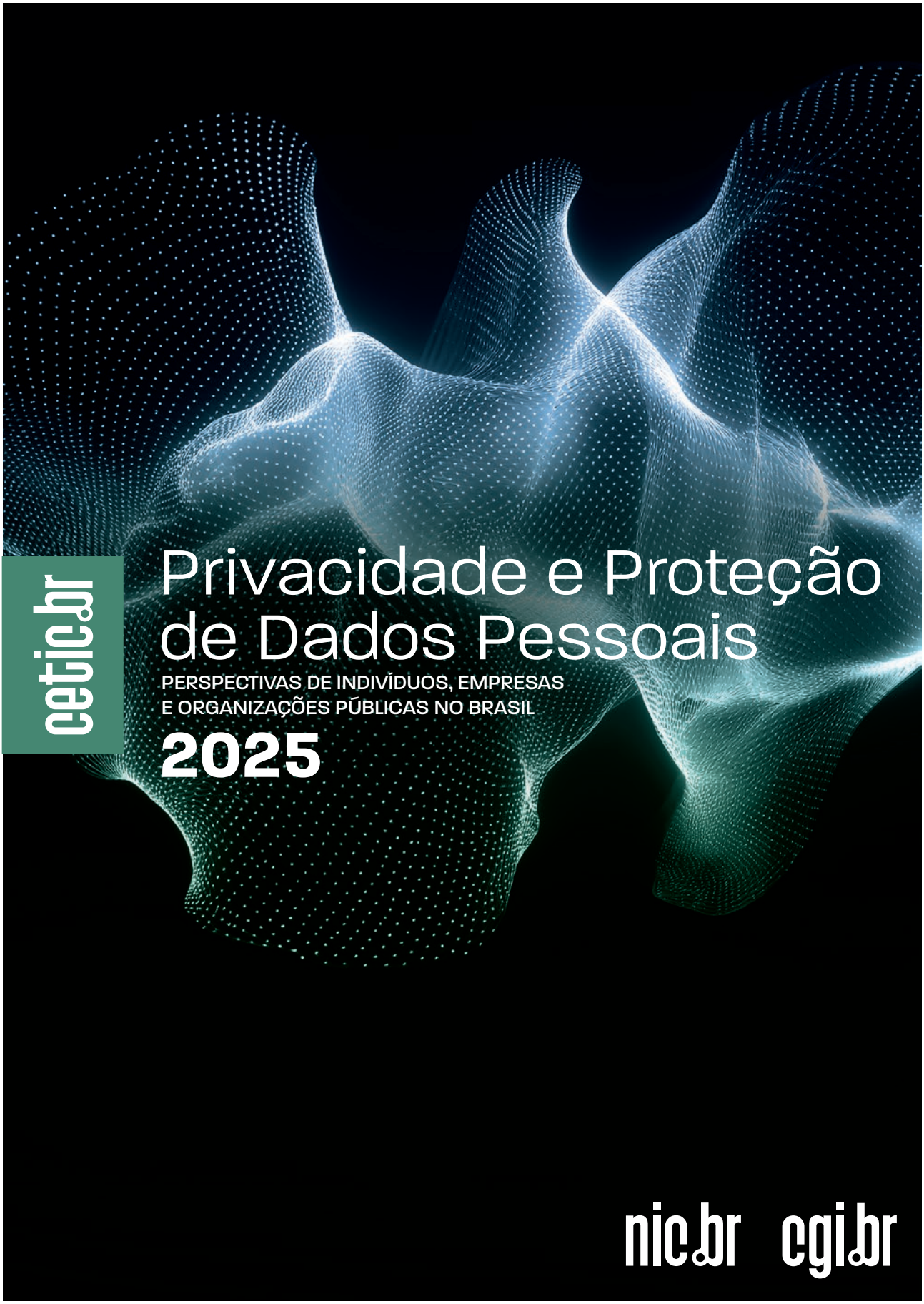


cetic.br

Privacidade e Proteção de Dados Pessoais

PERSPECTIVAS DE INDIVÍDUOS, EMPRESAS E ORGANIZAÇÕES PÚBLICAS NO BRASIL

2025

nic.br cgi.br

creative commons Atribuição Não Comercial 4.0 Internacional

Você tem o direito de:

Compartilhar: copiar e redistribuir o material em qualquer suporte ou formato.

Adaptar: remixar, transformar e criar a partir do material.

O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.

De acordo com os seguintes termos:

Atribuição: Você deve atribuir o devido crédito, fornecer um *link* para a licença, e indicar se foram feitas alterações. Você pode fazê-lo de qualquer forma razoável, mas não de uma forma que sugira que o licenciante o apoia ou aprova o seu uso.

Não comercial: Você não pode usar o material para fins comerciais.

Sem restrições adicionais: Você não pode aplicar termos jurídicos ou medidas de caráter tecnológico que restrinjam legalmente outros de fazerem algo que a licença permita.

http://creativecommons.org/licenses/by-nc/4.0/

Núcleo de Informação e Coordenação do Ponto BR

Privacidade e Proteção de Dados Pessoais

PERSPECTIVAS DE INDIVÍDUOS, EMPRESAS E ORGANIZAÇÕES PÚBLICAS NO BRASIL

2025

Comitê Gestor da Internet no Brasil
www.cgi.br

São Paulo
2026

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Diretor-Presidente : Demi Getschko
Diretor Administrativo : Ricardo Narchi
Diretor de Serviços e Tecnologia : Frederico Neves
Diretor de Projetos Especiais e de Desenvolvimento : Milton Kaoru Kashiwakura
Diretor de Assessoria às Atividades do CGI.br : Hartmut Richard Glaser

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br

Coordenação Executiva e Editorial : Alexandre F. Barbosa
Coordenação Geral de Pesquisas: Fabio Senne
Coordenação de Projetos de Pesquisa : Luciana Portilho e Manuella Maia Ribeiro (Coordenadoras), Ana Laura Martínez, Bernardo Ballardin, Daniela Costa, Fabio Storino, Leonardo Melo Lins, Lúcia de Toledo F. Bueno, Luísa Adib Dino e Luiza Carvalho
Coordenação de Métodos Quantitativos e Estatística : Marcelo Pitta (Coordenador), Camila dos Reis Lima, João Claudio Miranda, Mayra Pizzott Rodrigues dos Santos, Thiago de Oliveira Meireles e Winston Oyadomari
Coordenação de Métodos Qualitativos e Estudos Setoriais : Graziela Castello (Coordenadora), Javiera F. Medina Macaya, Manuela Cortez da Cunha Cruz, Mariana Galhardo Oliveira e Rodrigo Brandão de Andrade e Silva
Coordenação de Gestão de Processos e Qualidade : Nádilla Tsuruda (Coordenadora), Kayky Ferreira, Maísa Marques Cunha e Rodrigo Gabriades Sukarie
Gestão da pesquisa em campo : Ipsos-Ipec: Alexandre Carvalho, Denise Dantas de Alcântara, Guilherme Militão, Ligia Amstalden Rubega, Monize Arquer, Moroni Alves, Paulo Henrique Vieira e Rosi Rosendo (TIC Educação 2024 e 2025, TIC Empresas 2025, TIC Governo 2025 e TIC Saúde 2025); Quaest Pesquisa e Consultoria: Amábile Ochmat, Bárbara Lamounier, Bethânia Nascimento, Bruno Pinheiro, Giovani Roggia, Graziele Silotto, Guilherme Russo, João Zuquim, Maria Julia Timmers, Maria Luiza Oliveira, Matheus Moravia, Priscila Gregório e Renata Salvo (Painel TIC)
Apoio à edição : Comunicação NIC.br: Carolina Carvalho, Kauã Oliveira e Renata Barreto
Edição, preparação e revisão textual em português: Érica Santos Soares de Freitas
Projeto gráfico : Pilar Velloso
Editoração : Grappa Marketing Editorial (www.grappa.com.br)

Comitê Consultivo do Cetic.br

Carolina Botero Cabrera (Fundación Karisma), Eduardo Parajo (Durand Távola/Abranet), Guilherme Canela (UNESCO), Raúl Echeberría (ALAI) e Sonia Jorge (GDIP)

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Privacidade e proteção de dados pessoais 2025 [livro eletrônico] : perspectivas de indivíduos, empresas e organizações públicas no Brasil / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo : Comitê Gestor da Internet no Brasil, 2026.
PDF

Bibliografia
ISBN 978-65-6165-030-4

1. Direito à privacidade 2. Empresas 3. Organizações públicas 4. Privacidade na Internet 5. Proteção de dados pessoais 6. Tecnologia da informação e da comunicação I. Núcleo de Informação e Coordenação do Ponto BR.

26-379005.1 CDD-004.6072081

Índices para catálogo sistemático:
1. Brasil : Privacidade e proteção de dados pessoais : Tecnologias da informação e da comunicação : Relatório de pesquisa 004.6072081

Comitê Gestor da Internet no Brasil – CGI.br
(em agosto de 2026)

Coordenadora
Renata Vicentini Mielli

Conselheiros
Alexandre Reis Siqueira Freire
Beatriz Costa Barbosa
Bianca Kremer
Cláudio Furtado
Cristiane Vianna Rauen
Cristiano Reis Lobato Flôres
Débora Peres Menezes
Demi Getschko
Henrique Faulhaber Barbosa
Hermano Barros Tercius
José Roberto de Moraes Rêgo Paiva Fernandes Júnior
Lisandro Zambenedetti Granville
Luanna Sant'Anna Roncaratti
Marcelo Fornazin
Marcos Adolfo Ribeiro Ferrari
Nivaldo Cleto
Pedro Helena Pontual Machado
Percival Henriques de Souza Neto
Rafael de Almeida Evangelista
Rodolfo da Silva Avelino

Secretário executivo
Hartmut Richard Glaser

Agradecimentos

A pesquisa Privacidade e Proteção de Dados Pessoais 2025 contou com o apoio de um conjunto de especialistas, renomados por sua competência, que contribuíram de maneira significativa para a apuração dos resultados aqui apresentados. Essa colaboração é fundamental para a identificação de novos campos de pesquisa, para o aperfeiçoamento dos procedimentos metodológicos e para a produção de dados confiáveis. Cabe destacar que a importância das novas tecnologias para a sociedade brasileira e a relevância dos indicadores produzidos pelo Comitê Gestor da Internet no Brasil (CGI.br) para as políticas públicas e pesquisas acadêmicas serviram como motivação para que os especialistas participassem voluntariamente desse esforço coletivo. O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) agradece o apoio aos seguintes especialistas:

Agência Nacional de Proteção de Dados (ANPD)
Iagê Zendron Miola, Davi Teófilo Nunes Oliveira, Lucas Costa dos Anjos, Miriam Wimmer e Waldemar Gonçalves

Centro de Estudos e Pesquisas em Direito Sanitário (Cepedisa-FSP|USP)
Analluza Bolivar Dallari

Comitê Gestor da Internet no Brasil (CGI.br)
Bianca Kremer

Data Privacy Brasil
Rafael Zanatta

Fundação Getulio Vargas
Erica Bakonyi e Walter Britto Gaspar

Instituto Alana
Isabella Henriques

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)
Raquel Saraiva

Instituto EducaDigital
Priscila Gonsales

InternetLab
Fernanda Campagnucci

Menke Advogados
Fabiano Menke

Ministério da Saúde (MS)
Adriana Marques e Ana Estela Haddad

Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Jessica Maria dos Santos, Karen Ranieli Borges, Mariana Venancio Pereira, Nathan Paschoalini, Ramon Silva Costa e Raquel Gatto

Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Gabrielle Bezerra Sales Sarlet

Prado Vidigal
Ana Luiza Dornellas e Luis Fernando Prado

Rede Nacional de Ensino e Pesquisa (RNP)
Yuri Alexandro

Universidade da Virgínia (UVA)
Yasmin Curzi de Mendonça

Universidade Federal do Rio de Janeiro (UFRJ)
Chiara de Teffé

Sumário

7 Agradecimentos
13 Prefácio
17 Apresentação
21 Introdução

23 **Resumo Executivo – Privacidade e Proteção de Dados Pessoais 2025**

31 **Relatório Metodológico**

41 **Análise dos Resultados**
41 Usuários de Internet
67 Empresas
89 Organizações públicas

116 **Lista de Abreviaturas**

Lista de gráficos

27 Usuários de ferramentas de IA generativa, por frequência de uso segundo dispositivos e escolaridade (2025)

27 Usuários de Internet que vivenciaram situações envolvendo golpes, por canais em que essas situações ocorreram, segundo dispositivo de acesso utilizado (2025)

29 Empresas, por manutenção de dados pessoais de clientes e usuários com menos de 18 anos de idade, porte e setor (2021–2025)

29 Empresas, por área de origem do encarregado de proteção de dados pessoais (2021–2025)

47 Usuários de Internet, por categoria do conceito de privacidade (2021–2025)

48 Usuários de Internet, por práticas de gerenciamento de acesso a dados pessoais (2021–2025)

49 Usuários de Internet, por práticas de gerenciamento de acesso a dados pessoais e dispositivo de acesso utilizado (2025)

51 Usuários de Internet, por frequência de concordância com políticas de privacidade sem ler o que dizem e faixa etária (2025)

52 Usuários de Internet, por canal de atendimento em que buscaram sobre seus dados pessoais (2021–2025)

54 Usuários de Internet, por nível de preocupação com seus dados pessoais, segundo atividade realizada na Internet (2025)

56 Usuários de Internet, por nível de preocupação com o fornecimento de informações pessoais sensíveis, segundo tipo de informação pessoal sensível (2025)

57 Usuários de ferramentas de IA generativa, por frequência de uso segundo dispositivos e escolaridade (2025)

58 Usuários de ferramentas de IA generativa, por nível de preocupação com o uso dos dados pelas empresas fornecedoras de ferramentas de IA, segundo dispositivos de acesso e escolaridade (2025)

60 Usuários de Internet que vivenciaram situações envolvendo golpes, por canais em que essas situações ocorreram, segundo dispositivo de acesso utilizado (2025)

61 Usuários de Internet que vivenciaram situações envolvendo golpes, por decorrências dessas situações, segundo grau de instrução (2025)

70 Empresas, por tipo de dado pessoal mantido e porte (2021–2025)

71 Empresas, por tipo de dado sensível mantido (2021–2025)

73 Empresas, por manutenção de dados pessoais de clientes e usuários com menos de 18 anos de idade, porte e setor (2021–2025)

74 Empresas, por tipo de uso de dados pessoais de clientes e usuários (2021–2025)

75 Empresas, por tipo de finalidade de uso dos dados de funcionários e porte (2025)

76 Empresas, por realização de reuniões internas para tratar especificamente do tema de proteção de dados pessoais, porte e setor (2021–2025)

77 Empresas, por existência de uma área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais, porte e setor (2021–2025)

78 Empresas, por área ou departamento a que pertencem os funcionários responsáveis pelo tema de proteção de dados pessoais (2021–2025)

79 Empresas, por contratação de serviços de terceiros, como consultoria ou assessoria, para auxiliar com o tema de privacidade, proteção de dados e adequação à LGPD, porte e setor (2021–2025)

81 Empresas, por tipo de ação para adequação à LGPD (2021–2025)

83 Empresas, por tipo de ação para adequação a ações previstas pela LGPD e porte (2025)

84 Empresas, por área de origem do encarregado de proteção de dados pessoais (2021–2025)

85 Empresas, por recursos disponibilizados no *website* (2021–2025)

92 Órgãos públicos federais e estaduais, por existência de área ou pessoa responsável por procedimentos e políticas para a coleta, o armazenamento ou o uso de dados pessoais, ou pela implementação da LGPD (2021-2025)

93 Prefeituras, por existência de área ou pessoa responsável por procedimentos e políticas para a coleta, o armazenamento ou o uso de dados pessoais, ou pela implementação da LGPD (2021–2025)

94 Órgãos públicos federais e estaduais, por ações relacionadas à LGPD (2025)

96 Prefeituras, por ações relacionadas à LGPD (2021–2025)

98 Estabelecimentos públicos de saúde, por existência de documento que define uma política de segurança da informação (2023–2025)

99 Estabelecimentos públicos de saúde, por existência de treinamento sobre segurança da informação para os funcionários (2023–2025)

101 Estabelecimentos públicos de saúde, por medidas adotadas em relação à LGPD (2025)

104 Escolas públicas com documento que define a política de proteção de dados e de segurança da informação na instituição (2020–2025)

105 Gestores de escolas públicas, por atividades de gestão pedagógica, administrativa ou financeira realizadas por meio da adoção de IA (2025)

106 Gestores de escolas públicas, por temas discutidos durante as reuniões realizadas nos 12 meses anteriores à coleta de dados da pesquisa com professores, profissionais da escola, familiares e responsáveis sobre o uso de tecnologias digitais na instituição (2024–2025)

107 Escolas públicas, por público-alvo da oferta de debates ou palestras sobre privacidade e proteção de dados realizados na escola nos 12 meses anteriores à realização da pesquisa (2022–2025)

Prefácio

A Internet é uma rede construída de forma coletiva ao longo de décadas. Consolidou-se como infraestrutura essencial para a sociedade contemporânea, viabilizando atividades econômicas, políticas públicas, serviços fundamentais e diversas formas de interação social. Mais do que ofertar um conjunto de aplicações e serviços visíveis ao usuário final, a Internet se realiza sobre uma arquitetura técnica aberta, neutra, interoperável e distribuída, cuja integridade é *conditio sine qua non* para a inovação, a inclusão e o exercício de direitos no ambiente digital.

Seguindo os princípios norteadores da Internet e em constante interação com o Comitê Gestor da Internet no Brasil (CGI.br), o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) desempenha seu papel na coordenação e no fortalecimento da Internet no Brasil. Em 2025, 20 anos após sua reconfiguração como pessoa jurídica, o NIC.br reafirmou seu compromisso com a gestão de recursos críticos da rede, a operação de infraestrutura estável e a promoção de um ambiente digital seguro, acessível e de qualidade para os brasileiros. Esse marco institucional ocorreu em um contexto igualmente significativo, com a celebração dos 30 anos do CGI.br — internacionalmente reconhecido como uma exitosa experiência de governança multissetorial da Internet.

Entre as diversas áreas de atuação do NIC.br, voltado à segurança digital há o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que tem desempenhado papel central na coordenação de respostas a incidentes, na disseminação de boas práticas e no fortalecimento de capacidades técnicas para a segurança na rede, contribuindo para a resiliência da infraestrutura da Internet no país. Essas ações articulam-se à publicação de extenso material de conscientização e capacitação, sempre reforçando a importância de uma abordagem preventiva e colaborativa para a segurança no ambiente digital[1].

Também integra a agenda do NIC.br a promoção de uma Internet mais acessível e inclusiva. Nessa área atua o Centro de Estudos sobre Tecnologias Web (Ceweb.br), com o desenvolvimento de ações voltadas à acessibilidade digital e à padronização de tecnologias *web*[2].

[1] Mais informações sobre essas ações podem ser encontradas em https://internetsegura.br/

[2] Entre as iniciativas ligadas a normas técnicas, o Ceweb.br|NIC.br fez parte do comitê que elaborou a Norma ABNT NBR 17225, voltada para os requisitos de acessibilidade em conteúdo e aplicações *web*. Mais informações em https://ceweb.br/projetos/norma-abnt/

No campo mais técnico, o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (Ceptro.br) atua na busca do aperfeiçoamento contínuo da infraestrutura da Internet no Brasil, por meio de iniciativas de medição da qualidade da conexão, disseminação de boas práticas técnicas relacionadas a protocolos de rede, capacitação de profissionais e serviços essenciais à operação da rede[3]. Também foi da ação do Ceptro.br|NIC.br que se originou e se opera o Brasil Internet Exchange (IX.br)[4], que hoje atinge mais de 40 Tbit/s de tráfego agregado nas 38 localidades onde está presente, constituindo-se o maior conjunto de Pontos de Troca de Tráfego de Internet (PTT) do mundo, com cerca de 3.900 Sistemas Autônomos (AS) participantes. Ressalta-se que o ponto de São Paulo ocupa hoje a liderança mundial entre os PTT.

Soma-se aos esforços do NIC.br a criação do Observatório Brasileiro de Inteligência Artificial (OBIA), que disponibiliza dados e indicadores que ampliam a compreensão sobre os impactos e desafios da Inteligência Artificial (IA) no país, subsidiando o debate público e a formulação de políticas voltadas a seu uso responsável[5].

Ao longo de sua atuação, o NIC.br mantém e apoia ações que visam a promoção da Internet e seu uso seguro, responsável e consciente. Eventos anuais como o Dia da Internet Segura[6], o Seminário de Proteção à Privacidade e aos Dados Pessoais[7] e o Simpósio Crianças e Adolescentes na Internet[8] representam o esforço contínuo em articular debates técnicos, jurídicos e sociais sobre temas centrais da agenda digital. Essas ações ressaltam a importância da proteção de dados pessoais, da integridade da informação e da salvaguarda de direitos no ambiente digital, especialmente no que se refere a crianças e adolescentes.

Nesse contexto, o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) é o departamento do NIC.br responsável pela produção regular de indicadores e análises sobre o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) no Brasil. O Cetic.br|NIC.br consolidou-se como referência nacional e internacional na produção de dados confiáveis, comparáveis e alinhados a padrões metodológicos reconhecidos internacionalmente, os quais subsidiam, *per se*, a formulação de políticas públicas, a pesquisa acadêmica e o debate multissetorial sobre o desenvolvimento das tecnologias digitais.

Em 2025, o Cetic.br|NIC.br ampliou sua participação em fóruns e agendas internacionais, contribuindo com evidências empíricas e *expertise* metodológica para debates no âmbito das reuniões dos BRICS e do Mercado Comum do Sul (Mercosul)[9], além de outros espaços multilaterais. Nessas instâncias, temas como conectividade

[3] Os principais projetos e iniciativas do Ceptro.br|NIC.br podem ser acessados em https://ceptro.br/#projetos

[4] Mais informações disponíveis em https://ix.br/

[5] Mais informações disponíveis em https://obia.nic.br/

[6] Mais informações disponíveis em https://www.diadainternetsegura.org.br/

[7] Mais informações disponíveis em https://seminarioprivacidade.cgi.br/

[8] Mais informações disponíveis em https://criancaseadolescentesnainternet.nic.br/

[9] As publicações com os BRICS e o Mercosul, entre outras organizações internacionais, podem ser acessadas em https://cetic.br/pt/publicacoes/indice/outros/

significativa, adoção de IA e redução das desigualdades no acesso e uso das tecnologias digitais ocuparam lugar central, reforçando a importância de indicadores comparáveis e contextualizados para orientar tanto a cooperação regional como a internacional.

Neste ano, o Cetic.br|NIC.br iniciou novos estudos voltados a temas estratégicos para o desenvolvimento do ecossistema digital brasileiro, como a análise da infraestrutura de *data centers,* hoje fundamentais para o processamento, o armazenamento e o compartilhamento de dados, bem como para a expansão de aplicações baseadas em computação em nuvem e IA. Outro tema estratégico concerne à integridade da informação, central para a análise dos fluxos informacionais e da confiança nas fontes de dados, bem como para o enfrentamento de desafios associados à desinformação no ambiente digital.

Ao abordar de forma ágil temas emergentes e relevantes como qualidade da conectividade, competências digitais, privacidade, uso de IA, infraestrutura crítica e segurança, as pesquisas do Cetic.br|NIC.br colaboram para a compreensão dos múltiplos fatores que propiciam uma conectividade efetivamente significativa. Medir o acesso permanece essencial, mas torna-se cada vez mais necessário compreender suas condições de uso, riscos associados e as capacidades requeridas para que indivíduos e organizações possam se beneficiar plenamente das tecnologias digitais.

Os recursos financeiros gerados pelos registros de domínios .br, gerenciados pelo Registro.br|NIC.br, permitem investimentos contínuos em pesquisa, segurança, capacitação e desenvolvimento tecnológico, sustentando um ciclo virtuoso em prol da Internet no Brasil. Em um cenário de rápidas transformações tecnológicas e de crescente dependência das infraestruturas digitais, o modelo de governança adotado pelo país desde 1995 permanece atual e fundamental, apoiando uma Internet aberta, segura e orientada pelo interesse público.

Esta publicação visa contribuir para a qualificação do debate público e fortalecer a formulação, o acompanhamento e a avaliação de políticas públicas baseadas em evidências. Ao reunir dados confiáveis e análises consistentes, o NIC.br e o CGI.br reafirmam seu compromisso com a governança multissetorial, a promoção de direitos, a redução das desigualdades e a construção de um ambiente digital mais inclusivo, acessível e seguro, capaz de responder aos desafios contemporâneos e de ampliar as oportunidades para a sociedade brasileira.

Boa leitura!

Demi Getschko
Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Apresentação

A proteção de dados pessoais ocupa hoje posição central na transformação digital da economia, do Estado e das relações sociais. Nesse cenário, a expansão das plataformas digitais, a crescente circulação de informações e a rápida incorporação de sistemas de Inteligência Artificial (IA) ampliam oportunidades de inovação, eficiência e desenvolvimento; ao mesmo tempo, tornam mais complexos os desafios relacionados ao uso responsável de dados pessoais, à segurança da informação e à preservação da privacidade.

Desde a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD)[1], o Brasil tem consolidado um arcabouço jurídico e institucional orientado à proteção desses direitos fundamentais e à construção de relações digitais baseadas em confiança. Esse processo exige não apenas normas adequadas, mas também capacidade institucional, cooperação entre os diferentes setores e conhecimento qualificado sobre a realidade do país.

Nesse contexto, a terceira edição da pesquisa *Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil* assume especial relevância. Produzida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), a publicação reúne indicadores que permitem compreender, de forma abrangente e comparável, como a proteção de dados tem sido percebida e incorporada por diferentes segmentos da sociedade.

Por abordar os indivíduos, o estudo revela preocupações, comportamentos e práticas dos usuários da Internet relacionados à privacidade e ao uso de seus dados pessoais. No campo empresarial, oferece elementos para avaliar o tratamento de dados, o processo de adequação à LGPD e a preparação das organizações diante de novas exigências regulatórias, inclusive aquelas relacionadas à proteção de crianças e adolescentes no ambiente digital. Já no setor público, os indicadores provenientes das pesquisas TIC Governo, TIC Saúde e TIC Educação contribuem para o exame de temas como governança de dados, segurança da informação e proteção de dados pessoais no processo de transformação digital dos serviços públicos.

[1] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Essa visão integrada constitui uma das principais contribuições da publicação. Em razão de aproximar as perspectivas dos cidadãos e as práticas de empresas e organizações públicas, os indicadores ajudam a identificar avanços, lacunas e desigualdades, além de oferecer subsídios para a definição de prioridades, o aperfeiçoamento da regulação e a formulação de políticas públicas mais aderentes às necessidades da sociedade.

Para a Agência Nacional de Proteção de Dados (ANPD), a produção sistemática de evidências é indispensável ao exercício de suas atribuições de regulamentação, orientação, fiscalização e promoção da cultura de proteção de dados. Em um cenário marcado pela expansão da IA e por novas agendas regulatórias, como a proteção de crianças e adolescentes no contexto do Estatuto Digital da Criança e do Adolescente (ECA Digital)[2], decisões baseadas em dados contribuem para uma atuação pública mais efetiva, proporcional e capaz de acompanhar a evolução tecnológica.

Esta publicação também expressa a importância da cooperação institucional. A parceria entre a ANPD e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) tem contribuído para ampliar o conhecimento, disseminar boas práticas e qualificar o debate público sobre privacidade, proteção de dados e segurança no ambiente digital. O Seminário de Proteção à Privacidade e aos Dados Pessoais[3], promovido pelo Comitê Gestor da Internet no Brasil (CGI.br) e pelo NIC.br, é um exemplo relevante dessa atuação conjunta, o qual se consolidou como espaço de diálogo entre o poder público, o setor privado, a comunidade científica e a sociedade civil.

Ao lançar esta terceira edição, o Cetic.br|NIC.br reafirma seu compromisso com a produção de informações confiáveis para o desenvolvimento da sociedade da informação no Brasil. Nesse sentido, é uma satisfação apresentar uma obra que contribui para transformar evidências em conhecimento e conhecimento em melhores decisões. Que seus indicadores apoiem novas pesquisas, políticas e iniciativas capazes de assegurar que a inovação tecnológica avance de forma compatível com os direitos fundamentais, a confiança da sociedade e a construção de um ambiente digital mais seguro, inclusivo e responsável.

Waldemar Gonçalves Ortunho Junior
Agência Nacional de Proteção de Dados – ANPD

[2] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

[3] Mais informações disponíveis em https://seminarioprivacidade.cgi.br/

Introdução

A expansão da digitalização das atividades econômicas, dos serviços públicos e das relações sociais tem ampliado de forma significativa a coleta, o uso e o compartilhamento de dados pessoais em todo o mundo. Ao mesmo tempo em que os dados se tornaram recursos essenciais para a inovação, a implementação das políticas públicas e o desenvolvimento de produtos e serviços mais personalizados, sua adoção intensiva também amplia os riscos de acessos não autorizados, discriminação, fraudes e outras práticas que podem comprometer a proteção e o exercício de direitos humanos. Nesse cenário, a garantia da privacidade e a proteção de dados pessoais é condição necessária para o desenvolvimento de um ambiente digital seguro e responsável.

Foi nesse contexto de ampliação do uso de dados pessoais e de consolidação da privacidade e da proteção de dados como uma agenda central para a sociedade que o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) lançou, em 2021, a primeira edição da pesquisa bienal Privacidade e Proteção de Dados Pessoais. Desde então, o estudo tem produzido indicadores sobre as percepções dos usuários de Internet e as práticas adotadas por empresas e organizações públicas, permitindo acompanhar a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD)[1] e a evolução do tema no país.

Em relação à edição anterior, coletada em 2023, o cenário brasileiro de proteção de dados passou por importantes transformações institucionais, políticas e regulatórias. O período foi marcado pela ampliação das atribuições da Autoridade Nacional de Proteção de Dados, que passou a ser denominada Agência Nacional de Proteção de Dados (ANPD). Também foram estabelecidos novos marcos relacionados ao uso de tecnologias digitais, com implicações para o tratamento de dados pessoais, como o Plano Brasileiro de Inteligência Artificial (PBIA) 2024–2028[2], que incorpora a privacidade e a segurança entre seus princípios, e o Estatuto Digital da Criança e do Adolescente (ECA Digital)[3], que institui regras específicas para a proteção desse público nos ambientes digitais e atribui novas competências regulatórias e fiscalizatórias à ANPD.

[1] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[2] Disponível em https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial

[3] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

Paralelamente, observa-se uma rápida disseminação de sistemas de Inteligência Artificial (IA), como a IA generativa, plataformas digitais e outras tecnologias com uso intensivo de dados, que afetam indivíduos e organizações públicas e privadas. Além de criar oportunidades, essas aplicações introduzem desafios relacionados à transparência, à segurança, à responsabilização dos agentes de tratamento e à proteção de grupos mais vulneráveis, à medida que aumentam a exposição dos indivíduos a golpes e fraudes. Diante desse contexto, a produção de evidências sobre as percepções da população e as práticas adotadas por organizações públicas e privadas torna-se essencial para acompanhar a implementação da LGPD e de outras legislações e políticas correlatas, apoiar a atuação regulatória e orientar políticas e estratégias voltadas à consolidação de uma cultura de proteção de dados no Brasil.

Em sua terceira edição, a pesquisa Privacidade e Proteção de Dados Pessoais atualiza indicadores já coletados anteriormente, além de incluir um conjunto de dados inéditos referentes ao ano de 2025. Após a apresentação dos aspectos metodológicos que orientaram o estudo, a análise dos resultados da publicação está organizada nos seguintes capítulos:

- **Usuários de Internet:** apresenta os resultados do Painel TIC, realizado em 2025 com usuários de Internet (16 anos ou mais), que investiga a percepção desses usuários sobre o tratamento e a proteção de seus dados pessoais. Nesta edição também são abordados novos temas relacionados ao uso de IA e a golpes e fraudes.
- **Empresas:** identifica como as pequenas, médias e grandes empresas brasileiras tratam os dados pessoais no exercício de suas atividades, com base na aplicação de um módulo específico na pesquisa da TIC Empresas 2025.
- **Organizações públicas:** apresenta resultados das pesquisas TIC Governo 2025, TIC Saúde 2025 e TIC Educação 2024 e 2025 em relação a iniciativas de proteção de dados e de privacidade adotadas por órgãos federais e estaduais e prefeituras, por estabelecimentos públicos de saúde e por escolas públicas de Ensino Fundamental e Médio.

Com esta publicação, o Cetic.br|NIC.br reforça seu compromisso de produzir e disseminar estatísticas confiáveis e atualizadas sobre o desenvolvimento da sociedade da informação no Brasil. Ao reunir indicadores relacionados a diferentes setores, esta edição amplia a disponibilidade de evidências para subsidiar políticas públicas, iniciativas de governança e estratégias regulatórias relacionadas à privacidade e à proteção de dados pessoais. A consolidação da série histórica da pesquisa permite acompanhar a evolução dessa agenda no país, oferecendo subsídios para o monitoramento dos avanços e desafios relacionados à implementação da LGPD e de outros marcos regulatórios que orientam a transformação digital no Brasil.

Resumo Executivo

—

PRIVACIDADE E PROTEÇÃO
DE DADOS PESSOAIS 2025

Resumo Executivo Privacidade e Proteção de Dados Pessoais 2025

A proteção à privacidade e aos dados pessoais tem assumido um papel cada vez mais central nas agendas internacionais, impulsionada pela crescente digitalização de processos e pela incorporação de Inteligência Artificial (IA) em organizações públicas e privadas. Nesse cenário, diante da necessidade de informações atualizadas sobre o tema e dos desafios relacionados à consolidação da Lei Geral de Proteção de Dados Pessoais (LGPD)[1] no Brasil, desde 2021, a pesquisa Privacidade e Proteção de Dados Pessoais reúne indicadores sobre práticas e percepções de indivíduos, empresas e organizações públicas voltadas para uma cultura de proteção de dados no país. A terceira edição da pesquisa traz subsídios para a compreensão do modo como a temática tem sido percebida e incorporada no dia a dia dos indivíduos, ao mesmo tempo em que aponta tendências em relação à adoção de práticas de adequação à proteção de dados entre as organizações públicas e privadas, indicando pontos de atenção para ações futuras no campo.

