



Centro Universitário Processus

PORTARIA Nº 282, DE 14 DE ABRIL DE 2022

Tema: A proteção de dados pessoais como instrumento de prevenção a golpes digitais sob a perspectiva da governança e do *compliance*, à luz da Lei Geral de Proteção de Dados (LGPD).

1. Introdução

O avanço no uso de tecnologias digitais nas esferas sociais, econômicas e institucionais têm ampliado de maneira expressiva a coleta, a circulação e o tratamento de dados pessoais. Por outro lado, esse cenário tem contribuído para o crescimento de golpes digitais, fraudes eletrônicas e outras práticas ilícitas que se utilizam do uso indevido dessas informações. Diante disso, a proteção de dados pessoais deixa de ser apenas uma questão relacionada à privacidade individual e passa a assumir um papel estratégico na gestão de riscos, na integridade institucional e na conformidade regulatória. No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece princípios, deveres e mecanismos de responsabilização, exigindo das organizações a adoção de medidas técnicas e administrativas voltadas à segurança das informações.

Nesse contexto, a governança e o *compliance* ganham destaque, uma vez que a adequação à LGPD vai além do cumprimento formal da norma, envolvendo a implementação de políticas internas, controles e práticas organizacionais orientadas à prevenção de riscos e ao fortalecimento de uma cultura de proteção de dados. Assim, a ocorrência de golpes digitais está diretamente relacionada à eficácia dessas estruturas na redução de vulnerabilidades e na contenção do uso indevido de dados pessoais. Desse modo, a presente pesquisa busca analisar em que medida a proteção de dados, orientada pela LGPD e sustentada por práticas de

governança e *compliance*, pode contribuir para a prevenção de golpes digitais no contexto brasileiro.

2. Objetivo Geral

Analisar como a gestão ética e segura de dados pessoais, através de programas de *compliance* e governança, funciona como um mecanismo de prevenção a fraudes e golpes eletrônicos dentro do contexto brasileiro.

3. Objetivos Específicos

- Examinar os fundamentos jurídicos da proteção de dados pessoais previstos na LGPD e sua relação com a governança e o *compliance*.

Os fundamentos da lei têm como base o artigo 2º da LGPD. São eles: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; o desenvolvimento econômico, tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Buscando justamente equilibrar essa proteção à privacidade com o desenvolvimento econômico e tecnológico, a lei estabelece, além dos fundamentos, os princípios previstos no artigo 6º. Esses princípios atuam como diretrizes operacionais de boa-fé, de forma que o tratamento ocorra de maneira segura, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A governança de dados se dá através de um conjunto de práticas, políticas e estruturas organizacionais destinadas à administração adequada das informações pessoais. Ou seja, as empresas precisam estabelecer procedimentos internos, além de observar o princípio da *accountability*, que impõe o dever de prestação de contas e de demonstrar a conformidade com a lei. O *compliance*, por sua vez, tem o intuito de proteger dados sensíveis. Sendo assim, está mais ligado à execução, ou seja, as

organizações devem estar atentas e desenvolver controles preventivos para potenciais riscos.

Nesse sentido, o programa de *compliance* envolve auditorias internas, a análise de probabilidade versus o impacto do risco vir a existir, a implementação de medidas corretivas em caso de incidente e o treinamento dos colaboradores.

A cada dia que passa, a LGPD apresenta um avanço significativo; no entanto, sua efetividade depende da integração de seus fundamentos jurídicos, exigindo uma atuação mais proativa por parte das instituições.

- Identificar a relação entre o uso indevido de dados pessoais e a ocorrência de golpes digitais.

A relação entre o tratamento inadequado de dados e a criminalidade digital é de causalidade direta. No ecossistema do cibercrime, os dados pessoais (como CPF, RG, endereço, histórico de compras e comportamento de navegação) funcionam como o "combustível" para a execução de fraudes sofisticadas. Sob a ótica da LGPD e da Governança, essa relação pode ser segmentada em três pilares fundamentais:

A) O Dado Pessoal como Ativo para Engenharia Social

O uso indevido de dados permite que criminosos construam abordagens personalizadas, aumentando drasticamente a taxa de sucesso dos golpes. Ao obter acesso a dados vazados, o fraudador deixa de realizar disparos genéricos e passa a utilizar a Engenharia Social.

Exemplo: Um golpe de "falso sequestro" ou "falso funcionário de banco" torna-se muito mais convincente quando o criminoso cita o nome completo da vítima, o final do seu cartão de crédito ou uma transação financeira recente.

Conexão com a LGPD: O desrespeito ao princípio da finalidade e do livre acesso (Art. 6º, I e IV) facilita que dados coletados para fins legítimos acabem no mercado clandestino, alimentando essa base de informações.

B) O Ciclo do Vazamento e a Reidentificação

A ocorrência de golpes é muitas vezes o estágio final de um incidente de segurança anterior. Quando uma organização falha em seus protocolos de compliance e sofre um vazamento, esses dados são comercializados em fóruns da Deep Web.

