Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i5.26486

O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO SOB A ÓTICA DA LGPD

THE HUMAN FACTOR IN INFORMATION SECURITY FROM THE PERSPECTIVE OF THE LGPD

EL FACTOR HUMANO EN LA SEGURIDAD DE LA INFORMACIÓN BAJO LA ÓPTICA DE LA LGPD

Antonio Coutinho Ferreira[1]

RESUMO: O presente artigo analisa a persistência do fator humano como a principal vulnerabilidade nas estruturas de segurança da informação, sob o prisma da Lei Geral de Proteção de Dados Pessoais (LGPD). Embora o arcabouço normativo brasileiro tenha estabelecido padrões rigorosos de conformidade e as soluções de segurança lógica tenham alcançado níveis elevados de sofisticação, a falibilidade comportamental dos agentes de tratamento permanece como o vetor crítico para a concretização de incidentes de segurança. A investigação dedica-se a examinar como a negligência, a imperícia e a vulnerabilidade a táticas de engenharia social comprometem a eficácia das barreiras sistêmicas, gerando riscos de responsabilidade civil objetiva e administrativa para as organizações. Por meio de uma revisão bibliográfica e análise de relatórios globais de incidentes, o estudo demonstra que a conformidade técnica é insuficiente se desvinculada de uma cultura de proteção de dados enraizada. Conclui-se que a educação corporativa contínua e a alfabetização digital não são apenas medidas acessórias, mas instrumentos jurídicos indispensáveis para a mitigação de danos e para a consolidação de uma governança de dados resiliente e pautada pelo dever de vigilância.

Palavras-chave: LGPD. Segurança da Informação. Governança de Dados.

ABSTRACT: This article analyzes the persistence of the human factor as the main vulnerability in information security structures, from the perspective of the Brazilian General Data Protection Law (LGPD). Although the Brazilian regulatory framework has established strict compliance standards and logical security solutions have reached high levels of sophistication, the behavioral fallibility of processing agents remains the critical vector for the materialization of security incidents. The investigation examines how negligence, malpractice, and vulnerability to social engineering tactics compromise the effectiveness of systemic barriers, generating risks of strict civil and administrative liability for organizations. Through a literature review and analysis of global incident reports, the study demonstrates that technical compliance is insufficient if detached from an ingrained data protection culture. It is concluded that continuous corporate education and digital literacy are not merely accessory measures, but indispensable legal instruments for mitigating damages and consolidating a resilient data governance based on the duty of vigilance.

Keywords: LGPD. Information Security. Data Governance.

[1] Mestrando em Segurança Pública, Cidadania e Direitos Humanos - Universidade do Estado do Amazonas (UEA).

RESUMEN: Este artículo analiza la persistencia del factor humano como la principal vulnerabilidad en las estructuras de seguridad de la información, bajo la óptica de la Ley General de Protección de Datos Personales (LGPD) de Brasil. Aunque el marco normativo brasileño ha establecido estándares rigurosos de cumplimiento y las soluciones de seguridad lógica han alcanzado niveles elevados de sofisticación, la falibilidad conductual de los agentes de tratamiento sigue siendo el vector crítico para la materialización de incidentes de seguridad. La investigación examina cómo la negligencia, la impericia y la vulnerabilidad a las tácticas de ingeniería social comprometen la eficacia de las barreras sistémicas, generando riesgos de responsabilidad civil objetiva y administrativa para las organizaciones. A través de una revisión bibliográfica y del análisis de informes globales de incidentes, el estudio demuestra que el cumplimiento técnico es insuficiente si está desvinculado de una cultura de protección de datos arraigada. Se concluye que la educación corporativa continua y la alfabetización digital no son meras medidas accesorias, sino instrumentos jurídicos indispensables para la mitigación de daños y para la consolidación de una gobernanza de datos resiliente y basada en el deber de vigilancia.

Palabras clave: LGPD. Redes Seguridad de la Información. Gobernanza de Datos.

INTRODUÇÃO

A segurança da informação na contemporaneidade transcende a mera implementação de barreiras tecnológicas, como firewalls e protocolos de criptografia simétrica. Com a promulgação e vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) Lei nº 13.709/2018, as organizações brasileiras foram compelidas a reestruturar seus modelos de governança para assegurar a autodeterminação informativa e a privacidade dos titulares. Entretanto, observa-se que o vultoso investimento em infraestrutura lógica e física não tem sido acompanhado, na mesma proporção, pela mitigação de riscos subjetivos. O fator humano permanece como o vetor de maior instabilidade nos sistemas de segurança, uma vez que a falibilidade comportamental, seja por negligência, imperícia ou desconhecimento, é capaz de neutralizar os mecanismos de defesa mais sofisticados do mercado cibernético.