APLICATIVOS DE MENSAGENS (84%) E LIGAÇÕES TELEFÔNICAS (79%) SÃO OS PRINCIPAIS CANAIS DE GOLPES COM DADOS PESSOAIS

Usuários de Internet

PERCEPÇÕES SOBRE RISCOS

A pesquisa investigou os níveis de preocupação dos usuários de Internet em relação à exposição de seus dados pessoais em diferentes atividades *online*. As maiores proporções de preocupação foram registradas em compras *online* (35% muito preocupados) e acesso a serviços bancários (32%), indicando que o receio está concentrado em situações que possam resultar em prejuízos financeiros. Observam-se variações conforme faixa etária e classe social: entre os mais jovens (16 a 24 anos), a maioria declarou estar pouco ou nada preocupada com o uso de redes sociais, ao passo que, entre os de 45 a 59 anos, esse nível de preocupação foi mais elevado. Da mesma forma, a preocupação com serviços de governo foi maior entre as classes AB (27%) do que entre as classes DE (13%).

Apesar dessa percepção de risco, não se observam mudanças significativas nas práticas cotidianas de gerenciamento de dados pessoais, o que evidencia um descompasso entre percepção e comportamento. Esse contexto serve como pano de fundo para analisar temas emergentes, como o uso de IA e a crescente sofisticação de golpes e fraudes digitais, que trazem novos desafios à proteção de dados e interferem cada vez mais no cotidiano dos usuários de Internet no Brasil.

IA GENERATIVA

A edição de 2025 traz indicadores inéditos sobre o uso de IA generativa: frequência de uso, tipo de informação fornecida e níveis de preocupação. O uso diário foi mais frequente entre os usuários dessa tecnologia que combinam celular e computador e entre aqueles com maior escolaridade, indicando que a ferramenta faz parte da rotina de uma parcela da população (Gráfico 1).

[1] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Entre os tipos de informação compartilhados, destacam-se temas relacionados ao trabalho ou estudo (73%), preferências e gostos pessoais (58%), sentimentos e emoções (54%), dados de saúde (52%) e fotos suas ou de pessoas conhecidas (50%).

O uso da IA generativa também tem se ampliado para atividades de aconselhamento, suporte emocional e companhia. Este tipo de interação tende a estimular o usuário a compartilhar informações de natureza íntima, além de imagens. A maioria (66%) dos usuários declarou estar muito preocupada ou preocupada com o uso dos dados pelas empresas responsáveis por essas ferramentas, sugerindo que reconhecem os riscos associados a essas tecnologias.

GOLPES COM DADOS PESSOAIS

A pesquisa passou a investigar, de forma inédita, o tema dos golpes envolvendo dados pessoais. Em 2025, 32% dos usuários vivenciaram tentativas de golpes usando seus dados pessoais, enquanto 20% foram vítimas efetivas. Os canais mais mencionados foram aplicativos de mensagens (84%) e ligações telefônicas (79%), seguidos por *sites* ou aplicativos falsos (71%), SMS (71%), *e-mail* (69%) e redes sociais (67%). Os resultados evidenciam que essas fraudes ocorrem por múltiplos canais de comunicação, combinando meios digitais e tradicionais para alcançar potenciais vítimas. Tal cenário demonstra que a exposição a situações fraudulentas pode atingir inclusive indivíduos que não utilizam a Internet, uma vez que são comuns também as tentativas por meio de telefone e SMS.

O dispositivo utilizado apresentou variação significativa: a menção a *sites* ou aplicativos falsos foi mais frequente entre os que usam apenas telefone celular para acessar a Internet, ilustrando como condições de conectividade restritas podem dificultar práticas de verificação de segurança (Gráfico 2). Além disso, as consequências dos golpes extrapolam o dano patrimonial, incluindo impactos emocionais e repercussões sobre o bem-estar, com variações segundo o nível de escolaridade.

Empresas

GUARDA DE DADOS PESSOAIS

Assim como nas edições anteriores da pesquisa, em 2025, o tipo de dado pessoal mais frequentemente mantido pelas empresas brasileiras é proveniente de clientes e usuários: 69% das empresas declararam manter esse tipo de dado, enquanto 58% mantêm dados de parceiros e fornecedores. O mesmo padrão é observado segundo o porte, com maior proporção de grandes empresas que armazenam dados pessoais de clientes e usuários (73%). Quanto aos tipos de dados pessoais sensíveis mantidos e investigados pela pesquisa, a biometria permaneceu como o dado sensível mais frequentemente armazenado (31%). Em seguida, os dados sensíveis de saúde foram mantidos por 26% das empresas, percentual estável em relação à edição anterior.

Entre as empresas que mantêm dados pessoais de clientes e usuários, 9% afirmaram armazenar dados pessoais de menores de 18 anos de idade, percentual mais elevado entre as empresas de grande porte (21%) e as do setor de alojamento e alimentação (19%) (Gráfico 3). Nesse mesmo grupo, 63% informaram utilizar esses dados para entrar em contato diretamente com clientes e usuários, enquanto 39% usaram para checagem de crédito, padrão mantido desde a primeira edição da pesquisa. Em relação aos dados gerados internamente, 35% das empresas usaram os dados pessoais dos funcionários tanto para avaliação de desempenho quanto para controle de entrada e saída nos locais de trabalho.

69% DAS EMPRESAS ARMAZENAM DADOS PESSOAIS DE CLIENTES E USUÁRIOS

CAPACIDADES INTERNAS

Em 2025, 40% das empresas realizaram reuniões para tratar especificamente do tema de proteção de dados pessoais, mantendo estabilidade em relação às edições anteriores da pesquisa. Assim como observado em outros indicadores, as empresas de grande porte realizaram essas reuniões em maior proporção (66%) do que as pequenas (38%), mantendo-se

GRÁFICO 1

—

Usuários de ferramentas de IA generativa, por frequência de uso segundo dispositivos e escolaridade (2025)

Total de usuários de Internet com 16 anos ou mais que usaram ferramentas de IA generativa (%)

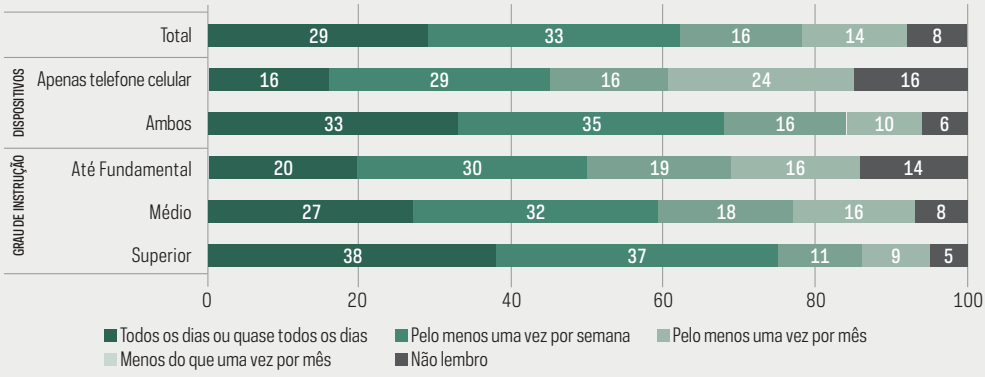
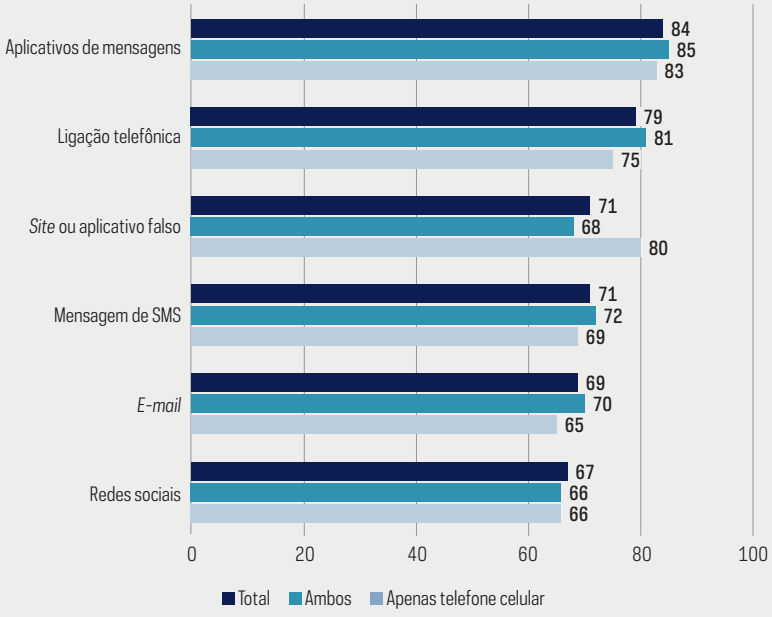


GRÁFICO 2

—

Usuários de Internet que vivenciaram situações envolvendo golpes, por canais em que essas situações ocorreram, segundo dispositivo de acesso utilizado (2025)

Total de usuários de Internet com 16 anos ou mais que vivenciaram tentativa de golpe ou foram vítimas de golpe usando dados pessoais (%)



estável esse padrão ao longo da série histórica. Em relação à estrutura organizacional, 20% das empresas possuíam uma área ou funcionários responsáveis dedicados às atividades de privacidade e proteção de dados, percentual estável em relação a anos anteriores. Do ponto de vista do perfil das empresas, as de grande porte (55%) e aquelas do setor de informação e comunicação (39%) foram as com maior mobilização de recursos humanos para tratar especificamente da proteção de dados pessoais.

ADEQUAÇÃO À LGPD

Em 2025, a medida mais adotada pelas empresas foi a alteração de contratos vigentes para se adequar à LGPD, mencionada por 30% delas, mantendo o padrão observado na edição anterior da pesquisa. Em seguida, 29% criaram uma política de uso de dados pessoais de funcionários e 28% desenvolveram uma política de privacidade. A nomeação de um encarregado pelo tratamento de dados pessoais foi mencionada por 14% das empresas. Entre estas, 28% informaram que esse profissional é oriundo da área de TI, enquanto 19% indicaram o setor administrativo da empresa, resultado que dialoga com a maior presença de estruturas organizacionais dedicadas à privacidade e à proteção de dados pessoais (Gráfico 4).

Metodologia da pesquisa e acesso aos dados

A pesquisa Privacidade e Proteção de Dados Pessoais 2025 reuniu dados inéditos coletados por diferentes estudos conduzidos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) com indivíduos, empresas e organizações públicas. A pesquisa Painel TIC entrevistou, via questionário *online,* 2.500 usuários de Internet com 16 anos ou mais de idade em dezembro de 2025. A pesquisa TIC Empresas 2025 incluiu um módulo específico sobre tratamento de dados pessoais no setor privado. Foram entrevistadas 1.775 empresas, entre fevereiro de 2025 e janeiro de 2026, que responderam às perguntas específicas do módulo sobre privacidade e proteção de dados. Além dos resultados inéditos, foi realizada uma análise sobre as organizações públicas no país baseada em indicadores relacionados ao tema de privacidade e proteção de dados pessoais nas pesquisas TIC Governo 2025, TIC Saúde 2025 e TIC Educação 2024 e 2025. Os resultados das pesquisas apresentadas nesta publicação estão disponíveis no *website* do Cetic.br|NIC.br (https://cetic.br). O "Relatório Metodológico" pode ser consultado tanto na publicação impressa como no *website*.

BOX 1

—

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO SETOR PÚBLICO

Como nas edições anteriores, a terceira edição do estudo Privacidade e Proteção de Dados Pessoais dedica um capítulo ao setor público a partir de indicadores das pesquisas TIC Governo 2025, TIC Saúde 2025 e TIC Educação 2024 e 2025. A análise contempla órgãos públicos federais e estaduais e prefeituras, estabelecimentos públicos de saúde e escolas públicas de Educação Básica.

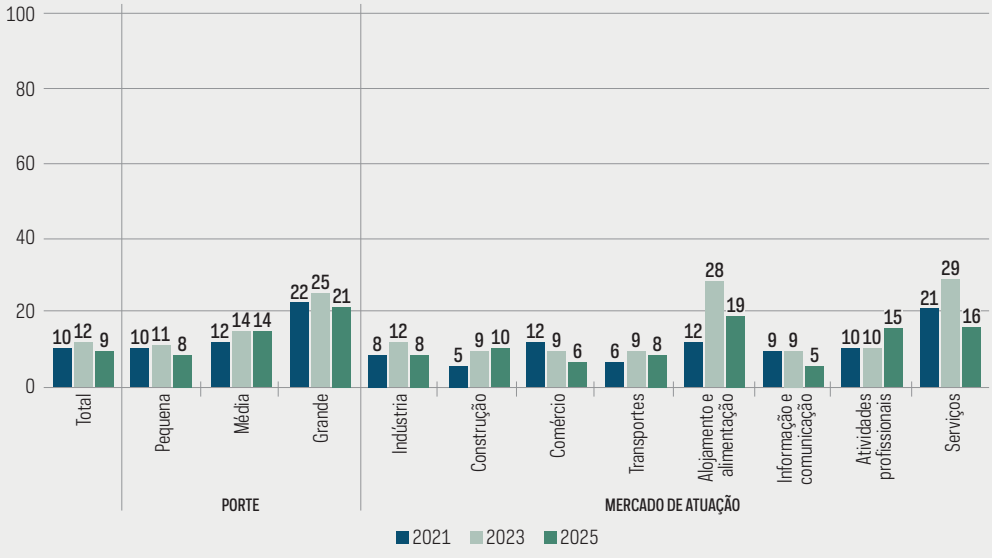
A crescente digitalização dos serviços públicos e a incorporação de aplicações de IA estão transformando a forma como as organizações públicas coletam, processam, compartilham e utilizam dados pessoais, trazendo novos desafios para a segurança da informação, a proteção de dados e sua governança. Os resultados desta edição mostram avanços na adoção de políticas de segurança da informação, na definição de áreas ou pessoas responsáveis pela implementação da LGPD e nas ações de capacitação e conscientização. No entanto, permanecem desafios relacionados à implementação de medidas específicas de adequação à LGPD, como a consolidação de estruturas de governança e a definição de responsabilidades institucionais. Os dados também revelam desigualdades entre diferentes tipos de organizações, indicando que a capacidade institucional permanece central para uma transformação digital segura, ética e capaz de acompanhar a digitalização dos serviços públicos.

GRÁFICO 3

—

Empresas, por manutenção de dados pessoais de clientes e usuários com menos de 18 anos de idade, porte e setor (2021–2025)

Total de empresas que mantêm dados pessoais de clientes e usuários (%)



Dados sensíveis armazenados pelas empresas em 2025:

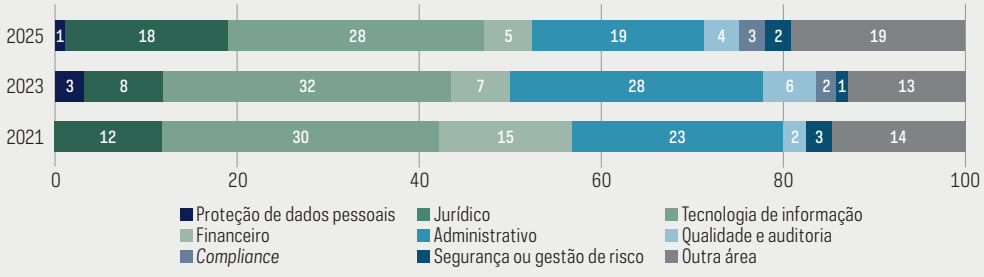
31%	26%	16%	12%
mantiveram dados biométricos	mantiveram dados sobre saúde	mantiveram dados sobre cor ou raça	mantiveram dados sobre orientação sexual

GRÁFICO 4

—

Empresas, por área de origem do encarregado de proteção de dados pessoais (2021–2025)

Total de empresas que possuem um encarregado de proteção de dados pessoais vindo da própria empresa (%)



Acesse os dados completos da pesquisa!

Além dos resultados apresentados nesta publicação, estão disponíveis no site do Cetic.br|NIC.br as tabelas de indicadores, os questionários, as informações para acessar os microdados e a apresentação dos resultados do evento de lançamento, além de outras publicações sobre o tema da pesquisa.

As tabelas de resultados (https://cetic.br/pt/pesquisa/privacidade-e-protecao-de-dados-pessoais/indicadores/), disponíveis para *download* em português, inglês e espanhol, apresentam as estatísticas produzidas, incluindo informações sobre os dados coletados e cruzamentos para variáveis investigadas no estudo. As informações disponíveis nas tabelas seguem o exemplo abaixo:

Código e nome do indicador

PR9C - USUÁRIOS DE INTERNET, POR FREQUÊNCIA COM QUE CONCORDA COM POLÍTICAS DE PRIVACIDADE SEM LER O QUE DIZEM

Total de usuários de Internet com 16 anos ou mais

População a que se referem os resultados

PERCENTUAL (%)		SEMPRE	QUASE SEMPRE	ALGUMAS VEZES	RARAMENTE	NUNCA
TOTAL		23	29	25	14	10
SEXO	Masculino	25	30	25	12	8
	Feminino	21	28	24	16	11
GRAU DE INSTRUÇÃO	Até Fundamental	24	23	25	15	13
	Médio	23	30	24	14	9
	Superior	22	31	26	13	8
FAIXA ETÁRIA	De 16 a 24 anos	25	29	23	13	10
	De 25 a 34 anos	27	27	21	16	9
	De 35 a 44 anos	22	34	24	11	8
	De 45 a 59 anos	23	28	25	15	8
	De 60 anos ou mais	13	24	32	13	18

Respostas do indicador

Recortes de tabulação dos resultados: total (conjunto da população) e características de análise (região, faixa etária, etc.), diferentes em cada pesquisa

Resultados: podem ser em % ou totais

Fonte: Núcleo de Informação e Coordenação do Ponto BR. (2026). *Painel TIC 2025: pesquisa* online *com usuários de Internet no Brasil: privacidade e proteção de dados pessoais* [Tabelas].

Como referenciar as tabelas de indicadores

Esta publicação está disponível também em inglês no *website* do Cetic.br|NIC.br.

Relatório Metodológico

—

PRIVACIDADE E PROTEÇÃO
DE DADOS PESSOAIS 2025

Relatório Metodológico
Privacidade e Proteção de Dados Pessoais 2025

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), apresenta os aspectos metodológicos da publicação *Privacidade e proteção de dados pessoais 2025: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. O objetivo da pesquisa é apurar o cenário atual e compreender os principais desafios para a construção de um ecossistema digital que garanta o respeito à privacidade e à proteção de dados pessoais no país. O levantamento de informações teve como base a coleta e o processamento de dados quantitativos obtidos por meio de pesquisas conduzidas regularmente pelo Cetic.br|NIC.br.

Do ponto de vista dos indivíduos, as informações incluem a percepção dos usuários de Internet sobre seus direitos e o tratamento de seus dados pessoais. Com relação às organizações, a publicação mostra como as empresas e organizações públicas estão se adaptando ao tema da privacidade e proteção de dados pessoais desde a vigência da Lei Geral de Proteção de Dados Pessoais ([LGPD], Lei n. 13.709/2018).

O projeto possui três objetivos específicos:

- investigar a percepção da população de usuários de Internet sobre o uso e a proteção de seus dados pessoais;
- compreender como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes/consumidores, bem como questões relevantes associadas à implementação da LGPD no Brasil;
- traçar um panorama da proteção de dados no contexto das políticas públicas, incluindo a adoção de práticas por parte dos órgãos governamentais, estabelecimentos de saúde e escolas públicas.

Na sequência, apresentamos os principais aspectos metodológicos das pesquisas utilizadas para a coleta dos indicadores e as referências para acesso integral ao "Relatório Metodológico" e ao "Relatório de Coleta de Dados" de cada estudo.

Painel TIC – Usuários de Internet (2025)

O Painel TIC foi criado com o objetivo de coletar informações sobre o uso da Internet durante a pandemia causada pelo novo coronavírus. Realizada por meio de questionários *online*, a pesquisa foi desenvolvida como uma alternativa à coleta de dados presencial, afetada pelas medidas de distanciamento social implementadas durante esse período. Desde então, a metodologia do Painel vem sendo adotada para o levantamento de dados sobre outros temas relevantes para o debate sobre a transformação digital.

Em 2021, um novo módulo do Painel TIC foi desenvolvido para investigar a percepção da população de usuários de Internet sobre o tratamento e a proteção de seus dados pessoais (CGI.br, 2021). A elaboração de um questionário específico sobre privacidade entre usuários de Internet tomou como ponto de partida diversas pesquisas anteriores com objetivos convergentes. Uma das primeiras coletas de dados identificada foi a pesquisa do Eurobarômetro *Special Eurobarometer 431: Data Protection*, de 2015, encomendada pela Comissão Europeia. Outra fonte relevante foi a edição de junho de 2019 da pesquisa *American Trends Panel* do Pew Research Center. Entre levantamentos oficiais produzidos por institutos nacionais de estatística, foi considerada a pesquisa *Survey of Canadians on Privacy-Related Issues*, realizada em 2020 por encomenda do Escritório do Comissariado de Privacidade do Canadá.

Também foi levada em conta a segunda edição da pesquisa Painel TIC COVID-19 do Cetic.br|NIC.br, que incluiu um módulo de privacidade. Esse módulo fazia parte de um esforço regional liderado pelo Banco Interamericano de Desenvolvimento (BID) com o objetivo de medir atitudes e percepções em relação à proteção de dados pessoais considerando o uso das tecnologias de informação e comunicação (TIC) em medidas de contenção da pandemia (CGI.br, 2020).

A pesquisa de 2025 segue os objetivos e referências do estudo de 2021. A população-alvo é composta de indivíduos usuários de Internet com 16 anos ou mais de idade no Brasil, considerando-se tais usuários as pessoas que fizeram uso da rede nos três meses que antecederam a entrevista, segundo recomendação metodológica da União Internacional de Telecomunicações (UIT, 2020).

Para seu desenho amostral, a pesquisa utilizou como base um painel *online* de indivíduos mantido pela Quaest Consultoria e Pesquisa, com aproximadamente 153 mil painelistas. O plano amostral empregado para a obtenção da amostra de respondentes foi do tipo amostragem por cotas, considerando as variáveis sexo, faixa etária, grau de escolaridade, macrorregião, classe social e propensão a ser usuário de Internet. A coleta de dados da pesquisa foi realizada em dezembro de 2025; ao todo, foram obtidas 2.500 entrevistas.

Com o objetivo de minimizar os vieses de seleção encontrados em abordagens por cotas, foi construída uma estrutura de pesos para o Painel TIC, tendo como referência uma pesquisa probabilística, a TIC Domicílios 2025[1]. Na etapa inicial, os resultados dessa pesquisa foram recalibrados para a população da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua) (Instituto Brasileiro de Geografia e Estatística [IBGE], s.d.), referente ao último trimestre divulgado.

[1] Mais informações disponíveis em https://www.cetic.br/pt/pesquisa/domicilios

Na sequência, com o intuito de estimar o contingente da população representada pelos respondentes do Painel TIC, adotou-se o procedimento de estimação com base em escores de propensão (*propensity scores*)[2]. Nessa metodologia, são calculados, inicialmente, os escores de propensão a ser usuário de Internet segundo variáveis socioeconômicas, com base na última edição disponível da pesquisa TIC Domicílios[3]. A seguir, esse mesmo modelo é utilizado para estimar os escores de propensão para os respondentes do Painel TIC.

Comparando a distribuição dos escores de propensão do Painel TIC com aquela verificada na última pesquisa TIC Domicílios, é possível determinar qual parcela da população do último levantamento poderia ser representada pelos respondentes do Painel, inclusive se essa representação abrange sua totalidade. Isso equivale a estimar o erro de cobertura do Painel TIC em relação à população-alvo inicialmente considerada para a pesquisa. Na presente edição do Painel TIC, o público representado equivale a toda a população-alvo da pesquisa – usuários de Internet com 16 anos ou mais de idade.

TIC Empresas – Pequenas, médias e grandes empresas (2025)

Realizada desde 2005, a pesquisa TIC Empresas tem como objetivo principal medir a posse e o uso das TIC entre as empresas brasileiras. O levantamento apresenta indicadores que traduzem em números a realidade das empresas brasileiras em relação a diversos temas, tais como acesso às TIC; uso da Internet; comércio eletrônico; habilidades em TIC; *software*; e segurança digital e novas tecnologias.

O universo abordado na pesquisa compreende todas as empresas brasileiras ativas com dez ou mais pessoas ocupadas[4] listadas no Cadastro Central de Empresas (Cempre) do IBGE, pertencentes aos setores da Classificação Nacional de Atividades Econômicas (CNAE) 2.0 de interesse da pesquisa TIC Empresas e à Natureza Jurídica 2 – entidades empresariais, exceto as empresas públicas (Natureza Jurídica 201-1).

As empresas investigadas correspondem às seguintes seções:

C – Indústria de transformação;

F – Construção;

G – Comércio e reparação de veículos automotores e motocicletas;

H – Transporte, armazenagem e correio;

[2] Diferentemente da estimativa baseada em um desenho amostral tradicional, as probabilidades de seleção no Painel são desconhecidas e indefinidas, por se tratar de um pseudodesenho amostral. A pseudoprobabilidade é a probabilidade estimada de pertencer à amostra não probabilística usada em vez de uma probabilidade conhecida. Mais informações disponíveis em Baker *et al*. (2013).

[3] Para esta edição do Painel TIC, foi utilizada a TIC Domicílios 2025 (CGI.br, 2026).

[4] A pesquisa TIC Empresas considera pequenas, médias e grandes empresas aquelas com, respectivamente, dez a 49 pessoas ocupadas, 50 a 249 pessoas ocupadas, e 250 pessoas ocupadas ou mais. As microempresas, aquelas com uma a nove pessoas ocupadas, não entram no escopo da pesquisa.

I – Alojamento e alimentação;

J – Informação e comunicação;

L – Atividades imobiliárias;

M – Atividades profissionais, científicas e técnicas;

N – Atividades administrativas e serviços complementares;

R – Artes, cultura, esporte e recreação;

S – Outras atividades de serviços.

A pesquisa TIC Empresas é desenvolvida com a preocupação de manter a comparabilidade internacional. Para isso, segue os padrões metodológicos propostos no manual da ONU Comércio e Desenvolvimento (UNCTAD, 2009), elaborado pela parceria entre a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o Instituto de Estatísticas da Comissão Europeia (Eurostat) e a Partnership on Measuring ICT for Development – esta última, uma coalizão formada por diversas organizações internacionais que busca a harmonização de indicadores-chave em pesquisas sobre TIC.

O plano amostral é estratificado em duas etapas, e as empresas são selecionadas aleatoriamente dentro de cada estrato. A primeira etapa compreende a definição de estratos naturais por meio do cruzamento das variáveis região geográfica e mercado de atuação (CNAE 2.0). Com base em cada estrato natural, são definidos os estratos finais, que consideram a divisão dos estratos naturais por porte da empresa[5]. Em 2025, a pesquisa entrevistou um total de 4.174 empresas, sendo que 1.775 responderam às perguntas específicas do módulo sobre privacidade e proteção dos dados pessoais.

As empresas são contatadas por meio da técnica de entrevista telefônica assistida por computador (do inglês, *computer-assisted telephone interviewing* – CATI). Em todas as entidades pesquisadas, busca-se entrevistar o responsável pela área de informática, tecnologia da informação (TI), gerenciamento da rede de computadores ou área equivalente, o que corresponde a cargos como:

- Diretor da divisão de informática e tecnologia;
- Gerente de negócios (vice-presidente sênior, vice-presidente de linha de negócios, diretor);
- Gerente ou comprador do departamento de tecnologia;
- Influenciador tecnológico (funcionário do departamento comercial ou de operações de TI com influência sobre as decisões a respeito de questões tecnológicas);
- Coordenador de projetos e sistemas;
- Diretor de outros departamentos ou divisões (excluindo informática);
- Gerente de desenvolvimento de sistemas;

[5] As faixas de porte consideradas são: 10 a 19 pessoas ocupadas; 20 a 49 pessoas ocupadas; 50 a 249 pessoas ocupadas; e 250 pessoas ocupadas ou mais.

- Gerente de informática;
- Gerente de projetos;
- Dono da empresa ou sócio.

Nas empresas que declaram ter, no momento da entrevista, 250 pessoas ocupadas ou mais, a estratégia foi entrevistar um segundo profissional, preferencialmente o gestor da área contábil ou financeira. Quando não encontrado, buscou-se o responsável pela área administrativa, jurídica ou de relações com instituições governamentais, a quem cabem exclusivamente as respostas sobre comércio eletrônico e atividades realizadas na Internet.

Em 2025, para atender à demanda por dados sobre temas emergentes, por exemplo, como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes/consumidores, bem como questões relevantes associadas à implementação da LGPD no Brasil, a pesquisa TIC Empresas passou a coletar os dados em três ondas. Em cada uma, módulos específicos de temas de interesse foram aplicados. Nessa edição, o módulo de privacidade foi aplicado em duas ondas da pesquisa: na segunda, entre julho e novembro de 2025 e, na terceira, que ocorreu entre outubro de 2025 e janeiro de 2026. Foi buscada a pessoa mais familiarizada com o tema na empresa, que pode ser tanto o primeiro respondente quanto uma pessoa ou área indicada por ele. Ao todo, 1.775 empresas responderam à pesquisa.

TIC Governo – Órgãos públicos federais e estaduais e prefeituras (2025)

Realizada a cada dois anos desde 2013, a pesquisa sobre o uso das TIC no setor público brasileiro – TIC Governo – investiga a incorporação das tecnologias digitais nos órgãos públicos e seu uso para a oferta de serviços públicos. O estudo ainda mede a existência de iniciativas relacionadas à promoção do acesso à informação pública e à participação da sociedade por meio das novas tecnologias. A partir de 2021, foram incluídos novos módulos relacionados à adoção de novas tecnologias, bem como indicadores sobre privacidade e proteção de dados pessoais.

A pesquisa tem abrangência nacional e inclui duas unidades de análise: órgãos públicos federais e estaduais de todos os poderes (Executivo, Legislativo, Judiciário e Ministério Público) e prefeituras. É realizado um censo em todos os públicos de interesse, excetuando órgãos do Executivo estadual, para os quais é selecionada uma amostra de aproximadamente 400 entidades públicas. As entrevistas são realizadas por meio de questionário estruturado pela técnica de CATI. Os indicadores analisados para esta publicação foram coletados entre julho de 2025 e abril de 2026, em 576 órgãos públicos federais e estaduais e 3.253 prefeituras.

TIC Saúde – Estabelecimentos públicos de saúde (2025)

Realizada anualmente desde 2013, a pesquisa TIC Saúde tem como objetivo compreender o estágio de adoção das TIC nos estabelecimentos de saúde, públicos e privados, e sua apropriação por médicos e enfermeiros. Para isso, identifica a infraestrutura tecnológica disponível e investiga o uso de sistemas e aplicações destinados a apoiar os serviços de assistência e a gestão dos estabelecimentos de saúde. Além disso, produz indicadores sobre as atividades realizadas pelos profissionais por meio dessas tecnologias, bem como sobre as motivações e barreiras para sua adoção e uso.

Em 2021, a pesquisa passou a investigar a adaptação dos estabelecimentos de saúde em relação a algumas medidas indicadas na LGPD. Em 2022, foram incluídos indicadores referentes a treinamentos em segurança da informação — tanto os oferecidos pelo estabelecimento de saúde quanto aqueles realizados pelos profissionais. A pesquisa também contempla informações sobre a existência de políticas de segurança da informação e as ferramentas de segurança da informação utilizadas pelos estabelecimentos de saúde.

A TIC Saúde tem abrangência nacional e coleta dados dos estabelecimentos de saúde nos três níveis de atenção, selecionados com base no Cadastro Nacional de Estabelecimentos de Saúde (CNES), mantido pelo Ministério da Saúde (MS). As entrevistas são realizadas por meio da técnica de CATI e há a possibilidade de autopreenchimento de questionário *web*, por meio de plataforma específica. Os dados da edição de 2025 foram coletados entre fevereiro e novembro desse mesmo ano com 3.270 gestores, representando um universo de aproximadamente 129.000 estabelecimentos de saúde brasileiros.

TIC Educação – Escolas públicas (2024 e 2025)

Realizada desde 2010, a pesquisa TIC Educação investiga o acesso, o uso e a apropriação das TIC pela comunidade educacional, principalmente alunos e professores, em atividades de ensino, de aprendizagem e de gestão escolar. Com abrangência nacional, a pesquisa é aplicada anualmente em escolas de Educação Básica, públicas e particulares, localizadas em áreas urbanas e rurais e que oferecem classes de Ensino Fundamental e Médio regular. Na edição 2020, a inclusão de um módulo específico sobre privacidade, com questões acerca da segurança digital e da coleta e proteção de dados pessoais, permitiu aprofundar o conhecimento sobre as percepções e as experiências dos diferentes atores escolares sobre essa temática específica.

Os dados analisados nesta publicação baseiam-se primordialmente nos indicadores coletados nas edições 2024 e 2025 da pesquisa TIC Educação. A edição 2024 foi realizada entre agosto de 2024 e março de 2025, de forma presencial, por meio da técnica de entrevista pessoal assistida por computador (do inglês *computer-assisted personal interviewing* [CAPI]), em 1.023 escolas. Ao todo, foram entrevistados 7.476 estudantes do 4º ano do Ensino Fundamental ao 3º ano do Ensino Médio, 1.462 professores, 864 coordenadores pedagógicos e 954 gestores escolares. Os dados da edição 2025 foram coletados entre os meses de agosto de 2025 e abril de 2026, por meio de entrevistas telefônicas (CATI), com 2.404 gestores escolares.

Disseminação dos dados

Os resultados das pesquisas mencionadas anteriormente são apresentados de acordo com as variáveis descritas no "Relatório Metodológico" de cada estudo, no item "Domínios de interesse para análise e divulgação".

Arredondamentos fazem com que, em alguns resultados, a soma das categorias parciais difira de 100% em questões de resposta única. O somatório de frequências em questões de respostas múltiplas usualmente é diferente de 100%. Vale ressaltar que, nas tabelas de resultados, o hífen (-) é utilizado para representar a não resposta ao item. Por outro lado, como os resultados são apresentados sem casa decimal, as células com valor zero indicam que houve resposta ao item, mas ele é explicitamente maior do que zero e menor do que um.