Vulnerabilidade: Dados que isoladamente parecem inofensivos podem ser cruzados para a reidentificação do titular, permitindo a abertura de contas bancárias fraudulentas, contratação de empréstimos em nome de terceiros ou invasão de dispositivos.

Responsabilidade Civil: Aqui entra a relevância da governança: a ausência de medidas técnicas e administrativas (Art. 46 da LGPD) gera a responsabilidade objetiva das empresas pelos danos causados por esses golpes decorrentes de falhas na segurança.

C) A Monetização da Inobservância Normativa

A relação se prova pelo fato de que golpes como *phishing*, *smishing* (SMS falso) e *ransomware* dependem da exploração de bases de dados desprotegidas. O uso indevido não é apenas o roubo, mas também o armazenamento excessivo.

Princípio da Necessidade (Minimização): Instituições que coletam mais dados do que o necessário (descumprindo o Art. 6º, III da LGPD) criam um "pote de ouro" para criminosos. Quanto maior o volume de dados tratados sem governança, maior o potencial lesivo de um eventual golpe digital.

- Explicar como práticas de governança e compliance podem contribuir para a prevenção de golpes digitais no contexto da LGPD.

As práticas de governança e compliance são essenciais para evitar golpes digitais no contexto da LGPD, pois ajudam a organizar e controlar o uso dos dados. A governança define regras claras sobre coleta e acesso, de acordo com o art. 50, que trata das boas práticas, e também segue o princípio da responsabilização e prestação de contas (art. 6º, X), exigindo que a empresa comprove que suas medidas são eficazes. Ao aplicar o *Privacy by Design* (privacidade desde a concepção), a segurança já é incorporada desde o início dos processos, diminuindo brechas e falhas que podem ser exploradas por criminosos.

O compliance garante que as normas sejam cumpridas e que haja uma separação clara entre as funções de controlador e operador (art. 5º, VI e VII), evitando lacunas contratuais. Essas práticas também incentivam auditorias e a adoção de medidas técnicas, como por exemplo criptografia e autenticação em múltiplos fatores, atendendo ao princípio da segurança (art. 6º, VII) e ao dever de proteção previsto no art. 46.

Além disso, promovem uma cultura de segurança por meio de treinamentos sobre phishing e engenharia social, colocando em prática o princípio da prevenção (art. 6º, VIII) para reduzir riscos antes que eles aconteçam. Também asseguram uma resposta rápida a incidentes, incluindo a comunicação obrigatória à Autoridade Nacional de Proteção de Dados e ao titular, conforme o art. 48, diminuindo impactos e reforçando o cumprimento da lei. Dessa forma, governança e compliance atuam tanto na prevenção quanto na correção, garantindo que a instituição esteja preparada para evitar e lidar com golpes dentro das exigências da LGPD.

- Descrever as medidas de segurança e boas práticas de prevenção, tanto no âmbito organizacional quanto no comportamento dos usuários.

As medidas organizacionais são fundamentais para estruturar o tratamento seguro de dados. São exemplos:

- A) Política de controle de acesso - onde cada pessoa acessa apenas os dados necessários para sua função. São providências simples, mas que reduzem significativamente o risco de exposição indevida.
- B) Criptografia, funciona como um “código secreto”, sendo útil, especialmente, em notebooks, celulares e e-mails.
- C) A anonimização elimina ou torna irreversível a identificação do titular, permitindo o uso das informações para fins estatísticos, analíticos ou científicos sem vínculo direto com a pessoa natural.
- D) Auditorias em registros de acesso: os logins e histórico de operações permitem identificar quem acessou o sistema, em que momento e com qual finalidade.

Se a organização estrutura as barreiras de proteção, o usuário precisa se resguardar também. Pois é nesse ponto que muitos incidentes acontecem: senhas fracas, compartilhamento de credenciais e cliques automáticos em links suspeitos são as causas mais frequentes de vazamento ou comprometimento de contas. Algumas ferramentas como senhas fortes, autenticação multifator e atenção a mensagens suspeitas são medidas básicas, mas essenciais de segurança.

O *phishing* é um exemplo típico de tática de invasão. O fraudador se passa por instituição confiável para induzir a vítima a fornecer dados, clicar em links ou

baixar arquivos maliciosos. A prevenção exige cautela, checagem da origem das mensagens e treinamento contínuo dos colaboradores.

A Autoridade Nacional de Proteção de Dados (ANPD), ao tratar da segurança da informação, reforça a relevância da conscientização e da adoção de práticas compatíveis com o porte e a realidade da organização. No trabalho remoto, a responsabilidade individual ganha ainda mais importância. Os equipamentos devem permanecer atualizados, protegidos por senha e, sempre que possível, com criptografia ativada. Também é recomendado evitar redes públicas sem proteção e bloquear a tela sempre que houver afastamento do computador. Essas atitudes simples, reduzem o risco de exposição de dados pessoais e corporativos.