Neste cenário, o "elo fraco" da corrente de proteção de dados não se encontra no código fonte, mas na interação do agente de tratamento com os ativos de informação. A exploração de vulnerabilidades humanas através da engenharia social e do phishing demonstra que o erro do colaborador é, muitas vezes, o catalisador de incidentes de segurança com repercussões jurídicas severas. Sob a ótica do Direito Digital, a ocorrência de um vazamento de dados decorrente de uma falha humana não é um evento isolado, mas o reflexo de uma lacuna na cultura de conformidade da instituição. A responsabilidade civil das empresas é acentuada pelo dever de vigilância e pela obrigação de implementar não apenas medidas técnicas, mas também medidas administrativas e educativas eficazes, conforme preceitua o Artigo 46 da LGPD.

O presente estudo propõe uma análise profunda sobre a necessidade de transposição do

foco puramente tecnológico para uma abordagem centrada no comportamento e na educação continuada. O rigor acadêmico desta pesquisa busca demonstrar que a efetividade da proteção de dados pessoais depende da consolidação de uma consciência coletiva dentro das organizações. Somente através de uma alfabetização digital robusta e de treinamentos que simulem a realidade dos riscos é possível transformar o agente de tratamento de uma vulnerabilidade potencial em uma barreira defensiva resiliente. Assim, a investigação aqui delineada justifica-se pela urgência em compreender como a gestão do fator humano pode assegurar a sustentabilidade jurídica e a integridade sistêmica das operações de tratamento de dados na era da informação.

MÉTODOS

A presente investigação científica pauta-se pelo método dedutivo, partindo da análise das diretrizes gerais estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) para a compreensão de fenômenos específicos de vulnerabilidade no tratamento de dados. A pesquisa caracteriza-se como qualitativa e de natureza básica, buscando o aprimoramento do conhecimento acerca da responsabilidade civil e administrativa das organizações frente ao erro humano. Quanto aos objetivos, o estudo assume um caráter exploratório e descritivo, uma vez que se propõe a detalhar as interações entre o comportamento do agente de tratamento e a eficácia das barreiras tecnológicas de proteção de dados.

O procedimento adotado fundamenta-se em uma rigorosa revisão bibliográfica e documental. A base teórica é constituída pelo exame da legislação nacional vigente, com ênfase na Lei nº 13.709/2018, e nas orientações expedidas pela Autoridade Nacional de Proteção de Dados (ANPD). Complementarmente, foram consultadas obras doutrinárias de referência no campo do Direito Digital e da Responsabilidade Civil, bem como periódicos científicos e artigos especializados que discutem a dogmática da segurança da informação. A fundamentação fática da pesquisa é sustentada pela análise de dados secundários extraídos de relatórios globais de incidentes cibernéticos e estudos de caso de renome internacional, o que permite confrontar a norma jurídica com a realidade estatística das violações de dados.

O percurso metodológico foi estruturado de forma a garantir a coesão lógica entre a problemática apresentada e os resultados obtidos. Inicialmente, procedeu-se ao levantamento do arcabouço normativo para identificar os deveres de vigilância impostos aos agentes de tratamento. Em seguida, realizou-se a intersecção desses dados com a literatura técnica sobre

engenharia social e falibilidade humana, permitindo uma análise interdisciplinar do objeto de estudo. Por fim, a síntese das informações coletadas proporcionou a sustentação teórica necessária para defender a tese de que a educação continuada e a cultura de proteção de dados são requisitos indispensáveis para o cumprimento do princípio da segurança e da prevenção, conforme preconizado pelo ordenamento jurídico brasileiro.

RESULTADOS

A extração de dados concernentes à materialização de vulnerabilidades cibernéticas quantificou a incidência direta do fator humano nos incidentes de segurança. O levantamento estatístico proveniente do Verizon Data Breach Investigations Report 2024 registrou a participação de usuários em 68% do volume global de violações, índice com projeção preliminar de estabilização na faixa de 60% para o exercício de 2025. A desagregação setorial das métricas isolou o segmento industrial, no qual falhas comportamentais internas compuseram a causa raiz de 27% das ocorrências documentadas no ano de 2024. No tocante à tipologia dos vetores de entrada, táticas de engenharia social ancoradas em phishing deflagraram entre 80% e 95% das intrusões dependentes de interação humana, registrando-se a incorporação tática de ferramentas de Inteligência Artificial pelos atacantes para a otimização dessas abordagens.