Os resultados das pesquisas são publicados em formato *online* e disponibilizados no *website* do Cetic.br|NIC.br (https://cetic.br/). As tabelas de proporções, totais e margens de erro calculadas para cada indicador estão disponíveis para *download* em português, inglês e espanhol. Mais informações sobre a documentação, os metadados e as bases de microdados estão disponíveis na página de microdados (https://cetic.br/microdados/).

Referências

Baker, R., Brick, J. M., Bates, N. A., Battaglia, M., Couper, M. P., Dever, J. A., Gile, K. J., & Tourangeau, R. (2013). *Report of the AAPOR Task Force on non-probability sampling*. https://aapor.org/wp-content/uploads/2022/11/NPS_TF_Report_Final_7_revised_FNL_6_22_13-1.pdf

Comitê Gestor da Internet no Brasil. (2020). *Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus – 2ª edição: Serviços públicos on-line, telessaúde e privacidade*. https://cetic.br/pt/publicacao/painel-tic-covid-19-pesquisa-sobre-o-uso-da-internet-no-brasil-durante-a-pandemia-do-novo-coronavirus-2-edicao-servicos-publicos-on-line-telessaude-e-privacidade/

Comitê Gestor da Internet no Brasil. (2021). *Painel TIC COVID-19: Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus*. https://cetic.br/pt/publicacao/pesquisa-web-sobre-o-uso-da-internet-no-brasil-durante-a-pandemia-do-novo-coronavirus-painel-tic-covid-19/

Comitê Gestor da Internet no Brasil. (2026). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2025*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2025/

Instituto Brasileiro de Geografia e Estatística. (s.d.). *Pesquisa nacional por amostra de domicílios contínua (Pnad Contínua)*. https://www.ibge.gov.br/estatisticas/sociais/trabalho/9173-pesquisa-nacional-por-amostra-de-domicilios-continua-trimestral.html

Lei Geral de Proteção de Dados Pessoais. Lei n. 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ONU Comércio e Desenvolvimento. (2009). *Manual for the production of statistics on the information economy 2009*. https://unctad.org/system/files/official-document/sdteecb20072rev1_en.pdf

União Internacional de Telecomunicações. (2020). *Manual for measuring ICT access and use by households and individuals, 2020 edition*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/manual.aspx

Análise dos Resultados

—

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS 2025

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2025
Usuários de Internet

Nos últimos anos, o aumento da oferta de serviços digitais, a intensificação do uso de Inteligência Artificial (IA), a ampliação da coleta de dados biométricos e a crescente incidência de golpes e fraudes envolvendo dados pessoais tornaram ainda mais relevante compreender como os indivíduos percebem os riscos associados ao ambiente digital e quais estratégias adotam para proteger suas informações.

Essa crescente digitalização da sociedade brasileira trouxe à tona desafios complexos relacionados à privacidade e à proteção de dados pessoais. Nesse cenário, a Lei Geral de Proteção de Dados Pessoais ([LGPD], Lei n. 13.709/2018) estabeleceu um marco regulatório essencial ao definir direitos fundamentais para os titulares de dados, como o acesso, a correção e a exclusão de informações pessoais, além de fomentar uma cultura de proteção de dados que envolve tanto organizações quanto cidadãos. A Agência Nacional de Proteção de Dados (ANPD), responsável pela regulamentação, implementação e fiscalização do cumprimento da LGPD, integra esse arranjo. Sua transformação em agência reguladora introduz mudanças na estrutura institucional da política brasileira de proteção de dados pessoais, com implicações para sua autonomia e para o exercício de suas atribuições regulatórias e fiscalizatórias.

Para compreender como esses avanços normativos ressoam na vida cotidiana dos brasileiros, torna-se fundamental investigar as percepções, as práticas e as preocupações da população em relação ao uso de seus dados no ambiente digital. Nesse contexto, insere-se a pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), que, em sua terceira edição, amplia o escopo da investigação iniciada em 2021. Ao consolidar essa série histórica, a pesquisa permite acompanhar a evolução das percepções e das práticas dos usuários de Internet ao longo do tempo, contribuindo para identificar mudanças no comportamento dos indivíduos diante das transformações tecnológicas e regulatórias.

Esta edição do livro Privacidade e Proteção de Dados Pessoais apresenta os resultados da pesquisa *online* realizada com usuários de Internet de 16 anos ou mais, dedicada a mapear o comportamento e as percepções dos indivíduos sobre temas centrais da agenda digital contemporânea. O questionário, elaborado com base em experiências internacionais de investigações semelhantes nos Estados Unidos (Auxier *et al.*, 2019) e na União Europeia

(Comissão Europeia, 2015), foi aprimorado para incorporar novos indicadores que refletem as tendências emergentes. Além de aprofundar tópicos abordados nas edições anteriores — como a leitura de políticas de privacidade e a preocupação com o uso de dados biométricos —, a pesquisa introduz questões inéditas sobre o uso de IA e a crescente exposição a golpes e fraudes que exploram dados pessoais, temas que ganharam relevância no debate público nos últimos anos.

Ao trazer à luz essas questões, esta publicação busca não apenas contribuir para o conhecimento sobre o tema, mas também subsidiar a formulação e a avaliação de políticas públicas, campanhas de conscientização e estratégias organizacionais, a fim de oferecer informações relevantes para pesquisadores, organizações que tratam dos dados pessoais e demais interessados na promoção de uma experiência digital mais segura e transparente para todos os cidadãos brasileiros. Assim, a presente análise está organizada nas seguintes dimensões:

- **Conceito de privacidade:** percepção dos usuários de Internet sobre o que significa privacidade, coletada por meio de pergunta aberta;
- **Práticas de proteção de dados:** medidas adotadas pelos indivíduos para proteger seus dados e buscar canais de atendimento para solicitações, reclamações ou denúncias;
- **Percepção de riscos:** níveis de preocupação em relação a atividades realizadas na Internet e principais riscos percebidos com relação aos dados pessoais;
- **Dados sensíveis e dados biométricos:** níveis de preocupação quanto ao fornecimento de dados biométricos de diversos tipos;
- **IA generativa:** frequência de uso de ferramentas de IA generativa, tipos de informações providas e níveis de preocupação associados;
- **Golpes com dados pessoais:** situações envolvendo golpes com dados pessoais, canais em que ocorreram e decorrências desses episódios.

Conceito de privacidade

Para compreender as percepções e práticas relacionadas à privacidade, a pesquisa iniciou o questionário com uma pergunta aberta, que permitiu captar, de forma não estruturada, os diferentes significados atribuídos pelos usuários ao conceito. Essa abordagem metodológica teve como objetivo evitar que as respostas fossem restritas a definições previamente estabelecidas pelos pesquisadores, oferecendo, assim, evidências sobre o entendimento dos indivíduos sobre o termo. As respostas foram analisadas e codificadas em categorias amplas, o que possibilitou identificar a quais domínios as pessoas se referem quando pensam em "privacidade", revelando como os usuários de Internet percebem a proteção de seus dados pessoais.

METODOLOGIA

A abordagem retoma a metodologia de classificação desenvolvida para a edição de 2021 da pesquisa Privacidade e Proteção de Dados Pessoais (Comitê Gestor da Internet no Brasil [CGI.br], 2022), reaplicada e atualizada na atual edição (2025), com uma nova amostra de respostas classificadas manualmente e um modelo preditivo reajustado. Assim, em um primeiro momento, foram selecionadas aleatoriamente 500 respostas, agrupadas nas seis categorias definidas na publicação anterior[1]: liberdade, individualidade, proteção de dados, controle, segurança e outras. A estratégia de classificação em 2021 havia passado por três etapas de desenvolvimento: (i) aproximação com as categorias de Auxier *et al.* (2019), do Pew Research Center; (ii) criação de categorias próprias ao contexto brasileiro; e (iii) seleção do número ideal de categorias por modelagem de tópicos, descritas em CGI.br (2022).

Para iniciar a análise estatística, foram removidas as palavras de uso mais frequente na língua portuguesa (*stop words*), acentos e caracteres especiais, e mantidos apenas os radicais das palavras remanescentes (*stemming*). A partir dos novos textos, foram realizadas análises descritivas para identificar possíveis termos comuns a diversas categorias sem significado substantivo (também removidos).

Por se tratar de um número limitado de respostas, foi utilizado um modelo com validação cruzada para regularização dos resultados, a fim de evitar que o modelo fosse sobreajustado, ou seja, que aprendesse muito somente sobre as respostas classificadas manualmente e não fosse capaz de generalizar para as demais respostas. Assim, foi aplicado o modelo LASSO com hiperparametrização das penalizações (Friedman *et al.*, 2010; Tibshirani, 1996) que, de forma resumida, identifica o melhor parâmetro para regularizar os resultados. Nesse processo, os textos foram divididos em cinco grupos para a validação cruzada, de dez diferentes formas, para aumentar a confiabilidade da validação dos dados de treinamento, ou seja, da capacidade de classificação das 500 respostas selecionadas aleatoriamente.

Antes de decidir se o modelo treinado com a amostra de 2021 continuava adequado para classificar as respostas de 2025 ou se seria necessário treinar um modelo novo, foram testados dois cenários de validação. Os testes reproduzem passo a passo a *tokenização*, a modelagem e as matrizes de confusão de cada cenário:

- **Novo-Antigo:** modelo treinado em 2021 e aplicado diretamente, sem novo treinamento, às 500 respostas de 2025 classificadas manualmente;
- **Novo-Novo:** modelo treinado e avaliado por validação cruzada (cinco grupos, dez repetições) exclusivamente para a amostra de 2025.

O modelo da edição de 2021 aplicado diretamente à nova base (Novo-Antigo) obteve um desempenho consideravelmente inferior ao retreinamento com dados de 2025 (Novo-Novo). Por esse motivo, optou-se por treinar um novo modelo com a amostra de 500 respostas de 2025 para gerar as estimativas populacionais desta edição, replicando a mesma arquitetura (LASSO com hiperparametrização das penalidades e validação cruzada).

[1] As categorias não foram redefinidas nesta edição por não haver diferenças significativas no contexto das respostas obtidas.

Para definição do modelo ajustado à presente edição da pesquisa e aplicado na nova amostra, foram realizadas duas etapas adicionais: na primeira, calculou-se a estimativa pontual para as proporções de cada categoria, ajustando seus respectivos pesos dentro das 2.500 respostas (das quais 500 foram classificadas manualmente e as demais 2.000, preditas pelo modelo). Na segunda, foram utilizadas 200 diferentes subamostras em um processo de *bootstrap*, um método de reamostragem, com os pesos atualizados para cada uma delas. A partir disso, foram geradas mais 200 estimativas pontuais que permitem estimar os intervalos de confiança para cada uma das categorias. Dessa forma, foi possível incorporar a incerteza do processo de classificação das respostas, considerando o plano amostral da pesquisa.

Para verificar a robustez dessas estimativas populacionais a diferentes escolhas de especificação do modelo, foram testadas seis especificações alternativas de validação cruzada, variando o número de grupos, a métrica usada para escolher o hiperparâmetro e a regra de seleção. A opção selecionada adota o hiperparâmetro de maior acurácia em valor absoluto, seguindo a mesma regra de escolha da edição de 2021. Entretanto, agora com dez grupos e dez repetições para validação cruzada, não mais cinco e dez. Desse modo, a estratégia combina um maior número de repetições e uma regra de seleção menos conservadora.

CLASSIFICAÇÃO DAS RESPOSTAS

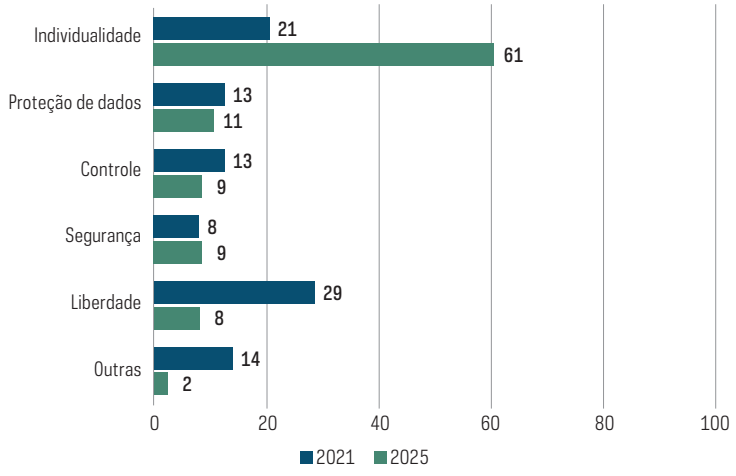
Foram criadas seis categorias para representar diferentes dimensões do conceito de privacidade presentes nas respostas dos entrevistados, utilizadas para classificar as 500 respostas manuais para que o modelo atribuísse essas categorias às respostas restantes, conforme segue:

- **Liberdade:** garantia da liberdade de aspectos privados da vida ("liberdade" [própria e de outros], "direito", "expressão", "opinião" e "interferência");
- **Individualidade:** busca pela individualidade, seja em espaços ou situações ("individualidade", "intimidade", "espaço", "particular", "privado", "respeito", "momento" e "sozinho");
- **Proteção de dados:** desejo de proteção de seus dados por terceiros ("proteção de dados contra terceiros", "vazamentos", "informação" e "sigilo");
- **Controle (de dados):** desejo de possuir controle sobre seus próprios dados ("controle sobre acesso a dados", "escolha sobre o que é público", "consentimento", "acesso", "informação" e "compartilhamento");
- **Segurança:** menções mais genéricas a segurança ("segurança", "proteção", "sigilo", "monitoramento", "guardar" e "confiança");
- **Outras:** respostas válidas não enquadradas nas demais categorias ("paz", "tranquilidade", "sossego", "importante", "essencial", "tudo" [não elaborado] e "não existe").

Na comparação com 2021, os resultados de 2025 mostram algumas mudanças na forma como os usuários de Internet associam diferentes conceitos à privacidade. A categoria "Individualidade", que permaneceu como a mais frequente, apresentou aumento em relação à edição anterior, enquanto as associações à "Liberdade" diminuíram. Já "Proteção de dados", "Controle" e "Segurança" apresentaram maior estabilidade entre as duas edições (Gráfico 1).

GRÁFICO 1
—

Usuários de Internet, por categoria do conceito de privacidade (2021–2025)
Total de usuários de Internet com 16 anos ou mais (%)



Algumas categorias apresentam proximidade conceitual, o que deve ser considerado na interpretação dos resultados. "Individualidade", por exemplo, possui em alguns casos distinções sutis em relação à "Liberdade". Da mesma forma, "Controle" se aproxima de "Proteção de dados", uma vez que ambas as categorias se referem ao que terceiros podem fazer com os dados pessoais ou informações dos respondentes, diferenciando-se principalmente quanto à ênfase: enquanto "Controle" está associado à posse e ao controle sobre as informações, "Proteção de dados" enfatiza sua proteção contra possíveis danos. A categoria "Outras", por sua vez, reúne respostas heterogêneas que não constituíram agrupamentos relevantes para desagregação, incluindo menções que variam de "importante" e "essencial" a "não existe".

De modo geral, os resultados evidenciam a diversidade de entendimentos sobre o conceito de privacidade entre os usuários de Internet e apontam mudanças em relação a 2021. O aumento das associações com "Individualidade" e a redução das menções à "Liberdade" podem indicar uma maior aproximação da ideia de privacidade com a proteção da vida privada e da intimidade, em detrimento de uma compreensão mais vinculada à liberdade individual. Essas mudanças ocorrem em um contexto de crescente digitalização das relações sociais e de ampliação da coleta, do uso e do compartilhamento de dados pessoais, no qual a privacidade passa a estar cada vez mais relacionada às possibilidades de definir limites sobre o acesso de terceiros a informações pessoais.

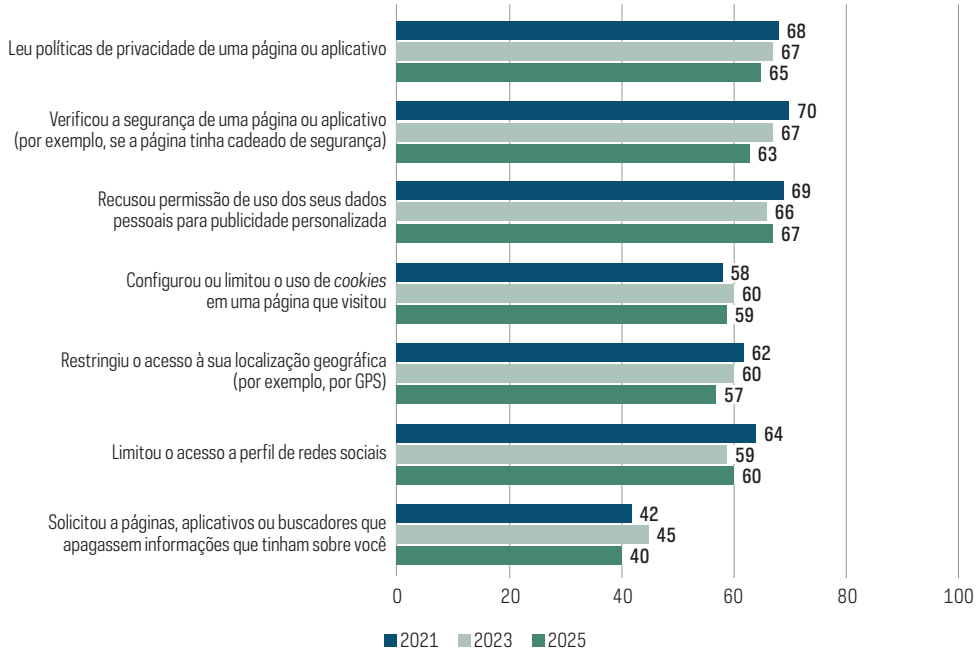
Práticas de proteção de dados

A dimensão dessas práticas investiga como usuários de Internet protegem seus dados pessoais, quais cuidados tomam no uso cotidiano da rede e das plataformas, e como procedem caso haja algum problema relacionado a esse tema. Desse modo, a análise

dessas práticas permite compreender em que medida a crescente preocupação com privacidade e proteção de dados se traduz em comportamentos concretos dos usuários no ambiente digital.

De acordo com a pesquisa, entre as atividades realizadas para gerenciar o acesso a seus dados pessoais, os usuários de Internet com 16 anos ou mais reportaram, em maior proporção, a recusa de permissão de uso de seus dados para publicidade personalizada (67%), seguida pela leitura de políticas de privacidade de páginas ou aplicativos (65%), e pela verificação de segurança de páginas ou aplicativos (63%). Entre as atividades investigadas, a menos mencionada foi solicitar a exclusão de dados a agentes de tratamento de dados, como páginas (*websites*), aplicativos ou buscadores (40%), ação que requer o conhecimento a respeito da possibilidade de exclusão de dados e do canal de contato para fazer a solicitação. Houve estabilidade em relação às estimativas da pesquisa em 2021 e 2023 para todas as categorias investigadas (Gráfico 2), indicando que as transformações no contexto regulatório e tecnológico nem sempre se traduzem, no curto prazo, em alterações no comportamento cotidiano dos indivíduos.

GRÁFICO 2
–
Usuários de Internet, por práticas de gerenciamento de acesso a dados pessoais (2021–2025)
Total de usuários de Internet com 16 anos ou mais (%)



Em 2025, 65% dos usuários de Internet acessavam a Internet exclusivamente pelo telefone celular, enquanto 34% também utilizavam computador. A distinção entre esses grupos é relevante porque o dispositivo utilizado pode afetar as condições de navegação, a visualização de informações e a realização de procedimentos relacionados ao gerenciamento e à proteção de dados pessoais. Assim como nas edições anteriores da pesquisa, os usuários exclusivos de telefone celular apresentaram proporções inferiores àquelas dos que combinam telefone celular e computador (Gráfico 3). A maior diferença em pontos percentuais ocorreu na verificação de segurança da página: enquanto, entre os que usam ambos os dispositivos, 70% afirmaram verificar a segurança da página ou do aplicativo pelo cadeado de segurança, entre os que usam apenas telefone celular, essa proporção foi de 48%.

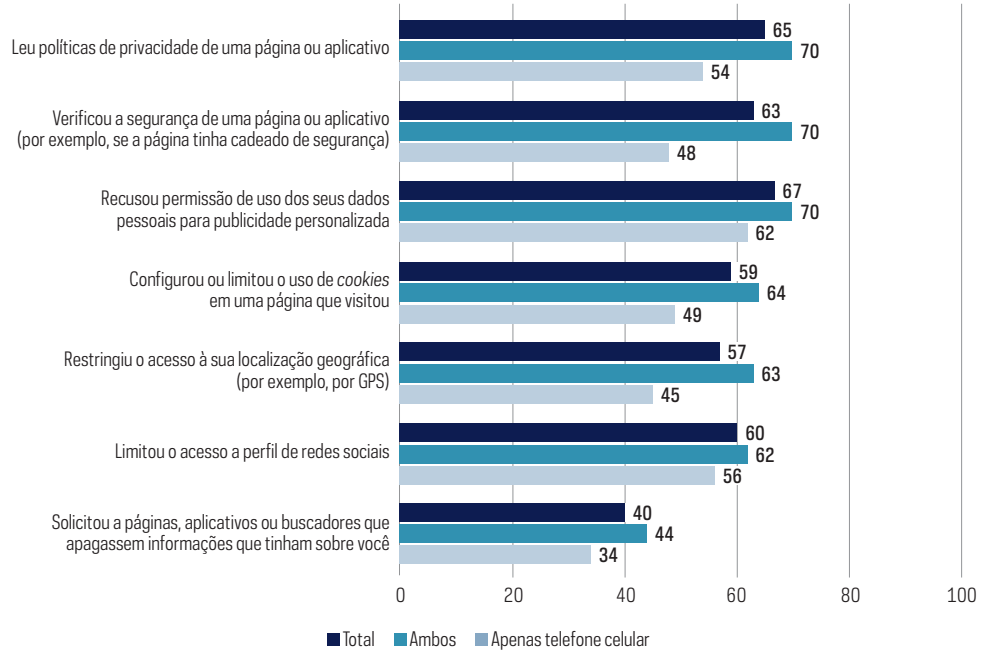
As três categorias mais mencionadas por usuários que combinam telefone celular e computador foram a leitura de políticas de privacidade, a verificação de segurança e a recusa de permissão para publicidade personalizada (todas com 70%). Entre os usuários exclusivos de telefone celular, esta última foi a mais mencionada (62%). Esses resultados reforçam que as condições de acesso e os dispositivos disponíveis constituem dimensões relevantes da conectividade significativa, podendo influenciar a capacidade dos usuários de adotar práticas de proteção de dados no ambiente digital.

GRÁFICO 3

—

Usuários de Internet, por práticas de gerenciamento de acesso a dados pessoais e dispositivo de acesso utilizado (2025)

Total de usuários de Internet com 16 anos ou mais (%)



Ainda sobre as práticas de gerenciamento de dados pessoais, a pesquisa complementou os indicadores com uma pergunta que busca diminuir um possível efeito de respostas socialmente desejadas. Seguindo as mesmas hipóteses descritas no estudo anterior (de que pode existir um efeito de resposta socialmente desejada ou que pode ocorrer uma compreensão heterogênea sobre o que são políticas de privacidade) (CGI.br, 2024b), na edição de 2025, foram repetidas perguntas com formulações que visam reduzir esses problemas. A questão sobre a frequência com que o usuário de Internet concorda com políticas de privacidade sem ler o que dizem indica que a proporção dos usuários de Internet que sempre concorda foi de 23%, enquanto outros 29% afirmaram que o fazem quase sempre e 25% concordam sem ler algumas vezes. Além disso, apenas 14% raramente concordam sem a leitura, e outros 10% nunca o fazem.

Assim como ocorreu em 2023, a desagregação por faixas etárias apresentou diferenças relevantes. Entre usuários de Internet de 25 a 34 anos, 27% afirmaram concordar sempre com as políticas de privacidade sem ler seu conteúdo, proporção que diminui para 13% entre aqueles com 60 anos ou mais. Também é possível identificar diferenças nas alternativas "raramente" e "nunca" na faixa de 60 anos ou mais (Gráfico 4), em que ocorreram as maiores proporções de indivíduos que raramente concordam com as políticas de privacidade sem ler (32%), e que nunca concordam (18%).

Os dados apresentados sugerem uma relação entre a faixa etária dos usuários e suas práticas relacionadas à privacidade e à proteção de dados pessoais que podem refletir diferenças tanto na intensidade de uso das tecnologias quanto na forma como diferentes gerações lidam com riscos digitais e mecanismos de consentimento. O fenômeno indica a necessidade de investigações mais aprofundadas que permitam compreender em que medida e por quais motivos isso ocorre; ademais, também aponta para a relevância de considerar recortes geracionais na formulação de políticas públicas voltadas ao fortalecimento da cultura de proteção de dados no país.

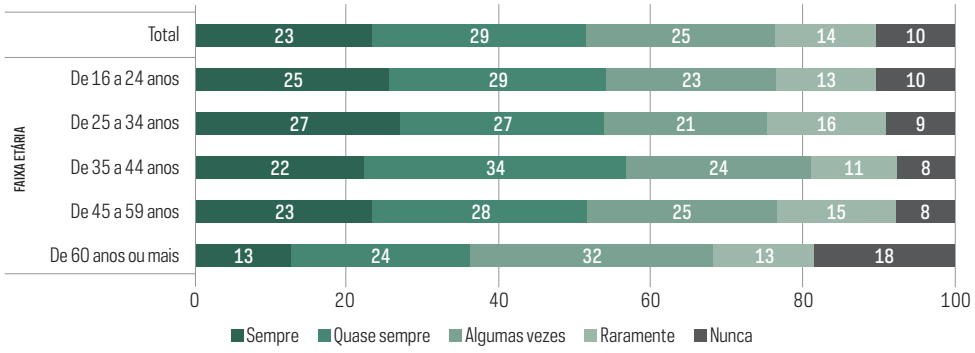
Essa hipótese é corroborada pelos dados da pesquisa TIC Domicílios 2025, que revelam diferenças significativas nos padrões de uso da Internet entre gerações: enquanto 95% dos indivíduos na faixa de 25 a 34 anos são usuários da rede, essa proporção cai para 54% entre os que têm 60 anos ou mais (CGI.br, 2026). Essa disparidade no engajamento digital abre caminho para novas perguntas de pesquisa acerca da influência dos distintos padrões de apropriação tecnológica sobre as percepções de riscos e as atitudes de autoproteção no ambiente *online*.

GRÁFICO 4

—

Usuários de Internet, por frequência de concordância com políticas de privacidade sem ler o que dizem e faixa etária (2025)

Total de usuários de Internet com 16 anos ou mais (%)



A combinação entre ambas as formas de perguntar sobre a leitura de políticas de privacidade permite interpretar que os indivíduos as leem ocasionalmente (ou somente informações que consideram equivalentes a elas), porém frequentemente aceitam os termos sem lê-los e não consultam essas políticas em todas as ocasiões em que são requisitados a fazê-lo. Em conjunto, esses resultados sugerem que a crescente preocupação com privacidade e proteção de dados pessoais não se traduz necessariamente em práticas consistentes de leitura das políticas de privacidade, evidenciando um descompasso entre percepção de risco e comportamento.

BUSCA POR CANAIS DE ATENDIMENTO

De acordo com a pesquisa, em 2025, 26% dos usuários de Internet com 16 anos ou mais buscaram algum canal de atendimento para fazer solicitações, reclamações ou denúncias sobre seus dados pessoais, resultado estável frente ao observado nas duas edições anteriores. A proporção foi maior entre os usuários de sexo masculino (29%) do que entre os de sexo feminino (24%) e entre os que possuem Ensino Superior (29%) do que entre aqueles com Ensino Fundamental (25%) e Ensino Médio (26%). Finalmente, também foi menor entre os usuários de Internet com 60 anos ou mais (17%) do que entre os de 25 a 34 e 35 a 44 anos (29% cada).

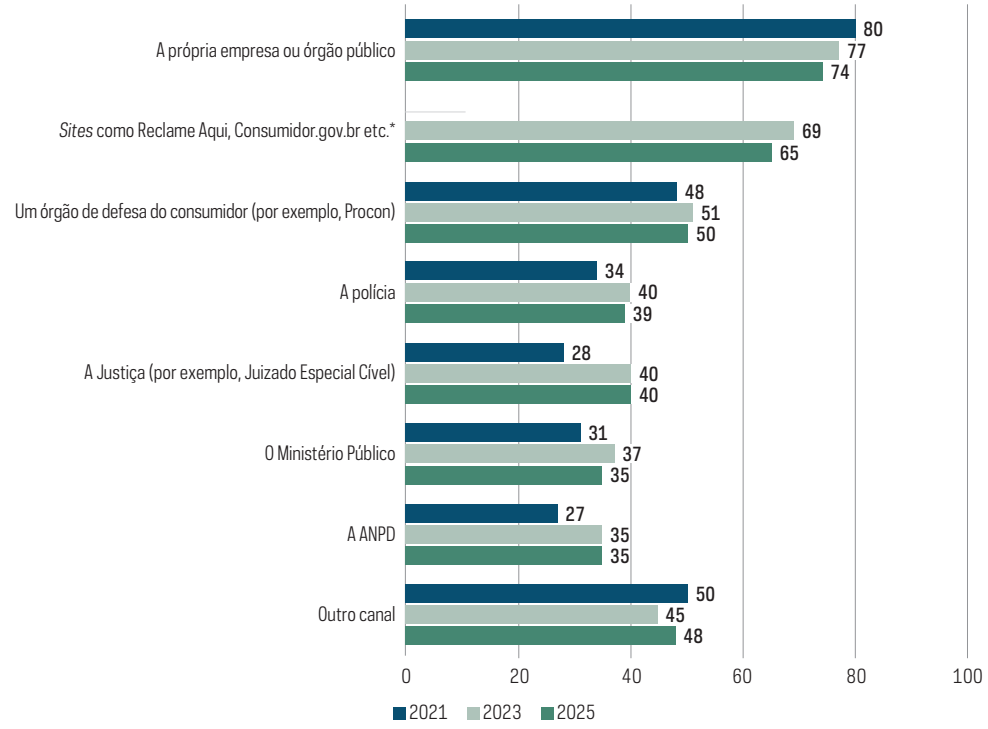
A compreensão acerca do que significa buscar canal de atendimento sobre dados pessoais pode ser ampla. A pergunta explicita "solicitações, reclamações ou denúncias", o que pode estimular na memória do respondente uma ampla variedade de situações. É possível que alguns usuários considerem, por exemplo, a busca por informações acerca dos dados pessoais como uma busca por atendimento.

Entre os que buscaram canal de atendimento, os meios mais mencionados foram a própria empresa ou órgão público controlador do dado (74%), e os *sites* de reclamações de consumidores (65%). O Gráfico 5 demonstra o comparativo entre os resultados observados entre 2021 e 2025.

GRÁFICO 5
—

Usuários de Internet, por canal de atendimento em que buscaram sobre seus dados pessoais (2021–2025)

Total de usuários de Internet com 16 anos ou mais que buscaram algum canal de atendimento sobre seus dados pessoais (%)



Nota: *Categoria de resposta incluída a partir de 2023.

Já entre os usuários que não buscaram canais de atendimento para solicitações, reclamações ou denúncias, os canais mais mencionados para uma eventual necessidade foram a empresa ou órgão público controlador do dado (74%), os órgãos de defesa do consumidor, como Procon (74%), e os *sites* de reclamações de consumidores (65%).

É possível afirmar que a maioria dos usuários busca a organização controladora dos dados, como empresa, órgão público, plataforma ou aplicativo, que registra e detém os dados referentes à solicitação. Em um segundo patamar, estão os órgãos de defesa do consumidor, como o Procon, ou os *sites* de reclamação de consumidores; em terceiro lugar, estão autoridades policiais e a Justiça, além da ANPD.

Assim como verificado nas edições anteriores da pesquisa, os usuários de Internet demonstram tratar as solicitações sobre dados pessoais na mesma lógica de uma relação de consumo ou de ocorrências policiais (Oyadomari *et al.*, 2023). Esse cenário indica que a proteção de dados pessoais como um campo específico de direitos ainda está em processo de apropriação pelos cidadãos. Será relevante para a agenda futura de pesquisa caracterizar melhor essas solicitações e ampliar a compreensão sobre o que está sendo solicitado, de que forma e através de qual canal.

O desafio para a implementação de canais efetivos e específicos para solicitações de serviços relacionados a dados pessoais também está presente na administração pública. A pesquisa TIC Governo Eletrônico 2023 apresenta uma ampla oferta de canais de atendimento genéricos entre os órgãos públicos brasileiros; porém, menos da metade das prefeituras oferece canais para solicitações acerca de dados pessoais (CGI.br, 2024a). Portanto, conforme cresce a oferta de serviços digitais e aumenta o volume de dados pessoais tratados por organizações públicas e privadas, torna-se cada vez mais importante ampliar o conhecimento da população sobre os canais disponíveis para exercer os direitos previstos na LGPD.

Percepção de riscos

A percepção dos usuários de Internet sobre os riscos relacionados ao uso de seus dados pessoais permite compreender como eles avaliam diferentes situações de exposição no ambiente digital. Nesse sentido, a pesquisa investigou os níveis de preocupação com o registro de suas atividades e os principais riscos percebidos no tratamento de seus dados pessoais.

