção de dados e o funcionamento da agora Agência Nacional de Proteção de Dados (ANPD) por sua implementação[15]. Nesse novo ciclo, a criptografia passa a ser tratada como tema prioritário de pesquisa, desenvolvimento e inovação, integrada a políticas de segurança cibernética e segurança da informação. Tal abordagem reforça a compreensão de que a criptografia não é apenas uma ferramenta técnica, mas um elemento estruturante da confiança digital e da soberania tecnológica.

---

[14] BRASIL. Estratégia Brasileira para a Transformação Digital - E-Digital. 2018. https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf.

[15] BRASIL. Estratégia Brasileira para a Transformação Digital - E-Digital (Ciclo 2022–2026). 2022. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf

Essa dimensão estratégica também se manifestava na Estratégia Nacional de Segurança Cibernética. O Decreto nº 10.222/2020 tratava a criptografia como elemento estruturante da governança cibernética nacional, vinculando seu uso à proteção de dados sensíveis, à segurança de serviços essenciais e à resiliência de infraestruturas críticas[16]. O decreto estabelecia que programas, processos e sistemas deveriam adotar recursos criptográficos compatíveis com o grau de sigilo das informações e com as restrições legais de acesso e compartilhamento, integrando a criptografia à gestão de riscos e à proteção de dados em trânsito e em repouso. Além disso, incentivava o desenvolvimento de soluções nacionais, a adoção de padrões internacionais e o fortalecimento da criptologia como área estratégica de pesquisa e inovação.

A substituição desse marco pelo Decreto nº 12.573/2025, que institui uma nova Estratégia Nacional de Cibersegurança, amplia o escopo institucional da política e enfatiza a soberania digital e a resiliência cibernética do Estado[17]. Entretanto, diferentemente da estratégia de 2020, a nova versão não menciona explicitamente a criptografia nem apresenta orientações técnicas detalhadas sobre seu uso. Essa mudança pode ser interpretada como um deslocamento da política de um nível técnico-operacional para um nível mais estratégico e institucional. Ainda assim, a ausência de referência direta à criptografia representa um enfraquecimento do detalhamento normativo sobre instrumentos essenciais para a proteção da informação e para a segurança das comunicações.

No plano regulatório setorial, o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, instituído pela Resolução nº 740/2020 da Anatel[18] e alterado pela Resolução nº 767/2024[19], estabelece obrigações de gestão de riscos, prevenção e resposta a incidentes para prestadoras de serviços de

[16] BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética - E-Ciber. 2020. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.
[17] BRASIL. Decreto nº 12.573, de 4 de agosto de 2025, que institui a Estratégia Nacional de Cibersegurança - E-Ciber). 2025. https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12573.htm#art12.
[18] Agência Nacional de Telecomunicações (Anatel). Resolução ANATEL nº 740, de 21 de dezembro de 2020. Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. 2020. https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740.
[19] Agência Nacional de Telecomunicações (Anatel). Resolução ANATEL nº 767, de 7 de agosto de 2024. Altera o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. 2024. https://informacoes.anatel.gov.br/legislacao/resolucoes/2024/1965-resolucao-767.

telecomunicações. Embora a criptografia também não seja mencionada explicitamente, a norma estrutura a proteção das redes e serviços a partir de princípios clássicos da segurança da informação, como confidencialidade, integridade, disponibilidade e autenticidade. A regulação adota uma abordagem voltada à mitigação de vulnerabilidades e à proteção de infraestruturas críticas, além de destacar a necessidade de respeito a direitos fundamentais, como privacidade, liberdade de expressão e proteção de dados dos usuários.

Outras políticas públicas complementam esse arcabouço institucional. A Política Nacional de Segurança de Infraestruturas Críticas, instituída pelo Decreto nº 9.573/2018, estabelece diretrizes para garantir a resiliência e continuidade de serviços essenciais, incorporando a segurança da informação e a gestão de riscos como elementos relevantes para a proteção desses sistemas[20]. A Estratégia Nacional de Governo Digital, instituída pelo Decreto nº 12.069/2024, enfatiza o compartilhamento seguro de dados e a necessidade de fortalecer a confiança nos serviços digitais prestados pelo Estado[21]. Já o Decreto nº 12.725/2025, que aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, destaca a importância da proteção de comunicações e infraestruturas críticas no contexto da defesa nacional, embora sem detalhar mecanismos técnicos específicos[22].