O escrutínio do impacto pecuniário atrelado às violações de privacidade, fundamentado no relatório IBM Cost of a Data Breach 2024, apurou um custo médio global de USD 4,88 milhões por evento cibernético. O mesmo instrumento de coleta evidenciou a correlação entre medidas administrativas preventivas e a atenuação de danos: entes corporativos dotados de programas estruturados de educação em segurança registraram uma retração média de USD 1,4 milhão nesses dispêndios, em comparação a instituições desprovidas de tais salvaguardas.

Sob a perspectiva do controle regulatório, a análise das resoluções da Autoridade Nacional de Proteção de Dados (ANPD) atestou a utilização da prova de aplicação de programas de conformidade e treinamento como critério material e objetivo na dosimetria de sanções. O arcabouço sancionatório mapeado restringe a imposição de multas ao teto de 2% do faturamento da entidade autuada. Por fim, a revisão bibliográfica atinente à governança informacional delimitou um interstício de três a cinco anos como o marco temporal exigido para a transição e consolidação empírica de uma cultura de proteção de dados no ambiente corporativo.

DISCUSSÃO

1. O FATOR HUMANO COMO VETOR CRÍTICO NA SEGURANÇA DE DADOS SOB A LGPD

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil estabeleceu um novo paradigma de responsabilidade civil e administrativa para as organizações, exigindo que o tratamento de dados pessoais seja pautado pelos princípios da segurança, da prevenção e da prestação de contas. No entanto, a eficácia das medidas técnicas previstas no Artigo 46 da referida Lei é frequentemente neutralizada pela falibilidade inerente ao comportamento humano. O agente de tratamento, ao operar sistemas e manipular fluxos de informação, posiciona-se como o componente de maior imprevisibilidade no ecossistema digital. Dados consolidados em relatórios globais de segurança cibernética indicam que a vasta maioria das violações de dados não decorre de falhas estruturais nos algoritmos de criptografia ou vulnerabilidades de software conhecidas como zero-day, mas sim de lapsos comportamentais, negligência ou execução inadequada de protocolos internos pelos colaboradores.

No cenário jurídico-administrativo, o "erro humano" não deve ser interpretado apenas como um acidente fortuito, mas como uma falha na gestão de riscos que a instituição tem o dever legal de mitigar. O comportamento inseguro de um preposto seja ao utilizar credenciais frágeis, ao negligenciar a autenticação de múltiplos fatores ou ao ser vítima de táticas de engenharia social materializa um risco que a legislação brasileira busca coibir. Sob a ótica da LGPD, a segurança da informação é uma obrigação de meio que exige diligência constante. Quando um colaborador ignora diretrizes institucionais por excesso de confiança ou pressão laboral, ele cria uma brecha que permite o acesso indevido por terceiros, comprometendo a integridade, a disponibilidade e a confidencialidade dos dados dos titulares.

Além disso, é imperativo destacar que os criminosos cibernéticos têm refinado suas táticas de intrusão para explorar gatilhos psicológicos e heurísticas de decisão humanas, em vez de tentarem romper barreiras puramente tecnológicas. Ataques de phishing e spear-phishing são desenhados para induzir o indivíduo ao erro através da urgência, do medo ou do respeito à autoridade, tornando o usuário final o alvo primário das ofensivas. Portanto, a análise do fator humano como vetor crítico revela que a conformidade legal exige uma transição da segurança puramente passiva para uma governança ativa. A vulnerabilidade comportamental do agente de tratamento só pode ser reduzida quando a organização assume que a proteção de dados

depende de uma vigilância cognitiva compartilhada, onde o conhecimento dos riscos jurídicos e técnicos é disseminado em todos os níveis hierárquicos, transformando o elo mais fraco em um componente consciente da defesa institucional.