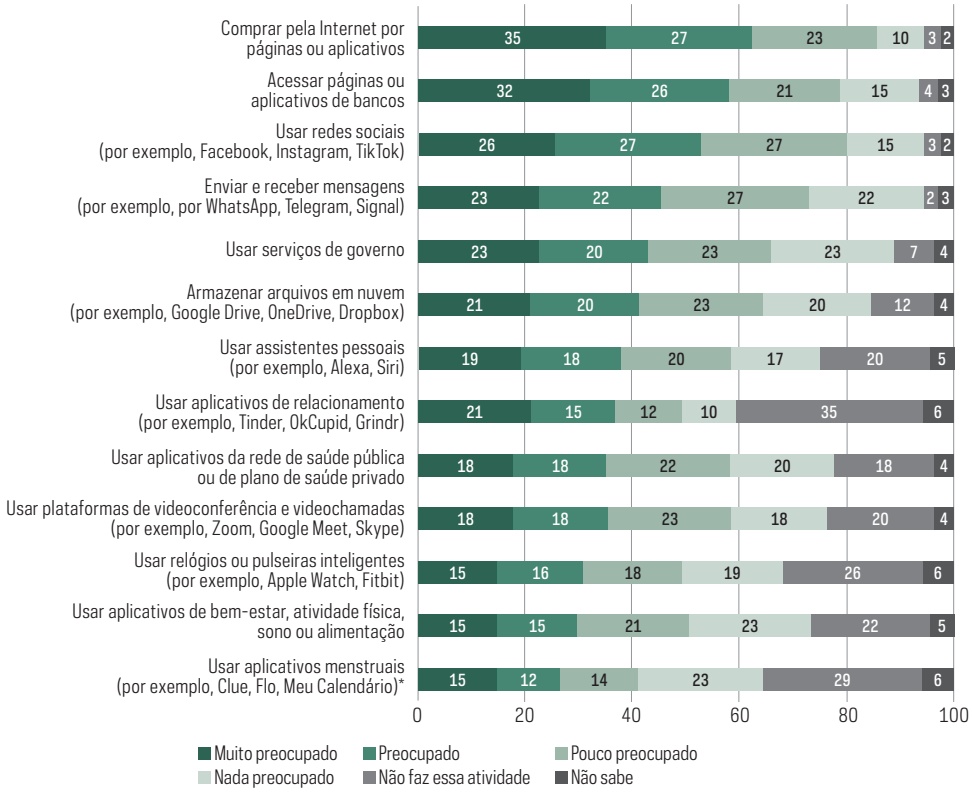
Em relação às atividades realizadas na Internet (Gráfico 6), o nível de preocupação mais elevado foi identificado no momento de realizar compras *online* por páginas e aplicativos (35% muito preocupados e 27% preocupados), seguido de acessar páginas e aplicativos de bancos (32% muito preocupados e 26% preocupados).

GRÁFICO 6

—

Usuários de Internet, por nível de preocupação com seus dados pessoais, segundo atividade realizada na Internet (2025)

Total de usuários de Internet com 16 anos ou mais (%)



Nota: *Considera apenas usuárias de Internet do sexo feminino.

No caso da atividade "usar redes sociais", ocorre uma variação relevante entre os usuários de Internet mais jovens: enquanto 23% dos usuários de 16 a 24 anos afirmam estar muito preocupados e 18%, preocupados, a maioria está pouco preocupada (32%) ou nada preocupada (19%). Em contraste, entre os usuários de 45 a 59 anos, 25% afirmaram estar muito preocupados, 36% preocupados, 24% pouco preocupados e 12% nada preocupados.

No que diz respeito à preocupação relacionada ao uso de serviços de governo, ocorre uma variação relevante por classe social: 27% dos usuários de Internet das classes AB afirmam estar preocupados, enquanto entre os das classes DE essa proporção é de 13%. Quando questionados sobre o nível de preocupação com possíveis tipos de uso dos dados pessoais, as categorias mais frequentes foram compartilhamento com terceiros sem consentimento e prejuízos financeiros por fraudes. Os resultados apontam para uma percepção de riscos concentrada sobretudo em situações de troca de dados pessoais que possam causar prejuízos financeiros e impactar a vida cotidiana dos indivíduos.

A percepção sobre o risco em relação aos dados pessoais explica atitudes cautelosas quanto a atividades realizadas na Internet, em especial com abstenção de atividades em aplicativos ou páginas sem variações significativas nesse indicador em relação à pesquisa de 2023. Segundo a pesquisa, 69% dos usuários de Internet de 16 anos ou mais afirmaram que a preocupação com dados pessoais os levou a desinstalar aplicativos, 68% a deixar de visitar algum *website*, 54% a abandonar algum serviço ou plataforma na Internet, 43% a não comprar algum aparelho eletrônico e 47% a desistir da aquisição de algum outro tipo de produto.

A percepção dos usuários sobre a insegurança do ambiente digital, as dúvidas sobre veracidade das informações, páginas, serviços e aplicativos, além da forma como os dados pessoais serão utilizados, armazenados ou compartilhados, constitui um fator limitador para a adoção de serviços transacionais digitais. Por outro lado, apesar de ser um cenário persistente ao longo de todas as edições da pesquisa, não houve mudanças significativas no conjunto de práticas cotidianas de gerenciamento de dados pessoais por parte dos usuários de Internet. Esse aparente descompasso entre percepção e comportamento evidencia que a conscientização sobre os riscos pode não ser suficiente para promover práticas mais consistentes de proteção de dados pessoais, um contexto que serve como pano de fundo para analisar novos temas emergentes, como o uso de IA e a crescente sofisticação de golpes e fraudes digitais, que trazem novos desafios para a proteção de dados pessoais e interferem cotidianamente na vida dos usuários de Internet no Brasil.

Dados sensíveis e dados biométricos

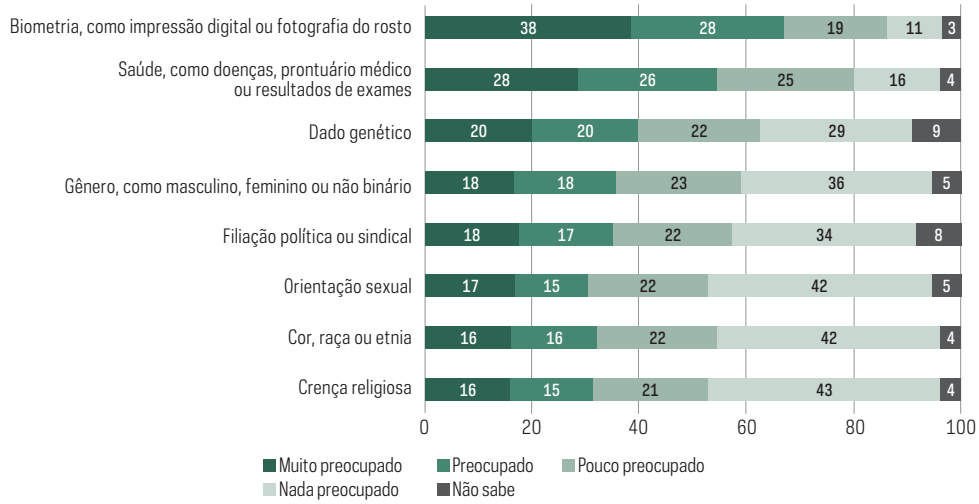
Desde a primeira edição, a pesquisa investiga o nível de preocupação dos usuários de Internet no Brasil em relação ao seus dados pessoais sensíveis. Em 2023, novos indicadores foram incorporados para aprofundar a compreensão sobre o tema, considerando os diferentes tipos de dados pessoais sensíveis indicados na literatura (Teffé, 2022). Esse tema foi investigado novamente na edição de 2025, visto que a crescente utilização de dados biométricos, tanto em organizações públicas quanto privadas, bem como sua incorporação a mecanismos de autenticação e identificação digital, torna-se especialmente relevante para compreender como os usuários percebem a coleta e o tratamento dessas informações.

Segundo a pesquisa, os usuários de Internet declararam nível de preocupação com o fornecimento de dados biométricos em proporção maior do que com relação aos demais tipos de dados pessoais investigados: 38% disseram estar muito preocupados e 28% preocupados (Gráfico 7). Outra categoria que se destacou foi a de dados de saúde: 28% declararam estar muito preocupados e 26% preocupados. Entre os demais tipos de dados sensíveis investigados, as proporções de "muito preocupado" não passam de 20%. O alto nível de preocupação em relação aos dados de saúde pode ocorrer em razão de seu caráter altamente pessoal e do potencial de gerar discriminação ou exposição indevida caso sejam utilizados sem o consentimento dos titulares.

GRÁFICO 7
—

Usuários de Internet, por nível de preocupação com o fornecimento de informações pessoais sensíveis, segundo tipo de informação pessoal sensível (2025)

Total de usuários de Internet com 16 anos ou mais (%)



Com relação ao tipo de dado biométrico fornecido, as preocupações de maior nível foram mais frequentes entre os dados cotidianamente coletados, como a impressão digital e o reconhecimento facial: a soma de usuários preocupados e muito preocupados foi de 83% e 81%, respectivamente. Uma parcela relevante dos usuários de Internet demonstrou estar muito preocupada com todos os tipos de dado biométrico investigados, mesmo aqueles menos presentes no cotidiano. O nível mais baixo de preocupação ocorreu em relação à categoria "Jeito como anda, escreve ou digita"; mesmo nesse caso, 63% dos usuários de Internet declararam estar preocupados ou muito preocupados, o que reforça o entendimento de que a coleta dos dados biométricos é considerada preocupante como um todo. Esse resultado sugere que os usuários atribuem maior preocupação às informações capazes de identificar de maneira única o indivíduo e que, ao contrário das senhas, não podem ser substituídas.

IA generativa

Segundo a TIC Domicílios 2025, 32% dos usuários de Internet usaram alguma ferramenta de IA generativa, com as maiores proporções entre os indivíduos de maior escolaridade e renda, e pertencentes às classes mais altas, além dos mais jovens (CGI.br, 2026). A pesquisa também identificou que os motivos mais mencionados para não utilizar este tipo de ferramenta foram a falta de necessidade ou interesse (76%) e preocupações com segurança e privacidade (63%).

Considerando a disseminação dessas ferramentas e seu potencial para envolver o compartilhamento de informações pessoais, verificou-se a necessidade de ampliar o entendimento sobre a percepção dos usuários de Internet no Brasil acerca do tema. Em vista disso, a pesquisa Privacidade e Proteção de Dados Pessoais 2025 traz três indicadores inéditos sobre o uso da IA generativa. Primeiramente, como forma de distinguir intensidade, investigou-se a frequência de uso dessas ferramentas. Em seguida, para direcionar a entrevista aos dados pessoais no contexto da IA generativa, perguntou-se o tipo de informação fornecida para a ferramenta. Finalmente, questionaram-se os níveis de preocupação ao utilizá-las.

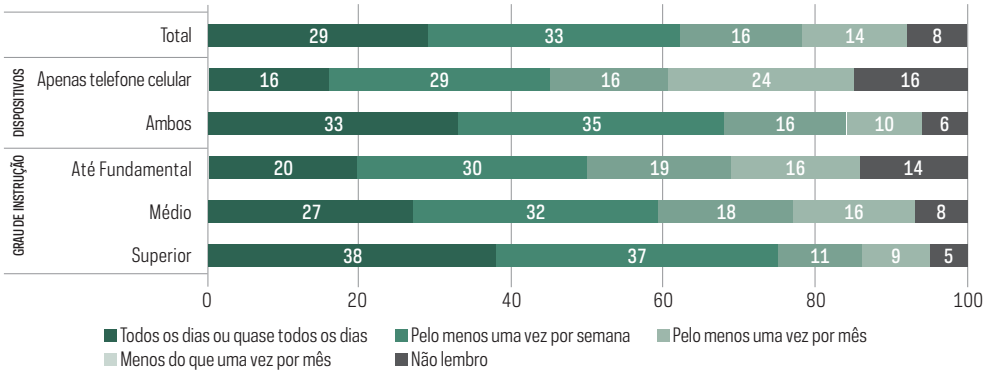
Entre os usuários de IA, a frequência de uso apresentou diferenças relevantes conforme a combinação de dispositivos e a escolaridade: o uso diário foi mais frequente entre os que combinam telefone celular e computador do que entre os que usam exclusivamente o telefone celular, assim como foi maior conforme avançava o grau de escolaridade (Gráfico 8). Os resultados indicam que a IA generativa faz parte da rotina de uma parcela dos usuários de Internet, visto que a maioria dos usuários reporta utilizar essas ferramentas ao menos semanalmente.

GRÁFICO 8

—

Usuários de ferramentas de IA generativa, por frequência de uso segundo dispositivos e escolaridade (2025)

Total de usuários de Internet com 16 anos ou mais que usaram ferramentas de IA generativa (%)



Para melhor caracterizar a natureza desse uso, a pesquisa investigou os tipos de informação fornecidos para as ferramentas de IA generativa. Das categorias investigadas, "temas de trabalho ou de estudo" foi a mais mencionada (73%). Em um segundo patamar inferior, mas com proporções semelhantes, estão: "preferências e gostos pessoais, como filmes ou músicas" (58%), "sentimentos e emoções" (54%), "dados de saúde, como sintomas e exames" (52%) e "fotos suas ou de pessoas conhecidas" (50%). Finalmente, as categorias menos mencionadas foram "finanças pessoais, como orçamentos e investimentos" (41%) e "dados pessoais, como nome, endereço, data de nascimento ou CPF" (37%).

Em linha com investigações recentes realizadas em diversos países, observa-se que o uso da IA generativa tem se ampliado para finalidades que ultrapassam o uso profissional e acadêmico, alcançando também atividades de aconselhamento, suporte emocional e companhia (Lira *et al.*, 2026; União Internacional de Telecomunicações [UIT], 2025). Este tipo de interação tende a estimular o usuário a compartilhar informações de natureza íntima e, em alguns casos, sensíveis, como sentimentos, gostos e dados de saúde. Também se popularizaram nas redes sociais imagens criadas ou editadas por ferramentas de IA, possibilitando o compartilhamento de fotografias próprias e de terceiros com essas plataformas, o que traz novos desafios relacionados à privacidade e à proteção de dados pessoais.

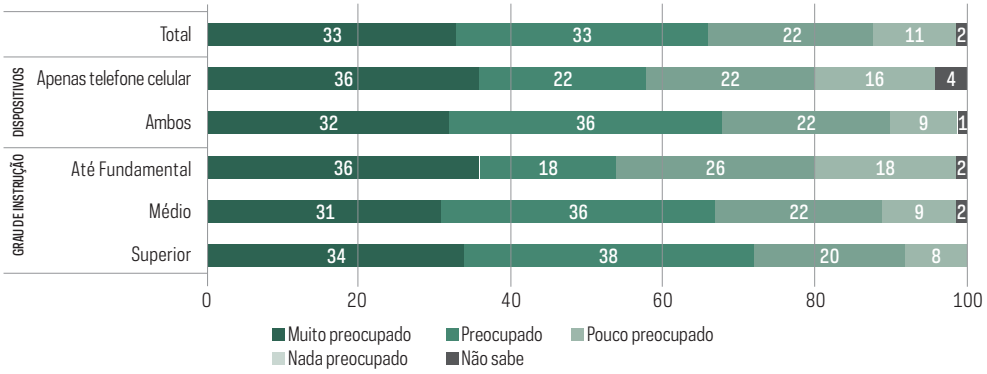
A maioria dos usuários de ferramentas de IA generativa declarou estar muito preocupada ou preocupada com o uso dos dados pelas empresas fornecedoras das ferramentas (Gráfico 9). Esses resultados indicam que, embora eles compartilhem diferentes tipos de informações pessoais com essas ferramentas, permanecem elevados os níveis de preocupação quanto ao tratamento desses dados, sugerindo que reconhecem os potenciais riscos associados a essas tecnologias.

GRÁFICO 9

—

Usuários de ferramentas de IA generativa, por nível de preocupação com o uso dos dados pelas empresas fornecedoras de ferramentas de IA, segundo dispositivos de acesso e escolaridade (2025)

Total de usuários de Internet com 16 anos ou mais que usaram ferramentas de IA generativa (%)



Assim como ocorre com relação ao indicador de frequência de uso, o nível de preocupação também é maior entre os que combinam dispositivos e entre aqueles com nível mais alto de escolaridade. Diante desse cenário, as diferenças observadas entre os usuários, associadas à diversidade de informações compartilhadas com essas ferramentas, reforçam a importância de acompanhar os impactos do uso da IA generativa sobre a privacidade e a proteção de dados pessoais.

Golpes com dados pessoais

Há um crescente debate sobre as estatísticas de criminalidade e sua intersecção com o ambiente digital, impulsionado por diagnósticos globais recentes. Conforme apontado no relatório *Global Financial Fraud Threat Assessment*, da Organização Internacional de Polícia Criminal (Interpol, 2026), os dados empíricos sobre a evolução das novas modalidades de estelionato e fraudes financeiras digitais apoiam governos e entidades privadas na antecipação de tendências complexas de engenharia social. Da mesma forma, relatórios publicados pelo Escritório das Nações Unidas sobre Drogas e Crime (UNODC, 2025) reforçam que a produção de estatísticas é indispensável para monitorar o prejuízo econômico real infligido às famílias e aprimorar os mecanismos institucionais de segurança cibernética.

No âmbito internacional, a principal referência para essas estatísticas sob a perspectiva do cidadão é o *Victimisation Survey Atlas*, desenvolvido pelo Centro de Excelência UNODC–INEGI para Informação Estatística sobre Governo, Segurança Pública, Vitimização e Justiça (Centro de Excelência UNODC–INEGI, 2025). Essa ferramenta padroniza metodologias utilizadas globalmente para dar visibilidade à chamada "cifra negra": a parcela de delitos que a sociedade sofre, mas não notifica às autoridades. No cenário atual, os crimes cibernéticos e os golpes virtuais representam a principal fronteira dessa subnotificação, já que a maioria das vítimas de fraudes digitais deixa de formalizar queixas por desacreditarem na recuperação dos valores ou na identificação dos criminosos.

Além de dimensionar a real extensão do estelionato digital e identificar os canais em que ele ocorre, tais indicadores permitem mapear o perfil demográfico dos grupos mais vulneráveis. Assim, esse diagnóstico gera evidências fundamentais tanto para conscientizar os cidadãos quanto para fortalecer as capacidades preventivas das instituições envolvidas.

A necessidade de dados precisos é urgente na América Latina e no Caribe, regiões que registraram uma digitalização acelerada nos últimos anos, acompanhada pelo aumento exponencial nas taxas de golpes virtuais. Para harmonizar esse diagnóstico regional e integrar o cibercrime às métricas de segurança, a Organização das Nações Unidas (ONU) promove, desde 2013, a Iniciativa de Pesquisas de Vitimização na América Latina e Caribe (Lacsi); por meio de questionários padronizados, a proposta busca medir, de forma comparável, o impacto real das fraudes eletrônicas nos diferentes países da região (Centro de Excelência UNODC–INEGI, 2013).

Apesar de a pesquisa Privacidade e Proteção de Dados Pessoais 2025 não comportar um questionário completo dedicado à temática, houve uma abordagem preliminar por meio da inclusão de três indicadores sobre golpes envolvendo dados pessoais. Antes da aplicação das perguntas, foi apresentado aos respondentes um breve texto explicativo para contextualizar o tema.

A pesquisa identificou que, em 2025[2], 32% dos usuários de Internet vivenciaram tentativas de golpes usando seus dados pessoais, enquanto 20% foram vítimas de golpes em que seus dados pessoais foram usados. Entre aqueles que passaram por essas situações, quando perguntados sobre os canais em que essas situações ocorreram (tanto as tentativas quanto os golpes bem-sucedidos), as categorias de resposta mais mencionadas foram aplicativos de mensagens (84%) e ligações telefônicas (79%). Outros canais investigados foram *sites* ou aplicativos falsos (71%), mensagens curtas (*Short Message Service* [SMS]) (71%), *e-mail* (69%) e redes sociais (67%). Os resultados evidenciam que os golpes envolvendo dados pessoais ocorrem por múltiplos canais de comunicação, combinando meios digitais e tradicionais, com o objetivo de alcançar potenciais vítimas. Tal cenário demonstra que a exposição a situações fraudulentas tem potencial de alcançar inclusive indivíduos não usuários de Internet, uma vez que são comuns também as tentativas por meio de telefone e SMS.

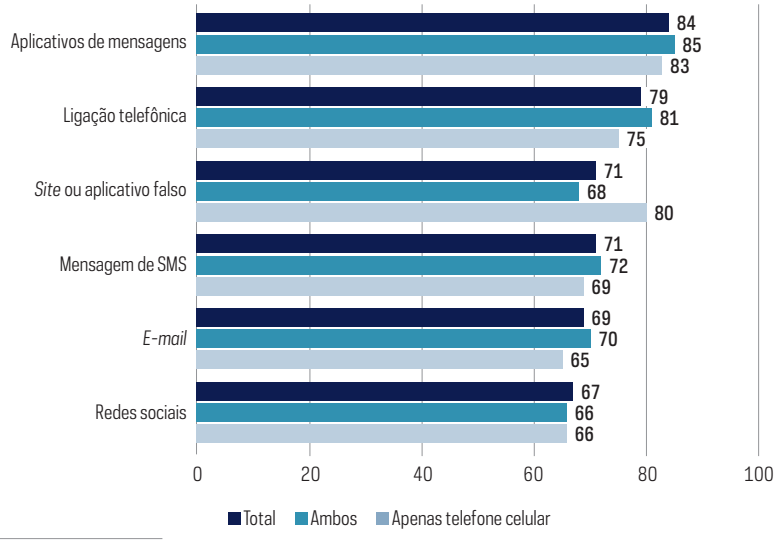
O dispositivo utilizado para acessar a Internet apresentou variação significativa para a categoria de resposta *site* ou aplicativo falso, sendo mais mencionada entre os indivíduos que utilizam apenas telefone celular (Gráfico 10). Essa diferença ilustra como dimensões de conectividade significativa se relacionam com a segurança e a proteção de dados, uma vez que os indivíduos inseridos em contextos de uso de uso mais restrito podem ter mais dificuldade em desempenhar práticas de verificação de segurança.

GRÁFICO 10

—

Usuários de Internet que vivenciaram situações envolvendo golpes, por canais em que essas situações ocorreram, segundo dispositivo de acesso utilizado (2025)

Total de usuários de Internet com 16 anos ou mais que vivenciaram tentativa de golpe ou foram vítimas de golpe usando dados pessoais (%)



[2] Diferentemente de outras atividades investigadas na pesquisa que adotaram como referência "nos últimos três meses", esse conjunto de perguntas considerou "no ano de 2025", na tentativa de reduzir uma possível sazonalidade e ampliar o escopo de investigação para 12 meses. Como a coleta ocorreu integralmente em uma quinzena do mês de dezembro de 2025, a formulação facilitou ao respondente situar corretamente os eventuais acontecimentos de que se recorda dentro ou fora do ano corrente.

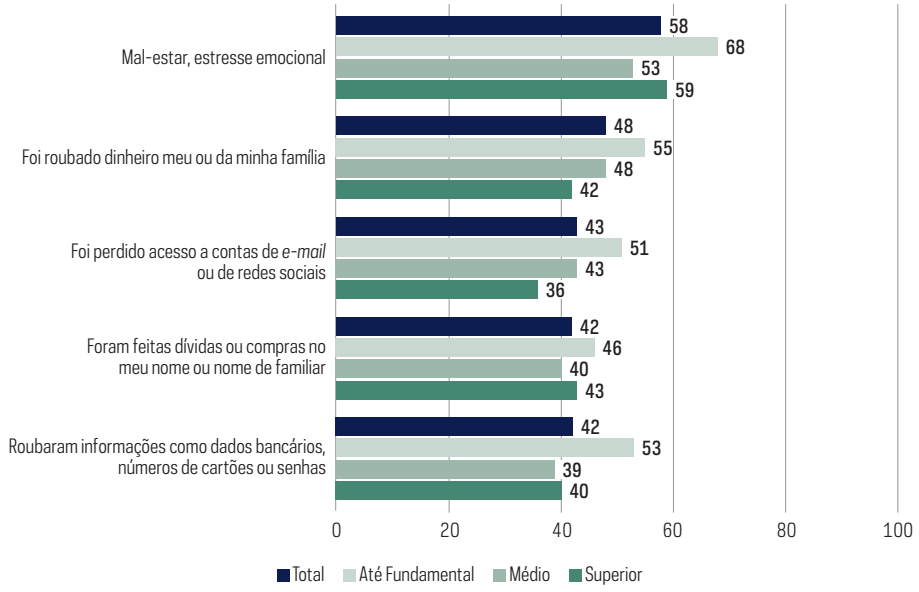
Quando perguntados sobre as decorrências das situações envolvendo golpes com dados pessoais, os respondentes mencionaram consequências que extrapolam o dano patrimonial e os efeitos diretamente relacionados aos dados, incluindo impactos emocionais e repercussões mais amplas sobre o bem-estar. Além disso, observam-se variações significativas segundo o nível de escolaridade: todas as categorias foram mais frequentemente mencionadas por indivíduos que concluíram até o Ensino Fundamental (Gráfico 11).

GRÁFICO 11

—

Usuários de Internet que vivenciaram situações envolvendo golpes, por decorrências dessas situações, segundo grau de instrução (2025)

Total de usuários de Internet com 16 anos ou mais que vivenciaram tentativa de golpe ou foram vítimas de golpe usando dados pessoais (%)



Diante desse cenário, observa-se que os golpes envolvendo dados pessoais representam uma dimensão relevante dos riscos associados ao uso das tecnologias digitais. Além da frequência das tentativas e da diversidade dos canais utilizados, suas consequências podem extrapolar as perdas financeiras, evidenciando a importância de acompanhar esse tema.

Considerações finais: agenda para políticas públicas

A análise da perspectiva dos usuários de Internet sobre questões de proteção de dados pessoais oferece subsídios valiosos para o aprimoramento de políticas públicas no Brasil. Desde a promulgação da LGPD e a subsequente atuação da ANPD, observa-se um avanço significativo na cobertura legal e regulatória do tema, especialmente no âmbito de organizações públicas e privadas. No entanto, para que essa agenda seja consolidada e disseminada no cotidiano dos cidadãos, torna-se fundamental compreender como os brasileiros percebem, vivenciam e respondem aos desafios da privacidade no ambiente digital.

A investigação das práticas cotidianas relacionadas à proteção de dados permite comparar as percepções dos indivíduos sobre privacidade com seus comportamentos efetivos no uso de tecnologias digitais. Nesta edição, a pesquisa aprofundou a análise sobre a leitura de políticas de privacidade, tema intrinsecamente ligado ao consentimento informado. Os resultados indicam um descompasso entre o comportamento declarado pelos usuários e suas práticas efetivas, com os usuários manifestando comportamentos socialmente esperados (como afirmar que leem os termos de uso) que não se confirmam na prática ou não são adotados de maneira consistente em todas as ocasiões. Além disso, identificaram-se diferenças relevantes associadas à faixa etária dos indivíduos, o que aponta para a necessidade de políticas públicas que considerem recortes geracionais no fomento à cultura de proteção de dados.

Outro aspecto relevante diz respeito à distinção de comportamento entre usuários que acessam a Internet exclusivamente via telefone celular e aqueles que combinam o uso de computador e telefone. Essa diferença ressalta a importância de considerar as várias realidades de acesso e conectividade no debate sobre proteção de dados, especialmente no que tange à capacidade dos usuários em situação de maior vulnerabilidade digital para adotar boas práticas de segurança. O conceito de conectividade significativa (Núcleo de Informação e Coordenação do Ponto BR [NIC.br], 2024), que considera dimensões como custo, dispositivo, qualidade e habilidades digitais, tem ganhado espaço no campo da inclusão digital; nesse cenário, os resultados desta pesquisa sugerem que a segurança e a proteção de dados devem ser incorporadas como qualificadores desses níveis de conectividade.

Tal como observado na edição anterior, os riscos percebidos pelos usuários de Internet permanecem majoritariamente associados a prejuízos financeiros e fraudes, seguidos por preocupações como vigilância em espaços públicos, risco de discriminação e sensibilidade inerente a dados pessoais de saúde ou biométricos. Esse padrão evidencia que a preocupação em relação a roubo de dados para o cometimento de golpes é predominante entre os brasileiros, reforçando a urgência de aprimorar a segurança no ambiente digital nacional.

Nesta edição, a pesquisa também aprofundou a mensuração de aspectos relacionados aos dados biométricos, dando continuidade à discussão iniciada no estudo anterior. Os resultados confirmam que esse tema é particularmente sensível aos usuários, dado o elevado potencial de risco percebido, especialmente em relação às categorias mais utilizadas, como reconhecimento facial e impressão digital. A percepção de risco é significativamente maior quando a coleta é realizada por organizações públicas e pelo setor bancário, sugerindo que os usuários associam essas informações ao risco de roubo de identidade para cometimento de fraudes. Por outro lado, a preocupação é menor em relação a organizações privadas de menor porte, o que indica que a multiplicação de pontos de coleta de dados biométricos e seu consequente armazenamento preocupam menos o usuário do que o fornecimento dessas informações a instituições de maior porte e relevância. Essa hipótese, bem como os resultados que a embasam, oferece um desafio à sociedade no que se refere à regulamentação de coleta, armazenamento e uso de informações biométricas para fins de identificação.

Os achados da pesquisa apontam para a convergência de duas tendências que se revelam particularmente desafiadoras para a agenda de proteção de dados no Brasil: a crescente utilização de IA generativa pelos usuários e a ampliação de golpes e fraudes que exploram dados pessoais. Esse diagnóstico é corroborado pelo *20º Anuário Brasileiro de Segurança Pública* (Fórum Brasileiro de Segurança Pública [FBSP], 2026), que registrou, no Brasil, 2,2 milhões de casos de estelionato em 2025, número mais de quatro vezes superior ao registrado em 2018. A pesquisa do Fórum também revelou que 26,3 milhões de brasileiros foram vítimas de golpes na Internet, evidenciando uma subnotificação expressiva, que não é capturada integramente pelos registros oficiais em sua totalidade.

Embora a LGPD e a atuação da ANPD tenham estabelecido marcos regulatórios importantes, a rápida disseminação de ferramentas de IA impõe novos patamares de complexidade ao debate sobre privacidade. A pesquisa Privacidade e Proteção de Dados Pessoais 2025 evidenciou que os usuários compartilham com essas plataformas informações cada vez mais íntimas e sensíveis, como sentimentos, dados de saúde e preferências pessoais.

Simultaneamente, a preocupação com o uso de dados para fraudes e golpes se mantém como o principal temor dos brasileiros, refletindo um cenário internacional descrito pelo UNODC (2025) e pelo *Victimisation Survey Atlas,* do Centro de Excelência do UNODC-INEGI (2025), que documentam a expansão global de centros de fraude e o uso crescente de IA por organizações criminosas. Esse diagnóstico sugere que as políticas públicas de proteção de dados não devem se restringir ao ambiente corporativo e às relações de consumo, pois precisam incorporar estratégias de conscientização e capacitação digital da população, bem como mecanismos de governança específicos para o uso de IA que considerem os riscos de manipulação, discriminação e fraudes. A coordenação entre a ANPD, o poder público, o setor privado e a sociedade civil será, portanto, fundamental para enfrentar esses desafios.

Referências

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Centro de Excelência UNODC–INEGI para Informação Estatística sobre Governo, Segurança Pública, Vitimização e Justiça. (2013). *Iniciativa de Pesquisas de Vitimização na América Latina e Caribe (LACSI)*. https://www.cdeunodc.inegi.org.mx/unodc/index.php/lacsi-initiative/index.htm

Centro de Excelência UNODC–INEGI para Informação Estatística sobre Governo, Segurança Pública, Vitimização e Justiça. (2025). *Victimisation Survey Atlas*. https://www.cdeunodc.inegi.org.mx/unodc/index.php/atlas-on-cvs/index.htm

Comissão Europeia. (2015). *Special Eurobarometer 431: Data protection.* (Special Eurobarometer 431 / Wave EB83.1). https://doi.org/10.2838/552336

Comitê Gestor da Internet no Brasil. (2022). *Privacidade e Proteção de Dados Pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-pessoais-2021-perspectivas-de-individuos-empresas-e-organizacoes-publicas-no-brasil/

Comitê Gestor da Internet no Brasil. (2024a). *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo Eletrônico 2023*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2023/

Comitê Gestor da Internet no Brasil. (2024b). *Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-pessoais-2023-perspectivas-de-individuos-empresas-e-organizacoes-publicas-no-brasil/

Comitê Gestor da Internet no Brasil. (2026). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2025*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2025/

Escritório das Nações Unidas sobre Drogas e Crime. (2025). *What to know about cybercrime in 2026*. https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html

Friedman, J., Hastie, T., & Tibshirani, R. (2010). Regularization paths for generalized linear models via coordinate descent. *Journal of Statistical Software*, *33*(1), 1–22. https://doi.org/10.18637/jss.v033.i01

Fórum Brasileiro de Segurança Pública. (2026). *20º Anuário Brasileiro de Segurança Pública: dados de 2025*. https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/

Lei Geral de Proteção de Dados Pessoais. Lei n. 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Lira, B., Folk, D., Ungar, L., & Duckworth A. L. (2026). *How Gen Z uses Gen AI – and why it worries them*. Harvard Business Review. https://hbr.org/2026/01/how-gen-z-uses-gen-ai-and-why-it-worries-them

Núcleo de Coordenação e Informação do Ponto BR. (2024). *Conectividade significativa: propostas para medição e o retrato da população no Brasil.* (Cadernos NIC.br de Estudos Setoriais). https://cetic.br/pt/publicacao/conectividade-significativa-propostas-para-medicao-e-o-retrato-da-populacao-no-brasil/

Organização Internacional de Polícia Criminal. (2026). *Global financial fraud threat assessment.* https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

Oyadomari, W., Costa, R. S., & Ribeiro, M. M. (2023). Perspectivas da sociedade brasileira em relação à privacidade e à proteção de dados pessoais. *Panorama Setorial da Internet*, *15*(2), 1–11. https://cetic.br/pt/publicacao/ano-xv-n-2-protecao-de-dados-pessoais-privacidade-e-confianca-no-ambiente-digital/

Teffé, C. (2022). *Dados pessoais sensíveis, qualificação, tratamento e boas práticas*. Foco.

