Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Larissa Bechedorf Silva Telles

TRATAMENTO DE DADOS PESSOAIS EM MICROEMPRESAS

Americana, SP

2025

Larissa Bechedorf Silva Telles

TRATAMENTO DE DADOS PESSOAIS EM MICROEMPRESAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança da Informação.

Orientador(a): Prof.(a) Dra. Maria Cristina Aranda

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Larissa Bechedorf Silva Telles e orientado pelo(a) Prof.(a) Dra. Maria Cristina Aranda.

Americana, SP
2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

TELLES, Larissa Bechedorf Silva

Tratamento de dados pessoais em microempresas. / Larissa Bechedorf Silva Telles – Americana, 2025.

33f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientadora: Profa. Dra. Maria Cristina Aranda

1. Análise de dados 2. Segurança em sistemas de informação 3. Sistemas de informação - governança. I. TELLES, Larissa Bechedorf Silva II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681516
681.518.5
681.518.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Larissa Bechedorf Silva Telles

Tratamento de dados pessoais em microempresas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 04 de dezembro de 2025.

Banca Examinadora:

Maria Cristina Aranda
Doutora
Fatec Americana "Ministro Ralph Biasi"

Cleberson Eugenio Forte
Doutor
Fatec Americana "Ministro Ralph Biasi"

Paula da Fonte Sanches
Mestre
Fatec Americana "Ministro Ralph Biasi"

DEDICATÓRIA

Dedico este trabalho à minha família, em especial aos meus pais, Carlos e Keila, e a minha irmã, Nayara. Este trabalho é o resultado do amor incondicional e do apoio constante que me deram em toda a minha trajetória. Minha profunda gratidão por me fornecerem a base e o incentivo para chegar até aqui, e, principalmente, por terem me concedido a liberdade e a autonomia para escolher o meu próprio caminho e seguir meus sonhos.

AGRADECIMENTOS

À professora doutora Maria Cristina Aranda, minha sincera e profunda gratidão. Aceitar a orientação deste trabalho de conclusão de curso foi o primeiro e mais significativo passo para que esta pesquisa se tornasse realidade. Agradeço imensamente por sua confiança, por ter aceito embarcar nesta jornada, e, sobretudo, pela paciência, dedicação e generosidade em compartilhar seu vasto conhecimento. Seus *insights* precisos, a orientação rigorosa e o incentivo constante foram cruciais para que eu pudesse superar os desafios inerentes à pesquisa e alcançar a conclusão deste projeto. Seu apoio não apenas moldou este trabalho, mas também contribuiu diretamente para a minha formação profissional e pessoal. Muito obrigado por ser a bússola que guiou esta trajetória.

À minha psicóloga, por ter sido um pilar fundamental de apoio emocional e inspiração. Sua orientação não apenas me ajudou a gerenciar a ansiedade e o estresse do processo, mas também foi fonte de ideias valiosas que nutriram minha resiliência e foco ao longo de toda a jornada da escrita.

Aos clubes do livro, capítulo 23, entre páginas viradas e reflorescer literário. Agradeço por terem proporcionado os preciosos e necessários momentos de relaxamento, desconexão e partilha de histórias que tornaram a árdua jornada da pesquisa e da escrita muito mais leve e prazerosa**.**

RESUMO

O presente texto conceitua e analisa o processo de adequação à lei geral de proteção de dados pessoais e as práticas de tratamento de dados pessoais em um microempreendedor individual do setor fotográfico, reconhecendo os desafios específicos de recursos enfrentados por micro e pequenas empresas para a conformidade legal. O objetivo central do trabalho visa diagnosticar o nível de maturidade em segurança da informação e conformidade legal de uma microempresa e, a partir desta avaliação, propor um plano de ação prático e realista para a mitigação de riscos e adequação a lei geral de proteção de dados pessoais. A metodologia desenvolvida adota o estudo de caso de natureza qualitativa e descritiva, utilizando o mapeamento de dados para traçar o fluxo de informações e um questionário diagnóstico para avaliar a governança e a infraestrutura de tecnologia da informação. Os resultados alcançados revelam que o principal ativo consiste em material visual e imagens classificados como dados sensíveis, e apontam um nível de maturidade baixo em segurança e conformidade. Esta baixa maturidade evidencia-se pela ausência de governança formal e por vulnerabilidades críticas na infraestrutura, como a dependência de mídias físicas não redundantes, o que expõe o negócio a perdas de dados e acessos indevidos já documentados. Para mitigar os riscos, o estudo propõe um plano de ação prático e escalável. Em conclusão, a pesquisa demonstra que a adequação à lei geral de proteção aos dados pessoais é plenamente viável para o microempreendedor por meio da implementação inteligente e priorizada dessas medidas, assegurando a proteção dos dados sensíveis dos clientes, a continuidade operacional e a reputação do negócio.

Palavras Chave: LGPD; governança de dados; segurança da informação.

ABSTRACT

The present text conceptualizes and analyzes the process of compliance with the general data protection law and the practices of personal data processing in a microentrepreneur within the photographic sector, recognizing the specific resource challenges faced by micro and small enterprises for legal compliance. The central objective of the work is to diagnose the level of maturity in information security and legal compliance of a microenterprise and, based on this assessment, to propose a practical and realistic action plan to mitigate risks and comply with the general data protection law. The developed methodology adopts a qualitative and descriptive case study, using data mapping to trace the information flow and a diagnostic questionnaire to evaluate governance and IT infrastructure. The results reveal that the main asset consists of visual material and images classified as sensitive data and indicate a low maturity level in security and compliance. This low maturity is evidenced by the absence of formal governance and critical vulnerabilities in the infrastructure, such as reliance on non-redundant physical media, which exposes the business to data loss and unauthorized access already documented. To mitigate the risks, the study proposes a practical and scalable action plan. In conclusion, the research demonstrates that compliance with the General Data Protection Law is fully viable for the microentrepreneur through intelligent and prioritized implementation of these measures, ensuring the protection of clients' sensitive data, operational continuity, and the business reputation.

Keywords: *LGPD; data governance; information security.*

SUMÁRIO

1 INTRODUÇÃO

Atualmente a sociedade está imersa na era da informação, um período caracterizado pela revolução tecnológica e pela transformação digital. Essa mudança impulsionou uma nova compreensão sobre o valor e a circulação de dados na economia e na vida social.

De acordo com Chiavenato (1999, *apud* Lemos, 2011), informação é “um conjunto de dados com um significado, que reduz a incerteza ou que aumenta o conhecimento a respeito de algo”. Essa definição reforça a importância da informação na era moderna, onde dados são gerados de modo constante, são processados e analisados para agregar valor e fornecer suporte a tomada de decisões em todos os níveis.

Nas últimas décadas, a Tecnologia da Informação (TI) tem evoluído rapidamente, trazendo mudanças significativas para diversos setores. A capacidade de transformar dados em informações valiosas tem permitido avanços notáveis na forma como se vive e trabalha.

A TI possibilitou a automação de processos, a melhoria da eficiência operacional e a criação de novas oportunidades de negócio, tendo desempenhado um papel fundamental na sociedade contemporânea. Porém, todo esse avanço tecnológico e a transformação digital resultaram em uma reestruturação do cenário empresarial.