1.1 A engenharia social e a fragilidade psicológica

A segurança da informação, sob o prisma da proteção de dados pessoais, não deve ser compreendida como um produto tecnológico estático, mas como um processo dinâmico e contínuo de gestão de riscos. A engenharia social representa a faceta mais complexa do erro humano, pois não se trata de uma falha acidental ou sistêmica, mas de uma manipulação deliberada e sofisticada do comportamento do indivíduo para a obtenção de vantagens ilícitas. Criminosos cibernéticos exploram sistematicamente gatilhos mentais e heurísticas de decisão para contornar protocolos de segurança que seriam tecnicamente intransponíveis. Ao focar na vulnerabilidade psicológica do agente de tratamento, o atacante consegue neutralizar camadas de criptografia e firewalls, transformando o colaborador em um vetor involuntário de intrusão e vazamento de dados.

A eficácia dessas abordagens reside na exploração de tendências comportamentais inerentes à condição humana, tais como a urgência, o medo, a curiosidade e a obediência à autoridade. Em um ambiente corporativo ou administrativo, a pressão por resultados e o cumprimento de metas podem induzir o agente a ignorar protocolos de verificação em favor da celeridade, materializando o risco subjetivo da segurança. O atacante utiliza princípios de persuasão para coagir o subordinado ao descumprimento de normas, muitas vezes emulando a identidade de gestores ou autoridades institucionais. Essa quebra de protocolo, motivada por uma percepção distorcida da realidade, demonstra que a fragilidade psicológica é capaz de anular o investimento em infraestrutura tecnológica se não houver um preparo cognitivo correspondente por parte do usuário.

Nesse contexto, a alfabetização digital e o treinamento de conscientização emergem como ferramentas jurídicas e administrativas indispensáveis para a mitigação de ataques baseados em manipulação psicológica. Um agente de tratamento devidamente capacitado desenvolve a resiliência necessária para identificar inconsistências em comunicações oficiais e resistir a gatilhos de urgência que fogem ao padrão institucional. A negligência resultante de um ataque bem-sucedido de engenharia social compromete a integridade da organização e a privacidade dos titulares, configurando uma falha no dever de vigilância. Portanto, a consolidação de uma cultura de segurança robusta exige que as organizações transponham a

visão tecnicista e invistam na compreensão dos fatores psicossociais que influenciam a tomada de decisão, garantindo que o colaborador atue como uma sentinela ativa na proteção dos dados pessoais.

1.2 Dados reais de mercado (2024-2025)

A análise estatística dos incidentes de segurança no biênio 2024-2025 revela que a tecnologia, embora essencial, não é autossuficiente na contenção de ameaças que exploram a falibilidade comportamental. Segundo o relatório IBM Cost of a Data Breach 2024, o custo médio global de uma violação de dados atingiu a marca histórica de USD 4,88 milhões, representando uma elevação significativa em relação aos anos anteriores. Esse aumento reflete não apenas a sofisticação dos ataques, mas a complexidade na identificação e contenção de brechas originadas por erros internos. Em setores altamente regulados, como o industrial e o financeiro, os custos são ainda mais alarmantes, sendo que, no setor industrial, o erro humano foi identificado como a causa raiz em aproximadamente 27% dos incidentes registrados em 2024.

A persistência do "fator humano" como catalisador de riscos é corroborada pelo Verizon Data Breach Investigations Report 2024, que aponta que o elemento humano esteve presente em 68% de todas as violações de dados analisadas globalmente. Projeções e dados preliminares de 2025 indicam uma estabilização dessa métrica em patamares elevados, oscilando em torno de 60%, evidenciando que, mesmo com o advento de ferramentas de Inteligência Artificial para defesa, os atacantes têm utilizado essas mesmas tecnologias para aprimorar técnicas de phishing e roubo de credenciais. Estima-se que ataques de phishing sejam responsáveis por iniciar entre 80% e 95% de todas as brechas associadas à interação humana, demonstrando a eficácia contínua das táticas de manipulação psicológica no ambiente corporativo.

No contexto brasileiro, a Autoridade Nacional de Proteção de Dados (ANPD) tem intensificado a fiscalização, elevando o rigor das sanções para organizações que falham em demonstrar o dever de vigilância. A existência de programas de conscientização e treinamento em segurança passou a ser considerada um fator fundamental para a dosimetria das penas, servindo como evidência de boa-fé e adoção de políticas de boas práticas. Organizações que investem em capacitação contínua chegam a reduzir o custo de uma violação em média USD 1,4 milhão em comparação àquelas que negligenciam o treinamento do usuário final. Assim, os dados demonstram que a educação digital não é um gasto acessório, mas um investimento estratégico indispensável para a mitigação de prejuízos financeiros e a preservação da reputação institucional perante o órgão regulador.