Tibshirani, R. (1996). Regression shrinkage and selection by the LASSO. *Journal of the Royal Statistical Society: Series B (Methodological)*, *58*(1), 267–288. https://academic.oup.com/jrsssb/article/58/1/267/7027929

União Internacional de Telecomunicações. (2025). *Report of the EGH subgroup on measuring artificial intelligence (AI) through household surveys*. https://www.itu.int/dms_pub/itu-d/md/22/egh.ai.2025/r/D22-EGH.AI.2025-R-0001!!PDF-E.pdf

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2025
Empresas

A crescente digitalização das atividades econômicas tem ampliado o volume e a diversidade de dados pessoais tratados pelas empresas brasileiras. Relações com clientes, fornecedores e trabalhadores, processos de contratação, comércio eletrônico, *marketing* digital e, mais recentemente, uso de sistemas baseados em Inteligência Artificial (IA) fazem com que organizações de diferentes portes passem a lidar cada vez mais com informações pessoais em suas operações. Nesse contexto, acompanhar como as empresas têm incorporado práticas de privacidade e proteção de dados torna-se fundamental para compreender o estágio de implementação da Lei Geral de Proteção de Dados Pessoais ([LGPD], Lei n. 13.709/2018) e as oportunidades e os desafios para o fortalecimento de uma economia digital transparente e segura.

Ao mesmo tempo, esse ambiente de crescente digitalização e transformação tecnológica pode contrastar com o ritmo de disseminação de práticas de privacidade e proteção de dados pessoais nas empresas brasileiras. Nesse sentido, ainda há desafios importantes para as empresas em sua busca por conformidade à LGPD. Por exemplo, se, de um lado, a IA amplia os desafios relacionados ao tratamento legítimo de dados pessoais[1], de outro, novas regras surgiram para complementar ou especificar aspectos abordados na lei com foco em públicos ou situações particulares.[2]

Dessa forma, o cenário colocado para as empresas é delineado por desafios oriundos do avanço tecnológico e da crescente demanda para adoção de tecnologias avançadas, como a IA, aliados à necessidade de buscar conformidade com regramentos que orientam e estabelecem parâmetros à sua atuação no ambiente digital. Nesse contexto, independentemente do porte das empresas, a adoção de boas práticas de privacidade e proteção de dados pessoais pode representar não somente um meio para evitar sanções e danos à sua imagem em relação ao público, mas também se tornar cada vez mais um ativo para diferenciar a empresa em relação a concorrentes, fortalecendo sua reputação

[1] O avanço do uso da IA generativa coloca desafios sobre o tratamento de dados pessoais, seja pela possibilidade de abusos ou pelo uso indiscriminado para treinamento (Agência Nacional de Proteção de Dados [ANPD], 2024). De acordo com a TIC Domicílios 2025, 32% dos usuários de Internet utilizaram ferramentas de IA generativa no Brasil, com uso mais frequente entre indivíduos da classe A (69%) e com Ensino Superior (59%) (Núcleo de Informação e Coordenação do Ponto BR [NIC.br], 2026c).

[2] Um exemplo é o debate em torno dos mecanismos de aferição de idade, associado à entrada em vigor do Estatuto Digital da Criança e do Adolescente ([ECA Digital], Lei n. 15.211/2025), e sua relação com a proteção de dados pessoais (ANPD, 2026).

e a confiança de clientes e parceiros, especialmente diante de vazamentos ou uso inadequado de seus dados pessoais.

Assim, os resultados da terceira edição da pesquisa sobre privacidade e proteção de dados pessoais nas empresas brasileiras devem ser interpretados nesse cenário de maior complexidade tecnológica e regulatória. Nesse contexto, a edição de 2025 mostra poucas alterações em relação aos dados de 2023, evidenciando que, apesar das transformações observadas em outros indicadores da pesquisa TIC Empresas, como a maior adoção de IA em todos os portes[3], em geral não houve mudanças significativas na proporção de empresas que adotam boas práticas de proteção de dados pessoais, sobretudo entre aquelas de pequeno porte. Além disso, nas grandes empresas e no setor de informação e comunicação, permanece uma maior proporção daquelas com ações em relação ao tratamento de dados pessoais investigadas pela pesquisa.

Entre a edição anterior da pesquisa e a presente, embora não tenham ocorrido alterações abrangentes no marco regulatório aplicável às práticas de privacidade e proteção de dados pessoais das empresas, o período foi marcado por mudanças institucionais relevantes. A principal delas foi a edição da Medida Provisória n. 1.317/2025[4], transformando a Autoridade Nacional de Proteção de Dados em uma agência reguladora de natureza autárquica, a Agência Nacional de Proteção de Dados. Um exemplo da ampliação do escopo de atuação decorrente do fortalecimento institucional do órgão regulador é o Decreto n. 12.622/2025, que designou a ANPD como autoridade administrativa autônoma responsável pela regulamentação, orientação e fiscalização dessa legislação voltada para a proteção dos direitos de crianças e adolescentes no ambiente digital.[5]

No caso do ECA Digital, há implicações para a atuação *online* das empresas, principalmente aquelas com serviços e plataformas de acesso provável por crianças e adolescentes[6]. Entre elas, a necessidade de implementar mecanismos efetivos de aferição de idade deve ser considerada pelas empresas, o que pode demandar o desenvolvimento ou a adoção de soluções tecnológicas específicas no mercado. Tal fato é importante, uma vez que essas ferramentas devem observar os princípios e as regras aplicáveis ao tratamento de

[3] A pesquisa TIC Empresas 2025 mostrou que 17% das empresas brasileiras usaram algum tipo de tecnologia de IA, representando crescimento de cinco pontos percentuais em relação ao ano de 2024. Entre as empresas que usaram IA, 44% afirmaram que a utilizaram para *marketing* ou vendas, o que requer cuidados acerca do tratamento de dados pessoais, sobretudo de menores de 18 anos de idade (NIC.br, 2026b).

[4] Posteriormente, a medida foi convertida na Lei n. 15.352/2026, tornando a ANPD uma autarquia especial sob a forma de agência reguladora, mantendo o vínculo com o Ministério da Justiça e Segurança Pública (MJSP).

[5] Um exemplo das atividades atribuídas à ANPD nesse âmbito é o recebimento de ordens de bloqueio de *sites* que descumpram requisitos previstos pela lei.

[6] O ECA Digital traz uma definição ampla sobre produtos e serviços de tecnologia, gerando interpretações diversas sobre o escopo da Lei, sobretudo em relação ao conceito de acesso provável. Segundo o Comitê Gestor da Internet no Brasil (CGI.br): "A amplitude da definição demonstra a intenção do legislador de alcançar diferentes agentes que participam da oferta de produtos e serviços digitais direcionados ou de provável acesso a crianças e adolescentes. Ao mesmo tempo, essa abrangência demanda critérios interpretativos que permitam distinguir adequadamente os diferentes tipos de fornecedores abrangidos pela definição legal, considerando suas funções e características no ecossistema digital." (CGI.br, 2026a, p. 4).

dados pessoais, já que se trata de impedir ou restringir o acesso de crianças e adolescentes a certas aplicações ou plataformas na Internet, por exemplo, lojas de aplicativos.[7]

Assim, é central para as empresas o acompanhamento da evolução das regulamentações, bem como a avaliação contínua de sua conformidade diante da atuação do regulador. Portanto, elas devem estar atentas ao tratamento de dados pessoais e suas relações com legislações correlatas, como o ECA Digital, bem como a outros marcos legais aplicáveis ao ambiente digital, a fim de fortalecer a governança de dados, contribuindo para um ambiente digital mais seguro e confiável.

Dessa forma, em um ambiente de crescente complexidade técnica e legal, é importante que as empresas promovam ações voltadas à conformidade com a legislação e o fortalecimento de boas práticas de segurança digital, com o intuito de redução de riscos que podem levar a danos financeiros e reputacionais. O aumento da presença *online* das empresas amplia sua exposição a ataques cibernéticos; quando não acompanhada de práticas adequadas de governança de dados, também aumenta os riscos de descumprimento da legislação aplicável. Portanto, amplia-se a responsabilização das empresas que atuam na economia digital, o que reforça a importância da cultura de proteção de dados e da segurança da informação nessas organizações.

Nesse contexto, considerando os dados coletados por meio de entrevistas com pequenas, médias e grandes empresas no Brasil, a presente análise está organizada em três seções:

- **Guarda de dados pessoais e finalidade de uso:** indicadores sobre os tipos de dados pessoais mantidos pelas empresas e para quais fins são utilizados;
- **Desenvolvimento de capacidades internas:** indicadores sobre ações para a sensibilização e capacitação da equipe interna das empresas sobre o tema de privacidade e proteção de dados pessoais;
- **Adequação à LGPD:** indicadores sobre ações que visam ampliar a conformidade com a lei e buscam fortalecer boas práticas de tratamento de dados pessoais na empresa.

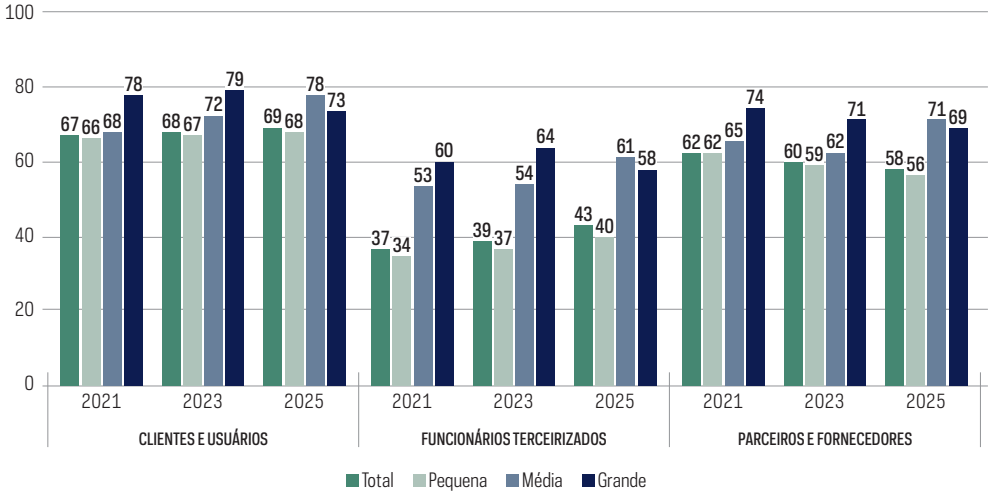
[7] De acordo com a ANPD, esses mecanismos devem se coadunar com os princípios de tratamento de dados pessoais descritos na LGPD, mas também devem considerar preceitos do Estatuto da Criança e do Adolescente (ECA) e do Código de Defesa do Consumidor (CDC): "É com base nesse modelo regulatório que se deve compreender o comando do art. 9º, *caput* e § 1º, do ECA Digital, que determina que os mecanismos de aferição de idade adotados sejam 'confiáveis'. Trata-se, nesse sentido, de uma obrigação que decorre do dever geral imposto aos fornecedores de serviços e produtos de atuar de forma proativa e diligente para prevenir e mitigar riscos a crianças e adolescentes no ambiente digital. O mesmo dispositivo estabelece, ainda, que devem ser adotadas medidas 'eficazes' para impedir o acesso de crianças e adolescentes a conteúdo, produtos ou serviços cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de dezoito anos." (ANPD, 2026, p. 5).

Guarda de dados pessoais e finalidade de uso

Assim como nas edições anteriores da pesquisa, o tipo de dado pessoal mais mantido pelas empresas brasileiras é proveniente de clientes e usuários[8]: em 2025, 69% das empresas afirmaram manter esse tipo de dado, seguidas de 58% que mantêm dados de parceiros e fornecedores (Gráfico 1). Do ponto de vista do porte, o mesmo padrão é observado, com as grandes empresas apresentando maior nível de manutenção de dados pessoais de clientes e usuários (73%).

GRÁFICO 1
—

Empresas, por tipo de dado pessoal mantido e porte (2021–2025)
Total de empresas (%)



Entre os dados pessoais tratados pelas empresas, a LGPD prevê que o tratamento de dados sensíveis requer cuidados especiais[9]. No conjunto investigado pela pesquisa, a biometria permaneceu como o dado mais frequentemente mantido pelas empresas: 31% delas o mantiveram em 2025, proporção que foi de 30% em 2023[10]. Em seguida, os dados

[8] A pesquisa TIC Empresas tem um indicador sobre o uso de dados e as fontes de coleta. Em 2025, 20% das empresas brasileiras coletaram dados internamente, a partir de processos e equipes, com proporção de 56% entre as grandes empresas. Por sua vez, 16% das empresas coletaram dados de clientes e usuários, atingindo 37% das grandes empresas (NIC.br, 2026b).

[9] De acordo com a LGPD, dado pessoal sensível é o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Lei n. 13.709/2018).

[10] Importante mencionar que, conforme a LGPD, os dados sensíveis podem ser tratados mediante consentimento dos titulares, mas também sem este, em ocasiões específicas conforme destacado pela lei no inciso II do art. 11.

sensíveis de saúde foram mantidos por 26% das empresas em 2025, mesma proporção da edição anterior (Gráfico 2). Em termos setoriais, a manutenção dos dados de saúde foi mais frequente nos setores de construção (35%) e atividades profissionais (36%). Tal qual previsto no § 4º do art. 11 da LGPD, o tratamento dos dados de saúde tem restrições específicas, sobretudo no uso compartilhado entre controladores, visando angariar vantagens econômicas.

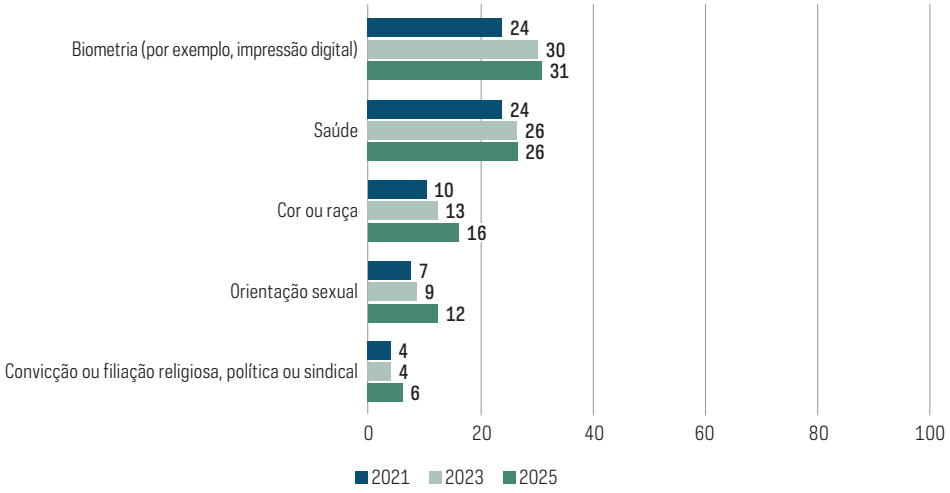
Os resultados indicam, portanto, que a guarda de dados sensíveis pelas empresas permanece nos patamares observados nas edições anteriores da pesquisa; o que reforça a necessidade de que esse tratamento seja feito conforme especificado na lei[11]. Esse cenário demanda que as empresas adotem práticas adequadas ao longo do ciclo de tratamento dos dados pessoais, sobretudo no caso de dados sensíveis, a fim de reduzir riscos associados e evitar abusos que possam levar a potenciais sanções e multas.[12]

GRÁFICO 2

—

Empresas, por tipo de dado sensível mantido (2021–2025)

Total de empresas (%)



[11] Por exemplo, no art. 38: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial." (Lei n. 13.709/2018).

[12] Um exemplo de obrigações na forma do tratamento de dados pessoais está na seção sobre segurança e sigilo de dados (art. 46), com a possibilidade de exigências de padrões técnicos mínimos para proteção de dados, principalmente aqueles de natureza sensível: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." (Lei n. 13.709/2018).

Entre as empresas que mantêm dados pessoais de clientes e usuários, 9% afirmaram armazenar dados pessoais de menores de 18 anos de idade, com maior frequência entre as empresas de grande porte (21%) e do setor de alojamento e alimentação (19%)[13] (Gráfico 3). Ainda que os resultados não tenham apresentado variações significativas em relação aos anos anteriores, é importante mencionar que a manutenção de dados pessoais de crianças e adolescentes requer cuidados específicos previstos na LGPD, a começar pelos requisitos relacionados ao melhor interesse e, no caso das crianças, pelo requisito de consentimento específico e em destaque de pelo menos um dos pais ou responsável legal, bem como a publicização dos tipos de dados coletados e a forma de utilização (art. 14)[14]. Aliado a isso, com a promulgação do ECA Digital em 2025, foram ampliadas as responsabilidades das empresas, especialmente em relação ao direcionamento de publicidade a esse público, envolvendo maior controle sobre essa prática[15]. Portanto, o tratamento de dados pessoais de menores de 18 anos demanda mecanismos de governança capazes de assegurar maior controle na coleta desses dados, com mais restrições na finalidade de uso e no compartilhamento dessas informações.[16]

[13] De acordo com a pesquisa TIC Kids Online Brasil 2025, 20% dos usuários de Internet de 9 a 17 anos afirmaram que compraram pela Internet. Entre os usuários de 11 a 17 anos, 84% relataram ter visto divulgação de produtos e marcas. Em relação a práticas para a proteção de privacidade, 61% dos usuários de Internet de 11 a 17 anos bloquearam mensagens de alguém que não queria conversar, enquanto 52% alteraram as configurações de privacidade para que menos pessoas pudessem acessar seu perfil (NIC.br, 2026a).

[14] Um exemplo da relação entre o ECA Digital e a LGPD, no sentido de maior controle ao tratamento de dados pessoais de menores de 18 anos, é a exigência prevista no art. 16, parágrafo único, do ECA Digital, segundo o qual, no caso de tratamento de dados pessoais para fins que não sejam estritamente necessários, deve o controlador: "I – mapear os riscos e envidar esforços para mitigá-los; e II – elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, na forma de regulamento." (Lei n. 15.211/2025).

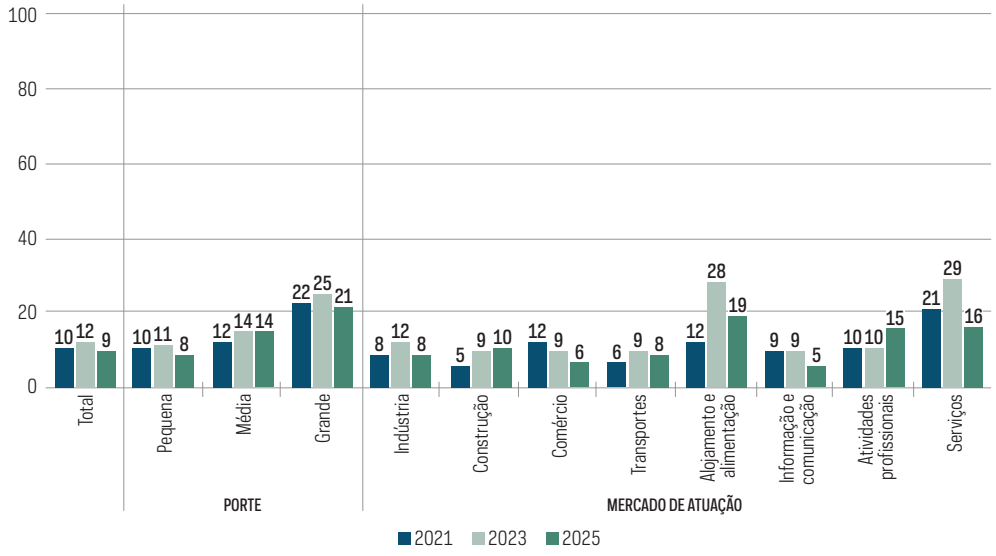
[15] De acordo com o capítulo IV do ECA Digital, acerca dos mecanismos de aferição de idade, em seu art. 10: "Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar mecanismos para proporcionar experiências adequadas à idade, nos termos deste Capítulo, respeitadas a autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros." (Lei n. 15.211/2025). Portanto, empresas que porventura possam direcionar seus produtos e serviços ao público menor de 18 anos devem ter como prática mecanismos de aferição de idade efetivos e usar os dados pessoais coletados somente para esse fim.

[16] Em publicação com orientações aos mecanismos de aferição de idade, a ANPD (2026) evidencia as implicações amplas do tratamento de dados pessoais de menores de 18 anos de idade, tendo em vista os diversos regramentos em vigor: "A proteção da privacidade dos usuários, nesse contexto, também se relaciona à necessidade de que os mecanismos adotados sejam compatíveis com a garantia constitucional da inviolabilidade da intimidade, da vida privada, da honra e da imagem dos usuários, nos termos do art. 5º, X, da Constituição Federal. Da mesma forma, devem igualmente ser observadas outras garantias previstas em normas como o Marco Civil da Internet (Lei n. 12.965/2014), que assegura a inviolabilidade e sigilo do fluxo das comunicações realizadas pela Internet, salvo por ordem judicial, na forma da lei. Assim, mecanismos de aferição de idade não podem gerar, direta ou indiretamente, violações à privacidade dos usuários em suas mais diversas dimensões." (ANPD, 2026, p. 17).

GRÁFICO 3
—

Empresas, por manutenção de dados pessoais de clientes e usuários com menos de 18 anos de idade, porte e setor (2021–2025)

Total de empresas que mantêm dados pessoais de clientes e usuários (%)

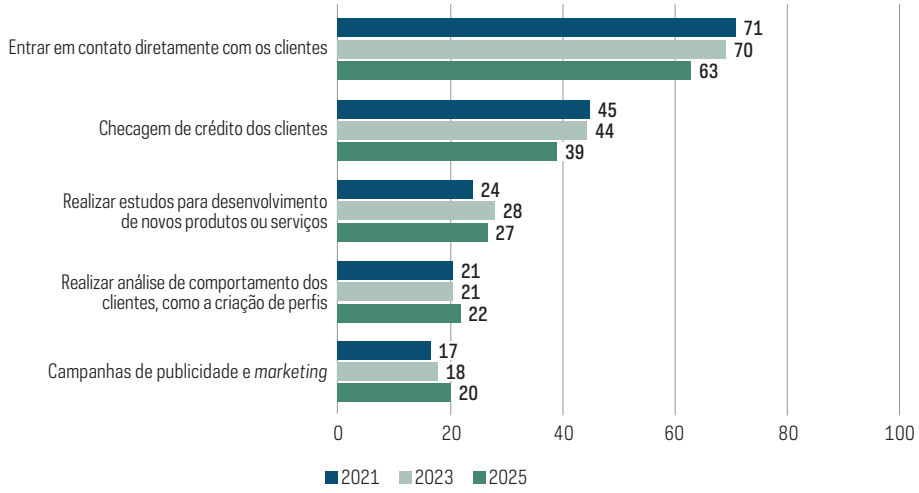


Tendo em vista as empresas que afirmaram manter os dados pessoais de clientes e usuários, em 2025, 63% informaram utilizá-los para entrar em contato diretamente com esses públicos, enquanto 39% informaram usá-los para checagem de crédito, padrão mantido desde a primeira edição da pesquisa (Gráfico 4). A pesquisa TIC Empresas 2025 mostrou que 41% das empresas brasileiras pagaram por anúncios na Internet, com maiores proporções entre as organizações do setor de alojamento e alimentação (51%), informação e comunicação (53%) e serviços (55%) (NIC.br, 2026b). Importante mencionar que estes são justamente os setores com maior proporção de manutenção de dados pessoais de menores de 18 anos de idade, reforçando a importância de observarem os requisitos estabelecidos pela LGPD e pelo ECA Digital para o tratamento desses dados. Nesse sentido, um estudo do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) sobre mecanismos de aferição de idade de diversas plataformas mostra que as estratégias adotadas são muito diversas e nem sempre efetivas para cumprir os requisitos legais, o que evidencia os desafios para a implementação dessas medidas (CGI.br, 2026b).

GRÁFICO 4
—

Empresas, por tipo de uso de dados pessoais de clientes e usuários (2021–2025)

Total de empresas que mantêm dados pessoais de clientes e usuários (%)

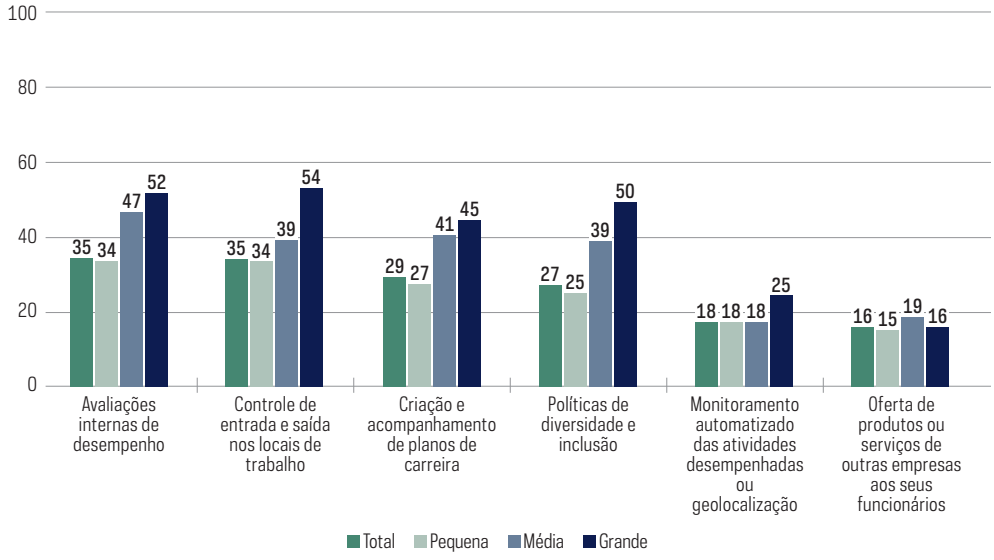


Do ponto de vista do tratamento de dados gerados internamente, em 2025, 35% das empresas usaram os dados pessoais dos funcionários para avaliação de desempenho, mesma proporção para o uso destinado ao controle de entrada e saída dos locais de trabalho (Gráfico 5)[17]. É importante mencionar que a finalidade de uso de dados pessoais pode envolver a coleta de biometria, frequentemente utilizada em sistemas de controle de acesso e segurança. Nesse caso, por ser dado pessoal sensível, seu tratamento deve seguir as hipóteses e os requisitos previstos na LGPD, sobretudo o consentimento do titular (art. 11).

[17] De acordo com a pesquisa TIC Empresas 2025, 14% das empresas usaram dispositivos inteligentes ou de Internet das Coisas (*Internet of Things* [IoT]). Em 90% dos casos daquelas que usaram esses dispositivos, a finalidade foi segurança de instalações, como sistemas de alarme, detectores de fumaça, travas de portas e câmeras de segurança inteligentes (NIC.br, 2026b).

GRÁFICO 5
—

Empresas, por tipo de finalidade de uso dos dados de funcionários e porte (2025)
Total de empresas (%)



A presente seção evidenciou que a manutenção de dados pessoais implica, por parte das empresas, diversas obrigações que se tornam mais complexas quando envolvem dados sensíveis ou de menores de 18 anos de idade. Além disso, os resultados reforçam a necessidade de que as empresas compreendam a relação entre os diversos regramentos que versam sobre suas práticas de coleta de dados pessoais, dadas as especificações exigidas a partir da natureza dos dados e da finalidade de uso.

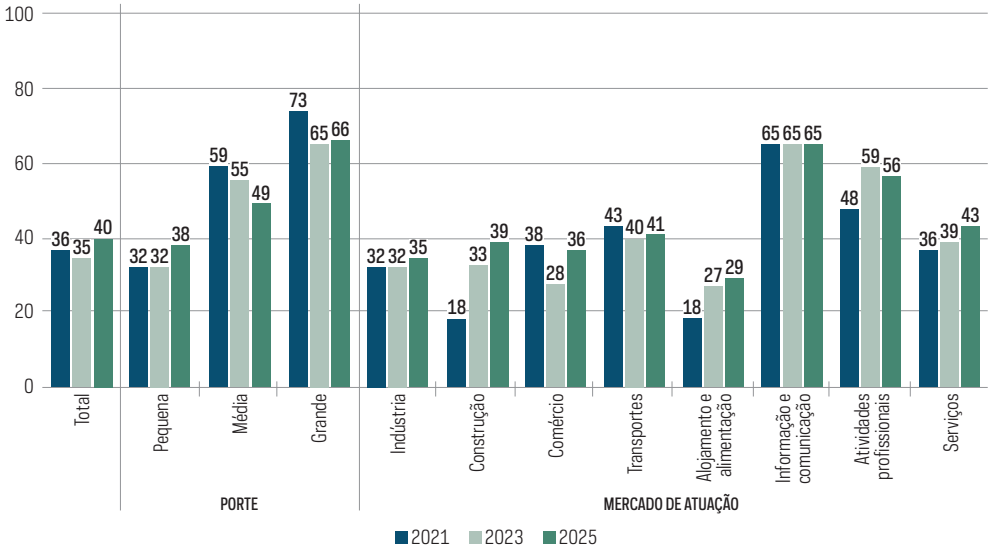
Desenvolvimento de capacidades internas

Conforme já apontado na seção de introdução dessa análise, em um cenário de crescente digitalização e evolução do marco regulatório de proteção de dados, é importante que as empresas tenham uma estrutura interna capaz de orientar ações de tratamento de dados pessoais, em conformidade com os regramentos. Em 2025, 40% das empresas realizaram reuniões para tratar especificamente do tema de proteção de dados pessoais, resultado estável em comparação com as edições anteriores da pesquisa. Assim como observado em outros indicadores associados ao porte da empresa, observa-se que as empresas de grande porte realizaram essas reuniões em maior proporção (66%) do que as pequenas (38%), mantendo-se a estabilidade em ambos os grupos ao longo da série histórica (Gráfico 6).

GRÁFICO 6
—

Empresas, por realização de reuniões internas para tratar especificamente do tema de proteção de dados pessoais, porte e setor (2021–2025)

Total de empresas (%)

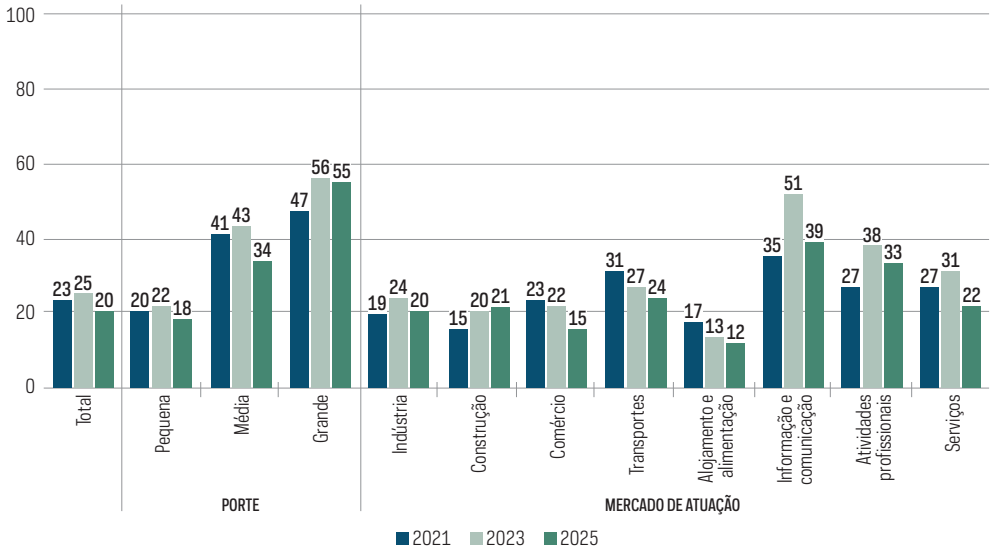


Em relação ao desenvolvimento de capacidades internas relacionadas à proteção de dados pessoais, observa-se que a existência de estruturas organizacionais dedicadas ao tema não apresentou alteração na presente edição da pesquisa. Em 2025, 20% das empresas possuíam uma área ou funcionários responsáveis por atividades voltadas ao tema da proteção de dados pessoais, mantendo a estabilidade em relação a anos anteriores (Gráfico 7). Do ponto de vista do perfil das empresas, as de grande porte e aquelas do setor de informação e comunicação são as com maior mobilização de recursos humanos para tratar especificamente da proteção de dados pessoais.[18]

[18] A ANPD previu assimetrias regulatórias, a depender do porte das empresas. Há dispensas de certas obrigações para empresas de pequeno porte, entretanto em termos de faturamento e não de pessoas ocupadas, tal qual na TIC Empresas. A Resolução CD/ANPD n. 2/2022 estabelece as diferenças para o que é chamado de "agentes de tratamento de pequeno porte", mas determina a aplicação integral da lei em casos de tratamento de alto risco.

GRÁFICO 7
—

Empresas, por existência de uma área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais, porte e setor (2021–2025)
Total de empresas (%)

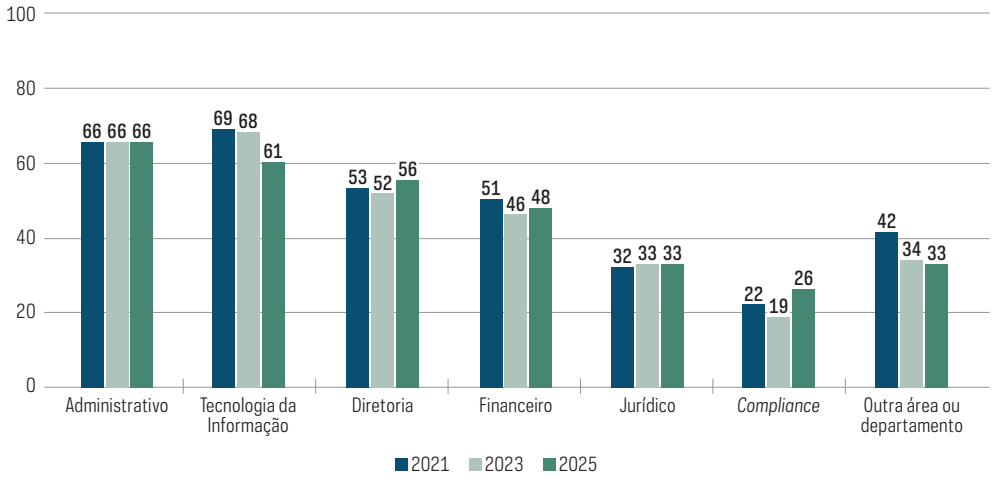


Em 2025, dentre as empresas que possuíam uma área ou funcionários responsáveis pela proteção de dados pessoais, 66% indicaram que estavam vinculados ao setor administrativo, enquanto 61% mencionaram que eram provenientes da área de tecnologia da informação da empresa, mantendo o padrão observado nos últimos anos. Há diferenças segundo o porte da empresa entre as origens mais mencionadas: em 2025, 71% das empresas de pequeno porte destacavam o setor administrativo para lidar com os temas de proteção de dados pessoais, ao passo que 82% das empresas de grande porte direcionavam essas atividades para o setor de tecnologia da informação (Gráfico 8). Esses resultados sugerem que a organização das atividades relacionadas à proteção de dados varia conforme a estrutura e a complexidade das empresas, refletindo diferentes estratégias para incorporar a governança de dados às rotinas organizacionais.