Em termos gerais, a análise conjunta desses atos revela uma convergência normativa voltada à segurança e à inviolabilidade das comunicações em rede. Observa-se que as políticas públicas brasileiras examinadas adotam uma postura predominantemente protetiva, priorizando a mitigação de riscos cibernéticos e a salvaguarda de garantias fundamentais. Prova disso é que, na quase totalidade do corpus analisado, inexistem previsões que autorizem explicitamente a quebra de

---

[20] BRASIL. Decreto nº 9.573, de 22 de novembro de 2018, que institui a Política Nacional de Segurança de Infraestruturas Críticas. 2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9573.htm.

[21] BRASIL. Decreto nº 12.069, de 21 de junho de 2024, que dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital - Rede Gov.br. 2024. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/Decreto/D12069.htm.

[22] BRASIL. Decreto nº 12.725, de 18 de novembro de 2025, que aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. 2025.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12725.htm#:~:text=DECRETO%20N%C2%BA%2012.725%2C%20DE%2018,Livro%20Branco%20de%20Defesa%20Nacional.

criptografia, a implementação de vulnerabilidades deliberadas ou a exploração de falhas em sistemas de segurança.

Contudo, essa evolução também apresenta ambiguidades. Isso porque, se, por um lado, alguns dos instrumentos anteriores reconheciam explicitamente a criptografia enquanto ferramenta central para a proteção de dados e comunicações, suas versões mais recentes passaram a tratar a segurança da informação de forma mais genérica, sem referência direta a esse mecanismo técnico. Essa tendência pode reduzir a força normativa quanto às ferramentas necessárias para garantir a efetividade da proteção informacional e dos direitos fundamentais no ambiente digital.

Diante desse quadro, é possível concluir que o arcabouço normativo brasileiro contribui, em termos gerais, para a construção de um ambiente institucional voltado à proteção da integridade informacional e à preservação de direitos fundamentais. Todavia, a redução de referências técnicas explícitas à criptografia em instrumentos mais recentes e a coexistência de políticas que enfatizam estratégias ofensivas do domínio cibernético indicam a necessidade de maior coerência normativa. Dessa forma, o fortalecimento da proteção da informação e da confiança digital depende não apenas da afirmação abstrata de princípios, mas também da explicitação clara dos mecanismos tecnológicos que tornam esses princípios efetivamente operacionais.

3.3. Análise da Dimensão Técnico-Operacional

Na análise da dimensão técnico-operacional, evidencia-se a consolidação da criptografia como elemento estruturante das políticas de segurança digital no setor de telecomunicações e na Administração Pública federal. De modo geral, nos documentos examinados, a criptografia é quase sempre abordada como ferramenta técnica voltada à gestão de riscos, à proteção de ativos informacionais e ao cumprimento de requisitos regulatórios.

No âmbito da computação em nuvem, a Instrução Normativa nº 5, de 2021, estabelece requisitos mínimos de segurança para a administração pública federal, determinando a adoção de padrões de encriptação internacionalmente reconhecidos

e a priorização do uso de chaves baseadas em hardware sempre que possível[23]. A norma também exige que as chaves de encriptação sejam geradas e armazenadas pelo próprio órgão ou entidade contratante, reforçando a preservação da soberania sobre os dados e evitando a delegação integral do controle informacional aos provedores de nuvem. Ao mesmo tempo, a decisão de criptografar deve ser fundamentada em análise técnica que considere riscos, custos, benefícios e o grau de criticidade das informações. Embora tal previsão se alinhe a uma lógica de gestão baseada em risco, ela introduz margem de discricionariedade que pode, a depender da interpretação adotada, resultar em níveis diferenciados de proteção para categorias distintas de dados.

Essa lógica de operacionalização da segurança também se manifesta no Plano Setorial de Gestão de Incidentes Cibernéticos de 2022[24], que institucionaliza a criptografia como requisito para o tráfego seguro de informações no contexto da cooperação entre as Equipes de Tratamento e Resposta a Incidentes (ETIRs). O documento determina o uso de chaves públicas para a proteção de e-mails e arquivos classificados segundo o padrão *Traffic Light Protocol* (TLP), estruturando um modelo de compartilhamento protegido de alertas e indicadores de comprometimento. Contudo, a eficácia operacional desse plano enfrenta o desafio de cláusulas vagas, especialmente no que tange aos critérios de sanitização de dados pela Anatel antes do repasse à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), o que pode gerar incertezas técnicas sobre as garantias reais de privacidade dos usuários no fluxo dessas informações.