2. A RESPONSABILIDADE CIVIL E A CULPABILIDADE ORGANIZACIONAL FRENTE AO ERRO HUMANO

A estruturação da Lei Geral de Proteção de Dados Pessoais (LGPD) não se limita a estabelecer normas de conduta ética; ela institui um rigoroso sistema de responsabilidade civil para os agentes de tratamento, sejam eles controladores ou operadores. No ordenamento jurídico brasileiro, o erro humano, ainda que destituído de dolo ou intenção de dano por parte do colaborador, não exime a instituição de sua responsabilidade perante o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A falha cometida por um preposto é absorvida pela responsabilidade da organização, uma vez que esta detém o bônus da atividade econômica ou administrativa e, consequentemente, deve arcar com o ônus dos riscos gerados por suas operações de tratamento.

Sob a ótica do Direito Civil contemporâneo e das especificidades da LGPD, a ocorrência de um incidente de segurança originado por erro humano é frequentemente interpretada como uma falha na implementação de medidas administrativas aptas a proteger os dados pessoais. A doutrina caracteriza essa situação através da culpa in vigilando e da negligência institucional, onde a falta de padronização e de rigor na execução de processos internos define a linha entre o acidente fortuito e a omissão culpável. Quando uma organização negligencia a instrução de seus agentes, ela assume o risco pelos danos decorrentes dessa inobservância, tornando-se diretamente responsável pela vulnerabilidade que o indivíduo representa no fluxo informacional.

Para a mitigação de sanções administrativas que podem atingir patamares severos de até 2% do faturamento é imperativo que a empresa demonstre de forma inequívoca que o erro humano ocorreu a despeito da existência de protocolos robustos e programas de conformidade efetivos. A ANPD sinaliza que a adoção de políticas de boas práticas e governança é um dos critérios fundamentais para a dosimetria das penas e a verificação da boa-fé objetiva da instituição. Portanto, o nexo de causalidade entre a falha do agente e o dano ao titular pode ter sua culpabilidade mitigada se a organização comprovar que agiu com o rigor necessário na seleção (culpa in eligendo) e na supervisão constante de seus colaboradores.

Diferente de modelos de segurança puramente tecnológicos, a LGPD exige o princípio da responsabilização e prestação de contas, conhecido como accountability. Isso implica que não basta a conformidade formal com a lei; é necessário que a instituição seja capaz de produzir provas dinâmicas de sua diligência. Documentar que os colaboradores passaram por

treinamentos de conscientização e que a cultura de privacidade é auditada regularmente constitui a principal defesa jurídica contra alegações de omissão institucional. Dessa forma, a segurança efetiva é atestada pela demonstração do compromisso da gestão com a educação contínua, transformando o registro de treinamentos em um instrumento de prova essencial para a sustentação da tese de autoria segura e diligência organizacional.

2.1 A culpa in vigilando e a negligência institucional

No ordenamento jurídico brasileiro, a responsabilidade das organizações pelos atos de seus subordinados é pautada pelo dever de vigilância, um conceito que ganha contornos específicos sob a égide da Lei Geral de Proteção de Dados Pessoais. A ocorrência de um incidente de segurança originado por erro humano é frequentemente interpretada como uma falha direta na implementação de medidas administrativas aptas a proteger os dados pessoais, conforme exigido pela legislação vigente. A configuração da culpa in vigilando ocorre quando a instituição, detentora do controle sobre os processos de tratamento, falha em fiscalizar adequadamente a conduta de seus colaboradores, permitindo que a inobservância de normas técnicas resulte em danos aos titulares dos dados.

A linha que separa o acidente fortuito da negligência institucional é definida pelo rigor e pelo critério aplicados na execução dos processos organizacionais. Conforme a doutrina jurídica e os manuais de conduta técnica, a ausência de padronização e de protocolos claros de atuação é o que caracteriza a negligência das organizações no tratamento de informações sensíveis. Sob a ótica da LGPD, não se admite que a empresa alegue desconhecimento ou erro individual do funcionário como excludente de responsabilidade, uma vez que cabe ao controlador estabelecer as diretrizes de segurança e garantir que estas sejam rigorosamente seguidas. A falha no monitoramento contínuo das atividades de tratamento demonstra uma omissão no dever de cuidado, expondo a instituição a sanções severas.