GRÁFICO 8
—

Empresas, por área ou departamento a que pertencem os funcionários responsáveis pelo tema de proteção de dados pessoais (2021–2025)

Total de empresas com área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais (%)

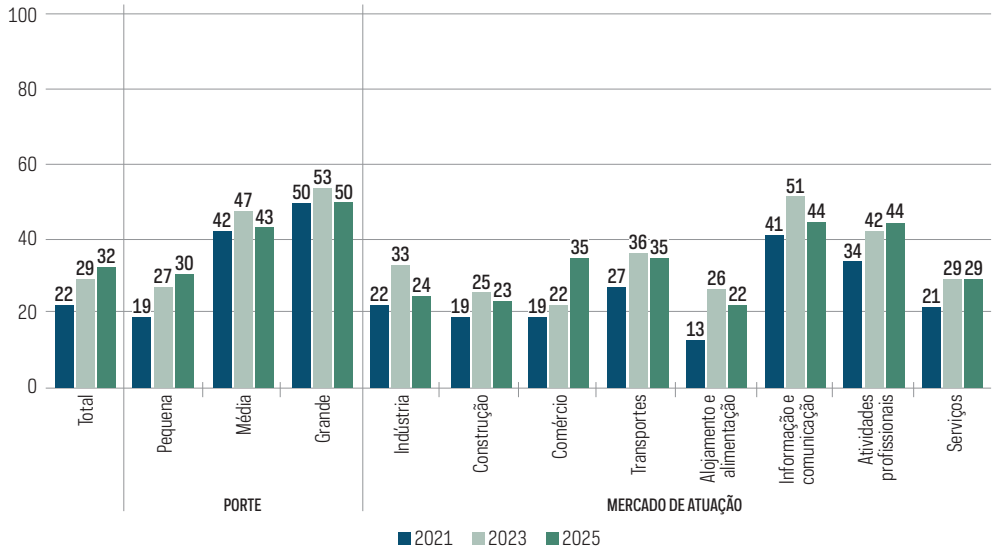


A despeito da presença de um departamento ou funcionários dedicados ao tema de proteção de dados pessoais, as empresas também podem recorrer à contratação de serviços especializados para apoiar os mais diversos aspectos abordados pela lei. De acordo com os resultados da TIC Empresas 2025, 32% das empresas contrataram serviços de terceiros, como consultoria ou assessoria, para auxiliar com o tema de privacidade, proteção de dados e adequação à LGPD, mantendo o patamar das edições anteriores. O padrão por porte e setor indicado segue como observado em outros indicadores, com maior presença da terceirização de serviços relacionados ao tema de proteção de dados pessoais nas grandes empresas e no setor de informação e comunicação e de atividades profissionais (Gráfico 9).

GRÁFICO 9
—

Empresas, por contratação de serviços de terceiros, como consultoria ou assessoria, para auxiliar com o tema de privacidade, proteção de dados e adequação à LGPD, porte e setor (2021–2025)

Total de empresas (%)



Em suma, os indicadores sobre desenvolvimento de competências internas, seja por meio de equipes próprias ou da contratação de serviços especializados, apresentam poucas alterações ao longo das três edições da pesquisa. Essa estabilidade sugere que ainda há espaço para ampliar a conscientização das empresas sobre os riscos associados à ausência ou à baixa adoção de boas práticas de tratamento de dados pessoais, especialmente entre as empresas de menor porte.

O conjunto dos marcos legais e regulatórios que afetam a atuação das empresas no ambiente digital também merecem atenção, o que torna necessária a preparação das equipes para atuar em um contexto de maior complexidade, demandando não apenas ações pontuais, mas um fortalecimento contínuo das capacidades institucionais para lidar com o tratamento dos dados. Nesta seção, foram abordados aspectos relacionados à estrutura organizacional e às capacidades internas para lidar com o tratamento de dados pessoais; na próxima, o objetivo é averiguar ações efetivas empreendidas pelas empresas para buscar sua conformidade com a LGPD.

Adequação à LGPD

A pesquisa TIC Empresas investiga como as empresas têm buscado adequação à LGPD, por meio de ações previstas pela lei e da adoção de boas práticas de segurança digital e proteção de dados pessoais[19]. Em 2025, a ação mais realizada pelas empresas foi a alteração de contratos vigentes para se adequar à LGPD, afirmada por 30% das empresas, mantendo o padrão observado na edição anterior da pesquisa.

Em seguida, 29% delas criaram uma política de uso de dados pessoais de funcionários, enquanto o desenvolvimento de uma política de privacidade foi mencionado por 28% (Gráfico 10). Portanto, os resultados indicam que as práticas mais adotadas pelas empresas em relação à lei dizem respeito ao estabelecimento de procedimentos internos voltados para a segurança jurídica em relação aos funcionários, com menos iniciativas relacionadas ao público externo.[20]

[19] Ainda que não explicitamente mencionadas na lei, algumas práticas listadas no indicador sobre adequação à LGPD têm relação com princípios dispostos na legislação, por exemplo os incisos VI, VII, VIII, IX e X do art. 6º: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (Lei n. 13.709/2018).

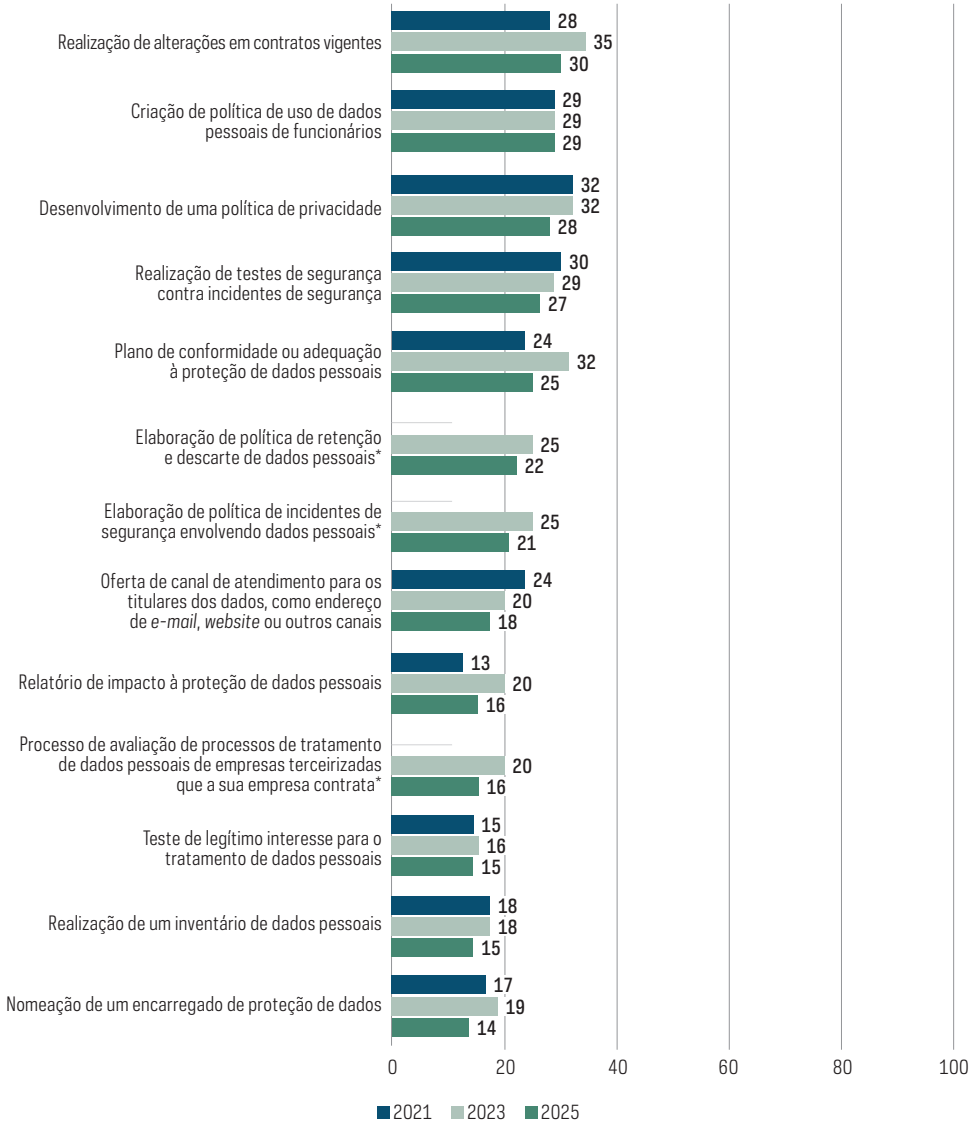
[20] A discussão mencionada na seção anterior sobre o uso de biometria para controle de acesso pode estar relacionada a esses resultados, em razão da necessidade de tratamento diferenciado dos dados sensíveis, em termos de explicitação da finalidade, práticas de compartilhamento, entre outras, visando cumprir com os princípios que orientam a lei. Nesse sentido, a ANPD publicou um radar tecnológico sobre as especificidades do tratamento de dados de biometria (Cebrian *et al*., 2024).

GRÁFICO 10

—

Empresas, por tipo de ação para adequação à LGPD (2021–2025)

Total de empresas que mantêm dados de pessoas físicas (%)



Nota: *Categoria de resposta incluída a partir de 2023.

Conforme apontado, algumas práticas listadas no Gráfico 10, embora não estejam expressamente previstas na LGPD, coadunam-se com os princípios estabelecidos por ela para o tratamento de dados pessoais. Dentre os itens destacados, quatro são previstos pela lei e constituem obrigações às empresas. Em 2025, a oferta de um canal de atendimento foi o item mais presente, declarado por 18% das empresas que mantêm dados de pessoas físicas (Gráfico 11)[21]; o segundo mais citado foi a elaboração de um relatório de impacto à proteção de dados pessoais[22], mencionado por 16% das empresas, seguido da realização de teste de legítimo interesse (15%) e da nomeação de encarregado (14%).[23]

Por fim, vale destacar que há maior busca por adequação entre as grandes empresas, o que pode refletir maior disponibilidade de recursos para estruturar ações de proteção de dados pessoais, bem como um provável maior volume de dados tratados em processos internos.[24]

[21] Tal qual disposto no art. 9º da LGPD: "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei." (Lei n. 13.709/2018).

[22] O relatório de impacto é mencionado diversas vezes no art. 38: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no *caput* deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados." (Lei n. 13.709/2018).

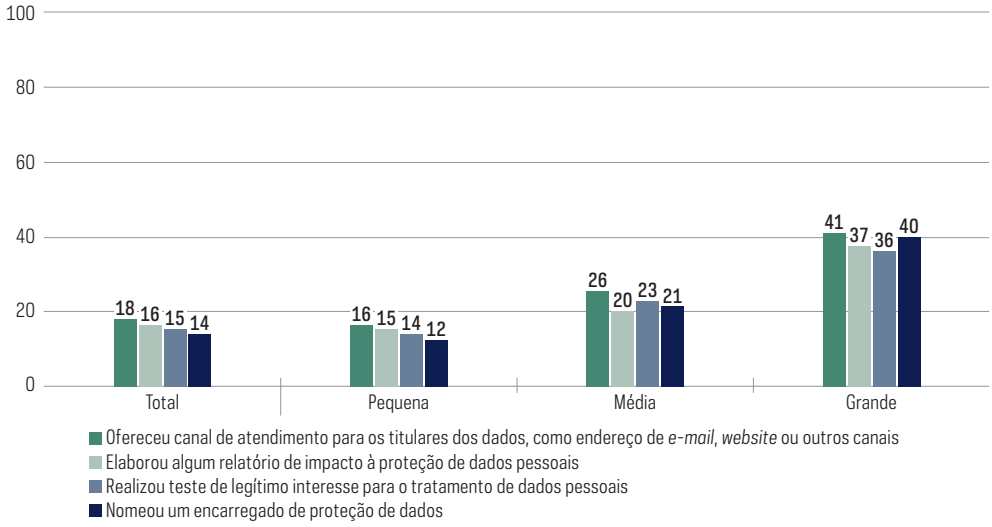
[23] O legítimo interesse fundamenta justamente um dos requisitos para o tratamento de dados pessoais, e sua especificação pode fazer parte do relatório de impacto à proteção de dados pessoais. Conforme o art. 10: "O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial." (Lei n. 13.709/2018).

[24] As assimetrias regulatórias estabelecidas pela CD/ANPD n. 2/2022 podem influenciar nesses resultados, uma vez que algumas obrigações deixam de ser exigidas das empresas de pequeno porte. Ainda que, como discutido, o conceito de porte usado na resolução e na TIC Empresas não seja o mesmo, pode haver empresas abrangidas pelos dois critérios.

GRÁFICO 11
–

Empresas, por tipo de ação para adequação a ações previstas pela LGPD e porte (2025)

Total de empresas que mantêm dados de pessoas físicas (%)



Uma das práticas previstas pela LGPD é a nomeação de um encarregado de proteção de dados pessoais. De acordo com o art. 41 da LGPD, o encarregado é responsável pela comunicação sobre as práticas de tratamento de dados na organização e atua como ponto focal para os titulares e o órgão regulador[25]. Além dessa função, cabe a ele orientar internamente sobre boas práticas de tratamento de dados, conferindo ao cargo um importante papel no desenvolvimento de capacitações internas. Entre as empresas com um encarregado de proteção de dados pessoais, em 2025, 28% informaram que esse profissional é oriundo da área de tecnologia da informação, e 19%, do setor administrativo da empresa, mostrando relação com o indicador sobre a existência de estruturas organizacionais destacadas exclusivamente para lidar com o tema (Gráfico 12).

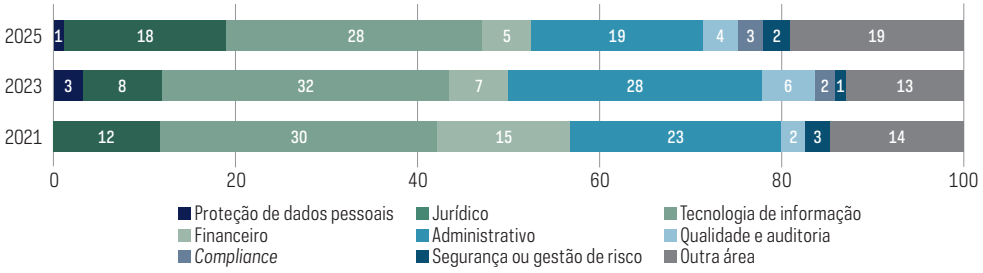
[25] A ANPD publicou, em 2024, a Resolução CD/ANPD n. 18/2024, que regula a atuação do encarregado pelo tratamento de dados pessoais, detalhando sua atuação em relação ao art. 41 da LGPD , sobretudo estabelecendo os parâmetros de sua atuação com o regulador.

GRÁFICO 12

—

Empresas, por área de origem do encarregado de proteção de dados pessoais (2021–2025)

Total de empresas que possuem um encarregado de proteção de dados pessoais vindo da própria empresa (%)



Em razão de seu papel de comunicação com os titulares e o regulador, espera-se que controladores tornem públicas as informações acerca do encarregado de dados. A Resolução CD/ANPD n. 18/2024, por exemplo, estabelece, em seu art. 9º, as informações exigidas sobre o encarregado que devem ser disponibilizadas no *website* do agente de tratamento, de forma clara e objetiva, em local de destaque e de fácil acesso no sítio eletrônico do agente de tratamento[26]. Além dessa exigência específica, de acordo com a LGPD, o sítio eletrônico é o meio determinado para a exibição de diversas informações, tais como a finalidade e os procedimentos de tratamento de dados pessoais da organização.

Assim, o *website* assume papel institucional relevante como meio de transparência e comunicação com titulares, sendo um repositório para informações previstas pela legislação e um importante instrumento para contribuir com a reputação da empresa entre clientes e usuários, por meio de critérios de transparência, como disponibilidade de informações e meios de comunicação[27]. Em 2025, dentre as empresas que possuíam *website*, 42% afirmaram oferecer canal de atendimento para os titulares dos dados, enquanto 41% disponibilizaram uma política de segurança da informação (Gráfico 13)[28]. No entanto, é importante mencionar que houve queda na proporção de empresas que disponibilizavam o nome e o contato do encarregado de dados no *website*, que passou a 7% das empresas em 2025, ante 17% em 2023.

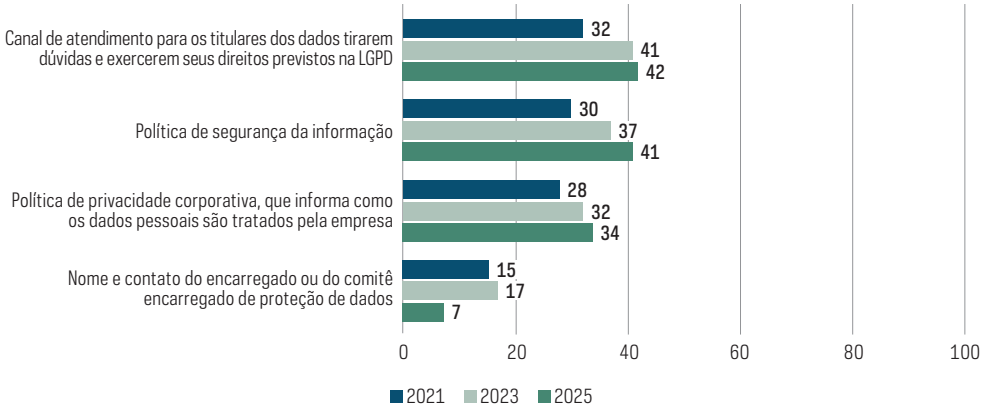
[26] "A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, em local de destaque e de fácil acesso, no sítio eletrônico do agente de tratamento, ressalvada a hipótese do § 3º deste artigo. § 1º A divulgação da identidade do encarregado abrangerá, no mínimo: I - o nome completo, se for pessoa natural; ou II - o nome empresarial ou o título do estabelecimento, bem como o nome completo da pessoa natural responsável, se pessoa jurídica." (ANPD, 2024b).

[27] De acordo com a pesquisa TIC Empresas 2025, 56% das empresas brasileiras possuíam *website*, atingindo 87% das grandes, 76% das médias e 53% das pequenas (NIC.br, 2026b).

[28] A disponibilização de informações via *website* é prevista também no art. 41 do ECA Digital, mantendo relação com os requisitos da LGPD, ainda que restrita aos provedores de aplicações de Internet ou de acesso provável com mais de um milhão de usuários crianças e adolescentes registrados.

GRÁFICO 13
—

Empresas, por recursos disponibilizados no *website* (2021–2025)
Total de empresas que possuem website *(%)*



Os dados da série histórica da pesquisa sobre adequação à LGPD evidenciam que persistem desafios tanto aos requisitos exigidos por lei quanto às boas práticas de privacidade e proteção de dados pessoais. Tal qual debatido ao longo deste capítulo, esse cenário merece atenção, na medida em que há um avanço das tecnologias digitais que amplia a exposição das empresas a riscos de segurança digital, além de tornar mais complexas as regras que orientam a atuação das organizações e, consequentemente, a governança do tratamento de dados pessoais. Nesse contexto, a conformidade com a lei tende a assumir um papel mais estratégico na agenda das empresas, não somente para cumprir exigências legais, mas também para contribuir com a resiliência organizacional, a segurança da informação e a confiança de clientes e usuários.

Considerações finais: agenda para políticas públicas

A nova edição da pesquisa sobre privacidade e proteção de dados pessoais entre as empresas brasileiras evidencia que ainda há espaço significativo para ampliar a adoção de boas práticas e fortalecer a conformidade com os parâmetros estabelecidos pela LGPD. Além disso, a promulgação do ECA Digital traz novos desafios, na medida em que estabelece obrigações adicionais às empresas relacionadas à sua atuação no ambiente digital quando envolve crianças e adolescentes.

Do ponto de vista tecnológico, a crescente digitalização dos processos produtivos e de serviços amplia a exposição das empresas a riscos relacionados ao tratamento de dados pessoais. Dessa forma, mesmo que a maior disponibilidade de ferramentas de automatização de processos possa facilitar a comunicação interna e possibilitar um uso mais estratégico do ambiente digital, é necessário que o uso da tecnologia seja também acompanhado de uma maior conscientização sobre sua relação com as boas práticas de tratamento de dados pessoais.

Nesse contexto, é importante que as empresas acompanhem como o regulador atuará na fiscalização de duas leis que se complementam em diversos aspectos. Ao longo deste capítulo, foram referenciados documentos da ANPD que evidenciam convergências entre a LGPD e o ECA Digital, as quais devem ser observadas pelas empresas, especialmente a relação entre os mecanismos de aferição de idade e o tratamento de dados pessoais de pessoas com menos de 18 anos. Portanto, entende-se que há um novo momento de regulação da economia digital no país, com regras mais definidas sobre a atuação *online* das empresas.

Nesse sentido, os resultados indicam que boas práticas de proteção de dados pessoais ainda possuem espaço para serem incorporadas nos processos das empresas. Observou-se estabilidade na maior parte dos indicadores em relação à primeira edição da pesquisa, conduzida em 2021. Há espaço para avanço, sobretudo entre as pequenas empresas e na maior parte dos setores da economia, tendo em vista que praticamente todas as empresas realizam algum tipo de tratamento de dado pessoal e estão, de alguma forma, expostas no ambiente digital.

Portanto, os resultados mostram que o avanço da transformação digital não foi acompanhado na mesma intensidade pela consolidação de práticas de proteção de dados pessoais entre as empresas brasileiras. Esse cenário revela que a adoção dessas medidas ainda ocorre de maneira desigual, concentrada nas empresas de grande porte e em alguns setores de atividade, principalmente no de informação e comunicação.

Por fim, os resultados apresentados neste capítulo reforçam a importância de políticas públicas voltadas à disseminação de orientações, instrumentos e boas práticas que apoiem a implementação da LGPD, especialmente entre pequenas e médias empresas e nos setores que apresentaram menor adoção das medidas analisadas. Além de contribuir para a conformidade regulatória, iniciativas de capacitação e orientação adaptadas às características de cada segmento podem contribuir para fortalecer a governança de dados, ampliar a cultura de proteção de dados pessoais e reduzir as disparidades identificadas pela pesquisa.

Referências

Agência Nacional de Proteção de Dados. (2024). *Radar tecnológico n.º 3: Inteligência artificial generativa*. Governo Federal. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf

Agência Nacional de Proteção de Dados. (2026). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf

Cebrian, F. S. P. F., Prudente, G. A., Guedes, M. S., Sá, M. L. D., & Thiago, G. M. (2024). *Radar tecnológico n. 2: biometria e reconhecimento facial: estudos preliminares*. Agência Nacional de Proteção de Dados. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf

Comitê Gestor da Internet no Brasil. (2026a, 24 de julho). *Contribuição do CGI.br à tomada de subsídios sobre o Guia Orientativo "Mecanismos de Aferição de Idade"*. https://cgi.br/publicacao/contribuicao-do-cgi-br-a-tomada-de-subsidios-da-anpd-sobre-mecanismos-de-afericao-de-idade/

Comitê Gestor da Internet no Brasil. (2026b). *Práticas de aferição de idade em 25 serviços digitais no Brasil*. https://cetic.br/pt/publicacao/praticas-de-afericao-de-idade-em-25-servicos-digitais-no-brasil/

Decreto n. 12.622, de 17 de setembro de 2025. (2025). Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, para designar a Agência Nacional de Proteção de Dados como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais, e estabelecer competências para cumprimento de ordens judiciais de bloqueio. https://www.in.gov.br/en/web/dou/-/decreto-n-12.622-de-17-de-setembro-de-2025-656777269

Estatuto Digital da Criança e do Adolescente. Lei n. 15.211, de 17 de setembro de 2025 (2025). Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

Lei Geral de Proteção de Dados Pessoais. Lei n. 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Lei n. 15.352, de 25 de fevereiro de 2026. (2026). Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, a Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente), para dispor sobre o início da vigência da referida Lei; altera as Leis nºs 9.008, de 21 de março de 1995, 11.890, de 24 de dezembro de 2008, 13.326, de 29 de julho de 2016, 13.848, de 25 de junho de 2019, e 14.600, de 19 de junho de 2023; revoga a Medida Provisória nº 1.319, de 17 de setembro de 2025; e dá outras providência. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15352.htm

Medida Provisória n. 1.317, de 17 de setembro de 2025. (2025). Altera a natureza jurídica da Autoridade Nacional de Proteção de Dados. Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/mpv/mpv1317.htm

Núcleo de Informação e Coordenação do Ponto BR. (2026a). *Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025* [Tabelas]. https://cetic.br/pt/pesquisa/kids-online/indicadores/

Núcleo de Informação e Coordenação do Ponto BR. (2026b). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras: TIC Empresas 2025* [Tabelas]. https://cetic.br/pt/pesquisa/empresas/indicadores/

Núcleo de Informação e Coordenação do Ponto BR. (2026c). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2025* [Tabelas]. https://cetic.br/pt/pesquisa/domicilios/indicadores/

Resolução CD/ANPD n. 2, de 27 de janeiro de 2022. (2022). Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), para agentes de tratamento de pequeno porte. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022

Resolução CD/ANPD n. 18, de 16 de julho de 2024. (2024). Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2025
Organizações públicas

A transformação digital tem provocado uma intensificação da adoção de tecnologias digitais na administração pública, nos estabelecimentos de saúde e nas instituições de ensino. Esse processo envolve desde a digitalização de serviços públicos até a adoção de sistemas eletrônicos para apoiar processos administrativos, assistenciais, pedagógicos e de gestão, contribuindo para ampliar o acesso da população a esses serviços, aumentar a eficiência administrativa e qualificar a formulação e a implementação de políticas públicas. Além disso, esse movimento tem sido cada vez mais associado à incorporação de tecnologias avançadas, como a Inteligência Artificial (IA), para redesenhar processos, aprimorar a tomada de decisão e oferecer serviços mais eficientes, responsivos e centrados nas necessidades da sociedade (Departamento de Assuntos Econômicos e Sociais das Nações Unidas [UN DESA], 2024; Organização das Nações Unidas para a Educação, a Ciência e a Cultura [UNESCO], 2022).

Nesse cenário, o uso e o compartilhamento de dados têm assumido papel central na implementação de políticas públicas e na prestação de serviços digitais em organizações públicas de todo o mundo. Um exemplo nesse sentido é a disseminação dos sistemas de identificação digital: segundo a edição de 2025 do relatório *ID4D Global Dataset 2025: Trends in Identification for Development*, do Banco Mundial, mais de cem países já haviam implementado alguma forma de identidade digital (Ansar *et al.*, 2026). O compartilhamento de informações entre órgãos públicos e sistemas eletrônicos também pode reduzir a necessidade de apresentação repetida de documentos e viabilizar serviços proativos ou "zero clique"[1], oferecidos a partir de informações já disponíveis no setor público (Maia, 2026).

[1] Proatividade nesse contexto refere-se à capacidade de os governos anteciparem as necessidades dos cidadãos e oferecer serviços antes que sejam explicitamente demandados, com base no princípio do fornecimento único de dados, na análise de dados, na IA e em ferramentas preditivas, a fim de promover a mudança de um modelo de atuação governamental reativo para um modelo antecipatório (Organização para a Cooperação e Desenvolvimento Econômico [OCDE], 2026).

Apesar do reconhecimento desses benefícios, ampliam-se também os desafios e os riscos relacionados ao uso e ao compartilhamento de dados pela administração pública. Entre esses desafios, destaca-se a necessidade de assegurar o direito à privacidade e à proteção de dados pessoais, de modo que as iniciativas de transformação digital no setor público sejam acompanhadas por medidas de governança de dados que promovam tais direitos.

Nesse sentido, a relevância do tema também se reflete na Agenda Regulatória da Agência Nacional de Proteção de Dados (ANPD) para o biênio 2025-2026 (Resolução CD/ANPD n. 31/2025), na qual foi incluído o uso compartilhado de dados pessoais pelo Poder Público como uma das prioridades. Em 2025, a ANPD submeteu à consulta e à audiência públicas uma proposta de regulamento sobre o tema, evidenciando a necessidade de estabelecer parâmetros mais claros para o compartilhamento de informações entre as organizações públicas e, em determinadas situações, entre o poder público e entidades privadas.[2]

A adoção de medidas de proteção é especialmente relevante em áreas que tratam dados pessoais sensíveis ou informações de grupos sujeitos à proteção específica. Nos estabelecimentos de saúde, sejam públicos ou privados, prontuários, resultados de exames, diagnósticos e outras informações sobre as condições de saúde dos pacientes constituem dados pessoais sensíveis nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD). O uso e o compartilhamento dessas informações, embora possam ser essenciais para a continuidade do cuidado, a gestão do sistema de saúde e a formulação de políticas públicas, também podem gerar danos aos titulares de dados caso ocorram acessos não autorizados, vazamentos ou utilizações incompatíveis com as finalidades previstas.

Nas instituições de ensino, especialmente na Educação Básica, há uma crescente adoção de plataformas educacionais, sistemas de gestão, aplicativos e outros recursos digitais que envolvem o tratamento de dados de crianças e adolescentes, inclusive informações sobre desempenho, comportamento, frequência e condições pessoais e familiares (Comitê Gestor da Internet no Brasil [CGI.br], 2025). Além da proteção conferida pela LGPD, esse contexto passou a ser disciplinado recentemente pelo Estatuto Digital da Criança e do Adolescente (ECA Digital), instituído pela Lei n. 15.211, de 17 de setembro de 2025, o qual estabeleceu as regras para a proteção de crianças e adolescentes em ambientes digitais, incluindo medidas de prevenção e mitigação de riscos e obrigações relacionadas à proteção de seus direitos.

O ECA Digital também ampliou as atribuições institucionais da ANPD, designada como autoridade administrativa autônoma responsável por zelar pela aplicação da nova legislação (Decreto n. 12.622/2025). Essa competência soma-se às funções já exercidas pela agência no âmbito da LGPD e reforça a relação entre a proteção integral desse público e a garantia dos direitos à privacidade e à proteção de dados pessoais. No contexto escolar, embora muitas obrigações do ECA Digital sejam direcionadas aos fornecedores de produtos e serviços digitais, a nova legislação amplia a relevância de avaliar como tecnologias utilizadas por escolas tratam dados de estudantes e incorporam medidas adequadas à cada faixa etária e ao melhor interesse dessa população.

[2] Mais informações disponíveis em https://www.gov.br/participamaisbrasil/regulamento-sobre-o-uso-compartilhado-de-dados-pessoais-pelo-poder-publico

Considerando o contexto brasileiro, instrumentos relacionados à transformação digital do setor público, como o Plano Brasileiro de Inteligência Artificial (PBIA) (Ministério da Ciência, Tecnologia e Inovação [MCTI] & Centro de Gestão e Estudos Estratégicos [CGEE], 2025) e a Estratégia Nacional de Governo Digital (ENGD) (Ministério da Gestão e da Inovação em Serviços Públicos [MGI], s.d.), incluem a privacidade e a proteção de dados entre os princípios que devem orientar sua implementação, assim como a Lei n. 14.129/2021, que estabelece princípios, regras e instrumentos para o governo digital, e inclui a proteção de dados pessoais entre suas diretrizes. Portanto, diante da ampliação dos serviços digitais, da integração e do compartilhamento de bases governamentais e do uso de tecnologias baseadas no tratamento intensivo de dados, como a IA, torna-se fundamental acompanhar em que medida os direitos relacionados à privacidade e à proteção de dados pessoais têm sido incorporados às práticas das organizações públicas.

Com esse objetivo, este capítulo apresenta indicadores produzidos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), sobre privacidade e proteção de dados pessoais em diferentes organizações do setor público. O capítulo é organizado da seguinte forma:

- **Órgãos públicos federais e estaduais, e prefeituras:** a primeira seção apresenta os resultados da pesquisa TIC Governo 2025 (CGI.br, 2026b) e analisa as principais medidas adotadas por essas organizações em relação à privacidade e à proteção de dados pessoais.
- **Estabelecimentos públicos de saúde:** a segunda seção aborda iniciativas de promoção da segurança digital, da privacidade e da proteção de dados nos estabelecimentos públicos de saúde, com base nos indicadores da pesquisa TIC Saúde 2025 (CGI.br, 2026c), incluindo comparações com os estabelecimentos privados.
- **Instituições de ensino públicas de Educação Básica:** a terceira seção analisa os principais desafios para a consolidação de uma cultura de proteção de dados nessas instituições, a partir da perspectiva de diferentes atores escolares investigados pelas edições de 2024 e 2025 da pesquisa TIC Educação (CGI.br, 2025, 2026a).

Órgãos públicos federais e estaduais e prefeituras

Em 2025, a pesquisa bienal TIC Governo mediu, pela terceira vez, o módulo G – "Privacidade e proteção de dados pessoais". Esse conjunto de indicadores permite acompanhar a adoção de ações nessa área pelas organizações públicas brasileiras e identificar desafios para a consolidação de uma cultura de proteção de dados no setor público, abrangendo órgãos federais e estaduais dos Poderes Executivo, Legislativo e Judiciário, o Ministério Público e as prefeituras brasileiras.