Dessa forma, essa nova fase do mercado, colocou o tratamento de dados pessoais no centro das atividades para organizações de todos os portes. Nesse contexto, o Brasil estabeleceu um novo marco regulatório com a publicação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018).

O objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Ainda que a lei se aplique a todas as pessoas jurídicas de direito público ou

privado que realizam o tratamento de dados, o processo de adequação não é igual para todos.

Um bom exemplo dessa diferença são as empresas de pequeno porte (EPP) e as microempresas (ME), pois elas enfrentam desafios específicos para a se adequarem. A escassez de recursos financeiros, humanos e tecnológicos, junto à complexidade da legislação, acaba dificultando o processo de adaptação dessas organizações.

Reconhecendo essa realidade, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a Resolução CD/ANPD nº 2, de 27 de fevereiro de 2022, que flexibiliza ou dispensa obrigações específicas da LGPD para os agentes de tratamento de pequeno porte (Brasil, 2022). Ainda assim, mesmo com as flexibilizações, a conformidade ainda exige a adoção de medidas eficazes e a implementação de uma governança de dados.

De acordo com a CNN Brasil (2024) e o CartaCapital (2024), as micro, pequenas e médias empresas (MPMEs) representaram cerca de 30% do produto interno bruto (PIB) do país e foram responsáveis por mais de 50% dos empregos com carteira assinada no setor privado. Esse cenário evidencia a importância do tratamento de dados pessoais adequado nessas organizações, destacando a necessidade de compreender como as MPMEs estão implementando as diretrizes da LGPD em suas rotinas operacionais.

Dessa forma, o presente trabalho tem como objetivo principal analisar o processo de adequação à LGPD e as práticas de tratamento de dados pessoais em um microempreendedor individual (MEI) do setor fotográfico e apresentar soluções viáveis. Para alcançar o objetivo, a pesquisa se desenvolverá pela metodologia de estudo de caso, de natureza qualitativa e descritiva. Será apresentado o referencial teórico e em sequência o desenvolvimento do estudo. Esta abordagem permitirá uma análise detalhada da realidade da empresa estudada, identificando os principais desafios enfrentados, as soluções adotadas e o nível de conformidade alcançado no tratamento de dados sensíveis e não sensíveis de clientes, fornecedores e também de colaboradores.

2 REFERENCIAL TEÓRICO

2.1. Segurança da Informação

O termo Tecnologia da Informação recebeu as mais diversas definições, conforme afirma Lemos (2011). No início, a computação era considerada um mecanismo que possibilitava automatizar determinadas tarefas. Com a evolução da tecnologia, as máquinas se tornam cada vez menores e mais poderosas. Essa evolução levou à interação entre máquinas, fazendo com que os computadores passassem a lidar com informação ao invés de só automatizar tarefas. O termo TI foi definido por Lemos (2011) como "um conjunto de atividades e soluções providas por recursos de computação.”; em outras palavras, a TI é um conjunto de ações que os computadores fazem para resolver problemas e realizar tarefas.

No entanto, a crescente complexidade e interconexão dos sistemas de TI, trouxeram consigo novos desafios, como a necessidade de proteger a informação que circula por esses sistemas, (Santos e Silva, 2021). Diante desse contexto que surgiu a ramificação da TI, a área de Segurança da Informação.

Segurança da Informação é o campo que busca proteger os dados de acessos não autorizados, interrupções, modificações e destruições. Na era da informação, a proteção de dados tornou-se essencial. De acordo com O Committee on National Security Systems (CNSS), *apud* Whitman e Mattord (2011), Segurança da Informação é definida como sendo a “[...] proteção da informação e de seus elementos críticos, incluindo os sistemas e *hardware* que utilizam, armazenam e transmitem essa informação." Em outras palavras, o objetivo é a proteção contra adversários, aqueles que poderiam causar dano, intencional ou não.

A crescente dependência de sistemas digitais em todos os aspectos da vida moderna torna a segurança da informação um fator crítico para indivíduos e organizações, (Santos e Silva, 2021). Desse modo, Segurança da Informação torna-se a garantia de que suas informações permaneçam sempre seguras e disponíveis quando desejadas.

De acordo com Holdsworth e Kosinski (2024), em seu artigo publicado pela IBM, a Segurança da Informação é fundamentada em conceitos antigos, mas que se atualizam constantemente para acompanhar as ameaças cada vez mais sofisticadas. Eles também enfatizam a diferença entre termos comumente confundidos, como cibersegurança e segurança da informação, que embora interligados, possuem escopos diferentes.

Segundo a empresa de tecnologia Siemens, que atua na área de automação e digitalização industrial, infraestrutura, tecnologia predial e transporte, afirma que o termo segurança da informação possui significado abrangente, já que se trata da proteção de todos os dados sigilosos, sendo eles físicos ou digitais. Enquanto que o termo cibersegurança faz parte de uma segmentação específica da área de segurança da informação, sendo a área responsável por definir metodologias e tecnologias que serão usadas para a proteção de dados digitais.

Para garantir a integridade e a confidencialidade dos dados, normas como a ISO/IEC 27001:2022 são amplamente utilizadas, estabelecendo padrões internacionais para implementação de controles de segurança.

Nos últimos anos, a facilidade de acesso à informação também aumentou a exposição a riscos. Ataques cibernéticos, como *phishing*, *malware*, d*istributed denial of service* (DDoS) e *ransomware*, se tornaram cada vez mais sofisticados e frequentes. Esses ataques visam roubar dados pessoais, financeiros e corporativos, além de causar interrupções nos serviços e sistemas. Sendo assim, com o aumento desses ataques e a possível violação da segurança, podem acarretar grandes prejuízos financeiros e danos à reputação. Um exemplo notável foi o ataque à *Equifax* em 2017, onde informações pessoais de mais de 140 milhões de americanos foram comprometidas (Thomas, 2022). Portanto, a implementação de medidas de segurança robustas é essencial para a proteção de informações.

Para atender a essa necessidade de segurança e enfrentar as ameaças, a segurança de redes é fundamental, pois as redes são o coração da infraestrutura de TI, conectando dispositivos e permitindo a troca de informações. A segurança de redes se refere às políticas e práticas adotadas que consistem em medidas para dissuadir, prevenir, detectar e corrigir violações de segurança que envolvam a

transmissão de informações (Stallings, 2017). Em outras palavras, o principal objetivo da segurança de redes é proteger os ativos da rede contra ameaças como ataques de negação de serviço (DDoS), ataques *man-in-the-middle*, *malwares* e outros.

Um caso relevante foi o ataque DDoS contra o provedor de DNS *(domain name system)* Dyn em 2016, que derrubou grandes *sites*, como X (antigo *twitter*), *Spotify*, *Reddit*, *Airbnb* e *Vox*, ao explorar dispositivos IoT vulneráveis. O ataque fez com que os dispositivos infectados enviassem requisições de acesso simultâneas em um único ponto, o que causou sobrecarga e consequente queda do sistema. No caso desse ataque, o problema chegou a afetar outros *sites* pois os *hackers* miraram no gerenciamento de DNS, multiplicando o alcance e servindo como ponte para os *sites* afetados (O Globo, 2016).

Machado *et al*. (2019) afirmam que episódios como esse evidenciam como a falta de mecanismos de proteção efetivos pode gerar impactos de larga escala, atingindo não apenas empresas específicas, mas todo um ecossistema digital. Diante de situações como essa, cresce a preocupação com a segurança da informação e, principalmente, com a proteção dos dados pessoais dos usuários que circulam nesses ambientes, além da garantia de privacidade.