Dessa forma, a negligência institucional manifesta-se na falta de investimento em mecanismos de controle e na ausência de uma estrutura de governança que previna o erro antes de sua ocorrência. Se uma organização não fornece as ferramentas necessárias nem o treinamento adequado, ela assume o risco inerente à atividade, configurando a culpa in eligendo e in vigilando ao tornar-se diretamente responsável pela vulnerabilidade que o colaborador representa. Portanto, a mitigação da culpa organizacional exige a demonstração de um esforço concentrado e documentado na vigilância das operações, assegurando que o tratamento de dados pessoais ocorra dentro de um ambiente de conformidade técnica e jurídica inquestionável.

2.2 Nexo de causalidade e medidas de mitigação

A configuração da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados Pessoais exige a demonstração inequívoca do nexo de causalidade, ou seja, o liame lógico e jurídico entre a falha na conduta do agente de tratamento e o dano efetivo causado ao titular dos dados. No contexto do erro humano, o nexo de causalidade estabelece-se quando a inobservância de protocolos de segurança por parte de um colaborador atua como a causa direta ou determinante para uma violação de privacidade ou vazamento de informações. Todavia, para que a organização possa mitigar sanções administrativas — que podem atingir a cifra de até 2% do faturamento — é imperativo demonstrar que o incidente ocorreu a despeito da existência de protocolos robustos e que não houve omissão institucional na gestão de riscos.

A Autoridade Nacional de Proteção de Dados (ANPD) enfatiza que a adoção de políticas de boas práticas e governança é um dos critérios fundamentais para a dosimetria das penas e para a avaliação do esforço concentrado da organização em evitar o incidente. Nesse sentido, as medidas de mitigação devem ser comprovadas mediante a existência de planos de resposta a incidentes e, principalmente, através da evidência de que a instituição agiu com rigor e critério no tratamento dos dados antes da ocorrência da falha. O uso de normas institucionalizadas e a aplicação de salvaguardas administrativas atuam como prova de diligência perante o órgão regulador, permitindo que o nexo de causalidade seja analisado sob a ótica do "risco permitido" e da "boa-fé" organizacional.

Dessa forma, a prevenção técnica e a documentação constante tornam-se ferramentas de defesa jurídica essenciais. A precisão nos processos de tratamento de informações e a manutenção de registros de conformidade demonstram o compromisso da instituição com a transparência e a segurança efetiva. Se uma organização comprova que forneceu as ferramentas necessárias, implementou barreiras sistêmicas e capacitou seus prepostos, ela possui subsídios para sustentar que agiu de forma zelosa, buscando romper ou atenuar o nexo de causalidade que a vincularia à negligência institucional pura. Assim, a mitigação não é apenas uma estratégia de redução de danos financeiros, mas a certificação de que a governança de dados é tratada com o rigor acadêmico e técnico exigido pela complexidade do cenário contemporâneo.

2.3 O princípio da responsabilização e prestação de contas (accountability)

Diferente de modelos de segurança puramente tecnológicos ou passivos, a Lei Geral de Proteção de Dados Pessoais introduz o princípio da responsabilização e prestação de contas,

amplamente conhecido na doutrina como accountability. Este princípio estabelece que não é suficiente que os agentes de tratamento declarem estar em conformidade com as normas de proteção de dados; é imperativo que sejam capazes de demonstrar, por meio de evidências concretas e auditáveis, a eficácia das medidas adotadas. No contexto do erro humano, o accountability exige que a organização comprove que tomou todas as precauções administrativas e educativas necessárias para evitar que o comportamento do colaborador se tornasse um vetor de vulnerabilidade.

A prestação de contas manifesta-se como um dever de transparência ativa perante os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Sob essa ótica, a documentação de treinamentos de conscientização, a realização de testes de vulnerabilidade comportamental e a manutenção de registros de acesso não são meras formalidades burocráticas, mas sim a principal defesa jurídica contra a alegação de omissão institucional. A segurança efetiva, portanto, é atestada a posteriori, uma vez que o rigor educacional aplicado aos colaboradores serve como lastro para comprovar que a instituição agiu com a diligência esperada, mesmo na ocorrência de um incidente.

Além disso, o princípio da responsabilização obriga as organizações a manterem uma postura proativa na gestão de riscos. A precisão nos processos de tratamento de informações e a clareza nas comunicações oficiais constituem a prevenção técnica fundamental para impedir que falhas críticas ocorram por simples desconhecimento. Ao investir na transformação do comportamento humano em uma barreira defensiva resiliente, a organização atende ao critério de boa-fé exigido pela ANPD, qualificando seu ambiente de governança e garantindo a sustentabilidade das operações de dados no cenário contemporâneo.