A dimensão técnico-operacional é complementada, ainda, pelos documentos de natureza orientativa, entre os quais se destacam o Guia Orientativo de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações (2023)[25]

---

[23] Gabinete de Segurança Institucional da Presidência da República (GSI). Instrução Normativa Nº 5, de 30 de agosto de 2021. 2021. https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684.

[24] Agência Nacional de Telecomunicações (Anatel). Plano Setorial de Gestão de Incidentes Cibernéticos. 2022. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYFCya2oAzHQYNhzkRRsnLjD-tN64mWeskgcU_hr34jetvMQ5TiPf52bMeBtGks3PGeZDvuAiDx4c81YqwzKpgd.

[25]Agência Nacional de Telecomunicações (Anatel). Guia Orientativo de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações. 2023. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZ2HzV7pQor_uuxREh18J3Uudb6CTERhXP0S4cd3uwKgaVaCTjFK3en6G5rF19eRcBOqoN2PCw94zGOYWsdmvHZ.

e o Guia Orientativo DevSecOps (2023)[26], ambos adotando uma abordagem protetiva.

O Guia Orientativo de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações apresenta escopo mais amplo de governança organizacional e conformidade regulatória. Ele recomenda a encriptação de dados em trânsito e em repouso como requisito essencial e dedica atenção significativa à governança organizacional, à gestão de riscos, à definição de políticas internas e à implementação de controles como retenção de *logs*, monitoramento de redes e detecção de intrusões. Seu escopo está fortemente associado à conformidade regulatória e à proteção de consumidores, especialmente para prestadoras com menor porte. Ainda que não vinculante, o guia estimula a adoção de mecanismos contínuos de registro e análise de eventos, o que pode ampliar a coleta e o armazenamento de metadados operacionais.

De forma similar, o Guia Orientativo DevSecOps apesar de ter um enfoque distinto na integração da segurança ao ciclo de vida do desenvolvimento de software, posicionando a criptografia como componente estrutural da arquitetura dos sistemas (e não apenas como requisito de conformidade), sob os princípios de *security by design* e *privacy by design*, o documento converge com o guia anterior quanto a promoção de práticas protetivas de monitoramento e retenção de registros operacionais.

Nesse contexto, é relevante destacar que, embora as medidas de monitoramento e registro sejam justificadas pela lógica de prevenção, detecção e resposta a incidentes cibernéticos de segurança, sua implementação demanda salvaguardas para evitar desvio de finalidade, acumulação desnecessária de dados ou expansão indevida de capacidades de inspeção. A governança técnico-operacional da segurança digital não se limita, portanto, à adoção de ferramentas, mas exige definição clara de limites, responsabilidades e controles institucionais.

---

[26] Agência Nacional de Telecomunicações (Anatel). DevSecOps Guia Orientativo. 2023. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYAHRbPZD4IyjHVrVE1lGFpJ0XBdoGuy3IvgTwNBzOeSHWwkbm0RTQYCZ3cNJiD3fF951IYCChNOxMQu5Ei2Gj2.

Além disso, cabe mencionar as Normas Complementares editadas pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República constituem um arcabouço técnico e normativo destinado a disciplinar o uso de recursos criptográficos no âmbito da Administração Pública Federal, tratando a criptografia como mecanismo essencial para a proteção do patrimônio informacional do Estado e para a garantia da integridade, confidencialidade e autenticidade das informações públicas.

A Norma Complementar nº 07/2014 aborda a criptografia principalmente como instrumento de proteção de sistemas de identificação e autenticação. No âmbito dessa norma, os dados biométricos recebem tratamento específico, sendo classificados como informações sigilosas e devendo ser protegidos preferencialmente por meio de mecanismos criptográficos[27]. Considerando que dados biométricos possuem natureza altamente sensível e características de irreversibilidade, a ausência de uma exigência normativa categórica representa um ponto de vulnerabilidade estrutural.

A norma também estabelece que aplicações voltadas ao controle de acesso e ao tratamento de informações sensíveis devem utilizar ativos de informação previamente homologados para a execução de funções criptográficas, de modo a garantir conformidade com padrões de segurança definidos pela administração pública. Além disso, os recursos criptológicos são classificados como ativos de nível crítico elevado, considerados de alto impacto institucional, uma vez que seu comprometimento pode acarretar interrupções na missão institucional dos órgãos públicos ou provocar danos significativos à segurança do Estado e da sociedade.