2.2 Criptografia

Para atender à crescente demanda por segurança e privacidade e proteger de modo eficaz as redes, a criptografia surge como um mecanismo fundamental. Ela pode ser definida como o estudo e aplicação de técnicas matemáticas que visam garantir aspectos fundamentais da segurança da informação, como confidencialidade, integridade, autenticação e verificação da origem. Segundo Barbosa *et al*. (2003), “criptografar significa transformar uma mensagem em outra (‘escondendo’ a mensagem original)”, desse modo, a mensagem original é escondida através de funções matemáticas, com o objetivo de dificultar o seu deciframento.

Como explicam Barbosa *et al*. (2003), existem duas classes de criptografia: a simétrica e a assimétrica, sendo que a criptografia simétrica utiliza uma única chave

tanto para cifrar quanto para decifrar a mensagem, já a assimétrica se baseia em um par de chaves, sendo uma pública e uma privada.

A criptografia simétrica utiliza apenas uma chave secreta para criptografar e decifrar informações, costuma ser usada para a transmissão de dados em massa, porque é mais simples e executa de forma mais ágil (Fortinet, [s.d.]).

A criptografia assimétrica, segundo informa o *site* da empresa de tecnologia especializada em soluções de segurança cibernética e rede, a Fortinet [s.d.], “uma chave é secreta e uma chave é pública. A chave pública é usada para criptografar dados e a chave privada é usada para descriptografar (e vice-versa).”

Conforme o desenvolvimento da tecnologia, as vantagens e desvantagens de ambos os tipos de criptografia, naturalmente surgiu um método que unisse as duas formas, afim de eliminar as desvantagens, são exemplos dessa união os protocolos TLS (*Transport Layer Security*) e SSL (*Secure Sockets Layer*), que busca compensar a lentidão do processamento (Castelló; Vaz, [s.d.]).

Para micro e pequenas empresas, a criptografia representa não somente uma medida de segurança técnica, mas também se torna um diferencial competitivo e se adequa aos novos padrões exigidos pelo mercado. Conforme afirma o *site* do Sebrae (2025), três a cada quatro vítimas de ciberataques são pequenas e médias empresas pois muitos não investem na proteção e muitos não sabem como agir quando são vítimas desse tipo de crime.

Após a pandemia de COVID-19, várias empresas modificaram sua forma de atuação, se tornando cada vez mais digitais (Microsoft, 2023). Segundo uma pesquisa publicada pela Microsoft em 2023 afirma que “a segurança cibernética é um dos principais desafios enfrentados, principalmente, pelos negócios de médio (37%) e pequeno porte (35%).”, onde empresas originalmente digitais enfrentaram mais problemas do que empresas não originalmente digitais.

No cenário brasileiro, algumas empresas vêm oferecendo soluções acessíveis de criptografia voltadas para essas empresas. Um dos exemplos é a empresa de segurança digital e segurança da informação, a Neotel, que lançou o serviço

“Criptografia as a Service”, que visa ajudar pequenas empresas a se adequarem à LGPD, oferecendo anonimização e criptografia de dados (Neotel, [s.d.]).

Outro exemplo é a empresa pioneira em cibersegurança e criptografia no Brasil, a Dinamo Networks, que por sua vez, desenvolveu a plataforma DINAMO Super Cloud, que disponibiliza criptografia e anonimização de dados em nuvem, permitindo que empresas de pequeno porte mantenham controle de suas chaves criptográficas e garantam conformidade com normas de segurança e privacidade (Dinamo Networks, 2021).

2.3 Inteligência Artificial

Em paralelo com os desenvolvimentos citados anteriormente, a Inteligência Artificial (IA), também cresceu. A IA é uma área da ciência da computação voltada para o desenvolvimento de sistemas que exibem características associadas à inteligência humana, como a tomada de decisões e o aprendizado. Conforme Feigenbaum (1981, *apud* Silva e Vanderlinde, [s. d.]), a IA se preocupa com a criação de agentes inteligentes, ou seja, sistemas que conseguem perceber o ambiente e tomar decisões que maximizem os seus objetivos.

De acordo com Russell e Norvig (2020), “O campo da inteligência artificial, ou IA, está preocupado não apenas em compreender, mas também em construir entidades inteligentes”.

Quando aplicada corretamente, a IA pode gerar inúmeros benefícios em áreas como saúde, educação, finanças e logística. Na área da saúde, por exemplo, ela é capaz de auxiliar no desenvolvimento de novos tratamentos médicos, diagnósticos precoces e personalização de tratamentos, sem substituir o julgamento clínico dos profissionais da saúde, como demonstrado em um estudo conduzido por graduandos em medicina, a IA comprovou sua eficiência em diagnosticar e monitorar o câncer de mama, proporcionando melhorias substanciais na precisão, sensibilidade e acurácia dos exames de imagem (Pellenz *et al*., 2024). Na educação, a IA pode personalizar o aprendizado, oferecer *feedback* em tempo real e automatizar tarefas administrativas, otimizando o processo de ensino (Luckin *et al*., 2016).

A história da IA remonta à década de 1950, quando Alan Turing publicou o artigo pioneiro *Computing Machinery and Intelligence*, no qual explorava a possibilidade de máquinas pensarem de maneira semelhante aos seres humanos (Turing, 1950 *apud* Gonçalves, 2024). No entanto, foi em 1955 que o campo da IA foi oficialmente estabelecido, durante um *workshop* de verão na Faculdade de *Dartmouth*, onde John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon, apresentaram o primeiro programa de IA, que simulava as habilidades de resolução de problemas de um ser humano (McCarthy *et al*., 1955 *apud* Possa, 2025). Esse evento é considerado o marco fundador da IA como área de estudo.

Outro marco significativo foi a criação do computador Deep Blue, desenvolvido pela IBM em 1997, que se tornou notável por derrotar o campeão mundial de xadrez Garry Kasparov, demonstrando o potencial da IA em tarefas complexas (Campbell *et al*., 2002). Em 2009, a criação do ImageNet marcou um avanço significativo, ao permitir que a IA reconhecesse objetos em imagens, abrindo novas possibilidades para o desenvolvimento de tecnologias como veículos autônomos e assistentes virtuais (Deng *et al*., 2009).

Desde então, a IA tem experimentado um crescimento exponencial, evoluindo para sistemas avançados capazes de realizar uma imensa variedade de tarefas, incluindo reconhecimento de voz, processamento de linguagem natural, robótica, e até mesmo a geração de imagens e vídeos realistas (Gomes, 2010).

A IA é frequentemente classificada em IA fraca e IA forte, onde a IA fraca tem seu foco em desempenhar uma tarefa específica, como fornecer a resposta a dúvidas baseado no *input* do usuário ou jogar xadrez. Ela depende da interferência humana para definir os parâmetros de seus algoritmos e para oferecer dados de treinamento relevantes a fim de assegurar a precisão (Duarte, 2024). Já a IA forte, tem capacidade semelhante ou superior à de um ser humano nas questões que envolvem entender, aprender e aplicar o conhecimento em diversas áreas, embora esse nível de IA seja teórico, atualmente (IBM, [s.d.]).