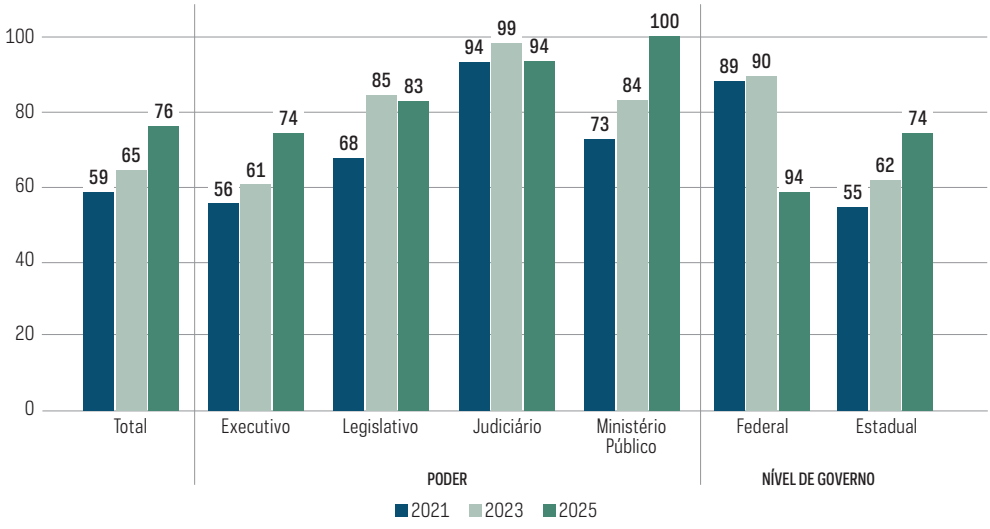
No conjunto das ações relacionadas à privacidade e à proteção de dados pessoais investigadas pela TIC Governo, uma das mudanças observadas em relação à edição anterior, coletada em 2023, foi o aumento da proporção de organizações públicas com área ou pessoa responsável por procedimentos e políticas para a coleta, o armazenamento

ou o uso de dados pessoais. Nos órgãos federais e estaduais, a presença de uma pessoa ou estrutura institucional voltada para esse tema permaneceu mais elevada no Ministério Público (100%), no Judiciário (94%) e no Legislativo (83%) em relação aos do Executivo (74%), assim como nos órgãos públicos federais (94%) em comparação aos estaduais (74%). Conforme o Gráfico 1, houve crescimento significativo na presença de uma área ou pessoa voltada para a LGPD no Ministério Público, com aumento de 16 pontos percentuais, e no Executivo e nos órgãos estaduais, ambos com crescimento de 13 pontos percentuais, em relação à 2023.

GRÁFICO 1
—

Órgãos públicos federais e estaduais, por existência de área ou pessoa responsável por procedimentos e políticas para a coleta, o armazenamento ou o uso de dados pessoais, ou pela implementação da LGPD (2021–2025)

Total de órgãos públicos federais e estaduais (%)

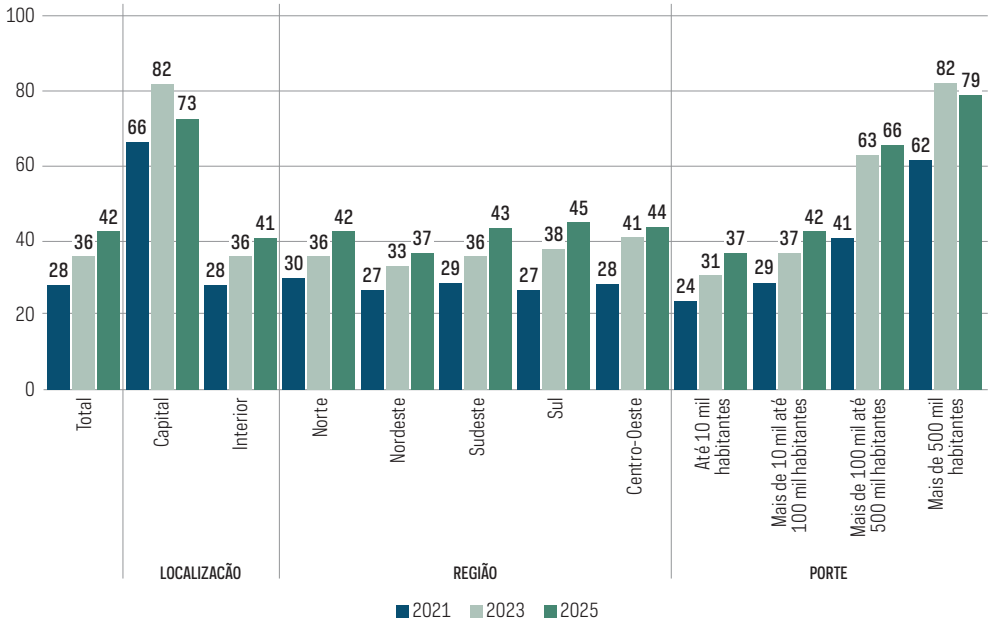


No nível local, também foi identificado o aumento na presença de estruturas ou alguma pessoa responsável pelo tema de privacidade e proteção de dados, passando de 36% em 2023 para 42% em 2025. Essa mudança foi decorrente do crescimento observado entre as prefeituras com até 10 mil habitantes: a presença de área ou pessoa responsável por dados pessoais foi mencionada por menos de um terço das prefeituras desse porte em 2023 e alcançou 37% em 2025 (Gráfico 2).

GRÁFICO 2
—

Prefeituras, por existência de área ou pessoa responsável por procedimentos e políticas para a coleta, o armazenamento ou o uso de dados pessoais, ou pela implementação da LGPD (2021–2025)

Total de prefeituras (%)



Além da existência de uma área ou pessoa responsável, a capacitação interna é fundamental para consolidar uma cultura de proteção de dados no setor público. Nesse sentido, a ENGD recomenda ações de sensibilização, conscientização e capacitação de agentes públicos, lideranças governamentais e da sociedade sobre privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, no âmbito do Objetivo 4 – Privacidade e Segurança (MGI, s.d.).

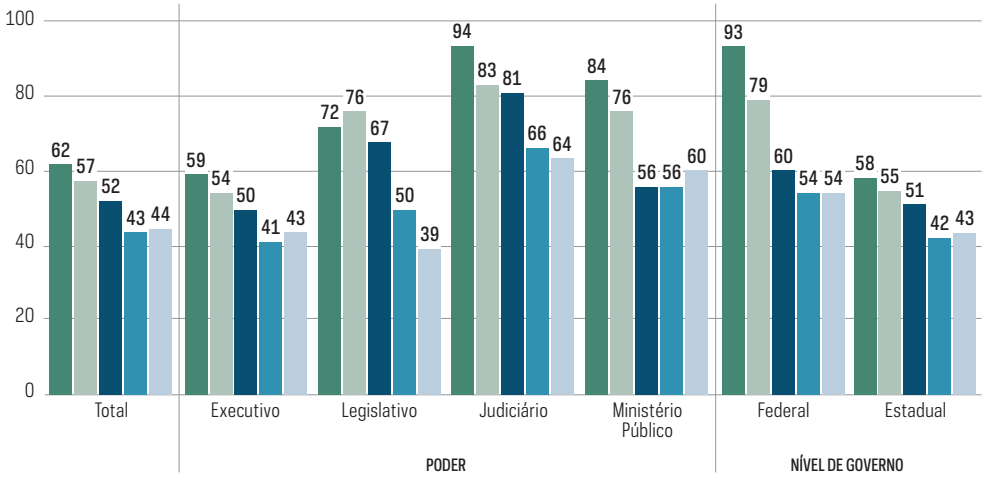
A TIC Governo investiga a realização de capacitações, cursos ou treinamentos sobre a LGPD para profissionais da área de tecnologia da informação (TI)[3]. Em 2025, essas iniciativas foram promovidas por 95% dos órgãos do Judiciário, 83% do Ministério Público e 75% do Legislativo. As proporções foram menores no Executivo (61%) e nos órgãos estaduais (62%), em comparação aos federais (85%). Entre as prefeituras com área de TI, 35% capacitaram ao menos um funcionário do setor, com maior proporção nas capitais (72%), nos municípios com mais de 100 mil e até 500 mil habitantes (51%) e naqueles com mais de 500 mil habitantes (82%).

[3] Vale ressaltar que, de acordo com a TIC Governo 2025, 86% dos órgãos federais e estaduais possuem departamento de TI, sendo esse tipo de setor mais presente entre os órgãos do Judiciário (100%), Legislativo (96%), Ministério Público (96%) e aqueles de nível federal (99%). Entre os órgãos estaduais, 85% tinham uma área voltada para tecnologia; no nível municipal, 49% das prefeituras possuíam área ou departamento de TI em 2025 (CGI.br, 2026b).

A pesquisa TIC Governo também mede ações específicas para a implementação da LGPD, como a nomeação de encarregado pelo tratamento de dados pessoais e a oferta de canais pela Internet para o envio de mensagens pelos cidadãos sobre o uso de seus dados. Entre os órgãos federais e estaduais, foram investigadas cinco ações. Mais da metade deles já havia nomeado encarregado (62%), disponibilizado canais de atendimento *online* sobre o uso de dados pessoais (57%) e publicado sua política de privacidade na Internet (52%). Em proporções menores, foram mencionadas a implementação de um plano de resposta a incidentes de segurança da informação relacionado a dados pessoais (43%) e a existência de programa de governança em privacidade e proteção de dados pessoais (44%).

Entre 2023 e 2025, observou-se um crescimento na adoção de medidas relacionadas à LGPD, sobretudo entre os órgãos estaduais. A nomeação de encarregado de dados pessoais ultrapassou a metade dos órgãos desse nível de governo (de 46%, em 2023, para 58% em 2025), enquanto a implementação de um plano de resposta a incidentes passou de 30% para 42%. No entanto, essas proporções permanecem inferiores aos resultados do nível federal, em que 93% tinham nomeado o encarregado de dados e 54% tinham um plano de resposta a incidentes em 2025. Como nas edições anteriores, o Judiciário destacou-se pelas maiores proporções nas ações investigadas (Gráfico 3). Em 2025, mais de 80% de seus órgãos haviam nomeado encarregado, disponibilizado canais de atendimento *online* e publicado sua política de privacidade na Internet.

GRÁFICO 3
—
Órgãos públicos federais e estaduais, por ações relacionadas à LGPD (2025)
Total de órgãos públicos federais e estaduais (%)



Em 2025, a pesquisa passou a investigar a existência de programas de governança em privacidade e proteção de dados nos órgãos federais e estaduais. Assim como os planos de resposta a incidentes, essa foi uma das iniciativas menos mencionadas. O programa estava presente em 54% dos órgãos federais e em 43% dos estaduais. Entre os poderes, as maiores proporções foram observadas no Judiciário (64%) e no Ministério Público (60%), seguidos pelo Executivo (43%) e pelo Legislativo (39%).

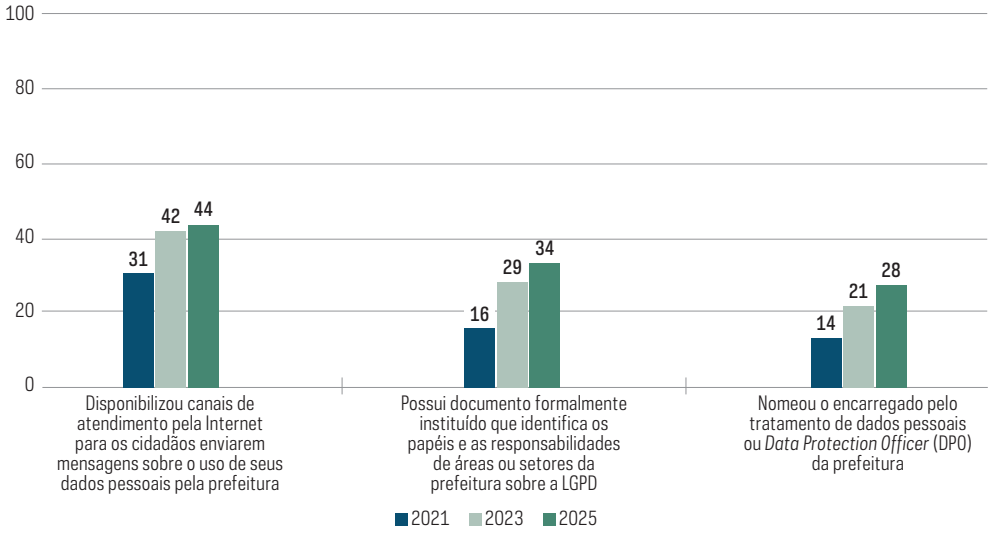
O art. 50 da LGPD trata dos programas de governança em privacidade no âmbito da seção de boas práticas e de governança, estabelecendo requisitos mínimos para sua implementação. Esse tipo de programa pode ser definido como um "instrumento capaz de demonstrar a integridade e o comprometimento do agente de tratamento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais" (ANPD, 2024, p. 33). Algumas organizações públicas já contam com normas específicas sobre o tema, como a Resolução n. 281/2023, do Conselho Nacional do Ministério Público (CNMP); no nível federal, também foi elaborado um guia para apoiar a implementação de programas de governança em privacidade (MGI, 2024).

A relevância do tema foi reforçada pela inclusão da iniciativa "Regras de boas práticas e de governança" entre as prioridades da Agenda Regulatória da ANPD para o biênio 2025-2026 (Resolução CD/ANPD n. 31/2025). Os resultados da Tomada de Subsídios sobre a agenda regulatória também destacaram o papel desses programas para assegurar o respeito à LGPD na adoção de ferramentas de IA (ANPD, 2025). Apesar do crescente respaldo normativo e regulatório, os dados da TIC Governo 2025 indicam que a adoção de programas de governança em privacidade e proteção de dados ainda não foi disseminada entre os órgãos públicos federais e estaduais. Tais dados reforçam ainda a importância de acompanhar o desenvolvimento de tais políticas nas próximas edições da pesquisa, considerando o papel estratégico desses programas na institucionalização de práticas de conformidade com a LGPD e na promoção de um uso responsável de dados pessoais e de tecnologias avançadas, como a IA.

Entre as prefeituras, a pesquisa mede três ações relacionadas à LGPD. Entre 2023 e 2025, houve crescimento significativo na nomeação de encarregado e na existência de documento formal que define os papéis e as responsabilidades das áreas ou dos setores da prefeitura em relação à LGPD (Gráfico 4). Esse avanço decorreu principalmente das mudanças observadas nos municípios com até 10 mil habitantes, nos quais a nomeação de encarregado passou de 17% para 24% e a presença de documento aumentou de 27% para 32%. Também houve crescimento de 21% para 34% na nomeação de encarregado entre os municípios com mais de 10 mil e até 100 mil habitantes.

GRÁFICO 4
—

Prefeituras, por ações relacionadas à LGPD (2021–2025)
Total de prefeituras (%)



Os canais *online* para o envio de mensagens pelos cidadãos sobre o uso de seus dados pessoais continuam sendo a iniciativa mais mencionada, embora ainda estejam presentes em menos da metade das prefeituras (44%). As ações investigadas também são citadas com maior frequência nos municípios de maior porte populacional e nas capitais. A existência de documento formal que define os papéis e as responsabilidades das áreas ou dos setores da prefeitura em relação à LGPD, por exemplo, foi apontada por sete em cada dez municípios com mais de 500 mil habitantes e por 62% das capitais. Assim, apesar dos avanços observados no período, especialmente entre as prefeituras de menor porte populacional, permanecem as desigualdades entre os municípios na adoção de medidas relacionadas à privacidade e à proteção de dados pessoais.

Estabelecimentos públicos de saúde

A transformação digital tem provocado mudanças profundas na organização dos sistemas de saúde e na prestação dos serviços assistenciais. Nesse cenário, a incorporação crescente de tecnologias digitais aos processos clínicos e administrativos tem ampliado a informatização dos estabelecimentos de saúde e a oferta de serviços digitais, como prontuários eletrônicos, prescrição eletrônica de medicamentos, solicitação e compartilhamento de exames, sistemas de apoio à decisão clínica, plataformas de telessaúde e outras aplicações voltadas à gestão e ao cuidado dos pacientes. Esse processo não somente amplia as oportunidades para melhorar a qualidade da assistência, a

coordenação do cuidado e a eficiência dos sistemas de saúde, mas também reforça a relevância da segurança da informação nos sistemas que armazenam e processam dados pessoais de saúde, considerados pela LGPD como dados pessoais sensíveis. Assim, a crescente digitalização da saúde tem intensificado o volume, a circulação e o uso de dados sensíveis, tornando a proteção dessas informações um dos principais desafios para o desenvolvimento de uma saúde digital ética, responsável e alinhada à garantia dos direitos fundamentais (Aith *et al.*, 2025).

Os resultados da pesquisa TIC Saúde evidenciam o avanço desse processo de digitalização nos estabelecimentos públicos de saúde brasileiros. Em 2025, considerando os três níveis de atenção, 91% dos estabelecimentos públicos utilizavam algum sistema eletrônico de registro de informações dos pacientes, 35% disponibilizavam resultados de exames pela Internet, 32% ofereciam agendamento *online* de consultas e 34% realizavam teleconsulta. Além disso, 11% dos estabelecimentos públicos utilizavam aplicações de IA, tecnologia cuja adoção tem ocorrido de forma desigual entre os diferentes níveis de atenção, com proporção que chegava a 10% dos estabelecimentos sem internação e 23% dos hospitais públicos com mais de 50 leitos de internação (CGI.br, 2026c). Desse modo, observa-se que a utilização dessas ferramentas, além de ampliar o potencial de análise e compartilhamento de dados, automatizar processos e apoiar decisões clínicas e gerenciais, também introduz novos desafios relacionados à segurança da informação, à governança dos dados e à proteção da privacidade dos pacientes.

Nesse contexto, organismos internacionais têm ressaltado que a transformação digital da saúde deve ser acompanhada pelo fortalecimento da governança de dados e da segurança da informação. A Organização Pan-Americana da Saúde (OPAS), ao estabelecer os princípios orientadores para a transformação digital do setor de saúde, destaca que a confiança nos sistemas digitais depende da adoção de políticas e mecanismos capazes de assegurar a confidencialidade, a integridade, a disponibilidade e o uso ético dos dados de saúde (OPAS, 2021). Ainda nessa linha, a OCDE ressalta que a ampliação do uso dos dados em saúde para assistência, gestão, pesquisa e formulação de políticas públicas requer estruturas robustas de governança, privacidade e segurança da informação, capazes de fortalecer a confiança da população e garantir a utilização responsável desses dados (OCDE, 2022).

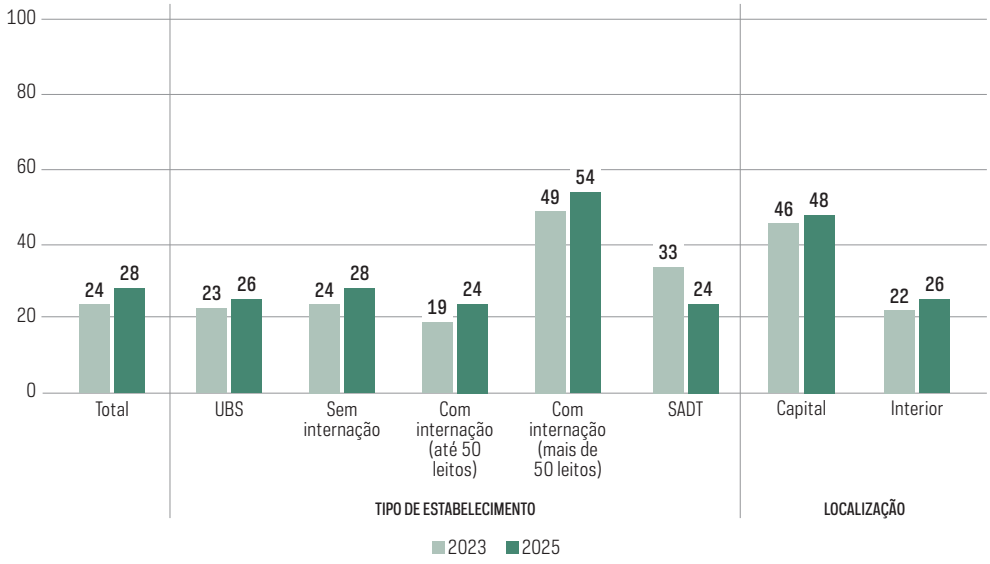
Em consonância com essas recomendações, a Organização Mundial da Saúde (OMS) tem destacado, em sua Estratégia Global de Saúde Digital 2020-2025, que a maturidade da segurança digital em saúde depende da adoção de soluções tecnológicas e da implementação de estruturas de governança, políticas institucionais, capacitação dos profissionais e mecanismos de gestão de riscos e resposta a incidentes (OMS, 2021).

No plano nacional, essa agenda encontra respaldo nos guias orientativos da ANPD voltados ao tratamento de dados pessoais pelo poder público e elaborados para orientar órgãos e entidades públicas na adequação à LGPD (ANPD, 2023). Sob essa perspectiva, os indicadores apresentados nesta seção permitem analisar o grau de institucionalização dessas capacidades nos estabelecimentos públicos de saúde brasileiros, oferecendo um panorama sobre a implementação de políticas de segurança da informação, ações de capacitação, ferramentas de proteção dos sistemas e medidas relacionadas à adequação à LGPD.

A existência de uma política de segurança da informação representa um dos principais instrumentos de governança para orientar a proteção dos ativos informacionais de uma organização: além de definir normas para o uso e a proteção dos dados, também estabelece responsabilidades, procedimentos e diretrizes para prevenir incidentes de segurança e promover uma cultura organizacional voltada à proteção dos dados. Os resultados de 2025 da pesquisa mostram que a institucionalização dessas políticas ainda permanece limitada e sem mudanças significativas entre os estabelecimentos de saúde brasileiros, visto que menos da metade (42%) declarou possuir um documento com a política de segurança da informação definida, ante 40% em 2023. Além disso, observa-se uma discrepância entre os estabelecimentos públicos (28%) e privados (54%), resultado que registrou um aumento de 4 pontos percentuais nos públicos e estabilidade nos privados.

Analisando especificamente os estabelecimentos públicos, o principal diferencial observado refere-se ao porte e à complexidade dos serviços: enquanto 54% dos hospitais públicos com mais de 50 leitos possuem política de segurança da informação, esse percentual fica em torno de um quarto nos demais tipos de estabelecimentos (Gráfico 5). Também são observadas diferenças segundo a localização dos estabelecimentos, visto que, nas capitais, 48% das unidades possuem política de segurança da informação, percentual superior ao registrado no interior (26%).

GRÁFICO 5
—
Estabelecimentos públicos de saúde, por existência de documento que define uma política de segurança da informação (2023–2025)
Total de estabelecimentos públicos de saúde com acesso à Internet (%)



O treinamento dos profissionais constitui outro componente fundamental da segurança da informação. Embora políticas institucionais estabeleçam diretrizes para a proteção dos dados, sua efetividade depende da incorporação dessas práticas à rotina de trabalho dos profissionais que utilizam sistemas de informação e trabalham com dados pessoais de pacientes.

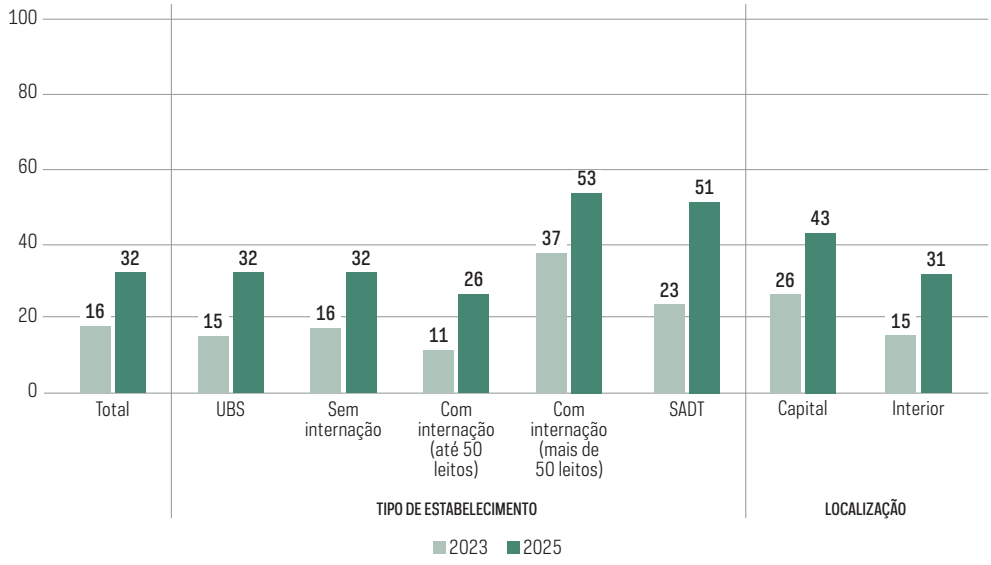
Os resultados indicam que 47% dos estabelecimentos de saúde ofereceram treinamento em segurança da informação a seus profissionais em 2025, percentual que representa um avanço em relação a 2023, quando 31% dos estabelecimentos declaravam realizar esse tipo de capacitação. Esse aumento ocorreu tanto nos estabelecimentos públicos, de 16% para 32% no período analisado, quanto nos privados, que passaram de 44% para 60%.

Apesar dessa mudança, a oferta de treinamentos permanece menos frequente no setor público. Entre essas unidades, os hospitais com mais de 50 leitos (53%) e os serviços de apoio à diagnose e terapia (SADT) (51%) apresentam os maiores percentuais dessa oferta, enquanto os demais tipos de estabelecimento registram proporção significativamente inferior (Gráfico 6). Também foram observadas diferenças segundo a localização dos estabelecimentos: nas capitais, 43% das unidades ofereceram treinamento em segurança da informação, enquanto, no interior, foram 31% dos estabelecimentos.

GRÁFICO 6
—

Estabelecimentos públicos de saúde, por existência de treinamento sobre segurança da informação para os funcionários (2023–2025)

Total de estabelecimentos públicos de saúde com acesso à Internet (%)



Além das políticas de segurança da informação e da capacitação dos profissionais, a pesquisa investigou a adoção de medidas relacionadas à implementação da LGPD. Foram analisadas iniciativas voltadas à governança de dados, como a nomeação do encarregado pelo tratamento de dados pessoais, e à implementação de planos de resposta a incidentes de segurança, bem como ações relacionadas à transparência e à conscientização institucional, incluindo a disponibilização de canais de atendimento aos titulares de dados, a publicação da política de privacidade e a realização de campanhas internas sobre a LGPD.

A comparação entre 2023 e 2025 indica que a implementação dessas medidas permaneceu relativamente estável no período. No conjunto dos estabelecimentos de saúde, observou-se pequeno aumento na realização de campanhas internas de conscientização sobre a LGPD (de 43% para 46%), na publicação da política de privacidade (de 30% para 32%) e na disponibilização de canais de atendimento aos titulares de dados (de 28% para 30%). Em contrapartida, a proporção de estabelecimentos que nomearam um encarregado manteve-se estável (30%), assim como a implementação de planos de resposta a incidentes, que passou de 31% para 30%.

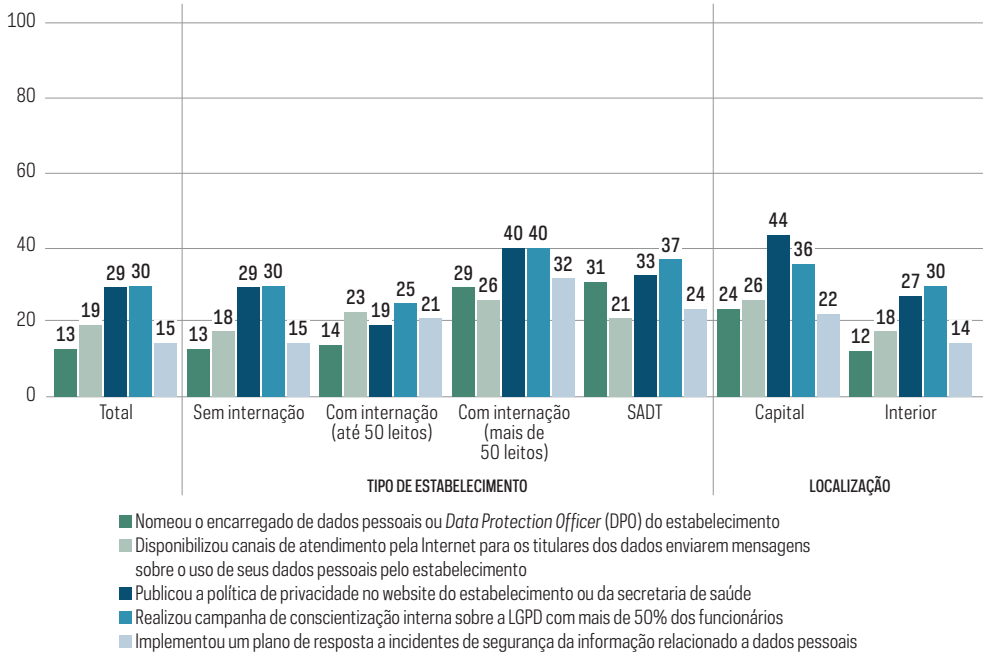
Esse padrão também foi observado quando se analisam separadamente os estabelecimentos públicos e privados. Nos estabelecimentos públicos, a realização de campanhas internas sobre a LGPD passou de 28%, em 2023, para 30%, em 2025. A publicação da política de privacidade passou de 25% para 29%, enquanto a disponibilização de canais de atendimento aos titulares dos dados, de 16% para 19%. Por outro lado, verificou-se redução na proporção de estabelecimentos que nomearam encarregado (de 16% para 13%) e implementaram planos de resposta a incidentes de segurança (de 17% para 15%). Entre os estabelecimentos privados, as variações também foram pequenas, mantendo um patamar superior ao observado no setor público em todos os indicadores analisados.

A análise dos estabelecimentos públicos em 2025 revela, portanto, diferenças importantes na adoção das medidas relacionadas à LGPD conforme o tipo de estabelecimento e a localização (Gráfico 7). De forma geral, observa-se que os hospitais com mais de 50 leitos e os SADT apresentam percentuais mais altos na maior parte dos indicadores analisados, enquanto os estabelecimentos sem internação, os hospitais com até 50 leitos e as Unidades Básicas de Saúde (UBS) registram níveis mais baixos de implementação.

GRÁFICO 7
—

Estabelecimentos públicos de saúde, por medidas adotadas em relação à LGPD (2025)

Total de estabelecimentos públicos de saúde com acesso à Internet (%)



Os hospitais públicos com mais de 50 leitos destacam-se principalmente pela publicação da política de privacidade (40%), realização de campanhas internas de conscientização sobre a LGPD (40%) e implementação de planos de resposta a incidentes de segurança da informação relacionados a dados pessoais (32%). Já os SADT apresentam o maior percentual de estabelecimentos que nomearam um encarregado pelo tratamento de dados pessoais (31%), além de também registrarem elevada adoção de políticas de privacidade (33%) e campanhas de conscientização (37%).

Em contraste, os estabelecimentos sem internação, os hospitais com até 50 leitos e as UBS apresentam percentuais inferiores na maior parte dos indicadores, especialmente na nomeação de encarregado e na implementação de planos de resposta a incidentes, que permanecem abaixo de um quarto das unidades. Esses resultados sugerem que medidas relacionadas à governança de dados e à preparação para incidentes de segurança ainda estão pouco disseminadas nos estabelecimentos públicos de menor porte e menor complexidade assistencial.

Também são observadas diferenças segundo a localização dos estabelecimentos. Em todos os indicadores analisados, as unidades localizadas nas capitais apresentam percentuais superiores aos observados no interior. As maiores diferenças concentram-se na publicação da política de privacidade (44% nas capitais e 27% no interior), na nomeação do encarregado (24% e 12%, respectivamente) e na implementação de planos de resposta a incidentes (22% e 14%).

Assim, os resultados apresentados evidenciam que a adoção de práticas de segurança da informação e de proteção de dados pessoais nos estabelecimentos de saúde está diretamente associada à capacidade institucional e à complexidade do atendimento. De forma consistente, hospitais públicos com mais de 50 leitos, os SADT e estabelecimentos localizados nas capitais apresentam níveis mais elevados de institucionalização das práticas de governança da informação, possivelmente em razão de estruturas organizacionais mais complexas, maior disponibilidade de recursos técnicos, infraestrutura, equipes especializadas e maior volume de dados e sistemas sob sua responsabilidade.

Os resultados também sugerem que as diferentes dimensões da segurança da informação não avançam de forma homogênea. Houve aumento na adoção de políticas de segurança da informação e na oferta de capacitação aos profissionais, ao passo que as medidas diretamente relacionadas à implementação da LGPD geralmente permaneceram estáveis entre 2023 e 2025, especialmente aquelas que demandam maior estrutura organizacional, como a nomeação do encarregado e a implementação de planos de resposta a incidentes. Esse cenário indica que o fortalecimento da segurança da informação nem sempre é acompanhado pela consolidação de mecanismos formais de governança e conformidade.

Além disso, os resultados sugerem uma gradação na implementação dessas medidas. Ações voltadas à conscientização dos profissionais e à transparência, como campanhas internas sobre a LGPD e publicação de políticas de privacidade, apresentam maior disseminação entre os estabelecimentos públicos. Em contrapartida, mecanismos que exigem maior capacidade institucional e definição de responsabilidades, como a nomeação do encarregado e a implementação de planos de resposta a incidentes, permanecem menos frequentes. Esse padrão é consistente com modelos internacionais de maturidade em segurança digital, segundo os quais a consolidação da governança da informação depende da integração entre políticas institucionais, capacitação, mecanismos técnicos de proteção e estruturas formais de gestão e resposta a riscos.

Escolas públicas de Educação Básica

Em 2026, foi aprovado o Plano Nacional de Educação (PNE) (Lei n. 15.388, de 14 de abril de 2026), que integra os objetivos, as metas e as estratégias a serem alcançados pelo país na oferta de Educação Básica durante o decênio 2026-2036. O Objetivo 7 apresenta metas específicas relacionadas à conectividade escolar, à educação midiática e à integração de tecnologias digitais de informação e comunicação (TDIC) aos processos de ensino e de aprendizagem, e às atividades de gestão escolar. Cinco das 20 estratégias previstas nesse objetivo fazem referência direta à transparência, à segurança, à privacidade e à proteção de dados na oferta de educação digital nas escolas, o que demonstra a relevância que tais temas adquiriram nas políticas educacionais nos últimos anos.

Além de equitativa, acessível e de qualidade, a interação de crianças e adolescentes com os ambientes digitais deve ocorrer por meio de ações que promovam o respeito aos níveis de desenvolvimento dessa população, a fim de protegê-la contra riscos diretos e indiretos no uso de recursos digitais, e preservar direitos, como privacidade e proteção de dados pessoais. Essas medidas devem orientar a adoção de serviços digitais por familiares e responsáveis, cuidadores, educadores, decisores políticos, entre outros atores.