A Norma Complementar nº 09/2014, por sua vez, constitui o principal instrumento normativo específico sobre recursos criptográficos no âmbito da administração pública federal, estabelecendo conceitos, classificações e exigências metodológicas relacionadas ao uso de algoritmos criptográficos[28]. Um dos

---

[27] Gabinete de Segurança Institucional da Presidência da República (GSI). Norma Complementar nº 07/IN01/DSIC/GSIPR. 2014. https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-07IN01DSICGSIPR.pdf.

[28] Gabinete de Segurança Institucional da Presidência da República (GSI). Norma Complementar nº NC 09/IN01/DSIC/GSIPR. 2014.

elementos centrais dessa norma é a distinção entre algoritmo de Estado e algoritmo registrado. O algoritmo de Estado corresponde a soluções criptográficas desenvolvidas pelo próprio Estado brasileiro e não destinadas à comercialização, sendo de uso obrigatório para a proteção de informações classificadas nos graus reservado, secreto ou ultrassecreto. Já o algoritmo registrado refere-se a algoritmos cujo código-fonte pode ser auditado pelo GSI, sendo voltado à proteção de informações sigilosas que não se enquadram formalmente no regime de classificação previsto na legislação.

A norma também incorpora uma dimensão estratégica relacionada à soberania tecnológica, ao vedar a contratação de empresas ou profissionais externos para o desenvolvimento de algoritmos de Estado, admitindo exceções apenas quando se tratar de Empresas Estratégicas de Defesa que utilizem tecnologia nacional e atuem sob regime contratual sigiloso. Adicionalmente, o anexo técnico da norma estabelece parâmetros mínimos de segurança para diferentes métodos criptográficos, incluindo tamanhos de chave para algoritmos como RSA e curvas elípticas, bem como restrições quanto ao uso desses métodos para a proteção de informações classificadas no grau ultrassecreto, hipótese em que se exige a utilização de sistemas de chave única baseados em sequências aleatórias. A norma também explicita uma dimensão ética no uso de recursos criptográficos, proibindo sua utilização para interceptação indevida de dados de terceiros ou para a ocultação de conteúdos ilícitos ou antiéticos.

Por fim, a Norma Complementar nº 20/2014 incorpora a criptografia como medida de salvaguarda transversal que deve acompanhar a informação ao longo de todo o seu ciclo de vida, desde a produção até a transmissão[29]. No que se refere à produção e à custódia de documentos, a norma determina que informações classificadas devem ser geradas e mantidas sob proteção criptográfica baseada em algoritmos de Estado, em conformidade com os parâmetros definidos pela Norma Complementar nº 09.

---

https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-09IN01DSICGSIPR.pdf.

[29] Gabinete de Segurança Institucional da Presidência da República (GSI). Norma Complementar nº 20/IN01/DSIC/GSIPR. 2014. https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-20IN01DSICGSIPR.pdf.

Em relação ao armazenamento, estabelece-se a obrigatoriedade de utilização de criptografia compatível com o grau de sensibilidade da informação, sendo que, para documentos classificados nos graus secreto ou ultrassecreto, exige-se adicionalmente a adoção de mecanismos físicos de proteção, como cofres ou estruturas equivalentes de segurança. No que diz respeito à transmissão e à disseminação de informações, a norma determina que informações sigilosas em geral devem ser protegidas mediante o uso de algoritmos registrados, enquanto documentos classificados devem necessariamente utilizar algoritmos de Estado quando transmitidos por meios eletrônicos.

Em conjunto, os documentos analisados demonstram a institucionalização de uma governança técnico-operacional caracterizada pela padronização de controles, definição de procedimentos e incorporação da criptografia como infraestrutura essencial à proteção de dados, à resiliência cibernética e à coordenação interinstitucional. Ao mesmo tempo, revelam que as principais aberturas a potenciais impactos sobre direitos não decorrem de autorizações explícitas de flexibilização da criptografia, mas de cláusulas abertas, margens de discricionariedade técnica e práticas de monitoramento e retenção de dados que, sem salvaguardas ou especificações adequadas, podem afetar garantias de privacidade, proteção de dados e liberdade de comunicação.

4. Conclusões e Recomendações

Por todo o exposto, o mapeamento evidencia que o Brasil dispõe de um conjunto relevante de políticas públicas e instrumentos infralegais voltados à segurança da informação e à cibersegurança, predominantemente estruturados por atos regulamentares gerais de maior densidade normativa. Esse arranjo contribui para a institucionalização de padrões de proteção da informação no âmbito do Poder Executivo, com políticas que, no plano discursivo, tendem a enquadrar a segurança digital como mecanismo de proteção de direitos, especialmente da privacidade e da proteção de dados pessoais.