3. ESTRATÉGIAS DE TREINAMENTO E CONSOLIDAÇÃO DA CULTURA DE SEGURANÇA

A mitigação do erro humano sob a égide da Lei Geral de Proteção de Dados Pessoais exige que a capacitação corporativa transcenda a condição de mero requisito burocrático, consolidando-se como um processo educacional contínuo. O investimento massivo em infraestrutura tecnológica revela-se inócuo se o colaborador não internalizar seu papel como agente ativo na defesa digital. A governança de dados contemporânea preconiza metodologias de aprendizagem integradas à rotina laboral, como simulações de ataques em tempo real. A execução de testes controlados de phishing, por exemplo, converte a falha eventual em uma

oportunidade de correção comportamental imediata, aumentando significativamente a retenção cognitiva e a vigilância diária.

Para reverter a estatística em que a falibilidade humana protagoniza as violações de dados, as organizações devem evoluir do foco exclusivo no compliance formal para uma cultura de segurança integrada. Nesse estágio de maturidade, a proteção informacional deixa de ser uma imposição externa e torna-se um valor intrínseco, onde todos os prepostos atuam proativamente como sensores de risco. A consolidação dessa cultura preventiva deve ser pautada em indicadores de eficácia, como a redução dos custos de mitigação de incidentes e o aumento substancial na taxa de reporte prévio de ameaças. O incremento na capacidade dos colaboradores de identificar comunicações suspeitas atesta a ativação da rede humana de defesa, consubstanciando a prova jurídica de diligência da instituição perante a Autoridade Nacional de Proteção de Dados.

3.1 Metodologias de aprendizagem e engajamento

A efetividade da capacitação corporativa, sob a ótica da governança de dados, requer a adoção de metodologias de aprendizagem ativas que superem a ineficiência histórica de exposições puramente teóricas. A doutrina de conformidade digital orienta a substituição de treinamentos exaustivos por abordagens contínuas e engajadoras, como o uso de microlições (microlearning) e técnicas de gamificação, que garantem a assimilação de conceitos críticos de segurança sem comprometer a produtividade laboral. Adicionalmente, a execução de testes práticos no ambiente de trabalho, a exemplo das simulações de phishing em tempo real, revela-se uma estratégia indispensável para materializar o risco cibernético abstrato no cotidiano do agente de tratamento. Essas metodologias interativas não apenas reforçam condutas seguras no exato momento da tomada de decisão, convertendo a falha técnica em aprendizado imediato, mas também produzem os registros e métricas comprobatórias necessários para atestar a diligência institucional e a boa-fé da organização perante a Autoridade Nacional de Proteção de Dados (ANPD).

3.2 Do compliance à maturidade cultural

A transição do compliance formal para a maturidade cultural representa o estágio mais elevado da governança de dados, onde a proteção da privacidade deixa de ser uma obrigação jurídica externa para se tornar um valor intrínseco à identidade da organização. No estágio

inicial, o foco reside estritamente na conformidade normativa, em que os treinamentos e protocolos são implementados apenas para atender aos requisitos legais da LGPD ou às exigências de auditoria, resultando numa proteção superficial e reativa. Para que a segurança seja efetiva, a instituição deve percorrer um caminho de mudança de comportamento que, segundo relatórios globais de segurança, pode levar de três a cinco anos para se consolidar. Este processo exige a repetição constante de diretrizes e a influência sobre hábitos específicos, transformando a conduta passiva do colaborador numa postura vigilante e consciente.

A maturidade cultural é alcançada quando a segurança da informação é integrada na cultura organizacional, fazendo com que todos os agentes de tratamento, independentemente do nível hierárquico, actuem como "sensores de risco" no ecossistema digital. Nesse patamar, o indivíduo compreende as consequências jurídicas e éticas das suas acções, sendo capaz de identificar vulnerabilidades que, muitas vezes, passam despercebidas por sistemas automatizados. Esta evolução mitiga significativamente o risco subjetivo, uma vez que a protecção de dados passa a ser uma responsabilidade partilhada e não apenas uma atribuição do departamento de tecnologia ou do encarregado de dados (DPO). Assim, a consolidação de uma cultura de segurança robusta garante que a conformidade com a LGPD seja sustentável a longo prazo, protegendo a reputação institucional e assegurando a integridade dos direitos dos titulares perante a falibilidade humana.