A aprovação do ECA Digital, que entrou em vigor em março de 2026 (Decreto n. 12.880, de 18 de março de 2026), atribuiu ainda maior relevância ao debate que estava sendo realizado em torno da LGPD, por expandir o escopo de atuação dos múltiplos setores da sociedade em sua aplicação. Indivíduos e organizações passaram a ser responsáveis pela proteção de crianças e adolescentes nos ambientes digitais de forma integral, considerando também seu bem-estar, os impactos do desenho dos sistemas em seu desenvolvimento e a criação de oportunidades no uso de tecnologias digitais, prevenindo os possíveis riscos. (Oliveira *et al.*, 2026).

Nesse sentido, a aplicação do ECA Digital vai além de recursos e serviços digitais destinados ao uso corrente por crianças e adolescentes — como jogos, plataformas educacionais e aplicações lúdicas — contemplando também recursos que possam se configurar como de provável utilização ou interesse desses indivíduos, tais como "aplicações de Internet, programas de computador, *software*, sistemas operacionais de terminais, lojas de aplicações de Internet e jogos eletrônicos ou similares conectados à Internet ou a outra rede de comunicações" (Lei n. 15.211/2025). Dessa forma, a responsabilidade pela adoção de medidas de segurança, privacidade e monitoramento da prevenção de riscos ao bem-estar de crianças e adolescentes passa a ser compartilhada com fornecedores de produtos ou serviços digitais, incluindo as plataformas e soluções contratadas por instituições de ensino.

Os dados coletados com a comunidade escolar pela pesquisa TIC Educação permitem observar a disseminação de tais temas nas instituições educacionais. Para 39% dos gestores de escolas públicas (municipais, estaduais e federais) de Ensino Fundamental e Médio, por exemplo, a preocupação em relação aos riscos à privacidade e à proteção de dados pessoais estava entre os principais desafios enfrentados pelas escolas que não utilizavam programas, sistemas e plataformas digitais na gestão escolar. De acordo com os dados da edição 2025 da pesquisa, tal receio foi mencionado por 36% dos gestores de escolas municipais e 58% dos de escolas estaduais.

Ademais, a preocupação com a privacidade e a proteção de dados dos alunos foi também citada por 25% dos gestores como motivo para deixar de adotar dispositivos, plataformas ou outros recursos educacionais digitais. O fato de o recurso digital representar riscos de vazamento ou roubo de dados dos alunos (16%) ou os termos de uso dos recursos digitais não dizerem de forma objetiva quais usos seriam realizados dos dados dos alunos (15%) estavam entre os motivos citados em maiores proporções pelos gestores escolares da rede pública.

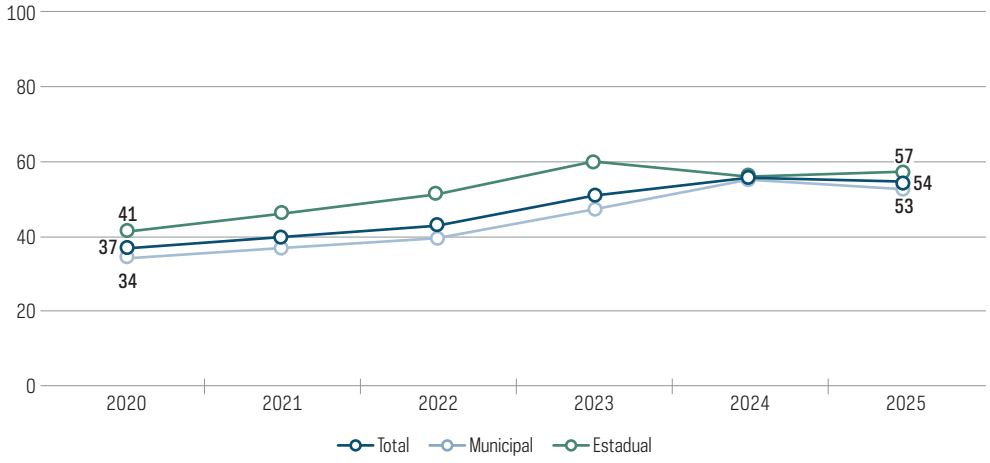
A escolha por não adotar dispositivos, plataformas ou outros recursos educacionais digitais devido à preocupação em relação aos riscos à privacidade e à proteção de dados pessoais foi mais frequente entre gestores de escolas da rede particular (41%), em comparação com os dados coletados com gestores de escolas públicas — escolas municipais (23%) e escolas estaduais (27%) — o que pode se relacionar à maior autonomia usufruída

pelas equipes da rede particular para seleção e adoção de recursos educacionais. De acordo com dados coletados com coordenadores pedagógicos para a edição 2024 da pesquisa TIC Educação, 40% desses profissionais informaram participar sempre da seleção de recursos educacionais digitais utilizados na escola, proporção de 32% entre os coordenadores de escolas municipais, 42% entre os coordenadores de escolas estaduais e 61% entre aqueles que atuavam na rede particular. Assim, a centralização das decisões em relação aos serviços digitais utilizados nas atividades de ensino, de aprendizagem e de gestão escolar nos órgãos da administração pública torna ainda mais relevante a atenção dispensada por essas redes de ensino aos temas relacionados à garantia de direitos digitais, como a privacidade e a proteção de dados pessoais.

Em relação à presença de um documento que define a política de proteção de dados e de segurança da informação na instituição, em 2020, 37% do total de escolas públicas de Ensino Fundamental e Médio possuíam esse tipo de documento, proporção que chegou a 54% na edição 2025 da pesquisa. Conforme o Gráfico 8, é possível observar um crescimento gradual na presença desse documento nas escolas públicas, embora ainda sejam necessárias ações para uma maior disseminação do tema, uma vez que pouco mais da metade dos gestores afirmaram que as instituições contavam com tais diretrizes.

GRÁFICO 8
–
Escolas públicas com documento que define a política de proteção de dados e de segurança da informação na instituição (2020–2025)

Total de escolas públicas de Ensino Fundamental e Médio (%)

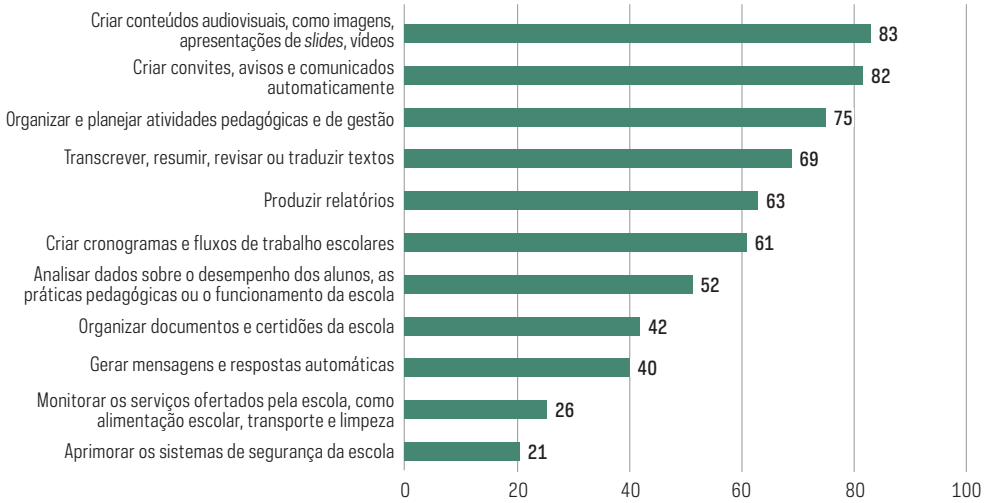


No que se refere ao apoio das redes de ensino, 73% dos gestores de escolas públicas disseram ter recebido orientações sobre o tratamento de dados pessoais de alunos, professores e profissionais da escola, proporção que foi de 71% entre as escolas municipais e 71% entre as escolas estaduais.

A disseminação do uso de tecnologias emergentes, como os sistemas baseados em IA preditiva ou generativa nas atividades de ensino e de aprendizagem e de gestão escolar, adiciona ainda maior relevância à discussão sobre privacidade e proteção de dados pessoais nas instituições educacionais, especialmente da rede pública de ensino (Ministério da Educação [MEC], 2026a). Na edição 2025 da pesquisa, 14% das escolas da rede pública localizadas na região Sul declararam possuir sistema de identificação dos alunos por meio de reconhecimento facial, proporção de 1% entre as escolas localizadas na região Norte, 4% na região Sudeste, 5% na região Nordeste e 7% na região Centro-Oeste. Destaca-se que o uso de sistemas baseados em dados biométricos é considerado de alto risco, devido à sensibilidade do tipo de dado coletado, armazenado e tratado pelas empresas que fornecem esse tipo de serviço (MEC, 2026b; Internetlab, 2025).

No caso do uso de IA generativa em atividades de gestão escolar, esse tipo de tecnologia foi mencionado por 53% dos gestores escolares (51% entre os gestores de escolas municipais e 58% entre os de escolas estaduais). Grande parte dos gestores escolares de escolas públicas disse adotar esses recursos digitais na produção de conteúdos visuais ou de comunicação, como imagens, apresentações de *slides*, vídeos, entre outros (83%), convites, avisos e comunicados (82%), ou transcrição, resumo, revisão e tradução de textos (69%). Além disso, metade dos gestores afirmaram adotar tais recursos digitais na análise de dados sobre o desempenho dos alunos, as práticas pedagógicas ou o funcionamento da escola para embasar decisões da gestão (52%), atividades que poderiam ser consideradas mais complexas em termos de habilidades digitais e mais críticas em relação à privacidade e à proteção de dados (Gráfico 9).

GRÁFICO 9
—
Gestores de escolas públicas, por atividades de gestão pedagógica, administrativa ou financeira realizadas por meio da adoção de IA (2025)
Total de gestores de escolas públicas de Ensino Fundamental e Médio que adotam IA em atividades de gestão (%)



Embora grande parte das escolas não contasse ainda com orientações sistematizadas sobre o uso desses recursos nas atividades de gestão (22%), uma proporção relevante de gestores de escolas da rede pública (60%) mencionou ter discutido com educadores, profissionais da escola, familiares e responsáveis sobre o uso de sistemas baseados em IA por alunos e professores — 57% entre os gestores de escolas municipais e 57% entre os gestores de escolas estaduais.

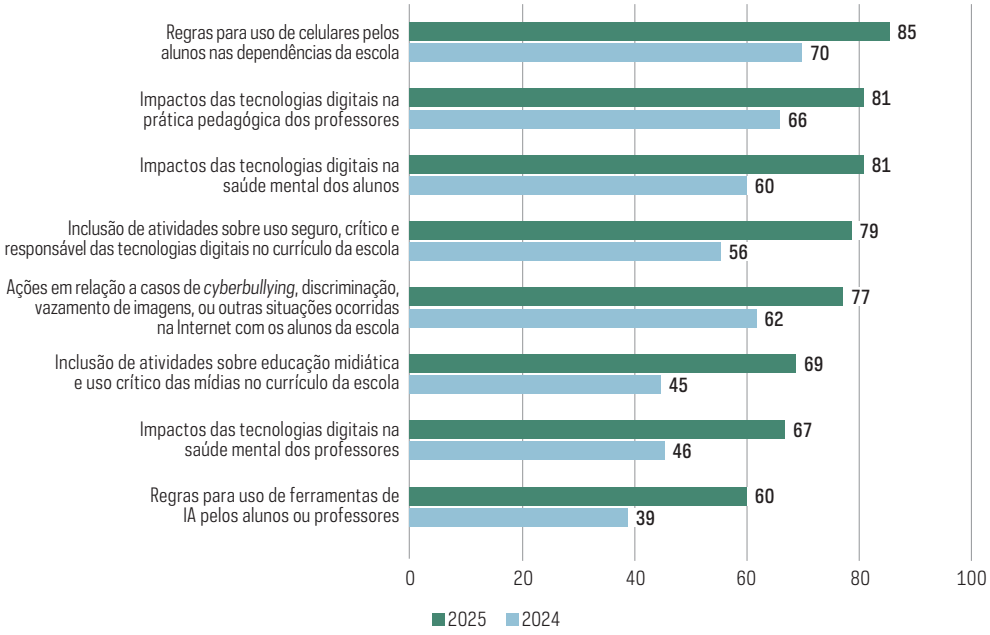
Entre as edições de 2024 e 2025, foram observadas variações nos dados sobre a realização (nos 12 meses anteriores à pesquisa) de reuniões com professores e outros profissionais para discutir o uso de tecnologias digitais na escola (de 66% para 87%), e de reuniões com pais, mães e responsáveis (de 60% para 78%). A possível influência das discussões que cercaram a aprovação da Lei n. 15.100/2025, de restrição ao uso de telefones celulares pelos alunos nos ambientes escolares, e do ECA Digital pode ser observada ainda na análise dos temas discutidos pelos gestores escolares nas reuniões com educadores, profissionais da escola, familiares e responsáveis. Entre as edições 2024 e 2025 da pesquisa, o debate sobre os impactos das tecnologias digitais na saúde mental dos alunos passou de 60% para 81%; a inclusão de atividades relacionadas ao uso seguro, crítico e responsável das tecnologias digitais no currículo da escola, de 56% para 79%; e a inclusão de atividades sobre educação midiática, de 45% para 69% (Gráfico 10).

GRÁFICO 10

—

Gestores de escolas públicas, por temas discutidos durante as reuniões realizadas nos 12 meses anteriores à coleta de dados da pesquisa com professores, profissionais da escola, familiares e responsáveis sobre o uso de tecnologias digitais na instituição (2024–2025)

Total de gestores de escolas públicas de Ensino Fundamental e Médio com acesso à Internet (%)

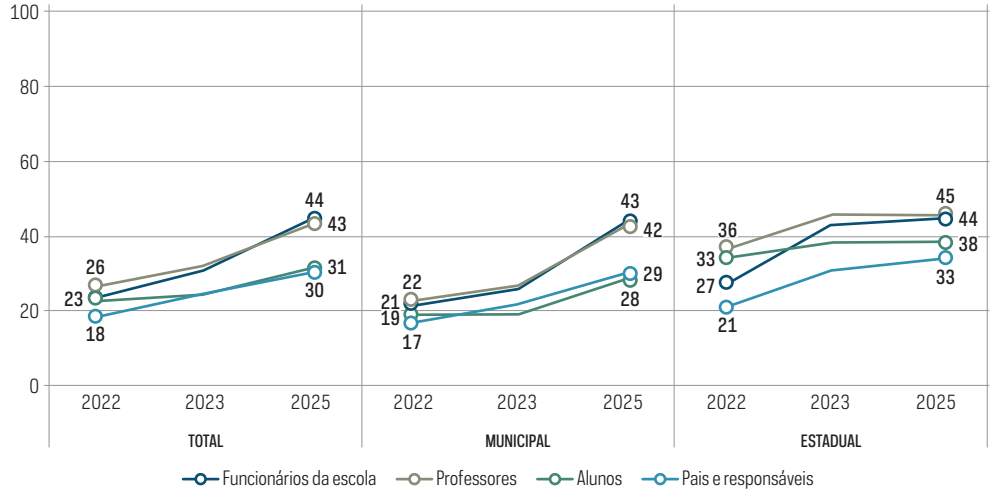


A comparação entre os dados coletados nas edições 2023 e 2025 da pesquisa indica uma variação positiva também na proporção de instituições que realizaram debates ou promoveram palestras especificamente sobre privacidade e proteção de dados pessoais nos 12 meses anteriores à realização da pesquisa, passando de 32% para 46% entre as escolas públicas, com maiores variações entre as escolas municipais (de 27% para 45%).

No geral, as equipes internas, como professores (44%) e outros profissionais que atuam na instituição (43%), foram o principal público-alvo das iniciativas realizadas nas escolas sobre privacidade e proteção de dados. Além de uma proporção maior de gestores ter mencionado a oferta de debates e palestras para esses profissionais na última edição do estudo, a comparação dos dados com a edição 2023 evidencia ainda uma variação positiva, conforme observado no Gráfico 11.

GRÁFICO 11
–
Escolas públicas, por público-alvo da oferta de debates ou palestras sobre privacidade e proteção de dados realizados na escola nos 12 meses anteriores à realização da pesquisa (2022–2025)

Total de escolas públicas de Ensino Fundamental e Médio (%)



Do total de escolas da rede pública, 24% ofertaram atividades sobre o tema para os alunos, proporção que atinge maiores patamares entre as escolas estaduais (33%); ainda assim, apenas um terço das instituições haviam contemplado os alunos nas iniciativas desenvolvidas nas escolas. No entanto, os estudantes são o principal foco das políticas previstas nas normativas e nos documentos orientadores sobre educação digital e midiática, como a Política Nacional de Educação Digital (Pned) (Lei n. 14.533, de 11 de janeiro de 2023), a Estratégia Brasileira de Educação Midiática (Ebem) (Secretaria de Comunicação Social [Secom], 2023), as diretrizes operacionais nacionais do Conselho Nacional de Educação (CNE) (Resolução CNE/CEB n. 2/2025), o ECA Digital e o PNE 2026-2036.

Os dados analisados revelam avanços na discussão sobre direitos, privacidade e proteção de dados nas escolas públicas. Os debates realizados pela sociedade durante a aprovação da Lei n. 15.100/2025 e do ECA Digital, relacionados aos riscos a que crianças e adolescentes estão expostos nos ambientes digitais e sobre o papel das escolas na rede de proteção e apoio psicossocial aos alunos, possivelmente tenham impulsionado tais discussões. Por outro lado, a transformação dos debates em iniciativas efetivas ainda demanda maior atenção da comunidade escolar e das políticas educacionais públicas, especialmente no que diz respeito ao acesso dos alunos a orientações e aprendizados sobre como interagir com tais ambientes de forma ética, segura, crítica, criativa e responsável.

Considerações finais: agenda para políticas públicas

Os resultados apresentados neste capítulo permitem analisar, de forma integrada, como organizações públicas de diferentes áreas têm estruturado iniciativas voltadas à privacidade e à proteção de dados pessoais em um contexto de crescente digitalização. Embora as três pesquisas analisadas revelem avanços importantes, também evidenciam desafios persistentes relacionados à consolidação dessas capacidades institucionais e à redução das assimetrias entre os diferentes tipos de organizações públicas.

As três edições da TIC Governo que investigaram indicadores de privacidade e proteção de dados pessoais evidenciam avanços na criação de estruturas institucionais e na implementação de ações relacionadas ao tema nas organizações públicas brasileiras. Em 2025, foram observados aumentos significativos na adoção dessas iniciativas, sobretudo entre grupos que, nas edições anteriores, apresentavam menores proporções, como os órgãos públicos estaduais e as prefeituras de menor porte populacional.

Apesar desses resultados, permanece o cenário de disparidades entre as organizações públicas, identificado em 2021 e 2023. Em geral, as iniciativas medidas continuam mais presentes nos órgãos federais e do Poder Judiciário, bem como nas capitais e nos municípios de maior porte populacional. A nomeação do encarregado pelo tratamento de dados pessoais ilustra essas diferenças: embora prevista no art. 41 da LGPD e regulamentada pela Resolução CD/ANPD n. 18/2024, foi declarada por apenas 28% das prefeituras. Os resultados indicam, portanto, que a consolidação de estruturas de governança em privacidade e proteção de dados ainda ocorre de forma desigual entre os níveis de governo e os diferentes portes de municípios.

Esse panorama contrasta com o avanço da transformação digital identificado em outros módulos da TIC Governo 2025. A oferta de serviços públicos digitais está disseminada, enquanto cresce o uso de tecnologias de IA, especialmente entre órgãos federais e estaduais, capitais e municípios de maior porte. Como essas iniciativas frequentemente envolvem o tratamento intensivo de dados pessoais e podem incluir decisões automatizadas com efeitos sobre os cidadãos, sua expansão deve ser acompanhada pelo fortalecimento de estruturas de privacidade, proteção de dados e segurança da informação.

Por outro lado, os resultados da TIC Saúde 2025 evidenciam que a ampliação da digitalização dos estabelecimentos de saúde tem sido acompanhada por avanços na institucionalização de práticas de segurança da informação, como a adoção de políticas formais e a realização de capacitações para os profissionais. No entanto, as medidas diretamente relacionadas à implementação da LGPD apresentaram pouca evolução em relação às edições anteriores da pesquisa, permanecendo menos disseminadas, especialmente entre os estabelecimentos públicos sem internação e as UBS. Os resultados também revelam desigualdades na capacidade institucional dos estabelecimentos, com maior presença de práticas de governança da informação em hospitais com mais de 50 leitos, SADT e unidades localizadas nas capitais.

Esse cenário ocorre em um contexto de rápida transformação digital do setor de saúde, marcado pela expansão dos prontuários eletrônicos, da interoperabilidade entre sistemas, da telessaúde e da incorporação de aplicações de IA para apoiar processos clínicos, administrativos e de segurança digital. À medida que essas tecnologias ampliam o processamento e o compartilhamento de dados pessoais sensíveis, torna-se cada vez mais necessário fortalecer a governança de dados, segurança da informação e proteção da privacidade dos pacientes. Os resultados da pesquisa sugerem, portanto, que a consolidação dessas capacidades institucionais constitui um elemento essencial para promover o uso responsável de dados em saúde, fortalecer a confiança nos serviços digitais de saúde e assegurar que a inovação tecnológica avance em consonância com a proteção dos direitos dos pacientes.

Quanto às instituições de ensino, os resultados da TIC Educação evidenciam que a incorporação de tecnologias digitais nas escolas públicas continua avançando, tanto para apoiar a gestão escolar quanto os processos de ensino e aprendizagem. Contudo, a consolidação de práticas voltadas à proteção de dados pessoais e à segurança da informação ainda ocorre de forma desigual entre as instituições de ensino. Embora tenham sido observados avanços em algumas iniciativas investigadas, permanecem desafios importantes voltados à institucionalização dessas práticas, especialmente em um contexto de crescente utilização de plataformas digitais, ambientes virtuais de aprendizagem e outros sistemas que envolvem o tratamento de dados de estudantes, professores e demais membros da comunidade escolar.

Esses desafios tornam-se ainda mais relevantes diante da expansão do uso de aplicações de IA na educação e da crescente adoção de recursos digitais voltados ao ensino e à aprendizagem. Ao mesmo tempo em que essas tecnologias ampliam as possibilidades de apoio às atividades pedagógicas e à gestão escolar, também reforçam a necessidade de assegurar a proteção dos dados pessoais, especialmente de crianças e adolescentes. Nesse contexto, o fortalecimento da governança de dados, da segurança da informação e da capacitação das equipes escolares torna-se fundamental para que a transformação digital da educação ocorra de forma ética, segura e alinhada à LGPD e ao ECA Digital.

Em conjunto, os resultados das pesquisas TIC Governo, TIC Saúde e TIC Educação evidenciam que a transformação digital das organizações públicas brasileiras continua avançando em diferentes aspectos. A ampliação da oferta de serviços públicos digitais, o avanço na informatização dos estabelecimentos de saúde, a incorporação de tecnologias digitais às atividades de ensino e aprendizagem, e o crescente uso de ferramentas de IA apontam para um processo de intensificação do uso de dados no setor público brasileiro. Esse movimento amplia as possibilidades de inovação, eficiência e melhoria da gestão pública; por outro lado, torna mais complexos os desafios relacionados à governança de dados, à segurança da informação e à proteção dos dados pessoais.

Nesse contexto, a consolidação da LGPD e a entrada em vigor do ECA Digital reforçam a necessidade de fortalecer as capacidades institucionais das organizações públicas. Os resultados das três pesquisas mostram que, apesar dos avanços em iniciativas relacionadas à segurança da informação e à criação de estruturas de governança, essas ações ainda se distribuem de forma desigual entre diferentes níveis de governo, estabelecimentos de saúde e instituições de ensino.

Por fim, os resultados apresentados neste capítulo reforçam que, para além da consolidação de marcos regulatórios, a implementação de medidas de proteção de dados nas organizações públicas depende do desenvolvimento de capacidades institucionais. Logo, torna-se fundamental ampliar políticas públicas voltadas à disseminação de boas práticas, à capacitação contínua de servidores e profissionais, e à maior institucionalização da governança de dados com o fim de assegurar que a transformação digital ocorra de forma segura, ética, transparente e alinhada à proteção dos direitos dos cidadãos.

Referências

Agência Nacional de Proteção de Dados. (2023). *Guia orientativo: tratamento de dados pessoais pelo Poder Público*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

Agência Nacional de Proteção de Dados. (2024). *Glossário de proteção de dados pessoais e privacidade*. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf

Agência Nacional de Proteção de Dados. (2025). *Nota Técnica n. 12/2025/CON1/CGN/ANPD*. https://www.gov.br/anpd/pt-br/acesso-a-informacao/participacao-social/outras-acoes/documentos/ts-06-2024-nt-12-2025-consolidacao-das-contribuicoes.pdf/@@display-file/file

Aith, F., Santana, S., & Dallari, S. G. (2025). Transformação digital da saúde e proteção de dados pessoais: Desafios para a governança dos sistemas de saúde. *Revista de Direito Sanitário, 25*, e0025. https://doi.org/10.11606/issn.2316-9044.rdisan.2025.240814

Ansar, S., Clark, J. M., & Wolff, J. M. (2026). *ID4D Global Dataset 2025 : Trends in identification for development.* World Bank Group. http://documents.worldbank.org/curated/en/099061526195037307

Comitê Gestor da Internet no Brasil. (2024*). Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2023*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2023/

Comitê Gestor da Internet no Brasil. (2025). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2024*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-escolas-brasileiras-tic-educacao-2024/

Comitê Gestor da Internet no Brasil. (2026a). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2025*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-escolas-brasileiras-tic-educacao-2025/

Comitê Gestor da Internet no Brasil. (2026b). *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo 2025*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2025/

Comitê Gestor da Internet no Brasil. (2026c). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2025*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2025/

Decreto n. 12.622, de 17 de setembro de 2025. (2025). Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, para designar a Agência Nacional de Proteção de Dados como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais, e estabelecer competências para cumprimento de ordens judiciais de bloqueio. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12622.htm

Decreto n. 12.880, de 18 de março de 2026. (2026). Regulamenta a Lei n. 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. https://www.in.gov.br/en/web/dou/-/decreto-n-12.880-de-18-de-marco-de-2026-693683613

Departamento de Assuntos Econômicos e Sociais das Nações Unidas. (2024). *E-Government Survey 2024: Accelerating digital transformation for sustainable development: With the addendum on Artificial Intelligence*. https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024

Estatuto Digital da Criança e do Adolescente. Lei n. 15.211, de 17 de setembro de 2025. (2025). Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

InternetLab. (2025). *Tecnologias de vigilância e inteligência artificial na educação: promessas de modernização, realidades de opacidade.* https://internetlab.org.br/pt/biblioteca/relatorio-completo-tecnologias-de-vigilancia-e-inteligencia-artificial-na-educacao-promessas-de-modernizacao-realidades-de-opacidade/

Lei Geral de Proteção de Dados Pessoais. Lei n. 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Lei n. 14.129/2021, de 29 de março de 2021. (2021). Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

Lei n. 15.100, de 13 de janeiro de 2025. (2025). Dispõe sobre a utilização, por estudantes, de aparelhos eletrônicos portáteis pessoais nos estabelecimentos públicos e privados de ensino da educação básica. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

Lei n. 15.388, de 14 de abril de 2026. (2026). Aprova o Plano Nacional de Educação (PNE). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15388.htm

Maia, G. (2026, 6 de março). *Zero-click government: Why it's time to rethink when and how the state acts.* Fórum Econômico Mundial. https://www.weforum.org/stories/all/digital-government-ai-zero-click/

Ministério da Ciência, Tecnologia e Inovação & Centro de Gestão e Estudos Estratégicos. (2025). *IA para o bem de todos: Plano Brasileiro de Inteligência Artificial.* https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial-pbia-_vf.pdf

Ministério da Educação. (2026a). *Inteligência Artificial na Educação Básica: documento orientador sobre caminhos curriculares e práticas éticas de uso de IA nas escolas*. https://www.gov.br/mec/pt-br/escolas-conectadas/arquivos/ia-basica.pdf

Ministério da Educação. (2026b). *Referencial para desenvolvimento e uso responsáveis de inteligência artificial na educação*. https://www.gov.br/mec/pt-br/referencial-de-ia-na-educacao/referencial-ia-na-educacao

Ministério da Gestão e da Inovação em Serviços Públicos. (s.d.). *Estratégia Nacional de Governo Digital*. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional/

Ministério da Gestão e da Inovação em Serviços Públicos. (2024). *Guia de elaboração de Programa de Governança em Privacidade* (Versão 2.3). https://tce.pb.gov.br/wp-content/uploads/2025/09/11guia_programa_governanca_privacidade.pdf

Oliveira, D. T. N., Machado, D. C., Barbosa, J. D. & Carvalho, L. B. (2026). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. http://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf

Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2022). *Artificial intelligence and digital transformation: competencies for civil servants*. https://unesdoc.unesco.org/ark:/48223/pf0000383325

Organização Mundial da Saúde. (2021). *Estratégia global sobre saúde digital 2020–2025*. OMS. https://www.who.int/publications/i/item/9789240020924

Organização Pan-Americana da Saúde. (2021). *Oito princípios orientadores da transformação digital do setor da saúde: um apelo à ação pan-americana (OPAS/EIH/IS/21-0004)*. https://iris.paho.org/handle/10665.2/54669

Organização para a Cooperação e Desenvolvimento Econômico. (2022). *Governança de dados de saúde para a era digital: Implementando a Recomendação da OCDE sobre Governança de Dados de Saúde*. OECD Publishing. https://doi.org/10.1787/a5731b0e-en

Organização para a Cooperação e Desenvolvimento Econômico. (2026). *Digital Government Outlook 2026: From foundations to transformational impact*. OECD Publishing. https://doi.org/10.1787/0496b2bc-en

Política Nacional de Educação Digital. Lei n. 14.533, de 11 de janeiro de 2023. (2023). Institui a Política Nacional de Educação Digital e altera as Leis n. 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), n. 9.448, de 14 de março de 1997, n. 10.260, de 12 de julho de 2001, e n. 10.753, de 30 de outubro de 2003. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm

Resolução CD/ANPD n. 18, de 16 de julho de 2024. (2024). Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074

Resolução CD/ANPD n. 31, de 22 de dezembro de 2025. (2025). Altera a Agenda Regulatória para o biênio 2025-2026. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080

Resolução CNE/CEB n. 2, de 21 de março de 2025. (2025). Institui as Diretrizes Operacionais Nacionais sobre o uso de dispositivos digitais em espaços escolares e integração curricular de educação digital e midiática. Conselho Nacional de Educação, Câmara de Educação Básica. https://www.gov.br/mec/pt-br/cne/2025/marco/rceb002_25.pdf

Resolução n. 281, de 12 de dezembro de 2023. (2023). Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público e dá outras providências. Conselho Nacional do Ministério Público. https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-281-de-2023.pdf

Secretaria de Comunicação Social da Presidência da República. (2023). *Estratégia Brasileira de Educação Midiática.* https://www.gov.br/secom/pt-br/arquivos/2023_secom-spdigi_estrategia-brasileira-de-educacao-midiatica.pdf

Lista de Abreviaturas

ANPD – Agência Nacional de Proteção de Dados

BID – Banco Interamericano de Desenvolvimento

CAPI – *computer-assisted personal interviewing*

CATI – *computer-assisted telephone interviewing*

CDC – Código de Defesa do Consumidor

Cempre – Cadastro Central de Empresas

Ceptro.br – Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Cetic.br – Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

Ceweb.br – Centro de Estudos sobre Tecnologias Web

CGEE – Centro de Gestão e Estudos Estratégicos

CGI.br – Comitê Gestor da Internet no Brasil

CNAE – Classificação Nacional de Atividades Econômicas

CNE – Conselho Nacional de Educação

CNES – Cadastro Nacional de Estabelecimentos de Saúde

CNMP – Conselho Nacional do Ministério Público

Ebem – Estratégia Brasileira de Educação Midiática

ECA – Estatuto da Criança e do Adolescente

ECA Digital – Estatuto Digital da Criança e do Adolescente

ENGD – Estratégia Nacional de Governo Digital

Eurostat – Instituto de Estatísticas da Comissão Europeia

FBSP – Fórum Brasileiro de Segurança Pública

IA – Inteligência Artificial

IBGE – Instituto Brasileiro de Geografia e Estatística

Interpol – Organização Internacional de Polícia Criminal

IoT – Internet das Coisas

IX.br – Brasil Internet Exchange

Lacsi – Iniciativa de Pesquisas de Vitimização na América Latina e Caribe

LGPD – Lei Geral de Proteção de Dados Pessoais

MCTI – Ministério da Ciência, Tecnologia e Inovação

MEC – Ministério da Educação

Mercosul – Mercado Comum do Sul

MGI – Ministério da Gestão e da Inovação em Serviços Públicos

MJSP – Ministério da Justiça e Segurança Pública

MS – Ministério da Saúde

NIC.br – Núcleo de Informação e Coordenação do Ponto BR

OBIA – Observatório Brasileiro de Inteligência Artificial

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OMS – Organização Mundial da Saúde

ONU – Organização das Nações Unidas

OPAS – Organização Pan-Americana da Saúde

PBIA – Plano Brasileiro de Inteligência Artificial

PNAD Contínua – Pesquisa Nacional por Amostra de Domicílios Contínua

PNE – Plano Nacional de Educação

Pned – Política Nacional de Educação Digital

PTT – Pontos de Troca de Tráfego

SADT – serviço de apoio à diagnose e terapia

Secom – Secretaria de Comunicação Social

SMS – *Short Message Service*

TDIC - tecnologias digitais de informação e comunicação

TI – tecnologia da informação

TIC – tecnologias de informação e comunicação

UBS – Unidades Básicas de Saúde

UIT – União Internacional de Telecomunicações

UNCTAD – ONU Comércio e Desenvolvimento

UN DESA – Departamento de Assuntos Econômicos e Sociais das Nações Unidas

UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura

UNODC – Escritório das Nações Unidas sobre Drogas e Crime

unesco

Centro
sob os auspícios
da UNESCO

cetic.br

Centro Regional
de Estudos para o
Desenvolvimento
da Sociedade
da Informação

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgi.br

Comitê Gestor da
Internet no Brasil