A LGPD adota expressamente a lógica da prevenção, o que significa antecipar riscos e reduzir a probabilidade de dano. Nessa perspectiva, backups regulares, atualização de sistemas e segmentação de acessos são medidas indispensáveis para a continuidade dos serviços. O backup, em particular, é uma das ferramentas mais eficazes, pois possibilita a recuperação dos dados de forma rápida.

O Guia de Boas Práticas do Governo Federal e o Guia de Segurança da Informação da ANPD demonstram que a conformidade deve ser proporcional ao risco e ao porte da instituição. Isso significa que pequenas organizações não estão dispensadas da proteção, mas podem adotar soluções simples, efetivas e compatíveis com sua realidade operacional. Em resumo, a segurança de dados é um conjunto de medidas adotadas de forma contínua.

4. Justificativa

O crescimento dos golpes digitais no Brasil demonstra que a exposição indevida de dados pessoais representa não apenas violação à privacidade, mas também fator de risco para fraudes, prejuízos econômicos e danos à confiança nas relações digitais. Nesse cenário, a proteção de dados pessoais assume relevância jurídica, social e institucional.

A Lei Geral de Proteção de Dados estabelece dispositivos normativos para o tratamento adequado de dados pessoais e impõe às organizações deveres de segurança, transparência, responsabilidade e prestação de contas. Entretanto, a

efetividade desses comandos legais depende da incorporação de práticas internas de governança e compliance capazes de transformar exigências normativas em procedimentos concretos de prevenção, controle e resposta a riscos.

A relevância acadêmica da pesquisa decorre da necessidade de compreender a proteção de dados não apenas como obrigação legal, mas como componente de governança organizacional e de integridade institucional. Além disso, o estudo mostra-se pertinente para a disciplina de Governança e *Compliance*, ao evidenciar como estruturas de conformidade podem atuar na mitigação de riscos associados ao uso indevido de dados pessoais e à ocorrência de golpes digitais.

5. Referencial Teórico

A proteção de dados pessoais no Brasil encontra fundamento na Constituição da República Federativa de 1988, que assegura, em seu texto, direitos fundamentais como a privacidade, a intimidade e a inviolabilidade das comunicações. Nesse cenário, a proteção de dados surge como um desdobramento natural desses direitos, especialmente diante da crescente digitalização das relações sociais e econômicas. A necessidade de resguardar informações pessoais torna-se ainda mais evidente devido ao aumento de crimes cibernéticos, o que exige não apenas instrumentos legais, mas também mecanismos eficazes de governança e *compliance* nas organizações.

Nesse contexto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece regras claras sobre o tratamento de dados pessoais, impondo princípios como finalidade, necessidade, transparência e segurança. A legislação atribui responsabilidades às organizações quanto à coleta, armazenamento e compartilhamento de dados, exigindo a adoção de medidas técnicas e administrativas capazes de proteger essas informações contra acessos não autorizados e situações ilícitas. Assim, a LGPD se apresenta como um importante instrumento de prevenção a golpes digitais, ao estruturar práticas que reduzem vulnerabilidades e fortalecem a confiança nas relações digitais.

A relevância da proteção de dados se torna ainda mais evidente diante de casos concretos de uso indevido de informações pessoais. Notícia veiculada pela CNN Brasil relata a investigação de um casal na Bahia por envolvimento na venda

ilegal de dados sensíveis, evidenciando como a ausência de controles adequados pode facilitar práticas criminosas. Situações como essa demonstram que o tratamento inadequado de dados não apenas viola direitos fundamentais, mas também serve como base para a aplicação de golpes e fraudes, reforçando a necessidade de conformidade com a LGPD.

Além disso, o cenário nacional revela um crescimento significativo dos ataques digitais. Segundo reportagem da CNN Brasil, o país ocupou a sétima posição entre os maiores alvos de ataques cibernéticos em 2025, o que evidencia a amplitude do problema. De forma semelhante, o Valor Econômico destaca que os ataques digitais têm se intensificado, acendendo um alerta para empresas e cidadãos. Esse aumento expressivo reforça a importância da implementação de programas de governança e compliance que priorizem a proteção de dados como estratégia essencial de mitigação de riscos.

Os golpes virtuais também têm se diversificado e atingido públicos de todas as idades, conforme apontado por matéria do Senado Notícias. Essa realidade demonstra que a vulnerabilidade não está restrita a um grupo específico, exigindo uma abordagem ampla que envolva educação digital e conscientização. Nesse sentido, a Agência Nacional de Telecomunicações (ANATEL) ressalta, por meio de entrevista com o delegado Emmanoel David, titular da Delegacia de Estelionato de Curitiba e referência nacional no combate a crimes cibernéticos, estelionato e fraudes, que os golpes mais comuns exploram falhas humanas e tecnológicas, destacando a importância da informação e da prevenção como ferramentas fundamentais no combate a essas práticas.