Para uma empresa fotográfica de pequeno porte, a IA pode trazer benefícios importantes, como automação da edição de imagens, personalização de *marketing* e aumento da produtividade. Ferramentas de IA, como o Adobe Photoshop com

preenchimento generativo e aplicativos como Remini, permitem que fotógrafos editem e melhorem fotos com rapidez e precisão, economizando tempo e recursos (CNN Brasil, 2025). Além disso, a IA auxilia na segmentação de clientes com base em padrões de comportamento, o que facilita a personalização da comunicação e a fidelização (Data Stone, 2024). A automatização de tarefas administrativas, como agendamento e resposta a clientes, pode reduzir custos operacionais e liberar a equipe para focar em atividades criativas e estratégicas (Sebrae, 2025).

Apesar dos benefícios, a adoção da IA apresenta riscos e malefícios. A dependência excessiva da IA pode criar vulnerabilidades operacionais caso os sistemas falhem, especialmente se processos críticos forem totalmente automatizados sem supervisão humana adequada (Alura, 2025). Há ainda questões éticas, como vieses nos algoritmos que podem prejudicar decisões, e riscos relacionados à proteção de dados pessoais, com possíveis multas severas em caso de descumprimento das leis como a LGPD (Alura, 2025). Empresas pequenas podem enfrentar dificuldades por falta de *expertise* para implementar a IA corretamente, o que pode levar a gastos extras e falhas técnicas (TOPdesk, 2024). Portanto, é fundamental que essas empresas façam uma adoção planejada da tecnologia, com avaliação cuidadosa dos custos, benefícios e riscos.

2.4 Lei Geral de Proteção de Dados Pessoais

Conforme apresentado, a intensificação dos ataques cibernéticos e o mau uso dos dados promoveram a criação de leis regulatórias voltadas à proteção da informação. De acordo com Garcia *et al*. (2020), “a privacidade já é uma garantia constitucional reafirmada em mecanismos legais de proteção, com destaque para o Marco Civil da Internet (Lei n. 12.965/2014) e a Lei do Consumidor (Lei n. 8.078/1990)”. Essa perspectiva demonstra que a preocupação com a privacidade e a segurança de dados já estava presente no ordenamento jurídico brasileiro, sendo posteriormente consolidada e ampliada com a LGPD.

A LGPD instituída pela Lei n. 13.709/2018, representa um marco regulatório no Brasil ao estabelecer regras para o tratamento de dados pessoais, com foco na proteção da privacidade e da liberdade dos indivíduos. Inspirada no regulamento geral

sobre a proteção de dados da união europeia (GDPR), a LGPD busca garantir maior transparência, segurança e responsabilidade no uso das informações pessoais pelas organizações.

Segundo o guia elaborado por Garcia *et al*. (2020), a LGPD aplica-se a qualquer pessoa física ou jurídica que realize o tratamento de dados pessoais, independentemente do porte da organização. Portanto, isso indica que micro e pequenas empresas também estão sujeitas às obrigações legais, ainda que enfrentem desafios maiores para adequação considerando a limitação de recursos financeiros e tecnológicos.

De acordo com a lei (Brasil, 2018), é fundamental diferenciar os conceitos de dados pessoais e dados pessoais sensíveis. Enquanto os primeiros abrangem informações que identificam ou podem identificar uma pessoa natural, como nome e CPF, os dados sensíveis referem-se a informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos (Lei n. 13.709/2018). Esses dados possuem maior potencial de discriminação e violação de direitos, exigindo tratamento mais rigoroso.

A autoridade nacional de proteção de dados (ANPD) publicou a resolução CD/ANPD n. 2/2022, que estabelece regras diferenciadas e simplificadas para agentes de tratamento de pequeno porte, reconhecendo a necessidade de reduzir a carga regulatória sobre microempresas, empresas de pequeno porte e *startups*. No entanto, essa flexibilização, não elimina a responsabilidade das organizações, mas procura adequar exigências como prazos de resposta a titulares e relatórios de impacto (ANPD, 2022).

3. ESTUDO DE CASO

O desenvolvimento deste trabalho será realizado através de um estudo de caso, conforme indicado por Gomes (2006), que se refere à investigação de situações envolvidas em um determinado ambiente, onde fatores diversos são observados em busca de evidências que descrevam uma determinada situação.

A empresa a ser estudada é classificada como microempreendedor individual, localizada na cidade de Jundiaí, no interior do estado de São Paulo, que possui uma população estimada de 443.221 habitantes (IBGE, 2022). A organização conta com 2 funcionários (o proprietário e um colaborador) e possui um faturamento anual inferior a R$81.000,00. A empresa exerce atividades de produção de fotografias, exceto aérea e submarina, com foco principal em serviços para o consumidor final. Os principais serviços prestados incluem acompanhamento infantil, ensaios de gestantes, sessões temáticas de época (páscoa, festa junina, natal, etc.), e cobertura de eventos sociais como batizados, aniversários e casamentos. O nome da empresa ou do empresário não será citado neste artigo por motivos éticos, a fim de não expor vulnerabilidades, informações confidenciais e demais informações sigilosas da mesma.

Para uma análise detalhada da segurança da informação e dos riscos cibernéticos envolvendo essa microempresa do ramo fotográfico, serão adotadas diversas atividades relacionadas à gestão adequada dos dados pessoais, junto com as boas práticas recomendadas pela LGPD. Para isso, o mapeamento de dados é o ponto inicial dessa metodologia, que consiste em identificar onde e como os dados pessoais de clientes e colaboradores são coletados, armazenados e utilizados. Essa etapa é fundamental para compreender o fluxo e a exposição potencial dessas informações, que incluem desde imagens e dados de contato até mesmo informações financeiras.

Foi identificado que o principal ativo de dados desta microempresa é composto por dados pessoais e dados sensíveis de seus clientes e colaboradores. No contexto da prestação de serviços fotográficos, a coleta abrange as seguintes categorias de informação:

- Imagens e material visual (dados sensíveis): As fotografias e vídeos produzidos, que, por retratarem características físicas e aspectos íntimos (como gestação e eventos pessoais), são o foco da gestão de dados sensíveis.
- Dados de identificação e contato (comuns): Incluem nome, CPF, endereço e *e-mail* dos clientes e responsáveis.
- Informações contratuais e financeiras (comuns): Englobam os contratos de prestação de serviços e dados de pagamento.
- Autorização de uso de imagem (consentimento específico): Documentos formais para a utilização do trabalho em portfólio.
- Dados do colaborador (comuns e sensíveis): Informações de identificação, registro e, se aplicável, saúde do funcionário.

A infraestrutura de TI da microempresa é composta por recursos básicos, o que simplifica a operação, mas concentra riscos. O ambiente é sustentado por um *laptop* para a edição e gerenciamento de arquivos, complementado por um servidor local de baixo porte utilizado principalmente como *backup* e repositório primário. O armazenamento dos arquivos brutos de alta resolução, que incluem os dados sensíveis de imagem, é realizado majoritariamente em dois discos rígidos (HDs) externos, além dos cartões de memória das câmeras. A organização do fluxo de trabalho e o tratamento das imagens são realizados por meio dos *softwares* Lightroom e Photoshop da empresa multinacional de tecnologia desenvolvedora de *softwares* de criação, *marketing*, e gerenciamento de documentos, a Adobe, e também do Google Drive, plataforma da empresa multinacional de tecnologia com foco em serviços online, software e computação em nuvem, a Google.