Apesar dessa orientação protetiva, a análise indica também que a criptografia é tratada majoritariamente como ferramenta técnica de gestão da segurança da informação, voltada à conformidade e à mitigação de riscos, sendo raramente

vinculada explicitamente à proteção de direitos individuais. Observa-se também uma dissociação relevante entre o discurso de proteção das comunicações e a explicitação dos mecanismos técnicos que a viabilizam.

Nesse contexto, destaca-se ainda que uma parcela significativa dos documentos analisados não menciona diretamente o uso de criptografia, inclusive entre instrumentos voltados diretamente à segurança digital e à cibersegurança. Além disso, observa-se o que documentos normativos mais recentes têm deixado de mencionar de forma explícita a criptografia, o que pode reduzir a clareza e a força normativa dos instrumentos tecnológicos necessários para proteger dados e comunicações. Embora os documentos não contenham previsões de quebra de criptografia ou criação de vulnerabilidades, alguns instrumentos apresentam cláusulas abertas ou margens de discricionariedade técnica que podem gerar incertezas quanto ao nível efetivo de proteção conferido aos dados.

Outro ponto de atenção refere-se à crescente ênfase em práticas de monitoramento, retenção de *logs* e análise de eventos operacionais como instrumentos de gestão de riscos e resposta a incidentes cibernéticos. Embora justificadas pela lógica de prevenção e resiliência institucional, essas medidas podem ampliar a coleta e o armazenamento de metadados sensíveis, exigindo salvaguardas institucionais claras. Por fim, a análise também aponta limitações na previsão de mecanismos estruturados de participação social na formulação e revisão dessas políticas.

Diante desse cenário, recomenda-se:

1. Fortalecer a explicitação normativa da criptografia em políticas e documentos estratégicos de segurança digital, reconhecendo-a como componente essencial da infraestrutura de confiança e da proteção de direitos fundamentais.
2. Promover maior alinhamento entre medidas técnico-operacionais de segurança e princípios de proteção de direitos, assegurando que estratégias de resiliência cibernética sejam compatíveis com garantias de privacidade, proteção de dados e liberdade de comunicação.
3. Aprimorar critérios normativos para decisões baseadas em análise de risco, reduzindo margens excessivas de discricionariedade técnica em instrumentos regulatórios.

4. Estabelecer limites claros para práticas de monitoramento e retenção de dados, incluindo prazos máximos de armazenamento, vinculação estrita à finalidade declarada, políticas de descarte seguro e restrições ao uso secundário das informações coletadas.

5. Reforçar mecanismos de transparência e *accountability*, incluindo a divulgação de diretrizes institucionais sobre retenção e monitoramento e a realização periódica de avaliações de impacto à proteção de dados.

6. Harmonizar políticas de segurança da informação, cibersegurança e defesa, reduzindo lacunas normativas e promovendo maior coerência regulatória.

7. Fortalecer mecanismos de governança participativa, ampliando a transparência e a inclusão da sociedade civil na formulação e revisão das políticas de segurança digital.

Em síntese, os resultados indicam que a política pública de criptografia no Poder Executivo brasileiro encontra-se em processo de consolidação, marcada por avanços institucionais relevantes, mas ainda demandando maior clareza normativa, integração entre tecnologia e direitos e fortalecimento de salvaguardas institucionais.

ANEXO - LISTA DE DOCUMENTOS ANALISADOS

1. Ato da Agência Nacional de Telecomunicações nº 2.436, de 7 de março de 2023.
2. Estratégia Brasileira para a Transformação Digital (E-Digital), período 2018–2022, instituída pelo Decreto nº 9.319, de 21 de março de 2018.
3. Guia Orientativo de Cibersegurança para Prestadores de Telecomunicações - Outubro/2023
4. Orientações de Segurança da Informação e Cibernética (OSIC) nº 02/2023
5. Orientações de Segurança da Informação e Cibernética (OSIC) nº 08/2023
6. Orientações de Segurança da Informação e Cibernética (OSIC) nº 09/2023
7. Orientações de Segurança da Informação e Cibernética (OSIC) nº 11/2023
8. Orientações de Segurança da Informação e Cibernética (OSIC) nº 12/2023
9. Orientações de Segurança da Informação e Cibernética (OSIC) nº 13/2023
10. Orientações de Segurança da Informação e Cibernética (OSIC) nº 14/2023
11. Orientações de Segurança da Informação e Cibernética (OSIC) nº 15/2024
12. Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (Resolução Anatel nº 767, de 7 de agosto de 2024)
13. Ato da Agência Nacional de Telecomunicações nº 16.417, de 22 de novembro de 2024
14. Ato da Agência Nacional de Telecomunicações nº 77, de 5 de janeiro de 2021
15. Crianças, Adolescentes e Telas: Guia sobre Usos de Dispositivos Digitais (2025)
16. Declaração do Going Dark Brasil (2019)
17. Declaração Global sobre Integridade da Informação Online (2023)
18. Diretriz para a Proteção de Dados Pessoais no Ministério da Defesa (Portaria GM-MD nº 5.814, de 29 de novembro de 2022)
19. Diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública (Portaria do Ministério da Justiça e Segurança Pública nº 648/2024)