No que se refere às formas de prevenção, é essencial que tanto indivíduos quanto organizações adotem medidas práticas de segurança, como a utilização de senhas fortes e autenticação em dois fatores, a verificação da autenticidade de links e mensagens recebidas, bem como a cautela no compartilhamento de dados pessoais. Ademais, a conscientização digital se mostra indispensável, uma vez que muitos golpes se baseiam em engenharia social. Caso o indivíduo seja vítima de um golpe, é fundamental agir rapidamente, registrando boletim de ocorrência, comunicando imediatamente a instituição financeira para bloqueio de possíveis transações indevidas e alterando senhas de contas comprometidas. Também é recomendável informar órgãos competentes e monitorar movimentações financeiras e cadastros em seu nome.

Outro aspecto relevante diz respeito à responsabilidade das organizações na implementação de programas efetivos de compliance voltados à proteção de dados. A adoção de políticas internas, treinamentos contínuos e mecanismos de monitoramento contribui para a criação de uma cultura organizacional pautada na segurança da informação. Além disso, tais práticas auxiliam na identificação precoce de riscos e na resposta rápida a incidentes, reduzindo significativamente os impactos de eventuais vazamentos de dados e dificultando a atuação de agentes mal-intencionados.

Nesse contexto, a proteção de dados pessoais, aliada a práticas eficazes de governança e *compliance*, mostra-se essencial para a prevenção de golpes digitais. A LGPD não apenas estabelece diretrizes legais, mas também incentiva uma cultura organizacional voltada à segurança da informação e à responsabilidade no tratamento de dados. Assim, a integração entre legislação, conscientização social e medidas organizacionais constitui um caminho indispensável para reduzir riscos, proteger os cidadãos e fortalecer a confiança no ambiente digital.

Para diagnosticar a percepção prática sobre o tema, realizou-se uma pesquisa de campo com 107 respondentes. O perfil demográfico revelou predomínio de pessoas entre 31 e 50 anos (68,2%), seguidas pelas faixas com mais de 50 anos (21,5%) e de 18 a 30 anos (8,4%). Quanto ao gênero, 60,7% identificaram-se como do sexo masculino e 39,3% como do sexo feminino. A amostra apresentou alto nível de instrução formal: 43% possuem Pós-Graduação/Especialização, 38,3% têm Ensino Superior e 10,3% alcançaram o Mestrado/Doutorado, enquanto apenas 8,4% concluíram o Ensino Médio.