A infraestrutura de TI da microempresa e o tratamento de dados não estão alheios à evolução tecnológica. O MEI faz uso de *softwares* modernos, como os já citados anteriormente, e que são cada vez mais impulsionados por recursos de inteligência artificial e aprendizado de máquina para tarefas como seleção automática de objetos, retoque de pele, remoção de fundo e marcação inteligente de fotos. Essa dependência de IA, que utiliza os dados de imagem dos clientes para treinar e executar algoritmos, eleva a complexidade do tratamento de dados. A IA transforma as fotos (dados pessoais sensíveis) em *inputs* e *outputs* de processamento automatizado, introduzindo novos vetores de risco, como o potencial de vieses

algorítmicos e a dificuldade em garantir o controle total sobre como esses dados são processados e retidos pelos provedores de *software*. Portanto, a conformidade com a LGPD deve considerar as obrigações relacionadas ao tratamento automatizado de dados e a necessidade de garantir que os termos de serviço dos editores de foto estejam alinhados com a política de privacidade da microempresa.

Além dos desafios impostos pelo processamento via inteligência artificial, a própria simplicidade e a fragilidade dos ativos físicos e lógicos que compõem a infraestrutura básica da microempresa também introduzem um conjunto de vulnerabilidades diretas.

A dependência dessa infraestrutura simples expõe a empresa a ameaças significativas, sendo elas:

- Ameaças físicas: A segurança dos HDs externos, do *laptop* e dos cartões de memória está vulnerável a perda, roubo ou dano físico (como incêndios ou inundações), o que resultaria na perda irrecuperável de dados do cliente.
- Ameaças cibernéticas: A falta de *backups* em nuvem robustos ou criptografia adequada pode levar a riscos de ataques de *ransomware* (sequestro de dados) e vazamento de informações confidenciais a partir do servidor ou *laptop*.
- Vulnerabilidades de processo: A movimentação constante de arquivos entre cartões, *laptop*, servidor e HDs externos cria pontos de falha e aumenta o risco de erros humanos como exclusão acidental ou manuseio incorreto dos dados, também pode facilitar o acesso não autorizado quando armazenado incorretamente.

Apesar da infraestrutura simplificada, a microempresa está sujeita a uma variedade de ameaças à segurança da informação que comprometem a confidencialidade e a disponibilidade dos dados. As principais ameaças identificadas incluem: acesso não autorizado (seja por falha na gestão de senhas ou invasão de sistemas), a perda ou indisponibilidade de dados (devido a falhas de *hardware* ou erros humanos) e ataques cibernéticos como o uso de *malware* e golpes de *phishing*, que visam roubar credenciais de acesso ou infectar o *laptop* e o servidor.

Como medidas de segurança e mitigação de riscos atuais, a empresa conta com os seguintes controles:

1. Antivírus: A instalação e atualização regular de um *software* antivírus no *laptop* e, possivelmente, no servidor, que atua como uma barreira inicial contra *malware* conhecido.
2. Autenticação de dois fatores: A utilização da autenticação de dois fatores em plataformas-chave (como *e-mail* e sistemas de armazenamento em nuvem) eleva a proteção contra o acesso não autorizado, mesmo que uma senha seja comprometida.
3. Seguro de equipamentos: A contratação de seguro para as câmeras fotográficas mitiga o risco financeiro de perda, roubo ou dano desses ativos, garantindo a continuidade da operação.

No entanto, é crucial notar que, embora o seguro proteja o equipamento, a dependência excessiva de HDs externos e a ausência de uma rotina de *backup* robusta continuam a representar uma falha na proteção dos dados sensíveis dos clientes e na conformidade com a LGPD.

A relevância do estudo sobre segurança da informação é acentuada pelos incidentes já vivenciados pela microempresa, que ilustram a materialização dos riscos de falha humana e vulnerabilidade física. Os eventos mais notórios incluem:

- Falha humana e acesso indevido (vazamento de *link*): Em uma ocasião, um erro humano no processo de envio resultou no compartilhamento de um *link* de entrega de fotos incorreto para um cliente. Embora o *link* não tenha dado acesso a todo o portfólio, ele permitiu que o cliente visualizasse, momentaneamente, o conteúdo destinado a outra pessoa, configurando um incidente de acesso não autorizado e quebra de confidencialidade dos dados de imagem.
- Perda física de dados (cartão de memória): Houve um incidente de perda de dados resultante do sumiço de um cartão de memória da câmera. Por ser o ponto inicial de armazenamento das fotos, esse evento representou a perda total e irrecuperável do material fotográfico de um cliente, afetando a disponibilidade dos dados e o cumprimento do contrato.

Esses incidentes demonstram que, mesmo em operações de pequena escala, a ausência de controles de processo e a dependência de mídias físicas elevam o risco

de comprometer a integridade e a confidencialidade dos dados pessoais, independentemente de ataques cibernéticos externos.

Para realizar uma avaliação aprofundada da maturidade em segurança da informação e da conformidade com a LGPD no contexto da microempresa, foi desenvolvido um questionário direcionado aos funcionários, apresentado a seguir, o qual está estruturado em duas partes: a tabela 1, que avalia o estado atual de proteção de dados e a governança interna, e a tabela 2, que identifica as ameaças, suas consequências e o caminho para a conformidade. Esta abordagem metodológica visa diagnosticar não apenas os controles de segurança técnica em vigor, mas também a percepção do empresário sobre os riscos e a sua capacidade de resposta a incidentes.

As perguntas, contidas nessas tabelas, foram estruturadas para abordar as vulnerabilidades identificadas na infraestrutura de TI, os controles de proteção de dados sensíveis e os desafios inerentes à operação de um MEI no ramo fotográfico.

Tabela 1 – Controles atuais e governança

Perguntas	Respostas
1. A empresa possui uma política de segurança da informação atualmente? (governança e documentação).	Não, a empresa não possui uma política de segurança da informação definida e formalizada. A ausência de um documento ou manual estabelecido resulta na dependência de práticas informais e eleva o risco de erros humanos e inconsistências no tratamento dos dados.
2. As informações da empresa estão sempre disponíveis quando o proprietário ou pessoas autorizadas necessitam? (disponibilidade)	Não, a disponibilidade é um ponto de falha. O histórico de perda de dados (sumiço de cartão de memória) e a dependência de HDs externos demonstram que a indisponibilidade de dados (fotos de clientes) é uma ocorrência real. O *backup* não é robusto nem segue padrões recomendados, comprometendo o acesso em caso de falha de *hardware* ou incidente.
3. A empresa cuida da integridade das informações, possuindo algum controle para que as informações não sejam manipuladas indevidamente? (integridade)	Os controles de integridade são mínimos. A empresa utiliza autenticação de dois fatores e depende da proteção básica do antivírus. Não há mecanismos avançados de controle de acesso ou trilhas de auditoria para garantir que as fotos originais (*raw files*) e os contratos não sejam alterados indevidamente após o registro inicial.
4. Como a empresa protege seus dados sensíveis atualmente? (controles existentes)	A empresa utiliza controles de segurança básicos: Antivírus instalado no *laptop* e servidor e autenticação de dois fatores ativada em plataformas-chave (*e-mail*, armazenamento em nuvem). Há também a contratação de seguro para as câmeras fotográficas, que mitiga o risco financeiro de perda dos ativos físicos, mas não protege diretamente os dados dos clientes.