20. Estratégia Brasileira para a Transformação Digital (E-Digital), revisada para o período 2022–2026, conforme previsto no art. 3º do Decreto nº 9.319, de 21 de março de 2018

21. Estratégia Nacional de Cibersegurança (Decreto nº 12.573, de 4 de agosto de 2025)

22. Estratégia Nacional de Governo Digital e Rede Nacional de Governo Digital – Rede Gov.br (Decreto nº 12.069, de 21 de junho de 2024)

23. Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222, de 5 de fevereiro de 2020, revogado pelo Decreto nº 12.573, de 2025)

24. Estudo sobre poder social dos serviços digitais (2024)

25. Grupo de Trabalho com o objetivo de debater e propor as bases e diretrizes para o estabelecimento de uma Iniciativa Brasileira para Tecnologias Quânticas (Portaria do Ministério da Ciência, Tecnologia e Inovação nº 8.194/2024)

26. Guia Orientativo DevSecOps - GT-Ciber Anatel (2023)

27. Norma Complementar nº 07/IN01/DSIC/GSIPR de 2014

28. Norma Complementar nº 09/IN01/DSIC/GSIPR de 2014

29. Norma Complementar nº 19/IN01/DSIC/GSIPR de 2014

30. Norma Complementar nº 20/IN01/DSIC/GSIPR de 2014

31. Nota declaratória - Adesão do Brasil à Parceria Internacional para a Informação e a Democracia (2023)

32. Plano Setorial de Gestão de Incidentes Cibernéticos para o Setor de Telecomunicações (2022)

33. PNCiber – Audiência Pública Relatório da Audiência Pública Análise das Contribuições Transcrição da Sessão Pública (2023)

34. Política Cibernética de Defesa (Portaria Normativa do Ministério da Defesa nº 3.389, de 21 de dezembro de 2012)

35. Política de Segurança da Informação da Administração Central do Ministério da Defesa – POSIN-MD (Portaria GM-MD nº 5.659, de 18 de novembro de 2022)

36. Política Nacional de Cibersegurança e Comitê Nacional de Cibersegurança (Decreto nº 11.856, de 26 de dezembro de 2023)

37. Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco de Defesa Nacional (Decreto nº 12.725, de 18 de novembro de 2025)

38. Política Nacional de Inteligência (Decreto nº 8.793, de 29 de junho de 2016)

39. Política Nacional de Segurança da Informação (Decreto nº 10.641, de 2 de março de 2021, revogado pelo Decreto nº 12.572, de 2025)

40. Política Nacional de Segurança da Informação (Decreto nº 12.572, de 4 de agosto de 2025)

41. Política Nacional de Segurança da Informação (Decreto nº 9.637, de 26 de dezembro de 2018, revogado pelo Decreto nº 12.572, de 2025)

42. Política Nacional de Segurança de Infraestruturas Críticas (Decreto nº 9.573, de 22 de novembro de 2018)

43. Rede Federal de Gestão de Incidentes Cibernéticos (Decreto nº 10.748, de 16 de julho de 2021)

44. Regimentos Internos e Quadro Demonstrativo de Cargos em Comissão e Funções de Confiança do Ministério da Defesa (Portaria Normativa nº 12, de 14 de fevereiro de 2019)

45. Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (Resolução da Agência Nacional de Telecomunicações nº 740, de 21 de dezembro de 2020)

46. Relatório de Revisão do Cybersecurity Capacity Maturity Model for Nations (CMM) Brasil (2023)

47. Requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G (Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República nº 4, de 26 de março de 2020)

48. Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal (Instrução Normativa do Gabinete de Segurança Institucional nº 5, de 30 de agosto de 2021)

Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

Internet Society
Capítulo Brasil