Figura 1 - Faixa etária dos respondentes

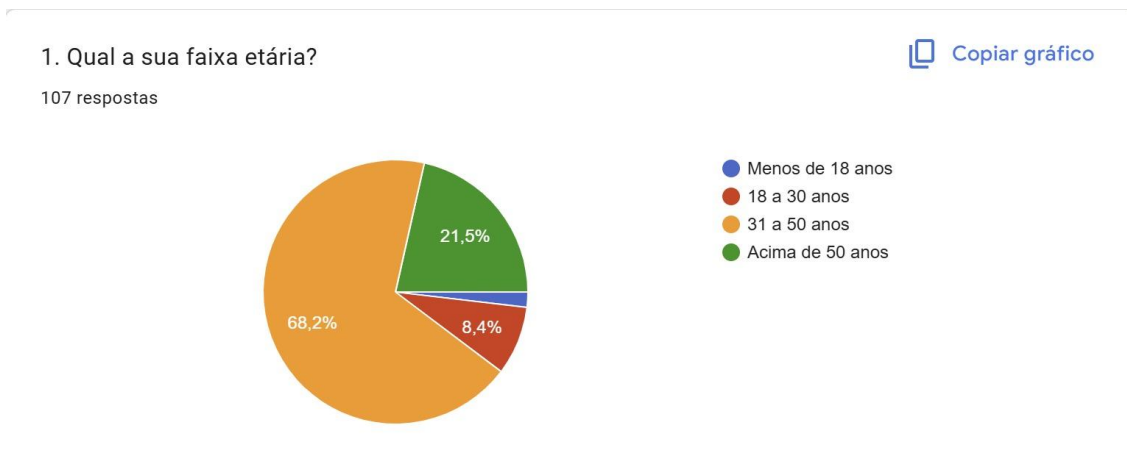


Figura 2 - Distribuição por gênero dos participantes

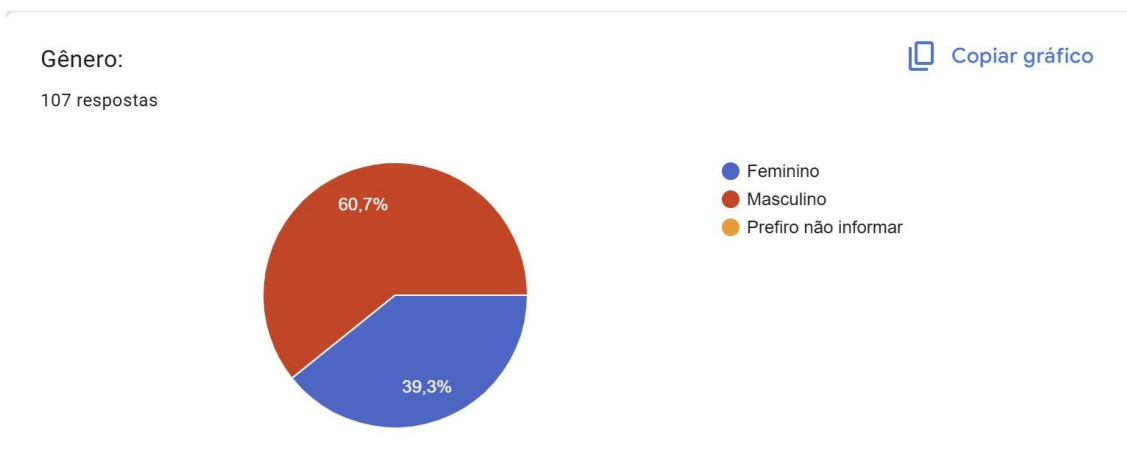
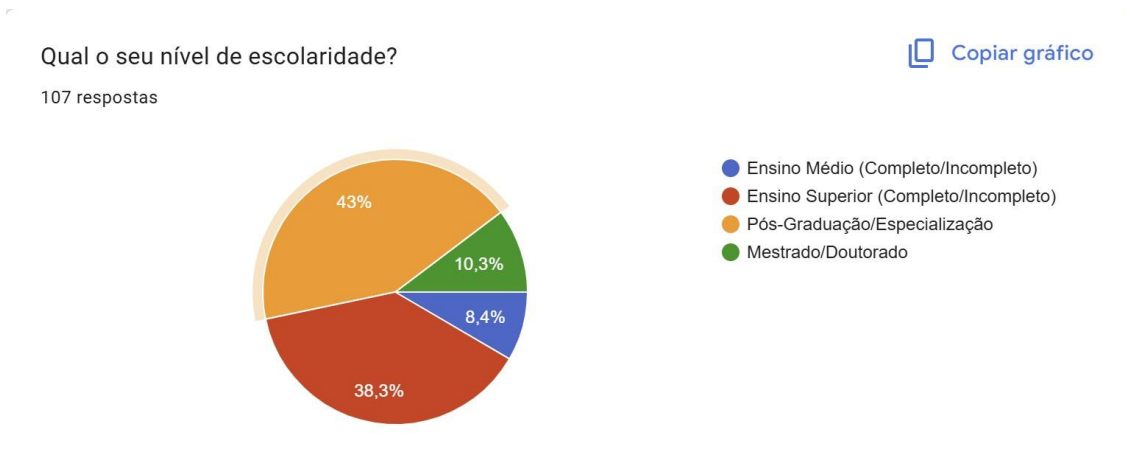


Figura 3 - Nível de escolaridade



No que se refere ao conhecimento sobre a LGPD, a maior parte dos entrevistados (57,9%) afirmou que apenas "ouviu falar" sobre a lei, mas não conhece seus detalhes; 32,7% declararam conhecer bem seus direitos e 9,3% não a conhecem. Esse cenário reflete-se na avaliação sobre a eficácia da norma no Brasil: apenas 9,3% a consideram "muito eficaz" para proteger a privacidade, enquanto 45,8% a veem como "parcialmente eficaz", 25,2% como "pouco eficaz/ineficaz" e 19,6% não souberam opinar.

Figura 4 - Nível de conhecimento sobre a LGPD

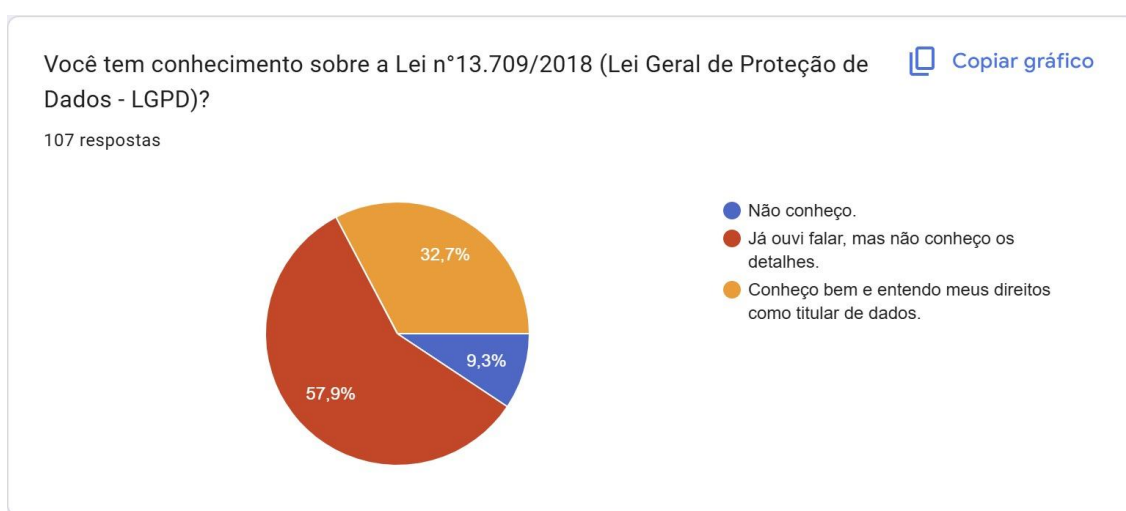


Figura 5 - Percepção sobre a eficácia da implementação da LGPD no Brasil



A urgência dessa discussão é evidenciada pela alta exposição a riscos digitais. Do total de participantes, 39,3% afirmaram já ter tomado ciência de que seus dados pessoais foram expostos em vazamentos — citando episódios como