Fonte: Próprio autor

Tabela 2 – Riscos e melhorias

Perguntas	Respostas
1. Quais são os principais riscos de segurança da informação para a empresa de fotografia? (identificação de ameaças)	Os riscos se concentram em falhas operacionais e vulnerabilidades da infraestrutura básica: Perda e Indisponibilidade de dados (falha de HDs externos ou sumiço de mídias), falha humana (erro no envio de *links*, manuseio incorreto de arquivos), acesso não autorizado e vazamento (incidentes como o envio de *link* errado), ataques cibernéticos (*malware, ransomware, phishing)* e vulnerabilidade física (roubo de *laptop* ou HDs).
2. Quais as consequências de uma violação de segurança para a empresa? e para os clientes? (impacto)	Para a empresa: Prejuízo à reputação (principalmente após um vazamento de fotos), perdas financeiras (necessidade de refazer o trabalho ou indenizações), multas e penalidades legais (em caso de não conformidade com a LGPD) e interrupção das operações (após um ataque de *ransomware* ou perda de dados essenciais). Para os clientes: exposição da privacidade (vazamento de fotos íntimas ou sensíveis de família, gestantes, etc.) e dano moral resultante da quebra de confiança e da manipulação indevida de suas imagens.
3. Como a empresa pode melhorar sua segurança da informação? (recomendações)	As melhorias devem focar em robustez e governança: implementação da regra de *backup* 3-2-1 (três cópias, em duas mídias diferentes, sendo uma externa/nuvem), adoção de criptografia em HDs externos e no servidor, elaboração de uma política de segurança da informação e a instituição de um programa de conscientização sobre LGPD e *phishing* para o proprietário/colaborador.
4. Quais são as dificuldades enfrentadas para implementação das melhorias propostas? (barreiras)	As principais dificuldades para um MEI são: custo elevado (soluções de *backup* em nuvem, *softwares* de segurança avançados), falta de tempo/recursos humanos (o proprietário acumula funções e não tem tempo dedicado à gestão de TI e segurança) e baixa priorização (a segurança é vista como custo, e não como investimento ou diferencial competitivo).

Fonte: Próprio autor

Com base na análise das respostas dos questionários, da infraestrutura, dos controles existentes e do histórico de incidentes, a microempresa do setor fotográfico é classificada em um nível baixo em segurança da informação e conformidade com a LGPD. Essa posição é justificada pela adoção de controles mínimos e insuficientes para a mitigação dos riscos.

O plano de ação para elevar a segurança da microempresa e garantir a conformidade com a LGPD requer a implementação de medidas protetivas detalhadas em três frentes: governança, infraestrutura e controles de acesso. A seguir, serão apresentadas duas soluções para cada problema enfrentado, sendo uma das propostas considerada a ideal e a outra que se encaixa no orçamento da microempresa.

- No que se refere a governança:

A prioridade máxima é a criação de uma política de segurança da informação completa, que não apenas defina a postura da empresa, mas também estabeleça os procedimentos para o tratamento de dados, retenção e descarte (LGPD).

A proposta ideal focada na excelência e na garantia de *compliance* completo sugere que a microempresa deve contratar uma consultoria especializada para gerenciar a conformidade e os riscos de forma contínua. A contratação de uma consultoria é justificada pela ausência de um departamento de TI ou jurídico dedicado,

dessa forma também há a interpretação legal precisa, pois, a consultoria possui conhecimento aprofundado sobre a LGPD e sobre o órgão regulador, a ANPD. A consultoria também pode fornecer um olhar externo e imparcial afim de identificar vulnerabilidades e riscos que a gestão interna pode ignorar. O MEI também se beneficia com a contratação de uma consultoria, pois mantém seu foco na atividade principal (a produção de fotografias e atendimento ao cliente) enquanto a terceirizada faz o mapeamento de dados, implementa a política de segurança da informação (PSI) e estabelece a política de privacidade através de metodologias e ferramentas já definidas.

Portanto a consultoria seria responsável pela elaboração formal e completa da PSI e da política de privacidade, além da criação do registro de operações de tratamento de dados pessoais, que é um inventário detalhado de onde, como e por que os dados são tratados. Essa abordagem garantiria a precisão legal dos documentos, o desenvolvimento de um programa de treinamento formal e recorrente para os funcionários e a implementação de uma plataforma de GRC (governança, risco e conformidade) para monitoramento centralizado de políticas e acessos.

Em contraste com a solução de consultoria externa, a proposta que melhor se encaixa para o MEI e que é proposta por esse estudo, tem como prioridade a praticidade, o baixo custo e a facilidade de manutenção pelo próprio proprietário, portanto o próprio MEI deve focar na criação de um guia de boas práticas e segurança interna, um documento simplificado e de linguagem acessível, que cumpra a função de PSI, mas que seja focado em regras operacionais diárias (como gestão de senhas, manuseio seguro de *links* de entrega e procedimentos de *backup*). Para o inventário de dados, o estudo propõe utilizar uma planilha digital simples, mas que possuam formas de proteção como bloqueio de planilhas e/ou controle de acesso (Excel ou Google Sheets) para mapear os dados coletados (cliente, colaborador, financeiro), indicando o responsável, a finalidade do uso e o prazo de retenção/descarte, transformando o registro de operações de tratamento de dados pessoais em um controle básico, mas funcional. Essa solução estabelece uma cultura de segurança e atende aos princípios básicos da LGPD sem sobrecarregar o orçamento ou o tempo do microempresário.

- Em relação à infraestrutura,

Considerando o diagnóstico de vulnerabilidades e visando o restabelecimento integral dos pilares da segurança da informação (confidencialidade, disponibilidade, integridade e autenticidade), a proposta ideal para a infraestrutura busca, através da implementação de sistemas de nível empresarial, a robustez necessária. Para a confidencialidade e autenticidade, seria instalada uma solução paga e robusta de detecção e resposta de *endpoint* (EDR) no *laptop* e servidor, complementada por acesso remoto seguro via VPN (rede privada virtual), garantindo monitoramento e *patch management* centralizados. A disponibilidade e integridade seriam asseguradas pela implementação de um serviço de *backup* gerenciado híbrido (por exemplo, Acronis ou Veeam), que replicaria os dados em tempo real para a nuvem (*cloud*) e para um Storage Attached Network (SAN) local, garantindo a recuperação rápida e a imutabilidade dos dados. Por fim, para a segurança de perímetro e controle de acesso, seria adquirido e configurado um *firewall* de *hardware* (UTM/NGFW) robusto, separando o negócio da rede doméstica.

Já a proposta que este estudo propõe e que melhor se adapta ao MEI foca na maximização da segurança com recursos acessíveis e processos de fácil manutenção. Para garantir a confidencialidade e a autenticidade, o foco recai no uso obrigatório da criptografia de disco completa (BitLocker) em todo o *laptop* e nos discos de *backup* SSDs, combinada com a migração da autenticação de dois fatores para um aplicativo gerador de código externo em todos os serviços *online*. A disponibilidade e integridade seriam restauradas através da implementação da regra de *backup* 3-2-1 (Kingston, 2025) utilizando: SSDs criptografados (cópia local), serviço de *cloud* pago (para a cópia *off-site*) e a utilização de um *software* de *backup* simples que realize a verificação de *checksum* (EaseUS) após cada cópia. Estruturalmente, a substituição dos HDs por SSDs aumenta a resistência física, e o particionamento do disco do *laptop*, juntamente com o uso de um *firewall* de *software* configurado de forma restritiva (Windows Defender), protege o perímetro. Essa solução, embora de baixo custo, exige a formalização do processo no guia de boas práticas para assegurar que os processos sejam mantidos e auditados periodicamente.