3.3 Indicadores de eficácia e retorno sobre investimento

A eficácia dos programas de capacitação e conscientização corporativa não pode ser meramente presumida; ela deve ser objetivamente mensurada por meio de indicadores de desempenho que comprovem a evolução da maturidade institucional. Sob a perspectiva da governança de dados e do princípio da prestação de contas (accountability), a adoção de métricas tangíveis é o mecanismo primário pelo qual a organização atesta a sua diligência e boa-fé perante a Autoridade Nacional de Proteção de Dados (ANPD). O retorno sobre o investimento em educação digital transcende a clássica análise financeira, configurando-se como uma estratégia jurídica basilar para a mitigação de danos e sanções. Dados empíricos de relatórios globais de segurança demonstram que organizações detentoras de programas maduros conseguem reduzir o impacto financeiro de uma violação cibernética em cifras que chegam a 1,4 milhão de dólares, evidenciando de forma inconteste que a prevenção ativa é econômica e juridicamente mais viável do que a reparação civil.

Ademais, a mensuração do comportamento do agente de tratamento fornece os elementos probatórios necessários para a defesa administrativa da organização. Indicadores operacionais, como o incremento substancial na taxa de reporte voluntário de incidentes e de e-mails suspeitos (antes de qualquer interação nociva), atestam que a "rede de sensores humanos" foi ativada com sucesso. Esse comportamento proativo comprova a transição de uma postura corporativa reativa para uma cultura preventiva sólida. Ao demonstrar que o colaborador é capaz de identificar e neutralizar a ameaça na ponta da operação, a empresa afasta a presunção de negligência ou de culpa in vigilando, qualificando o seu ambiente de tratamento de dados e robustecendo o nexo de causalidade a favor da lisura e do compromisso institucional com a privacidade dos titulares.

CONCLUSÃO

A investigação desenvolvida ao longo deste artigo permite concluir que a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no cenário brasileiro, embora tenha estabelecido um marco regulatório robusto e exigido avanços tecnológicos significativos, encontra no fator humano o seu desafio mais persistente e complexo. A análise evidenciou que a tecnologia, isoladamente, é incapaz de neutralizar riscos que emergem da subjetividade e do comportamento dos agentes de tratamento. O erro humano, longe de ser um evento meramente fortuito ou escusável, manifesta-se como um sintoma direto da carência de uma cultura organizacional que priorize a educação digital e a compreensão profunda das responsabilidades individuais no ecossistema de dados.

Sob a ótica da responsabilidade civil e administrativa, demonstrou-se que a falibilidade humana é frequentemente potencializada pelo desconhecimento técnico e pela vulnerabilidade psicológica explorada por técnicas de engenharia social. Nesse contexto, a conformidade institucional não deve ser interpretada como um estado estático de adequação jurídica formal, mas como um processo dinâmico de gestão de riscos. A negligência na capacitação dos colaboradores configura omissão no dever de cuidado e caracteriza a culpa in vigilando, atraindo para a organização o ônus integral pelas violações de privacidade perpetradas em suas operações. Em contrapartida, a aplicação do princípio da prestação de contas (accountability) exige que a instituição produza provas materiais de sua diligência, sendo o treinamento contínuo a principal salvaguarda para atenuar o nexo de causalidade e mitigar sanções perante a Autoridade Nacional de Proteção de Dados (ANPD).

Por fim, depreende-se que a proteção efetiva de dados é uma obra coletiva e multidisciplinar. Para que a inovação tecnológica e o direito fundamental à privacidade coexistam de forma segura, as organizações devem transpor a visão limitada do cumprimento burocrático e investir na transformação do comportamento humano. A governança de dados contemporânea exige que o agente de tratamento deixe de ser o "elo mais fraco" para se tornar uma barreira defensiva ativa e resiliente. A consolidação de uma cultura de segurança integrada, pautada na vigilância constante e na educação corporativa, é o único caminho juridicamente sustentável para assegurar a integridade das informações e garantir a efetividade plena dos preceitos estabelecidos pela LGPD.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (BRASIL). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento-final.pdf. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 abr. 2026.

IBM SECURITY. Cost of a data breach report 2024. [S. l.]: IBM Corporation, 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 19 abr. 2026.

SANS INSTITUTE. SANS 2024 security awareness report: managing the human risk. North Bethesda: SANS, 2024. Disponível em: https://www.sans.org/white-papers/. Acesso em: 19 abr. 2026.

VERIZON. 2024 data breach investigations report. [S. l.]: Verizon Business, 2024. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 19 abr. 2026.