vazamentos generalizados no INSS, invasões a bancos e exposição de e-mails corporativos. Como consequência direta, o assédio por contatos suspeitos (tentativas de golpe ou *phishing* via e-mail, SMS ou WhatsApp) é uma realidade rotineira: 60,4% recebem essas mensagens diariamente e 33% frequentemente (algumas vezes por semana).

Figura 6 - Ciência sobre exposição de dados pessoais em vazamentos

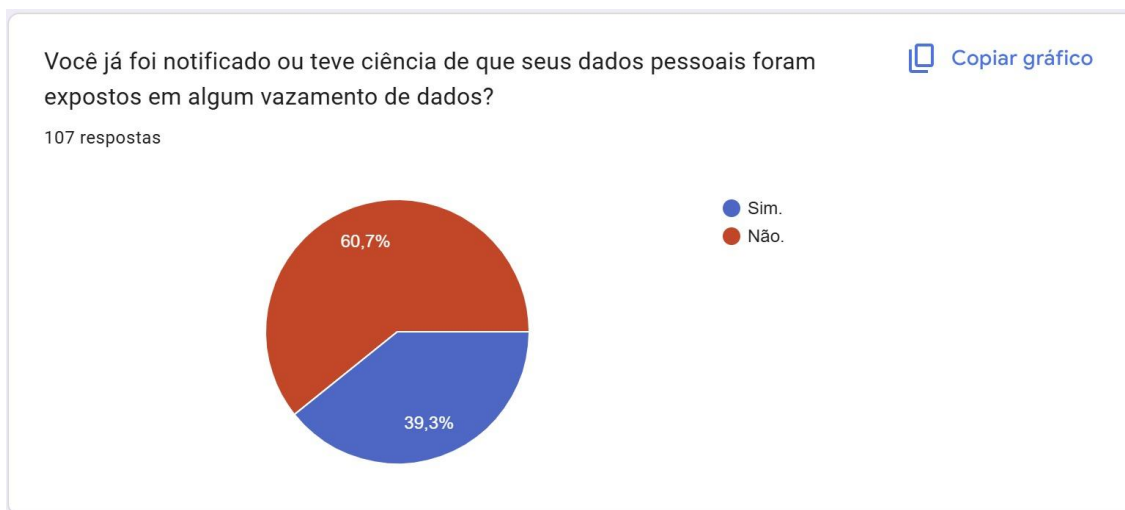
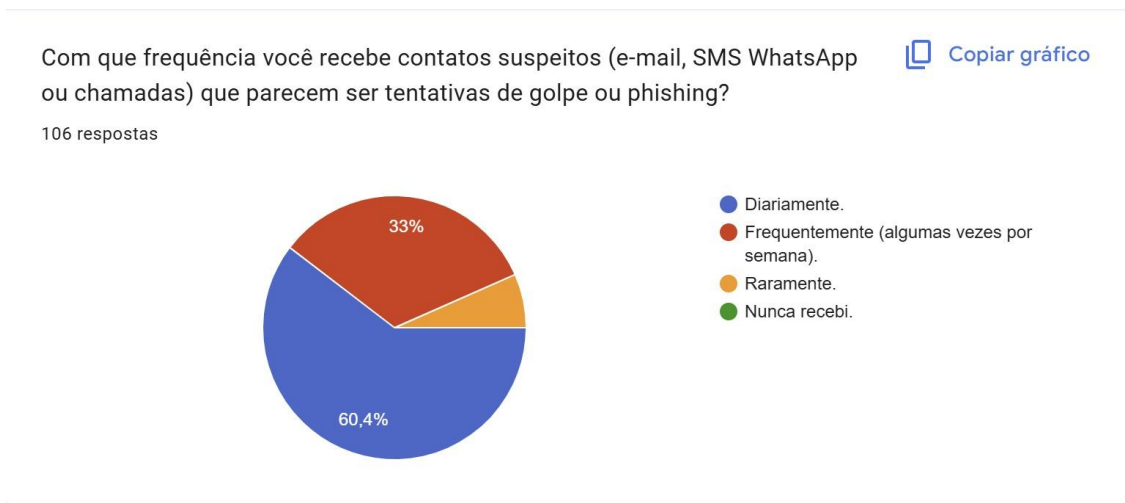