- Os controles de segurança e acesso

A segurança de acesso é fundamental para proteger os dados sensíveis de clientes e a propriedade intelectual da empresa. A proposta ideal para este tópico exige a implementação de soluções de nível corporativo. A base seria a adoção de um sistema de gerenciamento de identidade e acesso (GdA), como o Azure Active Directory ou similares, para centralizar a criação e o controle de usuários. Isso permitiria a aplicação rigorosa do princípio do privilégio mínimo, garantindo que o colaborador só acesse pastas e *links* estritamente necessários para a sua função, o que teria impedido o vazamento de *link* por erro humano. Adicionalmente, o GdA possibilitaria a revisão periódica e automatizada de acessos e a emissão de relatórios de auditoria detalhados, registrando quem acessou qual arquivo, quando e de onde, garantindo a plena autenticidade e integridade do registro de acesso.

No entanto, a proposta que este estudo sugere, foca em ferramentas de baixo custo e alta eficácia. O ponto de partida é a migração da autenticação de dois fatores para um aplicativo gerador de código externo (como Google Authenticator) para todos os serviços essenciais (*e-mail*, Google Drive, Lightroom), abandonando métodos menos seguros como SMS. Em termos de controle de acesso, a solução prática é a implementação manual do princípio do privilégio mínimo através do uso diligente de recursos nativos dos sistemas: a criação de contas de usuário separadas e não administradoras no *laptop* para o colaborador e o proprietário, e a gestão de permissões restritivas (somente leitura ou acesso temporário) nos serviços de armazenamento em nuvem (como o Google Drive). Essa abordagem exige a revisão de acessos feita manualmente e de forma periódica (mensal, por exemplo), garantindo a confidencialidade sem a necessidade de software de gerenciamento complexo.

4. CONSIDERAÇÕES FINAIS

O presente trabalho se propôs a analisar o processo de adequação à LGPD e as práticas de tratamento de dados pessoais em um microempreendedor individual do setor fotográfico, através da metodologia de estudo de caso, de natureza qualitativa e descritiva. A abordagem permitiu uma análise detalhada da realidade operacional da empresa, confirmando que, embora a operação seja de pequena escala, a complexidade no tratamento de dados sensíveis, como imagens de clientes, expõe o negócio a riscos significativos. O diagnóstico revelou um nível de maturidade básico em segurança e conformidade, caracterizado pela ausência de governança formal e por vulnerabilidades críticas na infraestrutura, como a dependência de mídias físicas não redundantes, que resultou em perdas de dados já documentadas. Identificou-se que a maior parte dos desafios enfrentados pelo MEI reside no contraste entre a necessidade de controles rigorosos e a limitação de recursos financeiros e de tempo.

Para endereçar esses desafios e reestabelecer os pilares de confidencialidade, disponibilidade, integridade e autenticidade, foram propostas soluções práticas e eficazes, equilibrando o ideal técnico com a realidade orçamentária do MEI. As sugestões abrangem desde a implementação de um *backup* híbrido 3-2-1 e o uso de criptografia de disco completa em todos os ativos, até a adoção de controles de acesso reforçados por autenticação de dois fatores via aplicativo externo. No pilar de governança, a solução adequada consistiu na criação de um guia de boas práticas e na adequação contratual para obter consentimento explícito, medidas que garantem a adequação com a LGPD.

Em suma, a transição da microempresa de uma postura reativa para uma proativa, com a adoção dessas medidas, demonstra que a adequação à LGPD é plenamente viável para pequenos negócios, desde que as ações sejam priorizadas de forma inteligente e escalável. O estudo de caso serviu, portanto, não apenas para identificar as falhas, mas para construir um plano de ação robusto que eleva o nível de conformidade e protege o principal ativo da empresa, os dados pessoais e sensíveis de seus clientes, assegurando a continuidade e a reputação do negócio no mercado.

REFERÊNCIAS

ALURA. **Os 10 maiores riscos da inteligência artificial**. 2025. Disponível em: https://www.alura.com.br/empresas/artigos/riscos-da-ia. Acesso em: 7 out. 2025.

BARBOSA, Luís Alberto de Moraes; BRAGHETTO, Luís Fernando B.; BRISQUI, Marcelo Lotierso; SILVA, Sirlei Cristina da. **RSA – criptografia assimétrica e assinatura digital**. Campinas: Universidade Estadual de Campinas, 2003. Acesso em: 30 set. 2025.

BRASIL. Presidência da República. **Lei n. 8.078, de 11 de setembro de 1990**. **Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor).** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 12 out. 2025.

BRASIL. Presidência da República. **Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco Civil da Internet)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 ago. 2025.

BRASIL. Presidência da República. **Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais - LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 ago. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 2, de 27 de janeiro de 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. Disponível em: 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. Acesso em: 22 ago. 2025.

BRASIL. Instituto Brasileiro de Geografia e Estatística. Jundiaí (SP) | **Cidades e Estados**. Disponível em: https://www.ibge.gov.br/cidades-e-estados/sp/jundiai.html. Acesso em: 12 nov. 2025.

CAMPBELL, Murray; HOANE, A. Joseph; HSU, Feng-Hsiung. Deep Blue. **Artificial Intelligence,** v. 134, n. 1-2, p. 57-83, jan. 2002.

CASTELLÓ, Thiago; VAZ, Verônica. **Assinatura digital**. Universidade Federal do Rio de Janeiro, Rede de Computadores I. Disponível em: https://www.gta.ufrj.br/grad/07_1/ass-dig/index.html. Acesso em: 12 out. 2025.

CNN BRASIL. **Conheça 5 ferramentas que usam IA para facilitar a edição de fotos**. 2025. Disponível em: https://www.cnnbrasil.com.br/tecnologia/conheca-5-ferramentas-que-usam-ia-para-facilitar-a-edicao-de-fotos/. Acesso em: 7 out. 2025.

DATA STONE. **Inteligência artificial na prospecção de negócios:** o futuro é agora**!** 30 jan. 2024. Disponível em: https://datastone.com.br/blog/2024/01/30/inteligencia-artificial-na-prospeccao-de-negocios/. Acesso em: 10 out. 2025.

DENG, Jia et al. ImageNet: a large-scale hierarchical image database. **IEEE Conference on Computer Vision and Pattern Recognition**, 2009. Disponível em: https://www.image-net.org/static_files/papers/imagenet_cvpr09.pdf. Acesso em: 7 out. 2025.

DIAS, Maria Clara. **Cinco dados que comprovam a importância dos pequenos negócios para o Brasil**. CNN Brasil, São Paulo, 23 jun. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/cinco-dados-que-comprovam-a-importancia-dos-pequenos-negocios-para-o-brasil/. Acesso em: 20 out. 2025.

DUARTE, Julio. **IA fraca...IA forte-ai**. DIO, 25 fev. 2024. Disponível em: https://www.dio.me/articles/ia-fraca-ia-forte-ai-asi. Acesso em: 14 nov. 2025.