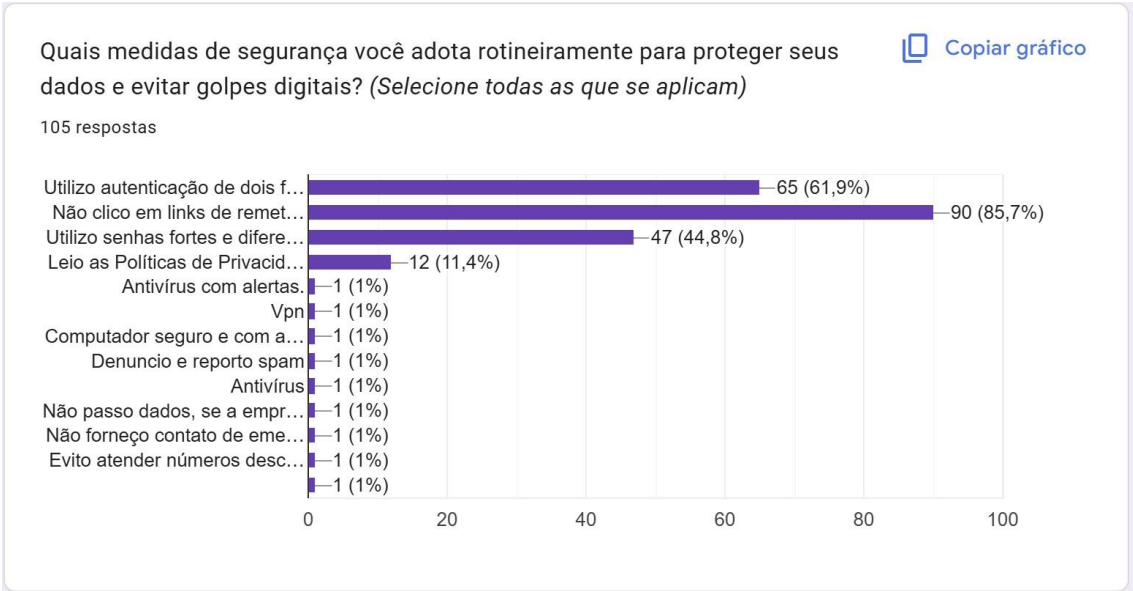
Figura 7 - Frequência de recebimento de contatos suspeitos ou tentativas de phishing



Por fim, a pesquisa mapeou as medidas de segurança adotadas pelos respondentes. As ações mais comuns são evitar clicar em links desconhecidos (85,7%) e utilizar a autenticação em dois fatores (61,9%). O uso de senhas fortes e exclusivas é praticado por 44,8%, enquanto o hábito de ler Políticas de Privacidade

foi mencionado por apenas 11,4%. Outras ferramentas, como antivírus e VPN, foram citadas de forma isolada (1% cada). Quanto às providências pós-vazamento, os relatos variaram entre a inércia por se tratar de incidentes generalizados, o monitoramento por softwares de segurança e a dependência de medidas tomadas pelas próprias instituições afetadas.

Figura 8 - Medidas de segurança adotadas rotineiramente pelos usuários



Quadro 1 - Relatos de providências tomadas após vazamentos de dados

Detalhes Adicionais

Poderia descrever brevemente o ocorrido e quais providências tomou?

37 respostas

Nenhuma providência

Fui informado pelo trabalho e eles mesmos tomaram as providências. Nao precisei fazer nada.

INSS - meus dados pessoais - divulgação para empresas de crédito. Não tomei providências porque o vazamento foi generalizado.

Tenho uma vpn q neste software há dispositivo para ver se já ocorreu vazamentos de dados. O programa acusou vazamento de email

Xx

Vi reportagem na tv que determinado banco no qual possuo conta sofreu invasão de hacker e possivelmente dados foram clonados e repassados a terceiros. Depois desse episódio recebi muitos telefones de golpes.

Exposição de dados do e-mail corporativo do EB. A Instruicao tomou as providências

Esses dados confirmam que a consolidação de uma cultura de proteção e conformidade com a LGPD ainda enfrenta grandes desafios práticos no país.

6. Metodologia

Foi trabalhada com dados primários e secundários. Os dados primários foram obtidos através de um formulário respondido por pessoas aleatórias e os dados secundários através de fontes de terceiros (dados disponibilizados por fontes idôneas na internet).

A metodologia adotada neste projeto será por abordagem qualitativa, buscando compreender, interpretar e analisar sobre a proteção de dados pessoais e a prevenção de golpes digitais.

Inicialmente, será realizada uma pesquisa exploratória sobre a legislação vigente, com ênfase na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como sobre conteúdos informativos relacionados ao aumento de fraudes digitais.

Foi aplicado um questionário por meio da plataforma Google Forms, com o objetivo de identificar o nível de conhecimento do público em geral acerca da LGPD, além de suas percepções sobre a segurança de dados e experiências com possíveis golpes digitais.

Por fim, desenvolvemos um podcast educativo, com a finalidade de promover a conscientização sobre a importância da proteção de dados pessoais e apresentar formas de prevenção e atuação diante de golpes digitais. Também serão coletadas evidências das atividades realizadas, que contribuirão para a elaboração do relatório final da prática extensionista.