DINAMO NETWORKS. **DINAMO Super Cloud**. 2021. Disponível em: https://dinamonetworks.com/dinamo-networks-lanca-plataforma-mundial-de-criptografia-e-lgpd-em-nuvem/. Acesso em: 12 out. 2025.

FORTINET. **O que é criptografia? Definição, importância, tipos**. [S.l.: s.n.], [s.d.]. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/what-is-cryptography. Acesso em: 30 set. 2025.

GARCIA, Lara Rocha et al. **Lei geral de proteção de dados pessoais (LGPD):** guia de implantação. São Paulo: Edgard Blücher, 2020.

GOMES, Dennis dos Santos. Inteligência Artificial: Conceitos e Aplicações**. Revista Olhar Científico – Faculdades Associadas de Ariquemes**, Ariquemes, v. 1, n. 2, ago./dez. 2010. Disponível em: https://www.professores.uff.br/screspo/wp-content/uploads/sites/127/2017/09/ia_intro.pdf. Acesso em: 30 set. 2025.

GOMES, J. S. **O método de estudo de caso aplicado à gestão de negócios**. 1. ed. São Paulo: Atlas, 2006.

GONÇALVES, Bernardo. Turing's Test, a Beautiful Thought Experiment. **IEEE Annals of the History of Computing**, v. 46, n. 3, p. 1-13, 2024. Disponível em: https://www.computer.org/csdl/magazine/an/2024/03/10614793/1Z0o1iK0CY0. Acesso em: 12 nov. 2025.

IBM. **O que é a segurança da informação?** 26 jul. 2024. Colaboradores: Jim Holdsworth, Matthew Kosinski. Disponível em: https://www.ibm.com/br-pt/think/topics/information-security. Acesso em: 7 out. 2025.

IBM. **O que é inteligência artificial (IA)?** 2024. Disponível em: https://www.ibm.com/br-pt/think/topics/artificial-intelligence. Acesso em: 7 out. 2025.

ISO/IEC. ISO/IEC 27001:2022: **Sistemas de gestão da segurança da informação.** Disponível em: https://www.27001.pt/. Acesso em: 15 out. 2025.

KINGSTON. **The 3-2-1 data backup method**: your best defense. Disponível em: https://www.kingston.com/br/blog/data-security/321-data-backup-method. Acesso em: 12 nov. 2025.

LEMOS II, Dalton Luiz. **Tecnologia da informação**. 2. ed. Florianópolis: Publicações do IF-SC, 2011.

LUCKIN, Rosemary et al. **Intelligence unleashed:** an argument for AI in education. London: Pearson, 2016.

MACHADO, Rodrigo; KREUTZ, Diego; PAZ, Giulliano; RODRIGUES, Gustavo. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. **Anais da XVII Escola Regional de Redes de Computadores (ERRC)**, Alegrete, RS, 17., 2019. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 154-159. DOI: https://doi.org/10.5753/errc.2019.9230.

MICROSOFT. **10 insights essenciais do relatório de defesa digital da microsoft de 2023**. 2023. Disponível em: https://www.microsoft.com/pt-br/security/security-insider/emerging-threats/microsoft-digital-defense-reports/10-essential-insights-from-the-microsoft-digital-defense-report-2023. Acesso em: 13 out. 2025.

NEOTEL. **Segurança digital e segurança da informação**. [S.l.: s.n.], [s.d.]. Disponível em: https://blog.neotel.com.br/sem-categoria/neotel-lanca-servico-de-criptografia-as-a-service-para-as-pmes-a-se-adequarem-a-lgpd/. Acesso em: 13 out. 2025.

O GLOBO. **Ataque de 'cibercriminosos' tirou grandes sites do ar nos EUA, incluindo Twitter e Spotify**. 21 out. 2016. Disponível em: https://oglobo.globo.com/economia/ataque-hacker-derruba-parte-da-internet-nos-eua-20332302. Acesso em: 14 out. 2025.

PELLENZ, André Eduardo et al. Aplicação da inteligência artificial no diagnóstico e monitoramento do câncer de mama. **Brazilian Journal of Health Review**, v. 7, n. 3, p. 231-240, 2024. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJHR/article/view/73198. Acesso em: 7 out. 2025.

POSSA, Alisson. O papel das escolhas humanas no desenvolvimento da IA. **JOTA Portal**, Colunas IA, Regulação e Democracia, 24 set. 2025. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/o-papel-das-escolhas-humanas-no-desenvolvimento-da-ia. Acesso em: 13 nov. 2025.

RAVAGNANI, Allan. Micro, pequenas e médias empresas impulsionam a economia brasileira. **CartaCapital**, São Paulo, 5 out. 2024. Disponível em: https://www.cartacapital.com.br/do-micro-ao-macro/micro-pequenas-e-medias-empresas-impulsionam-a-economia-brasileira/. Acesso em: 20 out. 2025.

RUSSELL, Stuart; NORVIG, Peter**. Artificial intelligence:** a modern approach. 4. ed. Upper Saddle River: Prentice Hall, 2020.

SANTOS, Rogério Batista dos; SILVA, Tiago Barros Pontes e. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. RDBCI: **Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 19, n. 00, p. e021024, 2021. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8665529. Acesso em: 12 nov. 2025.

SEBRAE. **Cibersegurança para pequenas empresas**: proteja seus dados. Atualizado em 05 fev. 2025. Disponível em:https://sebrae.com.br/sites/PortalSebrae/ufs/pe/artigos/ciberseguranca-para-pequenas-empresas-proteja-seus-dados,d90dcfe35d7d4910VgnVCM1000001b00320aRCRD. Acesso em: 14 nov. 2025.

SEBRAE. **IA nas pequenas empresas**: ferramentas inteligentes. 2025. Disponível em: https://sebrae.com.br/sites/PortalSebrae/ufs/am/artigos/ia-nas-pequenas-empresas-ferramentas-inteligentes,28d5b840c93d5910VgnVCM1000001b00320aRCRD. Acesso em: 7 out. 2025.

SIEMENS. **As diferenças entre cibersegurança e segurança da informação**. Disponível em: https://www.siemens.com/br/pt/empresa/stories/cidades/ciberseguranca-e-seguranca-da-informacao.html. Acesso em: 14 ago. 2025

SILVA, Brigiane Machado da; VANDERLINDE, Marcos. **Inteligência artificial e aprendizado de máquina**. Trabalho apresentado à disciplina de Metodologia da Pesquisa Científica, UDESC – Universidade do Estado de Santa Catarina, [s. d.]. Disponível em: https://www.ceavi.udesc.br/arquivos/id_submenu/387/brigiane_machado_da_silva___marcos_vanderlinde.pdf. Acessado em 30 set. 2025.

STALLINGS, William. **Network security essentials:** applications and standards. 6. ed. Malaysia: Pearson, 2017.

THOMAS, Jason E. **A case study analysis of the Equifax data breach**. 2022.

TOPDESK. **Riscos da IA:** entenda os desafios e como mitigá-los. 2024. Disponível em: https://www.topdesk.com/pt/blog/investir-em-ia-riscos-que-nao-devem-ser-ignorados/. Acesso em: 7 out. 2025.

WHITMAN, Michael E.; MATTORD, Herbert J. **Management of information security**. 3. ed. Boston: Course Technology, Cengage Learning, 2011.