7. Considerações finais

Por fim, ao analisar a proteção de dados pessoais como instrumento de prevenção a golpes digitais sob a perspectiva da governança e do compliance, torna-se evidente a urgência de implementar medidas de segurança e conformidade estruturadas na Lei Geral de Proteção de Dados (LGPD). Diante disso, o presente projeto alcançou plenamente seus objetivos ao correlacionar o tratamento inadequado de informações com a incidência de fraudes eletrônicas, demonstrando o papel estratégico dos mecanismos de governança no cenário brasileiro. O ponto marcante desta pesquisa foi o levantamento da realidade da população, que revelou tanto a vulnerabilidade dos usuários diante de tentativas frequentes de golpes quanto o desconhecimento generalizado sobre direitos digitais básicos. Como resposta prática a essa lacuna, o desenvolvimento do podcast educativo consolidou-se como uma ferramenta eficaz de extensão, ampliando o debate e promovendo a conscientização. Concluída esta etapa de fundamentação e análise teórica, este trabalho constitui uma base sólida para ações futuras. Sugere-se, portanto, a continuidade do projeto por meio do monitoramento da eficácia do compliance corporativo na redução de golpes cibernéticos, além da expansão de campanhas pedagógicas que democratizem o acesso à segurança da informação.

Assim, este estudo reafirma que a integração entre rigor legislativo, inovação tecnológica e educação digital é o caminho indispensável para assegurar a confiança e a cidadania no ecossistema virtual.

8. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

ATAQUES digitais disparam no Brasil e acendem alerta. **Valor Econômico**, [s. l.], 17 mar. 2026. Patrocinado, Dino. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2026/03/17/ataques-digitais-dispara-m-no-brasil-e-acendem-alerta-1.ghtml>. Acesso em: 08 abr. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD publica Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Brasília, DF: ANPD, 2021. Disponível em: <https://www.gov.br/anpd/>. Acesso em: 05 maio 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 abr. 2026.

BRASIL. [Lei nº 12.965, de 23 de abril de 2014]. **Marco Civil da Internet**: estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 maio 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, [2018]. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 abr. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Proteção de dados pessoais agora é um direito fundamental**. Brasília, DF: ANPD, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental>. Acesso em: 07 maio 2026.

BRASIL. Ministério Público Federal (MPF). **Fundamentos e Princípios**. Brasília, DF: MPF, [202-?]. Disponível em:

<https://www.mpf.mp.br/servicos/lcpd/o-que-e/fundamentos-e-principios-1>. Acesso em: 07 maio 2026.

BRASIL foi 7º maior alvo de ataques digitais em 2025; veja como se proteger. **CNN Brasil**, [s. l.], 23 mar. 2026. Tecnologia. Disponível em:

<https://www.cnnbrasil.com.br/tecnologia/brasil-foi-7o-maior-alvo-de-ataques-digitais-e-m-2025-veja-como-se-proteger/>. Acesso em: 08 abr. 2026.

CERT.BR. **Fascículo Golpes na Internet**: Cartilha de Segurança para Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em:

<https://cartilha.cert.br/>. Acesso em: 06 maio 2026.

CNN BRASIL. **Casal é investigado por venda ilegal de dados sensíveis na Bahia**. [S. l.]: CNN Brasil, 2026. Disponível em:

<https://www.cnnbrasil.com.br/nacional/nordeste/ba/casal-e-investigado-por-venda-ilegal-de-dados-sensiveis-na-bahia/>. Acesso em: 08 abr. 2026.

DELEGADO fala sobre os golpes mais comuns, desafios no combate e a importância da conscientização digital. **Agência Nacional de Telecomunicações**, Brasília, DF, 26 fev. 2026. Assuntos, Notícias. Disponível em:

<https://www.gov.br/anatel/pt-br/assuntos/noticias/delegado-fala-sobre-os-golpes-mais-comuns-desafios-no-combate-e-a-importancia-da-conscientizacao-digital>. Acesso em: 08 abr. 2026.

GOLPES virtuais aumentam e não fazem distinção de idade. **Senado Notícias**, Brasília, DF, 4 abr. 2025. Info Matérias. Disponível em: <https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade>. Acesso em: 08 abr. 2026.

LEGAL, ETHICS & COMPLIANCE (LEC). **Aplicações práticas da LGPD**. [S. l.]: LEC, 22 ago. 2024. Disponível em: <https://lec.com.br/aplicacoes-praticas-da-lgpd/>. Acesso em: 07 maio 2026.

LEGAL, ETHICS & COMPLIANCE (LEC). **Compliance e LGPD: qual a relação?** [S. l.]: LEC, 17 out. 2024. Disponível em: <https://lec.com.br/compliance-e-lgpd-qual-a-relacao/>. Acesso em: 07 maio 2026.

MENDONÇA, Maria Carolina. **A importância da governança corporativa e do compliance à LGPD**. Migalhas, 26 jan. 2022. Disponível em: <https://www.migalhas.com.br/depeso/358621/a-importancia-da-governanca-corporativa-e-do-compliance-a-lgpd>. Acesso em: 07 maio 2026.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.